



Legislation and practice of foreign countries in the field of digital forensics

Bekzod ATAKULOV¹

Azim BARATOV²

Tashkent State Law University

ARTICLE INFO

Article history:

Received February 2021

Received in revised form

28 February 2022

Accepted 20 March 2022

Available online

15 April 2022

Keywords:

cyber forensics,
digital evidence,
cyber security,
digital forensics,
hashing,
electronic data.

ABSTRACT

This article analyzes some aspects of the practice and legislation regarding digital forensics in some foreign countries. In addition, the article focuses mainly on the practice of using digital evidence and highlights the rules for collecting, examining, evaluating and submitting digital evidence to court. Questions regarding methods for ensuring and evaluating the integrity of digital evidence are also considered.

2181-1415/© 2022 in Science LLC.

DOI: <https://doi.org/10.47689/2181-1415-vol3-iss3/S-pp557-562>

This is an open access article under the Attribution 4.0 International (CC BY 4.0) license (<https://creativecommons.org/licenses/by/4.0/deed.ru>)

Raqamli kriminalistikaga oid xorijiy mamlakatlar qonunchiligi va amaliyoti

Kalit so'zlar:

kiber kriminalistika,
raqamli dalillar,
kiber xavfsizlik,
raqamli ekspertiza,
xeshlash,
elektron dalillar

ANNOTATSIYA

Ushbu maqolada ayrim xorijiy mamlakatlarning raqamli kriminalistika bo'yicha amaliyoti va qonunchiligining ba'zi jihatlari tahlil qilingan. Ushbu maqolada, asosan, raqamli dalillardan foydalanish amaliyoti bilan bog'liq bo'lib, unda raqamli dalillarni to'plash, tekshirish, baholash hamda sudga taqdim etish bilan bog'liq qoidalar yoritilgan. Shuningdek, raqamli dalillarning yaxlitligini ta'minlash va baholash usullari tadqiq etilgan.

¹ Master's student at Tashkent State Law University. Tashkent, Uzbekistan. E-mail: bekatakuloff@gmail.com.

² PhD, head of the department of Criminalistics and forensic examination, Tashkent state university of law, Tashkent, Uzbekistan

Законодательство и практика зарубежных стран в области цифровой криминалистики

АННОТАЦИЯ

Ключевые слова:

кибер криминалистика,
цифровые доказательства,
кибербезопасность,
цифровая экспертиза,
хэширование,
электронные данные.

В данной статье анализируются некоторые аспекты практики и законодательства касательно цифровой криминалистики некоторых зарубежных стран. Кроме того, в статье рассматривается в основном практика использования цифровых доказательств и освещаются правила сбора, проверки, оценки и представления в суд цифровых доказательств. Также рассмотрены вопросы, касательно методов обеспечения и оценки целостности цифровых доказательств.

“Kiber kriminalistika” yoki “raqamli sud kriminalistikasi”ning standart qonuniy ta’rifi hali mavjud emas. Sedona Konferensiya lug’ati: Elektron kashfiyot va raqamli axborotni boshqarish (4-nashr, 2014-yil aprel) quyidagi ta’riflarni beradi:

“Kompyuter kriminalistikasi – tergov yoki sud jarayonida kompyuterdan foydalanish, saqlangan ma’lumotlarni tekshirish va ma’lumotlarni texnik xususiyatlarini tahlil qilish bilan bog’liq masalalarni o’z ichiga olgan holda elektron ma’lumotni tiklash, autentifikatsiya qilish va axborotlarni tahlil qilish uchun maxsus texnikadan foydalanishdir. Kompyuter kriminalistikasi undan foydalanuvchilarga va uni qo’llovchi xodimlarga ma’lumotlarni to’plash va saqlash mahoratiga ega bo’lgan mutaxassislarni talab etadi”.

US-CERT kompyuter kriminalistika jurnalida shunday deyiladi: Kompyuter kriminalistikasi mutlaqo yangi tartib-tamoyil hisoblanadi. Shuning uchun ham sudlar va sanoat sohasida standartlashtirish yoki muvofiqlashtirish metodikasi juda kam bo’lib, u quyidagicha belgilanadi:

“Biz kompyuter kriminalistikasini kompyuter tizimlaridan, tarmoqlardan, simsiz aloqa va saqlash qurilmalaridan ma’lumotlarni sudda dalil sifatida qabul qilinadigan tarzda to’plash va tahlil qilish uchun huquq va kompyuter fanlari elementlarini birlashtirgan fan sohasi sifatida belgilaymiz”.

Raqamli kriminalistikaning umumiy tavsifi.

Texnolog va muallif Simson Garfinkel raqamli sud-kriminalistikasiga yaxshi xulosa berilgan bir maqola yozdi. U shunday so’zlar bilan boshladi:

“1980-yildan buyon kompyuterlar inson hayotining barcha jabhalarida, jumladan, jinoiy faoliyatda ishtirok etishda tobora muhim rol o’ynamoqda. Ushbu rivojlanish raqamli sud-kriminalistikasining internet tarmog’i, telefon, kompyuter va raqamli xotira kabi barcha elektron qurilmalarda joylashgan raqamli dalillarni tekshirish va aniqlashga bo’lgan ehtiyoji ham tobora ortib bormoqda. Raqamli sud ekspertlari va amaliyotchilari axborot texnologiyalari sohasida eng katta muammolarni, jumladan, katta ma’lumotlarni tahlil qilish, dasturiy til jarayoni, axborot ko’rinishi va kiberxavfsizlikning eng qiyin muammolari oldida turishibdi”.

“An’anaviy sud kriminalistikasi bilan solishtirganda, raqamli sud-kriminalistikasi katta muammolarni keltirib chiqaradi. Kompyuter tizimidagi ma’lumotlar iz qoldirmasdan o’zgartirilishi mumkin, tahlil qilinadigan ma’lumotlar miqdori katta va

axborot turlarining xilma-xilligi juda keng. Raqamli kriminalistika mutaxassisi yoki tergovchi manbaga qaramasdan, har qanday iz yoki parchani tahlil qilishga tayyor bo'lishi kerak, chunki raqamli tergovchi dunyoning istalgan nuqtasida joylashgan biron-bir qurilmada har qanday ma'lumotni topilishi mumkinligini garchi bu qiyin bo'lsa-da anglashi lozim".

Muallif turli holatlarda raqamli kriminalistikaning 2 ta maqsadini tavsiflaydi:

Birinchidan, ko'p hollarda kompyuterlar dunyoda sodir etilayotgan jinoyatlarga aloqador bo'lgan dalillari o'z ichiga oladi. Bu tasodif emas, albatta. Ikkinchidan, kompyuter tizimlarini o'z ichiga olgan jinoyatlardir. (masalan, hakerlik) Bunday holatlarda tergovchilar, ko'pincha, tizimning texnik jihatdan murakkabligi va tahlil qilish uchun katta miqdordagi dalillarga duch keladilar [1].

Amerika Qo'shma Shtatlarida ekspertlarning xulosalari, dalillarning sudda qabul qilinishi "Dalillar to'g'risida Federal qoidalar" bilan tartibga solinadi.

Yaqinda qayta ko'rib chiqilgan Fuqarolik sudlari bo'yicha Federal qoidalar va Dalillar to'g'risida Federal qoidalar, sud ishlarini yuritish uchun raqamli dalillarni ishlatish, to'plash va qayta ishlashga sezilarli ta'sir ko'rsatmoqda. Qoidalar elektron hujjat va raqamli dalillarni rasman qog'oz va boshqa dalillar bilan bir xil maqomga ega ekanligini ta'minladi. Natijada potensial ravishda tegishli elektron dalillar mavjudligi va ularni to'g'ri saqlab qolish sud jarayonining har qanday bosqichida muhim bo'lib bormoqda. Mutaxassislar uchun voqea yoki dastlabki tergov va jinoyatni aniqlashning dastlabki bosqichlarida raqamli dalillarni saqlash va tatbiq qilishga oid maxsus qoidalar va qonunlarni bilishi muhimdir.

Fuqarolik ishlari bo'yicha Federal qoidalar zamonaviy sud jarayonining *raqamli davri* qiyinchiliklarini bartaraf etishga qaratilgan. Hozirda eng muhim narsa shuki, huquqni muhofaza qiluvchi organ xodimlari va mutaxassislar raqamli o'yin qoidalarini o'rganishni boshlashlari shartdir.

Amerika Menejment Assotsiatsiyasi va Elektron Siyosat Institutining 2004-yildagi tadqiqotlariga ko'ra, AQSh dagi har beshta kompaniyadan bittasi da'vo yoki tergov davomida elektron pochta orqali sudga chaqirilgan. (2004-yilda 20 % ni tashkil qilgan). Bundan tashqari, 13 % ishchilar ish joyi bilan bog'liq da'volarni elektron tarzda olib borgan [2]. 2005 yilda sud muhokamasi tendensiyasini o'rganishga javoban, korporativ maslahatchi ushbu natijani kompaniyalar uchun **yangi sud ishi** sifatida baholagan [3].

Biroq raqamli dalillar bilan bog'liq ikkilanishlar sud boshlanishdan ancha oldin paydo bo'ladi. Ko'proq biznes tekshiruvi va qonuniy tergovlar sonining ortib borishi bilan kompyuterning qattiq disklari, shaxsiy raqamli qurilmalar va uyali aloqa telefonlar kabi raqamli qurilmalardan olingan dalillarni o'z ichiga olmoqda. Tergov yoki tekshiruv davomida raqamli ma'lumotlardan foydalanish kerakligi ma'lum bo'lganda ekspertlar tegishli dalillarni diqqat bilan aniqlashi, to'plashi, saqlashi va tekshirishi kerak. Raqamli qurilmadan olingan ma'lumotning "surati" batafsil va metodik jihatdan to'planishi kerak, chunki to'plangan dalillarning birortasi yoki barchasi aniqlash, ko'rsatish yoki sinov uchun ishlatilishi mumkin. Yangi federal qoida zamonaviy sud jarayonida elektron hujjatlarni muhokama qilish va ko'rib chiqish bo'yicha umumiy ko'rsatmalar beradi.

Dalillar to'g'risida Federal qoidalar o'zgartirilmagan bo'lsa-da, sudlar ularni raqamli dalillar sifatida qanday tatbiq etishga e'tibor qaratishlari kerak. Ya'ni sud maslahatchisi muhofaza qilish yoki to'plash uchun mumkin bo'lgan raqamli dalil manbalari aniqlangach, qabul qilinishi yuzasidan yakuniy xulosa berishi lozim. Qog'ozdan

foydalanish kamayib borayotganligi va raqamli axborotga qaramlik ortib borayotgani sababli elektron axborotning maqbulligini e'tiborga olgan holda, ko'plab sud ishlarida elektron ma'lumotlarning qabul qilinishi mumkinligiga ishora qilinmoqda. Albatta, elektron tarzda saqlanadigan ma'lumotlarning sudda qabul qilinishi, ko'pincha, qanday to'plangani, saqlanishi va ishlab chiqarilishiga bog'liq. Sudlar raqamli dalillarni to'plash va tahlil qilish uchun "Dalillar to'g'risida Federal qoidalarining" 901-qoidasiga muvofiq uning haqiqiylikini ta'minlash uchun yuqori standartlarni kiritmoqdalar. Raqamli dalillarning ishonchliligini ta'minlash "Dalillar to'g'risida Federal qoidalarining" 702-qoidasiga ko'ra ishonchliligini sinovdan o'tkazish kerak bo'lgan sud ekspertlarining ko'rsatuvlariga asoslanadi.

Raqamli dalillarni tasdiqlash, moddiy dalillar kabi "da'vogarning da'vosi nimani anglatishini aniqlash" uchun yetarli bo'lishi bilan bog'liqdir [4]. Agar sudya qaror qabul qiladigan bo'lsa, hakamlar hay'atining dalillarni haqiqiy ekanligini tasdiqlash yetarli bo'lsa, sudya dalillarni maqbul deb hisoblaydi. Dalillarning haqiqiylikini aniqlash sudyaning isbot qilish to'g'risidagi ko'rsatmasidan kelib chiqib, qarshi dalillar taqdim etilgandan va dalillarning muhimligi tekshirilgandan so'ng hakamlar ixtiyoriga o'tadi. Aslida, dalillarning haqiqiylikini hal qilish hakamlar hay'ati tomonidan hal qilinadi. Raqamli ma'lumotlarning haqiqiylikini tekshirish o'ziga xos muammolarni keltirib chiqaradi. Masalan, qog'oz yozuvlari bilan o'zgarishlar osongina aniqlanishi mumkin va muallif yoki saqlovchi imzo yoki harf uslubi bilan aniqlanishi mumkin. Aksincha, elektron axborotni o'zgartirish qiyin yoki imkonsiz bo'lishi mumkin hamda muallifni yoki yaratuvchini farqlab ko'rsatishning imkoni yo'q. Qog'oz kabi elektron yozuvlar ham to'g'ridan to'g'ri yoki holat yuzasidan biror isbot bilan tasdiqlanishi mumkin. Masalan, biror dasturning yaratuvchisi mualliflikning bevosita guvohligini berishi mumkin. Ammo muammo esa raqamli axborotning o'zgarishi, yo'q qilinishi yoki ishonchli tarzda ishlab chiqarilishi mumkin bo'lgan qulayliklardadir. Bu hatto yangi boshlang'ich kompyuter foydalanuvchisi tomonidan qasddan yoki tasodifan bajarilishi mumkin va bu ekspert uchun muammo tug'diradi hamda hushyorlikni talab qiladi. Aslida, raqamli dalillarning yaxlitligini isbotlash, raqamli sud ekspertlarining kompyuter fanlari va axborot xavfsizligi kompleks usullari va vositalarini qo'llash bo'yicha bilim, ko'nikma va tajribaga ega bo'lishini talab qiladi [5]. Raqamli sud ekspertlari dalillarning yaxlitligi va ishonchliligiga doir aniq dalillarni olish uchun yoki elektron ma'lumotlarning haqiqiylikiga shubha qiladigan dalillar va guvohliklarni taqdim etish uchun o'z bilim va ko'nikmalaridan foydalanadilar. Raqamli dalillarni yig'ish, tashish, saqlash va tahlil qilish vaqtdan boshlab sudda taqdim etishgacha bo'lgan bo'shliq yoki ehtimoliy shubha raqamli dalillarning muhimligi va ishonchliligini jiddiy ravishda zaiflashtirishi mumkin.

Aslida, 34-qoidada faqat "hujjatlar" va "narsalar"ga e'tibor qaratilgan, ammo "hujjatlar" atamasi keyinchalik "ma'lumotlar to'plamini" o'z ichiga oladi. Shu yillar mobaynida sudlar "hujjatlar" atamasiga elektron ko'rinishda saqlanadigan ma'lumotni kiritishni izohlab berishdi, bu qog'ozda aks ettiriladigan shakllarda saqlanishi ham mumkin. Yangi 34-qoida (a) "hujjatlar"ni "elektron tarzda saqlanadigan ma'lumot" deb ta'riflaydi va bu ibora, shuningdek, qoidaning yangi nomiga kiritilgan bo'lib, elektron ma'lumotlarning topilishi qog'oz hujjatlarini ochish bilan teng ravishda tasdiqlanadi [4]. Shuning uchun "hujjatlarni" yaratish bo'yicha so'rovlarni qabul qiluvchilar hozirda faqatgina qog'oz hujjatlarni emas, balki saqlanadigan ommaviy axborot vositalaridan qat'i nazar, barcha elektron tarzda saqlanadigan axborotlarni qamrab olishini talab qilmoqda.

34-qoida (a) bandiga kiritilgan o'zgartirishlarga ko'ra, sudda qatnashayotgan taraflarni "testdan o'tkazish" yoki "namunaviy" javob beruvchi hujjatlarni yoki boshqa aniq narsalarni, shu jumladan, elektron tarzda saqlanadigan axborotni olish imkoniyatini so'rashi mumkin. Shu bilan birga, maslahat qo'mitasi ushbu o'zgarish "elektron axborot tizimiga taraflardan biri tomonidan to'g'ridan to'g'ri kirish huquqini yaratish uchun mo'ljallanmaganligi" haqida ogohlantirishini eslatib o'tadi. Eslatmalar taraflar va sudlarga maxfiylik, xavfsizlik va nojo'ya tajavvuzkorlikdan saqlanishini bildirib o'tadi. 34-qoida (b) bandiga ko'ra, da'vogar sudda taqdim etiladigan dalillar shaklini aniqlash huquqiga ega bo'ldi, agarda da'vogar bu ishni qilmasa, bu huquq javobgarga beriladi [4]. 34-qoida (a) bandi, 1-qismiga binoan raqamli axborotning qanday shaklda bo'lishidan qat'iy nazar, zarurat tug'lsa, javobgar tomonidan "foydalanish uchun maqbul shaklga aylantirish" talab qilinishi mumkin [6]. Bundan tashqari, sud o'qilishi mumkin bo'lmagan bo'sh joy fayllarini ishlab chiqaruvchi ekspertdan tegishli qismlarni ajratib olish va tarjima qilishni yoki tomonlarni axborotni osongina o'qishni ta'minlash uchun vositani taqdim etishni talab qilishi mumkin.

Yangi qoidalar elektron axborotni ochishga qaratilgan bo'lsa-da, qabul qilingan qarorlarning aksariyati sud jarayonida raqamli dalillarning qabul qilinishi bilan bog'liq muammolarni keltirib chiqarmoqda. Ajablanarlisi shuki, raqamli dalillarni qabul qilish bog'liq chiqarilgan qarorlarning aksariyati jiyoat ishlariga aloqadordir. Raqamli dalillarni sudda oshkor qilishdan oldin, dalillar bilan bog'liq to'siqlar, ularni to'plash, tiklash, tahlil qilish va taqdim etishning samarasiz usullari bilan amalga oshirilishi qanchalik jiddiy muammolarga olib kelishini baholashi kerak.

Sudda ko'rilayotgan ish xoh fuqarolik, xoh jinoyat bilan bog'liq bo'lsin, tergov dalillarni to'plash bilan boshlanadi. Noto'g'ri bajarilgan bo'lsa, dalillar o'z ahamiyatini yo'qotishi mumkin. Ayni paytda, raqamli dalillarni kompyuterning qattiq disklaridan yig'ish va tadqiq qilish uchun eng ommalashgan vosita Guidance Software Inc. ning EnCase dasturi hisoblanadi [7]. Dalillarni to'plashni amalga oshirish uchun ekspertlar EnCase Imager dasturidan foydalanib, qattiq diskni eng kichik elementlarini ham o'zgartirmasdan to'liq nusxa ko'chirishadi. Ushbu jarayon "aks ettirish" yoki "kriminalistik nusxalash" deb ataladi va ushbu metodologiya Qo'shma Shtatlar v. Kuk, 777 N.E.2d 882 (Ogayo shtati App., 2002) ishida birinchi marta amalga oshirilgan. Bu jinoiy ishda sudlanuvchi kompyuterining qattiq diskidan olingan dalillarga yo'l qo'yilmasligiga asoslanib, sudlanganligiga e'tiroz bildirgan. Nusxa ko'chirish jarayonining batafsil muhokamasidan so'ng, olingan ma'lumotlarning haqiqiyliigi va shubhalanish ehtimoli yo'qligi haqida appellyatsiya sudi dalillarni to'g'ri tan olinganligi to'g'risida qaror chiqaradi.

Nusxa ko'chirishning boshqa usullari hozircha potensial jihatdan tegishli barcha ma'lumotlarni saqlamaydi [8]. Natijada, bunday usullar to'plash natijalarini to'liq to'ldirmaydi va qarshilik ko'rsatish uchun kuchli imkoniyat yaratuvchi materiallarini keltirib chiqaradi va dalillarni qabul qilish uchun to'siqlar hosil qiladi. Bunday vaziyatda sudlar uchinchi tomon – mustaqil va xolis ekspertlarni sud dalillarini to'ldirish uchun qattiq disklardan "aks ettirish" yoki "klon qilish" shaklida nusxa ko'chirish uchun yollaydi [9]. Sudlar raqamli axborotning, dalilning yuqori darajadagi nusxalarini yaratishda o'z talablarini doimiy ravishda takomillashtirmoqda. Taylor vs Qo'shma Shtatlar ishida 93 SW.3d 487, 507 (TEXAS, 2002), sud tomonidan olingan nusxalar o'zgartirilmaganligini isbotlash uchun nusxalangan kompyuterning **xesh**larini [10] yaratish muhimligini tan

olgan. Xash qiymati – ma'lumotlarning o'zgarganligini tekshirish uchun tez-tez ishlatiladigan ma'lumotlarning kichik raqamli izlari hisoblanadi. O'sha vaziyatda sud, qisman jinoyat ishini bekor qildi, chunki tergov xodimi xesh qiymatlarini e'tiborga olmagan edi va shu bilan ma'lumotlarning haqiqiyliги va natijada yuzaga keladigan tahlillarni shubha ostiga qo'ydi [11]. Sud maslahatchilari raqamli dalillar bilan bog'liq bu jarayon haqida aniq ma'lumotga ega bo'lishi, raqamli dalillarni to'plash va tergov qilish bo'yicha aniqroq qarorlar chiqarishga yordam beradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Simson L. Garfinkel, "Digital Forensics", Scientific American (September-October 2013), available at: www.americanscientist.org/issues/pub/digital-forensics.
2. "2004 Workplace E-Mail and Instant Messaging Survey", American Management Association, New York, New York 2004.
3. Dillard, Stephen C., "Litigation as the Great Equalizer: New Fulbright & Jaworski Survey Finds," Sarbanes-Oxley Compliance Journal, 2005.
4. Federal Rules of Evidence, December 2006.
5. Hosmer, Chet, "Proving the Integrity of Digital Evidence with Time," 1st Int'l J. Of Digital Evidence, 2002.
6. Ryan, Daniel J., Shpantzer, Gal, "Legal Aspects of Digital Forensics", The George Washington University, Washington, D. C., September 2002.
7. Palmer G., 'A Road Map for Digital Forensic Research,' the First Digital Forensic Research Workshop (DFRWS), November, Utica, New York, 2001.
8. Carrier B. 'Open Source Digital Forensics Tools: The Legal Argument', @stake Research Report, October 2002 and Digital Data Acquisition Tool Specification, Nat'l Inst. Standards & Tech. U.S. Dep't Commerce, Oct. 4, 2004.
9. Simon Prop. Group L.P. v. my Simon, Inc., 2000 U.S. Dist. LEXIS 8950 (S.D. Ind. 2000) and United States v. Alexander, 2004 U.S. Dist. LEXIS 27790 (E.D. Mich. 2004).
10. Xesh (hash) – xesh funktsiyasi turli hajm va o'lchamdagi ma'lumotlarni muayyan hajmdagi ma'lumotlarga xaritalash uchun ishlatiladigan funktsiyalar. Xesh funktsiyasi tomonidan qaytarilgan qiymatlarga xesh qiymatlari, xash kodlari, tizimlashtirilgan kodlar yoki oddiy xeshlar deyiladi. $H(z, n + 1) = H(z, n) \rightarrow n / (n + 1)$.
11. Taylor v. State, 93 S.W.3d 487 (Tex. App. 2002).
12. Khamidov Bakhtiyor Khamidovich et al. "General Theoretical Issues of Improving Private Forensic Methods In The Field Of Combat Against Cybercrime". Psychology and education (2021) 58(1): 2705-2712 DOI: <https://doi.org/10.17762/pae.v58i1.1153>.
13. Топилдиева Д. Кибержиноятларни тергов қилиш муаммолари // Общество и инновации. – 2021. – Т. 2. – №. 11/5. – С. 292–296.
14. Каримов Бобуржон Научно-теоретические вопросы категории цифровых доказательств // Review of law sciences. 2020. № Спецвыпуск. URL: <https://cyberleninka.ru/article/n/nauchno-teoreticheskie-voprosy-kategorii-tsifrovyyh-dokazatelstv> (дата обращения: 14.03.2022).