

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

ISSN
3093-9364



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING

 Google Scholar

 Zenodo

 DOI

 OpenAIRE

 Open Access



AI

! Unauthorized Access

UNAUTHORIZED
ACCESS

SYSTEM
BREACH



CYBER ATTACK



DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global



VOLUME 2

ISSUE 1



AUGUST 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali
Journal of Digital Law and
Innovation**

**August, 2026
VOLUME 2, ISSUE 1**



ADVANCED SCIENCE INDEX



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

TARMOQ VA KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI KRIMINALISTIKA METODLARINI QO‘LLASH

Ro‘zmetova Dinora Abdulla qizi

“Cyber University” davlat universiteti 1-kurs talabasi

dinararozmetova58@gmail.com

Samarov Sherzod Hamrayevich

“Cyber University” davlat universiteti

“Huquq va biznes” fakulteti uslubchisi

samarovsherzod78@gmail.com

MAQOLA MA'LUMOTI

Kalit so‘zlar:

raqamli kriminalistika,
tarmoq kriminalistikasi,
kiberjinoiyat,
raqamli dalil,
tarmoq trafigi,
log-fayl,
forensik nusxa,
SIEM,
sud ekspertizasi.

ANNOTATSIYA

Mazkur maqolada tarmoq va kiberjinoiyatlarni tergov qilish jarayonida raqamli kriminalistika metodlaridan foydalanishning huquqiy, protsessual va texnik jihatlari tahlil qilinadi. Tadqiqot O‘zbekiston Respublikasining raqamli dalillar, sud ekspertizasi va kiberxavfsizlik sohasidagi qonunchiligi, NIST SP 800-86 va SP 800-92 qo‘llanmalari, ISO/IEC 27037 standarti hamda tegishli ilmiy adabiyotlarga asoslanadi. Tahlil natijalari tarmoq trafigi, tizim jurnallari, IDS ogohlantirishlari va SIEM tizimlarida shakllantirilgan ma’lumotlar ularning kelib chiqishi, yig‘ish vakolati, vaqt ko‘rsatkichlarining muvofiqligi, yaxlitligi hamda dalilni olishdan sudga taqdim etishgacha bo‘lgan saqlash va uzatish jarayoni tegishli tartibda hujjatlashtirilgan taqdirdagina ishonchli raqamli dalil sifatida baholanishi mumkinligini ko‘rsatadi. Shu asosda raqamli dalillarni aniqlash, yig‘ish, saqlash, tahlil qilish va sudga taqdim etish bosqichlarini qamrab oluvchi besh bosqichli model taklif etiladi.

APPLICATION OF DIGITAL FORENSICS METHODS IN INVESTIGATING NETWORK AND CYBERCRIMES

ARTICLE INFO

Keywords:

digital forensics,
network forensics,
cybercrime,
digital evidence,
network traffic,
log file,
forensic image,
SIEM,
forensic examination.

ABSTRACT

This article analyses the legal, procedural, and technical aspects of applying digital forensic methods in the investigation of network-related crimes and cybercrime. The study is based on the legislation of the Republic of Uzbekistan governing digital evidence, forensic examination, and cybersecurity, as well as the NIST SP 800-86 and SP 800-92 guidelines, the ISO/IEC 27037 standard, and relevant academic literature. The findings demonstrate that network traffic, system logs, intrusion detection system alerts, and data generated by security information and event management (SIEM) systems may be regarded as reliable digital evidence only when their origin, the authority under which they were collected, timestamp consistency, integrity, and the process of their preservation and transfer—from acquisition to presentation before the court—are properly documented. On this basis, a five-stage model encompassing the identification, collection, preservation, analysis, and presentation of digital evidence in court is proposed.

ПРИМЕНЕНИЕ МЕТОДОВ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ПРИ РАССЛЕДОВАНИИ СЕТЕВЫХ И КИБЕРПРЕСТУПЛЕНИЙ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

цифровая криминалистика,
сетевая криминалистика,
киберпреступление,
цифровое доказательство,
сетевой трафик,
лог-файл,
криминалистическая копия,
SIEM,
судебная экспертиза..

АННОТАЦИЯ

В статье анализируются правовые, процессуальные и технические аспекты применения методов цифровой криминалистики при расследовании сетевых преступлений и киберпреступлений. Исследование основано на законодательстве Республики Узбекистан в области цифровых доказательств, судебной экспертизы и кибербезопасности, руководствах NIST SP 800-86 и SP 800-92, стандарте ISO/IEC 27037, а также соответствующей научной литературе. Результаты анализа показывают, что сетевой трафик, системные журналы, предупреждения систем обнаружения вторжений и данные, сформированные в системах управления информацией и событиями безопасности (SIEM), могут быть признаны достоверными цифровыми доказательствами только при условии надлежащего документирования их происхождения, полномочий на сбор, согласованности временных меток, целостности, а также процесса хранения и передачи доказательств — с момента их получения до представления в суд. На этой основе предлагается пятиэтапная модель, охватывающая выявление, сбор, сохранение, анализ и представление цифровых доказательств в суде.

KIRISH

Raqamli muhitda sodir etiladigan jinoyatlar an'anaviy izlar bilan bir qatorda tarmoq paketlari, autentifikatsiya yozuvlari, DNS so'rovlari, qurilma metama'lumotlari, bulutli servis jurnallari va boshqa elektron ma'lumotlarni hosil qiladi. Bunday ma'lumotlar tez o'zgarishi, avtomatik qayta yozilishi, shifrlanishi yoki turli yurisdiksiyalarda saqlanishi mumkin. Shu sababli kiberjinoyatni tergov qilish faqat texnik hujumni aniqlash bilan tugamaydi; topilgan ma'lumotni qonuniy yo'l bilan olish, uning yaxlitligi va kelib chiqishini isbotlash hamda xulosani sudda tekshirish imkonini yaratish talab etiladi [1–4].

Raqamli kriminalistika raqamli manbalardan ish uchun ahamiyatli ma'lumotni aniqlash, yig'ish, saqlash, tekshirish, tahlil qilish va tushunarli shaklda taqdim etishga qaratilgan ilmiy-amaliy faoliyatdir. Tarmoq kriminalistikasi uning maxsus yo'nalishi bo'lib, uzatilayotgan trafik va tarmoq hodisalari asosida hujumning vaqti, manbasi, yo'nalishi va oqibatlarini rekonstruksiya qiladi. NIST SP 800-86 kompyuter va tarmoq forensikasini hodisaga javob berish jarayoniga integratsiya qilishni, ISO/IEC 27037 esa potensial raqamli dalilni aniqlash, yig'ish, olish va saqlash faoliyatlarini tizimlashtiradi [5, 7].

O'zbekistonda 2024-yil 21-noyabrda O'RQ–1003-son Qonun bilan raqamli dalil tushunchasi va u bilan ishlash tartibi Jinoyat-protsessual kodeks hamda boshqa protsessual hujjatlarga kiritildi. Elektron fayllar, audio va videoyozuvlar, internetda saqlanayotgan hamda boshqa elektron ma'lumotlar ish uchun ahamiyatli holatlar to'g'risidagi axborotni o'z ichiga olsa, raqamli dalil sifatida baholanishi mumkin. Qonunchilik raqamli dalilning ko'chirma nusxasidan foydalanishga uning yaxlitligi va aynan o'xshashligi saqlangan taqdirda yo'l qo'yadi [1, 2].

Mazkur huquqiy yangilanish raqamli dalilni alohida protsessual kategoriya sifatida mustahkamladi, biroq tarmoq trafikini qayd etish, turli loglarni korrelyatsiya qilish, vaqt manbalarini sinxronlashtirish, forensik vositalarni validatsiya qilish va ekspert xulosasining takroriy tekshiriluvchanligini ta'minlash bo'yicha yagona amaliy protokol masalasi dolzarbligicha qolmoqda. "Sud ekspertizasi to'g'risida"gi Qonun ekspert tadqiqotining qonuniyligi, mustaqilligi, xolisligi va ilmiy asoslanganligini talab qiladi; ushbu talablar raqamli ekspertizaga ham tatbiq etiladi [3].

Ilmiy adabiyotlarda Eoghan Casey raqamli dalilni texnik topilma emas, balki kelib chiqishi, konteksti va yaxlitligi izohlanishi lozim bo'lgan daliliy obyekt sifatida ko'radi [8]. Brian Carrier fayl tizimi va ma'lumotlar tuzilishini qatlamlar bo'yicha tahlil qilish xulosaning

manbaga qaytib tekshirilishini kuchaytirishini ko'rsatadi [9]. Simson Garfinkel esa ma'lumotlar hajmi, yangi qurilmalar va vositalarning eskirishi sharoitida standartlashtirilgan hamda modulli forensik jarayonlar zarurligini asoslaydi [10].

Tadqiqotning maqsadi tarmoq va kiberjinoyatlarni tergov qilishda raqamli kriminalistika vositalarining daliliy funksiyasini aniqlash, milliy protsessual qoidalarni xalqaro metodik standartlar bilan taqqoslash va raqamli dalil ishonchliligini ta'minlaydigan uzluksiz modelni ishlab chiqishdan iborat. Tadqiqot texnik vositaning o'zi dalil yaratadi degan yondashuvni rad etib, vosita natijasi protsessual qonuniylik, yaxlitlik, hujjatlashtirish va tekshiriluvchanlik bilan birgalikda baholanishi kerakligini asoslaydi.

METODOLOGIYA

Tadqiqotda formal-yuridik, tizimli-huquqiy, qiyosiy, doktrinal va funksional tahlil metodlaridan foydalanildi. Formal-yuridik tahlil doirasida O'zbekiston Respublikasi Jinoyat-protsessual kodeksi, O'RQ-1003-son Qonun, "Sud ekspertizasi to'g'risida"gi va "Kiberxavfsizlik to'g'risida"gi qonunlarning raqamli ma'lumotni olish, tekshirish va baholashga oid qoidalari o'rganildi [1-4].

Qiyosiy va funksional tahlilda NIST SP 800-86 dagi yig'ish-tekshirish-tahlil-hisobot jarayoni, NIST SP 800-92 dagi loglarni markazlashtirish va boshqarish talablari hamda ISO/IEC 27037 dagi aniqlash, yig'ish, olish va saqlash qoidalari milliy protsessual tartib bilan solishtirildi [5-7]. Qiyoslashning mezonlari sifatida vakolatning aniqligi, ma'lumot kelib chiqishi, nusxa yaxlitligi, vaqt izchilligi, saqlash zanjiri, usulning takroriy tekshirilishi va natijani sudga tushunarli taqdim etish olindi.

Doktrinal tahlil Casey, Carrier, Garfinkel, Reith, Carr va Gunsch, shuningdek Beebe va Clarkning raqamli forensika jarayoni haqidagi yondashuvlarini qamrab oldi [8-12]. Vositalar texnik qulayligi bo'yicha emas, hosil qiladigan artefakti, daliliy funksiyasi va xatolik xavfi bo'yicha baholandi. Wireshark, tcpdump, Zeek, Snort/IDS, SIEM va SHA-256 xeshlash usuli misol sifatida tanlandi.

Tadqiqot empirik tergov statistikasi yoki real jinoyat ishining yopiq materiallariga asoslanmaydi. Dastlabki matnda qayd etilgan 30-40 foizlik samaradorlik ko'rsatkichi reproduktiv tajriba bayonnomasi va tekshiriladigan ma'lumotlar to'plami bilan asoslanmagani sababli ushbu tahrirga kiritilmadi. Natijalar normativ, metodik va doktrinal manbalarni sifat jihatdan sintez qilish orqali shakllantirildi.

NATIJALAR

Tahlilning birinchi natijasi raqamli dalil va raqamli artefakt aynan bir tushuncha emasligini ko'rsatdi. PCAP fayli, autentifikatsiya logi, IDS ogohlantirishi yoki SIEM hodisa kartasi avvalo elektron ma'lumot manbasidir. U ishga aloqadorligi, qonuniy olingani, asl manba bilan bog'liqligi, yaxlitligi va mazmuni tekshirilgandan keyingina daliliy ahamiyat kasb etadi. Masalan, IDS ogohlantirishi ma'lum qoida ishga tushganini ko'rsatadi, biroq hujum sodir etilganini yoki muayyan shaxs aybdorligini o'z-o'zidan isbotlamaydi.

Ikkinchi natija tarmoq hodisasini to'liq rekonstruksiya qilish uchun bitta vosita yetarli emasligini tasdiqladi. Paket yozuvi protokol darajasidagi tafsilotni beradi, Zeek hodisalarni strukturaviy loglarga ajratadi, IDS ma'lum imzolarga mos faollikni ko'rsatadi, SIEM esa turli manbalardagi yozuvlarni vaqt va kontekst bo'yicha birlashtiradi. Shu sababli xulosa turli manbalarni o'zaro tasdiqlashga tayanishi, avtomatik korrelyatsiya natijasi esa asl log va trafik bilan tekshirilishi kerak [5, 6].

Uchinchi natija yaxlitlikni ta'minlashning kriptografik xesh bilan cheklanmasligini ko'rsatdi. SHA-256 qiymatlarining mosligi asl va nusxa fayllar bitlar darajasida o'zgarmaganini tasdiqlaydi, ammo ma'lumot qachon, kim tomonidan, qaysi vakolat asosida va qanday vosita bilan olinganini ko'rsatmaydi. Shu bois xesh qiymati chain of custody bayonnomasi, vaqt belgisi, qurilma va dastur versiyasi, filtr parametrlari, saqlash joyi va har bir topshirish holati bilan birga qayd etilishi lozim [5, 7].

To'rtinchi natija vaqt sinxronligi tarmoq kriminalistikasining markaziy daliliy sharti ekanini ko'rsatdi. Turli server, qurilma va bulutli xizmatlar vaqt zonasi, tizim soati yoki NTP sozlamalari bo'yicha farq qilsa, hodisalar noto'g'ri ketma-ketlikda ko'rinishi mumkin. Shu sababli ekspert xulosasida vaqt manbasi, zona, aniqlangan og'ish va qo'llangan tuzatish ochiq ko'rsatilishi zarur.

Beshinchi natija shifrlangan va bulutli muhitlarda paketning foydali yukini bevosita o'qish imkoniyati cheklanishini aniqladi. Bunday holatda oqim metama'lumotlari, DNS yozuvlari, endpoint loglari, autentifikatsiya tarixi va bulut provayderining audit izlari birgalikda qo'llanadi. Biroq ma'lumotni provayderdan olishda yurisdiksiya, saqlash muddati, vakolat va shaxsiy hayot daxlsizligi talablari hisobga olinishi kerak [4, 13].

Vositalarning daliliy funksiyasi va cheklovlari quyidagi jadvalda umumlashtirildi.

1-jadval. Tarmoq kriminalistikasida vositalar, daliliy artefaktlar va ishonchlilik shartlari

Vosita yoki usul	Asosiy vazifa	Hosil qilinadigan daliliy artefakt	Ishonchlilik sharti va cheklov
Wireshark	Paketlarni ushlash va protokol maydonlarini batafsil tahlil qilish	PCAP/PCAPNG fayli, paket va sessiya metama'lumotlari	Yig'ish interfeysi, vaqt va filtrlar qayd etilishi; shifrlangan foydali yuk ochilmasligi mumkin
tcpdump	Server va terminal muhitida trafikni tezkor yozib olish	PCAP fayli va buyruq parametrlari	Buyruq, interfeys, vaqt oraliq'i va fayl xeshi hujjatlashtirilishi kerak
Zeek	Tarmoq hodisalarini protokolga xos jurnallarga ajratish	conn.log, dns.log, http.log va boshqa strukturaviy loglar	Konfiguratsiya va skriptlar saqlanishi; xulosa asl trafik bilan tekshirilishi lozim
Snort/IDS	Ma'lum imzo yoki qoida bo'yicha shubhali faollikni aniqlash	Ogohlantirish, vaqt belgisi, qoida identifikatori	Ogohlantirishning o'zi aybni isbotlamaydi; false positive va noma'lum hujum ehtimoli baholanadi
SIEM	Turli manbalardagi loglarni vaqt va kontekst bo'yicha korrelyatsiya qilish	Hodisa kartasi, korrelyatsiya natijasi, audit izi	Manba loglari, vaqt sinxronligi va korrelyatsiya qoidalari mustaqil tekshirilishi kerak
SHA-256 xeshlash	Forensik nusxa va asl ma'lumotning yaxlitligini nazorat qilish	Xesh qiymati va tekshiruv bayonnomasi	Xesh mazmunning to'g'riligini emas, nusxaning o'zgarmaganini ko'rsatadi; hisoblash jarayoni hujjatlashtiriladi

Manba: Muallif tomonidan NIST SP 800-86, NIST SP 800-92, ISO/IEC 27037 va texnik adabiyotlar asosida tuzilgan [5–11].

Jadvaldan ko'rinadiki, har bir vosita tarmoq hodisasining faqat muayyan qatlamini aks ettiradi. Ishonchli xulosa dastur natijasini avtomatik haqiqat deb qabul qilishga emas, manba ma'lumotlari, konfiguratsiya, vaqt, xesh va muqobil izohlarni hujjatlashtirishga tayanadi.

Ayniqsa SIEM va IDS natijalarida qoida identifikatori, versiya va false positive ehtimoli ko'rsatilishi lozim.

Normativ va metodik tahlil asosida raqamli dalilning ishonchliligini ta'minlashning besh bosqichli modeli ishlab chiqildi.



1-rasm. Raqamli dalilning ishonchliligini ta'minlashning besh bosqichli modeli

Manba: Muallif tomonidan milliy protsessual qonunchilik, NIST va ISO/IEC metodikasi asosida ishlab chiqilgan [1–7].

Modelda aniqlash bosqichi dalil manbasi, tergov ko'لامي va vakolatni belgilaydi; yig'ish bosqichi trafik, log va forensik nusxani protsessual tartibda oladi; saqlash bosqichi xesh, kirish nazorati va chain of custody orqali yaxlitlikni himoya qiladi; tahlil bosqichi korrelyatsiya, vaqt chizig'i va muqobil gipotezalarni tekshiradi; taqdim etish bosqichi esa usul, natija, xatolik va cheklovlarni ekspert xulosasida ochiq bayon etadi. Bir bosqichdagi hujjatlashtirish uzilishi keyingi bosqichdagi xulosaning ishonchliligini pasaytiradi.

MUHOKAMA

Olingan natijalar Eoghan Caseyning raqamli dalilni kontekstdan ajratib baholab bo'lmisligi haqidagi yondashuvi bilan mos keladi [8]. Mazkur tadqiqot bu fikrni tarmoq hodisalari misolida rivojlantirib, paket yoki logning daliliy qiymati faqat texnik mazmun bilan emas, uni hosil qilgan tizim, vaqt, konfiguratsiya va saqlash tarixi bilan belgilanishini ko'rsatadi. Shuning uchun ekspert xulosasi “nimani topdi” degan savol bilan birga “qanday, qayerdan va qaysi cheklovlar ostida topildi” degan savollarga ham javob berishi kerak.

Brian Carrierning qatlamli tahlil yondashuvi ma'lumotni fizik yoki xom darajadan fayl tizimi va ilova darajasigacha tekshirish orqali xulosani qayta ko'rib chiqish imkonini beradi

[9]. Tarmoq kriminalistikasida bunga o'xshash qatlamlilik PCAP, protokol logi, endpoint hodisasi va SIEM korrelyatsiyasini ajratib tekshirishda namoyon bo'ladi. Ushbu tadqiqot natijasiga ko'ra, yuqori darajadagi avtomatik xulosa quyi darajadagi asl artefakt bilan bog'lanmagan bo'lsa, uning suddagi tekshiriluvchanligi zaiflashadi.

Mark Reith, Clint Carr va Gregg Gunsch taklif etgan model raqamli forensikani aniqlash, tayyorlash, yondashuvni belgilash, saqlash, yig'ish, tekshirish, tahlil, taqdim etish va natijani qaytarish bosqichlari orqali izohlaydi [11]. Beebe va Clark esa murakkab tekshiruv uchun umumiy jarayonni ishga xos quyi bosqichlar bilan to'ldiruvchi ko'p qatlamli modelni asoslaydi [12]. Taklif etilgan besh bosqichli model ushbu konsepsiyalarni takrorlamaydi; ularni O'zbekistonning raqamli dalil haqidagi protsessual qoidalariga mos, amaliyotchi uchun ixcham huquqiy-metodik zanjirga birlashtiradi.

Simson Garfinkel forensik ma'lumotlar hajmining ortishi va vositalarning tez eskirishi sharoitida standartlashtirilgan, modulli va avtomatlashtirishga mos yondashuv zarurligini ta'kidlaydi [10]. Bu xulosa milliy amaliyotda vosita nomini majburiy belgilashdan ko'ra, uning validatsiyasi, versiyasi, konfiguratsiyasi, xatolik ko'rsatkichi va natijaning takroriy tekshirilishi uchun minimal talablarni belgilash maqsadga muvofiqligini ko'rsatadi. Texnologiyaga bog'lanib qolgan yo'riqnoma tez eskiradi, funksional talab esa yangi vositalarga ham tatbiq etilishi mumkin.

O'RQ-1003-son Qonun raqamli dalillarni protsessual tizimga kiritib, huquqiy bo'shliqning muhim qismini bartaraf etdi [2]. Endingi bosqich qonundagi umumiy qoidalarni amaliy standart bilan to'ldirishdan iborat. Yagona milliy protokolda raqamli dalil manbasini identifikatsiya qilish, jonli tizimdan ma'lumot olishning ustuvorligi, forensik nusxa yaratish, vaqt og'ishini qayd etish, xesh algoritmi, chain of custody, xavfsiz saqlash, vosita validatsiyasi va ekspert hisobotining minimal tarkibi belgilanishi lozim.

"Sud ekspertizasi to'g'risida"gi Qonundagi ilmiy asoslanganlik va xolislik talabi raqamli ekspertning faqat tasdiqlovchi ma'lumotlarni tanlamasligini, muqobil izoh va texnik cheklovlarni ham ko'rsatishini talab qiladi [3]. Masalan, bitta IP-manzilni shaxs bilan tenglashtirish, IDS signalini yakunlangan hujum deb qabul qilish yoki xesh mosligini ma'lumotning haqqoniyligi bilan aralashtirish metodologik xatodir. Ekspert xulosasi texnik natijaning ehtimoliy talqinlarini va shaxsga nisbat berish uchun zarur qo'shimcha dalillarni farqlashi kerak.

Transchegaraviy elektron dalillar uchun tezkor saqlab qolish va hamkorlik mexanizmi alohida ahamiyatga ega. Budapesht konvensiyasi kiberjinoyat va elektron dalillar bo'yicha protsessual hamda xalqaro hamkorlik uchun keng qo'llaniladigan yo'riqnoma vazifasini bajaradi [13]. Milliy tizimda xorijiy provayderdagi logni saqlab qolish so'rovi, vakolatli aloqa nuqtalari va huquqiy yordam tartiblarini raqamli dalilning qisqa saqlanish muddatiga moslashtirish zarur.

Amaliy taklif sifatida, birinchidan, tergovchi, tezkor xodim va ekspert uchun rolga mos alohida chek-listlar; ikkinchidan, davlat ekspertiza muassasalarida forensik vositalarning sinov va validatsiya reyestri; uchinchidan, standartlashtirilgan elektron chain of custody jurnali; to'rtinchidan, tarmoq, mobil, bulut va IoT forensikasi bo'yicha muntazam malaka oshirish; beshinchidan, anonimlashtirilgan o'quv ma'lumotlari va takroriy laboratoriya sinovlarini joriy etish maqsadga muvofiq.

XULOSA

Tarmoq va kiberjinoyatlarni tergov qilishda raqamli kriminalistika samaradorligini oshirish dalilning texnik aniqlanishidan sudga baholanishigacha bo'lgan protsessual ketma-ketlikni aniq belgilashni talab etadi. Tarmoq trafigi, loglar, IDS ogohlantirishlari va SIEM korrelyatsiyasi kelib chiqish manbasi, qonuniy yig'ish, vaqt sinxronligi, yaxlitlik, saqlash zanjiri va takroriy tekshiruv bilan bog'langandagina ishonchli daliliy ahamiyat kasb etadi. Shu sababli yagona milliy metodik protokol, elektron chain of custody jurnali va forensik vositalarni validatsiya qilish tizimini joriy etish maqsadga muvofiq.

Xulosa qilib aytganda, raqamli kriminalistikaning ishonchliligi yangi dasturlarni xarid qilish bilangina emas, aniqlash, yig'ish, saqlash, tahlil va taqdim etish bosqichlarining uzluksizligi bilan belgilanadi. Taklif etilgan besh bosqichli model tergovchi va ekspert faoliyatini yagona mezonlarga bog'lash, raqamli dalilning sudga tekshiriluvchanligini oshirish hamda shaxs huquqlari bilan kiberjinoyatlarni samarali tergov qilish o'rtasida muvozanatni ta'minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasining Jinoyat-protsessual kodeksi. 22.09.1994 (amaldagi tahrir). <https://lex.uz/docs/-111460>
2. O'zbekiston Respublikasining "O'zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o'zgartirish va qo'shimchalar kiritish to'g'risida"gi O'RQ-1003-son Qonuni. 21.11.2024. <https://lex.uz/docs/-7228758>
3. O'zbekiston Respublikasining "Sud ekspertizasi to'g'risida"gi O'RQ-249-son Qonuni. 01.06.2010 (amaldagi tahrir). <https://lex.uz/docs/-1633102>
4. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi O'RQ-764-son Qonuni. 15.04.2022 (amaldagi tahrir). <https://lex.uz/uz/docs/-5960604>
5. Kent, K., Chevalier, S., Grance, T., & Dang, H. Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86, 2006. <https://doi.org/10.6028/NIST.SP.800-86>
6. Kent, K., & Souppaya, M. Guide to Computer Security Log Management. NIST SP 800-92, 2006. <https://doi.org/10.6028/NIST.SP.800-92>
7. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. <https://www.iso.org/standard/44381.html>
8. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2011.
9. Carrier, B. File System Forensic Analysis. Addison-Wesley, 2005.
10. Garfinkel, S. L. Digital forensics research: The next 10 years. Digital Investigation, 7(S), S64–S73, 2010. <https://doi.org/10.1016/j.diin.2010.05.009>
11. Reith, M., Carr, C., & Gunsch, G. An Examination of Digital Forensic Models. Digital Forensic Research Workshop, 2002. <https://dfrws.org/presentation/an-examination-of-digital-forensic-models/>
12. Beebe, N. L., & Clark, J. G. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167, 2005. <https://doi.org/10.1016/j.diin.2005.04.002>
13. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185. 23.11.2001. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>