Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

KATTA TIL MODELLARI VA RETRIEVAL-AUGMENTED GENERATION TEXNOLOGIYASI ASOSIDA RAQAMLI KRIMINALISTIK TERGOVDA VOQEALAR XRONOLOGIYASINI TIKLASH: NAZARIY-TEXNIK TAHLIL

Yusupova Surayyo Muyasar qizi
suray31052002@gmail.com

Annotatsiya

Mazkur maqolada raqamli kriminalistika va hodisalarga chora ko'rish (DFIR) sohasida eng dolzarb muammolardan biri — kiber hodisalar vaqt chizig'ini (timeline) tiklash jarayonini avtomatlashtirish masalasi nazariy-texnik jihatdan tahlil qilinadi. An'anaviy metodlarning (log2timeline, Timesketch, EnCase kabi vositalarning) tizimli cheklovlari, xususan ma'lumotlar hajmi va xilma-xilligi tufayli yuzaga keladigan vaqt sarfi va inson omiliga bog'liqlik ko'rsatib o'tiladi. Ishning markazida katta til modellari (LLM) va Retrieval-Augmented Generation (RAG) texnologiyasining kriminalistik tahlilga integratsiyalashuvi, jumladan GenDFIR va ForensicLLM kabi zamonaviy freymvorklarning arxitekturaviy tamoyillari yotadi. Shuningdek, AQSh (NIST), Yevropa (Elsevier/DFRWS) va Osiyo (Hindiston) davlatlarining ilmiy-texnik tajribasi O'zbekiston milliy qonunchiligi va ilmiy-tadqiqot amaliyoti bilan qiyoslanadi. Tadqiqot natijalari shuni ko'rsatadiki, LLM asosidagi yechimlar tergov samaradorligini sezilarli oshirish salohiyatiga ega, biroq gallyutsinatsiya xavfi, dalilning huquqiy ishonchliligi va milliy tilga moslashtirish masalalari qo'shimcha ilmiy-amaliy tadqiqotlarni talab qiladi.

Kalit so'zlar: raqamli kriminalistika, DFIR, katta til modellari, LLM, Retrieval-Augmented Generation, RAG, voqealar xronologiyasi, kiberxavfsizlik, xotira kriminalistikasi, kiber hodisa.

Kirish

So'nggi o'n yillikda raqamli texnologiyalarning jamiyat hayotining barcha jabhalariga — davlat boshqaruvi, moliya tizimi, sog'liqni saqlash, ta'lim va kundalik shaxsiy muloqotga — chuqur kirib borishi, bir tomondan, iqtisodiy va ijtimoiy taraqqiyotga xizmat qilsa, ikkinchi tomondan, kiberxavfsizlik sohasida yangi turdagi, tobora murakkablashib borayotgan tahdidlarning (to'lov dasturlari, fishing hujumlari, ruxsatsiz kirish holatlari, IoT qurilmalariga qaratilgan hujumlar) paydo bo'lishiga olib keldi va bu, o'z navbatida, raqamli kriminalistika va hodisalarga chora ko'rish (Digital Forensics and Incident Response, DFIR) sohasining ahamiyatini keskin oshirdi. Zamonaviy kiber hodisalarning ko'lami va murakkabligi endilikda faqat texnik infratuzilmani himoya qilishni emas, balki hodisa yuz berganidan so'ng uni tezkor, ishonchli va huquqiy jihatdan asoslangan tarzda tergov qilish qobiliyatini ham talab qiladi, bu esa vaqt chizig'ini tahlil qilishning DFIR jarayonidagi markaziy o'rnini yanada mustahkamlaydi. DFIR — raqamli dalillarni aniqlash, yig'ish, tahlil qilish va sud-huquq jarayonida taqdim etishdan iborat murakkab jarayon bo'lib, uning markazida kiber hodisa davomida sodir bo'lgan voqealarning xronologik ketma-ketligini tiklash, ya'ni vaqt chizig'ini (timeline) tahlil qilish muhim o'rin egallaydi [2]. Xalqaro tadqiqotlar shuni ko'rsatadiki, DFIR mutaxassislarining atigi 40 foizi o'z ish jarayonlariga avtomatlashtirilgan tizimlarni joriy etgan, ulardan esa faqat beshdan bir qismi (taxminan 20 foizi) sun'iy intellektga asoslangan yechimlardan foydalanadi, natijada tergovchilar bitta ish (case) bo'yicha raqamli dalillarni tekshirishga o'rtacha 45 soat vaqt sarflaydi, mutaxassislarning esa 52 foizi ish jarayonini tezlashtirish uchun yanada ilg'or vositalarga bo'lgan ehtiyoj oshgan [2]. Bunday vaziyat, bir tomondan, tashkilotlarning ko'p sonli maxsus vositalar (masalan, log2timeline/Plaso, Timesketch, EnCase, FTK, Velociraptor) o'rtasida ma'lumotlarni qo'lda ko'chirish va bog'lashga majbur bo'lishi bilan, ikkinchi tomondan esa, yig'ilgan ma'lumotlarning hajmi ortib borayotgani bilan izohlanadi. Shu bilan birga, generativ sun'iy intellekt, xususan katta til modellari (Large Language Models, LLM) va ularning kontekstga boyitilgan variant — Retrieval-Augmented Generation (RAG) texnologiyasining

so'nggi 2025–2026-yillardagi jadal rivojlanishi DFIR jarayonlarini, xususan voqealar xronologiyasini avtomatik tiklash vazifasini tubdan o'zgartirish salohiyatiga ega ekanligini ko'rsatmoqda [2; 3; 4; 12]. Mazkur maqolaning maqsadi — raqamli kriminalistikada voqealar xronologiyasini tahlil qilishning nazariy-metodologik asoslarini, an'anaviy yondashuvlarning tizimli cheklovlarini hamda katta til modellari va RAG texnologiyasi integratsiyasining ilmiy-texnik imkoniyatlarini tahlil qilish, shuningdek, ushbu yo'nalishdagi xalqaro tajribani (AQSh, Yevropa, Osiyo davlatlari) O'zbekiston milliy qonunchiligi va ilmiy-amaliy kontekstiga nisbatan qiyosiy baholashdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi: birinchidan, DFIR sohasidagi asosiy nazariy tushunchalar va an'anaviy metodlarning ilmiy adabiyotlar asosida tizimlashtirilgan tahlilini berish; ikkinchidan, LLM va RAG texnologiyalarining arxitekturaviy-funksional tamoyillarini hamda ularning GenDFIR, ForensicLLM kabi zamonaviy freymvorklardagi amaliy qo'llanilishini yoritish; uchinchidan, xalqaro tajriba bilan O'zbekistonning kiberxavfsizlik sohasidagi qonunchilik va ilmiy-tadqiqot salohiyatini qiyosiy tahlil qilib, milliy sharoitda ushbu texnologiyalarni joriy etishning istiqbollari va cheklovlarini aniqlash. Tadqiqot predmeti sifatida raqamli kriminalistikada sun'iy intellektga asoslangan avtomatlashtirish jarayonlari, tadqiqot ob'ekti sifatida esa voqealar xronologiyasini tiklashning nazariy-metodologik modeli olindi. Maqolada qo'llanilgan metodologiya ilmiy adabiyotlarni tizimli tahlil qilish, qiyoslash va sintez qilish usullariga asoslanadi. Tadqiqotning ilmiy-nazariy ahamiyati shundaki, u DFIR sohasidagi generativ sun'iy intellekt yo'nalishidagi tarqoq xalqaro tadqiqotlarni yagona nazariy tizimga jamlab, ularni O'zbekiston ilmiy-huquqiy makoni bilan bog'liq holda tahlil qiladi, amaliy ahamiyati esa mazkur tahlil natijalarining kelgusi texnik-uslubiy tadqiqotlar, jumladan milliy DFIR amaliyoti uchun mo'ljallangan dasturiy vositalarni ishlab chiqishda dastlabki nazariy asos bo'lib xizmat qilishi mumkinligidadir.

1. Raqamli kriminalistikada voqealar xronologiyasini tahlil qilishning nazariy-metodologik asoslari va an'anaviy yondashuvlarning tizimli cheklovlari

Raqamli kriminalistika va hodisalarga chora ko'rish tushunchasi ilmiy adabiyotda ikki o'zaro bog'liq, ammo farqlanuvchi jarayonning birlashmasi sifatida talqin etiladi: raqamli kriminalistika (Digital Forensics, DF) raqamli dalilni dastlabki aniqlanishidan tortib sud-huquq jarayonida taqdim etilishigacha bo'lgan boshqaruv va tahlil jarayonini, jumladan dalilni identifikatsiya qilish, yig'ish va tahlil qilishni o'z ichiga oladi, bunda voqealar xronologiyasini tahlil qilish alohida o'rin tutadi, chunki aynan shu jarayon orqali harakatlarning xronologik ketma-ketligi tiklanib, hodisaning to'liq manzarasini tushunishga imkon beradi; hodisalarga chora ko'rish (Incident Response, IR) esa tashkilotning kiber hodisani aniqlash, boshqarish va yumshatish bo'yicha amalga oshiradigan chora-tadbirlari majmuasi bo'lib, u tayyorgarlik, aniqlash, tahlil, cheklash, yo'q qilish, tiklash va hodisadan keyingi faoliyat bosqichlaridan iborat, bunda tahlil bosqichida ham xronologik tartibni belgilash hodisaning qanday rivojlanganini baholashga xizmat qiladi [2]. Muhim nazariy jihat shundaki, DF va IR bir-birini o'zaro to'ldiruvchi jarayonlar sifatida qaraladi: agar IR ko'proq tashkiliy va tezkor choralarni, jumladan huquqiy-normativ jihatlarni boshqarishni o'z ichiga olsa, DF aynan shu boradagi bo'shliqni dalillarni to'g'ri yig'ish, hujjatlashtirish va sud jarayonida ishonchli taqdim etish orqali to'ldiradi, natijada vaqt chizig'ini tahlil qilish nafaqat texnik, balki huquqiy jarayonni ham bevosita qo'llab-quvvatlaydigan ko'prik vazifasini bajaradi. Ilmiy adabiyotda "raqamli artefakt" tushunchasining yagona rasmiy ta'rifi mavjud emasligi qayd etiladi, biroq amaliyotda u raqamli qurilmalardan yig'ilgan va tahlil uchun qayta ishlangan tegishli ma'lumotlar, jumladan fayl tizimi, operatsion tizim fayllari, tarmoq faoliyati, internet tarixi va kesh ma'lumotlari sifatida tushuniladi, "kiber hodisa voqeasi" esa tizimning xavfsizlik holatini buzishi mumkin bo'lgan harakat, "anomaliya" esa tizimning kutilgan me'yoriy xatti-harakatidan chetlanish sifatida belgilanadi [2].

AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan va xalqaro miqyosda keng tan olingan 800-86-sonli maxsus nashrda kriminalistik jarayon to'rtta asosiy bosqichga

— identifikatsiya/yig'ish, tekshirish, tahlil va hisobot berishga — bo'lib ko'rsatiladi hamda tergov ob'ekti bo'lishi mumkin bo'lgan to'rtta asosiy ma'lumot manbai turi, ya'ni fayllar, operatsion tizimlar, tarmoq trafigi va ilovalar bo'yicha batafsil uslubiy tavsiyalar beriladi, biroq bu hujjat huquqni muhofaza qilish nuqtai nazaridan emas, balki axborot texnologiyalari nuqtai nazaridan yozilganligi va bosqichma-bosqich to'liq qo'llanma sifatida emas, balki umumiy uslubiy asos sifatida qaralishi lozimligi alohida ta'kidlanadi [5].

Amaliyotda raqamli artefaktlarni dastlabki tahlil qilish odatda EnCase, FTK, Velociraptor, Dissect kabi ixtisoslashtirilgan vositalar yordamida amalga oshiriladi, so'ngra esa yig'ilgan voqealarni izchil va mazmunli xronologiyaga birlashtirish uchun log2timeline (Plaso) va Timesketch kabi maxsus vositalardan foydalaniladi, ular voqealarni bir-biriga bog'lash va vizualizatsiya qilish orqali tahlilni soddalashtiradi, Splunk kabi ilg'or platformalar esa sun'iy intellekt va mashinaviy o'qitish elementlaridan foydalanib, katta hajmdagi ma'lumotlar orasidan anomaliyalarni va g'ayrioddiy naqshlarni aniqlashga yordam beradi [2]. Shunga qaramay, aynan ushbu ko'p bosqichli va bir necha mustaqil vositaga tayangan yondashuv tizimli cheklovlarni keltirib chiqaradi: ma'lumotlarning tobora ortib borayotgan hajmi tufayli tahlil jarayoni sezilarli vaqt talab qiladi, bir vositadan ikkinchisiga ma'lumotlarni qo'lda o'tkazish xatolik ehtimolini oshiradi, tahlilchining shaxsiy tajribasi va malakasiga bog'liqlik esa natijalarning barqarorligini pasaytiradi, chunki turli tahlilchilar bir xil ma'lumot asosida turlicha xulosaga kelishi mumkin, bu esa dalilning ob'ektivligi va takrorlanuvchanligi (reproducibility) borasida qo'shimcha savollar tug'diradi — bu, ayniqsa, natija sud jarayonida raqib tomon ekspertizasiga topshirilishi mumkin bo'lgan hollarda alohida ahamiyat kasb etadi. Bu muammo, ayniqsa, xotira kriminalistikasi (memory forensics) sohasida yanada dolzarb tus oladi, chunki tizim operativ xotirasida (RAM) saqlanadigan volatil (o'zgaruvchan) ma'lumotlar tizim o'chirilishi yoki qayta ishga tushirilishi bilan yo'qolib ketadi va ularni tahlil qilish yuqori texnik malaka hamda vaqt talab qiladi; 2014–2024-yillar oralig'idagi 30 ta taqrizdan o'tgan tadqiqotni qamrab olgan tizimli sharh shuni ko'rsatadiki, xotira kriminalistikasi sohasida xotirani olish, artefaktlarni ajratib olish va mashinaviy o'qitishga asoslangan zararli dastur aniqlash usullari faol rivojlanmoqda, biroq bu usullarning aksariyati alohida-alohida ishlab chiqilgan bo'lib, ularni yagona integratsiyalashgan tizimga birlashtirish hamon dolzarb muammo bo'lib qolmoqda [6].

Xuddi shunday, xotira va tarmoq kriminalistikasini birlashtirgan SPECTRE nomli gibrid platforma taklif etilishi ham aynan shu integratsiya muammosini bartaraf etishga qaratilgan bo'lib, u xotira ma'lumotlarini (memory snapshot) samarali solishtirish orqali murakkab va tez rivojlanayotgan kiber tahdidlarni aniqlash imkonini beradi [7].

Umumiy tendensiyani baholovchi so'nggi sharhlar esa raqamli kriminalistikaning an'anaviy kompyuter tergovidan bulutli, IoT, kriptovalyuta va sun'iy intellektga asoslangan murakkab muhitlarga tomon rivojlanayotganini, shu bilan birga dalillarni olish, hodisa zanjirini (chain of custody) saqlash va anti-kriminalistik (iz yashiruvchi) texnikalarga qarshi kurashish borasidagi muammolar ham yanada murakkablashib borayotganini ta'kidlaydi [8]. Bundan tashqari, jinoyatchilarning iz yashirish maqsadida qo'llaydigan anti-kriminalistik texnikalari — masalan, fayl vaqt tamg'alarini sun'iy o'zgartirish (timestomping), tizim jurnallarini o'chirish yoki shifrlash — an'anaviy vositalar uchun qo'shimcha murakkablik yaratadi, chunki bunday holatlarda tergovchi nafaqat mavjud vaqt tamg'alariga, balki zaxira nusxalar, tarmoq darajasidagi loglar va server tomonidagi audit ma'lumotlari kabi bir necha mustaqil manbani o'zaro solishtirishga majbur bo'ladi, bu esa qo'lda bajariladigan tahlil hajmini yanada oshiradi. Yuqorida keltirilgan barcha omillar — ko'p vositaga bog'liqlik, ma'lumotlar hajmining ortishi, volatil ma'lumotlarning beqarorligi, muhitlarning xilma-xilligi hamda anti-kriminalistik qarshilik — birgalikda shuni ko'rsatadiki, voqealar xronologiyasini shunchaki vaqt oralig'i (timestamp) bo'yicha saralash emas, balki hodisalar o'rtasidagi vaqtinchalik, sabab-oqibat va semantik bog'liqliklarni chuqur tushunishga asoslangan tizimli avtomatlashtirish zarurati DFIR sohasida obyektiv ilmiy-amaliy

ehtiyojga aylanmoqda, bu esa keyingi bo'limda ko'rib chiqiladigan generativ sun'iy intellekt yechimlarining nazariy asoslanishini ta'minlaydi.

2. Katta til modellari va Retrieval-Augmented Generation texnologiyasining kriminalistik voqealar xronologiyasini avtomatlashtirishdagi arxitekturaviy-funksional imkoniyatlari

Katta til modellari generativ sun'iy intellektning eng ilg'or ko'rinishi sifatida inson tilini tushunish va generatsiya qilishga mo'ljallangan bo'lib, ular katta hajmdagi matnli ma'lumotlar asosida o'qitiladi va kirish ma'lumotlariga asoslanib so'zlar ketma-ketligini bashorat qilish qobiliyatiga ega, biroq ularning barchasi bir xil arxitekturaga ega emas: dekoderga asoslangan modellar (GPT, LLaMA, Mistral, Microsoft Phi kabi) avtoregressiv tarzda, ya'ni har bir keyingi tokenni oldingi tokenlar asosida bashorat qilib, matn generatsiya qilishda ustunlik qiladi va bu yerda so'rovni (prompt) to'g'ri shakllantirish, ya'ni prompt-injiniring alohida ahamiyat kasb etadi, chunki bu jarayon modelning kontekstni to'g'ri tushunishi va kriminalistik tahlil talablariga muvofiq javob berishini ta'minlaydi; enkoderga asoslangan modellar (masalan, BERT) esa tasniflash va aniqlash kabi vazifalarda, faqat kirish ma'lumotiga tayanib natija chiqarishda samarali; enkoder-dekoder modellar (T5, BART kabi) esa tarjima va matnni qisqartirish kabi vazifalarda kirish ma'lumoti va kontekstning birgalikdagi tahliliga asoslanadi [2]. Modelning matnni tushunishi tokenizatsiya va joylashtirish (embedding) jarayonlari orqali amalga oshiriladi: matn dastlab belgi, so'z yoki bo'g'in darajasidagi tokenlarga bo'linadi, so'ngra har bir token semantik ma'noni o'zida mujassam etuvchi zich sonli vektorga aylantiriladi, bu esa modelga matnlar o'rtasidagi o'xshashlik va bog'liqlikni matematik jihatdan baholash imkonini beradi [2].

Shu bilan birga, faqat LLM'ga tayangan yondashuv jiddiy nazariy cheklovlarga ega: birinchidan, model haqiqatda mavjud bo'lmagan ma'lumotni ishonchli tarzda "o'ylab topishi" mumkin (gallyutsinatsiya hodisasi), ikkinchidan, modelning kontekst oynasi cheklangan bo'lib, bu katta hajmdagi log fayllari yoki hodisa hisobotlarini bir vaqtning o'zida to'liq qayta ishlashga to'sqinlik qiladi, uchinchidan, model o'qitilgan ma'lumotlar bazasida mavjud bo'lmagan domenga xos yoki yangi kontekstdagi bilimlarga ega bo'lmaydi [2]. Aynan shu cheklovlarni bartaraf etish maqsadida Retrieval-Augmented Generation (RAG) texnologiyasi taklif etiladi, u ikkita asosiy funksiyani — qidirib topish (retrieval) va kengaytirilgan generatsiyani (augmented generation) — birlashtiradi: birinchi bosqichda tizim foydalanuvchi so'roviga eng mos keluvchi ma'lumotni tashqi bilim bazasidan (masalan, kosinus o'xshashligi, BM25 yoki TF-IDF kabi usullar yordamida) tanlab oladi, ikkinchi bosqichda esa topilgan tegishli ma'lumot LLM'ga uzatilib, u asosida aniqroq va kontekstga boy javob shakllantiriladi, bunda muhim jihat shundaki, RAG modelni qayta o'qitmaydi, balki faqat inferens vaqtida tashqi bilimni dinamik tarzda taqdim etadi [2].

Bunday yondashuvning kriminalistika uchun alohida qimmati shundaki, RAG orqali LLM'ga yo'naltiriladigan "bilim bazasi" aynan tergov qilinayotgan hodisaning o'ziga tegishli hujjatlar (masalan, hodisa davomida yig'ilgan log fayllari) bo'lib, bu modelning umumiy, ochiq internetdan olingan ma'lumotlarga emas, balki bevosita tekshirilayotgan ishning o'ziga xos kontekstiga tayanishini, shu orqali esa noaniq yoki tegishsiz ma'lumotlar asosida xulosa chiqarish xavfini kamaytirishni ta'minlaydi. Ushbu nazariy asosga tayangan holda ishlab chiqilgan GenDFIR freymvorki kiber hodisa ma'lumotlarini (odatda CSV formatidagi jurnal fayllarini) tizimlashtirilgan matnli hujjatga aylantirish va so'ngra RAG agenti orqali tegishli hodisalarni qidirib topish hamda ularni semantik jihatdan boyitish kabi ikki bosqichli yondashuvni taklif qiladi. Bunda alohida ilmiy yangilik sifatida "DFIR kontekstiga xos bo'laklarga bo'lish (chunking)" usuli ishlab chiqilgan — unga ko'ra har bir alohida hodisa yaxlit semantik bo'lak sifatida ko'riladi va bu vaqt tamg'alari kabi mayda, ammo kriminalistik jihatdan hal qiluvchi detallarning yo'qolib ketishining oldini oladi, bunga qo'shimcha ravishda, har bir hodisa yoki bo'lakning token sig'imi o'rta hisobda har bir tokenga to'g'ri keluvchi belgilar sonidan kelib chiqib hisoblanadi va bu qiymat qabul qiluvchi embedding modelning maksimal token sig'imidan oshmasligi lozimligi matematik cheklov sifatida belgilanadi. Bu esa bo'lakning o'lchami tanlangan modelning

texnik imkoniyatlariga muvofiq bo'lishini ta'minlaydi; bunday yondashuv Llama 3.1 8B modeli asosida, "zero-shot" (oldindan maxsus o'qitilmagan) rejimda sinovdan o'tkazilgan bo'lib, SYN-flood hujumi, "Rhino Hunt" nomli murakkab tarmoq hujumi stsenariysi, firibgarlik xatlari (phishing), ruxsatsiz kirish va DNS-spoofing kabi bir necha sintetik stsenariylarda DFIR sohasiga moslashtirilgan maxsus metrikalar hamda inson tomonidan qo'shimcha tekshiruv orqali baholangan [2].

GenDFIR'ga muqobil va uni to'ldiruvchi yondashuv sifatida ForensicLLM freymvorki taklif etilgan bo'lib, u bulutli infratuzilmaga bog'liqlik va umumiy maqsadli LLM'larning gallyutsinatsiya (mavjud bo'lmagan ma'lumotlarni o'ylab topish) xavfini kamaytirish maqsadida mahalliy (lokal) muhitda ishlaydigan va aynan raqamli kriminalistika vazifalari uchun maxsus sozlangan (fine-tuned) modeldan foydalanadi. Bu model DFRWS Yevropa 2025 konferensiyasida tanlangan model sifatida taqdim etilgan bo'lib, asosiy LLaMA-3.1-8B modeli va an'anaviy RAG usuliga nisbatan yuqoriroq natija ko'rsatgan hamda manba ma'lumotlarini to'g'ri ko'rsatishda 86,6 foizlik aniqlikka erishgan [12].

Sohadagi yana bir muhim muammo — LLM asosidagi kriminalistik yechimlarni baholash uchun yagona standartlashtirilgan metodologiyaning yo'qligi bo'lib, bu bo'shliqni to'ldirish maqsadida AQShning NIST tashkiloti tomonidan ishlab chiqilgan Computer Forensic Tool Testing (CFTT) dasturidan foydalanib, LLM'larning vaqt chizig'i tahlilidagi samaradorligini miqdoriy baholash uchun BLEU va ROUGE kabi metrikalarni qo'llashni tavsiya etuvchi va ChatGPT modeli asosida eksperimental tarzda tekshirilgan standartlashtirilgan metodologiya taklif etilgan [3]. Nihoyat, sohani yanada kengroq qamrab oluvchi so'nggi sharhlar shuni ko'rsatadiki, LLM'lar yordamida bulutli muhitlarda forensik tergovni avtomatlashtiruvchi freymvorklar jurnal ma'lumotlarini tasniflashda taxminan 89 foizlik o'qitish aniqligiga erishgan, shuningdek, mobil qurilmalar ma'lumotlaridan GPT-4o modeli yordamida "Forensic Intelligence Graphs" (kriminalistik intellektual grafiklar) deb ataluvchi dalillar tarmog'ini avtomatik quruvchi yechimlar ham ishlab chiqilmoqda [4].

Shunga qaramay, barcha ko'rib chiqilgan tadqiqotlarda umumiy va bir ovozdan ta'kidlanadigan xulosa shundan iboratki, LLM'ning chiqargan natijasi hozircha mustaqil kriminalistik xulosa sifatida emas, balki tergovchi-tahlilchining ishini yengillashtiruvchi yordamchi vosita sifatida qaralishi lozim, chunki gallyutsinatsiya (mavjud bo'lmagan ma'lumotlarni o'ylab topish) xavfi va dalil ishonchliligini saqlash zarurati inson tomonidan majburiy tekshiruv va tasdiqlashni talab qiladi. Shu bilan bir qatorda, sohada ChatGPT kabi umumiy maqsadli suhbat modellarining artefaktlarni tahlil qilish, muntazam ifodalar (regular expressions) va kalit so'zlar ro'yxatini generatsiya qilish, fayllarni qayta tiklash (file carving) uchun skriptlar yozish, RAID disklarini olish va parollarni buzish jarayonlarida yordamchi vosita sifatidagi imkoniyatlari alohida o'rganilgan bo'lib, bunda ham model natijalarining har doim inson tomonidan tekshirilishi zarurligi qat'iy shart sifatida qayd etiladi, shuningdek CADO kabi mahalliy LLM asosida ishlaydigan maxsus dasturiy platformalar tergovchilarga tahlil jarayonida amaliy yordam berish maqsadida ishlab chiqilmoqda.

3. Xalqaro tajriba va O'zbekiston milliy kontekstida qo'llashning huquqiy-institutsional istiqbollari: qiyosiy tahlil

Xalqaro miqyosda ushbu yo'nalishdagi ilmiy-texnik salohiyatni mintaqalar kesimida qiyoslash shuni ko'rsatadiki, Shimoliy Amerika, xususan AQSh, uzoq yillik institutsional tajribaga tayangan holda uslubiy yetakchilikni ta'minlaydi — buning yaqqol namunasi sifatida NIST tashkilotining 800-86-sonli maxsus nashrini keltirish mumkin, u hanuzgacha kriminalistik jarayonning bosqichma-bosqich uslubiy asosini belgilovchi asosiy me'yoriy-uslubiy hujjat sifatida xizmat qilmoqda [5]; Yevropa davlatlari, xususan Buyuk Britaniya va boshqa Yevropa mamlakatlaridagi tadqiqot markazlari (masalan, London Metropolitan universiteti Kiberxavfsizlik tadqiqot markazi) Elsevier nashriyotining Forensic Science International: Digital Investigation jurnali va unga bog'liq DFRWS Yevropa konferensiyasi platformasi orqali amaliy-empirik tadqiqotlarni faol nashr etmoqda, bu esa GenDFIR va ForensicLLM kabi freymvorklarning aynan shu hududda shakllanganligini izohlaydi [2; 3; 4; 12]; Osiyo davlatlari, xususan

Hindiston misolida ko'rish mumkinki, mintaqaviy ilmiy jurnallar (IJECS, IJERST) orqali xotira kriminalistikasi va raqamli kriminalistikaning umumiy holatini tizimli sharhlovchi ishlar soni ortib bormoqda, bu esa mintaqada ilmiy-tadqiqot salohiyatining bosqichma-bosqich shakllanayotganidan dalolat beradi [6; 8].

Uchta mintaqaning o'zaro nisbatini umumlashtirsak, AQSh uslubiy-me'yoriy asosni, Yevropa amaliy-texnologik innovatsiyani, Osiyo esa sohaviy bilimlarni tizimlashtirish va tarqatishda yetakchilik qilayotgani ko'zga tashlanadi, bu esa raqamli kriminalistikada LLM integratsiyasi bo'yicha global ilmiy manzaraning bir-birini to'ldiruvchi uch tarkibiy qismdan iborat ekanligini ko'rsatadi va bu uchala yo'nalishning birortasisiz ham sohaning izchil rivojlanishi to'liq bo'lmasligini anglatadi — uslubiy asossiz amaliy innovatsiya tartibsiz bo'ladi, amaliy sinovlarsiz uslubiy hujjat esa nazariy qolib ketadi, tizimli sharhlarsiz esa erishilgan yutuqlar keng ilmiy jamoatchilikka yetib bormaydi. Ushbu xalqaro manzaraga nisbatan O'zbekistonning holatini tahlil qilganda, avvalo, mamlakatda kiberxavfsizlik sohasini tartibga soluvchi asosiy huquqiy asos — 2022-yil 15-aprelda kuchga kirgan, 8 bob va 40 moddadan iborat "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasi Qonuni (O'RQ-764-son) ekanligini ta'kidlash lozim, unda kiberjinoyat, kibertahdid, kiberxavfsizlik, kibermudofaa va kiberhujum kabi asosiy tushunchalar belgilangan, Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi sifatida tayinlangan hamda xalqaro kiberjinoyatchilikka qarshi kurashish borasida xorijiy davlatlar va xalqaro tashkilotlar bilan axborot almashish tartibi (36-modda) mustahkamlangan [1].

Shu bilan birga, milliy ilmiy adabiyotni tahlil qilish shuni ko'rsatadiki, mavzu bo'yicha nashr etilgan so'nggi maqolalarning katta qismi hali texnik-metodologik emas, balki huquqiy-nazariy yo'nalishga ega: xususan, bir tadqiqotda kompyuter va raqamli kriminalistika sohasida xalqaro hamkorlikni kengaytirish, qonunchilikni modernizatsiya qilish va yuqori malakali kadrlar tayyorlash zarurligi asoslab berilgan bo'lsa [9], boshqa bir ishda kiberjinoyat tushunchasining nazariy-huquqiy tahlili doirasida elektron pochta dalillari va raqamli kriminalistika masalalari jinoyat huquqi nuqtai nazaridan yoritilgan [10], yana bir tadqiqotda esa jinoyat sodir bo'lgan joydan bevosita raqamli dalillarni qidirib topish, olish va protsessual jihatdan rasmiylashtirishning amaliy xususiyatlari — jumladan qurilmalarni to'g'ri o'chirish yoki o'chirmaslik qarorini qabul qilish, dalil zanjirini boshlang'ich bosqichdayoq hujjatlashtirish kabi masalalar — ko'rib chiqilgan [11], bundan tashqari, raqamli kriminalistikaning tarixiy taraqqiyoti va raqamli dalillardan foydalanish amaliyotini umumlashtiruvchi ishlar ham mavjud [13].

Ushbu tahlildan ko'rinib turibdiki, O'zbekistonda kiberxavfsizlik va raqamli kriminalistikaning huquqiy-institutsional asosi so'nggi yillarda izchil mustahkamlanib borayotgan bo'lsa-da, ikkinchi bo'limda batafsil yoritilgan LLM va RAG texnologiyalariga asoslangan vaqt chizig'ini avtomatik tiklash Jinoyat-protsessual kodeksida belgilangan dalil rasmiylashtirish talablariga moslashtirilmagan va sinovdan o'tkazilmagan holicha qolmoqda, bu esa global texnik chegara bilan milliy ilmiy-huquqiy infratuzilma o'rtasida aniq bo'shliq mavjudligini ko'rsatadi hamda kelgusi tadqiqotlar uchun kriminalistik bilim bazasini shakllantirish, RAG freymvorklarini mahalliy hodisa ma'lumotlarida sinash va bunda dalilning protsessual ishonchliligi hamda inson nazorati talablariga to'liq rioya qilishni ta'minlovchi metodologiyani ishlab chiqishdan iborat aniq va dolzarb ilmiy bo'shliqni belgilaydi. Shuni ham alohida ta'kidlash lozimki, so'nggi yillarda O'zbekistonda ushbu bo'shliqni institutsional darajada qisqartirishga qaratilgan dastlabki qadamlar ham qo'yilmoqda — jumladan, ixtisoslashtirilgan kadrlar tayyorlash va amaliy-ilmiy salohiyatni oshirishga yo'naltirilgan yangi ta'lim va tadqiqot tuzilmalarining tashkil etilishi — biroq bunday institutsional o'zgarishlarning texnik-metodologik natijalarga, xususan LLM/RAG asosidagi vositalarning milliy tilga moslashtirilgan holda amaliyotga joriy etilmagan, shu sababli bu yo'nalish o'rta muddatli istiqbolda alohida ilmiy kuzatuv predmeti bo'lib qolishi mumkin.

Xulosa

Mazkur maqolada raqamli kriminalistikada voqealar xronologiyasini tahlil qilishning nazariy-metodologik asoslari, an'anaviy yondashuvlarning tizimli cheklovlari hamda katta til modellari va Retrieval-Augmented Generation texnologiyasi integratsiyasining ilmiy-texnik imkoniyatlari tahlil qilindi. Tahlil jarayinlari shuni ko'rsatdiki, GenDFIR, ForensicLLM kabi zamonaviy freymvorklar an'anaviy ko'p vositali yondashuvning vaqt va inson resursi sarfini sezilarli darajada qisqartirish salohiyatiga ega, biroq bu texnologiyalar hali gallyutsinatsiya (mavjud bo'lmagan ma'lumotlarni o'ylab topish) xavfi, standartlashtirilgan baholash metodologiyasining yetishmasligi va dalil ishonchliligini ta'minlash kabi jiddiy ilmiy-amaliy muammolarga ega bo'lib qolmoqda, shu sababli ularning natijalari mustaqil kriminalistik xulosa emas, balki inson tomonidan tasdiqlanishi lozim bo'lgan yordamchi vosita sifatida baholanishi zarur. Xalqaro tajribani O'zbekiston bilan qiyoslash shuni ko'rsatdiki, mamlakatda kiberxavfsizlikning huquqiy-institutsional asosi (xususan, "Kiberxavfsizlik to'g'risida"gi Qonun) izchil mustahkamlanayotgan bo'lsa-da, milliy ilmiy adabiyot hozircha asosan huquqiy-nazariy yo'nalishda rivojlanmoqda va LLM/RAG asosidagi texnik-metodologik tadqiqotlar deyarli mavjud emas. Shu bois, keyingi bosqichda milliy tilidagi kriminalistik ma'lumotlar bazasini shakllantirish va mahalliy hodisa stsenariylarida RAG freymvorklarini amaliy sinovdan o'tkazishga qaratilgan texnik-amaliy tadqiqot muhim ahamiyat kasb etmoqda.

Foydalanilgan adabiyotlar

I. Qonunchilik hujjatlari

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 2022-yil 15-aprel, O'RQ-764-son (Oliy Majlis Senati tomonidan qabul qilingan; 2022-yil 17-iyuldan kuchga kirgan; 8 bob, 40 modda) // Qonunchilik ma'lumotlari milliy bazasi. https://lex.uz/uz/docs/-5960604

II. Ilmiy maqolalar

2. Loumachi F.Y., Ghanem M.C., Ferrag M.A. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models // Computers (MDPI, Shveytsariya). — 2025. — Vol. 14, No. 2, Art. 67. — 25 b. DOI: 10.3390/computers14020067. Havola: https://www.mdpi.com/2073-431X/14/2/67
3. Towards a standardized methodology and dataset for evaluating LLM-based digital forensic timeline analysis // Forensic Science International: Digital Investigation (Elsevier, Niderlandiya). — 2025. Havola: https://www.sciencedirect.com/science/article/pii/S2666281725001222
4. Large language models in digital forensics: capabilities, challenges and future directions // Forensic Science International: Digital Investigation (Elsevier, Niderlandiya). — 2026, yanvar. Havola: https://www.sciencedirect.com/science/article/pii/S2666281725001830
5. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response // NIST Special Publication 800-86. — Geythersburg: AQSh Savdo vazirligi huzuridagi Milliy standartlar va texnologiyalar instituti (NIST), 2006. — 121 b. Havola: https://csrc.nist.gov/pubs/sp/800/86/final
6. Analysis of Developments in Memory Forensics for Malware Detection: A Systematic Review (2014–2024) // International Journal of Engineering and Computer Science (Hindiston). — 2026. — Vol. 15, No. 2. Havola: https://ijecs.in/index.php/ijecs/article/view/5433
7. SPECTRE: a hybrid and adaptive cyber threats detection and response in volatile memory // International Journal of Information Security (Springer Nature, Germaniya). — 2026. DOI: 10.1007/s10207-026-01212-6. Havola: https://link.springer.com/article/10.1007/s10207-026-01212-6
8. A Review on Digital Forensics // International Journal of Engineering Research and Science & Technology (Hindiston). — 2026. Havola: https://ijerst.org/index.php/ijerst/article/view/3856

9. Kompyuter va raqamli kriminalistika sohasida xalqaro hamkorlik va qonunchilikni modernizatsiya qilish masalalari // International Journal of Science and Technology (O'zbekiston). — 2026. — B. 3–8. Havola: https://science-technology.uz/index.php/journal/article/download/695/651/1256
10. Kiberjinoyat tushunchasining nazariy-huquqiy tahlili, kelib chiqish tarixi va mazmuni // Multidisciplinary Journal of Science and Technology (O'zbekiston). — 2026. — 6-jild, 6-son. Havola: https://mjstjournal.com/index.php/mjst/article/view/7668
11. Hodisa sodir bo'lgan joydan raqamli dalillarni qidirib topish, olish va rasmiylashtirishning o'ziga xos xususiyatlari // TADQIQOTLAR jahon ilmiy-metodik jurnali (O'zbekiston). — 2025. — 59-son, 3-qism. Havola: https://scientific-jl.com/tad/article/view/7498

III. Ilmiy tezislar va konferensiya materiallari

12. ForensicLLM: A local large language model for digital forensics // Forensic Science International: Digital Investigation (Elsevier) — DFRWS Yevropa 2025 (Digital Forensics Research Workshop Europe) konferensiyasida tanlangan maqola. — 2025. Havola: https://www.sciencedirect.com/science/article/pii/S2666281725000113
13. Raqamli kriminalistika va raqamli dalillardan foydalanish tarixi // "Jamiyat va innovatsiyalar" (Society and Innovations) ilmiy jurnali materiallari asosida, ResearchGate ilmiy platformasida joylashtirilgan. Havola: https://www.researchgate.net/publication/378464400_Raqamli_kriminalistika_va_raqamli_dalillardan_foydalanish_tarixi

IV. Veb-manbalar

14. Kiberxavfsizlik to'g'risidagi qonun: DXXga qanday yangi vakolatlar berildi? // Kun.uz axborot agentligi, 2022-yil 18-aprel. Havola: https://kun.uz/news/2022/04/18/kiberxavfsizlik-togrisidagi-qonun-dxxga-qanday-yangi-vakolatlar-berildi
15. "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasi Qonuni — huquqiy sharh // Regulations.AI — The Site on AI Laws and Regulations. Havola: https://regulations.ai/regulations/RAI-UZ-NA-ZRU7640-2022