Rəqəmsal Kriminalistika Sahəsində Elmi-Texnoloji Problemlərin Cari Vəziyyətinin Tədqiqi və Müqayisəli Analizi

Sənan Vəlizadə
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
senanvalizade@gmail.com

***Xülasə*— Məqalədə rəqəmsal kriminalistika sahəsinin nəzəri əsasları, metodoloji çərçivələri və müasir texnoloji inkişaf istiqamətləri sistemli şəkildə təhlil olunur. Tədqiqat çərçivəsində böyük həcmli verilənlərin emalı, bulud və IoT mühitlərində kriminalistika, eləcə də rəqəmsal sübutların hüquqi qəbul olunması ilə bağlı əsas problemlər araşdırılmışdır. Ənənəvi kriminalistika metodları ilə süni intellekt, blokçeyn və paylanmış sistemlərə əsaslanan müasir yanaşmaların müqayisəli analizi aparılmışdır. Nəticələr texnoloji effektivlik ilə kriminalistik tələblərə uyğunluq arasında mövcud ziddiyyəti göstərir. Eyni zamanda beynəlxalq standartların və milli qanunvericilikdəki yeniliklərin rolu vurğulanır, gələcək tədqiqat istiqamətləri müəyyən edilir.**

Açar sözlər— rəqəmsal kriminalistika; rəqəmsal sübutlar; rəqəmsal artefaktlar; kriminalistik tələblərə uyğunluq.

I. GİRİŞ

Rəqəmsal texnologiyaların sürətli inkişafı və informasiya sistemlərinin cəmiyyətin bütün sahələrinə inteqrasiyası kibercinayətkarlığın həm miqyasının, həm də mürəkkəblik səviyyəsinin əhəmiyyətli dərəcədə artmasına səbəb olmuşdur. Müasir dövrdə kibercinayətlər yalnız fərdi istifadəçiləri deyil, həm də dövlət qurumlarını, maliyyə institutlarını və kritik infrastruktur obyektlərini hədəf alır. Bu kontekstdə rəqəmsal kriminalistika rəqəmsal mühitdə baş verən hadisələrin aşkar edilməsi, təhlili və hüquqi baxımdan əsaslandırılmış şəkildə təqdim olunması üçün əsas alətlərdən biri kimi çıxış edir [1, 2].

Rəqəmsal kriminalistikanın rolu yalnız texniki analizlə məhdudlaşmır. Bu sahə eyni zamanda sübutların bütövlüyünün qorunması, onların əldə olunması prosesinin düzgün sənədləşdirilməsi və məhkəmə proseslərində etibarlı sübut bazasının formalaşdırılması kimi mühüm funksiyaları yerinə yetirir. Klassik yanaşmalarda bu proseslər müəyyən standartlara əsaslansa da, müasir texnoloji mühitlərdə bu yanaşmaların effektivliyi müəyyən hallarda məhdud qalır [3].

Son illərdə aparılan tədqiqatlar göstərir ki, rəqəmsal kriminalistika sahəsi yeni texnoloji çağırışlarla üz-üzədir. Xüsusilə böyük həcmli verilənlərin sürətlə artması, bulud əsaslı xidmətlərin geniş yayılması, əşyaların interneti (IoT) cihazlarının sayının çoxalması və süni intellekt texnologiyalarının tətbiqi kriminalistik proseslərin mürəkkəbləşməsinə səbəb olmuşdur [4, 5, 6].

Bundan əlavə, rəqəmsal sübutların elmi əsaslandırılması və onların hüquqi baxımdan istifadəsi ilə bağlı problemlər hələ də aktual olaraq qalır [3, 7].

Müasir yanaşmalar, xüsusilə süni intellekt və maşın təlimi əsaslı metodları, bu problemlərin həllində yeni imkanlar təqdim edir. Lakin bu metodların tətbiqi zamanı nəticələrin izah olunması və hüquqi əsaslandırılması kimi yeni məsələlər meydana çıxır [5, 8].

Tədqiqatın əsas məqsədi rəqəmsal kriminalistika sahəsində mövcud elmi-texnoloji problemlərin sistemli şəkildə təhlil edilməsi və müasir texnoloji yanaşmalar əsasında müqayisəli analizinin aparılmasıdır.

II. RƏQƏMSAL KRİMİNALİSTİKANIN ƏSASLARI VƏ METODOLOJİ ÇƏRÇİVƏSİ

A Əsas anlayışların formal tərifi və konseptual çərçivə

Elektron sübutlar elektron mühitdə saxlanılan və hüquqi əhəmiyyət daşıyan məlumatları ifadə edir və bu məlumatlar kompüter sistemləri, mobil qurğular, şəbəkə infrastrukturları və bulud mühitləri daxil olmaqla müxtəlif mənbələrdən əldə oluna bilər [1]. Müasir informasiya sistemlərində məlumatların dinamik xarakter daşıması və tez-tez dəyişməsi onların sabit sübut kimi qiymətləndirilməsini çətinləşdirir və sübutların vaxtında əldə olunmasını zəruri edir [5].

Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində elektron sübut anlayışı cinayət təqibi üzrə əhəmiyyət kəsb edən halların müəyyən edilməsinə kömək edən elektron verilənlər kimi müəyyən edilmişdir. Bu verilənlərə abunəçi məlumatları, trafik və məzmun verilənləri daxildir və onlar cinayət prosesini həyata keçirən orqanın qərarı ilə, bu Məcəllənin tələbləri nəzərə alınmaqla, elektron formada sübut kimi qəbul olunur [9].

Sübutların qorunma zənciri (chain of custody) sübutların əldə edilməsindən təqdim olunmasına qədər bütün mərhələlərdə aparılan əməliyyatların ardıcıllıqla sənədləşdirilməsini və sübutların bütövlüyünün qorunmasını təmin edən prosedurlar sistemidir [1]. Bu yanaşma sübutların hansı şəraitdə və hansı üsullarla əldə olunduğunu müəyyən etməyə imkan verir və onların hüquqi baxımdan etibarlılığını təmin edir, lakin paylanmış və bulud mühitlərində bu prosesin həyata keçirilməsi əlavə çətinliklər yaradır [10].

DOI: 10.25045/forensic.gov.2026.32

Kriptoqrafik heş funksiyaları (hash functions) rəqəmsal məlumatın tamlığını təmin etmək üçün istifadə olunur və məlumat üçün sabit uzunluqlu unikal heş qiyməti yaradır [1]. Bu mexanizm sübutların bütövlüyünün yoxlanılması üçün fundamental vasitə hesab olunur və kriminalistik analiz prosesində geniş tətbiq edilir.

Statik və canlı əldə etmə (static vs live acquisition) sübutların hansı şəraitdə toplanmasını ifadə edir. Statik əldə etmə sistemin söndürülmüş vəziyyətində həyata keçirilir və məlumatların dəyişməz qalmasını təmin edir. Canlı əldə etmə isə işlək sistem üzərindən məlumatların toplanmasını nəzərdə tutur və operativ yaddaş kimi dəyişkən məlumatlara çıxış imkanı yaradır [1]. Lakin bu yanaşma sübutların dəyişməsi riskini də artırır və xüsusi metodoloji yanaşma tələb edir.

Volatil məlumatlar (volatile data) qısa müddət ərzində dəyişə və ya silinə bilən məlumatlardır və əsasən operativ yaddaş, keş məlumatları və şəbəkə trafiki kimi mənbələrdə mövcud olur [5]. Bu məlumatların vaxtında əldə olunmaması sübutların itirilməsi ilə nəticələnə bilər.

Volatil məlumatların prioritetləşdirilməsi (volatile data prioritization) tez dəyişən məlumatların ilk növbədə əldə olunmasını nəzərdə tutur və kriminalistik prosesin səmərəliliyinə birbaşa təsir göstərir [5]. Müasir tədqiqatlar göstərir ki, bu yanaşma xüsusilə dinamik sistemlərdə kritik əhəmiyyət daşıyır.

Metaverilənlər fayllar və ya məlumatlar haqqında əlavə məlumatları, o cümlədən yaradılma vaxtı, dəyişdirilmə tarixi və digər atributları əhatə edir [3]. Bu məlumatlar hadisələrin zaman ardıcıllığının müəyyənləşdirilməsində mühüm rol oynayır.

Rəqəmsal artefaktlar sistem və istifadəçi fəaliyyətinin nəticəsi olaraq yaranan məlumat izləridir və hadisələrin bərpası üçün əsas məlumat mənbələrindən biri hesab olunur [2]. Bu artefaktlar loqlar, keş faylları və sistem qeydləri kimi müxtəlif formalarda mövcud ola bilər.

Zaman ardıcıllığı analizi müxtəlif mənbələrdən əldə olunmuş məlumatların zaman ardıcıllığı üzrə birləşdirilməsini və hadisələrin xronoloji şəkildə bərpa olunmasını təmin edir [5]. Bu yanaşma mürəkkəb insidentlərin təhlilində səbəb-nəticə əlaqələrinin müəyyənləşdirilməsinə imkan verir.

Məlumatın bütövlüyü (data integrity) sübutların əldə olunması və saxlanması prosesində onların dəyişdirilməzliyinin təmin edilməsi prinsipidir [1]. Bu prinsip kriminalistik prosesin etibarlılığının əsas göstəricilərindən biridir. Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsinin 133-3-cü maddəsi elektron verilənlərin mühafizəsinin təmin olunmasına yönəlmiş mühüm hüquqi mexanizmləri müəyyən edir. Maddəyə əsasən, cinayət təqibi üçün əhəmiyyət kəsb edən elektron verilənlərin itkiyə və ya modifikasiyaya məruz qalmasının qarşısını almaq məqsədilə şifrləmə və digər texniki tədbirlərin tətbiqi nəzərdə tutulur. Bu yanaşma rəqəmsal kriminalistikada əsas prinsiplərdən biri olan kriminalistik tələblərə uyğunluğun (forensic soundness) təmin edilməsi ilə birbaşa əlaqəlidir. Belə ki, elektron sübutların əldə olunması və saxlanılması prosesində onların bütövlüyünün qorunması və dəyişdirilməzliyinin təmin edilməsi həm texniki, həm də hüquqi baxımdan əsas tələb kimi çıxış edir. Bu baxımdan qeyd olunan norma rəqəmsal sübutların etibarlılığının təmin olunması üçün normativ baza rolunu oynayır [9].

Kriminalistik tələblərə uyğunluq (forensic soundness) rəqəmsal sübutların əldə olunması və analizi prosesinin sübutların məzmununa təsir etmədən, bütün əməliyyatlar sənədləşdirilməklə və sonradan yoxlanıla bilən üsullarla həyata keçirilməsini ifadə edir [1, 3]. Müasir texnoloji mühitlərdə bu prinsipin təmin olunması xüsusilə çətinləşir və əlavə metodoloji yanaşmalar tələb edir.

Müasir texnoloji mühitlərdə, xüsusilə bulud və paylanmış sistemlərdə, bu anlayışların tətbiqi daha mürəkkəb xarakter alır və əlavə metodoloji yanaşmalar tələb edir [4, 5]. Bu isə rəqəmsal kriminalistikanın inkişafında yeni konseptual modellərin işlənib hazırlanmasını zəruri edir.

B Beynəlxalq standartlar və metodoloji çərçivələr

Beynəlxalq standartlar və metodoloji çərçivələr (international standards and frameworks) rəqəmsal kriminalistika proseslərinin vahid prinsiplər əsasında həyata keçirilməsini təmin edən əsas mexanizmlərdən biri hesab olunur. Bu standartlar rəqəmsal sübutların identifikasiyası, toplanması, əldə olunması, qorunması və analizi mərhələlərində tətbiq olunan metodların sistemli və hüquqi baxımdan əsaslandırılmış şəkildə icrasına imkan yaradır.

Rəqəmsal kriminalistika sahəsində ilkin sistemli metodoloji yanaşmalardan biri "DFRWS" (Digital Forensic Research Workshop) tərəfindən təklif olunmuş çərçivə hesab edilir. Bu model identifikasiya, mühafizə, toplama, analiz və təqdimat mərhələləri üzrə strukturlaşdırılmış yanaşma təqdim etməklə sonrakı metodologiyaların formalaşmasına təsir göstərmişdir [11].

Metodoloji yanaşmaların sonrakı inkişaf mərhələsində Reith, Carr və Gunsch tərəfindən irəli sürülmüş "Abstract Digital Forensics Model" (ADF) rəqəmsal araşdırma prosesini daha geniş və detallı mərhələlər üzrə sistemləşdirmişdir. Sözügedən model hazırlıq, strategiyanın müəyyən olunması, qorunma, toplama, analiz, təqdimat və sübutların geri qaytarılması kimi mərhələləri özündə birləşdirir [11].

Ümumilikdə, rəqəmsal kriminalistika modellərinin inkişafı sadə sübut toplama yanaşmalarından çoxmərhələli və strukturlaşdırılmış metodoloji çərçivələrə doğru təkamül etdiyini göstərir. Bu yanaşmalar müasir standartların və praktik metodların formalaşmasına nəzərəçarpacaq təsir göstərmişdir.

Bununla yanaşı, "ACPO" (Association of Chief Police Officers) prinsipləri rəqəmsal sübutlarla işləmə zamanı məlumatların dəyişdirilməməsi, proseslərin sənədləşdirilməsi və məsuliyyət bölgüsünün aydın müəyyən olunması baxımından praktik əhəmiyyət daşıyır [1].

ISO/IEC 27037 standartı rəqəmsal sübutların identifikasiyası, toplanması, əldə olunması və qorunması üzrə əsas prinsipləri müəyyən edir və sübutların bütövlüyünün qorunmasını prioritet kimi qəbul edir [12]. Bu standart sübutların əldə olunması prosesində müdaxilənin minimuma endirilməsini və bütün əməliyyatların sənədləşdirilməsini tələb etməklə kriminalistik tələblərə uyğunluğun təmin olunmasında fundamental rol oynayır.

ISO/IEC 27041 və ISO/IEC 27042 standartları rəqəmsal

sübutların analizi və interpretasiyası mərhələlərinə yönəlmişdir və istifadə olunan metodların elmi əsaslandırılmasını təmin etməyə xidmət edir [12]. Bu çərçivələr kriminalistik proseslərin obyektivliyinin artırılmasına və nəticələrin əsaslandırılmış şəkildə təqdim olunmasına imkan yaradır.

ISO/IEC 27043 standartı isə insidentlərin araşdırılması prosesinin ümumi metodoloji çərçivəsini müəyyən edir və kriminalistik fəaliyyətlərin strukturlaşdırılmış şəkildə həyata keçirilməsini təmin edir [14]. Bu standart müxtəlif mərhələlər arasında əlaqənin qurulmasına və proseslərin sistemli şəkildə idarə olunmasına şərait yaradır.

NIST SP 800-86 sənədi rəqəmsal kriminalistika metodlarının insidentlərin idarə olunması prosesinə inteqrasiyasını təsvir edən əsas metodoloji sənədlərdən biridir [13]. Bu çərçivə praktik mühitdə kriminalistik fəaliyyətlərin həyata keçirilməsi üçün geniş istifadə olunur və xüsusilə əməliyyat səviyyəsində tətbiq baxımından əhəmiyyətlidir.

Beləliklə, beynəlxalq standartlar rəqəmsal kriminalistika sahəsində vahid metodoloji yanaşmanın formalaşdırılmasına, sübutların etibarlılığının təmin olunmasına və müxtəlif sistemlər arasında uyğunluğun artırılmasına xidmət edir.

C Rəqəmsal kriminalistik prosesin mərhələləri və onların analizi

Rəqəmsal kriminalistik proses (digital forensic process) rəqəmsal mühitdə baş vermiş hadisələrin aşkar edilməsi, sübutların əldə olunması, təhlili və nəticələrin hüquqi baxımdan təqdim olunmasını əhatə edən mərhələli fəaliyyətlər sistemidir və bu mərhələlərin hər biri ümumi nəticənin etibarlılığına birbaşa təsir göstərir [1, 2]. Müasir tədqiqatlar göstərir ki, bu proses yalnız texniki əməliyyatların ardıcıllığı deyil, həm də metodoloji və hüquqi tələblərlə şərtlənən kompleks yanaşmadır [3].

Aşkarlanma mərhələsi (identification) araşdırma üçün əhəmiyyətli olan rəqəmsal sübut mənbələrinin müəyyən edilməsini nəzərdə tutur və bu mərhələdə sistemlər, cihazlar və potensial məlumat daşıyıcıları identifikasiya edilir [1]. Lakin müasir mühitlərdə məlumatların paylanmış şəkildə saxlanılması və müxtəlif platformalarda yerləşməsi bu mərhələnin həyata keçirilməsini mürəkkəbləşdirir və sübut mənbələrinin tam müəyyən edilməsini çətinləşdirir [10].

Qorunma mərhələsi (preservation) əldə olunmuş sübutların dəyişdirilmədən saxlanılmasını və onların etibarlılığının sonrakı mərhələlər üçün təmin edilməsini nəzərdə tutur. Bu məqsədlə kriptoqrafik heş mexanizmləri və sənədləşdirmə prosedurları tətbiq olunur [1].

Toplanma mərhələsi (collection) müəyyən edilmiş mənbələrdən məlumatların əldə olunmasını əhatə edir və bu proses zamanı sübutların bütövlüyünün qorunması əsas tələb kimi çıxış edir [1]. Klassik yanaşmalarda bu mərhələ bit səviyyəsində surətlərin çıxarılması ilə həyata keçirilsə də, müasir sistemlərdə böyük həcmli verilənlər və paylanmış arxitektura bu yanaşmanın tətbiqini çətinləşdirir [5]. Bu səbəbdən selektiv məlumat toplama və prioritetləşdirmə metodlarının tətbiqi aktuallaşır.

Analiz mərhələsi (analysis) toplanmış məlumatların təhlil olunmasını və hadisələrin bərpasını əhatə edir [2]. Ənənəvi metodlar fayl sistemləri, loqlar və şəbəkə trafiki üzərində aparılan analizlərə əsaslansa da, müasir dövrdə süni intellekt və maşın təlimi əsaslı yanaşmaların tətbiqi geniş yayılmışdır [5]. Bununla belə, bu metodların nəticələrinin izah olunması və hüquqi baxımdan əsaslandırılması problemləri hələ də aktual olaraq qalır [8].

Təqdimat mərhələsi (presentation) əldə olunmuş nəticələrin hüquqi tələblərə uyğun şəkildə təqdim edilməsini nəzərdə tutur və kriminalistik prosesin ən məsuliyyətli mərhələlərindən biri hesab olunur [1]. Bu mərhələdə texniki nəticələrin aydın, əsaslandırılmış və yoxlanıla bilən formada təqdim olunması tələb olunur. Müasir tədqiqatlar göstərir ki, mürəkkəb analitik nəticələrin hüquqi müstəvidə izah edilməsi xüsusilə süni intellekt əsaslı yanaşmalarda çətinlik yaradır [3, 8].

Kriminalistik tələblərə uyğunluq (forensic soundness) rəqəmsal kriminalistik prosesin bütün mərhələlərində kriminalistik tələblərə uyğunluğun qorunması və istifadə olunan metodların yoxlanıla bilməsi əsas prinsip kimi çıxış edir [1, 3].

Müasir rəqəmsal mühitlərdə proses mərhələləri hər zaman xətti ardıcıllıqla icra olunmur və bəzi hallarda paralel şəkildə həyata keçirilə bilər. Bu xüsusiyyət araşdırma prosesində daha çevik əməliyyat koordinasiyasını tələb edir [4, 5]. Bu baxımdan rəqəmsal kriminalistika sahəsində metodoloji yanaşmaların yenilənməsi və müasir texnoloji mühitlərə uyğunlaşdırılması əsas tədqiqat istiqamətlərindən biri kimi çıxış edir.

III. RƏQƏMSAL KRİMİNALİSTİKADA ELMİ-TEXNOLOJİ PROBLEMLƏRİN CARİ VƏZİYYƏTİ

Rəqəmsal kriminalistika sahəsində mövcud elmi-texnoloji problemlər informasiya texnologiyalarının sürətli inkişafı və rəqəmsal mühitlərin mürəkkəbləşməsi ilə sıx bağlıdır. Klassik kriminalistik yanaşmalar əsasən məhdud və strukturlaşdırılmış mühitlər üçün nəzərdə tutulmuşdur və bu səbəbdən müasir paylanmış sistemlərdə onların tətbiqi məhdudlaşır [1, 2]. Xüsusilə bulud texnologiyaları, IoT mühitləri və böyük həcmli verilənlər yeni problemlərin yaranmasına səbəb olur [4, 10].

A *Texniki problemlər*

Böyük həcmli verilənlərin (big data) emalı müasir rəqəmsal kriminalistikanın əsas texniki problemlərindən biridir. Verilənlərin həcminin sürətlə artması onların tam şəkildə toplanması və analizini çətinləşdirir və ənənəvi alətlərin effektivliyini azaldır [5]. Bu kontekstdə böyük verilənlərin emalı üçün xüsusi yanaşmaların tətbiqi zəruri hesab olunur [14].

Bulud mühitlərində sübutların əldə olunması (cloud forensics) məlumatların fiziki yerləşmə yerinin qeyri-müəyyən olması və müxtəlif hüquqi məkanlarda saxlanılması ilə əlaqədardır [10]. Bu problem yalnız texniki deyil, həm də hüquqi çətinliklər yaradır və sübutların əldə olunmasını mürəkkəbləşdirir [15].

IoT mühitlərində kriminalistika (IoT forensics) cihazların heterogenliyi və məlumat formatlarının müxtəlifliyi səbəbindən mürəkkəbləşir [5, 16]. Bu cihazlarda məlumatların tez dəyişməsi onların operativ şəkildə əldə olunmasını tələb edir.

Şifrələmə və anonimlik texnologiyaları (encryption and

anonymization) sübutlara çıxışı məhdudlaşdırır və bəzi hallarda məlumatların təhlilini çətinləşdirir [3]. Bu isə kriminalistik prosesin səmərəliliyinə birbaşa təsir göstərir.

B *Metodoloji və elmi problemlər*

Rəqəmsal sübutların elmi əsaslandırılması (scientific validation) bu sahədə əsas problemlərdən biri olaraq qalır. Mövcud tədqiqatlar göstərir ki, vahid metodoloji çərçivənin olmaması nəticələrin obyektiv qiymətləndirilməsini çətinləşdirir [7].

Nəticələrin təkrar əldə olunması problemi (reproducibility) müxtəlif mühitlərdə aparılan analizlərin fərqli nəticələr verməsi ilə əlaqədardır və bu, istifadə olunan metodların etibarlılığına təsir göstərir [3].

Kriminalistik metodların qiymətləndirilməsi (evaluation problem) üçün vahid "benchmark" mühitlərinin olmaması yeni yanaşmaların effektivliyinin müqayisəsini çətinləşdirir [4, 17].

C *Hüquqi və etik problemlər*

Transsərhəd hüquqi problemi (cross-border jurisdiction) məlumatların müxtəlif ölkələrdə yerləşən serverlərdə saxlanılması ilə bağlıdır və bu, sübutlara çıxışı məhdudlaşdırır [10, 15].

Məxfilik və şəxsi məlumatların qorunması (privacy concerns) sübutların əldə olunması prosesində hüquqi məhdudiyyətlər yaradır və bəzi hallarda məlumatların tam əldə olunmasına mane olur.

Etik problemlər (ethical challenges) xüsusilə süni intellekt əsaslı sistemlərin tətbiqi zamanı aktuallaşır və bu sistemlərin qərar mexanizmlərinin qeyri-şəffaf olması ilə bağlıdır [7].

Qeyd etmək lazımdır ki, son dövrlərdə milli qanunvericilikdə də rəqəmsal sübutların hüquqi statusu ilə bağlı mühüm dəyişikliklər baş vermişdir. Belə ki, Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsinə elektron sübut anlayışının daxil edilməsi (124-cü maddənin 124.2.3-1-ci bəndi) rəqəmsal kriminalistika sahəsinin hüquqi əsaslarının gücləndirilməsi baxımından əhəmiyyətli addım kimi qiymətləndirilə bilər. Bu dəyişiklik rəqəmsal sübutların məhkəmə proseslərində istifadə imkanlarını genişləndirməklə yanaşı, onların əldə olunması və təqdim olunması ilə bağlı metodoloji yanaşmaların da daha dəqiq müəyyənləşdirilməsini zəruri edir [9].

D *Anti-kriminalistika və təhlükə faktorları*

Anti-kriminalistika üsulları (anti-forensics) sübutların gizlədilməsi və ya dəyişdirilməsi məqsədilə istifadə olunur və kriminalistik prosesin effektivliyini azaldır. Müasir tədqiqatlar bu üsulların daha mürəkkəb xarakter aldığını göstərir [18].

Məlumatların silinməsi və manipulyasiyası sübutların bərpasını çətinləşdirir və analiz nəticələrinin etibarlılığına təsir göstərir.

E *İnsan faktoru və təşkilati problemlər*

İnsan faktoru kriminalistik analiz nəticələrinə təsir edən əsas amillərdən biridir və ekspertlərin təcrübə səviyyəsi nəticələrin düzgünlüyünə birbaşa təsir göstərir [3]. Kadr çatışmazlığı və ixtisaslı mütəxəssislərin azlığı müasir kriminalistik mühitdə əsas problemlərdən biri olaraq qalır.

Standartlaşdırma problemləri müxtəlif təşkilatlar arasında yanaşma fərqlərinə səbəb olur və bu, insidentlərin araşdırılması prosesində uyğunsuzluqlar yaradır.

F *Kriminalistik tələblərə uyğunluq problemi*

Kriminalistik tələblərə uyğunluq (forensic soundness) rəqəmsal kriminalistik prosesin əsas prinsiplərindən biri olub, sübutların dəyişdirilmədən əldə olunmasını və bütün əməliyyatların sənədləşdirilməsini tələb edir [1, 3].

Süni intellekt əsaslı yanaşmaların tətbiqi böyük həcmli verilənlərin təhlilində effektiv olsa da, bu modellərin nəticələrinin izah olunması çətin olduğundan onların hüquqi baxımdan əsaslandırılması problem yaradır [5, 8].

Bulud və paylanmış mühitlərdə sübutlara tam nəzarətin olmaması kriminalistik tələblərə uyğunluğun təmin olunmasını çətinləşdirir [10, 15].

IV. MÜASİR YANAŞMALAR VƏ TEXNOLOJİ HƏLLƏR

Rəqəmsal kriminalistika sahəsində mövcud problemlərin aradan qaldırılması üçün müasir texnologiyaların tətbiqi və metodoloji yanaşmaların təkmilləşdirilməsi əsas istiqamətlərdən biri kimi çıxış edir. Xüsusilə böyük həcmli verilənlərin emalı, paylanmış mühitlərdə sübutların idarə olunması və kriminalistik tələblərə uyğunluğun təmin edilməsi kimi məsələlər yeni texnoloji həllərin tətbiqini zəruri edir [4, 5].

A *Süni intellekt və maşın təlimi əsaslı yanaşmalar*

Rəqəmsal kriminalistika sahəsində süni intellekt və maşın təlimi metodlarının tətbiqi son illərdə əhəmiyyətli dərəcədə genişlənmişdir. Bu yanaşmalar əsasən böyük həcmli verilənlərin avtomatlaşdırılmış emalı, rəqəmsal artefaktların prioritetləşdirilməsi, anomal fəaliyyətlərin aşkarlanması və insidentlərin daha səmərəli təhlili məqsədilə istifadə olunur. Ənənəvi üsullarla müqayisədə bu metodlar mürəkkəb və çoxölçülü məlumat strukturlarında gizli əlaqələrin müəyyən edilməsinə imkan verir [5, 19].

Nəzarətli maşın öyrənmə modelləri, o cümlədən "Random Forest", "Support Vector Machine (SVM)", "XGBoost" və oxşar alqoritmlər loq qeydlərinin təsnifləşdirilməsi, zərərli fəaliyyət nümunələrinin identifikasiyası və insident kateqoriyalarının avtomatik müəyyən olunması üçün geniş tətbiq edilir. Bu yanaşmalar əvvəlcədən etiketlənmiş verilənlər bazası əsasında öyrədildiyindən yüksək dəqiqlik göstəricilərinə nail olmaq mümkündür.

Nəzarətsiz öyrənmə metodları, xüsusilə klasterləşdirmə alqoritmləri və Autoencoder əsaslı modellər əvvəlcədən məlum olmayan davranış nümunələrinin aşkarlanması baxımından mühüm əhəmiyyət daşıyır. Bu yanaşmalar ənənəvi imza əsaslı metodlarla müəyyən edilə bilməyən anomal fəaliyyətlərin, o cümlədən yeni hücum ssenarilərinin və qeyri-adi sistem davranışlarının aşkar edilməsində istifadə oluna bilər.

Dərin öyrənmə modelləri, o cümlədən "Convolutional Neural Network (CNN)", "Long Short-Term Memory (LSTM)"

və "Transformer" arxitekturaları böyük həcmli və heterogen verilənlər üzərində daha mürəkkəb əlaqələrin müəyyən olunmasına imkan verir. Bu modellər xüsusilə zaman ardıcıllığına malik loq məlumatlarının, şəbəkə trafikinin və istifadəçi davranış nümunələrinin təhlilində effektiv hesab olunur.

Təbii dil emalı (Natural Language Processing – NLP) metodları hadisə hesabatlarının, təhlükə kəşfiyyatı məlumatlarının, fişinq məktublarının və strukturlaşdırılmamış mətn əsaslı rəqəmsal sübutların avtomatlaşdırılmış təhlili üçün tətbiq edilir. Bu yanaşma müxtəlif mənbələrdən daxil olan böyük həcmdə mətn məlumatlarının operativ emalına şərait yaradır.

Bununla yanaşı, süni intellekt əsaslı modellərin rəqəmsal kriminalistikada tətbiqi müəyyən metodoloji məhdudiyyətlərlə müşayiət olunur. Təlim verilənlərinin keyfiyyəti, model qərəzliliyi, yanlış nəticələr və qərar mexanizmlərinin qeyri-şəffaflığı bu sahədə əsas problemlər sırasındadır. Xüsusilə məhkəmə və ekspertiza proseslərində nəticələrin əsaslandırılması tələb olunduğundan, "SHAP", "LIME" və digər izah edilə bilən süni intellekt yanaşmalarının tətbiqi xüsusi aktuallıq kəsb edir [8, 19].

B *Blokçeyn əsaslı kriminalistik yanaşmalar*

Blokçeyn əsaslı yanaşmalar rəqəmsal sübutların bütövlüyünün qorunması və onların dəyişdirilməzliyinin təmin olunması üçün innovativ həll kimi çıxış edir. Paylanmış reyestr texnologiyaları məlumatların mərkəzləşdirilmədən saxlanılmasına və dəyişikliklərin izlənilə bilməsinə imkan yaradır.

Sübutların qorunma zənciri mexanizminin paylanmış reyestrlərlə təmin olunması (blockchain-based chain of custody) sübutların əldə olunmasından təqdim olunmasına qədər bütün əməliyyatların dəyişdirilə bilməyən şəkildə qeyd olunmasını təmin edir. Bu yanaşma sübutların kim tərəfindən və hansı mərhələdə emal olunduğunu şəffaf şəkildə izləməyə imkan verir və kriminalistik tələblərə uyğunluğun təmin olunmasına əsaslı töhfə verir [1, 4].

Sübutların dəyişdirilməzliyi və audit imkanları (immutability and auditability) blokçeyn texnologiyasının əsas üstünlüklərindən biridir. Sübutlara aid heş qiymətlərinin bloklarda saxlanılması məlumatların dəyişdirilməsinin qarşısını alır və istənilən dəyişiklik cəhdini aşkar etməyə imkan verir. Bununla belə, bu texnologiyanın tətbiqi yüksək hesablama xərcləri və miqyaslanma problemləri ilə müşayiət olunur və real sistemlərdə geniş tətbiqi üçün əlavə optimallaşdırmalar tələb olunur.

C *Bulud və IoT kriminalistikası*

Bulud və IoT mühitlərində rəqəmsal kriminalistikanın effektiv həyata keçirilməsi üçün texniki və təşkilati yanaşmaların inteqrasiyası zəruri hesab olunur. Bu məqsədlə xidmət təchizatçıları ilə koordinasiyalı məlumat əldə etmə mexanizmləri, standartlaşdırılmış loq formatları və avtomatlaşdırılmış sübut toplama prosedurları xüsusi əhəmiyyət daşıyır [20].

Bulud mühitlərində rəqəmsal araşdırma imkanlarının artırılması məqsədilə "forensic-by-design" yanaşmasının, yəni sistemlərin layihələndirilməsi mərhələsində kriminalistik tələblərin əvvəlcədən nəzərə alınmasının tətbiqi məqsədəuyğun hesab olunur. Bu model çərçivəsində sistemlərin ilkin layihələndirmə mərhələsindən etibarən audit qeydləri, zaman sinxronizasiyası, məlumat saxlanma siyasətləri və sübutların ixrac imkanları nəzərə alınır.

Paylanmış infrastrukturlarda məlumatların operativ emalı üçün federativ analiz və uzaqdan əldə etmə mexanizmləri tətbiq oluna bilər. Bu yanaşmalar müxtəlif regionlarda yerləşən sistemlər üzrə araşdırma prosesinin sürətləndirilməsinə imkan yaradır.

IoT cihazlarında isə yüngül agent əsaslı monitorinq sistemləri, mərkəzləşdirilmiş hadisə toplama platformaları və standart interfeyslərdən istifadə sübutların daha səmərəli əldə olunmasına şərait yaradır [16].

Bununla yanaşı, bulud və IoT kriminalistikası sahəsində texniki həllərlə yanaşı hüquqi prosedurların, xidmət səviyyəsi razılaşmalarının (SLA) və beynəlxalq əməkdaşlıq mexanizmlərinin də inkişaf etdirilməsi məqsədəuyğun hesab olunur [10, 15].

V. RƏQƏMSAL KRİMİNALİSTİKA YANAŞMALARININ MÜQAYİSƏLİ ANALİZİ

Rəqəmsal kriminalistika sahəsində istifadə olunan yanaşmaların müqayisəli təhlili göstərir ki, bu sahədə tətbiq olunan metodlar yalnız texnoloji inkişafın nəticəsi olaraq dəyişmir, eyni zamanda kriminalistik tələblər, hüquqi çərçivələr və əməliyyat mühitlərinin xüsusiyyətləri ilə də müəyyən olunur. Müasir şəraitdə ənənəvi və yeni nəsil yanaşmalar arasında balansın qurulması rəqəmsal sübutların etibarlı şəkildə əldə olunması və təhlili üçün əsas şərtlərdən biri kimi çıxış edir.

A *Klassik və müasir yanaşmaların müqayisəsi*

Ənənəvi kriminalistika metodları rəqəmsal sübutların dəyişdirilmədən əldə olunması və analiz prosesinin tam nəzarət altında həyata keçirilməsi prinsiplərinə əsaslanır. Bu yanaşmalar çərçivəsində sübutların bit səviyyəsində surətlərinin çıxarılması, kriptoqrafik heş funksiyaları ilə yoxlanılması və bütün prosesin detallı sənədləşdirilməsi əsas tələblər kimi qəbul edilir [1, 14]. Bu metodların əsas üstünlüyü onların yüksək etibarlılığı və hüquqi müstəvidə qəbul edilə bilmə səviyyəsinin yüksək olmasıdır.

Bununla belə, ənənəvi yanaşmaların effektivliyi əsasən statik və nəzarət olunan mühitlərlə məhdudlaşır. Müasir rəqəmsal sistemlərdə məlumatların paylanmış şəkildə saxlanılması, dinamik olaraq dəyişməsi və müxtəlif platformalarda yerləşməsi bu yanaşmaların tətbiq imkanlarını əhəmiyyətli dərəcədə məhdudlaşdırır. Nəticədə, klassik metodlar müasir kibermühitdə baş verən insidentlərin tam əhatəli analizini təmin etməkdə çətinlik çəkir.

Müasir texnologiyalara əsaslanan yanaşmalar isə bu məhdudiyyətləri aradan qaldırmaq məqsədilə inkişaf etdirilmişdir. Bu yanaşmalar böyük həcmli verilənlərin emalı, real-vaxt rejimində analiz imkanları və avtomatlaşdırılmış qərar dəstəyi mexanizmlərini özündə birləşdirir [4, 5]. Xüsusilə paylanmış və bulud mühitlərində bu yanaşmaların tətbiqi daha

effektiv hesab olunur.

Lakin müasir yanaşmaların tətbiqi ilə bağlı yeni problemlər də yaranır. Ən vacib məqam ondan ibarətdir ki, bu yanaşmaların çoxu kriminalistik prosesin klassik prinsiplərindən müəyyən dərəcədə uzaqlaşır. Məsələn, avtomatlaşdırılmış analiz və süni intellekt modelləri nəticələrin necə əldə olunduğunu tam şəkildə izah etməyə imkan vermədikdə, bu nəticələrin hüquqi müstəvidə əsaslandırılması çətinləşir [8]. Bu isə texniki effektivlik ilə hüquqi etibarlılıq arasında ziddiyyət yaradır.

Beləliklə, aparılan müqayisə göstərir ki, klassik və müasir yanaşmalar bir-birini əvəz edən deyil, əksinə tamamlayan metodlar kimi qiymətləndirilməlidir. Müasir praktikada bu yanaşmaların inteqrasiyası, yəni hibrid kriminalistik modellərin tətbiqi daha effektiv nəticələrin əldə olunmasına imkan yaradır.

B *Texnoloji yanaşmaların müqayisəli qiymətləndirilməsi*

Süni intellekt və ənənəvi analiz metodlarının müqayisəsi göstərir ki, bu iki yanaşma fərqli üstünlüklərə malikdir və müxtəlif məqsədlər üçün daha uyğun hesab olunur. Süni intellekt əsaslı metodlar böyük həcmli verilənlərin emalında və mürəkkəb nümunələrin aşkarlanmasında yüksək effektivlik nümayiş etdirir [5]. Bu yanaşmalar vasitəsilə insan tərəfindən aşkar edilməsi çətin olan əlaqələr və davranış modelləri müəyyən edilə bilir.

Bununla belə, ənənəvi analiz metodları daha şəffaf və izah edilə bilən nəticələr təqdim edir. Bu xüsusiyyət kriminalistik prosesdə xüsusi əhəmiyyət daşıyır, çünki əldə olunan nəticələrin məhkəmədə əsaslandırılması tələb olunur. Süni intellekt modellərinin isə "qara qutu" xarakteri onların nəticələrinin izahını çətinləşdirir və bu, onların praktik tətbiqində əsas məhdudiyyətlərdən biri kimi çıxış edir [8]. Bu baxımdan, izah edilə bilən süni intellekt (XAI) yanaşmalarının inkişafı bu sahədə əsas tədqiqat istiqamətlərindən biri hesab olunur.

Blokçeyn və klassik sübutların qorunma zənciri (chain of custody) mexanizmlərinin müqayisəsi sübutların idarə olunması baxımından fərqli konseptual yanaşmaları ortaya qoyur. Klassik yanaşma mərkəzləşdirilmiş idarəetmə və sənədləşdirmə prinsiplərinə əsaslanır və uzun müddət ərzində öz etibarlılığını sübut etmişdir. Bununla yanaşı, bu yanaşma insan faktorundan və potensial manipulyasiya risklərindən tam sığortalanmamışdır.

Blokçeyn texnologiyası isə sübutların dəyişdirilməzliyini təmin edən paylanmış və kriptoqrafik əsaslı mexanizm təqdim edir. Bu yanaşma sübutların şəffaf şəkildə izlənməsinə və dəyişikliklərin dərhal aşkarlanmasına imkan yaradır. Lakin bu texnologiyanın tətbiqi yüksək hesablama xərcləri, miqyaslanma problemləri və real sistemlərə inteqrasiya çətinlikləri ilə müşayiət olunur. Bu isə onun geniş tətbiqini məhdudlaşdıran əsas amillərdən biridir.

Bulud kriminalistikası və lokal kriminalistikanın müqayisəsi isə nəzarət və əlçatanlıq arasında balans problemini ortaya qoyur. Lokal mühitlərdə sübutlara tam nəzarət və birbaşa çıxış təmin olunur ki, bu da kriminalistik prosesin daha stabil və proqnozlaşdırıla bilən şəkildə həyata keçirilməsinə imkan yaradır. Lakin bu yanaşma müasir paylanmış sistemlərdə kifayət qədər effektiv deyil.

Bulud mühitlərində isə məlumatlara genişmiqyaslı və çevik çıxış imkanı mövcuddur, lakin bu mühitlərdə sübutlar üzərində tam nəzarət mümkün olmur [10, 15]. Məlumatların müxtəlif coğrafi regionlarda saxlanılması və üçüncü tərəf xidmət təminatçılarından asılılıq hüquqi və texniki riskləri artırır. Bu isə kriminalistik prosesin etibarlılığına birbaşa təsir göstərir.

Ümumilikdə aparılan müqayisəli təhlil göstərir ki, müasir texnoloji yanaşmalar kriminalistik prosesin sürətini və miqyasını artırsa da, onların tətbiqi yeni risklər və məhdudiyyətlər yaradır. Bu səbəbdən effektiv kriminalistik analiz üçün müxtəlif yanaşmaların inteqrasiyası və konkret vəziyyətə uyğun seçilməsi zəruri hesab olunur.

Mövcud elmi ədəbiyyat və aparılmış təhlil əsasında klassik və müasir rəqəmsal kriminalistika yanaşmalarının əsas fərqləri Cədvəl I-də ümumiləşdirilmişdir.

CƏDVƏL I. KLASSIK VƏ MÜASIR RƏQƏMSAL KRIMINALISTIKA YANAŞMALARININ MÜQAYISƏLI ANALIZI

Əsas xüsusiyyətlər	**Klassik yanaşmalar**	**Müasir yanaşmalar**
Sübutların əldə olunma üsulu	Bit səviyyəli tam surət çıxarma	Selektiv, canlı və uzaqdan əldə etmə
Tətbiq mühiti	Lokal və nəzarət olunan sistemlər	Bulud, IoT və paylanmış mühitlər
Verilənlərin emal həcmi	Məhdud	Böyük həcmli verilənlərlə işləmə imkanı
Analiz üsulu	Əl ilə aparılan və qayda əsaslı	Sİ/MÖ və avtomatlaşdırılmış analiz
Hüquqi qəbul olunma səviyyəsi	Daha sabit	Metoddan asılı olaraq dəyişkən
Standartlaşdırma səviyyəsi	Daha formalaşmış	İnkişaf mərhələsində
İnsan faktorundan asılılıq	Yüksək	Nisbətən az

VI. MÖVCUD PROBLEMLƏR VƏ GƏLƏCƏK TƏDQİQAT İSTİQAMƏTLƏRİ

Aparılmış təhlillər göstərir ki, rəqəmsal kriminalistikanın gələcək inkişafı yalnız mövcud metod və alətlərin təkmilləşdirilməsi ilə məhdudlaşmır. Rəqəmsal mühitlərin dinamik xarakter alması, paylanmış infrastrukturların genişlənməsi və məlumat həcminin davamlı artması yeni nəsil metodoloji yanaşmaların formalaşdırılmasını zəruri edir [6]. Bu baxımdan, gələcək tədqiqatların həm texniki, həm də hüquqi və təşkilati aspektləri paralel şəkildə əhatə etməsi məqsədəuyğun hesab olunur.

Perspektiv istiqamətlərdən biri avtonom və intellektual kriminalistik sistemlərin inkişafıdır. Süni intellekt əsaslı agentlərin ilkin sübut seçimi, hadisələrin prioritetləşdirilməsi, çoxmənbəli məlumatların avtomatik korrelyasiyası və ekspertlər üçün qərar dəstəyi funksiyalarında tətbiqi gələcəkdə daha geniş əhəmiyyət kəsb edə bilər. Bu cür yanaşmalar insan resurslarından daha səmərəli istifadə olunmasına və araşdırma müddətinin azaldılmasına şərait yarada bilər [5, 8].

Digər mühüm istiqamət rəqəmsal kriminalistikanın real-vaxtda monitorinq və insidentlərə cavabvermə sistemləri ilə inteqrasiyasıdır. Ənənəvi yanaşmalar əsasən hadisədən sonra aparılan analizə söykəndiyi halda, müasir şəraitdə sübut xarakterli məlumatların hadisə baş verən anda qorunması və paralel şəkildə ilkin təhlilin aparılması xüsusi aktuallıq qazanır. Bu yanaşma insidentlərə operativ reaksiya verilməsi və məlumat itkisinin minimuma endirilməsi baxımından əhəmiyyətli hesab

olunur [5, 13].

Paylanmış və transsərhəd mühitlərin genişlənməsi beynəlxalq qarşılıqlı fəaliyyət mexanizmlərinin inkişafını da aktuallaşdırır. Xüsusilə müxtəlif ölkələrdə yerləşən sistemlər üzrə araşdırmalar zamanı standartlaşdırılmış məlumat mübadilə formatlarının, uzaqdan sübut əldə etmə prosedurlarının və institusional əməkdaşlıq modellərinin formalaşdırılması mühüm istiqamətlərdən biri hesab oluna bilər. Bu, həm texniki uyğunluğun, həm də hüquqi prosedurların uzlaşdırılması baxımından əhəmiyyətlidir [10, 12, 15].

Bulud və IoT ekosistemlərinin geniş yayılması rəqəmsal kriminalistika üçün yeni texniki tələblər də yaradır. Bu baxımdan, resurs məhdudiyyətli cihazlar üçün yüngül kriminalistik agentlərin hazırlanması, avtomatlaşdırılmış loq toplama sistemlərinin inkişafı və paylanmış mühitlərdə sübutların sinxron idarə olunması gələcək tədqiqat istiqamətləri sırasında qiymətləndirilə bilər [10, 16].

Bununla yanaşı, post-kvant hesablama texnologiyalarının inkişafı şəraitində mövcud kriptoqrafik mexanizmlərin davamlılığı məsələsi də aktuallaşır. Rəqəmsal sübutların autentifikasiyası, dəyişdirilməzliyinin qorunması və uzunmüddətli etibarlılığının təmin olunması məqsədilə kvant-davamlı kriptoqrafik yanaşmaların tətbiqi gələcəkdə xüsusi əhəmiyyət kəsb edə bilər.

Ümumilikdə, rəqəmsal kriminalistikanın gələcək inkişafı klassik kriminalistik prinsiplərlə innovativ texnologiyaların uzlaşdırılmasını, beynəlxalq standartların yenilənməsini və multidissiplinar əməkdaşlığın gücləndirilməsini tələb edir. Bu istiqamətdə aparılacaq tədqiqatlar sahənin yeni texnoloji çağırışlara uyğunlaşmasına şərait yarada bilər.

NƏTİCƏ

Aparılmış təhlillər göstərir ki, rəqəmsal kriminalistika sahəsi sürətlə dəyişən texnoloji mühitin təsiri altında transformasiya mərhələsinə daxil olmuşdur. Müasir informasiya sistemlərinin mürəkkəbləşməsi, verilənlərin həcminin artması, bulud infrastrukturlarının və IoT ekosistemlərinin genişlənməsi ənənəvi kriminalistika metodlarının tətbiq imkanlarını müəyyən dərəcədə məhdudlaşdırmışdır.

Müəyyən edilmişdir ki, klassik yanaşmalar sübutların bütövlüyünün qorunması, prosedur sabitliyi və hüquqi etibarlılıq baxımından yüksək əhəmiyyət daşısa da, müasir rəqəmsal insidentlərin dinamikası və miqyası şəraitində əlavə texnoloji dəstəyə ehtiyac yaranır. Bu baxımdan, süni intellekt, avtomatlaşdırılmış analiz sistemləri və paylanmış texnologiyalar kriminalistik proseslərin sürətinin və səmərəliliyinin artırılması üçün perspektivli vasitələr kimi qiymətləndirilə bilər.

Təhlil nəticəsində müəyyən edilmişdir ki, kriminalistik tələblərə uyğunluq ilə texnoloji effektivlik arasında balansın qorunması müasir rəqəmsal kriminalistikanın əsas inkişaf istiqamətlərindən biridir. Bu balansın təmin olunması həm metodoloji yanaşmaların təkmilləşdirilməsini, həm də tətbiq olunan texnologiyaların hüquqi və praktiki tələblərə uyğunlaşdırılmasını zəruri edir.

Ümumilikdə, rəqəmsal kriminalistikanın gələcək inkişafı klassik prinsiplərlə innovativ texnologiyaların inteqrasiyasına əsaslanan hibrid modellərin formalaşdırılması, beynəlxalq standartların yenilənməsi və multidissiplinar əməkdaşlığın gücləndirilməsi ilə bağlıdır. Bu istiqamətlər üzrə aparılacaq tədqiqatlar sahənin elmi və praktiki potensialının genişlənməsinə mühüm töhfə verə bilər.

ƏDƏBİYYAT

[1] E. Casey, Digital Evidence and Computer Crime, 3rd ed. Academic Press, 2011.

[2] V. Roussev, Digital Forensic Science: Issues, Methods, and Challenges. Springer, 2017.

[3] A. A. Khan et al., "Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues and future direction," Int. J. Electronic Security and Digital Forensics, 2022.

[4] F. Casino, T. Dasaklis, and C. Patsakis, "Research trends, challenges, and emerging topics of digital forensics: A review of reviews," 2021.

[5] T. Nayerifard et al., "Machine learning in digital forensics: A systematic literature review," 2023.

[6] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," arXiv preprint arXiv:1604.03850, 2016.

[7] H. Arshad, A. Jantan, and O. I. Abiodun, "Digital forensics: Review of issues in scientific validation of digital evidence," Journal of Information Processing Systems, vol. 14, no. 2, pp. 346–376, 2018.

[8] "Digital forensics and strong AI: A structured literature review," Forensic Science International: Digital Investigation, 2023.

[9] Azərbaycan Respublikası, "Cinayət-Prosessual Məcəlləsi," Bakı, 2000 (son dəyişikliklər və əlavələr ilə).

[10] A. M. Alenezi, "Digital and cloud forensic challenges: Issues and future directions," IEEE Access, vol. 11, pp. 45678–45695, 2023.

[11] G. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," International Journal of Digital Evidence, vol. 1, no. 3, pp. 1–12, 2002.

[12] ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence.

[13] NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, National Institute of Standards and Technology, 2006.

[14] B. Carrier, File System Forensic Analysis. Addison-Wesley, 2005.

[15] S. Zawoad and R. Hasan, "Cloud forensics: A meta-study of challenges, approaches, and open problems," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1201–1224, 2016.

[16] M. Conti, A. Dehghantanha, K.-K. R. Choo, and N. Beebe, "Forensics investigation of IoT devices: A survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2177–2191, 2018.

[17] S. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64–S73, 2010.

[18] M. Rogers, "The role of anti-forensics in digital forensic investigations," Digital Investigation, vol. 3, pp. S3–S9, 2006.

[19] X. Du, C. Hargreaves, J. Sheppard, F. Anda, A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation," arXiv:2012.01987, 2020.

[20] A. M. Alenezi, "Digital Forensics in the Age of Smart Environments: A Survey of Recent Advancements and Challenges," arXiv:2305.09682, 2023.

Investigation and Comparative Analysis of the Current Scientific and Technological Challenges in Digital Forensics

Sanan Valizada

Institute of Information Technology, Baku, Azerbaijan

senanvalizade@gmail.com

Abstract- This paper presents a systematic analysis of theoretical foundations, methodological frameworks, and technological developments in digital forensics. The study

examines key challenges related to large-scale data analysis, cloud environments, IoT systems, and legal admissibility of digital evidence. Both traditional forensic methods and modern approaches based on artificial intelligence, blockchain, and distributed systems are comparatively evaluated. The results highlight the existing gap between technological efficiency and forensic soundness. Additionally, the paper emphasizes the role of international standards and recent legal developments in strengthening the reliability of digital evidence. Future research directions focus on explainable AI, real-time forensics, interoperability, and quantum-resilient security mechanisms.

Keywords- digital forensics; digital evidence; digital artifacts; forensic soundness.