Fiziki və Rəqəmsal Obyektlərin Hibrid Kriminalistikası: Problemlər və Həll Yolları

Ramiz Şıxəliyev[1], Sənan Vəlizadə[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*shikhramiz61@gmail.com*, [2]*senanvalizade@gmail.com*

***Xülasə*— Rəqəmsallaşmanın sürətlənməsi və IoT ilə kiber-fiziki sistemlərin geniş tətbiqi nəticəsində fiziki və rəqəmsal sübutların qarşılıqlı inteqrasiyası kriminalistika sahəsində yeni problemlər yaratmışdır. Bu hibrid mühitlərdə sübutların toplanması, analiz və hüquqi etibarlılığının təmin olunmasını aktual elmi-praktik problemə çevirir. Məqalədə fiziki və rəqəmsal obyektlərin inteqrasiyası şəraitində formalaşan hibrid kriminalistika yanaşması analiz edilir. Müasir IoT və kiber-fiziki sistemlərdə sübutların heterogenliyi, toplanması, saxlanması və hüquqi etibarlılığı ilə bağlı əsas problemlər müəyyən olunur. Eyni zamanda, bu problemlərin həlli üçün müxtəlif mənbələrdən toplanan verilənlərin inteqrasiyası, süni intellekt əsaslı analiz metodları və standartlaşdırılmış kriminalistika çərçivələri təklif edilir.**

Açar sözlər*— *hibrid kriminalistika; fiziki sübut; rəqəmsal sübut; kiber-fiziki sistemlər; sübutların inteqrasiyası; IoT kriminalistikası.

I. GİRİŞ

Müasir dövrdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı, rəqəmsallaşmanın genişlənməsi və fiziki sistemlərin elektron idarəetmə infrastrukturu ilə inteqrasiyası kriminalistika sahəsində yeni çağırışlar formalaşdırmışdır. Ənənəvi yanaşmalarda fiziki sübutlar və rəqəmsal sübutlar əsasən ayrı istiqamətlər üzrə araşdırılsa da, müasir hadisələrin əhəmiyyətli hissəsində bu iki kateqoriya paralel şəkildə meydana çıxır və qarşılıqlı əlaqəli xarakter daşıyır.

Əşyaların interneti (IoT), ağıllı müşahidə sistemləri, biometrik giriş nəzarəti, bulud texnologiyaları, ağıllı nəqliyyat vasitələri və kiber-fiziki sistemlərin geniş tətbiqi nəticəsində bir hadisə üzrə həm fiziki, həm də rəqəmsal izlər formalaşa bilir [1, 2, 3]. Bu baxımdan hadisənin tam və obyektiv araşdırılması üçün müxtəlif mənbələrdən əldə olunan məlumatların birlikdə qiymətləndirilməsi zəruri hesab olunur.

Rəqəmsal kriminalistika sahəsində son illər ərzində mühüm metodoloji inkişaflar müşahidə olunsa da, fiziki və rəqəmsal sübutların inteqrasiya olunmuş şəkildə araşdırılması məsələsi hələ də tam formalaşmış istiqamət hesab edilmir. Mövcud çətinliklər sırasında məlumatların heterogenliyi, zaman göstəricilərinin uyğunlaşdırılması, müxtəlif platformalar üzrə məlumatların əlaqələndirilməsi, sübutların bütövlüyünün qorunması və hüquqi qəbul edilmə məsələləri xüsusi yer tutur [4, 5, 6].

Bu kontekstdə hibrid kriminalistika anlayışı fiziki və rəqəmsal obyektlərlə bağlı sübutların vahid metodoloji çərçivədə toplanması, qorunması, təhlili və təqdim olunmasını ifadə edir. Bu yanaşma klassik kriminalistika metodlarının rəqəmsal mühitin xüsusiyyətlərinə uyğunlaşdırılmasını ı, eyni zamanda çoxmənbəli hadisələrin daha sistemli araşdırılmasını nəzərdə tutur.

Tədqiqatın məqsədi fiziki və rəqəmsal obyektlərin hibrid kriminalistikası sahəsində mövcud elmi yanaşmaları təhlil etmək, əsas problemləri sistemləşdirmək və perspektiv metodoloji istiqamətləri müəyyənləşdirməkdir. Bu məqsədlə mövcud modellər, IoT və kiber-fiziki sistemlər üzrə kriminalistika çərçivələri, süni intellekt əsaslı yanaşmalar, bulud mühitlərində araşdırma problemləri və inteqrasiya olunmuş sübut idarəetmə mexanizmləri nəzərdən keçirilmişdir.

II. NƏZƏRİ ƏSASLAR VƏ ƏSAS ANLAYIŞLAR

A. Rəqəmsal kriminalistika anlayışı

Rəqəmsal kriminalistika müasir kriminalistika elminin mühüm istiqamətlərindən biri olub, elektron mühitdə formalaşan məlumatların sübut xarakterli şəkildə müəyyən edilməsi, əldə olunması, qorunması, təhlili və təqdim olunması proseslərini əhatə edir. Bu sahə kompüter sistemləri, mobil qurğular, server infrastrukturu, şəbəkə mühitləri, bulud platformaları və digər rəqəmsal ekosistemlərdə yaranan məlumatların araşdırılmasına yönəlmişdir [4, 6].

Ənənəvi fiziki sübutlardan fərqli olaraq, rəqəmsal sübutlar maddi deyil, elektron formada mövcud olur və çox vaxt dəyişkən xarakter daşıyır. Fayl sistemləri, loq qeydləri, istifadəçi fəaliyyəti tarixçəsi, metaverilənlər, yaddaş məlumatları, brauzer artefaktları və şəbəkə trafik izləri bu sahənin əsas araşdırma obyektlərinə daxildir. Belə məlumatlar qısa müddətdə dəyişdirilə, silinə və ya üzərinə yeni məlumat yazıla bildiyi üçün operativ müdaxilə və düzgün əldəetmə prosedurları xüsusi əhəmiyyət daşıyır [4, 5].

Rəqəmsal kriminalistikanın əsas məqsədlərindən biri kibercinayətkarlıq əməlləri, daxili təhdidlər, məlumat sızmaları, dələduzluq halları və digər hüquqpozmalarla bağlı elektron izlərin elmi və kriminalistik əsaslarla araşdırılmasıdır. Bu prosesdə məlumatın bütövlüyünün qorunması, əldə olunmuş sübutun etibarlılığı və ekspertiza nəticələrinin təkrarlana bilməsi vacib prinsiplər hesab olunur. Bu baxımdan heş alqoritmlərindən istifadə, sənədləşdirilmiş ekspertiza metodları və sübutların qorunma zəncirinin (chain-of-custody) təmin olunması geniş tətbiq edilir [5, 6, 7].

Müasir dövrdə rəqəmsal kriminalistika yalnız kompüter

DOI: 10.25045/forensic.gov.2026.48

ekspertizası ilə məhdudlaşmır. Mobil kriminalistika, şəbəkə kriminalistikası, bulud kriminalistikası, yaddaş kriminalistikası və IoT kriminalistikası kimi alt istiqamətlər formalaşmışdır. Bu inkişaf rəqəmsal mühitlərin mürəkkəbləşməsi, cihaz müxtəlifliyinin artması və sübut mənbələrinin genişlənməsi ilə əlaqədardır [2, 3].

Rəqəmsal kriminalistika prosesində əsas mərhələlər kimi sübutun identifikasiyası, əldə olunması, qorunması, analizi və təqdimatı göstərilir. Lakin müasir paylanmış sistemlərdə, şifrələnmiş platformalarda və bulud mühitlərində bu mərhələlərin icrası daha mürəkkəb xarakter alır. Xüsusilə uzaq mühitlərdən məlumat əldə olunması, çoxistifadəçili sistemlərdə mənsubiyyətin müəyyən edilməsi və böyük həcmli məlumatların təhlili əlavə metodoloji çətinliklər yaradır.

Təhlillər göstərir ki, rəqəmsal kriminalistika kibertəhlükəsizlik insidentlərinin araşdırılması və elektron sübutların hüquqi qiymətləndirilməsi baxımından mühüm əhəmiyyət daşıyır. Bununla yanaşı, fiziki obyektlərlə rəqəmsal sistemlərin inteqrasiyası nəticəsində bu sahənin klassik sərhədləri genişlənməkdədir ki, bu da hibrid kriminalistika yanaşmalarının aktuallığını artırır.

B. Fiziki kriminalistika və klassik metodlar

Fiziki kriminalistika hadisə yeri ilə əlaqəli maddi sübutların aşkar olunması, toplanması, qorunması, tədqiqi və qiymətləndirilməsi ilə məşğul olan kriminalistika istiqamətidir. Bu sahə uzun müddət hüquqpozmaların araşdırılmasında əsas rol oynamış və klassik kriminalistika məktəbinin formalaşmasında mühüm yer tutmuşdur. Fiziki kriminalistikanın əsas obyekti hadisə ilə əlaqəli maddi izlər və material sübutlar hesab olunur.

Bu kateqoriyaya barmaq izləri, ayaqqabı və təkər izləri, alət izləri, sənədlər, bioloji nümunələr, liflər, şüşə qırıntıları, silah və güllə izləri, mexaniki zədələnmələr və digər maddi obyektlər aid edilir. Belə sübutlar hadisənin başvermə mexanizmi, iştirakçıların kimliyi, istifadə olunmuş vasitələr və hadisə yerində baş vermiş proseslər barədə mühüm məlumat verə bilər.

Fiziki kriminalistikada geniş istifadə olunan klassik metodlar sırasında daktiloskopiya, trasologiya, ballistika, bioloji ekspertiza, sənəd ekspertizası və materialşünaslıq üsulları xüsusi yer tutur. Daktiloskopiya vasitəsilə şəxsin identifikasiyası, trasoloji üsullarla alət və ayaq izlərinin müqayisəsi, ballistik analizlə odlu silahın istifadəsinin müəyyən edilməsi mümkündür. Bioloji ekspertiza isə qan, tüpürcək, saç və digər nümunələrin araşdırılması yolu ilə şəxsiyyətin müəyyənləşdirilməsində tətbiq olunur.

Klassik metodların mühüm xüsusiyyətlərindən biri sübutun maddi xarakter daşıması və laborator şəraitdə təkrar yoxlanıla bilməsidir. Bu, ekspert rəyinin etibarlılığı və prosessual baxımdan qəbul edilə bilməsi üçün mühüm üstünlük hesab olunur. Eyni zamanda fiziki sübutun hadisə yerində yerləşməsi, qarşılıqlı mövqeyi və digər obyektlərlə əlaqəsi əlavə informativ əhəmiyyət daşıyır.

Bununla yanaşı, müasir dövrdə bəzi hallarda yalnız klassik metodlarla kifayətlənmək mümkün olmur. Elektron idarəetmə sistemləri, ağıllı cihazlar, biometrik keçid mexanizmləri və ağıllı nəqliyyat vasitələri kimi obyektlər həm maddi, həm də rəqəmsal xüsusiyyətlər daşıyır [1, 8].

Təhlillər göstərir ki, fiziki kriminalistika və klassik metodlar bu gün də aktuallığını qoruyur. Lakin texnoloji inkişaf nəticəsində onların tətbiqi sahəsi dəyişməkdə, rəqəmsal sübutlarla inteqrasiya ehtiyacı artmaqdadır. Bu baxımdan klassik metodların müasir araşdırma modelləri ilə uyğunlaşdırılması perspektiv istiqamət kimi qiymətləndirilə bilər.

C. Hibrid mühitlər

Müasir dövrdə rəqəmsal texnologiyalar fiziki mühitlə daha sıx inteqrasiya olunmuş formada inkişaf edir. Bu proses nəticəsində məlumat emalı yalnız virtual sistemlərdə deyil, real obyektlərin idarə olunması, monitorinqi və avtomatlaşdırılması ilə birlikdə həyata keçirilir. Belə ekosistemlər ümumilikdə hibrid mühitlər kimi xarakterizə olunur və onların əsas nümunələri sırasında kiber-fiziki sistemlər (CPS) və əşyaların interneti (IoT) xüsusi yer tutur [2, 3].

Kiber-fiziki sistemlər anlayışı hesablama komponentləri ilə fiziki proseslərin qarşılıqlı əlaqədə fəaliyyət göstərdiyi sistemləri ifadə edir. Bu sistemlərdə sensorlar vasitəsilə fiziki mühitdən məlumat toplanır, proqram təminatı həmin məlumatı emal edir və nəticə etibarilə aktuatorlar vasitəsilə fiziki proseslərə təsir göstərilir. Sənaye avtomatlaşdırma sistemləri, ağıllı enerji şəbəkələri, tibbi monitorinq qurğuları, nəqliyyat idarəetmə sistemləri və istehsalat xətləri bu sistemlərə aid nümunələr kimi göstərilə bilər.

Əşyaların interneti isə internetə qoşulmuş, məlumat toplayan və qarşılıqlı əlaqə quran müxtəlif qurğuların ekosistemidir. Buraya ağıllı kameralar, sensor qurğular, qapı kilidləri, ev avtomatlaşdırma sistemləri, GPS izləmə cihazları, geyilə bilən texnologiyalar və digər qoşulmuş obyektlər daxildir. IoT cihazlarının geniş yayılması nəticəsində gündəlik həyat və təşkilati fəaliyyət sahələrində böyük həcmdə rəqəmsal izlər formalaşır [2].

Kriminalistika baxımından bu mühitlərin əsas xüsusiyyəti fiziki və rəqəmsal sübutların eyni hadisə çərçivəsində paralel şəkildə yaranmasıdır. Məsələn, ağıllı qapı sisteminə icazəsiz müdaxilə zamanı fiziki zədələnmə, barmaq izləri ilə yanaşı giriş cəhdlərinə dair loq qeydləri, kamera görüntüləri, istifadəçi identifikasiya məlumatları və şəbəkə trafik qeydləri mövcud ola bilər. Eyni qaydada qoşulmuş nəqliyyat vasitəsində fiziki qəza əlamətləri ilə yanaşı telemetriya məlumatları, GPS tarixçəsi və idarəetmə modulu qeydləri də sübut xarakteri daşıya bilər [8].

Bu mühitlərdə araşdırma aparılması bir sıra çətinliklərlə müşayiət olunur. Cihaz müxtəlifliyi, istehsalçı fərqləri, fərqli alqoritmli proqram təminatı, məhdud yaddaş həcmi, sürətlə dəyişən volatil məlumatlar və bulud asılılığı əsas problemlər sırasında göstərilə bilər. Bir çox IoT cihazlarında ənənəvi kriminalistika alətlərinin birbaşa tətbiqi mümkün olmur və xüsusi yanaşmalar tələb olunur [3].

Hibrid mühitlərlə bağlı digər mühüm məsələ məlumatların paylanmış xarakter daşımasıdır. Hadisə ilə bağlı qeydlərin bir hissəsi lokal cihazda, digər hissəsi mobil tətbiqdə, bir hissəsi isə bulud serverində saxlanıla bilər. Bu səbəbdən araşdırma zamanı yalnız cihazın özü deyil, əlaqəli ekosistem bütövlükdə nəzərə alınmalıdır.

Təhlillər göstərir ki, kiber-fiziki sistemlər və əşyaların interneti mühitləri hibrid kriminalistikanın ən aktual tətbiq sahələrindəndir. Bu baxımdan həmin sistemlər üçün xüsusi əldəetmə metodlarının, vahid sistemli yanaşmalarının, real-vaxtlı monitorinq mexanizmlərinin və çoxmənbəli analiz çərçivələrinin inkişaf etdirilməsi məqsədəuyğun hesab olunur.

D. Hibrid kriminalistika anlayışı və tətbiq sahələri

Müasir texnoloji mühitdə fiziki və rəqəmsal sistemlərin qarşılıqlı inteqrasiyası nəticəsində bir çox hadisələr artıq yalnız klassik kriminalistika və ya yalnız rəqəmsal kriminalistika çərçivəsində tam qiymətləndirilə bilmir. Ağıllı qurğuların, IoT ekosistemlərinin, biometrik giriş sistemlərinin, qoşulmuş nəqliyyat vasitələrinin və sənaye idarəetmə platformalarının geniş yayılması fiziki və rəqəmsal sübutların eyni hadisə daxilində paralel şəkildə yaranmasına səbəb olmuşdur [1, 2, 3]. Bu şərait yeni metodoloji yanaşma kimi hibrid kriminalistika anlayışını aktuallaşdırmışdır.

Hibrid kriminalistika fiziki və rəqəmsal sübutların vahid araşdırma çərçivəsində müəyyən edilməsi, toplanması, qorunması, təhlili və təqdim olunmasını ifadə edir. Bu yanaşmada məqsəd müxtəlif sübut növlərini sadəcə toplamaq deyil, onların qarşılıqlı əlaqəsini, zaman ardıcıllığını və hadisənin ümumi mexanizmi daxilində rolunu müəyyən etməkdir. Beləliklə, hibrid kriminalistika klassik fiziki ekspertiza ilə rəqəmsal kriminalistikanın əlaqələndirilmiş tətbiqinə əsaslanır.

Bu istiqamətin formalaşmasının əsas səbəblərindən biri müasir obyektlərin hibrid xarakter daşımasıdır. Bir çox texnoloji qurğular maddi obyekt olmaqla yanaşı, eyni zamanda rəqəmsal məlumat yaradır və uzaqdan idarə oluna bilir. Məsələn, ağıllı qapı sistemi fiziki cihazdır, lakin onun fəaliyyəti autentifikasiya logları, istifadəçi tarixçəsi və şəbəkə trafik qeydləri ilə müşayiət olunur. Oxşar xüsusiyyətlər ağıllı kameralar, təhlükəsizlik sensorları, nəqliyyat vasitələri və sənaye nəzarət sistemlərində də müşahidə edilir [8].

Hibrid kriminalistikanın tətbiq sahələri kifayət qədər genişdir. Ən aktual istiqamətlərdən biri giriş nəzarəti və təhlükəsizlik sistemləri ilə bağlı hadisələrdir. Bu tip hallarda fiziki müdaxilə izləri, biometrik identifikasiya qeydləri, video görüntülər və sistem jurnalları birlikdə araşdırılmalıdır. Digər tətbiq sahəsi isə ağıllı nəqliyyat vasitələridir. Belə hadisələrdə fiziki zədələnmə əlamətləri ilə yanaşı GPS tarixçəsi, telemetriya məlumatları və idarəetmə modulu qeydləri sübut xarakteri daşıya bilər.

Sənaye və enerji sektorunda istifadə olunan kiber-fiziki sistemlər də hibrid kriminalistikanın mühüm istiqamətlərindəndir. İstehsalat xətlərinə və ya SCADA tipli idarəetmə sistemlərinə müdaxilə zamanı həm fiziki avadanlıq dəyişiklikləri, həm də rəqəmsal idarəetmə qeydləri araşdırma predmeti olur. Eyni zamanda ağıllı ev sistemləri, tibbi cihazlar və şəhər infrastrukturunda tətbiq olunan sensor şəbəkələri üzrə hadisələr də bu sahəyə aid edilə bilər.

Bulud platformaları ilə inteqrasiya olunmuş lokal cihazlarda aparılan kriminalistikada fərqi yanaşmaların tətbiqi tələb olunur. Bir çox hallarda hadisə ilə bağlı məlumatların bir hissəsi cihazın özündə, digər hissəsi isə uzaq serverlərdə saxlanılır. Buna görə də araşdırma yalnız fiziki obyektlə məhdudlaşmır, əlaqəli rəqəmsal ekosistemin də bütöv şəkildə qiymətləndirilməsini tələb edir.

Təhlillər göstərir ki, hibrid kriminalistika mürəkkəb texnoloji hadisələrin daha dolğun araşdırılması üçün perspektiv istiqamət hesab oluna bilər. Bu baxımdan fiziki və rəqəmsal sübutların inteqrasiya olunmuş metodlarla qiymətləndirilməsi, gələcək kriminalistika fəaliyyətində getdikcə daha böyük əhəmiyyət kəsb edə bilər.

III. HİBRİD KRİMİNALİSTİKANIN PROBLEMLƏRİ

A. Sübutların heterogenliyi və məlumat formatlarının müxtəlifliyi

Hibrid kriminalistikada əsas problemlərdən biri eyni hadisə üzrə əldə olunan məlumatların struktur və məzmun baxımından bir-birindən ciddi şəkildə fərqlənməsidir. Araşdırma zamanı maddi obyektlər, video qeydlər, sistem loqları, sensor axınları, mobil tətbiq məlumatları və bulud platformalarından əldə olunmuş qeydlər paralel şəkildə mövcud ola bilər. Bu müxtəliflik sübutların vahid analitik mühitdə emal edilməsini çətinləşdirir.

Problemin əsas tərəflərindən biri məlumatların eyni texniki standartlara malik olmamasıdır. Müxtəlif istehsalçılara məxsus sistemlər fərqli tarix formatları, kodlaşdırma üsulları, vaxt zonaları, identifikator strukturları və qeyd mexanizmlərindən istifadə edə bilər. Nəticədə müxtəlif mənbələrdən alınmış məlumatların birbaşa müqayisə edilməsi çox vaxt mümkün olmur.

Digər çətinlik məlumatların etibarlılıq səviyyəsinin eyni olmamasıdır. Bəzi mənbələr avtomatik generasiya olunan dəqiq sistem qeydləri təqdim etdiyi halda, digər məlumatlar istifadəçi fəaliyyəti, natamam loqlar və ya dolayı göstəricilər əsasında formalaşır. Bu səbəbdən bütün sübutların eyni çəkidə qiymətləndirilməsi metodoloji baxımdan düzgün hesab olunmur.

Məlumatların həcminin böyük olması da bu sahədə əlavə problem yaradan faktorlardandır. Belə ki, kamera sistemləri, sensor şəbəkələri və şəbəkə infrastrukturu qısa müddətdə böyük həcmdə qeyd yarada bilər. Bu şəraitdə hadisə ilə bağlı məlumatların seçilməsi, lazımsız qeydlərin ayrılması və prioritetləşdirmə mühüm mərhələyə çevrilir.

Sübutların heterogenliyi problemin araşdırılması zamanı prosesin müddətinə də təsir göstərir. Müxtəlif formatlı məlumatların əl üsulu ilə çevrilməsi, uyğunlaşdırılması və yoxlanılması əlavə vaxt və resurs tələb edir. Xüsusilə çoxsaylı sistemlərin iştirak etdiyi hadisələrdə bu yük daha da artır.

Təhlillər göstərir ki, hibrid kriminalistikada sübutların heterogenliyi yalnız texniki deyil, həm də analitik və təşkilati problemdir. Bu baxımdan vahid metaverilənlər standartlarının tətbiqi, avtomatlaşdırılmış çevirmə vasitələrinin hazırlanması və çoxmənbəli məlumatların inteqrasiyasına yönəlmiş platformaların istifadəsi məqsədəuyğun hesab olunur.

B. Sübutların toplanması və qorunması

Hibrid kriminalistikada sübutların toplanması və qorunması

araşdırmanın nəticəsinə birbaşa təsir göstərən əsas mərhələlərdən biridir. Fiziki və rəqəmsal sübutların eyni hadisə üzrə paralel mövcudluğu səbəbindən əldəetmə prosesində fərqli prosedurların əlaqələndirilmiş şəkildə tətbiqi tələb olunur. Bu isə metod seçimi, prioritetləşdirmə və sənədləşdirmə baxımından əlavə çətinliklər yaradır.

Əsas problemlərdən biri sübutların dəyişkənlik səviyyəsinin fərqli olmasıdır. Fiziki obyektlər uyğun şəraitdə daha uzun müddət saxlanıla bildiyi halda, rəqəmsal məlumatların bir hissəsi qısa müddətdə dəyişə və ya itə bilər. Operativ yaddaş məlumatları, aktiv şəbəkə sessiyaları, müvəqqəti fayllar, bulud sessiya qeydləri və bəzi sensor loqları gecikmə olduqda əlçatmaz vəziyyətə düşə bilər. Buna görə də hansı sübutun ilk növbədə əldə olunacağı strateji əhəmiyyət kəsb edir [4, 5].

Sahədə mövcud olan digər mühüm məsələ müxtəlif mühitlər üzrə fərqli əldəetmə metodlarının tələb olunmasıdır. Fiziki sübutların qablaşdırılması, markalanması və laborator qaydada saxlanılması ilə rəqəmsal məlumatların bit-bit surətinin çıxarılması, heş dəyərləri ilə təsdiqlənməsi və təhlükəsiz daşıyıcılarda qorunması arasında metodoloji fərqlər mövcuddur. Bu proseslərin düzgün əlaqələndirilməməsi sonrakı ekspertiza mərhələsinə mənfi təsir göstərə bilər.

Bulud və paylanmış sistemlərdə sübutların toplanması əlavə çətinlik yaradır. Bir çox hallarda məlumat araşdırma aparan tərəfin birbaşa nəzarətində olmayan platformalarda saxlanılır. Loq qeydlərinə çıxış məhdud ola, saxlanma müddəti qısa ola və ya məlumat yalnız xidmət təminatçısının prosedurları əsasında təqdim edilə bilər. Nəticədə vacib sübutların vaxtında qorunması hər zaman mümkün olmur [3].

Sübutların qorunması prosesində bütövlüyün təmin olunması əsas prinsipdir. Fiziki sübutlarda çirklənmə, zədələnmə və mənşəyin qarışması riski mövcud olduğu kimi, rəqəmsal sübutlarda dəyişdirilmə, natamam kopyalama və meta verilən itkisi riski vardır. Bu səbəbdən bütün əməliyyatların sənədləşdirilməsi və yoxlana bilən qaydada aparılması vacib hesab olunur [4, 6].

Hibrid mühitlərdə əlavə ehtiyaclardan biri sübutların vahid idarə olunması mexanizmidir. Eyni iş üzrə maddi obyektlər, rəqəmsal surətlər, loq ixracları, bulud qeydləri və ekspertiza nəticələri fərqli formatlarda formalaşdığından onların ümumi qeydiyyat sistemi daxilində izlənməsi zəruridir. Bu məqsədlə metaverilən əsaslı reyestrlər, vahid identifikatorlar və mərkəzləşdirilmiş sübut uçotu yanaşmaları praktik əhəmiyyət daşıyır.

Təhlillər göstərir ki, sübutların toplanması və qorunması problemi hibrid kriminalistikada yalnız texniki deyil, həm də təşkilati və prosessual məsələdir. Effektiv araşdırma üçün prioritet əsaslı əldəetmə planlarının hazırlanması, vahid sənədləşdirmə prosedurlarının tətbiqi, sübutların mərkəzləşdirilmiş idarə olunması və müxtəlif ekspert qrupları arasında koordinasiyanın gücləndirilməsi zəruri görünür.

Rəqəmsal sübutların əldə olunması zamanı orijinal məlumat daşıyıcısına müdaxilənin qarşısının alınması xüsusi əhəmiyyət daşıyır. Bu məqsədlə yazmanı bloklayan (write blocker) qurğularından istifadə edilir. Həmin vasitələr yaddaş daşıyıcısından məlumatın oxunmasına imkan versə də, onun üzərinə yeni məlumat yazılmasını və mövcud strukturun dəyişdirilməsini məhdudlaşdırır. Bu yanaşma sübutun bütövlüyünün qorunması və sonradan aparılan ekspertiza nəticələrinin etibarlılığı baxımından geniş tətbiq olunur [4, 6].

C. Standartlaşdırma problemləri

Hibrid kriminalistika sahəsində əsas çətinliklərdən biri vahid standartların kifayət qədər formalaşmamasıdır. Fiziki kriminalistika və rəqəmsal kriminalistika üzrə ayrıca metodik yanaşmalar mövcud olsa da, bu iki istiqamətin birgə tətbiqini əhatə edən ümumi prosedurlar məhdud səviyyədə inkişaf etmişdir. Nəticədə oxşar hadisələr müxtəlif qurumlar və ekspert qrupları tərəfindən fərqli metodlarla araşdırıla bilər.

Standartlaşma probleminin ilk tərəfi terminoloji uyğunsuzluqla bağlıdır. Müxtəlif sahələrdə istifadə olunan anlayışlar eyni məna daşısa da fərqli terminlərlə ifadə oluna, yaxud eyni termin müxtəlif kontekstlərdə fərqli məna verə bilər. Bu vəziyyət hesabatların hazırlanması, ekspert rəylərinin müqayisəsi və qurumlararası məlumat mübadiləsi zamanı anlaşılmazlıqlar yaradır.

Bəzi hallarda fiziki sübutlar üzrə tətbiq edilən qeydiyyat formaları rəqəmsal sübutlara uyğun gəlmir, rəqəmsal sübutlar üçün istifadə olunan texniki protokollar isə maddi obyektlərin uçot sistemləri ilə əlaqələndirilmir. Bu fərqlilik eyni iş üzrə paralel aparılan araşdırmalarda məlumatların birləşdirilməsini çətinləşdirir.

Texniki platformalar arasında uyğunluq problemi də geniş yayılmışdır. Müxtəlif ekspertiza proqramları, təhlükəsizlik sistemləri və loq idarəetmə platformaları fərqli ixrac formatlarından istifadə edə bilər. Bir sistemdən əldə olunmuş məlumatın digər mühitdə birbaşa emalı hər zaman mümkün olmadığından əlavə çevirmə və əl ilə uyğunlaşdırma tələb olunur. Bu isə həm vaxt itkisinə, həm də məlumat itkisi riskinə səbəb ola bilər.

Mövcud beynəlxalq çərçivələr müəyyən baza yaradır. ISO/IEC 27037 rəqəmsal sübutların identifikasiyası, toplanması, əldə olunması və qorunması üzrə ümumi prinsipləri müəyyən edir [4]. NIST SP 800-86 isə insident cavablandırma prosesində kriminalistika metodlarının tətbiqinə dair praktik tövsiyələr təqdim edir [5]. Bununla belə, həmin sənədlər IoT, kiber-fiziki sistemlər və fiziki-rəqəmsal inteqrasiya olunmuş hadisələrin bütün xüsusiyyətlərini tam əhatə etmir.

Standartlaşma sahəsində digər məsələ sübutun hərəkət zəncirinin fərqli formalarda aparılmasıdır. Müxtəlif qurumlarda istifadə olunan sənədləşdirmə üsulları, təsdiqləmə qaydaları və audit yanaşmaları eyni olmadıqda sübutun izlənə bilməsi çətinləşir. Xüsusilə çoxqurumlu araşdırmalarda bu problem daha qabarıq şəkildə ortaya çıxır.

Təhlillər göstərir ki, standartlaşma problemləri araşdırmaların keyfiyyətinə, nəticələrin təkrarlana bilməsinə və sübutların hüquqi qiymətləndirilməsinə birbaşa təsir edir. Bu səbəbdən vahid terminologiyanın formalaşdırılması, açıq məlumat formatlarının təşviqi, ümumi sənədləşdirmə modellərinin hazırlanması və hibrid kriminalistika üçün genişləndirilmiş metodiki çərçivələrin işlənməsi zəruri görünür.

D. Hüquqi və etik problemlər

Hibrid kriminalistika sahəsində hüquqi və etik məsələlər araşdırmanın texniki tərəfi qədər mühüm əhəmiyyət daşıyır.

Fiziki və rəqəmsal sübutların eyni iş çərçivəsində istifadə olunması müxtəlif hüquqi prosedurların paralel tətbiqini tələb edir. Sübutların qanuni əsas olmadan əldə olunması, şəxsi məlumatların həddindən artıq toplanması və prosedur pozuntuları sonradan nəticələrin hüquqi qüvvəsinə təsir göstərə bilər.

Əsas hüquqi məsələlərdən biri səlahiyyət və icazə çərçivəsinin düzgün müəyyən edilməsidir. Fiziki obyektlərə baxış keçirilməsi, cihazların götürülməsi, yaddaş daşıyıcılarından surət çıxarılması, istifadəçi hesablarının araşdırılması və uzaq serverlərdən məlumat əldə olunması eyni hüquqi rejimə tabe olmaya bilər. Xüsusilə bir hissəsi fiziki mühitdə, digər hissəsi isə onlayn platformalarda yerləşən sübutlar üzrə prosedur fərqləri meydana çıxır.

Mobil qurğular, ağıllı ev sistemləri, geolokasiya xidmətləri, biometrik giriş sistemləri və bulud platformaları istifadəçilər haqqında geniş həcmdə şəxsi məlumat saxlayır. Araşdırma zamanı hadisə ilə əlaqəli məlumatların seçilməsi ilə əlaqəsiz şəxsi məlumatların qorunması arasında balans saxlanılmalıdır. Əks halda proporsionallıq prinsipi pozula bilər.

Sübutların hüquqi qəbul edilə bilməsi ayrıca əhəmiyyət daşıyır. Əldəetmə mərhələsi düzgün sənədləşdirilmədikdə, sübutun hərəkət zənciri tam izlənmədikdə və ya məlumatın bütövlüyü təsdiqlənmədikdə sübutun etibarlılığı şübhə altına düşə bilər. Bu xüsusilə rəqəmsal surətlər, loq ixracları və üçüncü tərəf platformalarından təqdim olunmuş məlumatlar üçün daha aktualdır [4, 6].

Etik məsələlər sırasında avtomatlaşdırılmış analiz vasitələrinin istifadəsi də qeyd olunmalıdır. Süni intellekt əsaslı sistemlər vasitəsilə davranış nümunələrinin təhlili, risk göstəricilərinin hesablanması və şübhəli fəaliyyətlərin avtomatik seçilməsi şəffaflıq və qərəzsizlik baxımından suallar yarada bilər. Nəticələrin necə formalaşdığının izah edilə bilməməsi ekspert qiymətləndirməsini çətinləşdirə bilər.

Sərhədlərarası məlumat mübadiləsi də hüquqi baxımdan mürəkkəb sahə hesab olunur. Bulud xidmətləri və beynəlxalq platformalarda saxlanılan məlumatlar müxtəlif hüquqi məkanlarda yerləşə bilər. Bu səbəbdən məlumatın sorğu əsasında təqdim olunması, saxlanılması və istifadə qaydaları ölkələr üzrə fərqlənə bilər ki, bu da araşdırmanın müddətinə və effektivliyinə təsir göstərir.

Təhlillər göstərir ki, hüquqi və etik problemlər hibrid kriminalistikanın praktiki tətbiqində əsas məhdudlaşdırıcı amillərdən biridir. Bu səbəbdən aydın prosedur qaydalarının hazırlanması, şəxsi məlumatların minimallaşdırılması prinsiplərinin tətbiqi, şəffaf ekspertiza metodlarının seçilməsi və qanunvericiliyin texnoloji dəyişikliklərə uyğun təkmilləşdirilməsi zəruri görünür.

E. Böyük verilənlər və analiz çətinlikləri

Hibrid kriminalistika mühitində məlumat həcminin sürətlə artması araşdırma prosesini mürəkkəbləşdirən əsas amillərdən biridir. Sensor sistemləri, müşahidə kameraları, mobil qurğular, şəbəkə infrastrukturu, bulud platformaları və digər rəqəmsal mənbələr qısa müddətdə böyük həcmdə məlumat yaradır. Fiziki və rəqəmsal sübutların paralel toplandığı hadisələrdə bu məlumat axınının idarə olunması xüsusi çətinlik yaradır [2, 3].

Bir çox hallarda araşdırma materialı yalnız bir neçə fayldan ibarət olmur, əksinə müxtəlif mənbələrdən toplanmış geniş məlumat massivinə çevrilir. Video yazılar, sistem loqları, istifadəçi tarixçələri, cihaz məlumatları, telemetriya göstəriciləri və hadisə yerinə dair sənədləşdirilmiş materiallar eyni iş üzrə mövcud ola bilər. Bu şəraitdə bütün məlumatın əl üsulu ilə təhlili vaxt və resurs baxımından səmərəli hesab olunmur [6].

Məlumat axınının fasiləsiz yenilənməsi əlavə çətinlik yaradır. Təhlükəsizlik sistemləri, şəbəkə trafik qeydləri və canlı sensor platformaları davamlı şəkildə yeni verilənlər formalaşdırır. Buna görə bəzi hallarda araşdırma yalnız retrospektiv təhlillə məhdudlaşmır, operativ qiymətləndirmə imkanlarını da tələb edir [5].

Analitik yükü artıran digər amil məlumat növlərinin müxtəlifliyidir. Eyni hadisə üzrə strukturlaşdırılmış verilənlər bazası qeydləri, mətn tipli loqlar, video materiallar, şəkillər, coğrafi koordinatlar, fiziki sübut qeydləri və meta verilənlər mövcud ola bilər. Bu fərqli mənbələrin vahid analitik mühitdə uyğunlaşdırılması əlavə metodoloji yanaşmalar tələb edir [1, 9].

Böyük verilənlər şəraitində əsas məsələ yalnız məlumat toplamaq deyil, hadisə ilə əlaqəli dəyərli informasiyanı ümumi axın içərisindən seçə bilməkdir. Əhəmiyyətli qeydlər çox zaman çoxsaylı adi fəaliyyət məlumatları arasında gizlənmiş olur. Bu isə yanlış pozitiv nəticələrin yaranması və ya vacib məlumatın nəzərdən qaçırılması riskini artırır [10].

Texniki resurs məhdudiyyətləri də nəzərə alınmalıdır. Böyük həcmli məlumatların saxlanılması, indeksləşdirilməsi, sürətli axtarışı, vizuallaşdırılması və emalı yüksək hesablama gücü, yaddaş resursu və uyğun proqram vasitələri tələb edir. Bu imkanların məhdud olduğu mühitlərdə araşdırmanın müddəti və keyfiyyəti mənfi təsirlənə bilər [11, 12].

Təhlillər göstərir ki, böyük verilənlər problemi hibrid kriminalistikada yalnız həcm məsələsi deyil, eyni zamanda seçmə, prioritetləşdirmə və düzgün interpretasiya problemidir. Bu səbəbdən avtomatlaşdırılmış filtrasiya mexanizmləri, süni intellekt əsaslı ilkin təsnifat vasitələri, vizual analitika platformaları və çoxmənbəli məlumatların əlaqələndirilməsi imkanları xüsusi əhəmiyyət daşıyır [5, 10].

IV. HİBRİD KRİMİNALİSTİKA ÜÇÜN METODOLOJİ YANAŞMALAR

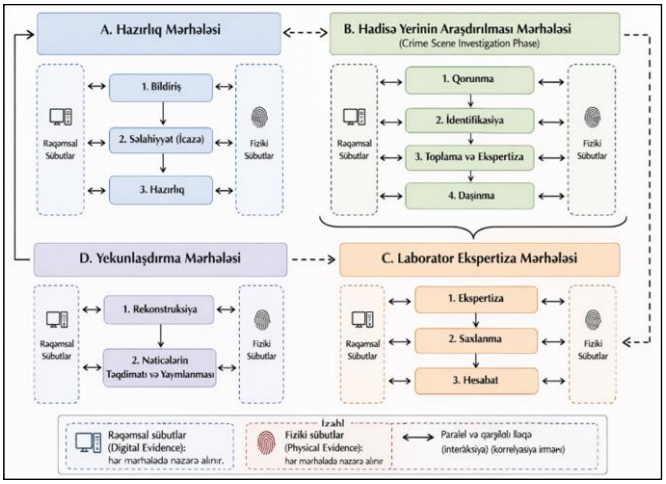
A. Hibrid kriminalistika modelləri

Ədəbiyyatda fiziki və rəqəmsal sübutların birgə araşdırılmasına yönəlmiş metodoloji yanaşmaların sayı məhdud olsa da, son illərdə bu istiqamətdə müəyyən modellər formalaşmağa başlamışdır. Klassik rəqəmsal kriminalistika çərçivələri əsasən rəqəmsal sübutların identifikasiyası, toplanması, qorunması, təhlili və təqdim olunmasına fokuslandığı halda, hibrid yanaşmalar bu prosesə fiziki sübutların da paralel inteqrasiyasını nəzərdə tutur [5, 6].

Bu baxımdan Vlachopoulos və həmmüəlliflər tərəfindən təklif olunmuş hibrid rəqəmsal sübutların araşdırılması modeli ("*A Model for Hybrid Evidence Investigation")* diqqət çəkən nümunələrdən biri hesab oluna bilər [1]. Həmin model araşdırma prosesini dörd əsas mərhələ üzrə strukturlaşdırır (Şəkil 1). Bunlar hazırlıq mərhələsi, hadisə yerinin araşdırılması mərhələsi, laborator ekspertiza mərhələsi və yekunlaşdırma

mərhələsidir. Modelin əsas xüsusiyyəti hər mərhələdə rəqəmsal və fiziki sübutların paralel şəkildə nəzərə alınmasıdır.

Hazırlıq mərhələsində bildirişin qəbulu, zəruri səlahiyyətlərin alınması və əməliyyat hazırlığı kimi məsələlər nəzərdə tutulur. Hadisə yerinin araşdırılması mərhələsində sübutların qorunması, identifikasiyası, toplanması və təhlükəsiz daşınması həyata keçirilir. Sonrakı mərhələdə laborator ekspertiza çərçivəsində əldə olunmuş materialların təhlili, saxlanması və hesabatlaşdırılması aparılır. Yekun mərhələdə isə hadisənin rekonstruksiyası və nəticələrin aidiyyəti tərəflərə təqdim olunması nəzərdə tutulur.



Şəkil 1. Hibrid rəqəmsal sübutların araşdırılması modeli.

Şəkil 1-də göstərildiyi kimi, modelin əsas metodoloji üstünlüyü sübutların növünə görə ayrı-ayrı deyil, vahid proses daxilində idarə olunmasını təşviq etməsidir. Bu yanaşma xüsusilə həm fiziki izlərin, həm də rəqəmsal qeydlərin eyni hadisə üzrə mövcud olduğu hallarda praktik əhəmiyyət daşıyır. Məsələn, biometrik giriş sistemləri, müşahidə infrastrukturu, qoşulmuş nəqliyyat vasitələri və ağıllı obyektlərlə bağlı hadisələrdə belə inteqrasiyalı yanaşma məqsədəuyğun hesab oluna bilər.

Bununla yanaşı, müasir hibrid mühitlərdə yalnız mərhələli araşdırma modeli ilə kifayətlənmək bütün hallarda yetərli olmaya bilər. IoT cihazları, bulud platformaları, real-vaxt sensor sistemləri və çoxmənbəli loq infrastrukturu əlavə analitik tələblər yaradır [2, 9, 12]. Bu səbəbdən mövcud proses yönümlü modellərlə yanaşı, sübutların zaman, məkan və hadisə əlaqələri üzrə qiymətləndirilməsini nəzərdə tutan tamamlayıcı çərçivələrə ehtiyac müşahidə olunur.

Hibrid kriminalistika modellərinin mühüm istiqamətlərindən biri rəqəmsal insident cavablandırma prosesləri ilə klassik fiziki kriminalistika metodlarının inteqrasiyasıdır. Rəqəmsal kriminalistika və insidentlərə cavab (Digital Forensics and Incident Response) yanaşmaları ənənəvi olaraq rəqəmsal izlərin operativ aşkarlanması, insidentin lokallaşdırılması, sübutların qorunması və texniki təhlili üçün istifadə olunur. Fiziki kriminalistika isə hadisə yerinin baxışı, maddi sübutların toplanması, izlərin qiymətləndirilməsi və ekspertiza prosedurlarını əhatə edir. Müasir hibrid hadisələrdə bu iki istiqamətin ayrıca deyil, əlaqəli şəkildə tətbiqi daha məqsədəuyğun hesab olunur [1, 6].

Məsələn, server otağına icazəsiz giriş hadisəsində yalnız sistem loqlarının araşdırılması kifayət etməyə bilər. Eyni zamanda giriş nöqtəsindəki biometrik sistem qeydləri, müşahidə kamerası görüntüləri, fiziki izlər və avadanlıq üzərində müdaxilə əlamətləri də qiymətləndirilməlidir. Bu baxımdan kriminalistika yanaşmalarının fiziki kriminalistika prosedurları ilə birləşdirilməsi hadisənin daha dolğun rekonstruksiyasına imkan yarada bilər.

Digər istiqamət çoxqatlı yanaşmalarla bağlıdır. Bu yanaşmalarda sübutlar tək mənbə üzrə deyil, müxtəlif səviyyələr üzrə təhlil olunur. Adətən cihaz səviyyəsi, şəbəkə səviyyəsi, tətbiq səviyyəsi, istifadəçi fəaliyyəti səviyyəsi və fiziki mühit səviyyəsi ayrıca nəzərdən keçirilir [2, 9]. Belə strukturlaşdırma mürəkkəb hadisələrdə məlumatların sistemləşdirilməsinə və analiz prosesinin mərhələləndirilməsinə kömək edir.

Çoxqatlı modellərin üstünlüklərindən biri müxtəlif səviyyələrdə yaranmış izlər arasında əlaqələrin müəyyən edilməsidir. Məsələn, istifadəçi hesabında aparılmış əməliyyat, həmin vaxt şəbəkə trafikində müşahidə olunan aktivlik və fiziki giriş sistemində qeydə alınmış keçid hadisəsi birlikdə qiymətləndirilə bilər. Bu tip korrelyasiya hadisələrin səbəb-nəticə əlaqələrinin müəyyən edilməsinə şərait yaradır.

Təhlillər göstərir ki, kriminalistik proseslərinin fiziki kriminalistika metodları ilə inteqrasiyası və çoxqatlı yanaşmaların tətbiqi hibrid kriminalistikanın praktik effektivliyini artıran istiqamətlərdən biridir. Araşdırmalar göstərir ki, hibrid mühitlərdə səmərəli fəaliyyət üçün vahid əməliyyat prosedurları, inteqrasiya olunmuş analiz platformaları və çoxsəviyyəli sübut idarəetmə mexanizmləri əsas inkişaf istiqamətləri hesab oluna bilər.

B. IoT və kiber-fiziki sistemlər üçün kriminalistika çərçivələri

IoT və kiber-fiziki sistemlər (KFS) üzrə kriminalistika tədqiqatlarında əsas istiqamətlərdən biri bu mühitlər üçün xüsusi araşdırma çərçivələrinin hazırlanmasıdır. Ənənəvi rəqəmsal kriminalistika modelləri əsasən kompüter, server və mobil cihaz mərkəzli olduğundan, sensor şəbəkələri, idarəetmə modulları, aktuatorlar, telemetriya axınları və bulud inteqrasiyasından ibarət mürəkkəb IoT/KFS ekosistemlərini tam əhatə etmir. Bu səbəbdən son illərdə həmin mühitlərə uyğunlaşdırılmış metodoloji çərçivələr formalaşdırılmışdır [2, 3, 13].

Ədəbiyyatda geniş müzakirə olunan modellərdən biri IoTFR (Internet of Things Forensic Readiness) çərçivəsidir. Bu yanaşma hadisədən sonrakı araşdırmadan daha çox hadisədən əvvəl hazırlıq prinsipinə əsaslanır. IoTFR modelində audit jurnallarının aktiv saxlanılması, NTP/PTP əsaslı vaxt sinxronizasiyası, logların mərkəzləşdirilməsi, saxlanma siyasətlərinin müəyyənləşdirilməsi və sübutların hüquqi baxımdan qəbul edilə bilən formada qorunması nəzərdə tutulur. Məqsəd insident baş verdikdən sonra sübut çatışmazlığının qarşısını almaqdır.

Digər mühüm istiqamət təbəqələndirilmiş kriminalistik çərçivə (layered forensic framework) modelləridir. Bu yanaşmada sistem cihaz təbəqəsi, rabitə təbəqəsi, xidmət təbəqəsi və tətbiq təbəqəsi üzrə təhlil edilir. Cihaz səviyyəsində daxili proqram təminatı (firmware), "EEPROM/flash" yaddaş,

sensor oxunuşları və lokal keş məlumatları, rabitə səviyyəsində MQTT, CoAP, Zigbee, BLE və TCP/IP trafik qeydləri, xidmət səviyyəsində API loqları və bulud sessiya məlumatları, tətbiq səviyyəsində isə istifadəçi əməliyyat tarixçəsi araşdırılır [2, 3].

IoT sistemləri üçün istifadə olunan digər model üç zonalı kriminalistik əldəetmə çərçivəsi (three-zone forensic acquisition framework) hesab olunur. Burada sübut mənbələri cihaz zonası, lokal şəbəkə zonası və kənar zonalar və ya bulud zonası üzrə ayrılır. Bu yanaşma göstərir ki, ağıllı qurğular üzrə sübutlar çox vaxt yalnız cihazın daxilində deyil, şlüzdə (gateway), mobil tətbiqdə və uzaq platformalarda da saxlanılır [3, 14].

Kiber-fiziki sistem mühitləri üçün xüsusi əhəmiyyət daşıyan yanaşmalardan biri prosesyönümlü kriminalistik çərçivə (process-aware forensic framework) modelidir. Bu modeldə yalnız rəqəmsal qeydlər deyil, fiziki proses parametrləri də araşdırmaya daxil edilir. Temperatur, təzyiq, axın sürəti, enerji yüklənməsi, vibrasiya, aktuator reaksiyası və sistemin cavab gecikməsi kimi göstəricilər loq məlumatları ilə birlikdə qiymətləndirilir. Belə yanaşma SCADA, PLC, DCS və ICS tipli sənaye idarəetmə sistemlərində xüsusilə vacibdir [13].

Kiber-fiziki sistemlər üzrə digər terminoloji istiqamət vəziyyətəsaslı kriminalistik analiz (state-aware forensic analysis) yanaşmasıdır. Burada sistemin normal əməliyyat vəziyyəti ilə hadisə zamanı yaranmış vəziyyət müqayisə edilir. Sensor giriş məlumatları və idarəetmə komandalarının ardıcıllığı təhlil olunaraq anomaliya nöqtələri müəyyən edilir. Bu metod proses manipulyasiyası, göstərici qiymətlərinin dəyişdirilməsi və icazəsiz komanda ötürülməsi hallarının aşkarlanmasında istifadə olunur [13].

Son dövrdə ontologiya əsaslı kriminalistik çərçivə (ontology-based forensic framework) modellərinə maraq artmışdır. Bu çərçivələrdə cihaz növləri, sensor hadisələri, idarəetmə əmrləri, istifadəçi fəaliyyəti və sübut əlaqələri semantik struktur şəklində təqdim olunur. Bunun nəticəsində heterogen IoT və kiber-fiziki sistemlər platformalarından alınmış məlumatların əlaqələndirilməsi və avtomatlaşdırılmış analiz imkanları genişlənir [3].

Təhlillər göstərir ki, IoT və KFS mühitlərində vahid universal model mövcud deyil. IoTFR hazırlıq və sübut hazır vəziyyəti təmin etdiyi halda, təbəqələndirilmiş modellər strukturlaşdırılmış toplama, üç zonalı yanaşmalar paylanmış sübutların müəyyən edilməsi, prosesyönümlü və vəziyyətəsaslı modellər isə fiziki proseslərin interpretasiyası baxımından üstünlük təşkil edir. Bu səbəbdən gələcək inkişaf istiqaməti həmin çərçivələrin inteqrasiyası, standartlaşdırılması və real-vaxtlı araşdırma sistemlərinə uyğunlaşdırılması ilə bağlıdır [2, 3, 13, 14].

C. Süni intellekt və maşın təlimi

Süni intellekt və maşın təlimi texnologiyalarının inkişafı rəqəmsal kriminalistika sahəsində yeni analitik imkanlar yaratmışdır. Ənənəvi yanaşmalarda sübutların araşdırılması əsasən ekspert tərəfindən əl üsulu ilə aparılırdısa, müasir mərhələdə böyük həcmli məlumatların emalı, nümunələrin müəyyən edilməsi və anomaliyaların aşkarlanması üçün avtomatlaşdırılmış metodlardan istifadə genişlənməkdədir [10]. Xüsusilə hibrid kriminalistika mühitində fiziki və rəqəmsal mənbələrdən eyni vaxtda böyük həcmdə məlumat toplandığı üçün intellektual analiz alətlərinə ehtiyac daha aydın hiss olunur.

Kriminalistika sahəsində süni intellektin əsas tətbiq istiqamətlərindən biri anomaliyaların aşkarlanmasıdır. Bu yanaşmada normal davranış modelləri ilə müqayisədə qeyri-adi aktivliklər müəyyən edilir. Məsələn, istifadəçi hesabında qeyri-adi giriş saatları, şəbəkədə gözlənilməz trafik artımı, giriş nəzarət sistemində ardıcıl uğursuz autentifikasiya cəhdləri və ya sensor göstəricilərində normadan kənar dəyişikliklər potensial insident əlaməti kimi qiymətləndirilə bilər. Belə metodlar ilkin xəbərdarlıq və prioritetləşdirmə baxımından faydalı hesab olunur.

Maşın təlimi yanaşmaları müxtəlif tip məlumatların təsnifatı üçün istifadə oluna bilər. Məsələn, loq qeydlərinin risk səviyyəsinə görə qruplaşdırılması, zərərli və normal fəaliyyət nümunələrinin fərqləndirilməsi, şübhəli istifadəçi davranışlarının seçilməsi və ya fayl kolleksiyalarında prioritet obyektlərin müəyyən edilməsi bu istiqamətə aid edilə bilər. Bu baxımdan alqoritmik metodlar ekspert resurslarının daha səmərəli bölüşdürülməsinə kömək edə bilər.

Hibrid kriminalistika kontekstində süni intellektin daha mühüm tətbiqlərindən biri çoxmənbəli sübutların avtomatik analizi ilə bağlıdır. Fiziki giriş qeydləri, video müşahidə materialları, mobil cihaz məlumatları, şəbəkə loqları və geolokasiya göstəriciləri eyni hadisə ilə bağlı ola bilər. Çoxmənbəli verilənlərin birləşdirilməsi (Multi-model data fusion) yanaşmaları belə məlumatların vahid analitik mühitdə birləşdirilməsinə və əlaqəli nümunələrin avtomatik müəyyən edilməsinə imkan yarada bilər [10].

Bununla yanaşı, süni intellekt sistemlərinin tətbiqi müəyyən məhdudiyyətlərlə müşayiət olunur. Təlim məlumatlarının keyfiyyəti, yanlış pozitiv nəticələr, alqoritmik qərəzlilik və nəticələrin izah edilə bilməməsi kriminalistika baxımından mühüm məsələlərdəndir. Xüsusilə məhkəmə və ekspertiza proseslərində istifadə olunan nəticələrin yoxlanıla bilməsi və əsaslandırılması vacib şərt hesab olunur. Bu səbəbdən izah oluna bilən süni intellekt (Explainable AI) yanaşmaları xüsusi əhəmiyyət daşıyır.

Son illərdə görüntü analizi metodları da kriminalistika tədqiqatlarında geniş tətbiq olunur. Video müşahidə görüntülərinin təhlili, obyektlərin hərəkət trayektoriyasının müəyyən edilməsi, hadisə yerində aktivliyin seçilməsi və görüntü materiallarının sürətli indeksləşdirilməsi bu sahəyə daxildir.

Təhlillər göstərir ki, süni intellekt və maşın təlimi kriminalistika ekspertini əvəz edən deyil, onu dəstəkləyən alət kimi qiymətləndirilməlidir. Bu texnologiyalar ilkin süzgəcdən keçirmə, nümunə aşkarlanması, böyük verilənlərin prioritetləşdirilməsi və operativ analiz mərhələlərində yüksək səmərə verə bilər. Lakin yekun qərarların ekspert qiymətləndirməsi və hüquqi prosedurlarla tamamlanması məqsədəuyğun hesab olunur.

Bu baxımdan gələcək mərhələdə kriminalistika üçün izah oluna bilən maşın təlimi modellərinin, çoxmənbəli məlumat birləşdirmə sistemlərinin, real-vaxtda anomaliya aşkarlama platformalarının və insan-nəzarətli avtomatlaşdırılmış analiz mühitlərinin inkişaf etdirilməsi perspektiv istiqamət kimi qiymətləndirilə bilər.

D. Bulud və paylanmış sistemlərdə kriminalistika

Bulud texnologiyalarının, virtual infrastrukturun və paylanmış hesablama mühitlərinin geniş yayılması rəqəmsal kriminalistika sahəsində yeni yanaşmaların formalaşmasına səbəb olmuşdur. Ənənəvi kriminalistika modelləri əsasən istifadəçinin fiziki nəzarətində olan kompüterlər, serverlər və lokal daşıyıcılar üzərində qurulduğu halda, müasir mərhələdə məlumatların əhəmiyyətli hissəsi uzaq xidmət platformalarında, virtual resurslarda və müxtəlif coğrafi məkanlarda yerləşən məlumat mərkəzlərində saxlanılır. Bu dəyişiklik sübutların əldə olunması, qorunması və təhlili prosesinə birbaşa təsir göstərir [3].

Bulud kriminalistikası rəqəmsal sübutların bulud xidmətləri mühitində identifikasiyası, toplanması, qorunması və araşdırılması ilə bağlı metodoloji yanaşmaları əhatə edir. Bu sahədə əsas çətinliklərdən biri istifadəçinin fiziki infrastruktur üzərində birbaşa nəzarət imkanının məhdud olmasıdır. Bir çox hallarda server avadanlığına çıxış mümkün olmur, məlumatlar isə virtual mühitlərdə və çoxistifadəçili platformalarda saxlanılır. Bu səbəbdən klassik disk götürülməsi, lokal surətin çıxarılması və cihazın fiziki ekspertizası kimi metodlar bir sıra hallarda tətbiq edilə bilmir [3].

Bulud mühitlərində sübut mənbələri yalnız fayllarla məhdudlaşmır. Audit loqları, autentifikasiya qeydləri, istifadə tarixçələri, API loqları, ani vəziyyət surətləri (snapshot), ehtiyat nüsxələri, konteyner fəaliyyət qeydləri və meta verilənlər mühüm sübut xarakteri daşıya bilər. Bir çox insidentlərdə ən dəyərli məlumat məhz xidmət loqları və istifadəçi fəaliyyət tarixçəsində əks olunur.

Praktik baxımdan əlavə çətinliklərdən biri bəzi xidmət təminatçılarında genişləndirilmiş audit loqlarının, uzunmüddətli saxlanma imkanlarının, "snapshot" funksiyalarının və ehtiyat nüsxələrinin ayrıca kommersiya xidməti kimi təqdim edilməsidir. Bu halda istifadəçi və ya araşdırma aparan tərəf zəruri məlumatlara tam çıxış əldə etməyə bilər. Müəyyən hallarda loqların ixracı və ya saxlanma müddətinin artırılması yalnız əlavə xidmət paketləri çərçivəsində mümkün olur ki, bu da araşdırmanın operativliyinə və məlumatların tamlığına təsir göstərə bilər [3].

Paylanmış sistemlərdə məlumatların müxtəlif qovşaqlarda saxlanılması analiz üçün ayrıca çətinliklər yaradır. Hadisə ilə bağlı qeydlərin bir hissəsi mərkəzi serverdə, digər hissəsi isə fərqli regionlarda yerləşən replikalarda və ya lokal cihazlarda ola bilər. Bu səbəbdən sübutların tam şəkildə toplanması və vahid zaman xətti üzrə uyğunlaşdırılması əlavə metodoloji yanaşmalar tələb edir. kənar hesablama (edge computing) mühitlərində isə məlumatların bir hissəsi mərkəzi buluddan kənarda, istifadəçiyə yaxın hesablama qovşaqlarında emal olunur. Bu yanaşma gecikməni azaltmaq və real-vaxtlı xidmətləri sürətləndirmək baxımından üstünlük versə də, kriminalistika baxımından yeni problemlər yaradır. Çünki hadisə ilə bağlı məlumatlar mərkəzi sistemdə deyil, çoxsaylı kənar qurğularda və qısaömürlü hesablama mühitlərində saxlanıla bilər.

Hibrid kriminalistika baxımından bulud və paylanmış sistemlər xüsusi əhəmiyyət kəsb edir. Məsələn, ağıllı giriş sistemi lokal cihazda hadisə qeydi yarada, eyni zamanda autentifikasiya məlumatlarını bulud serverinə ötürə bilər. Belə hallarda fiziki cihaz, lokal şəbəkə və uzaq xidmət infrastrukturu birlikdə araşdırılmalıdır. Bu isə müxtəlif mənbələrdən əldə olunan sübutların korrelyasiyasını zəruri edir.

Bulud və paylanmış sistemlərdə effektiv araşdırma aparılması üçün xidmət təminatçıları ilə operativ əməkdaşlıq mexanizmləri, vahid metaverilən standartları, sübutların sürətli qorunması və çoxmənbəli loqların əlaqələndirilmiş təhlili xüsusi əhəmiyyət daşıyır.

NƏTİCƏ

Müasir texnoloji inkişaf nəticəsində fiziki və rəqəmsal mühitlər arasındakı sərhədlər getdikcə zəifləməkdə, hadisələr üzrə formalaşan sübutlar isə daha çox hibrid xarakter almaqdadır. Ağıllı qurğular, IoT ekosistemləri, kiber-fiziki sistemlər, bulud platformaları və paylanmış xidmət infrastrukturu şəraitində bir hadisə üzrə həm maddi, həm də rəqəmsal izlərin paralel şəkildə meydana çıxması kriminalistika sahəsində yeni metodoloji yanaşmaların aktuallığını artırmışdır.

Aparılmış təhlillər göstərir ki, ənənəvi fiziki kriminalistika və klassik rəqəmsal kriminalistika modelləri ayrı-ayrılıqda mühüm əhəmiyyət daşısa da, mürəkkəb çoxmənbəli hadisələrin tam araşdırılması üçün hər zaman kifayət etmir. Sübutların heterogenliyi, fərqli formatlarda mövcudluğu, böyük verilənlər mühiti, standartlaşma çatışmazlıqları, hüquqi məhdudiyyətlər və paylanmış platformalarda məlumatların yerləşməsi hibrid araşdırmalarda əsas çətinliklər sırasında çıxış edir.

Məqalədə nəzərdən keçirilən elmi yanaşmalar göstərir ki, hibrid kriminalistika sahəsində inkişaf əsasən inteqrasiya olunmuş modellər, IoT və kiber-fiziki sistemlər üçün xüsusi çərçivələr, süni intellekt əsaslı analiz metodları və bulud kriminalistikası istiqamətində gedir. Xüsusilə çoxmənbəli məlumatların korrelyasiyası, zaman xəttinin qurulması, avtomatlaşdırılmış ilkin analiz və real-vaxtlı monitorinq imkanları gələcək tədqiqatlar üçün perspektiv sahələr hesab oluna bilər.

Bununla yanaşı, praktik tətbiq baxımından vahid terminologiyanın formalaşdırılması, meta verilən əsaslı sübut idarəetmə mexanizmlərinin yaradılması, müxtəlif platformalar arasında qarşılıqlı fəaliyyət imkanlarının artırılması və hüquqi prosedurların texnoloji dəyişikliklərə uyğunlaşdırılması mühüm əhəmiyyət daşıyır. Xüsusilə xidmət təminatçıları ilə əməkdaşlıq, uzaq mühitlərdə sübutların operativ qorunması və ekspertiza nəticələrinin təkrarlana bilməsi gələcək mərhələdə diqqət tələb edən məsələlərdəndir.

Nəticə etibarilə, hibrid kriminalistika müasir kriminalistika elminin perspektiv istiqamətlərindən biri kimi qiymətləndirilə bilər. Fiziki və rəqəmsal sübutların vahid yanaşma əsasında araşdırılması həm elmi, həm də əməliyyat baxımından daha dəqiq, çevik və əsaslandırılmış nəticələrin əldə olunmasına imkan yarada bilər. Bu sahədə metodoloji və tətbiqi inkişafın davam etdirilməsi gələcək dövr üçün zəruri görünür.

ƏDƏBİYYAT

[1] K. Vlachopoulos, E. Magkos, and V. Chrissikopoulos, "A Model for Hybrid Evidence Investigation," in Emerging Digital Forensics

Applications for Crime Detection, Prevention, and Security. Hershey, PA, USA: IGI Global, 2013, pp. 1–20.

[2] 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.

[3] P. Sharma and L. K. Awasthi, "IoT forensics in ambient intelligence environments: Legal issues, research challenges and future directions," Journal of Ambient Intelligence and Smart Environments, vol. 16, no. 2, pp. 145–162, 2024.

[4] ISO/IEC 27037:2012, Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva, Switzerland: International Organization for Standardization, 2012.

[5] National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). Gaithersburg, MD, USA, 2006.

[6] E. Casey, Digital Evidence and Computer Crime, 3rd ed. Amsterdam, Netherlands: Academic Press, 2011.

[7] F. Casino, T. Dasaklis, and C. Patsakis, "Blockchain-based secure chain of custody for digital evidence management: A review," IEEE Access, vol. 7, pp. 18865–18878, 2019.

[8] A. M. Elmisery, "Collaborative forensic platform for electronic artefacts in the Internet of Vehicles," in Proc. International Conference, 2024, pp. 1–8.

[9] H. van Beek and C. van den Pol, "Criminalistic zoom levels: Unravelling the hierarchy of forensic traces," Science & Justice, vol. 65, no. 1, pp. 44–55, 2025.

[10] P. Senthil and S. Selvakumar, "A hybrid deep learning technique based integrated multi-model data fusion for forensic investigation," Journal of Intelligent & Fuzzy Systems, vol. 43, no. 5, pp. 1–15, 2022.

[11] "Digital Stratigraphy—A Pattern Analysis Framework Integrating Computer Forensics, Criminology, and Forensic Archaeology for Crime Scene Investigation," Forensic Sciences, vol. 5, no. 1, pp. 1–18, 2025.

[12] V. Pooryousef et al., "Criminator: An Easy-to-Use XR 'Crime Animator' for Rapid Reconstruction and Analysis of Dynamic Crime Scenes," arXiv preprint arXiv:2601.01234, 2026.

[13] "Framework for Forensic Analysis of Cyber-Physical Attacks: Correlating Digital Traces with Physical Outcomes," IEEE Access, vol. 12, pp. 55421–55439, 2024.

[14] "Accuracy of Three-Dimensional Gaussian Splatting for Virtual Crime Scene Reconstruction," Frontiers in Virtual Reality, vol. 6, Art. no. 102233, 2025.

Hybrid Forensics of Physical and Digital Objects: Problems and Solutions

Ramiz Shikhaliyev[1], Sanan Valizada[2]

[1,2] Institute of Information Technology, Baku, Azerbaijan

[1]*shikhramiz61@gmail.com*, [2]*senanvalizade@gmail.com*

Abstract- The acceleration of digitalization and the widespread adoption of IoT and cyber-physical systems have led to the integration of physical and digital evidence, creating new challenges in the field of forensics. This has turned the collection, analysis, and legal admissibility of evidence in hybrid environments into an important scientific and practical issue. The article examines the hybrid forensics approach emerging in the context of the integration of physical and digital objects. The main challenges related to the heterogeneity, collection, preservation, and legal admissibility of evidence in modern IoT and cyber-physical systems are identified. In addition, the study proposes the integration of data collected from various sources, artificial intelligence-based analysis methods, and standardized forensic frameworks to address these challenges.

Keywords- hybrid forensics; physical evidence; digital evidence; cyber-physical systems; evidence integration; IoT forensics.