Kibercinayətkarlıq Əməlləri: Rəqəmsal İzlər və Sübutlar

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

***Xülasə*— Məqalədə kibercinayətkarlıq əməllərinin müasir xüsusiyyətləri və onların araşdırılmasında rəqəmsal izlərin rolu təhlil edilmişdir. Müxtəlif informasiya sistemləri, kompüterlər, mobil cihazlar və şəbəkə mühitlərində formalaşan rəqəmsal izlərin əsas növləri sistemləşdirilmiş, onların sübut kimi istifadəsi şərtləri müəyyən edilmiş, rəqəmsal sübutların əldə olunması, qorunması, bütövlüyünün təmin edilməsi və təhlili məsələləri araşdırılmışdır. Həmçinin şifrələmə, anonimləşdirmə texnologiyaları, bulud mühitləri və böyük həcmli məlumatların emalı kimi müasir çağırışların istintaq prosesinə təsiri geniş şəkildə nəzərdən keçirilmişdir.**

Açar sözlər— rəqəmsal kriminalistika; rəqəmsal sübutlar; rəqəmsal artefaktlar; rəqəmsal izlər.

I. GİRİŞ

İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı, rəqəmsallaşmanın genişlənməsi və internet əsaslı xidmətlərin həyatın bütün sahələrinə inteqrasiyası kibercinayətkarlıq əməllərinin sayının və mürəkkəbliyinin artmasına səbəb olmuşdur. Müasir dövrdə dövlət qurumları, maliyyə institutları, kritik informasiya infrastrukturları, kommersiya təşkilatları və fərdi istifadəçilər müxtəlif növ kiberhücumların əsas hədəflərinə çevrilmişdir [1, 2].

Kibercinayətkarlıq əməllərinin transsərhəd xarakter daşıması, anonim kommunikasiya vasitələrindən istifadə imkanları və texnoloji vasitələrin davamlı inkişafı onların aşkar olunmasını və araşdırılmasını çətinləşdirən əsas amillərdən biri hesab olunur [3, 4].

Kibercinayətlərin araşdırılması prosesində rəqəmsal izlərin müəyyən olunması mühüm əhəmiyyət kəsb edir. İstifadəçi fəaliyyəti, sistem prosesləri və şəbəkə qarşılıqlı əlaqələri nəticəsində formalaşan rəqəmsal izlər hadisənin başvermə şəraitinin müəyyənləşdirilməsi, hücumun mənbəyinin identifikasiyası və hüquqpozmanın sübut olunması baxımından mühüm informasiya mənbəyi rolunu oynayır. Müxtəlif əməliyyat sistemləri, mobil qurğular, server infrastrukturları, bulud platformaları və şəbəkə avadanlıqları üzərində formalaşan məlumatlar rəqəmsal kriminalistika prosesində əsas araşdırma obyektlərindən biri hesab edilir [5, 6].

Rəqəmsal mühitdə formalaşan məlumatların sürətlə dəyişməsi və böyük həcmdə olması rəqəmsal sübutların əldə olunması və təhlili prosesində yeni problemlər yaradır.

Şifrələmə texnologiyalarının geniş tətbiqi, anonimləşdirmə vasitələri, virtual şəxsi şəbəkələr (VPN) və "The Onion Router" TOR texnologiyaları, eləcə də bulud hesablama mühitləri kibercinayətlərin araşdırılması prosesini daha mürəkkəb hala gətirir. Bununla yanaşı, böyük həcmli məlumat axınlarının emalı və müxtəlif mənbələrdən əldə olunan rəqəmsal izlərin əlaqələndirilməsi müasir rəqəmsal kriminalistika sahəsində aktual problemlərdən biri kimi qiymətləndirilir [7, 8].

Məqalənin məqsədi kibercinayətkarlıq əməlləri zamanı formalaşan rəqəmsal izlərin əsas xüsusiyyətlərinin sistemləşdirilməsi, onların rəqəmsal sübut kimi istifadəsi şərtlərinin təhlili və müasir kibertəhqiqat prosesində meydana çıxan problemlərin araşdırılmasından ibarətdir. Tədqiqat çərçivəsində rəqəmsal izlərin yaranma mənbələri, sübutların əldə olunması və bütövlüyünün təmin edilməsi mexanizmləri, eləcə də müasir texnoloji çağırışların istintaq prosesinə təsiri nəzərdən keçirilmişdir.

II. KİBERCİNAYƏTKARLIQ ƏMƏLLƏRİNİN NƏZƏRİ VƏ KRİMİNALİSTİK ƏSASLARI

A. *Kibercinayətkarlıq anlayışı və xüsusiyyətləri*

Kibercinayətkarlıq informasiya sistemləri, kompüter şəbəkələri və rəqəmsal platformalar üzərindən həyata keçirilən, məlumatların məxfiliyi, bütövlüyü və əlçatanlığına qarşı yönəlmiş hüquqazidd əməlləri əhatə edir. Bu tip cinayətlərin əsas fərqləndirici xüsusiyyəti onların fiziki mühitdən asılı olmadan, tam və ya qismən virtual mühitdə icra olunmasıdır. Nəticə etibarilə, cinayətkar və zərərçəkmiş arasında coğrafi məsafə istintaq prosesinə birbaşa təsir etmir və bu vəziyyət kibercinayətkarlığı klassik cinayət növlərindən fərqləndirir [4, 9].

Kibercinayətlərin digər mühüm xüsusiyyəti onların anonimlik imkanlarının yüksək olmasıdır. Hücum edən subyektlər çox zaman VPN, proxy serverlər, anonimləşdirici şəbəkələr və ya kompromatesiya olunmuş üçüncü tərəf sistemlərindən istifadə etməklə özlərini identifikasiya etmək imkanlarını gizlətməyə çalışırlar. Bu isə hücum mənbəyinin müəyyən olunmasını çətinləşdirir və rəqəmsal kriminalistika metodlarının daha kompleks tətbiqini tələb edir [7].

Bundan əlavə, kibercinayətkarlıq əməlləri yüksək avtomatlaşdırma səviyyəsi ilə xarakterizə olunur. Müasir zərərli proqram təminatları və hücum platformaları (attack frameworks) eyni vaxtda minlərlə sistemə təsir göstərə biləcək miqyasda əməliyyatlar icra edə bilir. Bu isə həm hücumların sürətini artırır, həm də onların aşkarlanmasını gecikdirir [5].

DOI: 10.25045/forensic.gov.2026.43

B. *Kibercinayət əməllərinin əsas növləri*

Kibercinayətkarlıq əməlləri məqsəd və icra mexanizminə görə müxtəlif kateqoriyalara ayrılır. Ən geniş yayılmış formalar arasında icazəsiz giriş (unauthorized access), zərərli proqram təminatının yayılması (malware), fişinq və sosial mühəndislik hücumları, məlumatların oğurlanması, eləcə də xidmətlərin əlçatanlığının pozulmasına yönəlmiş DDoS hücumları yer alır [3].

Bu cinayət növləri yalnız fərdi istifadəçiləri deyil, həm də dövlət informasiya sistemlərini, maliyyə institutlarını və kritik infrastruktur obyektlərini hədəf ala bilər. Xüsusilə maliyyə motivli hücumlar müasir kibercinayətkarlıqda dominant istiqamətlərdən biri hesab olunur. Eyni zamanda bəzi hücumlar yalnız texniki zərər vurmaq məqsədi daşımır, informasiya sızması və ya reputasiya zədələnməsi kimi dolayı təsirlər də yaradır [5].

Müasir dövrdə kibercinayətlərin avtomatlaşdırılmış alətlər vasitəsilə həyata keçirilməsi onların miqyasını əhəmiyyətli dərəcədə genişləndirmişdir. Botnet infrastrukturları və hazır hücum platformaları (attack-as-a-service modelləri) cinayətkar fəaliyyətlərin texniki bilik tələbini azaldaraq daha geniş yayılmasına şərait yaradır [7, 10].

Azərbaycan Respublikası qanunvericiliyində kibercinayətkarlıqla bağlı hüquqi məsuliyyət Azərbaycan Respublikasının Cinayət Məcəlləsində müəyyən edilmişdir. Məcəllənin müvafiq maddələrində kompüter sistemlərinə qanunsuz daxil olma, kompüter məlumatlarının qanunsuz əldə edilməsi, dəyişdirilməsi və məhv edilməsi, zərərli proqram vasitələrinin hazırlanması və yayılması, eləcə də kompüter sistemlərinin işinin pozulması ilə bağlı əməllər cinayət tərkibi kimi nəzərdə tutulmuşdur [11]. Bununla yanaşı, elektron məlumatların qanunsuz əldə keçirilməsi və informasiya sistemlərindən istifadə etməklə törədilən dələduzluq halları da kibercinayətkarlıq kontekstində qiymətləndirilir.

C. *Kibercinayətlərin kriminalistik xüsusiyyətləri*

Kibercinayətlərin kriminalistik xüsusiyyətləri onların törədilmə üsulu, istifadə olunan texniki vasitələr, rəqəmsal mühitdə formalaşdırdığı izlər və sübutların spesifik xarakteri ilə müəyyən olunur. Ənənəvi cinayət növlərindən fərqli olaraq kibercinayətlərdə hadisə yeri anlayışı fiziki məkanla məhdudlaşmır və bir neçə ölkənin informasiya infrastrukturlarını eyni vaxtda əhatə edə bilir. Bu xüsusiyyət kibercinayətlərin araşdırılması zamanı transsərhəd əməkdaşlıq, beynəlxalq hüquqi prosedurlar və müxtəlif hüquq sistemləri arasında informasiya mübadiləsini zəruri edən əsas amillərdən biridir [4].

Kibercinayətlərin digər mühüm kriminalistik xüsusiyyəti onların yüksək anonimlik imkanları ilə müşayiət olunmasıdır. Hücum edən şəxslər öz fəaliyyətlərini gizlətmək məqsədilə VPN xidmətlərindən, proxy serverlərdən, anonimləşdirici şəbəkələrdən və kompromatesiya olunmuş sistemlərdən istifadə edə bilirlər. Bu isə hücumun real mənbəyinin müəyyən edilməsini çətinləşdirir və rəqəmsal izlərin çoxpilləli şəkildə təhlilini tələb edir. Bəzi hallarda hücumun həyata keçirilməsi üçün istifadə olunan infrastrukturun müxtəlif ölkələrdə yerləşməsi istintaq prosesinin müddətini artırır və rəqəmsal sübutların əldə olunmasında əlavə prosedur çətinlikləri yaradır [7].

Kriminalistik baxımdan kibercinayətlərin əsas xüsusiyyətlərindən biri onların rəqəmsal izlər formalaşdırmasıdır. İstifadəçi fəaliyyəti, əməliyyat sistemi prosesləri, şəbəkə trafiki və tətbiq proqramlarının fəaliyyəti nəticəsində müxtəlif tipli log məlumatları, metadata və sistem artefaktları yaranır. Bu məlumatlar hadisənin vaxtının, istifadə olunmuş vasitələrin, hücum istiqamətinin və mümkün iştirakçıların müəyyən edilməsində mühüm əhəmiyyət daşıyır. Bununla yanaşı, kibercinayətkarlar anti-kriminalistika üsullarından istifadə etməklə həmin izlərin dəyişdirilməsinə, gizlədilməsinə və ya tamamilə silinməsinə çalışırlar [6, 12, 13].

Kibercinayətlərin araşdırılmasını çətinləşdirən digər mühüm xüsusiyyət rəqəmsal məlumatların volatil xarakter daşımasıdır. Operativ yaddaşda saxlanılan proseslər, aktiv şəbəkə bağlantıları və müvəqqəti sistem məlumatları qısa müddət ərzində dəyişə və ya tamamilə itə bilər. Bu səbəbdən rəqəmsal kriminalistika prosesində sübutların vaxtında əldə olunması və düzgün ardıcıllıqla toplanması xüsusi əhəmiyyət kəsb edir [14]. Xüsusilə canlı sistemlər üzərində aparılan araşdırmalar zamanı sübutların dəyişdirilməsi riskinin minimallaşdırılması əsas metodoloji tələblərdən biri hesab olunur.

Müasir kibercinayətlərin kriminalistik xüsusiyyətləri sırasında avtomatlaşdırılmış hücum mexanizmləri də xüsusi yer tutur. Botnet şəbəkələri, avtomatlaşdırılmış istismar platformaları və "malware-as-a-service" yanaşmaları hücumların daha geniş miqyasda və yüksək sürətlə həyata keçirilməsinə imkan yaradır. Bu vəziyyət kibercinayətlərin aşkarlanması və təhlili prosesində ənənəvi üsullarla yanaşı süni intellekt, davranış analizi və böyük həcmli məlumatların emalı kimi müasir texnologiyaların tətbiqini aktuallaşdırır [15].

Bundan əlavə, kibercinayətlərin bir çoxunda rəqəmsal sübutların müxtəlif sistemlər və platformalar üzrə parçalanmış formada mövcud olması müşahidə edilir. Eyni hadisəyə dair məlumatlar server jurnallarında, "firewall" qeydlərində, mobil cihazlarda, bulud platformalarında və şəbəkə avadanlıqlarında fərqli formalarda saxlanıla bilər. Bu isə rəqəmsal kriminalistika prosesində çoxmənbəli analiz yanaşmasının tətbiqini və müxtəlif məlumat mənbələrinin korrelyasiya olunmasını zəruri edir [5, 8, 16].

III. RƏQƏMSAL İZLƏRİN FORMALAŞMASI VƏ TƏSNİFATI

A. *Rəqəmsal iz anlayışı*

Rəqəmsal mühitdə həyata keçirilən hər bir fəaliyyət müəyyən məlumat izlərinin formalaşmasına səbəb olur. Bu izlər istifadəçi əməliyyatları, sistem prosesləri, tətbiqlərin fəaliyyəti və şəbəkə qarşılıqlı əlaqələri nəticəsində yaranan məlumat izləriini əhatə edir. Rəqəmsal kriminalistika sahəsində həmin məlumatlar "rəqəmsal iz" anlayışı altında qiymətləndirilir və onların təhlili kibercinayətlərin araşdırılmasında mühüm rol oynayır [5, 12].

Rəqəmsal izlər müxtəlif informasiya sistemlərində fərqli formalarda saxlanıla bilər. Bunlara əməliyyat sistemi jurnalları, tətbiq loqları, şəbəkə trafik qeydləri, metaverilənlər, brauzer tarixçəsi, fayl sistemləri üzərində yaranan dəyişikliklər və istifadəçi fəaliyyətinə dair digər artefaktlar aid edilir [6]. Müasir

informasiya infrastrukturlarında rəqəmsal izlərin həcmi və müxtəlifliyi sürətlə artdığından onların effektiv identifikasiyası və sistemləşdirilməsi rəqəmsal kriminalistikanın əsas problemlərindən biri hesab olunur.

Kriminalistik baxımdan rəqəmsal izlər hadisənin başvermə mexanizmini müəyyən etməyə imkan verən əsas informasiya mənbələrindən biridir. Bu izlər vasitəsilə istifadəçi fəaliyyətinin vaxt ardıcıllığı, sistemə giriş cəhdləri, məlumat ötürülməsi prosesləri və hücum zamanı istifadə olunmuş texniki vasitələr barədə məlumat əldə etmək mümkündür. Bununla yanaşı, rəqəmsal izlərin bir hissəsi dolayı xarakter daşıyır və onların interpretasiyası digər sübutlarla birlikdə aparılmalıdır [13, 15].

Rəqəmsal izlərin əsas xüsusiyyətlərindən biri onların yüksək dəyişkənliyidir. Müəyyən məlumatlar sistem fəaliyyəti nəticəsində avtomatik yenilənə, dəyişdirilə və ya silinə bilər. Xüsusilə operativ yaddaşda saxlanılan məlumatlar, aktiv proseslər və müvəqqəti fayllar volatil xarakter daşıdığından onların qısa müddət ərzində itirilməsi mümkündür [14]. Bu səbəbdən rəqəmsal kriminalistika prosesində sübut əhəmiyyətinə malik məlumatların vaxtında əldə olunması xüsusi əhəmiyyət kəsb edir.

Müasir kibermühitdə rəqəmsal izlərin yaranma mənbələri yalnız fərdi kompüter sistemləri ilə məhdudlaşmır. Bulud hesablama platformaları, mobil cihazlar, IoT (Internet of Things) infrastrukturları və virtual mühitlər də böyük həcmdə rəqəmsal izlər formalaşdırır. Bu isə rəqəmsal kriminalistika prosesində çoxmənbəli analiz yanaşmalarının və müxtəlif platformalar üzrə məlumat korrelyasiyasının tətbiqini zəruri edir [15, 16].

Rəqəmsal izlərin mühüm xüsusiyyətlərindən biri onların sonradan rəqəmsal sübuta çevrilmə potensialına malik olmasıdır. Lakin hər bir rəqəmsal iz hüquqi baxımdan avtomatik olaraq sübut hesab edilmir. Rəqəmsal məlumatın sübut statusu qazanması onun əldə olunma üsulu, bütövlüyünün qorunması, autentikliyi və etibarlılığının təmin edilməsi ilə birbaşa bağlıdır. Buna görə də rəqəmsal izlərin identifikasiyası və qorunması rəqəmsal kriminalistika prosesinin ilkin və ən mühüm mərhələlərindən biri hesab olunur [17].

B. *Rəqəmsal izlərin yaranma mənbələri*

Rəqəmsal izlərin formalaşması müxtəlif informasiya sistemləri və rəqəmsal platformalarda həyata keçirilən fəaliyyətlərin nəticəsi kimi meydana çıxır. Bu mənbələr sistemin arxitekturasından və istifadə sahəsindən asılı olaraq fərqlənir və hər biri kibercinayətlərin araşdırılması üçün spesifik informasiya daşıyıcısı rolunu oynayır. Rəqəmsal kriminalistika baxımından bu mənbələrin düzgün müəyyən edilməsi hadisənin rekonstruksiyası və sübutların əlaqələndirilməsi üçün əsas şərtlərdən biridir [5, 6].

Ənənəvi kompüter sistemləri rəqəmsal izlərin əsas yaranma mənbələrindən biri hesab olunur. Əməliyyat sistemləri səviyyəsində yaradılan loq faylları, istifadəçi profilləri, proses qeydləri, fayl sistemi dəyişiklikləri və reyestr məlumatları kibercinayətlərin təhlili zamanı mühüm rol oynayır. Bu tip məlumatlar sistemdə həyata keçirilən əməliyyatların zaman ardıcıllığını müəyyən etməyə və istifadəçi davranışını analiz etməyə imkan verir [14].

Şəbəkə infrastrukturu da rəqəmsal izlərin əsas mənbələrindən biridir. Yönləndirici və "firewall" loqları, paket analiz məlumatları, DNS sorğuları və trafik qeydləri şəbəkə səviyyəsində baş verən fəaliyyətləri əks etdirir. Bu məlumatlar hücumun istiqamətini, istifadə olunan protokolları və mümkün xarici əlaqələri müəyyən etmək üçün istifadə olunur. Xüsusilə paylanmış hücum ssenarilərində şəbəkə izləri kritik sübut mənbəyi hesab olunur [3].

Mobil cihazlar müasir dövrdə rəqəmsal izlərin ən zəngin mənbələrindən birinə çevrilmişdir. Smartfon və planşetlərdə saxlanılan mesajlaşma tətbiqləri, GPS məlumatları, zəng qeydləri, tətbiq istifadəsi statistikası və media faylları istifadəçi fəaliyyətinin detallı şəkildə rekonstruksiyasına imkan yaradır. Mobil platformalarda toplanan məlumatların dəyişkən və şifrələnmiş formatda olması onların təhlilini daha mürəkkəb edir [2].

Bulud hesablama mühitləri rəqəmsal izlərin paylanmış xarakter almasına səbəb olur. Virtual serverlər, SaaS xidmətləri, bulud saxlama sistemləri və platforma əsaslı xidmətlər (PaaS) istifadəçilərin fəaliyyətlərini müxtəlif coğrafi yerlərdə yerləşən serverlərdə saxlayır. Bu isə sübutların əldə olunması prosesində hüquqi əməkdaşlıq məsələlərini aktuallaşdırır [8].

Eyni zamanda IoT cihazları da rəqəmsal izlərin yeni və sürətlə genişlənən mənbələrindən biridir. Ağıllı ev sistemləri, sensorlar, sənaye avtomatlaşdırma qurğuları və geyilə bilən texnologiyalar davamlı olaraq məlumat toplayaraq şəbəkəyə ötürür. Bu məlumatlar həm istifadəçi davranışını, həm də fiziki mühitdə baş verən hadisələri rəqəmsal formada əks etdirir [2].

Beləliklə, rəqəmsal izlərin yaranma mənbələri çoxşaxəli xarakter daşıyır və bu müxtəliflik kibercinayətlərin araşdırılmasında kompleks və inteqrasiya olunmuş analiz yanaşmalarının tətbiqini tələb edir.

C. *Rəqəmsal izlərin təsnifatı*

Rəqəmsal izlərin effektiv təhlili və kriminalistik baxımdan düzgün qiymətləndirilməsi onların müəyyən meyarlar üzrə təsnifatını zəruri edir. Müxtəlif informasiya sistemlərində formalaşan rəqəmsal məlumatların struktur, saxlanma xüsusiyyətləri və funksional təyinat baxımından fərqlənməsi rəqəmsal kriminalistika prosesində sistemli yanaşmanın tətbiqini tələb edir [2]. Rəqəmsal izlərin təsnifatı sübutların identifikasiyası, prioritetləşdirilməsi və interpretasiyası baxımından mühüm əhəmiyyət kəsb edir.

Rəqəmsal izlər saxlanma xüsusiyyətlərinə görə volatil və qeyri-volatil olmaqla iki əsas qrupa ayrılır. Volatil məlumatlar operativ yaddaşda, aktiv proseslərdə və cari şəbəkə sessiyalarında saxlanılan, sistem söndürüldükdə və ya proses dayandırıldıqda itirilə bilən məlumatları əhatə edir. Aktiv şəbəkə bağlantıları, RAM məlumatları, aktiv proseslər və müvəqqəti sistem keşləri bu kateqoriyaya aid edilir [3]. Qeyri-volatil məlumatlar isə daimi yaddaş qurğularında saxlanılır və sistem söndürüldükdən sonra da mövcudluğunu qoruyur. Fayl sistemləri, loq faylları, verilənlər bazaları və arxiv faylları bu tip məlumatlara nümunə göstərilə bilər [5].

Funksional təyinatına görə rəqəmsal izlər identifikasiyaedici, kommunikasiya və fəaliyyət izləri kimi qruplaşdırılır. İdentifikasiyaedici izlər istifadəçinin və ya cihazın müəyyən edilməsinə imkan verən məlumatları əhatə edir. IP ünvanları, MAC ünvanları, istifadəçi hesabları və autentifikasiya qeydləri bu kateqoriyaya daxildir [3].

Kommunikasiya izləri elektron poçt yazışmaları, mesajlaşma tətbiqləri, VoIP əlaqələri və şəbəkə trafik məlumatları kimi informasiya mübadiləsini əks etdirən məlumatlardan ibarətdir. Fəaliyyət izləri isə istifadəçi və ya sistem tərəfindən həyata keçirilən əməliyyatların ardıcıllığını göstərən loqlar, proqram istifadəsi qeydləri və fayl əməliyyatlarını əhatə edir [6].

Rəqəmsal izlər yaranma mənbəyinə görə də təsnif edilə bilər. Bu baxımdan kompüter sistemləri, mobil qurğular, şəbəkə infrastrukturları, bulud platformaları və IoT cihazları üzrə formalaşan izlər fərqləndirilir. Hər bir mənbə özünəməxsus məlumat strukturu və saxlanma mexanizmi ilə xarakterizə olunur ki, bu da onların əldə olunması və təhlili metodlarına birbaşa təsir göstərir [2, 8].

Bundan başqa, rəqəmsal izlər strukturlaşdırılmış və strukturlaşdırılmamış məlumatlar formasında da mövcud ola bilər. Strukturlaşdırılmış məlumatlar verilənlər bazaları, sistem loqları və standartlaşdırılmış qeyd formatlarında saxlanılan məlumatları əhatə edir. Strukturlaşdırılmamış məlumatlar isə multimedia faylları, sənədlər, şəkillər və istifadəçi tərəfindən yaradılan digər məlumat növlərindən ibarətdir. Müasir kibermühitdə strukturlaşdırılmamış məlumatların həcminin sürətlə artması onların avtomatlaşdırılmış analiz metodlarına olan ehtiyacı artırır [7, 12].

Rəqəmsal izlərin təsnifatı kriminalistik analiz prosesində məlumatların prioritetləşdirilməsi və hadisənin rekonstruksiyası baxımından mühüm rol oynayır. Müxtəlif mənbələrdən əldə olunan izlərin qarşılıqlı əlaqələndirilməsi kibercinayətlərin daha dəqiq təhlilinə və sübut bazasının formalaşdırılmasına imkan yaradır [15].

IV. RƏQƏMSAL İZLƏRİN ƏLDƏ OLUNMASI VƏ TƏHLİLİ

Kibercinayətlərin araşdırılması prosesində rəqəmsal sübutlar hadisənin texniki və hüquqi baxımdan qiymətləndirilməsində mühüm əhəmiyyət kəsb edir. Müxtəlif informasiya sistemləri, kompüter qurğuları, mobil cihazlar və şəbəkə infrastrukturlarında formalaşan məlumatlar hüquqpozmanın başvermə mexanizminin müəyyənləşdirilməsi və iştirakçıların identifikasiyası baxımından əsas informasiya mənbələrindən biri hesab olunur [5].

Rəqəmsal sübutların yüksək dəyişkənliyə malik olması onların əldə olunması, qorunması və təhlili prosesində xüsusi metodoloji yanaşmaların tətbiqini zəruri edir. Bu baxımdan beynəlxalq standartlara uyğun prosedurların tətbiqi, sübutların bütövlüyünün qorunması və kriminalistik analiz metodlarının düzgün həyata keçirilməsi rəqəmsal kriminalistika prosesinin əsas tələblərindən hesab olunur [17, 19].

A. *Rəqəmsal sübut anlayışı*

Rəqəmsal kriminalistika sahəsində rəqəmsal sübut dedikdə istintaq və ya məhkəmə prosesində hüquqi əhəmiyyət daşıyan, müəyyən prosedurlar əsasında əldə edilən və etibarlılığı təsdiq olunan elektron məlumatlar nəzərdə tutulur. Bu anlayış yalnız məlumatın texniki mövcudluğunu deyil, həm də onun hüquqi baxımdan qəbul edilə bilməsini əhatə edir [17, 19].

Rəqəmsal sübutların əsas xüsusiyyəti onların müəyyən standartlara uyğun olaraq əldə olunması və emal edilməsidir. Bu prosesdə məlumatın dəyişdirilmədən saxlanılması, autentikliyinin qorunması və sonradan yoxlanıla bilməsi əsas tələblər kimi çıxış edir. Bu səbəbdən rəqəmsal sübutlar sadəcə sistemdə mövcud olan məlumat deyil, prosessual baxımdan təsdiqlənmiş informasiya kimi qiymətləndirilir [19].

Rəqəmsal sübutlar müxtəlif mənbələrdən əldə oluna bilər, o cümlədən əməliyyat sistemi jurnalları, şəbəkə qeydləri, elektron yazışmalar, mobil cihaz artefaktları və bulud platformalarında saxlanılan məlumatlar. Lakin bu məlumatların hamısı avtomatik olaraq sübut statusu daşımır və onların hüquqi dəyəri yalnız ekspertiza və kriminalistik analiz nəticəsində müəyyən edilir [20].

Rəqəmsal sübut anlayışı rəqəmsal iz anlayışından fərqli olaraq daha dar və formal çərçivəyə malikdir. Əgər rəqəmsal izlər sistemdə baş verən fəaliyyətin texniki nəticəsi kimi formalaşırsa, rəqəmsal sübut həmin izlərin hüquqi və kriminalistik baxımdan təsdiqlənmiş formasıdır. Bu fərq rəqəmsal kriminalistika prosesində izlərin sübuta çevrilməsi mərhələsinin əsas elmi əsasını təşkil edir [5].

Rəqəmsal sübutların etibarlılığı onların bütövlüyünün qorunması ilə birbaşa bağlıdır. Bu məqsədlə heş funksiyalarının tətbiqi, kriminalistik surətlərin yaradılması və sübutların qorunması zənciri prosedurlarının icrası geniş istifadə olunur. Bu yanaşmalar sübutun dəyişdirilmədiyini və orijinal mənbə ilə uyğunluğunu təsdiq etməyə imkan verir [17].

B. *Rəqəmsal izlərin rəqəmsal sübutlara transformasiyası*

Rəqəmsal kriminalistika prosesində rəqəmsal izlərin rəqəmsal sübuta çevrilməsi mərhələsi texniki məlumatın hüquqi və prosessual dəyər qazanmasını təmin edən əsas mərhələlərdən biridir. Bu proses avtomatik xarakter daşımır və yalnız müəyyən metodoloji yanaşmalar və standartlaşdırılmış prosedurlar əsasında həyata keçirilir [17].

Transformasiya prosesi çərçivəsində ilkin mərhələdə müxtəlif mənbələrdən toplanmış rəqəmsal izlər sistemləşdirilir, strukturlaşdırılır və hadisə kontekstinə uyğun şəkildə əlaqələndirilir. Daha sonra bu məlumatlar üzərində bütövlük və autentiklik yoxlamaları aparılır, mümkün dəyişdirilmə və ya müdaxilə riskləri qiymətləndirilir [20].

Rəqəmsal izlərin sübuta çevrilməsi prosesində əsas məqsəd onların etibarlılığının və dəyişdirilməmiş formada saxlanılmasının təmin edilməsidir. Bu məqsədlə heş yoxlamaları, kriminalistik nüsxələnmə (forensic imaging) və sübutların qorunma zənciri (chain of custody) mexanizmləri tətbiq olunur. Bu yanaşmalar sübutun ilkin mənbəyə uyğunluğunu təsdiq etməyə imkan yaradır [17].

Eyni zamanda transformasiya mərhələsində çoxmənbəli analiz yanaşması mühüm rol oynayır. Müxtəlif sistemlərdən əldə olunan loqlar, şəbəkə qeydləri və artefaktlar arasında korrelyasiya qurularaq hadisənin daha dəqiq rekonstruksiyası həyata keçirilir [6]. Bu yanaşma yanlış interpretasiya risklərini azaldır və nəticələrin etibarlılığını artırır.

Beləliklə, rəqəmsal izlərin sübuta çevrilməsi prosesi texniki məlumatın hüquqi status qazanmasını təmin edən əsas mərhələlərdən biri hesab olunur və rəqəmsal kriminalistika prosesinin əsas sütunlarından biri hesab olunur. Bu mərhələlər Şəkil 1-də göstərilmişdir.

Şəkil 1. Rəqəmsal izlərin rəqəmsal sübuta transformasiya prosesi.

C. *Rəqəmsal sübutların əldə olunma mərhələləri*

Rəqəmsal sübutların əldə olunması kibercinayətlərin istintaqında yalnız texniki prosedur deyil, həm də ciddi metodoloji və hüquqi çərçivəyə malik bir prosesdir. Bu prosesin əsas məqsədi rəqəmsal mühitdə mövcud olan məlumatların dəyişdirilmədən, bütövlüyü qorunmaqla əldə olunması və onların sonradan məhkəmə prosesində etibarlı sübut kimi istifadə edilə bilməsidir. Beynəlxalq təcrübədə bu yanaşma NIST və ISO standartlarına əsaslanır və mərhələli icra modeli ilə xarakterizə olunur [6].

Rəqəmsal sübutların əldə olunması prosesi bir-biri ilə əlaqəli mərhələlər zənciri kimi qəbul edilir və bu mərhələlər arasında sərt sərhəd yoxdur, əksinə, onlar praktikada paralel və ardıcıl şəkildə icra oluna bilər. Bu yanaşma real kibermühitdə baş verən hadisələrin dinamik təbiətindən irəli gəlir və sübutların itirilmə riskini minimuma endirməyə xidmət edir [4].

İlk mərhələ olan identifikasiya zamanı hadisə ilə əlaqəli ola biləcək bütün rəqəmsal mənbələr müəyyən edilir. Bu mərhələdə sistemlər, şəbəkə qurğuları, mobil cihazlar və bulud xidmətləri kimi müxtəlif mənbələrdə potensial sübut izləri aşkar edilir. Bu mərhələnin düzgün icrası sonrakı analizin keyfiyyətini birbaşa müəyyən edir [1].

Bundan sonrakı qorunma mərhələsində məqsəd mövcud rəqəmsal vəziyyətin stabil saxlanılmasıdır. Sistemə əlavə müdaxilələrin qarşısı alınır, aktiv proseslər mümkün qədər dəyişdirilmir və volatil məlumatların itirilməməsi üçün operativ tədbirlər görülür. Bu mərhələ sübutların "yaşayan sistemdən" qorunaraq çıxarılmasını təmin edir [3].

Toplanma mərhələsi isə artıq konkret sübutların kriminalistik tələblərə uyğun şəkildə əldə olunmasını əhatə edir. Bu zaman orijinal məlumatlara birbaşa müdaxilə edilmədən onların bit səviyyəsində dəqiq surətləri yaradılır. Beləliklə, analiz prosesi orijinal dəlillərə zərər vermədən həyata keçirilə bilir [17].

Əldə olunmuş məlumatlar daha sonra ekspertiza və analiz mərhələsində dərin təhlil edilir. Burada məqsəd təkcə məlumatı oxumaq deyil, həm də müxtəlif mənbələrdən gələn rəqəmsal izlər arasında əlaqə quraraq hadisənin başvermə ardıcıllığını bərpa etməkdir. Loqlar, şəbəkə qeydləri və sistem artefaktları birlikdə qiymətləndirilərək kibercinayətin icra mexanizmi rekonstruksiya olunur [6].

Son mərhələdə isə nəticələr strukturlaşdırılmış şəkildə təqdim edilir. Bu mərhələdə əldə olunan texniki nəticələr hüquqi baxımdan anlaşılacaq formaya salınır və sübutların qorunma zənciri prinsipləri əsasında sənədləşdirilir. Bu, sübutların məhkəmə prosesində qəbul olunmasının əsas şərtlərindən biridir [20].

D. *Rəqəmsal sübutların təhlili və təqdim olunması*

Rəqəmsal sübutların təhlili kibercinayətlərin araşdırılmasında ən kritik mərhələlərdən biridir və bu mərhələdə toplanmış məlumatlar hadisənin mahiyyətini və başvermə mexanizmini aşkar etmək üçün sistemli şəkildə qiymətləndirilir. Bu proses yalnız texniki analiz deyil, həm də kriminalistik interpretasiya tələb edən kompleks fəaliyyətdir. Təhlilin əsas məqsədi müxtəlif mənbələrdən əldə olunan rəqəmsal izlər arasında əlaqə quraraq hadisənin tam rekonstruksiyasını təmin etməkdir [6].

Təhlil mərhələsində əsas diqqət loq faylları, şəbəkə trafik məlumatları, sistem artefaktları, istifadəçi fəaliyyəti qeydləri və tətbiq səviyyəli məlumatlar üzərində cəmlənir. Bu məlumatlar bir-biri ilə müqayisə edilərək zaman ardıcıllığı müəyyən edilir və mümkün hücum ssenarisi formalaşdırılır. Xüsusilə korrelyasiya analizi müxtəlif mənbələrdən gələn məlumatların uyğunluğunu yoxlamağa və anomal davranışların aşkarlanmasına imkan yaradır [15].

Müasir kibermühitdə böyük həcmli və heterogen məlumatların təhlili avtomatlaşdırılmış analitik yanaşmaların tətbiqini zəruri edir. Süni intellekt əsaslı analiz metodları, davranış analitikası və anomaliya aşkarlama alqoritmləri rəqəmsal sübutların daha effektiv qiymətləndirilməsinə şərait yaradır. Bununla yanaşı, ekspert tərəfindən aparılan əl ilə aparılan analiz hələ də nəticələrin doğrulanmasında mühüm rol oynayır [7].

Təhlil prosesinin mühüm nəticələrindən biri hadisənin rekonstruksiyasıdır. Bu mərhələdə kibercinayətin necə həyata keçirildiyi, hansı sistemlərin hədəf alındığı və hücum zəncirinin hansı mərhələlərdən ibarət olduğu müəyyən edilir. Bu yanaşma hücum zənciri (attack chain) konsepsiyasına uyğun şəkildə həyata keçirilə bilər [5, 18].

Son mərhələ olan təqdimetmə isə əldə olunan nəticələrin hüquqi və texniki baxımdan strukturlaşdırılmış formada ifadə olunmasını əhatə edir. Bu mərhələdə hazırlanmış hesabatlar aydın, ardıcıl və yoxlanıla bilən formada təqdim edilməlidir. Sübutların qorunma zənciri prinsipi burada da mühüm rol oynayır və sübutların istintaqdan məhkəməyə qədər olan bütün hərəkət trayektoriyasını sənədləşdirir [17].

Beləliklə, rəqəmsal sübutların təhlili və təqdim olunması mərhələsi yalnız texniki analiz deyil, həm də hüquqi qərarvermə prosesini dəstəkləyən əsas elmi-praktik mərhələ kimi çıxış edir.

V. MÜASİR ÇAĞIRIŞLAR

Rəqəmsal kriminalistika sahəsində texnologiyaların sürətli inkişafı kibercinayətlərin araşdırılması prosesində yeni problemlərin və çağırışların yaranmasına səbəb olmuşdur. Müasir kibermühitdə istifadə olunan bulud texnologiyaları, anonimləşdirmə mexanizmləri, şifrələmə vasitələri və paylanmış infrastruktur modelləri rəqəmsal sübutların əldə olunması və təhlili prosesini daha mürəkkəb hala gətirmişdir [15, 16].

Əsas problemlərdən biri məlumatların böyük həcmdə və müxtəlif formatlarda formalaşmasıdır. Müasir informasiya sistemlərində gündəlik olaraq yaranan loq məlumatları, şəbəkə trafiki və istifadəçi fəaliyyətləri rəqəmsal kriminalistika

prosesində böyük həcmli məlumatların emalı problemini aktuallaşdırır. Bu vəziyyət ənənəvi əl ilə aparılan analiz metodlarının effektivliyini azaldır və avtomatlaşdırılmış analiz yanaşmalarının tətbiqini zəruri edir [18].

Bulud texnologiyalarının geniş yayılması rəqəmsal sübutların lokal sistemlərdən kənarda saxlanılmasına gətirib çıxarmışdır. Bulud mühitlərində məlumatların müxtəlif ölkələrdə yerləşən serverlərdə saxlanılması, multi-tenant infrastrukturlar və xidmət provayderindən asılılıq rəqəmsal sübutların əldə olunması və hüquqi baxımdan identifikasiyası prosesində ciddi çətinliklər yaradır [2]. Bundan əlavə, məlumatların dinamik şəkildə dəyişməsi və qısa müddətli saxlanılması bəzi rəqəmsal izlərin itirilməsi riskini artırır.

Müasir kibercinayətkarlar tərəfindən istifadə olunan şifrələmə və anonimləşdirmə texnologiyaları da istintaq prosesini çətinləşdirən əsas amillərdəndir. VPN xidmətləri, TOR infrastrukturu, kriptovalyuta əsaslı ödəniş mexanizmləri və "end-to-end" şifrələmə sistemləri hücum mənbələrinin müəyyən edilməsini və rəqəmsal fəaliyyətlərin izlənilməsini mürəkkəbləşdirir [10, 15]. Xüsusilə "ransomware" və təşkilatlanmış kibercinayət qrupları (APT) tərəfindən anonim kommunikasiya kanallarının istifadəsi rəqəmsal sübutların identifikasiyasına birbaşa təsir göstərir.

IoT və kiber-fiziki sistemlərin geniş tətbiqi rəqəmsal kriminalistika üçün yeni sübut mənbələri formalaşdırmışdır. Sensorlar, ağıllı qurğular və sənaye idarəetmə sistemlərində yaranan məlumatlar istintaq üçün əhəmiyyətli olsa da, bu cihazlarda standartlaşdırılmış log mexanizmlərinin olmaması və məhdud yaddaş resursları sübutların əldə olunmasını çətinləşdirir [8].

Digər mühüm problemlərdən biri anti-kriminalistik metodların tətbiqidir. Kibercinayətkarlar tərəfindən loqların silinməsi, məlumatların manipulyasiyası, steqanoqrafiya və faylsız (fileless) hücum texnikalarının istifadəsi rəqəmsal izlərin aşkarlanmasını və təhlilini mürəkkəbləşdirir [7, 12]. Bu yanaşmalar xüsusilə operativ yaddaşda fəaliyyət göstərən zərərli proqram təminatlarında daha geniş müşahidə olunur.

Müasir şəraitdə rəqəmsal kriminalistika prosesində süni intellekt əsaslı yanaşmaların tətbiqi perspektiv istiqamətlərdən biri hesab olunur. Maşın öyrənməsi və davranış analitikası metodları böyük həcmli məlumatların avtomatik emalına və anomal fəaliyyətlərin aşkarlanmasına imkan yaradır. Bununla belə, bu sistemlərin şəffaflığı, nəticələrin interpretasiyası və yanlış pozitiv halların qarşısının alınması hələ də aktual problemlərdən biri olaraq qalır.

Beləliklə, rəqəmsal kriminalistika sahəsində yaranan müasir çağırışlar yalnız texniki deyil, həm də hüquqi və metodoloji xarakter daşıyır. Bu səbəbdən rəqəmsal sübutlarla işləmə prosesində beynəlxalq standartların, avtomatlaşdırılmış analiz metodlarının və kompleks kriminalistik yanaşmaların tətbiqi xüsusi əhəmiyyət kəsb edir.

NƏTİCƏ

Müasir kibermühitdə kibercinayətkarlıq əməllərinin mürəkkəbləşməsi rəqəmsal kriminalistika və rəqəmsal sübutlarla işləmə prosesinin əhəmiyyətini daha da artırmışdır. İnformasiya sistemləri, mobil qurğular, bulud platformaları və şəbəkə infrastrukturlarında formalaşan rəqəmsal izlər kibercinayətlərin araşdırılması zamanı əsas informasiya mənbələrindən biri kimi çıxış edir.

Məqalədə rəqəmsal izlərin formalaşma xüsusiyyətləri, əsas mənbələri və təsnifatı təhlil edilmiş, rəqəmsal izlərin hüquqi və kriminalistik baxımdan rəqəmsal sübuta çevrilməsi prosesi araşdırılmışdır. Eyni zamanda rəqəmsal sübutların əldə olunması, qorunması, təhlili və təqdim olunması mərhələləri beynəlxalq standartlar əsasında sistemləşdirilmişdir.

Araşdırma nəticəsində müəyyən edilmişdir ki, rəqəmsal sübutların etibarlılığı onların bütövlüyünün qorunması, autentikliyinin təmin edilməsi və standartlaşdırılmış prosedurlar əsasında emal olunmasından birbaşa asılıdır. Müasir kibermühitdə bulud texnologiyaları, IoT infrastrukturları, anonimləşdirmə mexanizmləri və anti-kriminalistik yanaşmalar rəqəmsal kriminalistika prosesində yeni çağırışlar formalaşdırır və ənənəvi istintaq metodlarının təkmilləşdirilməsini zəruri edir.

Bununla yanaşı, süni intellekt və avtomatlaşdırılmış analiz metodlarının tətbiqi böyük həcmli rəqəmsal məlumatların daha effektiv emalına və kibercinayətlərin daha operativ araşdırılmasına imkan yaradır. Bu istiqamətdə beynəlxalq standartlara uyğun metodoloji yanaşmaların və müasir texnoloji həllərin tətbiqi rəqəmsal kriminalistikanın gələcək inkişaf istiqamətlərindən biri hesab oluna bilər.

ƏDƏBİYYAT

[1] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024. The Hague, Netherlands: European Union Agency for Law Enforcement Cooperation, 2024.

[2] [Verizon, 2024 Data Breach Investigations Report (DBIR). New York, NY, USA: Verizon Enterprise, 2024.

[3] ISO/IEC 27041:2015, Information Technology — Security Techniques — Guidance on Assuring Suitability and Adequacy of Incident Investigative Methods. Geneva, Switzerland: International Organization for Standardization, 2015.

[4] J. R. Lyle, B. Guttman, J. Butler, K. Sauerwein, C. Reed and C. Lloyd, Digital Investigation Techniques: A NIST Scientific Foundation Review, NISTIR 8354. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022.

[5] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed. Waltham, MA, USA: Academic Press, 2011.

[6] B. Carrier, File System Forensic Analysis. Boston, MA, USA: Addison-Wesley Professional, 2005.

[7] M. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix," Future Generation Computer Systems, vol. 78, pp. 558–567, Jan. 2018.

[8] ENISA, Threat Landscape 2024. Heraklion, Greece: European Union Agency for Cybersecurity, 2024.

[9] R. McKemmish, "What is Forensic Computing?," Australian Institute of Criminology Trends & Issues in Crime and Criminal Justice, no. 118, pp. 1–6, 1999.

[10] K.-K. R. Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions," Computers & Security, vol. 30, no. 8, pp. 719–731, Nov. 2011.

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

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

[13] N. Beebe and J. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," Digital Investigation, vol. 2, no. 2, pp. 147–167, Jun. 2005.

[14] K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2006.

[15] A. Pichan, M. Lazarescu and S. T. Soh, "Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis," Digital Investigation, vol. 13, pp. 38–57, Jun. 2015.

[16] M. Scanlon and J. Kechadi, "Toward a Digital Forensic Intelligence Model for Cloud Computing," Journal of Digital Forensics, Security and Law, vol. 5, no. 1, pp. 69–80, 2010.

[17] ISO/IEC 27042:2015, Information Technology — Security Techniques — Guidelines for the Analysis and Interpretation of Digital Evidence. Geneva, Switzerland: International Organization for Standardization, 2015.

[18] MITRE Corporation, MITRE ATT&CK Framework. Bedford, MA, USA: MITRE, 2024.

[19] ISO/IEC 27037:2012, Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva, Switzerland: International Organization for Standardization, 2012.

[20] B. Guttman, D. R. White, S. Williams and T. Walraven, Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022.

Cybercrime Activities: Digital Traces and Evidence

Sanan Valizada
Institute of Information Technology, Baku, Azerbaijan
senanvalizade@gmail.com

Abstract- The article analyzes the modern characteristics of cybercrime activities and the role of digital traces in their investigation. The main types of digital traces generated within various information systems, computers, mobile devices, and network environments are systematized, and the conditions for their use as evidence are identified. The study also examines the acquisition, preservation, integrity assurance, and analysis of digital evidence. Furthermore, the impact of modern challenges such as encryption, anonymization technologies, cloud environments, and large-scale data processing on the investigation process is comprehensively reviewed.

Keywords- digital forensics; digital evidence; digital artifacts; digital traces.