Proqram Sistemlərində Kiberinsidentlərin Rəqəmsal Kriminalistikası və Ekspertizası

Şəfəqət Mahmudova
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shafagat@gmail.com

***Xülasə*— Proqram sistemlərində kiberinsidentlərin rəqəmsal kriminalistikası hücum vaxtlarını yenidən qurmaq, təhdid aktorlarını və əsas səbəblərini müəyyən etmək üçün tətbiqlərdən, qeydlərdən və loq fayllardan rəqəmsal sübutların müəyyən edilməsini, əldə edilməsini, qorunmasını və təhlilini əhatə edir. Məqalədə proqram sistemlərində kiberinsidentlərin rəqəmsal kriminalistikası, onun növləri və aspektləri, bu sahədə görülmüş işlər, rəqəmsal ekspertizanın məqsədi və mərhələləri, istifadə olunan metodlar tədqiq edilmişdir. Aparılan tədqiqat nəticəsində proqram sistemlərində kiberinsidentlərin rəqəmsal ekspertizası sahəsində əsas problemlər müəyyənləşdirilmişdir.**

Açar sözlər*— *proqram sistemləri; kiberinsident; rəqəmsal ekspertiza; rəqəmsal kriminalistika zərərli fəaliyyət.

I. GİRİŞ

Proqram sistemlərində kiberinsidentlərin rəqəmsal kriminalistikası hücum vaxtlarını yenidən qurmaq, təhdid aktyorlarını və əsas səbəblərini müəyyən etmək üçün tətbiqlərdən, qeydlərdən və fayllardan rəqəmsal sübutların sistematik şəkildə müəyyən və əldə edilməsini, qorunmasını və təhlilini əhatə edir. Bu sahə beynəlxalq terminologiyada Rəqəmsal Kriminalistika (Digital Forensics) və ya Kiber Kriminalistika (Cyber Forensics) kimi tanınır.

Rəqəmsal kriminalistika kompüterlər, mobil telefonlar və bulud sistemləri kimi cihazlardan rəqəmsal sübutların müəyyən edilməsi, qorunması, təhlili və təqdim edilməsinin elmi, strukturlaşdırılmış prosesidir. Əsasən hüquqi və ya daxili araşdırmalar üçün istifadə edilən kriminalistika elminin bu sahəsi məhkəmədə sübutların qəbul edilməsi üçün məlumatların bütövlüyünü təmin edir.

Rəqəmsal kriminalistika müasir informasiya cəmiyyətində kibercinayətlərin araşdırılması və rəqəmsal sübutların hüquqi baxımdan etibarlı şəkildə əldə olunması üçün mühüm əhəmiyyət kəsb edir. Rəqəmsal kriminalistika proseslərinin inkişafı müstəntiqlərə və hüquq-mühafizə orqanlarına məhkəmədə qəbul edilə biləcək potensial cinayətlərə qarşı sübutlar toplamaq üçün strukturlaşdırılmış vasitələr təqdim edir.

Rəqəmsal kriminalistika istənilən növ rəqəmsal cihazdan zərərli fəaliyyətin araşdırılması və sonrakı təhlil və ya hesabat üçün dəlillərin toplanması təcrübəsidir. Bu sahə yüksək ixtisaslaşmış bilik və metodologiyalara əsaslanan fəaliyyət istiqamətidir, lakin kibercinayətkarlığın artması və rəqəmsal texnologiyanın həyatımızda getdikcə daha geniş tətbiq olunması ilə bu, istənilən təşkilat üçün vacib bir funksiyadır.

II. RƏQƏMSAL KRİMİNALİSTİKANIN MÜXTƏLİF NÖVLƏRİ

Bildiyimiz kimi rəqəmsal kriminalistikanın müxtəlif növləri mövcuddur (Şəkil 1).

Şəkil 1. Rəqəmsal kriminalistikanın müxtəlif növləri

Tədqiq olunan cihazın və ya sistemin növündən asılı olaraq dəyişən bir neçə fərqli rəqəmsal kriminalistika növü mövcuddur:

Kompüter kriminalistikası. Bu, ən çox yayılmış rəqəmsal kriminalistika növüdür və tez-tez daha geniş terminin özü ilə qarışdırılır. Bu kriminalistika kompüter elmlərinin kompüterlərə daha dərindən nüfuz etmək və dəlil tapmaq səylərini birləşdirir.

Mobil kriminalistika. Smartfonlar və planşetlər gündəlik həyatda getdikcə populyarlaşdıqca, xüsusən də kontaktlar, fotolar, videolar və digər şəxsi məlumatlar ehtiva edə bildikləri üçün mobil cihazlarda dəlil tapmaq getdikcə daha vacib hala gəlir.

Verilənlər Bazası Kriminalistikası. Çox miqdarda məlumat ehtiva edə bilən verilənlər bazaları ilə məlumat sızmaları və ya digər növ məlumat itkisi sübutlarını axtaran istintaq qrupları üçün faydalı hədəf ola bilər.

Yaddaş Kriminalistikası. Hər bir cihazın təsadüfi giriş yaddaşı (RAM), xüsusən də nisbətən yaxınlarda baş verdiyi güman edilirsə, zərərli fəaliyyəti göstərə bilər.

Şəbəkə Kriminalistikası. Şəbəkə trafiki və veb-saytlar cinayətkarı tapmağa çalışan istintaq qrupları üçün ümumi hədəfdir.

Fayl Sisteminin Kriminalistikası. İstənilən növ son nöqtə cihazlarında saxlanılan bütün fayl və qovluqlar, noutbuk kimi son istifadəçi cihazlarından tutmuş məlumat mərkəzlərindəki

DOI: 10.25045/forensic.gov.2026.27

böyük serverlərə qədər rəqəmsal kriminalistika qrupları üçün standart araşdırma sahəsidir [1].

Rəqəmsal kriminalistika, rəqəmsal sübutların təhlilini əhatə edən hüquqi məqsədlər üçün kompüter elmləri və istintaq prosedurlarının tətbiqidir. Bu sahə müxtəlif rəqəmsal mənbələrdən əldə edilən rəqəmsal sübutların müəyyənləşdirilməsini, qorunmasını, təhlilini və təqdimatını əhatə edir [2].

*Rəqəmsal Kriminalistikanın Əsas Aspektlər*i:

- Proses: Toplama, araşdırma, təhlil və hesabat verməni əhatə edir, tez-tez rəqəmsal kriminalistika və hadisələrə cavab (Digital Forensics and Incident Response, DFIR) adlanır;
- Sübut mənbələri: Kompüterlər, mobil cihazlar, serverlər, Əşyaların İnterneti cihazları və buludlar;
- Texnika: Silinmiş faylları bərpa etmək, gizli faylları araşdırmaq, meta məlumatları təhlil etmək və şifrələnmiş məlumatların kilidini açmaq;
- Məqsəd: Nə baş verdiyini, sistemin necə pozulduğunu anlamaq və məlumatların bütövlüyünü qoruyarkən hadisələrin gedişini yenidən qurmaq;
- Tətbiqlər: Məlumatların pozulmasına qarşı insidentlərə cavab olaraq cinayət araşdırmalarında, mülki məhkəmə işlərində və korporativ kibertəhlükəsizlikdə istifadə olunur;
- Rəqəmsal kriminalistika tez-tez reaktiv (cinayətdən sonrakı araşdırma) hesab olunur, ümumi kibertəhlükəsizlik isə proaktiv (hücumların qarşısının alınması) hesab olunur.

III. ƏLAQƏLİ İŞLƏR

1. Rəqəmsal kriminalistika, məhkəmədə bütövlüyünü və qəbuledilənliyini qoruyub saxlayan şəkildə rəqəmsal sübutların toplanması və təhlili prosesidir.

Rəqəmsal kriminalistika kriminalistika elminin bir sahəsidir. Kibercinayətləri araşdırmaq üçün istifadə olunur, eyni zamanda cinayət və mülki araşdırmalara da kömək edə bilər. Kibertəhlükəsizlik qrupları zərərli proqram hücumunun arxasında duran kibercinayətkarları müəyyən etmək üçün rəqəmsal kriminalistikadan istifadə edə bilər, hüquq-mühafizə orqanları isə qətl şübhəlisini cihazlarından məlumatları təhlil etmək üçün istifadə edə bilərlər.

Rəqəmsal kriminalistikanın geniş tətbiqləri var, çünki o, rəqəmsal sübutlara hər hansı digər sübut forması kimi yanaşır. Rəsmilər cinayət yerindən fiziki sübutlar toplamaq üçün xüsusi prosedurlara əməl edirlər. Eynilə, rəqəmsal kriminalistika müstəntiqləri düzgün işləməyi və müdaxilədən qorunmanı təmin etmək üçün ciddi kriminalistika prosesinə riayət edirlər.

Rəqəmsal kriminalistika və kompüter kriminalistikası tez-tez bir-birini əvəz edir. Lakin, rəqəmsal kriminalistika texniki olaraq istənilən rəqəmsal cihazdan sübutların toplanmasını əhatə edir, kompüter kriminalistikası isə xüsusilə kompüterlər, planşetlər, mobil telefonlar və s. hesablama cihazlarından sübutların toplanmasını əhatə edir.

Rəqəmsal kriminalistika və insidentlərə cavab kibertəhlükəsizlik əməliyyatlarını təkmilləşdirmək üçün kompüter kriminalistikası və insidentlərə cavab fəaliyyətlərini birləşdirən inkişaf etməkdə olan kibertəhlükəsizlik sahəsidir. Bu sahə kibertəhdidlərin aradan qaldırılmasını sürətləndirməyə kömək edir və eyni zamanda əlaqəli rəqəmsal sübutların pozulmamasını təmin edir [3].

2. Rəqəmsal kriminalistika və intellektual məlumatların konvergensiyası kibertəhqiqatlar sahəsində transformativ bir paradiqma təqdim edir, inkişaf etmiş imkanlar vəd edir, eyni zamanda mürəkkəb texniki çətinliklər yaradır. Bu tədqiqat rəqəmsal kriminalistika və kəşfiyyat inteqrasiyası mənzərəsini formalaşdıran beş əsas problemi araşdırır. Birincisi, şifrələmə texnologiyalarının geniş yayılması müstəntiqlərin təhlükəsiz şəkildə saxlanılan və ya ötürülən məlumatlara çıxışına mane olan maneə kimi çıxış edir. Məlumat həcminin eksponensial artımı və rəqəmsal cihazların müxtəlifliyi təhlil və sübutların çıxarılmasının mürəkkəbliyini artırır və innovativ həllər tələb edir. Cinayətkarlar tərəfindən tətbiq edilən anti-kriminalistika üsulları araşdırmaları daha da çətinləşdirir, rəqəmsal sübutların manipulyasiyasına və qarışdırılmasına qarşı adaptiv strategiyalar tələb edir. Kibercinayətlərin transmilli təbiəti səbəbindən hüquqi çətinliklər ortaya çıxır və rəqəmsal sübutların düzgün əldə edilməsinə və paylaşılmasına mane olur. Bundan əlavə, texnologiyanın sürətli inkişafı müstəntiqlərin aparat, proqram təminatı və kommunikasiya texnologiyaları sahəsindəki davamlı dəyişikliklər şəraitində, xüsusən də sübutların süni şəkildə yaradılması və ya manipulyasiyası ilə qarşılaşdıqda, peşəkar bacarıqların və texniki imkanların mütəmadi yenilənməsinin vacibliyini ön plana çıxarır. Bu çətinlikləri hərtərəfli şəkildə həll etməklə, bu tədqiqat rəqəmsal kriminalistika və intellektual məlumatlar arasındakı dinamik qarşılıqlı əlaqənin daha dərindən başa düşülməsini təşviq etməyi və kibertəhlükəsizlik və rəqəmsal ədalətin təmin edilməsində gələcək irəliləyişlər və əməkdaşlıqlar üçün təməl yaratmağı hədəfləyir [4].

3. Rəqəmsal kriminalistika sürətlə inkişaf edən bir sahədir və blokçeyn, kriptovalyuta və "qara veb" – İnternetin gizli hissəsi (Dark Web) daxil olmaqla müxtəlif sahələrdə kibercinayətkarlıq, məlumat sızmaları və qanunsuz fəaliyyətlərin araşdırılmasında mühüm rol oynayır. Bu məqalədə kompüter kriminalistikası, mobil kriminalistika, şəbəkə kriminalistikası, bulud kriminalistikası, Əşyaların İnterneti kriminalistikası və inteqrasiya olunmuş sistem kriminalistikası da daxil olmaqla rəqəmsal kriminalistikanın əsas sahələri araşdırılır. Dron və peyk kriminalistikası kimi inkişaf etməkdə olan tendensiyalar kriminalistika araşdırmalarının ənənəvi hesablama mühitlərindən kənarda artan əhatə dairəsini vurğulayır. Bundan əlavə, tədqiqat, çirkli pulların yuyulması, ransomware ödənişləri və "qaranlıq veb"-də qanunsuz ticarətlə mübarizə aparmaq üçün kriptovalyuta əməliyyatlarının izlənməsinə yönəlmiş blokçeyn kriminalistikasına da toxunur.

Proqram şantajçıları (Ransomware) qurbanın məlumatlarını şifrələyən və ya cihazlarından çıxaran, girişi bərpa etmək üçün kriptovalyuta ödənişi tələb edən bir növ zərərli proqramdır. Bu, tez-tez fişinq e-poçtları, zərərli linklər və ya pozulmuş veb-saytlar vasitəsilə yayılır. Müasir hücumlara tez-tez məlumatların həm şifrələndiyi, həm də oğurlandığı "ikiqat şantaj" daxildir və fidyə (girov pulu) ödənilmədiyi təqdirdə məlumatların

sızdırılması ilə hədələnir.

Rəqəmsal sübutları effektiv şəkildə izləmək üçün kriminalistika metodologiyalarında zəncirvari analiz (Chainalysis), dünyanın ən çox istifadə edilən kiber araşdırma platforması (Maltego) və açıq mənbəli intellektual avtomatlaşdırma vasitəsi (SpiderFoot) kimi qabaqcıl alətlərdən istifadə olunur. Məqalədə həmçinin kibercinayətkarlar tərəfindən istifadə edilən şifrələmə, məlumatların dəyişkənliyi, yurisdiksiya maneələri və anti-kriminalistika üsulları kimi çətinliklər də müzakirə olunur. Ümumi Məlumatların Qorunması Qaydaları (General Data Protection Regulation,GDPR), Tibbi Sığorta Daşınabilirliyi və Hesabatlılığı (Health Insurance Portability and Accountability, HIPAA) və Beynəlxalq Standartlaşdırma Təşkilatı (International Organization for Standardization, ISO) 27037 (informasiya texnologiyaları) daxil olmaqla hüquqi və uyğunluq məsələləri də qəbuledilmə və araşdırmalar kontekstində müzakirə olunur. Süni intellekt və maşın öyrənməsindəki irəliləyişlərlə rəqəmsal kriminalistika inkişaf etməyə davam edir və hüquq-mühafizə və kibertəhlükəsizlik sahəsində təcrübələr təklif edir [5].

4. Müasir sistemlər və şəbəkələr tərəfindən istehsal olunan böyük həcmli məlumatlarla birlikdə inkişaf etmiş davamlı təhdidlər kimi çoxmərhələli kiberhücumların mürəkkəbliyinin və incəliyinin artması məhkəmə araşdırmalarını bilik və resurslar baxımından daha tələbkar hala gətirib. Beləliklə, kiber kriminalistika tədqiqatçılarının resurslar və sübutların bərpası baxımından daha səmərəli fəaliyyət göstərmələri və geniş çeşidli kiberinsidentlərin öhdəsindən gəlmələri üçün dəstəklənməsi vacibdir.

5. Məqalədə müasir çoxmərhələli kiberinsidentlərin kiber kriminalistika araşdırmalarını dəstəkləməyi hədəfləyən 49 əsərin əhatəli icmalı təqdim olunur və sahədə qərar dəstəyi sistemlərinə ehtiyac vurğulanır.

Baxılan işlər qiymətləndirmə metodu, kriminalistika prosesini necə optimallaşdırmaları və ya araşdırmanın hansı mərhələsini öyrəndikləri kimi 11 meyardan istifadə etməklə müqayisə edilir. Həmçinin, sorğuda iştirak edən məqalələri təklif olunan kiber araşdırma metodunun və ya alətinin ümumi məqsədini təmsil edən 8 kateqoriyadan istifadə edərək təsnif edilir.

Bu geniş araşdırmadan irəli gələn açıq məsələləri, məsələn, real qiymətləndirməyə ehtiyac, eləcə də tətbiqi və performansı artırmaq üçün real və modelləşdirmə kimi məsələləri müəyyən edir və müzakirə edilir. Nəhayət, kiber kriminalistikanın ən müasir vəziyyətini təkmilləşdirmək üçün gələcək tədqiqatlar üçün istiqamətlər təqdim edilir [6].

Məsələnin aktuallığı bir neçə əsas səbəblə izah edilir: Kibertəhdidlərin sürətli artımı və mürəkkəbləşməsi, Hadisələrin səbəblərinin və mexanizmlərinin müəyyən edilməsi, rəqəmsal sübutların toplanması və hüquqi əhəmiyyəti, effektiv insident cavabı və bərpa prosesi, kibertəhlükəsizlik səviyyəsinin yüksəlməsi, böyük verilənlər və yeni texnologiyaların baş verən hadisələrə təsiri, qlobal səviyyədə strateji əhəmiyyəti və s.

Məsələnin qoyuluşu. Məqalədə rəqəmsal kriminalistikanın müxtəlif növləri, aspektləri, bu sahədə görülmüş işlər, rəqəmsal ekspertizasının məqsədi və mərhələləri, kiberinsidentlərin növləri, istifadə olunan metodların tədqiq edilməsidir. Aparılan tədqiqat nəticəsində proqram sistemlərində kiberinsidentlərin kriminal və rəqəmsal ekspertizası sahəsində əsas problemləri müəyyənləşdirməkdir.

IV. RƏQƏMSAL KRİMİNALİSTİKA VƏ EKSPERTİZANIN MƏQSƏDİ

Rəqəmsal kriminalistikanın məqsədi hadisələri yenidən qurmaq və sübutları qanuni olaraq qəbul edilən şəkildə aşkar etmək üçün elektron məlumatları müəyyən, əldə, emal, təhlil etmək və qorumaqdır. Bu, kibercinayətlərin, daxili korporativ hadisələrin və mülki məhkəmə proseslərinin araşdırılmasına imkan verir və rəqəmsal sübutların etibarlı və təhlükəsiz olmasını təmin edir.

Proqram sistemlərində kiberinsidentlərin rəqəmsal ekspertizası aşağıdakı məqsədlərə xidmət edir:

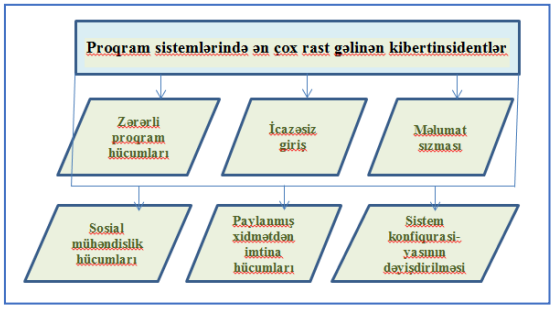
- Kibertəhlükəsizlik hadisəsinin baş vermə səbəbini müəyyən etmək;
- Hücumun mənbəyini və metodunu aşkarlamaq ;
- Sistemə vurulmuş zərərin miqyasını qiymətləndirmək;
- Rəqəmsal sübutları toplamaq və yadda saxlamaq;
- Növbəti hücumların qarşısını almaq üçün təhlükəsizlik tədbirlərini həyata keçirtmək [7].

V. KİBERİNSİDENTLƏRİN NÖVLƏRİ

Kiberinsidentlər kompüter sistemlərinin və məlumatlarının məxfiliyini, bütövlüyünü və ya mövcudluğunu təhlükə altına alan zərərli və ya icazəsiz hərəkətlərdir. Ümumi növlərə zərərli proqram təminatı, fişinq, paylanmış xidmətdən imtina (DDoS) hücumları, daxili təhdidlər, mümkün olan hücumlar və tez-tez məlumatları oğurlamaq və ya əməliyyatları pozmaq üçün hazırlanmış struklaşdırılmış sorğu dili (Structured Query Language, SQL) daxildir [8].

Proqram sistemlərində ən çox rast gəlinən kiberinsidentlər:

- Zərərli proqram hücumları (malware, ransomware);
- İcazəsiz giriş (unauthorized access);
- Məlumat sızması (data leakage);
- Sosial mühəndislik hücumları (social engineering attacks);
- Paylanmış xidmətdən imtina hücumları (Distributed Denial of Service (DDoS) attacks);
- Sistem konfiqurasiyasının dəyişdirilməsi (changing system configuration).



Şəkil 2. Proqram sistemlərində ən çox rast gəlinən kiberinsidentlər

VI.RƏQƏMSAL EKSPERTİZA MƏRHƏLƏLƏRİ

Rəqəmsal kriminalistika məhkəmə prosesi üçün sübutların bütövlüyünü təmin etmək üçün sistemli, prosedur həyat dövrü izləyir. Əsas mərhələlərə Müəyyənləşdirmə, Qorunma, Toplama, Təhlil və Hesabat/Təqdimat (daxildir.

Rəqəmsal ekspertiza prosesi adətən aşağıdakı mərhələlərdən ibarətdir [9]:

1. Sübutların toplanması
    - Sistem loqları;
    - Səbəkə trafiki;
    - Yaddaş (RAM) məlumatları;
    - Fayl sistemləri.
2. Sübutların qorunması
    - Məlumatların dəyişdirilməsinin qarşısı alınır;
    - Heş funksiyaları ilə doğrulama aparılır. Heş funksiya – istənilən uzunluqlu giriş verilənlərin sabit uzunluqlu ikili sətirə elə çevrilməsidir ki, giriş verilənlərdə hər hansı dəyişiklik (hətta ən kiçik dəyişiklik də) çıxış sətirində ciddi dəyişiklik etsin.
3. Analiz mərhələsi
    - Zərərli kodların analizi;
    - İstifadəçi fəaliyyətinin araşdırılması;
    - Hücum ssenarisinin qurulması.
4. Rekonstruksiya
    - Hadisələrin xronologiyası qurulur;
    - Hücumun necə baş verdiyi müəyyən edilir.
5. Hesabatın hazırlanması
    - Texniki nəticələr;
    - Hüquqi istifadə üçün sübutların təqdim edilməsi.

VII.RƏQƏMSAL EKSPERTİZADA İSTİFADƏ OLUNAN METODLAR

Rəqəmsal kriminalistika, saxlanılan məlumatları qoruyarkən rəqəmsal sübutları əldə və təhlil etmək üçün disk görüntüləməsi, yaddaşın təhlili və faylın bərpası kimi üsullardan istifadə edir. Əsas metodlara cihazlar arasında nümunələri müəyyən etmək üçün təhlil, operativ yaddaş (Random access memory, RAM) məlumatlarını əldə etmək üçün canlı təhlil və silinmiş faylları bərpa etmək üçün qaydalar daxildir [10].

- Log analiz metodları;
- Trafik analizi;
- Zərərli proqram analizi;
- Disk və yaddaş forensikası;
- Süni intellekt və maşın öyrənməsi əsaslı analiz.

VIII. AZƏRBAYCAN RESPUBLİKASINDA RƏQƏMSAL EKSPERTİZANIN İNKİŞAF PERSPEKTİVLƏRİ

"Azərbaycan Respublikasında məhkəmə ekspertizası sahəsinin inkişafına dair 2026-2030-cu illər üçün Konsepsiya" bu sahədə islahatların istiqamətini müəyyən edən strateji sənəd kimi qəbul olunub. Sənəd məhkəmə-hüquq sisteminin keyfiyyət transformasiyasına yönəlmiş kompleks yanaşmanı əks etdirir [11].

Konsepsiyada normativ-hüquqi bazanın təkmilləşdirilməsi, rəqəmsallaşdırma, kadr potensialının inkişafı və maddi-texniki təminat kimi istiqamətlər bir-biri ilə qarşılıqlı əlaqədə nəzərdə tutulub.

Sənədin ən mühüm komponentlərindən biri məhkəmə ekspertizası fəaliyyətinin rəqəmsal transformasiyasıdır. Bu istiqamətdə Azərbaycan Respublikası Prezidentinin 2025-ci il 4 noyabr tarixli "Məhkəmə Ekspertizası" informasiya sisteminin yaradılması haqqında Fərmanı mühüm institusional və hüquqi baza rolunu oynayır. Fərman məhkəmə ekspertizası prosesində şəffaflığın, operativliyin və obyektivliyin artırılmasını, bu sahədə bütün əsas prosedurların elektron platforma üzərindən həyata keçirilməsini nəzərdə tutur.

Yeni yaradılacaq sistem vasitəsilə ekspertiza təyin edilməsi ilə bağlı qərarların və müqavilələrin elektron qaydada qəbulu, onların icraata yönəldilməsi və prosesin real-vaxt rejimində izlənilməsi mümkün olacaq. Eyni zamanda, hər bir məhkəmə eksperti və istifadəçi üçün şəxsi kabinetlərin yaradılması, ekspertiza müddətlərinə nəzarət mexanizmlərinin tətbiqi və gecikmələrlə bağlı avtomatlaşdırılmış bildirişlərin göndərilməsi idarəetmədə çevikliyi əhəmiyyətli dərəcədə artıracaqdır.

NƏTİCƏ

Rəqəmsal kriminalistika istənilən növ rəqəmsal cihazdan zərərli fəaliyyətin araşdırılması və sonrakı təhlil və ya hesabat üçün dəlillərin toplanması təcrübəsidir.

Aparılan tədqiqat nəticəsində proqram sistemlərinin kiberinsidentlərin rəqəmsal ekspertizası sahəsində əsas problemləri müəyyənləşdirilmişdir. Bu sahədə əsas problemlər:

- Böyük həcmli məlumatların analizi;
- Şifrələnmiş trafikin araşdırılması;
- Bulud və Əşyaların İnterneti mühitlərində ekspertiza;
- Süni intellekt əsaslı hücumların artması və s.

Proqram sistemlərində kiberinsidentlərin rəqəmsal ekspertizası təşkilatların informasiya təhlükəsizliyinin təmin edilməsində mühüm rol oynayır. Bu proses hücumların səbəblərini müəyyən etməyə, sübutları qorumağa və gələcək təhlükələrin qarşısını almağa imkan verir.

ƏDƏBİYYAT

[1] Kaspersky, "Что такое цифровая криминалистика?," Nov. 26, 2025. https://www.kaspersky.ru/resource-center/definitions/digital-forensics.

[2] G. Horsman and A. Dodd, "Competence in digital forensics," Forensic Science International: Digital Investigation, vol. 51, pp. 1-10, 2024, doi: 10.1016/j.fsidi.2024.301840.

[3] A. Badman and A. Forrest, "What is digital forensics?," IBM, 2026. https://www.ibm.com/topics/digital-forensics.

[4] A. Singh and A. Raj, "Convergence of Digital Forensics and Intelligent Data in Cyberspace," in Proceedings of International Conference on Computing and Communication Systems for Industrial Applications (ComSIA), Data-driven and Industrial Computing, Singapore: Springer, 2024, pp. 111-119.

[5] P. Narasimhan and K. B. Emerging, "Trends in Digital Forensics: Investigating Cybercrime," International Journal of Scientific Research in

Computer Science Engineering and Information Technology, vol. 11, no. 1, pp. 3645-3652, 2025.

[6] A. Nisioti, G. Loukas, and E. Panaousis, "Forensics for multi-stage cyber incidents: Survey and future directions," Forensic Science International: Digital Investigation, vol. 44, pp. 1-16, 2023.

[7] L. Klasén, N. Fock, and R. Forchheimer, "The invisible evidence: Digital forensics as key to solving crimes in the digital age," Forensic Science International, vol. 362, pp. 1-7, 2024.

[8] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176-8186, 2021.

[9] R. L. Sveinsson, "What Are the 5 Stages of a Digital Forensics Investigation?," ERMProtect Cybersecurity Solutions, 2026. https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/.

[10] S. S. Iyengar, S. Nabavirazavi, Y. Hariprasad, P. H. B, and C. K. Mohan, "Digital Forensics: Tools, Techniques, and Methodologies," in Signals and Communication Technology, Springer, 2025, pp. 89–137.

[11] "Azərbaycan Respublikasının bəzi qanunvericilik aktlarına dəyişikliklər və əlavələr edilməsi haqqında," e-qanun.az, Hüquqi Aktların Dövlət Reyestri. https://e-qanun.az/framework/60993.

Digital Forensics and Investigation of Cyber Incidents in Software Systems

Shafagat Mahmudova
Institute of Information Technology, Baku, Azerbaijan
shafagat@gmail.com

Abstract- Digital forensics of cyber incidents in software systems involves the identification, acquisition, preservation, and analysis of digital evidence from applications, records, and log files to reconstruct attack timelines, identify threat actors, and determine root causes. The article investigates the types and aspects of digital forensics of cyber incidents in software systems, previous work in this field, the purpose and stages of digital forensics, and the methods utilized. As a result of the conducted research, the main challenges in the field of digital forensics of cyber incidents in software systems have been identified.

Keywords- software systems; cyber incident; digital investigation; digital forensics; malicious activity.