Informatics

MOBİL KİBER KRİMİNALİSTİKAYA HAZIRLIQ METODOLOGİYALARININ TƏDQİQİ

Rahib Rəsul oğlu Ağababayev
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

A RESEARCH OF THE METHODOLOGY OF MOBILE CYBER FORENSICS READINESS

Rahib Resul Aghababayev
Azerbaijan Technical University, Baku, Azerbaijan: rahib.agb@gmail.com
https://orcid.org/0000-0002-1536-0741

Summary. Mobile cyber forensics serves to recover potential digital evidence from mobile devices using digital forensics. The development and spread of mobile technologies, the need for mobile-based services and new requirements have led to the development and transformation of mobile cyber forensics into an important field. In this article, a component model is proposed to assess the readiness potential of the relevant organizations in the field of mobile cyber forensics for the detection of cybercrimes, collection of evidence, and investigation of criminal cases.

Keywords: *cybercrime, cyber forensics, digital forensics, mobile device, investigation.*

Giriş

Kibercinayətkarlıq bütün dünyada artmaqda davam edir və formalaşan mütəşəkkil beynəlxalq qruplaşmalar İKT infrastrukturlarına böyük təhdidlər yaradırlar. Beynəlxalq problem olan kiberterror, kibertəxribat, kibercasusluq, transmilli mütəşəkkil kibercinayətkarlıq məhz bu təhdidlərə aiddir və kiberməkanda bu fəaliyyətlərin həyata keçirilməsi imkanları genişlənir. Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası"nda kibercinayətkarlığa qarşı mübarizə, o cümlədən kiberkiminalistika sahəsində fəaliyyətin gücləndirilməsi prioritet istiqamətlərdən biri kimi müəyyən edilir [1, s. 11]. Strategiyada seçilmiş prioritetlərin həyata keçirilməsi üçün Tədbirlər Planında müxtəlif işlər də nəzərdə tutulub, o cümlədən haqqında danışılan istiqamət üzrə müvafiq ölçmə mexanizmləri formalaşdırmaq və qiymətləndirmələri həyata keçirmək də planlaşdırılır [1, s. 20].

Rəqəmsal əsrin hazırkı dövründə, şübhəsiz ki, mobil tətbiqlər insan həyatının hər anını əhatə etdiyi aydın görülməkdədir. İstifadəçilər artıq internetdə axtarış və alış-veriş etmək, pul köçürmək, biznes qurmaq, audio və ya video zənglərdən istifadə etməklə ünsiyyət qurmaq, mesajlaşmaq, əyləncə və təhsil kimi bir çox onlayn fəaliyyətləri yerinə yetirmək üçün mobil proqramlara etibar edirlər. Smartfon istifadəsinin bu kütləvi artımı hazırda inanılmaz dərəcədə populyardır və yaxın gələcəkdə də belə olacaq.

Təəssüf ki, onlayn cinayət fəaliyyəti də asanlıqla əldə edilə bilən ağıllı mobil cihazlar vasitəsilə hər yerdə yayılır. Mobil cihazlar gündəlik həyatımızın ayrılmaz hissəsinə çevrilib və onlarda kriminalistik araşdırmalarda istifadə oluna biləcək çox qiymətli məlumatlar ola bilər. Mobil kiberkriminalistika (MKK) kiberkriminalistikanın portativ və/və ya mobil cihazlardan rəqəmsal sübutların çıxarılması ilə əlaqəli altbölməsidir [2]. Quraşdırılmış əməliyyat sistemlərinin müxtəlifliyi, eləcə də dünya üzrə çoxsaylı smartfon istehsalçılarının fərqli yanaşmaları MKK istiqamətində mühüm problemlər kimi diqqəti cəlb edir.

Bu məqalədə kibercinayətlərin aşkarlanması, sübutların toplanılması, cinayət işlərinin istintaqının aparılması üzrə əlaqədar təşkilatların mobil kiberkriminalistika sahəsində hazırlıq potensialını qiymətləndirmək üçün komponent modelinin işlənməsi nəzərdə tutulur.

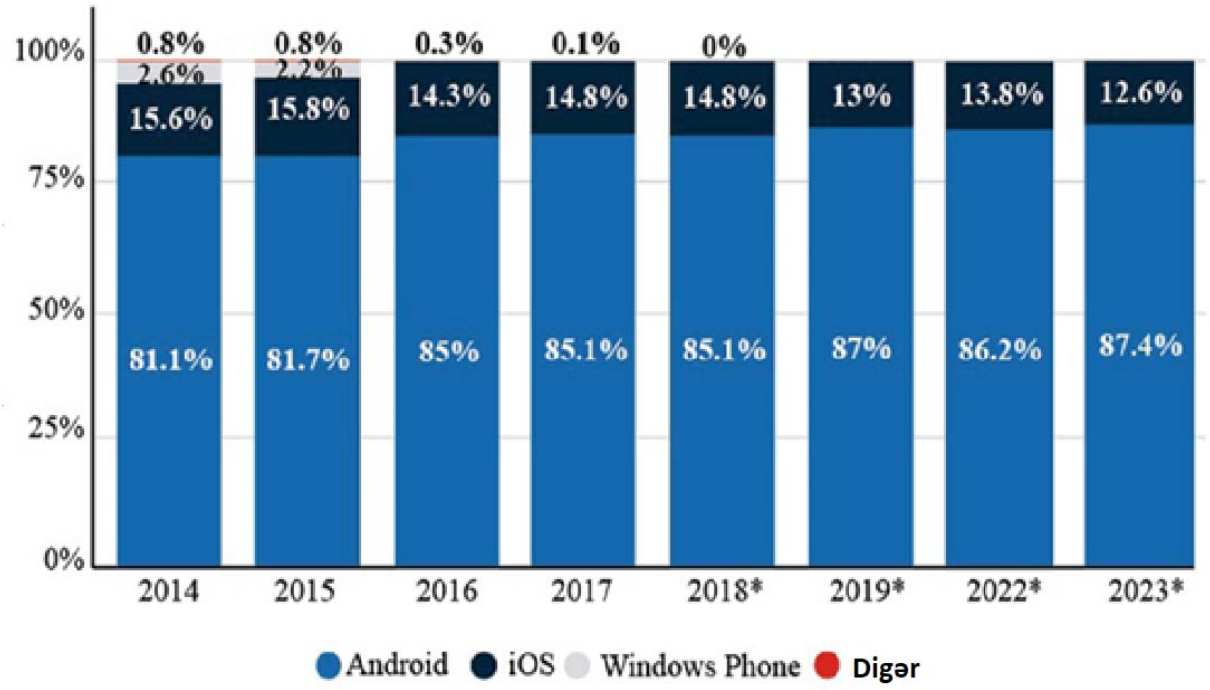
Tədqiqat məsələsinin qoyuluşu

Baxılan tədqiqat işində təşkilatın mobil cihazlarla bağlı insidentlərə operativ reaksiya vermək qabiliyyətini qiymətləndirmək üçün mobil kiberkriminalistikaya hazırlıq planına daxil olacaq

komponentləri müəyyənləşdirmək məsələsi qoyulur. Bu məsələni həll etmək üçün "mobil kiberkriminalistika" anlayışının mahiyyəti dəqiqləşdirilir, mobil kiberkriminalistika üçün proses modeli sintez edilir, mobil kiberkriminalistikada meydana çıxan çətinliklərə baxılır və nəhayət, Mobil kiberkriminalistika hazırlıq planının komponentləri təklif edilir.

Mobil kiberkriminalistikanın təşəkkülü

Smartfonların illik satışları dünya üzrə təqribən (1,56) milyard cihaza qədər böyük dərəcədə artıb, Android əməliyyat sistemi ilə işləyən smartfonlar 2019-cu ildə qlobal bazarın payına (87%) sahib olub və bunun qarşıdakı illərdə artacağı gözlənilir, Apple iOS isə ikinci ən populyar əməliyyat sistemi bütün cihazlarda (13%) bazar payına malikdir (Şəkil 1).



Şəkil 1. Smartfonların əməliyyat sistemləri üzrə 2014-2023 illər üzrə statistikası

2014-cü ildən 2023-cü ilə qədər əməliyyat sistemi üzrə qlobal smartfon tədarükünün payı, bütün dünyada smartfonların bu böyük istifadəsi ilə, texnoloji yönümlü xidmətlərin həyata keçirilməsi üçün bu cihazların geniş şəkildə mənimsənilməsi və mobil tətbiqlərin nəzarətsiz istifadəsi mobil mühiti bir çox qeyri-etik və qeyri-qanuni fəaliyyətlərin həyata keçirilməsi üçün münbit məkana çevirmişdir. Nəticə etibarilə, smartfonlar kiberhücumların məşhur hədəfinə çevrildi, çünki bu cihazlarda böyük həcmdə şəxsi məlumatlar var. Bu cihazların daşınma qabiliyyəti və onlarda olan məlumatların həssaslığı ənənəvi rəqəmsal təhqiqat metodologiyalardan istifadənin məqsədəuyğunluğu və onların bu sahədə nə dərəcədə mümkün olması ilə bağlı böyük narahatlıq doğurur. Həmçinin, smartfonlarda kiberkriminalistika addımlarının idarə olunmasını çətinləşdirən və böyük diqqət tələb edən bir çox imkanlar mövcuddur.

Bu imkanlara SMS, 3G, 4G, Wi-Fi, GPS və s. kimi müxtəlif kommunikasiya texnologiyalarının mövcudluğu, cihazı yandırmaq və ya söndürmək üçün uzaqdan göstəriş vermək imkanı və müxtəlif mobil telefonlardan istifadə edərək məlumatları uzaqdan silmək imkanı daxildir.

Bu və digər məsələlər mobil rəqəmsal sübutlarla məşğul olan zaman təhqiqatçılar üçün böyük problem yaradır [6].

Yeni mobil hesablama paradiqması ilə əlaqədar ortaya çıxan yeni kriminal vəziyyətləri təsvir edən bir sıra terminlər, təriflər və hüquqi məsələlər meydana çıxdı. Bu terminlərdən biri rəqəmsal cihazdan rəqəmsal sübutların toplanması və şəxslərin günahını və ya təqsirsizliyini sübut etmək üçün

təhliletmə prosesinə istinad edən "rəqəmsal məhkəmə ekspertizası" terminidir. Mobil kriminalistika rəqəmsal kriminalistikadan əldə edilən başqa bir termindir, o, smartfondan rəqəmsal sübutları təhqiqat cəhətdən sağlam vəziyyətdə saxlayacaq şəkildə bərpa etməyi hədəfləyir. Mobil kiberkriminalistika analizini aparmaq üçün mobil təhqiqat prosesinin həyat tsikli smartfonlardan etibarlı şəkildə rəqəmsal sübutları ələ keçirəcək, təcrid edəcək, daşıyacaq, saxlayacaq və sübut edəcək dəqiq qaydaları müəyyən etməlidir [2].

Mobil kiberkriminalistikanın çətinlikləri

Ümumiyyətlə, MKK çoxlu səbəblərə görə müxtəlif çətinlikləri mövcuddur. Tədqiqatçılar MKK araşdırmalarını uğurla həyata keçirmək üçün aşağıdakı məhdudiyyətləri müəyyən edirlər [2,7]:

1) Məlumatla bağlı məsələlər (anonimliyin tətbiqi ilə bağlı axtarış və digər anonimlik xidmətləri, təhqiqat zamanı əldə edilən əhəmiyyətli məlumat həcmi, müxtəlif mesaj növləri və qoşmalar);

2) Məhkəmə alətləri ilə bağlı məsələlər (MKK tədqiqat yanaşmaları uzun müddət əldə etmə üsullarına diqqət yetirir, MKK-nın istintaq prosesinin digər mərhələlərinə isə az əhəmiyyət verilir);

3) Cihaz və əməliyyat sistemlərinin müxtəlifliyi – Mobil cihazlar dizayn baxımından müxtəlifdir və mövcud texnologiyalar təkmilləşdikcə və yeni texnologiyalar tətbiq olunduqca davamlı dəyişikliklərə məruz qalırlar. Bazarda iOS, Android, Windows və BlackBerry platformaları ilə yanaşı, çox sayda digər açıq kodlu və xüsusi mobil telefon əməliyyat sistemləri də mövcuddur.

4) Təhlükəsizlik aspektləri – istehsalçılar tərəfindən yeni və daha mürəkkəb anti-kriminalistik üsullar işlənib hazırlanır;

5) Bulud texnologiyaları ilə əlaqəli problemlər cari MKK alətləri bulud aspektlərini, bir neçə yurisdiksiyaya aid hüquqi çərçivələrə görə kriminalistika məlumatlarına çıxış, məhkəmə məlumatlarının təhlükəsizliyi kimi bulud araşdırma maneələrini nəzərə almır;

6) Proseslərin avtomatlaşdırılması – rəqəmsal məhkəmə təhqiqatı prosesini sürətləndirmək və işin emalı imkanlarını artırmaq üçün proseslərin, o cümlədən süni intellektə əsaslanan üsullardan istifadə edərək avtomatlaşdırılmış sübut emalı nəzərdə tutula bilər.

Həmçinin qeyd etmək lazımdır ki, MKK ümumi proseslərinin diqqət mərkəzində olması ilə bağlı mühüm problemlərlə üzləşir. Məsələn, tədqiqat prosedurlarının hər bir cihaz üçün modelə xas olması və ya ekspertiza prosedurlarına tətbiq olunan standartlaşdırılmış təlimatlar toplusunu formalaşdırmaq üçün kifayət qədər ümumi olması aydın deyil.

Digər problem canlı ekspertizanın aparılması ehtiyacıdır (mobil qurğular işə salınmalıdır). Faktiki olaraq, MKK tədqiqatlarının aparılması üçün mühüm maneə smartfonların müxtəlif şəbəkə imkanları ilə bağlıdır ki, bu da ümumi MKK proseslərini, xüsusən də bulud hesablama mühitinin mürəkkəb strukturuna görə idarə etməyi çətinləşdirir. Nəhayət, müasir mobil cihazlara xas olan təhlükəsizlik tədbirləri ilə əlaqədar olaraq, tədqiqatçı cihaz məlumatlarını çox güman ki, dəyişdirəcək eksploytlardan istifadə edərək cihaza daxil olmalıdır. Aydındır ki, sonuncu məsul və nəzarət qurumlarının prinsipini pozur və kiberkriminalistik araşdırma üçün çoxsaylı prosedur məsələləri meydana çıxır.

Mobil kiberkriminalistika üçün proses modeli

Mobil kiberkriminalistika bir elmi istiqamət kimi müvafiq elmi kriminalistika şərtlərindən istifadə edərək mobil cihazlardan rəqəmsal sübutların bərpası ilə məşğul olur [4].

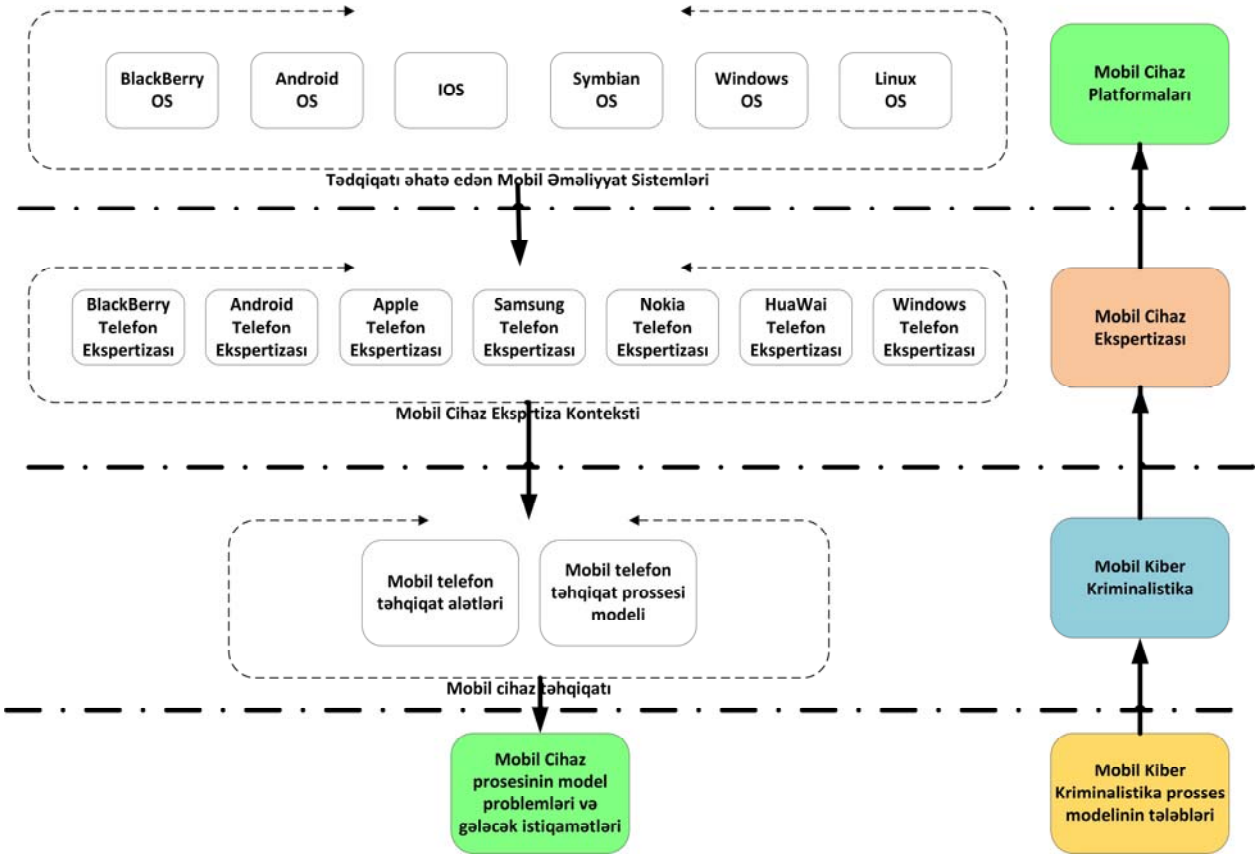
Bundan əlavə, mobil əsaslı xidmətlərə artan tələbat, artan istifadəçilər və mobil texnologiyalarda müşahidə olunan dəyişikliklər, hər yerdə, geniş yayılma və sürətlə böyüyən Əşyaların İnterneti (IoT) texnologiyası sayəsində bu sahə vacib hala gəlir.

Nəticədə, mobil hesablamaların populyarlığı artır və bu tendensiya yüksələn xətlə inkişafa meyllidir. Mövcud tədqiqat tendensiyaları əsasən MKK mütəxəssislərinin təhqiqat işlərinə tətbiq olunan ekspertiza hesabatlarının hazırlanması üçün istifadə oluna bilən rəqəmsal araşdırma proseslərinin olmaması ilə bağlı qavrayışını araşdırmağa yönəlib. Rəqəmsal kriminalistika, xüsusən də cəmiyyətdə mobil cihazların çoxalması ilə tədricən mürəkkəb bir predmet sahəsinə çevrilir.

Rəqəmsal sübutların mühafizəsi, əldə edilməsi, araşdırılması, təhlili və hesabatı üçün mobil kiberkriminalistika prosedurları NIST (National Institute of Standards and Technology) tərəfindən nəşr olunmuş tövsiyə xarakterli bir sıra sənədlərdə müzakirə edilir [3, s. 27-46], [4, s. 9-17].

MKK, müxtəlif təhqiqat prosesi modellərinin tətbiqi ilə erkən inkişaf mərhələsində hesab olunur [5]. Mövcud rəqəmsal kriminalistika təhqiqat prosesi modellərinin bir çoxunda ən böyük problem onların mobil məhkəmə ekspertizasına tam tətbiq edilməzdən əvvəl sınaqdan keçməməsidir. Bundan əlavə, hər hansı təklif olunan rəqəmsal məhkəmə təhqiqat prosesi modelinin elmi ictimaiyyət tərəfindən təsdiqlənməsi üçün sınaqdan keçirilməlidir [6].

Elmi və metodoloji ədəbiyyatın [5,6] analizi əsasında şəkil 2-də mobil telefonların ekspertizasının proses modeli təklif edilir. Bu proses modeli mobil ağıllı cihazların müxtəlif platformalarını əhatə edir və müvafiq ekspertiza kontekstlərini nəzərdə tutur. Mobil kiberkriminalistikanın model problemləri və gələcək istiqamətləri də proses modelinə daxildir. Bununla belə, bu məqalənin əhatə dairəsi mobil kiberkriminalistika hazırlıq planının komponentlərinin müəyyən edilməsi ilə məhdudlaşır.



Şəkil 2. Mobil kiberkriminalistikanın proses modeli

Mobil kiberkriminalistika hazırlıq planının komponentləri

Mobil qurğular cinayət işlərinin araşdırılmasında mühüm əhəmiyyət kəsb edən mətn mesajları, zəng qeydləri, baxış tarixçəsi və məkan məlumatları kimi qiymətli məlumatları saxlaya bilər. Buna görə də, təhqiqatçıların mobil cihazlardan rəqəmsal sübutları əldə etmək və təhlil etmək üçün lazımi alətlərə və bacarıqlara malik olmasını təmin etmək üçün MKK ekspertizasına hazırlıq planının olması vacibdir [4,6].

MKK ekspertizası hazırlığı bir təşkilatın və ya agentliyin mobil cihazlarla bağlı insidentlərə operativ reaksiya vermək qabiliyyəti kimi müəyyən edilə bilər. Bu hazırlığa mobil cihazın analizini effektiv şəkildə aparmaq üçün lazımi avadanlıq, proqram təminatı və kadrların olması daxildir. MKK ekspertizasına hazırlıq planı aşağıdakı sahələri əhatə etməlidir:

- **Avadanlıq və proqram təminatı:** Mobil kriminalistika vasitələri və proqram təminatı mobil cihazlardan rəqəmsal sübutların toplanması və təhlili üçün vacibdir. Təşkilatlar ən son texnologiyaya uyğun olmalarını və ən son mobil cihazlardan məlumatları bərpa edə bilmələrini təmin etmək üçün ən son avadanlıq və proqram təminatına sərmayə qoymalıdırlar.
- **Kadrlar:** Təhqiqatın uğuru əsasən ekspertlərinin bacarıq və təcrübəsinə əsaslanır. MKK ekspertizası ilə məşğul olan işçilər kompüter elmləri, məlumatların təhlili və rəqəmsal ekspertizada güclü təcrübəyə malik olmalıdırlar. Onlar həmçinin ən son texnika və alətlərdən xəbərdar olmaq üçün müntəzəm təlim keçməlidirlər.
- **Standart əməliyyat prosedurları (SƏP):** Bütün araşdırmaların ardıcıl və etibarlı şəkildə aparılmasını təmin etmək üçün standart əməliyyat prosedurları vacibdir. SƏP-lar rəqəmsal sübutların toplanması, təhlili və mühafizəsi də daxil olmaqla MKK ekspertizasının təhqiqatının bütün aspektlərini əhatə etməlidir.
- **Hüquqi və etik mülahizələr:** Təhqiqat bütün hüquqi və etik tələblərə cavab verməlidir. Təhqiqatçılar rəqəmsal sübutların toplanması və təhlilini tənzimləyən qanun və qaydaları hərtərəfli bilməlidirlər. Onlar həmçinin təhqiqatın ədalətli və qərəzsiz aparılmasını təmin etmək üçün etik standartlara və təlimatlara riayət etməlidirlər.
- **Əməkdaşlıq və kommunikasiya:** Əməkdaşlıq və kommunikasiya uğurlu mobil araşdırmaları üçün çox vacibdir. Təhqiqatın bütün aspektlərinin əhatə olunmasını təmin etmək üçün təhqiqata cəlb edilmiş digər idarə və qurumlarla sıx əməkdaşlıq etməlidirlər. Təhqiqatçılar və maraqlı tərəflər arasında səmərəli ünsiyyət, həmçinin bütün tərəflərin təhqiqat prosesi boyunca məlumatlı olmasını və yenilənməsini təmin etmək üçün vacibdir.

Nəticə

Mobil cihazlarda araşdırmalarda istifadə oluna bilən çoxlu məlumat var və təhqiqatçıların mobil cihazlardan rəqəmsal sübutları əldə etmək və təhlil etmək üçün lazımi alətlərə və bacarıqlara malik olmaları ilə yanaşı, mobil kiberkriminalistikaya hazırlıq planının olması da vacibdir. Hazırlıq planı avadanlıq və proqram təminatını, şəxsi heyəti, SƏP-ları, hüquqi və etik mülahizələri, əməkdaşlıq və kommunikasiyanı əhatə etməlidir. Güclü MKK hazırlıq planını həyata keçirməklə təşkilatlar mobil cihazlarla bağlı insidentləri daha dəqiq araşdırmaq və ədalətin təmin olunmasını təmin etmək imkanlarını artıra bilərlər.

ƏDƏBİYYAT

1. Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası. Azərbaycan Respublikası Prezidentinin 2023-cü il 28 avqust tarixli sərəncamı. 31 s.
2. Chernyshev M., Zeadally S., Baig Z., Woodward A. Mobile forensics: Advances, challenges, and research opportunities. IEEE Security & Privacy, 2017, vol. 15, no. 6, pp. 42-51.
3. Jansen W., Ayers R. Guidelines on cell phone forensics. Special Publication Special Publication 800-101. NIST: Gaithersburg, MD, USA, 2007, 96 p.
4. Jansen W., Delaitre A. NISTIR 7617: Mobile forensic reference materials: A methodology and reification. NIST: Gaithersburg, MD, USA, 2009, 31 p.
5. Goel A., Tyagi A., Agarwal A. Smartphone forensic investigation process model. International Journal of Computer Science & Security (IJCSS), 2012, vol. 6(5), pp. 322-341.
6. Horsman G., Sunde N. Part 1: The need for peer review in digital forensics. Forensic Science International: Digital Investigation, 2020, vol. 35, Article 301062, 10 p.
7. Barmpatsalou K., Cruz T., Monteiro E., Simoes P. Current and future trends in mobile device forensics: A survey. ACM Computing Surveys (CSUR), 2018, vol. 51(3), pp. 1-31.

Informatics

MOBİL KİBER KRİMİNALİSTİKAYA HAZIRLIQ METODOLOGİYALARININ TƏDQİQİ

R.R.Ağababayev

Xülasə. Mobil kiberkriminalistika rəqəmsal məhkəmə ekspertizasından istifadə etməklə mobil cihazlardan potensial rəqəmsal sübutların bərpasını həyata keçirməyə xidmət edir. Mobil texnologiyaların inkişafı və yayılması, mobil əsaslı xidmətlərə və yeni tələblərə ehtiyac mobil kiberkrminalistikanın inkişafına və mühüm bir sahəyə çevrilməsinə səbəb olmuşdur. Bu məqalədə kibercinayətlərin aşkarlanması, sübutların toplanılması, cinayət işlərinin istintaqının aparılması üzrə əlaqədar təşkilatların mobil kiberkriminalistika sahəsində hazırlıq potensialını qiymətləndirmək üçün komponent modeli təklif edilir.

Açar sözlər: *kibercinayətkarlıq, kiberkriminalistika, rəqəmsal kriminalistika, mobil cihaz, təhqiqat.*

Accepted: 12.12.2023