Rasim İSAQOV
DİN-in Polis Akademiyasının
"Kriminalistika" kafedrasında
baş müəllimi,
polis polkovnik-leytenantı.

RƏQƏMSAL KRİMİNALİSTİKA VƏ ONUN İNKİŞAF PERSPEKTİVLƏRİ

Açar sözlər: rəqəmsal kriminalistika, internet kriminalistika, informasiya sistemləri, rəqəmsal məhkəmə ekspertizası

Ключевые слова: цифровая криминалистика, интернет-криминалистика, информационные системы, цифровая експертиза

Keywords:digital forensics, internet forensics, information systems, digital forensics expertise

Rəqəmsal kriminalistika yaxşı qurulmamış və artıq sinonimləri olan yeni bir termindir (elektron kriminalistika, kompyuter kriminalistikası, internet kriminalistika və s.). Rəqəmsal kriminalistika müasir informasiya-kommunikasiya texnologiyalarının fəaliyyət xüsusiyyətlərinin dərk edilməsinə əsaslanan və cinayət xarakterli qanunauyğunluqları müəyyən etmək üçün istifadə olunan yeni biliklərdir.

Rəqəmsal kriminalistika onun rəqəmsal mənbələrdən əldə edilmiş rəqəmsal dəlillərin qorunması, toplanması, təsdiqlənməsi, eyniləşdirilməsi, təhlili, sistemləçdirilməsi, sənədləşdirilməsi və təqdimatı ilə əlaqəli elmi cəhətdən əldə edilmiş və sübut edilmiş metodların cinayət kimi tanınan və ya yenidən qurulması üçün istifadə edilməsi planlaşdırılan əməliyyatların qarışısını ala biləcək hərəkətlər sistemidirdir.

Rəqəmsal kriminalistikanın rəqəmsal məhkəmə araşdırması üçün qaydaları, tədqiqat prosesi, media, kod, və şəbəkə təhlili kimi analiz növləri möcuddur. Rəqəmsal kriminalistikanın əsas məzmunu milli təhlükəsizlik və informasiya təhlükəsizliyi, korporativ casusluq, ağ yaxalı cinayətkarlar, uşaq pornoqrafiyası, ənənəvi cinayət, insidentlərə reaksiya, insanların gizli izlənməsi, məxfiliyin pozulması kimi hallarən araşdırılması təşkil edir.

Müasir cinayətlər de-fakto iki dünyada törədilir ki, bunlardan biri maddi obyektlərin tanış dünyası, digəri isə virtualdır. Biz müxtəlif yollarla bu virtual dünyaya qərq oluruq. Məsələn, dolayı yolla - videomüşahidə sistemlərinin obyektivlərinə girməklə, mobil şəbəkələrin baza stansiyaları tərəfindən qeydiyyata alınmış mobil telefonları köçürməklə, mağazalarda bonus xal toplama kartlarından istifadə etməklə və ya avtomobildə GSM modulu və marşrut izləmə funksiyası olan siqnalizasiya sistemi quraşdırmaqla. Daha az olmayan hallarda biz bu dünyanın obyektləri ilə birbaşa qarşılıqlı əlaqədə oluruq, çünki biz İnternetdən məlumat mənbəyi (şəbəkə mediası), müxtəlif proqram təminatından sosial əlaqələr vasitəsi (sosial şəbəkələr Facebook, İnstaqram, V Kontakte və s.), ünsiyyət vasitəsi (WhatsApp, Telegram messencerləri və s.), peşəkar problemlərin həlli üçün alət (informasiyanın bulud saxlanmasını dəstəkləyən ofis proqramları və s.) kimi istifadə edirik.

Cib telefonlarından tutmuş smart televizorlara qədər insanın istifadə etdiyi müasir cihazların böyük əksəriyyəti öz elektron daşıyıcılarında və informasiyanın xarici yaddaşında insan istifadəsinin izlərini də saxlayır. Təbii ki, bu gün rəqəmsal izlərdən cinayətlərin açılması və araşdırılması, işdə həqiqətin üzə çıxarılması maraqları naminə istifadə etmək lazımdır. Lakin belə bir istək, bu imkanın mümkünlüyü və konkret həyata keçirilməsi hüquqmühafizə orqanlarının cinayətlərin araşdırılmasının fərqli təcrübəsinin müxtəlif komponentləridir.

Hələ 20 il əvvəl cinayətlərin hazırlanmasında və törədilməsində yüksək texnologiyalar sahəsində kompyuterləşdirilmiş cihazlardan və rəqəmsal informasiyadan istifadə edilən hər hansı cinayət

gizli elan edilirdi.

Bu kimi cinayətin tez bir zamanda araşdırılmasını, onun sifətlərini müəyyən etmək və günahlarının etibarlı sübutunu gözləmək üçün obyektiv olaraq mümkün deyildi. Bu bəyanatda rəqəmsal izlərin aşkar edilməsi, fiksasiyası və öyrənilməsi üçün məhkəmə-tibbi vasitələrin olmaması, bu cür hərəkətlərin həyata keçirilməsi üsullarının olmaması, rəqəmsal sübutların təhlükəsizliyini və aktuallığını təmin etmək üçün zəmanətlər, xüsusi biliklərin tətbiqi sisteminin olmaması nəzərə alındı. Hüquqmühafizə orqanının strukturunun səviyyəsi (onlarda ixtisaslaşmış bölmələrin və təlim keçmiş mütəxəssislərin olması). Amma daha önəmlisi, istintaqda əsas əlaqənin - təlimi prosessual sübutda istifadə etməyə imkan verən müstəntiqin cinayətin hazırlanması və törədilməsinə dair rəqəmsal formada müxtəlif məlumatları alması idi.

Bu gün rəqəmsal izlərin göründüyü cinayətlərin təhqiqatı ənənəvi cinayətlərdən daha çətin deyil və çox vaxt daha asandır, çünki mütəxəssislər müxtəlif informasiya sistemlərində, müxtəlif informasiya daşıyıcılarında izlərin əmələ gəlməsi mexanizmini bilir, əməliyyat sistemlərində fayllarla işləyərkən rəqəmsal izləri axtarmaq, fiksə etmək, şərh etmək üçün lazım olan xüsusi avadanlıq və proqram təminatı mövcuddur. Mütəxəssislər hazırlanır və məhkəmə ekspertizası texnologiyasının yeni nəslini düzgün tətbiq etməyi bacarırlar.

İnformasiya sistemlərinin, onların komponentlərinin normal fəaliyyətinə mane olmağa yönəlmiş cinayət fəaliyyəti və ya onlardan başqa cinayətlərin törədilməsi aləti kimi istifadə edilməsinə yönəldilmiş fəaliyyət; cinayətlərin hazırlanması, törədilməsi, gizlədilməsi ilə bağlı elektron daşıyıcılarda, informasiya və telekommunikasiya şəbəkələrində, virtual məkanda məlumatların yaradılması, dəyişdirilməsi, ötürülməsi, silinməsi; hüquqi əhəmiyyətini təmin etmək üçün texniki prosedurların həyata keçirilməsi ilə rəqəmsal məlumatların toplanması; ayrı-ayrı informasiya obyektlərində, habelə elektron informasiya daşıyıcısının informasiya mühitində saxlanılan rəqəmsal informasiyanın tədqiqi; əldə edilmiş nəticələrin qiymətləndirilməsi, onların subyektin hərəkətləri ilə əlaqələndirilməsi və cinayət əməlinin kvalifikasiyası üçün istifadə edilməsi; rəqəmsal sübutların onların alınmasının prosessual formasına uyğun olaraq mövcud sübutlar sisteminə inteqrasiyası.

Eyni zamanda bu ənənəvi məhkəmə-ekspertizası elminin yanaşmalarının müasir informasiya cəmiyyətinin inkişafı reallıqlarına elə ciddi və perspektivli uyğunlaşdırılmasıdır ki, hüquq-mühafizə təcrübəsi mümkün qədər tez bu informasiyanın elmi formalaşdırılması yolundan keçməyi istiqamətləndirir və cinayətlərin istintaqında onun müddəalarının kütləvi şəkildə praktiki həyata keçirilməsini tələb edir

Rəqəmsal məhkəmə ekspertizası bilik sistemi kimi formalaşma mərhələsindədir, onun yuxarıda sadalanan komponentləri uğurla, lakin ayrı-ayrılıqda inkişaf edir. Eyni zamanda, rəqəmsal kriminalistikanın komponentlərinin əldə edilmiş inkişaf səviyyəsi əvvəllər haqlı olaraq gizli hesab edilən xüsusilə mürəkkəb cinayətlərin açılmasını və istintaqını artıq təmin etməyə imkan verir. Baş vermiş cinayət hadisəsinin detallarına diqqət yetirək:

Rusiya Federasiyası İstintaq Komitəsinin müstəntiqi tərəfindən gənc qızın itkin düşməsi faktı ilə bağlı başlanmış cinayət işinin istintaqı zamanı onun ögey atası ifadə verib ki, evdən çıxmazdan əvvəl ona mobil telefonuna SMS göndərib. O, onun ünvanına bütün lazımi izahatlarla elektron məktub göndərildiyini bildirdi. Məktubun mətnindən belə nəticə çıxır ki, qızın itməsi cinayət deyil və onun qayıtmasını bir neçə ay gözləmək lazım gəlib.

Eyni zamanda, ögey ata versiyasının cinayəti gizlətmək məqsədi daşıdığını və mövcud rəqəmsal məlumatların (SMS mesajı, e-poçt) məcmusunun onun yaratdığı rəqəmsal alibi olduğunu düşünməyə əsaslar var idi. Bu fərziyyə müstəntiqin SMS mesajlarının göndərilməsi və qəbulu zamanı ögey ata və qızın mobil telefonlarına hansı baza stansiyalarının xidmət göstərdiyini yoxlamasının nəticələrinə əsaslanıb. Həmin anda hər iki telefona eyni baza stansiyası xidmət göstərirdi ki, bu da şəhərin xüsusiyyətlərini nəzərə alaraq, çox güman ki, aşağıdakıları ifadə edirdi: ögey ata ev kompyuterindən istifadə edərək qızının hesabından onun elektron poçtuna məktub göndərə bilərdi. poçt qutusuna, sonra isə öz mobil telefonundan istifadə edərək onu telefonunuza SMS mesajı göndərin.

Müstəntiq sübutların saxtalaşdırılması versiyasının yoxlanılmasında kömək üçün İstintaq Komitəsinin Kriminalistika Baş İdarəsinin ekspertlərinə müraciət edib.

Mütəxəssislər elektron yaddaş daşıyıcısı - qızın istifadə etdiyi ev komputeri ilə bağlı araşdırma apa-

rıb və onun şəbəkə fəaliyyətinin profilini (şəbəkə resurslarının məzmununa baxmaq, mesajlara baxmaq, musiqi dinləmək prioritetləri və adi ardıcıllığı) müəyyən ediblər. Uzun müddət və evdə qalmağın son günündə İnternetdə qeyri-adi iş əlamətləri yox idi. Eyni zamanda, yoxa çıxmazdan əvvəlki gecə işləyən komputer e-poçtu yükləmək tapşırığını yerinə yetirirdi və başa çatdıqdan sonra bu tapşırığı heç kim bağlamadı, bütün işləyən proqramların pəncərələri sonrakı 10 saata yaxın aktiv qaldı, lakin istifadə edilməmişdir, bu müddətdən sonra komputer güclə söndürülərək söndürüldü, halbuki komputeri belə qeyri-adi söndürmə üsulu əvvəllər heç vaxt istifadə edilməmişdi.

Ögey ata, buna görə də rəqəmsal sübutların saxtalaşdırılması versiyası əsas oldu və əlavə araşdırma tələb etdi. Bu cür tədqiqatlar təsdiqlənmiş e-poçtun hazırlanması və göndərilməsi şərtlərini müəyyən etmək üçün aparılmışdır.

Araşdırmaların nəticələri həyəcan verici idi. Birincisi, e-poçt kompyuterin qeyri-adi 10 saatlıq fasilədən dərhal əvvəl (bütün gecə və səhərə qədər) bir anda göndərildi. Əslində bu, kompyuterdə edilən son hərəkət idi.

İkincisi, e-poçt müəyyən bir mətn icraçısı üçün xarakterik ola biləcək xüsusi xüsusiyyətlərə (sözlər arasında boşluqların sayının artması, səhvlər) malikdir. E-poçta normal baxarkən, izləyici mətnin vizual görüntüsünü zorla yaxşılaşdırdıqda, bəzi xüsusiyyətlər görünmürdü və mütəxəssis tərəfindən yalnız məktuba baxmaq üçün xüsusi rejimdə aşkar edilmişdir.

İcraçını müəyyən etmək üçün qızın və onun ögey atasının poçt qutularından e-poçt yazışmalarının ələ keçirilməsi, ardınca məktubların mətnlərinin xüsusiyyətlərinin öyrənilməsi qərara alınıb.

Qızın və onun ögey atasının yazdığı məktubların öyrənilməsinin nəticəsi müstəntiqin versiyasını təsdiqlədi: ögey ata tərəfindən müxtəlif vaxtlarda göndərilən bütün məktublarda yoxlanılan məktubun xüsusiyyətləri ilə üst-üstə düşən icra xüsusiyyətləri var idi. Qızın uzun müddət tədqiq edilən hərflərinin heç birində belə xüsusiyyətlər yox idi. Həmin andan başlayaraq müstəntiq bütün səylərini qızın qətlində ögey atanın iştirakı ilə bağlı yeganə istintaq variantı üzərində cəmləyib.

Cinayət hadisəsinin dəqiq vaxtını (proqramların istifadəsinin əsassız dayandırılması anı) və komputerin məcburi söndürülməsinə qədər keçən vaxtı bilməklə yanaşı, ərazidə yol hərəkəti vəziyyətinin təhlili. Şübhəli şəxsin yaşayış yerinin müəyyən edilməsi, şübhəlinin şəxsi avtomobili ilə gəlib meyiti gizlədərək evə dönə bildiyi ərazini müəyyən etməyə imkan verdi. Sonradan məhz bu axtarış bölgəsində qızın cəsədinin dəfn edildiyi aşkarlanıb.

Rəqəmsal məhkəmə ekspertizası arsenalına daxil olan üsul və vasitələr istintaq prosesində tətbiq olunur. Tədqiqatçıların iştirakı ilə kompyuterlərin, mobil cihazların, elektron daşıyıcıların yoxlanılması və götürülməsi ilə bağlı istintaq hərəkətləri həyata keçirilir. Cinayətin "isti izlər"lə açılmasında istifadə oluna bilən elektron daşıyıcılarında yönləndirici və sübutedici məlumatların operativ şəkildə aşkar edilməsi məqsədi ilə götürülmüş avadanlığa dərhal baxış keçirilməsi və kompyuter-texniki, informasiya-analitik, videotexniki ekspertizanın aparılması təşkil edilir, cinayətlə əlaqəli rəqəmsal məlumatın ən hərtərəfli öyrənilməsinə imkan verir.

Bir çox Texniki profilli Universitetlərdə rəqəmsal informasiyanın sübut edilməsində istifadənin xüsusiyyətlərinə dair müstəntiqlərin təlimi, o cümlədən rəqəmsal informasiya tədqiqatları sahəsində ixtisaslaşan mütəxəssislərin məqsədyönlü hazırlanması həyata keçirilir. Bütün bunlar rəqəmsal kriminalistikanın nailiyyətlərindən istintaq orqanı tərəfindən cinayətlərin araşdırılmasında bundan sonra da səmərəli istifadə olunacağına zəmanətdir.

Bir çox hüquq mühafizə orqanlarının hazırkı və gələcək fəaliyyətində istintaqının aparılması üçün lazımi təlim, avadanlıq və kadr çatışmazlığı aradan qaldırılmalı, Rəqəmsal-kriminalistikanın köməyindən istifadə edərək onlayn fəaliyyət göstərən cinayətkarları tapmaq, və mühakimə etmək imkanlarına mane olan texniki çətinliklər, həmçinin kibercinayətkarlığı araşdırmaq üçün qanunlardan və hüquqi vasitələrdən irəli gələn məsələlərin texnoloji, struktur dəyişikliklər fonunda inkişaf etməsi həlli vacib olan əsas problemlər sırasındadır.

İstifadə edilmiş ədəbiyyat:

1. Azərbaycan Respublikası CPM. Bakı, 2000.
2. Azərbaycan Respublikası CM. Bakı, 2000.
3. «Dövlət məhkəmə ekspertizası fəaliyyəti» haqqında Azərbaycan Respublikasının 18 noyabr 1999-cu il tarixli Qanunu.
4. Sarıcalinskaya K.Q. «Kriminalistika» Ali məktəblər üçün dərslik. Bakı, 1999.
5. Sarıcalinskaya K.Q., Cavadov F.M.,Mahmudov A.M., Əliyev B.Ə. «Məhkəmə ekspertizası». Dərsvəsaiti. Bakı, 2003.
6. Mahmudov A.M., Əliyev B.Ə. «Kriminalistika» sxemlər albomu. Bakı, 2003.
7. Müəllif kollektivi. Məhkəmə ekspertizası sxemlər albomu. Bakı, 2007.
8. Abbasova F.M. «Yeniprosessualqanunveriçilikvəməhkəməekspertizasıfəaliyyəti». Bakı, 2000.
9. Müəllif kollektivi. Daktiloskopiyanın cinayətlərin açılmasında və araşdırılmasında rolu. Polis akademiyası. Bakı, 2013.
10. Cabbarova Ç, Məmmədli A, Hacıyev H, Rzayev K. Əlizlərinin eyniləşdirmə tədqiqatının metodikası. Bakı 2013.
11. Cavadov F.M., Əfəndiyev E.M., «Məhkəmə ekspertizası qarşısında qoyulan sualların nümunəvi siyahısı». Bakı, 1998
12. Cavadov F.M., Ataşova R.H. «Sənədlərin məhkəmə-texniki ekspertizasının yaranması və inkişafı». Bakı, 1997.
13. «İstintaq taktikası». K.Q. Sarıcalinskayanın redaktəsi ilə Ali məktəblər üçün dərs vəsaiti. Bakı,1991.
14. Mayılov Ü.A., Musayev H.Ə., Ələkbərov H.F., İbrahimova Ə.İ., Haçıyev Q.H. «Məhkəmə-xətşünaslıq ekspertizasına materialların hazırlanması». Bakı, 1999.
15. Müəllif kollektivi. Kriminalistik texnika. Bakı, 2016.
16. Цифровая криминалистика. Дмитрий Валерьевич Бахтеев, Виталий Борисович Вехов, Галина Сергеевна Русман, Евгений Владимирович Никитин, Евгений Владимирович Смахтин, Елена Анатольевна Буглаева, Елена Викторовна Христинина, Сергей Александрович Ковалев, Сергей Васильевич Зуев.ЮРАЙТ 2021
17. https://www.cybersecurityjobs.com/forensic-expert-jobs/
18. https://www.gmercyu.edu/academics/learn/computer-forensics

Исагов Расим

Цифровая криминалистика и его перспективы развития

В данной статье раскрывается сущность развития и перспективы цифровой криминалистики. Особое внимание уделено содержанию цифровой криминалистики, сборку цифровых следов преступлений и образцов для сравнительного исследования, назначения цифровой экспертиз, а также тактики проведения следственные действия с участием следователей по осмотру и изъятию компьютеров, мобильных устройств и электронных носителей.

İsaqov Rasim

Digital criminology and its prospects for development

This article reveals the dryness of development and the prospects of digital forensics. Particular attention is paid to the content of digital forensics, a collection of traces of digital offenses and models for comparative research, the purpose of digital expertise, as well as tactics of conducting follow-up activities and follow-up actions.