UOT 34:343.1. Cinayət mühakimə icraatı, s.109-123

LAMİƏ SÜLEYMANOVA

Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzinin
Sənədlərin texniki ekspertizası şöbəsinin böyük eksperti

E-mail:lamia.suleymanova@justice.gov.az
DOİ: https://doi.org/10.64498/VHOJ2229

KİBERCİNAYƏTLƏRİN KRİMİNALİSTİK XARAKTERİSTİKASI

Açar sözlər: kibercinayət, cinayət qanunvericiliyində kibercinayətlərə görə məsuliyyət nəzərdə tutan normalar, kibercinayətkarlığa qarşı BMT Konvensiyası, kibercinayətlərin kriminalistik xarakteristikası, kibercinayətlərin kriminalistik xarakteristikasının strukturu və əsas elementləri, kibercinayətkarın şəxsiyyəti, kibercinayətlərin törədilməsi üsulları.
Keywords: cybercrime, norms in criminal law providing for liability for cybercrimes, UN Convention against Cybercrime, forensic characteristics of cybercrimes, structure and main elements of forensic characteristics of cybercrimes, identity of cybercriminal, methods of committing cybercrimes.
Anahtar kelimeler: siber suç, siber suçlardan dolayı sorumluluğu öngören ceza hukuku normları, BM Siber Suçlara Karşı Sözleşme, siber suçların adli özellikleri, siber suçların adli özelliklerinin yapısı ve temel unsurları, siber suçlunun kimliği, siber suçların işlenme yöntemleri.
Ключевые слова: киберпреступность, нормы уголовного права, предусматривающие ответственность за киберпреступления, Конвенция ООН против киберпреступности, криминалистическая характеристика киберпреступлений, структура и основные элементы криминалистической характеристики киберпреступлений, личность киберпреступника, способы совершения киберпреступлений.

XX əsrin sonu, XXI əsrin ilk illərindən yeni informasiya-texnoloji inqilab dövrünə qədəm qoyan dünyanın hərəkətverici qüvvəsi qismində mikroelektronika, informatika, biotexnologiya, gen mühəndisliyi, enerjinin və materialların yeni növləri, peyk rabitəsi, süni intellekt və sair çıxış edir. Son illərdə süni intellektə, neyron şəbəkələrə əsaslanan rəqəmsal texnologiyaların imkanları və əlçatanlığı, ictimai həyatın bütün sahələrində istifadə səviyyəsi əhəmiyyətli dərəcədə artmış və bu artım meylləri davam etməkdədir. Rəqəmsal texniki vasitələr, mobil qurğular, informasiya-telekommunikasiya şəbəkələri, xüsusən də İnternet və sosial şəbəkələr bir-biri ilə qarşılıqlı bağlılıqda olan qloballaşmış dünyanın ən müxtəlif səviyyələrdə inkişafını şərtləndirən amilə, hər bir insanın gündəlik həyatının ayrılmaz hissəsinə çevrilmişdir [5; 35, s.138]. Müasir zamanın fərqləndirici cəhəti reallıqla virtuallıq, əşyaların dünyası və informasiya dünyası, onlayn və oflayn fəaliyyət, fiziki mühitlə kibermühit arasında sərhədlərin silinməsi, yox olmasıdır [18, s.377].

Yeni minilliyin ilk illərindən başlayaraq informasiya-telekommunikasiya texnologiyalarının sürətli inkişafı müxtəlif rəqəmsal-texniki qurğuların insan həyatının demək olar ki, bütün sahələrinə nüfuz etməsi, mobil rəqəmsal qurğuların, sosial və digər xarakterli qlobal şəbəkələrin yaranaraq aktiv şəkildə hər bir insanın həyatının ayrılmaz hissəsinə çevrilməsi kimi proseslər cinayətkar fəaliyyətə də təsirsiz ötüşməmişdir. Texnoloji və texniki tərəqqi hüquq pozucularına qanunazidd əməllərin törədilməsi məqsədilə yeni informasiya texnologiyalarından istifadə etməyə, cinayətkar fəaliyyətin təşkili metodlarını, üsul və vasitələrinin təkmilləşdirilməsinə də daha əlverişli şərait yaratmışdır [16, s.36; 20, s.218].

Bir sözlə, deyə bilərik ki, kompüterlərin, informasiya-telekommunikasiya texnologiyalarının, İnternetin, sosial şəbəkələrin, rəqəmsal texniki vasitələrin ictimai həyatın bütün sahələrinə nüfuz etməsi və onların əlçatanlıq dərəcəsinin yüksəlməsilə onlardan istifadə etməklə törədilən cinayətlərin, xüsusən də kiberoğurluq, kiberdələduzluq, kiberterrorçuluq, kibernarkoticarət və sair kimi kibercinayətlərin sayı, onların ictimai təhlükəlilik dərəcəsi də artmaqdadır. Müasir kibercinayətkarlar kriminal fəaliyyətin ən müxtəlif sahələrində elmi-

texniki tərəqqinin nailiyyətlərini və yeni informasiya texnologiyalarını aktiv şəkildə mənimsəyir və istifadə edirlər [11, s.179; 12, s.60-61; 30, s.196]. Mobil rabitənin, İnternet-bankçılığın, informasiya-telekommunikasiya şəbəkələrinin, o cümlədən sosial şəbəkələrin və İnternetin, neyroşəbəkələrə əsaslanan süni intellektin inkişaf etməsi kibercinayətlərin daha təhlükəli yeni növ və formaların yaranmasına gətirmişdir.

Son illərdə kibercinayətkar mütəşəkkil dəstə və təşkilatlar yüksək təhsilə və savada malik, kompüter texnikası və şəbəkə texnologiyaları sahəsində bilik və təcrübəyə yiyələnmiş gənc mütəxəssisləri öz kibercinayətkarlıq fəaliyyətinə cəlb etməyə başlamışlar. Bunun nəticəsində xeyli dərəcədə cinayətkar fəaliyyətin üsulları təkmilləşdirilmiş, yeni, daha yüksək kriminal peşəkarlıq səviyyəsi əldə edilmişdir. Hüquq-mühafizə orqanlarına VPN, Tor, anonim proksi-serverlər və sair kimi müasir texnologiyalardan istifadə olunmaqla həyata keçirilən cinayətlərin istintaqını aparmaq olduqca çətin və mürəkkəbdir, çünki qeyd olunan və digər müasir texnologiyalar törədilmiş əməldə cinayətkarın şəxsi iştirakını göstərən sübutların əldə edilməsində ciddi çətinliklər yaradır [5, s.113-114; 27, s.142-144].

Təsadüfi deyildir ki, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası"nda xüsusi olaraq qeyd olunmuşdur ki, Azərbaycan Respublikasının informasiya məkanının müasir təhdidlərdən qorunması milli təhlükəsizliyin əsas istiqamətlərindəndir. Qloballaşan dünyada informasiya təhlükəsizliyinin və kibertəhlükəsizliyin təmin olunması istər milli, istərsə də beynəlxalq səviyyədə əsas məsələyə çevrilmişdir. Son zamanlar Azərbaycanın informasiya məkanına, o cümlədən onun tərkib hissələrinə (dövlət, özəl və qeyri-hökumət qurumlarının, fiziki şəxslərin sahib olduğu informasiya ehtiyatlarına və infrastrukturlarına) qarşı texnoloji cəhətdən çoxşaxəli hücumlar genişlənməkdədir.

Cəmiyyətin rəqəmsal dövrə keçməsinin neqativ nəticələri təkcə yeni növ cinayətlərin (kibercinayətlərin) yaranması ilə deyil, həm də bütövlükdə cinayətkarlığın strukturunun, kəmiyyət və keyfiyyət parametrlərinin əhəmiyyətli dəyişməsi ilə bağlıdır. Mütəxəssislər "cinayətkarlığın rəqəmsallaşması"nı kibernetik metodların, həmçinin informasiya-kommunikasiya texnologiyalarının alət və vasitələrinin cinayətlərin törədilməsi üsullarına və mexanizmlərinə nüfuz etməsini qeyd edirlər [28, s.3].

Beləliklə, deyə bilərik ki, informasiya texnologiyalarının və rəqəmsal texniki vasitələrinin sürətli inkişafı, cəmiyyət həyatının bütün sahələrinin kompüterləşməsi, müsbət, mütərəqqi xarakterli proseslərlə yanaşı kompüterlərdən, kompüter sistemlərində və şəbəkələrində saxlanılan və işlənilən informasiyadan qanunsuz istifadə ilə bağlı yeni cinayət növləri yaratmışdır. Belə cinayətlər elmi ədəbiyyatda və məhkəmə-istintaq təcrübəsində "kibercinayayətlər" adını almışdır. Cinayətkarlar kompüter avadanlığından və telekommunikasiya sistemlərindən istifadə edərək elektron məlumatlar bazasına qanunsuz daxil olur, məlumatları əldə edir, dəyişdirir, silir və ya bloklayır, fiziki və hüquqi şəxslərə böyük maddi və mənəvi ziyan vururlar. Mexanizminə, törədilmə üsullarına, cinayətkarın şəxsiyyətinə görə özünəməxsus səciyyəvi xüsusiyyətlərə malik olan kibercinayətkarlıq, yüksək latentlik səviyyəsi ilə xarakterizə olunur [6, s.40-41; 21, s.451-452].

Xüsusi ədəbiyyatın, məhkəmə-istintaq təcrübəsinin öyrənilməsi əsasında kibercinayətlərin aşağıdakı kriminalistik xüsusiyyətlərini qeyd edə bilərik:

- virtual xarakter;
- yüksək latentlik;
- açılması və istintaqı üçün rəqəmsal ekspertizanın (xüsusi biliklər əsasında şəbəkə protokollarının, proqram təminatının və kompüter sistem və şəbəkələrinin digər aspektlərinin tədqiqi) təyini və aparılmasının zəruriliyi;
- növ və forma baxımından müxtəliflik və digər amillərə görə cinayət-hüquqi tövsifin mürəkkəbliyi;
- qloballıq və genişmiqyaslılıq;
- kibercinayətlərin açılması və istintaqının yalnız ixtisaslaşan xüsusi bölmələr, ixtisaslı şəxslər tərəfindən aparılması, o cümlədən bu sahədə xüsusi biliyə malik olan mütəxəssis-ekspertlərin cəlb edilməsi ilə mümkünlüyü;
- istintaqı zamanı sübutlar qismində çox vaxt rəqəmsal sübutların çıxış etməsi, virtual mühitdə, yəni kiberməkanda cinayətkar tərəfindən qoyulmuş rəqəmsal izlərin, elektron sübutların toplanması, götürülməsi, tədqiqi, analizi və məhkəməyə təqdim edilməsinə xüsusi yanaşma tələb etməsi [19, s.376].

Kibercinayətkarlığın başlıca əlamətlərindən biri informasiya-kommunikasiya mühitidir. Virtual məkan bilavasitə zərərçəkmişdən fiziki məsafəni və anonimliyi təmin edərək cinayətin törədilməsini əhəmiyyətli dərəcədə asanlaşdırır. Real dünyadan fərqli olaraq virtuallıq cinayətkarda şəxsi təhlükəsizlik hissini doğuran (və heç də həmişə yalan olmayan) cinayətkar fəaliyyətin həyata keçirilməsi yolunda

bir çox psixoloji maneələri aradan qaldırır.

Digər bir çox kriminal əməllərdən fərqli olaraq kibercinayətlərin eyni zamanda xeyli sayda zərərçəkənlərin olması, çoxsəviyyəli ictimai təhlükəli nəticələrin bütöv zəncirini hərəkətə gətirmə xüsusiyyəti də qeyd olunmalıdır. Məsələn, maliyyə sektoruna və ya ayrı-ayrı təsərrüfat subyektlərinin və ya fiziki şəxslərin bank hesablarına genişmiqyaslı virus hücumları zamanı zərərçəkmişlərin sayı yüzlərlə və minlərlə ola bilər [10, s.35; 28, s.9-10].

"Kibercinayətkarlıq haqqında" 23 noyabr 2001-ci il tarixli Avropa Şurasının Budapeşt Konvensiyasında iştirakçı-dövlətlərə kriminalllaşdırılması zəruri olan kiberəməllərə aşağıdakılar aid edilmişdir:

- kompüter verilənləri və sistemlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı cinayətlər – qanunsuz daxil olma, ələ keçirmə, verilənlərə müdaxilə, sistemlərə müdaxilə, qurğulardan qanunsuz istifadə;

- kompüter vasitələrindən istifadə ilə bağlı cinayətlər – kompüter texnologiyalarından istifadə etməklə saxtalaşdırma, kompüter texnologiyalarından istifadə etməklə dələduzluq;

- məlumatların məzmunu ilə bağlı cinayətlər – uşaq pornoqrafiyası ilə bağlı cinayətlər;

- müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər [2, s.6; 3, s.144-147].

Qeyd edək ki, Azərbaycan Respublikası sözügedən konvensiyanı 30 iyun 2008-ci il tarixdə imzalamış, 30 sentyabr 2009-cu il tarixdə isə ratifikasiya etmişdir.

Bu konvensiyada kriminallaşdırılması tövsiyə olunan əməllərin milli qanunvericiliyə implementasiya edildiyini qeyd etmək lazımdır. Belə ki, CM-də kibercinayətlərə görə məsuliyyət nəzərdə tutan normalar "Kibercinayətlər" adlanan 30-cu fəslə daxil edilmiş və bu fəsildə aşağıdakı cinayətlərə görə məsuliyyət müəyyən edən normalar nəzərdə tutulmuşdur:

- kompüter sisteminə qanunsuz daxil olma (maddə 271);

- kompüter məlumatlarını qanunsuz ələ keçirmə (maddə 272);

- kompüter sisteminə və ya kompüter məlumatlarına qanunsuz müdaxilə (maddə 273);

- kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (maddə 273-1):

- kompüter məlumatlarının saxtalaşdırılması (maddə 273-2).

Eyni zamanda, A.N.İbrahimovanın düzgün qeyd etdiyi kimi, "texnoloji inkişaf, süni intellekt sistemlərindən istifadə, əşyaların interneti kimi tandemlər kibercinayətlərin təsnifatının tez-tez yenilənməsini tələb edir. Ənənəvi bölgüdə yeni subkateqoriyaları artırmaqla yeni kiber pozuntuların da kriminallaşdırılması və onlara qarşı mübarizə aparılması vacibdir" [2, s.5].

Məhz bu amilləri nəzərə alaraq BMT Baş Məclisi 2024-cü ildə Kibercinayətkarlığa qarşı BMT Konvensiyasını qəbul etmiş və bu konvensiyada kibercinayət hesab edilən əməllərin dairəsi əhəmiyyətli dərəcədə genişləndirilmiş, kriminallaşdırılması zəruri olan əməllərə aşağıdakılar aid edilmişdir:

- elektron məlumatları əldə etmək məqsədilə informasiya-kommunikasiya sisteminə və ya onun istənilən hissəsinə qanunsuz qanunsuz daxil olma (maddə 7);

- elektron məlumatları qanunsuz ələ keçirmə (maddə 8);

- elektron məlumatların qəsdən və qanunsuz olaraq zədələmə, silimə, korlama, dəyişdirmə və ya bloklama (maddə 9);

- elektron məlumatları daxil etmə, ötürmə, zədələmə, məhv etmə, korlama, dəyişdirmə və ya bloklama yolu ilə informasiya-kommunikasiya sisteminin işinə qanunsuz və qəsdən ciddi maneə yaratma maddə (10);

- qəsdən və qanunazidd olaraq ilk növbədə hər hansı bir cinayətin törədilməsi məqsədilə hazırlanmış və ya adaptasiya edilmiş proqram təminatı da daxil olmaqla qurğuları əldə etmə, istehsal etmə, satma, istifadə üçün əldə etmə, yayma, həmçinin bütün informasiya-kommunikasiya sisteminə və ya onun istənilən hissəsinə daxil olmağa imkan verən parolları, daxil olma rekvizitlərini, elektron imzanı və ya analoji məlumatları əldə etmə, satma, yayma və ya digər üsulla təqdim etmə üçün qurğulardan qanunsuz istifadə etmə (maddə 11);

- qəsdən və qanunazidd olaraq qeyri-autentik məlumatların yaranmasına gətirən elektron məlumatların, onların hüquqi məqsədlər üçün autentik kimi nəzərdən keçirilə bilməsi və istifadə niyyəti ilə, daxil edilməsi, dəyişdirilməsi, silinməsi və ya bloklanması (maddə 12);

- informasiya-kommunikasiya sistemindən istifadə etməklə talama və ya dələduzluq (maddə 13);

- uşaqlar üzərində seksual xarakterli təhqir və həqarət və ya onların seksual istismarı səhnələri olan materialları internetdə yerləşdirmə (maddə 14);

- uşağa münasibətdə seksual cinayət törətmək məqsədilə aldatma və ya etibar doğuran münasibətlər yaratma (maddə 15);

- şəxsin razılığı olmadan onun intim təsvirlərini

yayma (maddə 16); cinayətdən əldə edilən gəlirləri yuma, yəni leqallaşdırma (maddə 17).

Göründüyü kimi, Budapeşt Konvensiyasının qəbul edilməsindən sonra keçən 23 il ərzində kibercinayətkarlığın forma və növlərində əhəmiyyətli dəyişikliklər baş vermiş, bu kateqoriyalı əməllərin ictimai təhlükəlilik dərəcəsi artmışdır ki, bu da beynəlxalq birliyə bu əməlləri milli səviyyədə kriminallaşdırılması zəruri olan əməllər sırasına aid etməyə əsas vermişdir.

Bütün bunlar isə kibercinayətlərə cinayət-hüquqi vasitələrlə qarşıdurma ilə yanaşı, həm də kibercinayətlərin kriminalistik xarakteristikasına, onların açılması və istintaqının bir sıra aktual məsələlərinə diqqətin xeyli artmasını şərtləndirmişdir.

Kriminalistika elmi mövqeyindən istənilən cinayətin istintaqının mahiyyəti, ilk növbədə kriminalistik əhəmiyyət kəsb edən informasiyanın axtarışı, onun tədqiqi və qiymətləndirilməsindən ibarətdir. Müəyyən dərəcədə informasiya cinayət subyektinin qanunazidd hərəkətlərinin nəticəsidir. Bu hal söyləməyə əsas verir ki, istənilən cinayətkar əməlin idrakı və deməli onun istintaqı üzrə fəaliyyətin əsasında ilk növbədə aşkar və qeyri-aşkar mənbələrdən məlumatların (o cümlədən rəqəmsal informasiyanın) əldə edilməsi, onların tədqiqi, bu və ya digər növ cinayətlərin açılması və istintaqı məqsədləri ilə sonradan istifadəsi ilə bağlı informasiya prosesləri durur [15, s.57-62].

Onlayn məkanda mövcud olan və ya informasiya-kommunikasiya texnoloji nailiyyətlərdən və imkanlardan istifadə edən cinayətkarlıq (rəqəmsal cinayətkarlıq) özünü yeni, zəif öyrənilmiş və araşdırılmış neqativ kibersosial hadisə kimi göstərir ki, onun idrakı, onunla mübarizə üçün xüsusi yanaşma, metod, üsul və vasitələr tələb olunur. Bu baxımdan kibercinayətkarlığın və onun ayrı-ayrı növ və formalarının kriminalistik xarakteristikasının, onun struktur elementlərinin müəyyən edilməsi, bu elementlərin hər birinin mahiyyət və məzmununun açılması, bu kateqoriyalı cinayətlərə qarşıdurmanın taktiki-kriminalistik aspektlərinin işlənib hazırlanması milli və beynəlxalq təhlükəsizliyin təmini üçün müasir cəmiyyət qarşısında duran ən mühüm vəzifələrdən biri hesab edilməlidir.

Məlum olduğu kimi, kriminalistik xarakteristika - cinayətlərin istintaqı və qarşısının alınmasının təşkili və həyata keçirilməsi üzrə elmi əsaslı tövsiyələr sistemindən ibarət olan kriminalistik metodikanın məzmununa daxil olan əsas struktur elementlərdən biridir [29, s.5-6; 33, s.8-9]. S.N.Pavlikovun qeyd etdiyi kimi, cinayətlərin kriminalistik xarakteristikasının praktiki əhəmiyəti ondan ibarətdir ki, onun öyrənilməsi istintaqın başlanğıc və sonrakı mərhələlərində təşəkkül tapan istintaq şəraitlərini düzgün qiymətləndirməyə, istintaqın istiqamətlərini müəyyən etməyə, istintaq fərziyyələrini irəli sürməyə, onların yoxlanılmasının optimal yollarını müəyyən etməyə, düzgün taktiki qərarlar qəbul etməyə imkan verir [24, s.45-47].

Cinayətkarlıqla mübarizə nəzəriyyəsi və təcrübəsinin analizi göstərir ki, kriminalistik xarakteristikadan düzgün və bacarıqla istifadə edilməsi bu və ya digər növ cinayətlərin hərtərəfli, tam və obyektiv istintaqının mühüm şərtidir. Cinayətlərin istintaqı metodikasının ayrılmaz tərkib hissəsi olmaqla, kriminalistik xarakteristika törədilmiş cinayətin arı-ayrı elementləri haqqında kriminalistik əhəmiyyət kəsb edən məlumatları əldə etməyə imkan verir.

Təsadüfi deyildir ki, J.L.Rişet, Y.S.Çanq və P.Qrabovski kimi tədqiqatçılar öz əsərlərində kibercinayətlərin istintaqı prosesinin təkmilləşdirilməsinə, təhlükəsiz kiberməkanın yaradılması məsələlərinə xüsusi diqqət yetirir, kibercinayətlərin istintaqının kriminalistik aspektlərinə, kriminalistik xarakteristikasının işlənib hazırlanması sahəsində problemlərin həllinə xüsusi önəm verirlər [6, s.321-339; 8].

Son illərdə kriminalist-alimlərin bir çoxu kriminalistik xarakteristikanın istənilən istintaq metodikasının mühüm struktur elementini təşkil etdiyini göstərirlər. Məsələn, A.V.Şmonin hesab edir ki, məhz kriminalistik xarakteristika tədqiq olunan obyektin – müəyyən kateqoriyalı cinayətlərin kriminalistik mahiyətini ən adekvat şəkildə əks etdirir [34, s.156].

M.X.Mustafayev və İ.S.Abbasova yazırlar ki, kriminalistik xarakteristikanın əsasında informasiyanın maddi və ideal daşıyıcılarında cinayətin törədilməsi mexanizminin əks olunmasının xarakterik qanunauyğunluqlarının üzə çıxarılması üçün zəruri olan və kəmiyyət-keyfiyyət nisbətində kifayətedəcək materialları əhatə edən müəyyən dövr ərzində uyğun cinayətkar fəaliyyət növünün istintaqı təcrübəsinin ümumiləşdirilməsi durur [23, s.302]. Fikrimizcə müəlliflərin qeyd etdikləri informasiyanın maddi və ideal daşıyıcılarına, müasir reallıqlar, məhkəmə-istintaq təcrübəsi nəzərə alınmaqla informasiyanın rəqəmsal, yəni elektron daşıyıcıları da aid edilməlidir.

Hesab edirik ki, kibercinayətlərin kriminalistik

xarakteristikası dedikdə, bu növ cinayətlərin əlamətləri və xüsusiyyətləri haqqında kriminalistik əhəmiyyət kəsb edən, ən xarakterik və qarşılıqlı bağlı olan məlumatların (informasiyanın) sistemli məcmusu, onların özünəməxsus informasiya-kriminalistik modeli başa düşülür ki, bunlar da cinayətin şəraiti və cinayətkarın şəxsiyyəti haqqında fərziyələrin irəli sürülməsinin əsası kimi çıxış edə bilər və kibercinayətlərin açılması və istintaqı prosesində yaranan şəraitləri düzgün qiymətləndirməyə imkan verməklə, uyğun kriminalistik metod, üsul və vasitələrin tətbiqini şərtləndirir [31, s.141].

Kibercinayətlərin kriminalistik xarakteristikasının formalaşması prosesinə təsir edən problemlər sırasında yüksək latentliyi, rəqəmsal sübutların axtarışı, götürülməsi, toplanması, qeydə alınması, saxlanması və tədqiqinin, ümumən sübutetmə prosesinin mürəkkəbliyini, kibercinayətlərin kriminalistik əhəmiyyət kəsb edən əlamətlərin geniş dairəsini, hüquqazidd əməllərin (hərəkətlərin) törədilməsi yeri ilə ictimai təhlükəli nəticələrin baş verdiyi yerin üst-üstə düşməməsini, Azərbaycanda kibercinayətlərlə mübarizə sahəsində məhkəmə-istintaq təcrübəsinin tam formalaşmamasını və ənənəvi cinayətlərlə müqayisədə ictimai rəy tərəfindən bu növ cinayətlərin çox zaman ciddi təhlükə kimi qiymətləndirilməməsini və s. göstərmək olar.

Cinayətlərin kriminalistik xarakteristikası strukturca və məzmunca müxtəlif elementlərdən təşkil olunmuşdur.

Xüsusi ədəbiyyatda cinayətlərin kriminalistik xarakteristikasının strukturuna bir qayda olaraq aşağıdakılar haqqında məlumatlar daxil edilir:

- cinayətin predmeti;
- cinayət şəraiti (yeri, vaxtı və cinayət hadisəsinin digər halları);
- cinayətin törədilməsinin tipik üsulları;
- cinayətin tipik maddi, ideal və rəqəmsal izləri;
- cinayətin törədilmə mexanizmi;
- cinayətin izlərinin aşkar olunmasının daha çox ehtimal olunan yerləri;
- cinayətkarın şəxsiyyətinin tipik cəhətləri;
- cinayət qrup halında törədildikdə cinayətkar qrupun xarakterik cəhətləri;
- izyaranma xüsusiyyətləri;
- digər hallar (məsələn, zərərçəkən haqqında məlumatlar, dəymiş zərərin xarakteri və həcmi, cinayətin törədilməsinə kömək edən səbəb və şəraitlər).

Z.İ.Xarisova hesab edir ki, kibercinayətlərin kriminalistik xarakteristikanın əsas elementləri qismində kibercinayətlərin törədilməsi üsulları (cinayətin tipik izlərinin, onların gizlədilməsi üsullarının təsviri ilə), onları törətmiş şəxslər, kibercinayətin törədilmə şəraiti (yeri, vaxtı və s.) bu kriminal əməllərdən zərərçəkmişlər və bu kateqoriyalı əməllərin törədilməsinə kömək edən hallar haqqında məlumatlar daxildir. Eyni zamanda bu sistemin sadalanmış elementləri onun mahiyyətini tam əks etdirmir, bunun üçün kriminalistik xarakteristikanın tərkib elementləri arasında qarşılıqlı əlaqə və asılılıqların üzə çıxarılması da zəruridir [32, s.97-98].

A.F.Abdulvaliyev hesab edir ki, kibercinayətlərin kriminalistik xarakteristikasının struktur elementlərinə cinayətin predmeti və obyekti, cinayətin törədilmə şəraiti, cinayətin törədilməsi üsulu, kibercinayətlərdən zərər çəkmiş şəxslər, cinayətkarın şəxsiyyəti və onun peşəkar bacarıq və vərdişləri daxil edilməlidir [9, s.315].

A.M.Mahmudov və B.Ə.Əliyev kompüter informasiyasına qanunsuz daxil olma kimi kompüter cinayəti növünün kriminalistik xarakteristikasına "Qanuna zidd əməllərin törədilmə üsulları və mexanizmi haqqında məlumatların, kompüter informasiyasına qanunsuz daxil olmanın gizlədilməsi üsulları haqqında məlumatların, qanuna zidd əməllərin törədilməsinin alət və vasitələri haqqında məlumatların, kompüter informasiyasına qanunsuz olaraq daxil olmanın yeri və şəraiti haqqında məlumatların, cinayət qəsdinin predmeti haqqında məlumatların və kompüter informasiyasına qanunsuz daxil olma cinayətini törədən şəxslər haqqında məlumatların" daxil olduğunu qeyd edirlər" [4, s.167-168].

Fikrimizcə, kibercinayətlərin kriminalistik xarakteristikasının əsas struktur elementlərinə aşağıdakıları aid etmək olar:

- cinayətkar qəsdin predmeti haqqında məlumatlar
- cinayətkar qəsdin istiqamətləndiyi kompüter informasiyasının növü və təyinatı, bu informasiyanın saxlanılması və işlənilməsi üçün istifadə olunan maddi və elektron daşıyıcılar;
- cinayətkar fəaliyyətin tipik maddi, ideal və rəqəmsal izləri, onların ən ehtimal olunan aşkar edilmə yerləri (məsələn, kompüter qurğuları və hissələrində, proqram təminatında, informasiya daşıyıcılarında, digər predmetlərdə iz informasiyasının lokalizasiyası xüsusiyyətləri) haqqında məlumatlar;
- kibercinayətlərə hazırlıq və onların törədilməsinin tipik üsulları və mexanizmi haqqında məlumatlar;
- kiberkriminal əməllərin gizlədilməsi üsulları

haqqında məlumatlar;

- kiberkriminal fəaliyyət gedişində istifadə olunan alətlər, vasitələr, yardımçı qurğu və avadanlıqlar, materiallar və sair haqqında məlumatlar;

- kibercinayətin törədilmə şəraiti (yeri, vaxtı və s.) haqqında məlumatlar;

- cinayətin törədildiyi virtual və fiziki mühit haqqında məlumatlar (cinayətin törədildiyi kompyuter, onların sisteminin apparat, proqram və informasiya təminatının növü və xüsusiyyətləri və s.);

- bu növ cinayətləri törədən şəxslər haqqında məlumatlar (burada ənənəvi elementlərlə yanaşı, cinayətkarın peşə hazırlığı, ixtisası, bacarıq və vərdişləri, informasiya-kompüter texnologiyaları haqqında biliklərin səviyyəsi, proqramlaşdırma dillərini bilməsi və s. xüsusi əhəmiyyət kəsb edir);

- kibercinayətlər mütəşəkkil dəstələr tərəfindən törədildiyi zaman mütəşəkkil dəstənin tipik tərkibi, dəstədə mövcud qarşılıqlı əlaqə sxemi, liderin və ya təşkilatçının şəxsiyyəti, hərəkət və davranış motivləri, məqsədləri, kriminal bacarıq və vərdişləri, dəstə üzvləri arasında qarşılıqlı münasibətlər haqqında məlumatlar.

Kibercinayətlərin kriminalistik xarakteristikasının mühüm struktur elementlərindən biri bu kriminal əməlləri törədənlərin şəxsiyyətidir. Bir çox kriminalistlərin fikrincə, kibercinayətkarın şəxsiyyətinin əsas səciyyəvi xüsusiyyəti onun kompüter texnologiyaları sahəsində yüksək bilik, bacarıq və vərdişlərə, informasiya-telekommunikasiya şəbəkəsinə, kompüter sisteminə asanlıqla daxil olma, rəqəmsal vasitələrdən istifadə etmə bacarığına malik olmasıdır [19, s.373].

Cinayətkarların "peşəkar" vərdişləri və dəsti-xətləri cinayətlərin törədilməsinin müəyyən üsullarında, metodlarında və vasitələrində ifadə olunur. Cinayət hadisəsi yerində qoyulan izlər onun (cinayətkarın) sosial-psixoloji portretinin təcrübə, peşə, cins, bilik və s. xüsusiyyətlərini göstərir. Məhz buna görə də cinayətkarların müxtəlif kateqoriyalarının tipik modelləri bankının formalaşdırılması aralarında cinayətkarın olması daha çox ehtimal olunan şəxslər dairəsini müəyyən etməyə və bu şəxslər qrupunda kriminal əməli törədənlərin axtarışı prosesini optimallaşdırmağa imkan verir. İstintaq prosesində cinayətkarın şəxsiyyəti, onun kriminal davranışı və təqsirliliyi barədə toplanmış məlumatlar cinayət təqibi üzrə əsaslı hüquqi qərarların qəbulu üçün faktiki baza yaradır.

Məlum olduğu kimi, hazırda insanların bir çoxu, xüsusən də yeniyetmə və gənclər elektron texniki vasitələrdən, kompüterlərdən istifadə etmək bacarıqlarına malikdirlər. Yaşlı insanların bu sahədə bilik və bacarıq səviyyələri o qədər də yüksək olmasa da, yeniyetmə və gənclər barədə bunu deyə bilmərik. Qeyd edək ki, məhz yaşlı şəxslərin kompüterlərdən istifadə sahəsində baza biliklərinə malik olmamalarından kibercinayətləri törədən şəxslər, xüsusən də informasiya-telekommunikasiya texnologiyaları sahəsində peşəkar biliklərə malik olanlar tərəfindən kriminal məqsədlərlə istifadə edilir [9, s.322].

M.Verşinanın məlumatlarına görə kibercinayətlərin böyük hissəsi informasiya texnologiyaları sahəsində dərin və peşəkar biliklərə malik olan 18-40 yaş arasında olan şəxslər tərəfindən törədilir [13]. A.A.Zaytsev və A.V.Smolin hesab edirlər ki, bu kateqoriyalı cinayətləri daha çox yaşı 18-35 arasında olan kişi cinsli kompüter texnikasının aktiv istifadəçiləri törədirlər [16, s.39]. S.V.Zuyev isə qeyd edir ki, kibercinayətləri, o cümlədən kompüter informasiyasına qanunsuz daxil olmanı həyata keçirən şəxs, bir qayda olaraq, ali və ya orta mühəndis-texniki və ya iqtisadi təhsilə, bu sahədə formalaşmış sabit cinayətkar vərdişlərə malikdir. Bu kateqoriyalı cinayətlərin yetkinlik yaşına çatmayanlar tərəfindən törədilməsi halları da az deyildir. Ümumiyyətlə isə kibercinayətkarlar əsasən 16-40 yaşda olan, kişi cinsli şəxslərdir [7; 17, s.77].

Bir qayda olaraq bu şəxslər sosial mühəndislik metodlarına mükəmməl yiyələnmişlər və onlar insanların emosiyaları, hissləri, qorxu və reflekslərı ilə oynamağa, onların davranışlarını idarə etməyə, təşəkkül tapmış şəraitdən asılı olaraq mümkün davranışlarını proqnozlaşdırmağa imkan verən sosiologiya və psixologiya sahəsində kifayət qədər biliklər məcmusuna malikdirlər.

V.B.Vexov kibercinayətkarların üç qrupunu fərqləndirir:

1. Kompüter texnikası və proqramlaşdırma sahəsində peşəkarlıqla özünəməxsus fanatizm və ixtiraçılıq elementlərini sabit şəkildə özündə birləşdirən şəxslər;

2. Yeni növ psixi xəstəliklərdən – informasiya xəstəliklərindən və ya kompüter fobiyalarından əziyyət çəkən şəxslər;

3. Açıq-aşkar ifadə olunan tamah məqsədləri olan peşəkar kompüter cinayətkarları [14, s.38-39].

Xüsusi ədəbiyyatda məqsəd və motivlərdən asılı olaraq kibercinayətkarların aşağıdakı tip və növlərini fərqləndirirlər:

1) frikerlər - kiminsə sifarişini yerinə yetirmək və ya əyləncə, habelə öz bacarıq və vərdişlərini təkmilləşdirmək xatirinə kompüterlərin, şəbəkələrin, rəqəmsal texniki və texnoloji qurğuların mühafizə sistemini sındırmaqla qanunsuz olaraq müxtəlif informasiya sistemlərinə, saytlara və akkauntlara giriş əldə etməyə istiqamətlənən şəxslər;

2) Kiberterrorçular - milli təhlükəsizliyi sarsıtmaq, həyati əhəmiyyətli infrastruktur obyektlərinin normal işini pozmaq və sıradan çıxarmaq üçün kiberhücumlardan istifadə edən kibercinayətkarların ən təhlükəli tipidir;

3) Krekerlər - kompüter sisteminə qanunsuz daxil olmanı həyata keçirirlər və bunun üçün belə daxil olmaları həyata keçirməyə imkan verən proqram təminatından, o cümlədən ziyanverici proqramlardan istifadə edirlər;

4) Virusmeykerlər və ziyandaşıyıcılar – viruslar, troyanlar və s. kimi ziyanverici proqramlar yaradırlar. Onlar bu proqramlardan informasiyaya daxil olmanı təmin etmək və ya informasiya sisteminin normal işini pozmaq, onu sıradan çıxarmaq üçün istifadə edirlər. Bu şəxslər, həmçinin darknetdə öz "məhsullarını" digər şəxslərə satmaqla da məşğul ola bilərlər;

5) Fişengerlər - elektron poçtdan, sosial şəbəkələrdən və digər informasiya-telekommunikasiya vasitələrindən istifadə etməklə dələduzluqla məşğul olan şəxslərdir. Onların mqəsədi qurbanın şəxsi məlumatlarını və pul vəsaitlərini ələ keçirmək, onlarda qeyd olunan məlumatları təqdim etməyə inandırmaqdır;

6) Karderlər – bank sistemlərinin və İnternet mağazaların elektron mühafizə sistemini sındırmaqla maliyyə məlumatlarının, fiziki və hüquqi şəxslərin hesab məlumatlarının, plastik kartların nömrə və parollarını, digər məxfi rekvizitlərin oğurlanması üzrə ixtisaslaşmış şəxslərdir. Onlar müxtəlif rəqəmsal vasitə və proqram komplekslərindən istifadə etməklə bank hesablarına, kredit kartların nömrələrinə və ödəniş vasitələri ilə bağlı digər məlumatlara qanunsuz girişi əldə edə bilirlər;

7) Bot-ustalar - kiberhücumların həyata keçirilməsi üçün botnetlərdən (virusa və digər ziyanverici proqramlara yoluxmuş kompüterlərdən) istifadə edirlər. Onlar digərlərinin kompüterlərinə giriş əldə edə və bu şəbəkələrdən ziyanverici proqram təminatını yaymaq, saytlara kiberhücumları həyata keçirmək və s. üçün istifadə edə bilərlər [19, s.373-374; 22, s.139].

Kompüter informasiyasına qanunsuz daxil olmanı həyata keçirən şəxslərin xüsusi kateqoriyasını xakerlər təşkil edir. Xakerlər müxtəlif "hesablara, akkauntlara, elektron poçtlara, mobil qurğulara qanunsuz daxil olaraq hesab məlumatlarını, digər məxfi rəqəmsal məlumatları oğurlayır və dəyişdirir, faylları modifikasiya edir, şəbəkəni və kompüter sisteminin işini bloklayır, proqram təminatını sıradan çıxarırlar. Əksər hallarda xakerlərin qəsd predmeti olaraq çıxış edir: istehsalçı firmalar tərəfindən buraxılan müxtəlif proqramların kommersiya və ya mətn variantları (kompüter oyunları, tətbiqi proqramlar, inteqrə olunmuş proqram paketləri, əməliyyat sistemləri və s.); müxtəlif tədqiqatlar üçün istifadə edilən kompüter sistemləri; internet şəbəkəsi istifadəçilərinin Web-səhifələri (onların dəyişdirilməsi və ya digərləri ilə əvəz edilməsi, elektron poçt ünvanlarının dəyişdirilməsi) və s.

Xüsusi ədəbiyyatda müasir xakerin tipik portreti belə verilir: kompüterlə erkən yaşlardan tanış olur, kompüter sistemi onun üçün həyatın mənasıdır, sosial cəhətdən təcrid olunmuşdur, ətraf aləmə fikir vermir. Psixofizioloji xarakteristika nöqteyi-nəzərindən, xaker – bir qayda olaraq yaradıcı şəxsiyyət, peşəkar, texniki çağırışa, riskə getmək iqtidarında olan şəxsdir. Hazırda bir çox nəhəng şirkətlər informasiyanın və kompüter sistemlərinin mühafizə sistemlərini yaratmaq məqsədi ilə təcrübəli xakerləri işə dəvət etməyə çalışırlar.

Xakerləri bəzən kiberxuliqanlar, elektron korsarlar da adlandırırlar. Xeyli dərəcədə onları texniki (proqram) mühafizəsində çətinliklərin – kompüterlərə daxil olma parollarını aşmaq cəlb edir. Sistem nə qədər mürəkkəb olarsa, xakerlər üçün bir o qədər də cəlbedici olur.

Kibercinayətlərin kriminalistik xarakteristikasının daha bir mühüm struktur elementi bu əməllərin törədilməsi üsuludur.

Cinayətlərin törədilməsi üsulları cinayət və cinayət-prosessual hüquq, kriminalistika və kriminologiya, habelə digər elmlər tərəfindən tədqiq edilir, bu elmlərdən hər biri də bu kateqoriyanı öz aspektində öyrənir. Məsələn, törədilmə üsulu cinayətin obyektiv tərəfini xarakterizə edən əlamətlərdən biri olduğundan cinayət-hüquqi əhəmiyyət kəsb edir. Eyni zamanda onun prosessual əhəmiyyəti də vardır, çünki sübutetmə predmetini xarakterizə edir. İstintaq təcrübəsi üçün cinayətlərin törədilməsi üsulunun öyrənilməsinin kriminalistik aspekti xüsusi əhəmiyyət kəsb edir. Belə ki, bu aspekt cinayətlərin açılması, istintaqı və qarşısının alınmasının metod, üsul və vasitələrinin işlənib hazırlanması üçün zəruri olan məlumatlar

mənbəyi kimi çıxış edir.

Kriminalistikada cinayətlərin törədilməsi üsulu cinayətlərin hazırlanmasına, törədilməsinə və gizlədilməsinə istiqamətlənmiş qarşılıqlı şərtlənən, daima inkişafda olaraq determinələnən hərəkətlər sistemidir ki, bu da uyğun alət və vasitələrdən istifadə, habelə cinayətlərin törədilməsi yeri, vaxtı və digər obyektiv şəraiti xarakterizə edən hallarla bağlıdır. V.B.Vexov yazır ki, kriminalistikada cinayətlərin törədilməsi üsulu olaraq adətən cinayət subyektinin cinayətin törədilməsinə qədər, törədilərkən və törətdikdən sonra obyektiv və subyektiv amillərlə şərtlənən davranış və hərəkətlərinin sistemi başa düşülür. Bu üsullar müxtəlif xarakterik izlər qoya bilirlər ki, onlar da kriminalistik vasitələrdən, metod və üsullardan istifadə etməklə baş verən hadisənin mahiyyəti, hüquq pozucusunun cinayətkar davranışının özünəməxsusluğu, onun ayrı-ayrı şəxsiyyət xarakteristikaları haqqında təsəvvürlər əldə etməyə və uyğun olaraq cinayətlərin açılması və istintaqı vəzifələrinin həllinin ən optimal metodlarını müəyyən etməyə imkan verir [14, s.12-13].

Bütövlükdə kibercinayətlərin törədilməsinin üsullarının tam və əhatəli dairəsini vermək mürəkkəb və çətindir, çünki onların məzmununa cinayətkarın texniki təminatı, motivi, intellektual səviyyəsi, bacarıq və vərdişləri, hiyləgərliyi və sairədən asılı olaraq ən müxtəlif hərəkətlər daxil ola bilər.

Xüsusi ədəbiyyatda kompüter informasiyasına qəsdən qanunsuz daxil olmanın əsas üsulları sırasında göstərilir:

- istifadəçilərin hesab məlumatlarını talamaqla kompüterin müdafiə sisteminin sındırılması;
- informasiyanın mühafizəsi sisteminin qeyri-təkmilliyindən istifadə edilməsi;
-proqramm təminatı və əməliyyat sistemində mövcud boşluqlardan istifadə edilməsi

(eksploytlərdən istifadə edilməsi – ingilis "exploit" sözündən);

- texniki vasitələrə və informasiya sistemlərinə, həmçinin yardımçı kompüter avadanlığına (xarici yaddaş qurğularına) qanunsuz qoşulma;
- fişinq (məlumatların sanksiyalaşdırılmamış əldə edilməsi üçün saxta resursların və ya bildirişlərin yaradılması) [32, s.98-99].

A.S.Kiselev və K.A.Qorbunova kibercinayətlərin törədilməsinin bəzi üsullarını qeyd edirlər:

1) virusların və ziyanverici proqramm təminatını yaratma;
2) fişinq və sosial mühəndislik;
3) şəbəkələrin, kompüterlərin və onların sisteminin, mobil qurğuların giriş kodlarının, yəni mühafizə sisteminin dəf olunması, yəni "sındırılması";
4) şəxsi məlumatların oğurlanması;
5) kibercəsusluq;
6) kiberterrorçuluq [19, s.374].

A.A.Zaytsev və A.V.Smolin cinayətkar fəaliyyətin subyektinin hərəkətlərinin xarakterinə görə bu kateqoriyalı cinayətlərin törədilməsinin kompüter informasiyasına qanunsuz daxil olma, kompüter informasiyasının ələ keçirilməsi, kompüter informasiyanı dəyişdirmə, silmə və ya bloklama kimi üsulları vardır. Müəlliflər kibercinayətlərin törədilməsi vasitəsilə pul vəsaitlərini talama əməllərinin alət və vasitələri qismində İnternet informasiya-telekommunikasiya şəbəkəsi, kompüter qurğuları, kompüter proqramları, informasiyanın elektron daşıyıcıları, ödəniş kartları, xüsusi rəqəmsal-texniki asitələr, ziyanverici proqramlar və sairə çıxış etdiyini göstərərək, xüsusi halda elektron ödəniş vasitələrindən istifadə etməklə kibercinayətlərin törədilməsinin iki əsas üsulunu fərqləndirirlər:

- elektron ödəniş vasitələrinə qanunsuz daxil olaraq pul vəsaitlərinin talanması (oğurlanması) məqsədilə istifadəçilərin şəxsi məlumatlarının ələ keçirilməsi və istifadəsi;
- ödəniş sistemlərində, proqramm təminatında, avadanlıq və qurğularda olan boşluqlardan istifadə etmə [16, s.39-40].

Z.İ.Xarisova kompüter informasiyasına qanunsuz daxil olma izlərinin gizlədilməsinin əsas üsullarına sistem jurnallarının təmizlənməsi və sistemdə baş verən hadisələrin şifrələnməsi, kompüterlərə və ya informasiya sistemlərinə qoşulmalar haqqında məlumatların silinməsini, qurğuların İP-ünvanlarının dəyişdirilməsi üçün anonimləşdirməni təmin edən proqram vasitələrindən istifadəni (VPN-serverlər və proksi-serverlər sistemi), məlumatların şifrələnməsini təmin edən messencerlərdən istifadəni və s. aid edirlər [32, s.99].

A.F.Abdulvaliyev tərəfindən isə kibercinayətlərin tam strukturlu törədilməsi üsulunun xüsusiyyətləri qismində aşağıdakılar xüsusi olaraq göstərilir:

1) Kibercinayətin törədilməsinə hazırlıq - qanunsuz daxil olmanın, dəyişdirilmənin, silinmənin və ya bloklanmanın həyata keçiriləcəyi kompüter informasiyasının müəyyən olunması, kompüter proqramının köməyi ilə parolun və ya elektron açarın tapılması, kompüterin sistem təminatının incəliklərini əks etdirən sənədlərin axtarışı və öyrənilməsi, ziyanverici kompüter proqramının təyinatının (kompüter informasiyasını dəyişdirmək, bloklamaq

və ya silmək) müəyyən edilməsi, ziyanverici proqramın yaradılması zamanı proqramlaşdırılma dilinin seçilməsi, ziyanverici kompüter proqramının yayılma üsulunun (bilavasitə kompüterin özündən və ya məsafədən, qlobal şəbəkələrdən istifadə etməklə) müəyyən edilməsi.

2) Kibercinayətin törədilməsi üsulları - kompüter informasiyasına qanunsuz daxil olma, kompüter informasiyasına ziyanverici və digər xarakterli təsiri həyata keçirmə, kompüter informasiyasının saxlanması, emalı və ya ötürülməsi vasitələrinin və informasiya-telekommunikasiya şəbəkələrinin istismarı qaydalarını pozma, ziyanverici proqramların yaradılması, istifadəsi və ya yayılması.

3) Kibercinayətlərin gizlədilməsi üsulları - özgənin parolu və ya elektron açarından (elektron imzasından) istifadə etməklə kompüter informasiyasına qanunsuz daxil olma və ziyanverici təsir göstərmə, başqa şəxsin MAC və ya İP-ünvanından istifadə etmə, lisenziyalaşdırılmış sistem təminatına ziyanverici proqramı əvvəlcədən daxil etmə [9, s.320-321].

A.N.İbrahimova kibercinayətlərin törədilməsinin müxtəlif üsullarının mövcudluğunu, onların sırasında isə Azərbaycanda daha çox sosial mühəndislik və fişinq kimi üsullarının daha geniş yayıldığını qeyd edərək yazır ki, "sosial mühəndislik – insanlarla qarşılıqlı əlaqədə olaraq onlardan məlumat toplamaqdır. Bu növün əsas amillərindən biri saxta profillərdən (başqa adla və ya hər hansı bir saxta şirkət, kampaniya və s.), virtual dostluq və tanışlıqdan istifadə edib istifadəçini aldatmaqdan ibarətdir. Əsas məqsədi tanşılıq, virtual dostluq və ya hər hansı digər etibar qazanmış mənbədən sui-istifadə etməklə məlumatın toplanmasıdır". Müəllif bizim ölkədə kibercinayətlərin törədilməsinin daha bir geniş yayılmış üsulunun fişinq olduğunu göstərir və qeyd edir ki, "fişinq – ingilis dilindən tərcümədə "balıq ovu" deməkdir və qlobal şəbəkədə balıq ovunu xatırladan fırıldaqçılığın bir növüdür. Belə ki, fırıldaqçı (Fişer) internetdə "tələ" quraraq, bu tələyə düşən İnternet istifadəçilərini aldatmaqla məşğul olur. Fişer müxtəlif üsullarla İnternet istifadəçilərindən bank hesablarını, kredit kartlarını və internetə çıxış üçün lazım olan informasiyaları öyrənir. Fişinq kiberdələduzluğun xüsusi növüdür, istifadəçiləri aldatma yolu ilə adətən maliyyə xarakterli fərdi məlumatların təqdim olunmasına məcbur etməyə yönəlir. Dələduz bank saytı kimi görünən (və ya maliyyə əməliyyatları aparılan digər sayt kimi, məsələn, eBay) saxta veb-sayt yaradır. Sonra cinayətkarlar istifadəçiləri bu sayta aldadıb aparmağa cəhd edirlər ki, bu saytda onlar login, parol və ya PİN-kod kimi konfidensial məlumatları daxil etsinlər" [2, s.8-9].

Təbii ki, informasiya-kompüter texnologiyaların, süni intellektin inkişafı ilə yeni-yeni təhlükələr və təhdidlərin də yaranmasının mümkünlüyü, kibercinayətkarların daima öz cinayətkar metodlarını, kriminal əməllərin həyata keçirilməsi üsullarını təkmilləşdirdiklərini də nəzərə almaq lazımdır.

Kompüter informasiyasına qanunsuz daxil olmanın əsas vasitələri qismində şəbəkə avadanlığı və informasiya sistemlərinə daxil olmanı təmin edən vasitələrlə yanaşı, həmçinin müxtəlif xarakterli proqram təminatı (məsələn, trafikin şifrələnməsini və cinayətkarın real İP-ünvanının gizlədilməsini təmin edən VPN servislər, məlumatların çoxsəviyyəli şifrələnməsini bazasında qurulan proksi-serverlər və s.), o cümlədən, lokal informasiya şəbəkəsində hər hansı bir pozucu hərəkətlərin (faylların silinməsi, bloklanması və ya dəyişdirilməsi) icra edilməsi məqsədilə ziyanverici proqramlar və s. göstərilir [32, s.99].

Cinayətin törədilmə şəraitinin müəyyən edilməsi istənilən cinayətin, o cümlədən olduqca spesifik xarakteristikaların daşıyıcıları olan kibercinayətlərin istintaqında da mühüm əhəmiyyət kəsb edir. İlk öncə qeyd edək ki, istantaqa bu kateqoriyalı cinayətlərin törədilməsi yerini və vaxtını müəyyən etmək kifayət qədər çətin və mürəkkəbdir. Eyni zamanda o da aydındır ki, bu məlumatlar səbəb-nəticə əlaqələrinin müəyyən olunması və törədilmiş qanunazidd əməldə şəxsin təqsirli olub-olmamasının müəyyən edilməsində olduqca əhəmiyyətlidir. Bu onunla şərtlənmişdir ki, bu kateqoriyalı cinayətlər virtual mühitdə törədəlir və bu mühitdə təkcə adi vətəndaşlar deyil, hətta dövlət də cinayətkarın qurbanı ola bilər. Bununla bağlı kibercinayətlərin törədildiyi yerin müəyyən olunmasına yanaşmanın spesifikliyi xüsusi olaraq qeyd olunmalıdır. Məsələn, cinayətkar VPN, TOR kimi serverlərdən istifadə etdiyi halda cinayətin törədilməsi yerinin müəyyən olunması olduqca mürəkkəbləşir [19, s.375].

Xüsusi ədəbiyyatda kibercinayətlərin törədilməsi şəraitinin xüsusiyyətləri ilə bağlı məsələlərə toxunularkən qeyd olunur ki, bu kateqoriyalı cinayətlərin törədilməsi zamanı təbiət və ya iqlim amillərindən asılı deyildir [16, s.39].

Kibercinayətlərin törədilməsi vaxtının təyini prosesi də özünəməxsus xüsusiyyətlərlə xarakterizə olunur. V.V.Polyakovun qeyd etdiyi kimi, bəzi proqramların işi kompüterdə müəyyən olunmuş

vaxtla bağlıdır və cinayətkar lazım gəldikdə bu vaxtı özü üçün rahat olan istənilən vaxta dəyişə bilər. Cinayətin törədilmə vaxtının təyini sadə məsələ deyildir və heç də həmişə bunu etmək mümkün deyildir [26, s.114-116]. Bu isə o deməkdir ki, kibercinayət, kibercinayətkarın məqsədlərindən, tələbatlarından, həmçinin texniki imkanlarından asılı olaraq sutkanın istənilən vaxtında törədilə bilər.

Kompüter informasiyasına qanunsuz daxil olmanın tipik izlərinə kompüterin pereferik qurğularında əks olunan rəqəmsal (qanunsuz daxil olma üçün istifadə edilən quraşdırılmış proqram təminatı, qurğunun əməliyyat sisteminin konfiqurasiyasında edilmiş dəyişikliklər, kompüterə və ya informasiya sistemlərinə qoşulma jurnalları, dəyişdirilmiş və ya bloklanmış məlumat faylları və s.) və maddi izlər aid edilə bilər. Kibercinayətlərdə izyaradan və izqəbul edən əsas obyektlər qismində bir qayda olaraq sistem və ya tətbiqi proqram təminatı, informasiya daşıyıcılarında qeydiyyat sahələri, elektron fayllar, məlumatlar bazası, elektron açarlar (elektron imzalar), məlumatların ötürülməsi şəbəkəsinin identifikatorları (məsələn, qurğunun İP ünvanı və onun şəbəkə kartının MAC ünvanı), mobil rabitə vasitələrinin İMEİ kodları, DNS ünvanları, əməliyyat sisteminin reyestrləri, şəbəkə trafiki, rəqəmsal maliyyə aktivləri və elektron pulqabıları, İMV, SMS və MMS bildirişlər və s. çıxış edir.

Generativ süni intellektin, kvant alqoritmlərinin, neyron şəbəkələrin və digər ən müasir innovativ metod, üsul və vasitələrin inkişafı ilə bağlı olan amillər də xüsusi olaraq qeyd olunmalıdır. Belə ki, elmi-texniki tərəqqinin bu yenilikləri kibercinayətlərin yeni növ və formalarının (şəxsi hesabların, virtual əmlakın, şəxsiyyəti eyniləşdirən rəqəmsal məlumatların oğurlanması, şifrələnmə açarlarının sındırılması və s.) yaranmasına gətirir. Bu və digər cinayətkar əməllərdə izyaradıcı və izqoyucu obyektlər qismində saxtalaşdırılmış mutlimediakontent, metaməlumatlar, metaməkanı formalaşdıran serverlər toplusu (üçölçülü virtual məkanları vizuallaşdırılmasını və mərkəzləşdirilməmiş şəbəkələrin işləməsini təmin edən proqram təminatının işləməsi ardıcıllığını əks etdirən jurnallar, rəqəmsal avatarların qarşılıqlı işinin şəbəkə ünvanları) və ya kvant kompüterlərin konfiqurasiyası (kvant tətbiqlərinin və kvant vəziyyətləri damplarının istismarı reyesterləri, kvant əlaqələrinin protokolları və s) çıxış edə bilər. Rəqəmsal kompüter informasiyasına qanunsuz daxil olmanın tipik izlərinin yerləşməsinin ehtimal olan yerlərinə rəqəmsal informasiya daşıyıcıları, server avadanlığı və "bulud" saxlanc yerləri, o cümlədən faylların və məlumatların saxlanıldığı kateloqlar, məsafədən daxil olma proqramlarının konfiqurasiya faylları və sair aid edilə bilər [32, s.100-103].

Beləliklə, kibercinayətlərin kriminalistik xarakteristikası faktiki olaraq istintaqın tipik alqoritmlərinin yaradılmasının nəzəri-informasiya bazasını, özünəməxsus rəqəmsal-kriminalistik modelini təşkil edir. Məhz bu rəqəmsal-kriminalistik model istintaq prosesini optimallaşdırmağa imkan verir.

Kriminalistik xarakteristikanın strukturundan danışarkən adətən onun elementlərini fərqləndirir, sonradan isə bu elementlərin hər birinin konkret məzmunla tamamlayırlar. Hər bir cinayətin, xüsusən də kibercinayətin kriminalistik xarakteristikası nəzərdən keçirilərkən"iz", "cinayətin iz mənzərəsi" xüsusi əhəmiyyət kəsb edir. Məhkəmə-istintaq təcrübəsi, həmçinin bu kateqoriyalı cinayətlərin nəzəri analizi göstərir ki, kibercinayətlərin istintaqı zamanı müstəntiqlər təkcə ənənəvi maddi və ideal izlərlə deyil, həm də virtual, yəni rəqəmsal izlərlə qarşılaşırlar. Qeyd edək ki, rəqəmsal izlər müəyyən spesifikliklə səciyyələnsələr də, onlar da ənənəvi izlər kimi, cinayətin mexanizminin müxtəlif elementlərinin (cinayətkar, zərərçəkmiş, cinayətin törədilməsi şəraiti, üsulu və s.) qarşılıqlı təsiri nəticəsində yaranırlar. Aşkar edilmiş, qeydə alınmış və götürülmüş virtual izlər hər bir cinayətin mexanizmi, onun törədilmə şəraiti, üsulları, cinayəti törədənlərin bir sıra spesifik xüsusiyyətləri haqqında müəyyən nəticələr çıxarmağa imkan verir [9, s.312-313].

Beləliklə, deyə bilərik ki, kibercinayətlərin kriminalistik xarakteristikası bu kateqoriyalı cinayətlərin açılması və istintaqının konkret vəzifələrinin həllinə xidmət edən və cinayət hadisəsinin tipik mənzərəsini yaratmaqla bir-birinə qarşılıqlı təsir edən və qarşılıqlı bağlı olan elementlər sistemi haqqında ümumiləşdirilmiş kriminalistik əhəmiyyət kəsb edən məlumatların məcmusu, kibercinayətin özünəməxsus informasiya-kriminalistik, yəni rəqəmsal-kriminalistik modelidir. Bu məlumatlar sisteminə, rəqəmsal-kriminalistik modelə isə kibercinayətkarın şəxsiyyəti, kriminal əməlin törədilməsi üsulu, şəraiti (yeri, vaxtı və s.), motiv və məqsədləri, kibercinayətin törədilməsi üçün istifadə olunan texniki-rəqəmsal vasitələr və texnologiyalar, proqramlar, kibercinayətin törədilməsi mexanizmi, rəqəmsal (elektron) izlərin aşkar olunmasının tipik yerləri, ümumən izyaranma mexanizmi və sair haqqında məlumatlar daxildir.

Kibercinayətlərin törədilmə üsullarının analizi göstərir ki, informasiya texnologiyaları, rəqəmsal qurğu və vasitələr, telekommunikasiya şəbəkələri kriminalistik xarakteristikanın formalaşmasına əhəmiyyətli dərəcədə təsir edir, müasir cinayətkarın sosial portretini dəyişdirir (onlarda informasiya sistemlərinin işləmə prinsipi və imkanları barədə biliklərin olması), izyaranma mexanizminin formalaşmasına təsir edir. Ona görə də bu istiqamətdə sonrakı elmi-nəzəri tədqiqatların aparılması olduqca aktual və əhəmiyyətli hesab edilməlidir.

Kibercinayətlərin başlıca kriminalistik xüsusiyyəti ondan ibarətdir ki, bu kateqoriyalı cinayətlərin üzə çıxarılması, açılması, istintaqı və qarşısının alınması informasiya texnologiyalarından, müasir aparat proqram vasitələrindən istifadə etmədən mümkün deyildir. Uyğun olaraq, bu növ cinayətlərlə mübarizə üzrə mütəxəssislərin hazırlanması, mövcud kadrların ixtisas artırmaları çox önəmlidir. Qeyd olunan kateqoriyalı cinayətlərin istintaqında kompüter-texniki ekspertizanın, yəni rəqəmsal kriminalistik ekspertizanın da rolu və əhəmiyyəti şəksizdir [7]. Buna görə də bu növ ekspertizaların elmi-metodiki və texniki-texnoloji əsaslarının təkmilləşdirilməsi xüsusi önəm kəsb edir. Bu da məcmu halda müxtəlif növ elektron sübutların aşkarı, qeydə alınması, götürülməsi, tədqiqi və istifadəsi vasitəsilə cinayətkarların daha effektiv şəkildə üzə çıxarmağa və onları cinayət məsuliyyətinə cəlb etməyə imkan verəcəkdir.

Kriminalistik ədəbiyyatda kibercinayətlərin istintaqı metodikasının işlənilib hazırlanması məsələlərinə diqqətin artırılmasına baxmayaraq bu sahədə bir sıra həll edilməmiş və diskussiya doğuran məsələlər hələ də qalmaqdadır. Ona görə də bu növ cinayətlərin istintaqı metodikasının işlənib hazırlanması kibercinayətkarlıqla mübarizə sahəsində ilk növbədə həlli vacib olan vəzifələrdən biridir.

Kibercinayətlərin istintaqı metodikasının əsas elementlərindən biri olan kriminalistik xarakteristika kompleks şəkildə işlənib hazırlanmalı, bu sahədə cinayətlərin törədilməsi və gizlədilməsi üsulları, kibercinayətkarın şəxsiyyəti haqqında sistemləşdirilmiş və ümumiləşdirilmiş məlumatlar bankı yaradılmalıdır. Hadisə yerinə baxış, dindirmə, axtarış, rəqəmsal ekspertizaların təyini kimi əsas istintaq hərəkətlərinin keçirilməsinin taktiki-kriminalistik xüsusiyyətlərinin də mükəmməl, elmi zəmin əsasında işlənilməsinə xüsusi diqqət yetirilməlidir.

Kibercinayətlərə qarşıdurmanın kriminalistik və prosessual aspektlərinin tədqiqi, bu ictimai təhlükəli əməllərə səmərəli qarşıdurma səviyyəsinin yüksəldilməsi üzrə təkliflərin və tövsiyələrin işlənib hazırlanması məqsədilə aşağıdakı problemlər kompleksinin həlli zəruri hesab edilməlidir:

- kibercinayətlərin anlayışının formulə edilməsi və səciyyəvi kriminalistik əlamətlərin üzə çıxarılaraq sistemləşdirilməsi;
- müasir reallıqlar nəzərə alınmaqla kibercinayətlərin kriminalistik təsnifatının işlənib hazırlanması;
- informasiya-kommunikasiya texnologiyalarından istifadə etməklə törədilən cinayətlərin açılması və istintaqı sahəsində beynəlxalq-hüquqi standartların, xarici ölkələrin müsbət təcrübəsinin öyrənilməsi və təhlili;
- xarici ölkələrin cinayət və cinayət-prosessual qanunvericiliyinin, beynəlxalq-hüquqi sənədlərin analizi əsasında ictimai münasibətlərin rəqəmsallaşması şəraitlərində milli cinayət və cinayət-prosessual qanunvericiliyinin modernləşdirilməsinin və təkmilləşdirilməsinin əsas istiqamətlərinin müəyyən edilməsi;
- kibercinayətkarın və kiberxarakterli cinayətləri törədənlərin ümumiləşdirilmiş kriminalistik portretinin işlənib hazırlanması;
- müasir şəraitlərdə kibercinayətlərin törədilməsinin daha çox yayılmış və daha təhlükəli olan üsullarının müəyyən edilərək sistemləşdirilməsi;
- kibercinayətlərin açılması və istintaqının elmi-nəzəri, təşkilati-texniki, texnoloji və kriminalistik təminatının təkmilləşdirilməsinin əsas istiqamətlərinin müəyyən edilməsi;
- kibercinayətlərin tövsifinin, bu cinayətlərin açılması və istintaqının problemli məsələləri üzrə hakimlər, prokurorlar, müstəntiqlər və digərləri üçün nəzərdə tutulmuş praktiki tövsiyələrin işlənib hazırlanması;
- kibercinayətlərin hər bir növünün kriminalistik xarakteristikasnın və bu xarakteristikaların struktur elementlərinin müəyyən edilməsi, onların mahiyyət və məzmununun açılması.

Ədəbiyyat siyahısı:

1. Cavadov F.M., Abdullayev Y.S. Kompüter informasiyası sahəsində cinayətlərlə mübarizə təcrübəsindən //Hüquqi dövlət və qanun. 2000, №7-8, s.40-41.

2. İbrahimova A.N. Kibertəhlükələr və onların təsnifatı//Bakı universitetinin xəbərləri. Sosisal-siyasi elmlər seriyası. 2020. №1.

3. Qasımov V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq. Bakı, 2007, s.144-147.

4. Mahmudov A.M., Əliyev V.Ə. Kriminalistika: sxemlər, şərhlər, terminlər (tədris-metodik vəsaiti). B., 2003, s.167-168.

5. Chang L., Grabosky P. Cybercrime and Establishing a Secure Cyberworld//The Handbook of Security. London, Palgrave Macmillan Publ., p.321-339.

6. Bonettini N., Guera D., Bondi L., Bestagini P. Image anonymization detection with deep handcrafted features. Conference: IEEE International Conference on Image Processing (ICIP), Cept. 2019.

7. Cybercrime and Digital forensics. Introduction/T.J.Holt, A.M.Bossler, K.c. Seigfried-Spellar. Abingdon-Routledge, 2018, 754p.

8. Richet J.L. Hoü Cybercriminal Communites Groü ChangeI A study of communities Engaged in advertising fraud//Technological and Social Change, 2022, vol. 17.

9. Преступления, совершаемые с использованием информационных технологий: пробелмы квалификации и особенности расследования: монография/А.Ф.Абдулваиев, А.В.Белаусов, Ж.В.Вассалатий и др.; под науч.ред.проф.Е.В.Смахтина, проф.Р.Д.Шарапавова, доц. В.И.Морозова. Тюмень: Издательство Тюменского государственного университета, 2021.

10. Агапов П.В., Борисов С.В. Вагурин Д.В., Коренюк А.Л, и др. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография. М., 2014, с.35.

11. Бирюкова Ю.В. Хищения, совершаемые с использованием компьютерных и телекоммуникационных технологий, способы итх совершения и пути их расследования//Вестник экономической безопасности. 2020. №3, с.179-184.

12. Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, так и борьбы с ними//Вестник Московского университета МВД России. 2022. №1, с.60-61.

13. Вершинин М. Современные молодежные субкультуры: хакеры. URL: http://yurpsy.com/files/xrest/2/222.htm

14. Вехов В.Б. Компьютерные преступления: Способы совершения, методики расследования. М.: Право и Закон, 1996.

15. Давыдов В.О. Исследование криминалистически значимой информации в ходе расследования экстремистских преступлений, совершенных с использованием компьютерных сетей//Известия Тульского государственного университета. 2013. №1-2, с.57-62.

16. Зайцев А.А., Смолин А.В. О некоторых элементах криминалистической характеристики киберпреступлений//Криминалистика: вчера, сегодня, завтра. 2019. №3(11), с.35-41.

17. Зуев С.В. ИТ-справочник следователя: монография/С.В.Зуев.- М.: Юрлитинформ, 2019, 232с.

18. Ищенко Е.П. О технологии искусственного интеллекта в криминалистике //30 лет юридической науки КубГАУ: сб.науч.трудов по материалам Всерос.науч.-практ.конф. с международ. Участием / Под ред В.Д.Зеленсского. Краснодар: Кубан.гос.аграрный ун-т им. И.Т.Трубилина, 2021, с.375-380.

19. Киселев А.С., Горбунова К.А. Особенности криминалистической характеристики преступлений в сфере компьютерной информации//Актуальные проблемы государства и права. 2023. Т.7. №3.

20. Копырин М.Ю., Журбенко А.М. Некоторыен аспекты расследования преступлений, связанных с мошенничеством в сети «Интернет»//Образование. Наука. Карьера: сб.науч.ст.межд.науч-метод. конф. В 2-х тт. Отв.ред. А.А.Горозов. 2018, с.218-220.

21. Курс криминалистики. В трех томах. Т.3. Криминалистическая методика: Расследование преступлений в сфере экономики, взятничества и компьютерных преступлений /Под ред. О.Н.Коршуновой и А.А.Степанова. СПб., 2004, с.451-452.

22. Могунова М.М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг)//Вестник Саратовской государственной юридической академии. 2020. №4(135), с.135-141.

23. Мустафаев М.Х., Аббасова И.С. Понятие криминалистической характеристики преступной деятельности и ее взаимосвязь с предметом криминалистики (первая часть)//Пробелы в российском законодательстве. 2016. №8, с.302.

24. Павликов С.Г.К вопросу о значении теории криминалистической характеристики преступлений// Российский судья.2012. №10, с.45-47.

25. Поляков В.В. Использование сети Интернет при совершении преступлений против детей. Сб.мат. криминалистических тений. 2014. №10.

26. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики//Известия Алтайского государственного университета. 2013. №2-1(78).

27. Поляков В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет//Известия Алтайского государственного университета. 2016. №3(91), с.142-144.

28. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуцникационных технологий, и проблемы их квалификации. Автореферат диссертации на соискание ученой степени доктора юридических наук. М., 2020.

29. Самойлов А.В. Современное состояние учения о криминалистической характеристике преступлений//Российский следователь. 2010. №22, с.5-6.

30. Седых Д.Ю., Лунев Д.Ю., Вильсон Н.Г. Форензика как наука о расследовании киберпреступлений// 20-я Юбилейная международная молодежная научно-практическая конференция «Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2024». 7-11 октября 2024. Севастополь, 2024.

31. Файзуллина А.А. К вопросу о соотношении понятий «криминалистическая характеристика преступлений» и «следственная ситуация»//Инновационная наука. 2017. №2-2, с.140-142.

32. Харисова З.И. Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации//Правовая государство: теория и практика. 2025. №2(80), с.96-105.

33. Шаталов А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции// Вестник Сибирского юридического института МВД России. 2018. №3(32), с.8-9.

34. Шмонин А.В. Методология криминалистической методики: монография. М.: Юрлитинформ, 2010, с.156.

35. Яким А.Д. Нейронная сеть как инструмент совершения преступлений// Проблемы проитводействия киберпреступности: материалы 2-й международной научно-практической конференции (Москва, 26 апреля 2024 года)/Под общ.ред. О.Ю.Антонова, Э.Б.Хатова. М.: Московская академия Следственного комитета имени А.Я.Сухарева, 2024, с.138-140.

XÜLASƏ

Məqalədə kibercinayətkarlığın kriminalistik xarakteristikası, onun strukturu və əsas struktur elementləri, əsas elementlərin mahiyyət və məzmunu nəzərdən keçirilərək araşdırılmışdır. Kibercinayətkarlığın informasiya-texnoloji inqilabın məhsulu olduğu qeyd olunmuş, cinayətkarlığın bu yeni növünün ictimai təhlükəliliyi, onun xarakterik xüsusiyyətləri göstərilmişdir. Kibercinayətkarlıqla beynəlxalq-hüquqi səviyyədə mübarizəyə istiqamətlənmiş 2001-ci il taixli Avropa Şurası Konvensiyasında, habelə 2024-cü il tarixli kibercinayətkarlığa qarşı BMT konvensiyasında nəzərdə tutulmuş kibercinayətlərin növləri, kibercinayətlərə görə məsuliyyət nəzərdə tutan Azərbaycan Respublikasının Cinayət Məcəlləsinin normaları qeyd olunmuşdur. Kibercinayətlərin səciyyəvi kriminalistik xüsusiyyətləri göstərilmiş və bu kriminal əməllərin kriminalistik xarakteristikasının anlayışı verilmiş, bu kriminalistik kateqoriyanın

cinayətlərin açılması və istintaqında rolu və əhəmiyyəti qeyd olunmuşdur. Kibercinayətlərin kriminalistik xarakteristikasının anlayışı verilmiş, onun strukturunu təşkil edən elementlər sistemləşdirilmişdir. Kibercinayətlərin kriminalistik xarakteristikasının kibercinayətkarın şəxsiyyəti və kibercinayətlərin törədilməsi üsulları daha ətraflı şəkildə təhlil edilmişdir. Kibercinayətkarların əsas tipləri və növləri, bu kateqoriyalı əməllərin törədilməsinin səciyyəvi üsulları göstərilmişdir. Kibercinayətlərə qarşıdurmanın kriminalistik aspektlərdən tədqiqi, bu ictimai təhlükəli əməllərə səmərəli qarşıdurma səviyyəsinin yüksəldilməsi üzrə təkliflərin və tövsiyələrin işlənib hazırlanması məqsədilə həlli zəruri olan problemlər kompleksinin dairəsi müəyyən edilmişdir.

CRİMİNALİSTİC CHARACTERİSTİCS OF CYBERCRİMES*LAMİA SULEYMANOVA*

Senior Expert, Department of Technical Expertise of Documents,
Forensic Science Center Ministry of Justice

SUMMARY

The article examines and examines the criminalistic characteristics of cybercrime, its structure and main structural elements, the essence and content of the main elements. It is noted that cybercrime is a product of the information-technological revolution, the social danger of this new type of crime, its characteristic features are shown. The types of cybercrimes provided for in the 2001 Council of Europe Convention on the International-Legal Fight against Cybercrime, as well as the 2024 UN Convention against Cybercrime, and the norms of the Criminal Code of the Republic of Azerbaijan, which provide for liability for cybercrimes, are noted. The specific criminalistic characteristics of cybercrimes are shown and the concept of the criminalistic characteristics of these criminal acts is given, the role and importance of this criminalistic category in the detection and investigation of crimes are noted. The concept of the criminalistic characteristics of cybercrimes is given, and the elements that make up its structure are systematized. The criminalistic characteristics of cybercrimes, the identity of the cybercriminal and the methods of committing cybercrimes have been analyzed in more detail. The main types and varieties of cybercriminals, the typical methods of committing acts of this category have been shown. The scope of the complex of problems that must be solved in order to study the fight against cybercrimes from criminalistic aspects, develop proposals and recommendations for increasing the level of effective fight against these socially dangerous acts has been determined.

SİBER SUÇLARIN KRİMİNALİZM ÖZELLİKLERİ

LAMİA SULEYMANOVA

Adalet Bakanlığı Adli Uzmanlık Merkezi Belge Teknik Uzmanlık Dairesi Kıdemli Uzmanı

ÖZET

Makalede, siber suçun kriminalistik özellikleri, yapısı ve temel yapısal unsurları, bu unsurların özü ve içeriği incelenmekte ve incelenmektedir. Siber suçun bilgi-teknolojik devrimin bir ürünü olduğu, bu yeni suç türünün toplumsal tehlikesi ve karakteristik özellikleri gösterilmektedir. 2001 tarihli Avrupa Konseyi Siber Suçlarla Uluslararası Hukuki Mücadele Sözleşmesi'nde ve 2024 tarihli BM Siber Suçlarla Mücadele Sözleşmesi'nde öngörülen siber suç türleri ve siber suçlardan sorumluluğu öngören Azerbaycan Cumhuriyeti Ceza Kanunu normları belirtilmektedir. Siber suçların kendine özgü kriminalistik özellikleri gösterilmekte ve bu suç eylemlerinin kriminalistik özellikleri kavramı ortaya konulmakta, bu kriminalistik kategorinin suçların tespiti ve soruşturulmasındaki rolü ve önemi vurgulanmaktadır. Siber suçların kriminalistik özellikleri kavramı ele alınmakta ve yapısını oluşturan unsurlar sistemleştirilmektedir.

Siber suçların kriminal özellikleri, siber suçlunun kimliği ve siber suçları işleme yöntemleri daha ayrıntılı olarak analiz edilmiştir. Siber suçluların başlıca türleri ve çeşitleri, bu kategorideki eylemleri işlemenin tipik yöntemleri ortaya konmuştur. Siber suçlarla mücadeleyi kriminal açıdan incelemek, bu toplumsal açıdan tehlikeli eylemlerle etkili mücadele düzeyini artırmak için öneriler ve tavsiyeler geliştirmek için çözülmesi gereken sorunlar kompleksinin kapsamı belirlenmiştir.

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ

ЛАМИЯ СУЛЕЙМАНОВА

Старший эксперт Отдела Технической экспертизы документов Центра Судебной Экспертизы Министерства Юстиции

РЕЗЮМЕ

В статье рассматривается и анализируется криминалистическая характеристика киберпреступности, её структура и основные структурные элементы, сущность и содержание основных элементов. Отмечается, что киберпреступность является порождением информационно-технологической революции, раскрывается социальная опасность этого нового вида преступлений, раскрываются её характерные черты. Отмечаются виды киберпреступлений, предусмотренные Конвенцией Совета Европы о международно-правовой борьбе с киберпреступностью 2001 года, а также Конвенцией ООН против киберпреступности 2024 года, и нормы Уголовного кодекса Азербайджанской Республики, предусматривающие ответственность за киберпреступления. Раскрывается специфика криминалистической характеристики киберпреступлений, дается понятие криминалистической характеристики этих преступных деяний, отмечаются роль и значение этой криминалистической категории в раскрытии и расследовании преступлений. Даётся понятие криминалистической характеристики киберпреступлений, систематизируются элементы, составляющие её структуру. Более подробно проанализированы криминалистическая характеристика киберпреступлений, личность киберпреступника и способы их совершения. Показаны основные виды и разновидности киберпреступников, типичные способы совершения деяний данной категории. Определен круг проблем, которые необходимо решить для криминалистического изучения борьбы с киберпреступностью, разработки предложений и рекомендаций по повышению уровня эффективности борьбы с этими общественно опасными деяниями.

Rəyçi: h.f.d. N.İ.Abbasov

Təqdim edən: L.R.Süleymanova

Daxil olma tarixi: 22.07.2025

Təkrar işlənmə tarixi: göndərilməyib

Çapa imzalanma tarixi: 15.09.2025