KIBERCINAYƏTLƏRIN APAŞDIRILMASININ KRIMINALISTIK TƏMINATI

2020

AZƏRBAYCAN RESPUBLİKASI
DAXİLİ İŞLƏR NAZİRLİYİ
POLİS AKADEMİYASI

Kibercinayətlərin apaşdırılmasının kriminalistik təminatı

Dərs vəsaiti

Dərs vəsaiti Azərbaycan Respublikası Daxili İşlər Nazirliyinin Polis Akademiyasının Elmi Şurasının 28 fevral 2020-ci il tarixli 2 nömrəli iclas protokolu ilə təsdiq edilmişdir.

Bakı 2020

Dərs vəsaiti Polis Akademiyasının «Kriminalistika» kafedrasında hazırlanmışdır.

Elmi redaktorlar:
DİN-in Polis Akademiyasının rəisi, polis general- mayoru, hüquq üzrə elmlər doktoru, dosent Nazim Tələt oğlu Əliyev

Polis Akademiyası rəisinin tədris və elmi işlər üzrə müavini, polis polkovniki, h.e.d., professor Mahir Bayram oğlu Əhmədov

Müəlliflər:
DİN-in Polis Akademiyasının "Kriminalistika" kafedrasının rəisi, polis polkovniki, hüquq üzrə fəlsəfə doktoru, dosent Allahverdi Mahmudov

DİN-in Polis Akademiyasının "Kriminalistika" kafedrasının baş müəllimi,polis polkovnik – eytenantı Ələkbər Allahverdiyev

DİN-in Polis Akademiyasının "Kriminalistika" kafedrasının baş müəllimi,polis polkovnik-leytenantı Rasim İsaqov

Rəyçilər:
BDU-nun "Cinayət prosesi" kafedrasının professoru, hüquq elmləri doktoru Midhəd Qəfərov

Milli Aviasiya Akademiyasının «Hüquqşunaslıq» kafedrasının dosenti, hüquq üzrə fəlsəfə doktoru Şöhlət Kərimov

MÜNDƏRICAT

Giriş

Cinayətkarlıqla mübarizə fəaliyyətində vacib əhəmiyyət kəsb edən istiqamətlərdən biri onun elmi cəhətdən təminatı sayılır. Bu baxımdan respublikamızda hüququn müxtəlif sahələrini əhatə edən fundamental elmi tədqiqatların aparılmasını təqdirəlayiq hal kimi qiymətləndirmək olar. Müasir dövrdə internetdən, elektron və rəqəmsal texnologiyalardan istifadənin sosial həyatımızın tələbatından irəli gəlməsini nəzərə alasaq, yanılmadan qeyd edə bilərik ki, aktuallıq təşkil edən belə sahələrdən biri də kibercinayətkarlıqla mübarizədir.

Son illərdə bu sahədə baş verən hüquqazid əməllər isə onun cinayət huquqi, cinayət prosessual, kriminalistik aspektlərinin öyrənilməsini və təhlil edilməsini tələb edir. Bu baxımdan kafedrada hazırlanan "Kibercinayətlərin araşdırılmasının kriminalisrik təminatı " adlı dərs vəsaitini həm nəzəri, həm də təcrübi nöqteyi-nəzərdən dəyərli hesab etmək olar.

Vurğulamaq lazımdır ki, qlobal şəbəkədə və informasiya kommunikasiyalarının inkişafı ilə əlaqədar movcud olan texnoloji fəaliyyətin prioritet sahələrində əsas insan huquq və azadlıqlarının, soz və ifadə azadlığının, şəxsi həyatın, şəbəkə istifadəçiləri haqqında məlumatların, habelə onların əqli mulkiyyət huquqlarının qorunması, xususilə muasir informasiya cəmiyyəti ucun daha aktual olan problem kibercinayətkarlıqla mubarizə məsələləri ön planda

cıxış edir. Aparılan təhlillər göstərir ki kompyuter sistemlərinin geniş yayılması, onların kommunikasiya sistemləri vasitəsilə əlaqələndirilməsi, bu sistemlərə elektron müdaxilə imkanını artırır. Ona görə də kibercinayətkarlıq təhlükəsi bütün dünya ölkələri kimi Azərbaycan üçün də aktuallıq təşkil edir və bu təhlükənin qarşısını almaq məqsədilə ölkəmizdə müvafiq qurumlar tərəfindən səmərəli tədbirlər həyata keçirilir.

Ölkəmizdə də artıq kibercinayətlərin təşəkkül tapmasını nəzərə alaraq bu istiqamətdə araşdırmanın xüsusiyyətlərinin nəzəri aspektlərinin tədqiqi, keçirilən əməliyyat-axtarış tədbirlərinin və istintaq hərəkətlərinin taktikası üzrə zəruri vərdiş və bacarıqların aşılanması, həmçinin onların təkmilləşdirilməsi zamanın tələbindən irəli gəlir.

1.**Kibercinayətkarlığın mahiyyəti və xarakterik xüsusiyyətləri**

Kibercinayətkarlıq – kompyuter sistemi və şəbəkələrinin, həmçinin buna imkan verən digər vasitələrin köməyi ilə kiberməkana daxil olmaqla kompyuter sistemləri və şəbəkələri çərçivəsində, eləcə də onların əleyhinə olaraq kibermühitdə törədilən və cinayət qanunvericiliyi ilə təhdid olunan əməllər başa düşülür. BMT mütəxəssislərinin fikrincə "kibercinayətkarlıq" termini kompyuter sistemləri və şəbəkələri vasitəsilə və ya kompyuter sistemləri və şəbəkələri çərçivəsində, eləcə də onların əleyhinə törədilən istənilən cinayəti əhatə edir. Beləliklə,

kibercinayətlərə elektron mühitdə törədilən istənilən cinayət aid edilə bilər.

Bu növ cinayətkarlığın nəinki milli səviyyədə, həmçinin qlobal səviyyədə qarşısının alınması və onunla mübarizənin hüquqi vasitələrinin hazırlanması baxımından çox zəruridir. Bununla belə BMT-nin cinayətkarlığın qarşısının alınması və qanunu pozanlarla davranış üzrə X Konqresi kibercinayətkarlıq probleminə toxunaraq kibercinayətkarlıq və kibercinayət anlayışlarının müəyyən olunması üçün tövsiyyələr vermişdir. Kompyuterlər, eləcə də kompyuter şəbəkələri ilə əlaqəli cinayətkarlıq problemi üzrə simpoziumda BMT mütəxəssisləri tərəfindən kibercinayətlərin dar və geniş mənada şərhi verilmişdir.

Kibercinayətlər dar mənada (kompyuter cinayətləri): elektron əməliyyatlar vasitəsilə törədilən və əsas məqsəd kimi kompyuter sistemləri, eləcə də onlar vasitəsilə işlənən məlumatların təhlükəsizliyi çıxış edən istənilən qanuna zidd əməllərdir.

Kibercinayətlər geniş mənada (kompyuterlərlə əlaqəli cinayətlər kimi): kompyuter vasitəsilə və ya kompyuterlər, kompyuter sistemləri və şəbəkələri ilə əlaqəli olan, eləcə də kompyuter sistem və şəbəkələri vasitəsilə informasiyanın qanunsuz əldə olunması, təklifi və ya yayılmasını özündə birləşdirən istənilən qanuna zidd əməllərdir. Bütün deyilənləri ümumiləşdirərək kibercinayətləri belə şərh etmək olar. Kibercinayətlər - kompyuterlərin, kompyuter

proqramlarının, kompyuter şəbəkəsinin işinə müdaxilə, kompyuter məlumatlarının icazəsiz modifikasiyası, eləcə də kompyuterlərin, kompyuter şəbəkə və sistemlərinin birbaşa və ya dolayı istifadə etməklə törədilən digər qanunazidd ictimai təhlükəli və qanunla cəzalandırılan əməllərdir. Eyni zamanda Azərbaycan Respublikasında informasiya sahəsində milli təhlükəsizliyinin təmin edilməsi istiqamətində məqsədyönlü tədbirlər həyata keçirir və bunlara aiddir:

1)Azərbaycan Respublikasında informa-siyanın, həmçinin dövlət informasiya ehtiyatlarının müdafiəsi sahəsində milli sistemin yaradılması və möhkəmləndirilməsi;

2)dövlət orqanları və vəzifəli şəxslər tərəfindən qərarların qəbul edilməsinin informasiya təminatının həyata keçirilməsi məqsədilə obyektiv və qabaqlayıcı məlumatların toplanılması;

3)informasiya infrastrukturunun inkişaf etdirilməsi;

4)dövlət sirlərinin qorunmasının hüquqi mexanizmlərinin təkmilləşdirilməsi;

5)kibercinayətlərə qarşı mübarizə;

6) informasiya təhlükəsizliyinin və azadlığının təmin olunması.

2.Kibercinayətlərin təsnifatı

Kibercinayətlərin təsnifatı məsələsi də müasir beynəlxalq hüquqda və xarici ölkələrin milli qanunvericiliklərində geniş müzakirə olunan problemlərdəndir.

Avropa Şurasının "Kibercinayətkarlıq haqqında Konvensiyası"nda kompyuter cinayətlərinin 4 növü müəyyən olunmuşdur: qanunsuz daxil olma (2-ci maddə); qanunsuz ələ keçirmə (3-cü maddə); məlumatlara müdaxilə (4-cü maddə); sistemə müdaxilə (5-ci maddə). Kibercinayətlərin məhz bu 4 növü "kompyuter cinayətləri" hesab olunur. Digərləri ya kompyuterlə əlaqəli olan , ya da kompyuter vasitəsilə törədilən cinayətlərdir. Bu cinayətlərə isə aşağıdakılar daxildir: kompyuterlərin bir üsul kimi çıxış etdiyi cinayətlər (elektron oğurluqlar, dələduzluq və s.); törədilməsində kompyuterin alət rolu oynadığı əməllər (saytlarda milli, dini, irqi münaqişəni qızışdıracaq informasiyanın yerləşdirilməsi və s.) Kibercinayətkarlığın bu iki növü müzakirə obyekti kimi çıxış edir. Bəzi xarici tədqiqatçılar hesab edir ki, bu cinayətlər müasir texnikalar vasitəsilə törədilən qanuna zidd əməllərdən başqa bir şey olmamaqla, artıq mövcud olan milli cinayət qanunvericiliklərində öz əksini taparaq heç də yeni növ cinayətlər deyillər. Digərləri isə hesab edir ki, kibercinayətlər cinayətlərin keyfiyyətcə yeni kateqoriyası olmaqla, beynəlxalq səviyyədə qarşısının alınması məqsədilə yeni normaların, tədqiqat metodlarının işlənib

hazırlanmasını tələb edir. Həqiqətən də, internet vasitəsilə törədilən bir çox cinayətlər yeni növ qanuna zidd əməllər hesab olunmur. Məsələn, dələduzluq mülkiyyət əleyhinə cinayət hesab olunur və onun internet vasitəsilə törədilməsi yeni tərkib yaratmır. Lakin bu cinayətin törədilmə üsulu yeni qanunvericilik normalarının və tədqiqat metodlarının işlənib hazırlanmasını tələb edir. Bu həm də onunla şərtlənir ki, kibercinayətlər əksər hallarda dövlət qanunvericiliyi çərçivəsindən çıxaraq transmilli xarakterə malik olurlar. Bununla yanaşı cinayətlərin virtual xarakteri dəlillərin tez bir zamanda məhv edilməsinə imkan yaradır ki, bu da cinayətkarın axtarışlarını daha da çətinləşdirir. Kompyuter cinayətləri nəticəsində vurulan zərərin aşağıdakı növləri mövcuddur[1].

1.Funksiyaların pozulması. Funksiyaların pozulmasının da 4 növü var ki, bu pozuntular aşağıdakı səbəblər üzündən baş verir.

− iş qrafiklərində, bu və ya digər fəaliyyət cədvəllərində dolaşıqlıqlara səbəb olan müvəqqəti pozuntular;

− sistemin istifadəçilər üçün əlçatmazlığı, cihazların zədələnməsi, proqram təminatının pozulması;

2.Əhəmiyyətli resursların itməsi. Kompyuter cinayətlərinin predmeti əsasən pul, əşya, xidmət,

---

1 Батурин Ю.М. Проблемы компьютерного права. - М.: Юрид. лит., 1991. - 272 с. 25

informasiya və s. olur. Cinayətkarların daha çox üstünlük verdiyi qəsd predmeti qismində isə pul çıxış edir. Bununla yanaşı informasiyanın - proqram təminatı və EHM yaddaşında olan məlumatların oğurlanması da geniş yayılmışdır.

3.Hüquqların pozulması. Kibercinayətlərin törədilmə üsulları isə çoxtərəfli olmaqla aşağıdakılardan ibarətdir:

1)Kompyuter texnikasının məhv edilməsi:

− avadanlıqların məhv edilməsi;

− informasiya daşıyıcılarının məhv edilməsi; − faylların məhvedilməsi (silinməsi);

− maşın daşıyıcılarında saxlanan informasiyaya icazəsiz girişdən müdafiə edən vasitələrin silinməsi.

2)Kompyuter texnikası obyektlərinin dəyişdirilməsi:

− avadanlıqların zədələnməsi;

−faylların icazəsiz dəyişdirilməsi (modifikasiyası);

− kompyuter sistemi informasiyasını icazəsiz müdaxilədən müdafiə edən vasitələrin icazəsiz dəyişdirilməsi;

− kompyuter sistemlərinin işinin bloklanması; − kompyuter sisteminə kənar, yad proqram vasitələrinin icazəsiz quraşdırılması.

3)Kompyuter texnikası obyektlərinin götürülməsi:

− avadanlıqların oğurlanması;

− hər hansı informasiya daşıyıcılarından informasiyanın oğurlanması;

− faylların sürətinin çıxarılması.

4)Oğurluq: maddi qiymətlilərin, pul və xidmətlərin, həmçinin müxtəlif məqsədlər üçün informasiyanın oğurlanması.

5)İcazəsiz giriş: icazəsiz olaraq maşın daşıyıcılarında saxlanan informasiyanın işlənməsi proqramının işə salınması.

Beləliklə, kibercinayətlərə aid edilən hücumların obyektlərini üç qrupa ayırmaq olar: − kompyuterlərin özləri; kompyuterdən yalnız üsul kimi istifadə edilərək hücum oluna bilən obyektlər; kompyuterin vasitə kimi çıxış etdiyi hücumların obyektləri. Kibercinayətləri törədən şəxsləri də 3 böyük qrupa ayırmaq olar ki, bunlar aşağıdakılardır: zərərçəkmiş təşkilatlarla heç bir əmək münasibətində olmamasına baxmayaraq müəyyən əlaqələri mövcud olan şəxslər; təşkilatda məsuliyyətli vəzifə daşıyan işçilər; öz vəzifə səlahiyyətlərindən sui-istifadə edən EHM-lərlə iş üzrə təşkilat işçiləri. Mütəxəssislər - kiberhücumlar törədən şəxsləri və təşkilatları şərti olaraq bir neçə kateqoriyaya ayırır. Bunlar aşağıdakılardır:

1.Xakerlər. Bu kateqoriyaya kompyuter texnologiyaları sahəsində yüksək biliyə sahib olan və kompyuter sistemlərinin zəif nöqtələrinin tapılması məqsədilə saatlarla kompyuterlə məşğul olan şəxslər daxildir.

2.Xaktivistlər. “Xaktivizm” termini elmi ədəbiyyata ilk dəfə kompyuter cinayətkarlığı üzrə

mütəxəssis D.Denninq tərəfindən gətirilib [2], belə ki, "hack" və "activism" sözlərinin birləşməsi olan bu termin yeni hal kimi qiymətləndirilən sosial etirazları ifadə etmək üçün istifadə olunur. Xaktivizm hər hansı bir şey əleyhinə etiraz məqsədi daşıyan sosial aktivliklə xakerliyin sintezi kimi başa düşülür. Qərb analitikləri qeyd edirlər ki, xakerlərin siyasiləşməsi və eləcə də sosial etiraz aktivistlərinin son vaxtlar daha çox İnternetə meyl etməsi ilə bu fəaliyyətin kompyuterləşməsi "kiberaktivistlərin" sayının artmasına səbəb olmuşdur. Bu şəxslər vətəndaş itaətsizliyinin ənənəvi üsulları əvəzinə "elektron etiraz" kimi yeni üsullardan istifadə etməklə bu hərəkatı kiber mühitə keçirməyə çalışırlar.

3.Kibercinayətkarlar. İnternet şəbəkəsinin geniş yayılması ilə kiber dələduzluq qeyri-qanuni gəlir əldə etməyin əsas növlərindən birinə çevrilmişdir. Onların fəaliyyət sxemi çox sadədir. İlk öncə onlar şəxsi informasiyaya giriş əldə etmək üçün kompyuter sistemlərinə hücum edirlər. Daha sonra isə bu şəxsi informasiyanın aşkara çıxarılması ilə təhdid edərək pul tələb edirlər. Fərdi kompyuter sistemləri ilə yanaşı dövlət orqanlarının kompyuter şəbəkələri də kibercinayətkarların hücumlarına məruz qala bilər.

4.Sənaye cəsusluğu ilə məşğul olan şəxslər. İnkişaf etmiş sənaye dövlətlərində sənaye cəsusluğu uzun tarixə malikdir və yeni texnologiyaların inkişafı ilə

---

[2] .**Международное право. Учебник. Под редакцией А.А.Ковалева, С.В.Черниченко. Издательство. Омега-Л. М. 2006. 832 с.**

cəsuslar qarşısında yeni imkanlar açılmışdır. Cəsusluq dövlətin, təşkilatın eləcə də fərdi "sifarişçilərin" xeyrinə həyata keçirilə bilər.

5.İnsayderlər. "insider" - ingilis dilindən hərfi tərcümədə "daxildən yaxşı məlumatlandırılmış şəxs" mənasını verir. Kompyuter təhlükəsizliyi xidməti içilərinin sistemi xarici hücumlardan qorumaq uğrunda böyük səylərinə baxmayaraq təşkilatlarda həmişə səlahiyyətli işçilər tərəfindən hücum təhlükəsi mövcud olur. İnsayderlərin motivləri işəgötürənə qarşı qisasdan tutmuş terrorçu təşkilata köməyə qədər müxtəlif ola bilər.

6.Məsləhətçilər (müqavilə əsasında işləyən şəxslər): Bir çox təşkilatlar təşkilatın proqram təminatını inkişaf etdirmək məqsədilə kənar təşkilatlarla autsorsinq müqavilələri bağlayır. Bununla da terrorçu əməliyyatlara cəlb olunmuş şəxslərin zəruri informasiya və texniki vasitələrə girişinə imkan yaranır.

7.Terroristlər. Hələki terrorçu qruplar tərəfindən təşkil olunan böyük miqyaslı kiber hücum baş verməsə də, bir çox mütəxəssislərin fikrinə görə terroristlər İnternetdən istifadə etməklə ciddi təhlükə törədə bilərlər[3]. FTB-nin kompyuter texnologiyaları şöbəsinin mütəxəssisləri iddia edirlər ki, kiberterrorizm gələcəkdə ənənəvi terror aktlarının alternativi kimi çıxış edə bilər. Buna isə kibercinayətlərin aşağıdakı xüsusiyyətləri şərait yaradır: anonimlik; məqsədlərin çox növlüyü; aşağı dəyərə malik olması; istənilən

ərazidən fəaliyyət imkanı; az miqdarda resurs tələb etməsi.

Kibercinayətlərdən müdafiə olunmaq məqsədilə üç istiqamətdə iş aparılmalıdır.

- cinayətkarların tutulması. Bu məqsədlə isə ilk növbədə kibercinayətlər haqqında qanunvericilik normaları işlənib hazırlanmalıdır;

- kibercinayətlərin törədilməsinə görə cəza tədbirlərinin təkmilləşdirilməsi;

- informasiyanın qorunması məqsədilə kompleks tədbirlərin həyata keçirilməsi.

Sadalanan bu istiqamətlər ictimai təhlükə hesab olunan kibercinayətlərinin qarışısının alınmasına yönəldilir.[3] Ən geniş yayılmış təsnifat daha öncə də qeyd edildiyi kimi kibercinayətlərin "kompyuter cinayətlərinə" və "kompyuter vasitəsilə törədilən cinayətlərə" bölgüsüdür.

Konvensiyada öz əksini tapmış bu təsnifat tam əhatəli və sabit təsnifat hesab oluna bilməz. Belə ki, elmi-texniki tərəqqinin inkişafı və kibermühitdə ictimai münasibətlərin genişlənməsi bu siyahının artacağını istisna etmir. Avropa Şurasının Konvensiyasında təqdim olunan bu təsnifatla yanaşı digər rəsmi, eləcə də qeyri-rəsmi təsnifatlar da mövcuddur. Belə təsnifatlardan biri 1991-ci ildə İnterpolun işçi qrupu tərəfindən hazırlanmışdır. Həmin ildə bu kodlaşma avtomatlaşdırılmış axtarış informasiya sisteminə daxil

---

3 .Международное право. УчебникОтветственный редактор Ю.М.Колосов, Э.С.Кривчикова. М., Международные отношения, 2005. 720с

edilmişdir. Bu təsnifatın üstünlüyü, onun vasitəsilə bir çox kibercinayət növləri və onların törədilmə üsulları haqqında sistemli təsəvvür əldə etmək imkanın mövcudluğundan ibarətdir. Lakin bununla belə bu təsnifatın çatışmayan cəhətləri də mövcuddur. Belə ki, bu təsnifat özündə kiberterrorizm, kiber izləmə və s. kimi yeni yaranmış kibercinayətləri əks etdirmir. Faktiki olaraq bu kodlaşmanı insan həyatı və sağlamlığına birbaşa təhlükə hesab olunmayan cinayətlərin təsnifatı kimi xarakterizə etmək olar. .

Ümumilikdə bu qeyri-qanuni əməlləri aşağıdakı kimi qruplaşdırmaq olar:

1)Kompyuterə qanunsuz daxil olma;

2)Kompyuter məlumatına və ya proqramlarına ziyanvurma;

3) Kompyuter sabotajı;

4)Kommunikasiyaların qanunsuz olaraq dayandırılması və ya kəsilməsi;

5)Kompyuter casusluğu.

Bu qeyd olunan məsələlər kibercinayətlərin anlayışı, növləri və cinayət tərkibi ilə bağlı təfsnifatı əks etdirə bilməz. Birincisi, bu cinayətlərin xarakteri elədir ki, bunlar daim inkişafdadır və texnoloji innovasiyalara həmişə uyğun gəlməlidir. İkincisi isə bunun üçün kibercinayətlərin unversal əsasda müvafiq ayrıca tərifinin müəyyən edilməsi daha məqsədəuyğun olardı. Kibercinayətlər beynəlxalq cinayətlərin sürətlə inkişaf edən sahəsidir. Əksər cinayətkarlar heç bir fiziki və ya virtual sərhədlər tanımadan cinayətkar

fəaliyyətlərinin müxtəlif diapazonunu genişləndirmək üçün sürət, rahatlıq və internetin anonimliyini axtarırlar. İnterpolun mövqeyinə əsasən, kontent təsnifatı həyata keçirilərək, bu cinayətlər üç geniş sahəyə bölünür:

– Kompyuter aparat vasitələrinə və proqram təminatına qarşı hücumlar;

– Maliyyə cinayətləri, onlayn dələduzluq, onlayn maliyyə xidmətlərinə nüfuz etmə;

– Xüsusilə gənclərin alçaldıcı hərəkətləri və ya "seksploitasiya" formalarından sui-istifadə etməsi. Kibercinayətlərin müxtəlif qəsd obyektlərinə, predmetlərinə və törədilmə xüsusiyyətlərinə münasibətdə müxtəlif növləri fərqləndirilir. Qeyd olunmalıdır ki, əslində kibercinayətlərlə bağlı yetkin elmi anlayışın verilməsi üçün onun növləri məsələsinə diqqətin ayrılması və bu əməllərin tərkib elementlərinin qruplaşdırılması mühüm təcrübi və elmi əhəmiyyətə malikdir. Müxtəlif ədəbiyyatlarda, beynəlxalq və milli hüquqi normalarda bununla bağlı fərqli bölgülərin aparılmasını nəzərə alaraq, onların bəzilərini araşdırmağa cəhd edəcəyik. Təhlillər göstərir ki, hüquqi qüvvəsinə görə kibercinayətlərin Kibercinayətkarlıq haqqında 2001-ci il Budapeşt Konvensiyasına müvafiq olaraq aparılan bölgüsü daha mükəmməl və məqsədəmüvafiqdir.

Həmçinin, bu Konvensiya əsasında aparılan təsnifat əksər beynəlxalq hüquq mütəxəsisləri və alimləri tərəfindən təqdir olunmaqla, müasir

beynəlxalq hüquqda və hətta bu sənədi ratifikasiya etməyən xarici ölkələrin milli hüquq sistemlərində də etalon kimi qəbul edilməkdədir. Kibercinayətkarlıq haqqında Konvensiyaya (və ona əlavə Protokola) görə kibercinayətləri beş əsas qrupa bölmək olar:

1) Kompyuter məlumatları və sisteminin konfidensiallığı, bütövlüyü, o cümlədən qeyri-qanuni çıxış, qeyri-qanuni ələ keçirmə, verilənlərə müdaxilə, sistemə müdaxilə və s. əleyhinə olan kibercinayətlər;

2) Kompyuterdən istifadə ilə əlaqədar, yəni kompyuterin cinayəti törətmə vasitəsi kimi, xüsusilə informasiya ilə manipulyasiya vasitəsi kimi törədilən kibercinayətlər. Bu qrupa əsasən kompyuter dələduzluğu və kompyuter saxtakarlığı aiddir.

3) Kompyuter şəbəkəsində yerləşdirilmiş verilənlərin məzmunu ilə əlaqədar kibercinayətlər. Qeyd etmək lazımdır ki, bu qrup cinayətlər ictimai təhlükəlilik dərəcəsinə görə və praktiki nöqteyi-nəzərindən daha ciddi xarakteri ilə diqqəti cəlb edir. Belə ki, bütün dövlətlər tərəfindən xüsusi önəm verilən uşaq pornoqrafiyası və ümumilikdə internetdə yayılan pornomateriallar ilə bağlı cinayətlər bu qrupa aid edilə bilər. Hazırda kompyuter şəbəkələrində, İnternetdə, Facebook, Tvitter, İnstagram və digər sosial şəbəkələrdə kontent məsələsində ciddi problemlər yaşanmaqdadır. Bu mənada kontent cinayətlərinin elmi baxımdan daha dəqiq və müasir beynəlxalq hüquqa uyğun şəkildə balanslaşdırılmış qaydada araşdırılması zəruridir. Çünki, bu zaman kibercinayətlərlə mübarizə

məsələsində insan hüquqları amili, o cümlədən şəxsi həyata, ifadə azadlığına müdaxilə problemləri xüsusilə aktual olacaqdır.

4) Şəbəkədə müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər. Yəni, "intellekt oğurluğu cinayətləri" son dövrlərdə aktualdır. Çünki, hazırda müasir beynəlxalq hüquqda, eyni zamanda milli qanunvericilik sistemlərində xüsusilə internetdə plagiatlıq, köçürmələr, CD, DVD və s. musiqi, habelə digər fayl və məlumatların qanunsuz olaraq yüklənməsi ilə müəllif və əlaqəli hüquqların kobud və kütləvi şəkildə pozulması faktları müşahidə edilməkdədir. Bu səbəbdən də, dövlətlər qeyd olunan istiqamətdə səylərini birləşdirməklə kibercinayətkarlığın bu növü ilə mübarizənin yeni formalarını düşünməyə başlamışlar.

5) Bu qrupa aid kibercinayətlərə kompyuter şəbəkələri vasitəsilə yayılan və törədilən rasizim və ksenofobiya aktlarını aid etmək olar. Bunlar eyni zamanda yeni nəsil cinayətlər də adlandırılır. Qeyd olunmalıdır ki, bu növ cinayətlər "Kibercinayətkalıq haqqında" Avropa Konvensiyasına Əlavə Protokolda da öz əksini tapmışdır.

Yuxarıda qeyd olunan təsnifatdan bir daha aydın olur ki, müasir dövrdə kibercinayətlərin diapazonu doğurdan da özünün geniş əhatəliliyi ilə diqqəti cəlb edir və bu hüquqazidd əməllərlə mübarizə aparılması əslində bütün digər cinayətləin də qarşısının alnması

və profilaktikasına özünün müsbət təsirini göstərə bilər.

Kibercinayətlər sahəsində tanınmış ekspertlər S. Holberq və A. Hubbard yazır ki, kompyuter cinayətləri özündə bütün cinayət növlərini ehtiva edə bilər ki, buraya da kompyuter texnologiyalarının istifadəsi, təfərrüatları və informasiya ilə əlaqədar məsələlər aid edilməlidir. Bir sözlə müəlliflər kibercinayət kateqoriyasına kompyuter sistemləri və şəbəkələri, o cümlədən internet infrastrukuru əleyhinə yönələn hücumları, bundan əlavə, internet saxtakarlığı və dələduzluğunu da aid edirlər. Azərbaycanlı alim, prof. R. Əliquliyev isə kibercinayətləri iki qrupa bölür: yalnız kiberməkana xas olan cinayətlər-kompyuter və internet vasitəsilə həyata keçirilən ənənəvi cinayətlər. Yalnız kiberməkana xas olan cinayət əməllərinə İnternet casusluğu, kiberdələduzluq, kompyuter informasiyasına qanunsuz daxilolma, xüsusi təyinatlı radioelektron sistemlərinin qanunsuz dövriyyəsi, internetdə maliyyə fırıldaqçılığı və s. daxildir. İnternet vasitəsilə həyata keçirilən ənənəvi cinayətlərə isə həyat və sağlamlıq, şərəf və ləyaqətin alçaldılması, iqtisadi sahədə, ictimai təhlükəsizlik, mülkiyyət əleyhinə olan cinayətlər aiddir. Bura eyni zamanda pornoqrafiyanın yayılması, narkobiznes, konstitusiya quruluşu və dövlət əleyhinə olan cinayətlər də daxildir. Qeyd olunan bölgünün müasir beynəlxalq hüquq nöqteyi-nəzərindən faydasını inkar etmədən, xüsusi

vurğulamaq lazımdır ki, beynəlxalq xarakterli cinayətlər kateqoriyasına aid olmaqla, kibercinayətlər əslində daha çox qəsd obyektləri baxımından təsnifləşdirilməlidir.

Bu səbəbdən də qəsd obyektinə görə kiberməkanda törədilən cinayətlərin fikrimizcə aşağıdakı şəkildə qruplaşdırılması daha məqsədəuyğun olardı: insanın əsas hüquq və azadlıqları əleyhinə olan kibercinayətlər – şəxsi həyat hüququna, söz və ifadə azadlığına olan kiber-müdaxilələr, kiberpiratlıq və s.; iqtisadi kompyuter cinayətləri – kompyuter dələduzluğu, bank hesablarına və postterminallara kiber müdaxilə və s.; ictimai və dövlət maraqları əleyhinə yönələn kibercinayətlər – dövlət orqanlarının və ictimai qurumların veb saytlarının haker hücumlarına məruz qalması, qanunsuz informasiya hücumları və s.; kompyuter məlumatlarının və şəbəkələrinin təhlükəsizliyi əleyhinə olan kibercinayətlər – bunlara istənilən fərdi və şəbəkəyə qoşulan və qoşulmayan hər hansı kompyuterdə, texniki informasiya daşıyıcısında olan məlumatların məxfiliyinin pozulması, onlara müdaxilə və s. aid edilə bilər. Kibercinayətlərin bu cür qruplaşdırılması özünün praktiki əhəmiyyəti ilə də seçilir. Çünki burada qeyd olunan hər bir kibercinayət növü üzrə hazırda beynəlxalq hüquqda bir sıra qurumlar çərçivəsində konkret araşdırma həyata keçirilərək, onlarla səmərəli mübarizə aparılır. Qeyd etmək lazımdır ki, son dövrlərdə kibercinayətlərin ayrı-

ayrı növləri ilə mübarizədə Avropa İttifaqının da xüsusi rolu vardır. Belə ki, bu qurumun daxilində dünyada ilk dəfə olaraq 2013-cü ildə kibercinayətlər üzrə ixtisaslaşmış ayrıca orqan – Avropa Kibercinayət Mərkəzi yaradılmış və fəaliyyəti dövründə kibercinayətlərin müxtəlif növləri üzrə təhqiqat və operativ əməliyyatlar baxımından üzv dövlətlərə yardımlar üzrə səmərəli fəaliyyət göstərmişdir. Evropolun nəzdində formalaşdırılan EC3-ün fəaliyyətinin təhlilindən biz kibercinayətlərin daha yeni təsnifatının şahidi oluruq. Belə ki, bu qurumda aşağıdakı kibercinayət növləri üzrə əməkdaşlıq həyata keçirilir: yüksək texno cinayətlər – kiber hücumlar, zərərli proqram təminatları; uşaqların onlayn cinsi istismarı (online child sexual exploitation); onlayn ödəniş dələduzluğu (payment fraud). Göründüyü kimi, kibercinayət termini o qədər geniş anlayışdır ki, onun cinayət tərkibi ilə bağlı müddəalarının müasir informasiya texnologiyalarının inkişafına müvafiq olaraq və sürətli texnoloji tərəqqi nəzərə alınmaqla genişlənməsi ehtimalı böyükdür.

Umumiyyətlə, Kibercinayətkarlıq haqqında Konvensiyaya görə kibercinayətlərin beş əsas qrupa bölgüsü müasir beynəlxalq hüquq normaları baxımından və xarici ölkələrin milli hüquq sistemlərinə nəzərən optimal və təcrübi əhəmiyyətli təsnifat kimi qəbul edilir. Törədilən hər hansı istənilən cinayətkar fəaliyyət məhz kompyuter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan

informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməl kibercinayətlər kateqoriyasına aid edilir. Kompyuter sistemləri və ya şəbəkəsindən, o cümlədən internetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər ediblərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən danışmaq mümkündür.

3. Kibercinayətkarlıqla mübarizənin hüquqi aspektləri.

Kompyuter cinayətlərinin obyektiv tərəfi hərəkətlə yanaşı hərəkətsizliklə də xarakterizə olunur. Hərəkət (hərəkətsizlik) kompyuter informasiyasının istifadəsi ilə bağlı hüquq və maraqların pozulması ilə əlaqəlidir. Daha öncə də qeyd olunduğu kimi kompyuter cinayətləri maddi tərkibə malikdirlər. Belə ki, bu hərəkət (hərəkətsizlik) şəxsiyyətin, cəmiyyət və ya dövlətin hüquq və maraqlarına əhəmiyyətli zərər vurmalıdır. Lakin AR CM-nin 272-ci maddəsində nəzərdə tutulmuş cinayət əməlləri yəni, elektron-hesablayıcı maşınlar üçün ziyan verici proqramlar yaratma, onlardan istifadə etmə və ya onları yayma istisna olaraq formal tərkibə malik cinayət əməlləridir. Cinayətin nəticələri isə Cinayət Məcəlləsində kompyuter cinayətlərinin növlərinə uyğun olaraq

konkretləşdirilmişdir. Belə ki, cinayət əməlləri və onların nəticələri arasında səbəb-nəticə əlaqəsinin mövcudluğu mütləqdir. Kompyuter cinayətlərinin subyektiv tərəfi təqsirin qəsd formasında ifadə olunmasıdır. AR CM-nin 24-cü maddəsinin 2-ci hissəsində qeyd olunur ki, ehtiyatsızlıqdan törədilmiş əməl (hərəkət və ya hərəkətsizlik) yalnız bu Məcəllənin Xüsusi hissəsinin müvafiq maddəsi ilə nəzərdə tutulmuş hallarda cinayət sayılır. Ehtiyatsızlıqdan törədilmə halı kompyuter cinayətlərinin bəzi növlərinə aid edilməklə CM-nin Xüsusi hissəsinin 272.2 və 273.2-ci maddələrində öz əksini tapmışdır. Kompyuter cinayətinin subyekti ümumidir və 16 yaşına çatmış istənilən fiziki şəxs ola bilər. Lakin CM-nin 271.2.2 və 273.1 maddələrində xüsusi subyektin əlamətləri də göstərilmişdir ki, bu da elektron-hesablayıcı maşınlara, elektron-hesablayıcı maşınlar sisteminə və ya onların şəbəkələrinə daxil olmaq hüququ olan şəxsdir.

Kompyuter informasiyasına qanunsuz olaraq daxil olma (CM-nin 271-ci maddəsi): Cinayətin bilavasitə obyekti qismində kompyuter sistemi sahibinin bu sistemdə saxlanılan informasiyanın toxunulmazlığına olan hüququdur. Bu cinayət əməlinin obyektiv cəhəti isə qanunla qorunan kompyuter informasiyasına, yəni maşın daşıyıcılarda, elektron-hesablayıcı maşınlarda, elektron-hesablayıcı maşınlar sistemində və ya onların şəbəkələrində saxlanılan informasiyaya bu informasiyanın məhvinə gətirib çıxaran qanunsuz daxil olmadır. Bu halda

informasiya dedikdə, informasiya sistemlərində saxlanılan şəxslər, əşyalar, faktlar, hadisələr və proseslər haqqında məlumatlar başa düşülür. Bu informasiyanın iki əsas əlaməti var: - informasiya qanunsuz daxil olmanı həyata keçirən şəxs üçün yad olmalıdır; informasiyaya sərbəst şəkildə daxil olma diğərləri üçün məhdud xarakter daşımalı, həmçinin istifadəçi tərəfindən mühafizə olmalıdır. Qanunla qorunan kompyuter informasiyasına "daxil olma" – şəxs tərəfindən informasiyanın əldə olunması, onun daxil edilməsi və ya informasiyanın işlənməsi prosesinə təsir etmə imkanının əldə olunması və ya istifadə edilməsidir. Bu daxil olma o halda "qanunsuz" hesab edilir ki, şəxs bu əməli kompyuter sistemi və ya şəbəkəsi sahibinin icazəsi və ya digər qanuni səlahiyyəti olmadan törədir. Bu cinayət əməlinin obyektiv cəhətinin məcburi əlaməti sahibkar və ya informasiyanın qoruyucusuna informasiyanın məhv edilməsi, təcrid olunması, modifikasiya olunması, onun surətinin çıxarılması, yaxud EHM-in işinin, sisteminin və ya onların şəbəkəsinin fəaliyyətinin pozulması şəklində zərərin vurulmasıdır. Bu isə o deməkdir ki, öz-özlüyündə kompyuterin əməli yaddaşında və ya maşın daşıyıcılarda (disket, disk və s.) saxlanılan informasiyaya baxılması halı cinayət tərkibi yaratmır. İnformasiyanın məhv edilməsi dedikdə, informasiyanın sadəcə silinməsi deyil, onların yenidən bərpasının qeyri-mümkünlüyünə səbəb olacaq silinməsi başa düşülür.

İnformasiyanın modifikasiya olunması – informasiya sahibinin icazəsi olmadan onun əhəmiyyətli şəkildə dəyişdirilməsi və beləliklə də bu informasiyanın qanuni istifadəsini çətinləşdirən əməldir.

İnformasiyanın təcrid olunması – bu informasiyanın tamlığının qorunub saxlanıldığı halda ona sərbəst daxil olmaya maneələr yaradılması və onun məhdudlaşdırılmasıdır. EHM-in işinin, sisteminin və ya onların şəbəkəsinin fəaliyyətinin pozulması isə kompyuter sisteminin öz funksiyalarını tamamilə və lazımı şəkildə yerinə yetirməməsi, eləcə də sistemin məhsuldarlığının nəzərə çarpacaq dərəcədə azalması halında baş verir. Bu halda fəaliyyətlə nəticələr arasında mütləq şəkildə səbəb-nəticə əlaqəsi qurulmalıdır. Cinayət əməlinin subyektiv cəhəti təqsirin qəsd forması ilə xarakterizə olunur. Şəxs qanunla qorunan kompyuter informasiyasına qanunsuz giriş həyata keçirdiyini dərk edir, törədəcəyi fəaliyyət nəticəsində qanunda qeyd olunmuş zərərli nəticələrin baş verə biləcəyini və ya baş verəcəyini qabaqcadan görə bilir və bunu arzu edir (birbaşa qəsd) və ya buna şüurlu surətdə yol verir . Bu cinayət əməlinin məqsəd və motivləri müxtəlif ola bilər: qərəzli motiv, hər hansı informasiyanın əldə etmək və ya zərər vurmaq istəyi. Motiv və məqsəd cinayət tərkibinin məcburi əlaməti deyildir və onun təsnifləşdirilməsinə təsir etmir. Subyekt qismində 16 yaşına çatmış anlaqlı

fiziki şəxs çıxış edir. Təsnifat əlamətlərinə aşağıdakılar daxildir:

- bu cinayət əməlinin qabaqcadan əlbir olan bir qrup şəxs tərəfindən törədilməsi; İlk əlamətin təsviri CM-nin 34-cü maddəsinin ö 2-ci hissəsində qeyd olunur. Belə ki, "Qabaqcadan razılaşmaqla iki və ya daha çox şəxsin birgə iştirakı ilə törədilən cinayət qabaqcadan əlbir olan bir qrup şəxs tərəfindən törədilmiş cinayət hesab olunur."

- vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə yaxud elektron-hesablayıcı maşınlara, elektron-hesablayıcı maşınlar sisteminə və ya onların şəbəkələrinə daxil olmaq hüququ olan şəxs tərəfindən törədilməsi; Burada vəzifəli şəxslər qismində proqramçılar, EHM-nın operatorları, avadanlıqların sazlayıcıları, ixtisaslaşmış iş yerlərinin mütəxəssis-istifadəçiləri və s.nəzərdə tutulur.

- bu cinayət əməlinin külli miqdarda ziyan vurmaqla törədilməsi. Külli miqdarda ziyan dedikdə, CM-nin 190-cı maddəsinin qeydinə əsasən, ziyan şərti maliyyə vahidinin 7000 mislindən artıq məbləğə bərabər olmalıdır.

Elektron-hesablayıcı maşınlara, elektron-hesablayıcı maşınlar sisteminə və ya onların şəbəkələrinə daxil olmaq hüququ olan şəxs dedikdə isə sistem sahibinin icazəsinə və ya xidməti səlahiyyəti əsasında kompyuter sistemində informasiya almağa, onu daxil etməyə və ya onda əməliyyatları həyata keçirməyə, həmçinin kompyuter avadanlığının texniki

xidmətini həyata keçirən və başqa qanuni əsaslarda kompyuter sisteminə girişə malik olan şəxs başa düşülür. Kompyuter sisteminə girişi olan şəxs bu cinayəti yalnız girişə malik olmadığı informasiyaya daxil olduğu halda törətmiş hesab olunur. Üçüncü əlamət olan

Elektron-hesablayıcı maşınlar üçün ziyan verici proqramlar yaratma, onlardan istifadə etmə və ya onları yayma (CM-nin 272 maddəsi). Bu cinayət əməlinin bilavasitə obyekti EHM-in, onun proqram təminatının və informasiya məzmununun təhlükəsiz istifadəsi üzrə ictimai münasibətlər təşkil edir. Bu maddənin 1-ci hissəsi aşağıdakı əməllərdən birinin törədilməsini nəzərdə tutur:

- informasiyanın icazəsiz məhvinə, təcrid olunmasına, modifikasiya edilməsinə və ya surətinin çıxarılmasına, EHM sisteminin və ya onların şəbəkələrinin işinin pozulmasına səbəb ola biləcək proqramları yaratma;

- mövcud proqramlara analoji halların baş verməsinə səbəb ola biləcək dəyişikliklər etmə;

- yuxarıda qeyd edilən hər iki növ proqramlardan istifadə etmə;

- onları yayma;

- belə proqramlarla yüklənmiş maşın daşıyıcılarından istifadə əetmə;

- belə maşın daşıyıcılarını yayma. Proqramın yaradılması və dəyişdirilməsi dedikdə, EHM dilində yazılmış maşın alqoritminin hazırlanması və

dəyişdirilməsi başa düşülür. Proqramın istifadəsi və onu yayma isə proqramın tətbiq edilməsi və onun tətbiq sferasının genişləndirilməsidir.

Cinayət əməli ziyan verici – virus proqramın yaradılması və ya onun istifadəsi və yayılması ilə başa çatmış hesab olunur. Obyektiv cəhətin cinayət əməlinin törədilməsinin üsul və vasitələrini xarakterizə edən iki məcburi əlaməti var. Bunlar: cinayət əməlinin nəticələri qanunsuz olmalıdır; zərərverici proqramın özünün və ya proqramda belə dəyişikliyin mövcudluğu. CM-in 272-ci maddənin 2-ci hissəsində isə eyni əməllərin ehtiyatsızlıqdan ağır nəticələrə səbəb olması halı qeyd olunmuşdur.

CM-nin 272-ci maddəsinə aid etdikdə ehtiyatsızlıqdan törədilmiş eyni əməlləri belə şərh etmək olar. Cinayət törətmiş şəxs zərərverici proqram yaratdığını, istifadə etdiyini, eləcə də belə proqramı və ya proqram daşıyıcısını yaydığını dərk etmiş, bu əməlin ağır nəticələrə səbəb olma ehtimalını öncədən görə bilmişdir. Lakin kifayət qədər əsas olmadan onun qarşısını alacağını güman etmişdirsə və ya bu əməlin ictimai təhlükəli nəticələr verə biləcəyi imkanını lazımi diqqət və ehtiyatlılıq göstərərək qabaqcadan görməli olduğu və görə biləcəyi halda, onları görməmişdirsə ehtiyatsızlıqdan törətmiş cinayət hesab olunur və CM-nin 272.2 maddəsi ilə cinayət məsuliyyətinə cəlb edilir. "Ağır nəticələr" anlayışı hər bir konkret cinayət işinin xüsusiyyətindən irəli gələrək qiymətləndirilir. Beləliklə, bu halda ağır nəticələr dedikdə, bir və ya bir

neçə şəxsin ölməsi, insan sağlamlığına ağır zərər vurma, fəlakət, işin ciddi nizamsızlığı, böyük maliyyə itkisi və s. bu kimi hallar başa düşülməlidir. Cinayət əməlinin subyektiv cəhəti birbaşa qəsdlə xarakterizə olunur. Belə ki, şəxs zərərverici virus proqramını yaratdığını və ya adi proqramı zərərli şəkilə salmaq üçün modifikasiya etdiyini dərk edir, bu proqramın digər EHM istifadəçiləri tərəfindən istifadəsi nəticəsində zərərli nəticələrə səbəb olacağını və ya səbəb olma ehtimalını qabaqcadan görə bilir və bunu arzu edir. Motiv və məqsəd bu cinayət tərkibinin əlamətləri qismində çıxış etmir və onun təsnifləşdirilməsinə təsir göstərmir. Cinayət subyekti – 16 yaşına çatmış anlaqlı şəxs hesab olunur. Qanunvericilik ictimaiyyət üçün zərərli əməllər törətmiş, lakin cinayət məsuliyyətinə cəlb etmə yaşına çatmamış şəxslərə inzibati yolla tərbiyəvi xarakterli məcburi ölçülərin tətbiqini də nəzərdən keçirir.

- Elektron hesablayıcı maşınların, onların sisteminin və ya şəbəkələrinin istismarı qaydalarını pozma - CM-in 273-cü maddəsi ilə tənzimlənir. Göstərilən maddə EHM-lə, onların sistemi və ya şəbəkələri ilə işləməyə icazəsi olan şəxs tərəfindən EHM-in və onların sisteminin və ya şəbəkələrinin istismarı qaydalarının pozulması nəticəsində EHM-dəki qanunla qorunan məlumatların məhvi, təcrid olunması və ya modifikasiya edilməsi əhəmiyyətli zərər vurulmasına səbəb olan cinayət əməllərinə görə məsuliyyəti müəyyən edir. Bu cinayət əməlinin

bilavasitə obyekti qismində kompyuter sistemi və ya şəbəkəsi sahibinin bu sistem və ya şəbəkənin düzgün istifadəsi üzrə marağı çıxış edir. Cinayətin obyektiv cəhəti kompyuter sisteminin və ya şəbəkəsinin istifadə qaydalarının pozulması ilə əhəmiyyətli zərərin vurulmasına səbəb ola bilən hərəkət və hərəkətsizliklə xarakterizə olunur. Bu hal faktiki olaraq kompyuter sistemi və ya şəbəkəsinin təhlükəsizliyini təmin edən müəyyən qaydalara (məsələn, təkrar istifadə olunan maşın daşıyıcılarında "virusların" möcvudluğunun yoxlanılmaması) əməl olunmamasında və ya onlara açıq şəkildə etinazsızlıq göstərilməsində öz əksini tapır. "Kompyuter sistemindən istifadə qaydaları" dedikdə, səlahiyyətli dövlət orqanı tərəfindən, eləcə də texniki istifadə qaydaları, proqramlarla iş üzrə qaydalar, EHM və digər kompyuter avadanlıqları istehsalçılarının müəyyən etdiyi qaydalar, həmçinin kompyuter sistemi sahibi və ya onun göstərişi ilə qurulmuş olan qaydalar başa düşülür. Kompyuter sisteminin istifadə qaydalarının pozulması EHM-in qanunla qorunan informasiyasının məhvi, təcrid edilməsi və ya modifikasiya olunması, eləcə də hüquqla qorunan qaydalara və fiziki, hüquqi şəxslərin, cəmiyyət və dövlətin maraqlarına əhəmiyyətli zərər vurulması ilə nəticələnməlidir. "Qanunla qorunan informasiya " isə CM-nin 271-ci maddəsində "Maşın daşıyıcılarda, EHM, EHM-in sistemi və ya şəbəkəsində saxlanılan informasiya" kimi müəyyən olunmuşdur. Əhəmiyyətli ziyan qiymətləndirilə bilən anlayış olub, istifadəçinin

təqsiri üzündən baş vermiş qanunla qorunan EHM informasiyasının məhv olması, təcrid olunması və modifikasiya edilməsinin birbaşa nəticəsi olmalıdır. "Əhəmiyyətli ziyan" əlamətinin müəyyən edilməsində ictimai təhlükəsizlik əleyhinə uyğun cinayətlər üzrə qanunvericilik və məhkəmə praktikası nəzərə alınmalıdır. Cinayətin subyektiv cəhəti birbaşa qəsdlə xarakterizə olunur. Günahkar şəxs istifadə qaydalarını pozduğunu dərk edir, məhv olma, təcrid etmə və ya modifikasiya olunma halının baş vermə mümkünlüyünü və ya qaçılmazlığını öncədən görür, bunu arzu edir və bilərəkdən bunun baş verməsinə şərait yaradır. 273-cü maddənin 2-ci hissəsində eyni əməllərin ehtiyatsızlıqdan ağır nəticələrə səbəb olma halı müəyyən edilmişdir ki, belə əməllərin nəticələri daha öncə 272-ci maddənin 2-ci hissəsinin şərhində qeyd olunmuşdur. Cinayətin subyekti xüsusi olmaqla EHM-ə, onun sistem və şəbəkəsinə daxil olmağa icazəsi olan şəxsdir. Bütün bu şərh olunan maddələri özündə əks etdirən AR CM-nin "Kompyuter informasiyası sahəsində cinayətlər" adlı 30-cu fəsli kompyuter cinayətkarlığı ilə mübarizə sahəsində əsas mənbə olsa da bu fəsil mövcud müasir vəziyyətə tam uyğun gəlmir. Belə ki, iqtisadi münasibətlərin daim yenilənməsi uyğun olaraq cinayət qanunvericiliyində də dəyişikliklərin edilməsini zəruri edir. AR CM qəbul olunandan bəri kompyuterlər də sürətli templərlə insan fəaliyyətinin demək olar ki bütün sferalarını əhatə etmişdir. Son illər ərzində Azərbaycanda İnternet

şəbəkəsi istifadəçilərinin sayında da əhəmiyyətli artım baş vermişdir.

Kompyuter cinayətlərinin mövcud tədqiqat metodları və bu cinayətlərin törədilməsinə görə məsuliyyəti müəyyən edən normaların müəyyən mənada müasir şərtlərə tam cavab verməməsi səbəbindən kompyuter texnologiyalarının bu inkişafı ictimai təhlükəli əməllərin törədilməsinə şərait yaratmışdır. Kompyuter informasiyası sferasında cinayətlərə görə məsuliyyət haqqında mövcud cinayət qanunvericiliyi isə kibercinayətkarlıq probleminin yalnız həlli görüntüsünü yaradır. Ən əsası isə bu normalar yalnız kompyuter cinayətləri, yəni kompyuterlər və kompyuter informasiyası əleyhinə törədilən cinayətləri əhatə edir. Belə ki, bu normalarda kompyuter vasitəsilə törədilən digər cinayətlərə görə məsuliyyət müəyyən olunmamışdır. Təbii ki, bu o demək deyil ki, qanunvericidən CM-nin kompyuter cinayətlərinə həsr olunmuş fəslinə kompyuter vasitəsilə törədilən lakin digər obyektlərə qəsd edən cinayətlər barəsində normaların əlavə edilməsi tələb olunur. Fikrimizcə, CM-də digər cinayət əməllərinin gizlədilməsi və ya onların törədilməsinin asanlaşdırılması məqsədilə kompyuter və kompyuter məlumatları ilə səlahiyyətsiz əməliyyatlara görə məsuliyyət nəzərdə tutulmalıdır. Beləliklə, qanunvericilikdə obyekti yalnız kompyuter şəbəkələrinin fəaliyyətinin təhlükəsizliyi təşkil edən əməllər deyil, həmçinin digər kibercinayətlərdə əks

olunmalıdır. Qeyd edək ki, MDB-yə üzv dövlətlərin Nümunəvi Məcəlləsi və onun kompyuter informasiyası sahəsində cinayətlər barəsində fəsli fikrimizcə kompyuter cinayətlərinə münasibətdə daha əhatəli sənəddir. Bu məcəllənin "informasiya təhlükəsizliyi əleyhinə cinayətlər" adlı XII fəslinə aşağıdakı 7 maddə daxildir. - "Kompyuter informasiyasına sanksiyalaşdırılmamış giriş"; - "Kompyuter informasiyasının modifikasiya olunması"; - "Kompyuter sabotajı"; - "Kompyuter informasiyasının qanunsuz ələ keçirilməsi"; - "Kompyuter sistemi və şəbəkəsinə qanunsuz girişi həyata keçirməyə imkan verən vasitələrin hazırlanması"; - "Zərərverici proqramların hazırlanması, istifadəsi və yayılması"; - "Kompyuter sistemi və şəbəkələrinin istifadəsi qaydalarının pozulması". AR CM-nin kibercinayətkarlığa həsr olunmuş normalarının təkmilləşdirilməsində sonralar bu maddələrdən istifadə etmək olar. 30-cu fəslin təhlili nəinki ayrı-ayrı maddələrdə, həmçinin bütövlükdə fəsildə bəzi təzadların, çatışmazlıqların mövcudluğunu aşkara çıxarır. Hər şeydən əvvəl qanunverici tərəfindən "EHM" termininin istifadəsi düzgün deyildir. Nəzərə alsaq ki, 271-ci maddədə "kompyuter informasiyası"-na qanunsuz girişə görə məsuliyyət nəzərdə tutulub, 272 və 273-cü maddələrdə isə "Elektron-hesablama maşınları" barəsində danışılır. Buradan belə bir nəticəyə gəlmək olar ki, "EHM" termini "kompyuter" sözünün tam sinonimi olaraq işlədilir. Lakin müasir zamanda texnologiyaların belə sürətli inkişafını nəzərə

alsaq deyə bilərik ki, EHM və kompyuterlər müasir mənalarına görə heç də sinonim sözlər deyildir. Bizim fikrimizcə "EHM" terminini daha universal və anlaşılan "kompyuter" sözü ilə əvəz etmək daha məqsədə uyğun olardı. Onu da qeyd edək ki, MDB-ə üzv dövlətlərin Nümunəvi Cinayət Məcəlləsindədə "EHM" termini deyil, "kompyuter" termini istifadə edilmişdir. Onu da qeyd edək ki, qanunsuz olaraq daxil olma anlayışında alimlərin fikrincə (AR CM-nin 271-ci maddəsi) hüquqi-texniki çatışmazlıqlar mövcuddur. Fikrimizcə, maddənin hərfi şərhi bu daxil olmanın hüquq normalarının pozulması vasitəsilə həyat keçirilməsi anlamına gəlir. Bununla yanaşı, "qanunsuz" anlayışı sahibkarın və ya qanuni mülkiyyətçinin ixtiyarı olmadan informasiyanın ələ keçirilməsi mənasını verir. Beləliklə, bu problem "qanunsuz olaraq daxil olma" anlayışını "sanksiyalaşdırılmamış daxil olma" termini ilə əvəz etməklə həll edilə bilər. AR CM-nin 271-ci maddəsinin daha bir çatışmayan cəhəti ondan ibarətdir ki, qanunverici bu cinayət əməlinin obyektiv cəhətinin məcburi əlaməti kimi informasiyanın məhv edilməsi, təcrid olunması, modifikasiya olunması, onun surətinin çıxarılması, yaxud EHM-in işinin, sisteminin və ya onların şəbəkəsinin fəaliyyətinin pozulmasını müəyyən etmişdir. Beləliklə, informasiyaya sadəcə səlahiyyətsiz daxil olma qanunla cəzalandırılmır. Bununla yanaşı, bizim fikrimizcə, informasiyanın oxunması halı da onun surətinin çıxarılması qədər təhlükəli əməldir.

Bəzi hallarda bəd niyyətli şəxsin informasiyanı görməsi və oxuması bu informasiyanın öz dəyərinin itirməsi və ya surətini çıxarmadan istifadəsi üçün kifayətdir. Məsələn, kompyuterin ekranının şəklinin çəkilməsi. Kompyuter şəbəkə və sistemlərinə giriş əldə edən bir çox şəxslər hesab edir ki, onlar heç bir qanunsuz əməl törətmirlər. Əgər hətta bu əməl istifadəçi tərəfindən qoyulmuş müdafiə sistemini pozmaqla törədilirsə də. Biz hesab edirik ki, kompyuter sistemlərinin normal fəaliyyətini, eləcə də informasiyanın saxlanması və göndərilməsini təmin etmək üçün cinayət qanunvericiliyi kompyuter sistemlərinin müdafiə vasitələrini istifadə edən hər bir istifadəçinin kompyuterini mühafizə etməlidir. Bununla belə, kompyuter informasiyasının surətinin çıxarılmasına görə cinayət məsuliyyət MDB-ə üzv dövlətlərin tövsiyə xarakterli Modul Cinayət Məcəlləsində olduğu kimi ayrıca maddədə nəzərdə tutula bilər. Beləliklə, CM-nin 271-ci maddəsindən "kompyuter informasiyasının sanksiyalaşdırılmamış ələ keçirilməsi", "informasiyanın sanksiyalaşdırılmamış modifikasiya edilməsi", "kompyuter sabotajı" (kompyuterlərin və kompyuter şəbəkələrinin fəaliyyətinə mane olmaq məqsədilə informasiyanın qəsdən bloklaşdırılması və ya məhvi) kimi tərkibləri ayırmaqla bu maddənin konkretləşdirilməsinə zərurət vardır. CM-nin 273-cü maddəsinə gəldikdə isə bu maddədə aşağıdakı çatışmazlıqlar mövcuddur. Birinci, verilən maddədə "Elektron hesablayıcı maşınların (EHM), EHM

sisteminin və ya onların şəbəkələrinin istismarı qaydalarını pozma" halı nəzərdə tutulub. Lakin hazırki dövrdə EHM-lərin istifadə qaydalarının müəyyən olunduğu heç bir normativ sənəd yoxdur. Bu səbəbdən də maddə hansı qaydaların pozulmasının cinayət məsuliyyətinə səbəb olduğu aydın deyildir. Qanunverici bu maddədə EHM-lərin texniki istifadə qaydalarının ya müəyyən proqramlarla işləmə qaydalarının və ya EHM-də saxlanılan informasiyanın işlənməsi qaydalarının nəzərdə tutulduğunu qeyd etmir. Maddə elə tərtib olunmuşdur ki, qanunverici tərəfindən bir neçə cinayət yaradan əlamət müəyyən olunmuşdur:

1) EHM sisteminin və ya onların şəbəkələrinin istismarı qaydalarının pozulması;

2) bu qaydaların pozulması nəticəsində EHM-dəki qanunla qorunan məlumatların məhvi, təcrid olunması və ya modifikasiya edilməsi;

3) əhəmiyyətli zərər vurulması. Beləliklə, çox mürəkkəb bir tərkib əmələ gəlir: sərhədləri qeyri-müəyyən olan qaydaların pozulması, bu pozulma informasiyaya münasibətdə müəyyən nəticələrə gətirməlidir, bu isə öz növbəsində sərhədlərinin qanunverici tərəfindən dəqiq müəyyən olunmadığı əhəmiyyətli zərər vurmalıdır. Qaydaların pozulub-pozulmamasından asılı olmayaraq məlumatların əhəmiyyətli zərər vurulmasına səbəb olan məhv edilməsi, təcrid olunması və ya modifikasiya edilməsinin kriminallaşdırılması daha məqsədə-

uyğundur. Belə alınır ki, əgər hüquqi sahibkarın razılığı ilə və EHM-in istifadə qaydalarını pozmadan EHM və EHM-də saxlanılan informasiyaya giriş əldə etmiş şəxs 273-cü maddədə göstərilmiş nəticələrə səbəb olan əməl törətmişsə, bu əməl nə AR CM-nin 271-ci maddəsinin (qanunsuz daxil olma əlamətlərinin mövcud olmaması), nə də 273-cü maddənin təsir dairəsinə düşmür. Bundan başqa AR Cinayət Məcəlləsində "kompyuter dələduzluğu" – kompyuter məlumatlarının daxil edilməsi, dəyişdirilməsi, silinməsi və ya təcrid olunması vasitəsilə özgənin əmlakının oğurlanması və ya özgəsinin əmlakına hüquqların ələ keçirilməsi və ya kompyuter sistemlərinin fəaliyyətinə istənilən müdaxilə haqqında normalar mövcud deyildir. Həm ayrı-ayrı şəxslər üçün, həm də cinayətkar qrupların qeyri-qanuni fəaliyyətinə geniş imkan yaradan informasiya texnologiyalarının istifadə sferasının genişlənməsi ilə əlaqədar artmaqda olan kibercinayətkarlıq təhlükəsi ilə mübarizə aparmaq üçün daima beynəlxalq əməkdaşlıq zəruridir. Kibercinayətkarlığı tənzimləmək və onunla mübarizə aparmaq bir dövlət səviyyəsində demək olar ki, mümkünsüzdür. Beynəlxalq normaların qəbulu isə milli qanunvericilikləri dəyişikliklərin edilməsi ilə müşaiyət olunmalıdır. Dövlətlərin səylərinin koordinasiyası kompyuter texno-logiyalarının inkişafına cəld reaksiya vermək və uyğun normaların qəbul edilməsini təmin etmək baxımından çox zəruridir. Hal-hazırda kibercinayətkarlıqla mübarizə

üzrə beynəlxalq strategiyanın formalaşdırılmasında dünyanın 40-dan çox dövləti fəaliyyətdədir və bu fəaliyyətin uzunmüddətli olacağı gözlənilir. Lakin, bütün çətinliklərə baxmayaraq, beynəlxalq əməkdaşlığın qanunvericiliyin unifikasiyası ilə bağlı bir qərara gəlmələrinin zəruriliyi aydın bir məsələdir. Əks halda, kibercinayətkarlığın transsərhəd xarakterini nəzərə alaraq ayrı-ayrı milli qanunvericiliklərdə müəyyən uyğunsuzluqlar ictimai təhlükəli əməl törətmiş şəxslərin məsuliyyətdən yayınmasına və cinayətlərin tədqiqində çətinliklərin yaranmasına səbəb olacadır. Azərbaycan Respublikasında da bu istiqamətdə artıq ilk addımlar atılmışdır. Məlum olduğu kimi, Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyi hələ 2005-ci ildə Azərbaycan Respublikasının bu sahədə yeganə beynəlxalq mexanizm olan "Kibercinayətkarlıq haqqında" konvensiyaya qoşulması təşəbbüskarı kimi çıxış etmişdi. 2008-ci ildə Prezident İlham Əliyevin sərəncamı ilə ölkəmiz bu konvensiyaya qoşulması haqqında Avropa Şurasında, Strasburqda sənəd imzalayıb. 2009-cu ilin sentyabrın 30-da isə bu sənəd parlament tərəfindən qəbul olunmuşdur. 2010-cu il iyulun 1-də nəzərdə tutulan müvafiq prosedurlar həyata keçirildikdən sonra ölkəmiz adıçəkilən konvensiyaya qoşulmuşdur. Bu, kibertəhlükəsizliyin təmin olunması və onun ayrılmaz hissəsi olan kibercinayətkarlığa qarşı mübarizə sahəsində istifadə olunan beynəlxalq mexanizmlərdən biridir. Sözügedən

konvensiyanın 35-ci maddəsinə görə, hər bir ölkə həftənin 7 günü və 24 saatı ərzində fəaliyyət göstərən, əlaqələndirici bir qurumu müəyyənləşdirir. Konvensiyada bununla əlaqədar Daxili Təhlükəsizlik Xidmətini əlaqələndirici qurum kimi müəyyənləşdirilib.

Ondan əlavə, sözsüz ki, bu Konvensiyaya görə hər bir ölkənin milli qanunvericiliyində də müvafiq dəyişikliklərin edilməsi də tələb olunur. Beləliklə, 29 iyun 2012-ci il tarixində Məsələn, "Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında" qanun qəbul olunmuşdur. Bu qanuna görə kibercinayətkarlıqla bağlı bölməyə də yeni müddəalar əlavə olunub. Əlavələrdə beynəlxalq təcrübə, eləcə də "Kibercinayətkarlıq haqqında" konvensiyanın tələbləri əks olunub. CM-in yeni redaksiyasında AR CM-nin "Kompyuter informasiyası sahəsində cinayətlər" adlı 30-cu fəslinin adı dəyişdirilərək "Kibercinayətlər" adlandırılmaqla bu fəsilə daxil maddələrdə də dəyişikliklər edilməsi qərara alınmışdır. Beləliklə, Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında 29 iyun 2012-ci il tarixli qanuna görə "Kibercinayətlər" adlı 30-cu fəslə aşağıdakı maddələrdən ibarət olacaqdır: - Kompyuter sisteminə qanunsuz daxil olma (Maddə 271); - Kompyuter məlumatlarını qanunsuz ələ keçirmə (Maddə 272); - Kompyuter sisteminə və ya kompyuter məlumatlarına qanunsuz müdaxilə (Maddə 273); - Kibercinayətlərin törədilməsi üçün hazırlanmış

vasitələrin dövriyyəsi (Maddə 273-1); - Kompyuter məlumatlarının saxtalaşdırılması (Maddə 273-2). Qanuna əsasən kompyuter sisteminə qanunsuz daxil olma, məlumatları qanunsuz ələ keçirmə, həmin məlumatları saxtalaşdırmaya, kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi, kompyuter məlumatlarının saxtalaşdırılmasına görə cəzalar sərtləşdirilib. Belə ki, yuxarıda göstərilən qanun pozuntularına yol vermiş şəxs iki ilədək müəyyən vəzifə tutma hüququndan məhrum edilməklə 1000 manatdan 2000 manatadək cərimə və ya 2 ilədək azadlıqdan məhrumetmə cəzası ilə cəzalandırılacaq. Bu cinayət vəzifəli şəxs tərəfindən öz qulluq mövqeyindən istifadə etməklə törədilərsə, 3 ilədək müddətdə vəzifə tutma hüququndan məhrum edilməklə 2000 manatdan 3000 manatadək cərimə və ya 2 ildən 4 ilədək azadlıqdan məhrumetmə cəzası tətbiq olunacaq. Əgər əməllər ictimai əhəmiyyətli infrastruktur obyektinin kompyuter sisteminə və ya onun hər hansı bir hissəsinə törədilərsə, 3 ilədək vəzifə tutma hüququndan məhrum edilməklə 4 ildən 6 ilədək müddətə azadlıqdan məhrumetmə ilə cəzalandırılacaq. Bundan başqa qanunda Məcəllənin 271-273-2-ci maddələrində istifadə olunan "kompyuter sistemi", "kompyuter məlumatları" kimi anlayışların izahı verilmişdir. Belə ki, 271-ci maddənin qeydinə əsasən "kompyuter sistemi" dedikdə, müvafiq proqramlara uyğun olaraq verilənlərin avtomatlaşdırılmış işlənməsini həyata keçirən hər hansı qurğu və ya bir-birinə qoşulmuş və

ya əlaqələndirilmiş qurğular qrupu başa düşülür. "Kompyuter məlumatları" dedikdə isə, kompyuter sistemində işlənməsi, emal edilməsi üçün yararlı olan istənilən informasiya (faktlar, məlumatlar, proqramlar və anlayışlar) başa düşülür. Beləliklə, yeni yaranmış bir sahə olan kompyuter hüquq münasibətləri sferasında cinayət hüquqi siyasətin reallaşması üzrə ilk cəhdlər edilmişdir. Lakin insan fəaliyyətinin demək olar ki, bütün sferalarını əhatə edən informasiya texnologiyaları inkişaf etdikcə qanunvericiliyində bu dəyişikliklərə uyğunlaşdırılmasına daima zərurət olacaqdır.

4. Kibercinayətkarlığın araşdırılmasının ümumi xüsusiyyətləri

İKT-nin geniş istifadəsi və yaratdığı imkanlar həmçinin cinayət əməllərinin törədilməsindəki müxtəlifliklərlə müşayiət olunur.

Digər cinayətlərdən fərqli olaraq kibercinayətlərin araşdırılması özündə həm texniki, həm də hüquqi cəhətləri birləşdirir. Kibercinayətkarlıqla effektiv mübarizə üçün cinayət hüququ ilə yanaşı, cinayət - prosessual hüquqi mexanizmlərin və müvafiq araşdırma texnikalarının inkişaf etdirilməsi zərurəti Kibercinayət haqqında Konvensiyanın izahedici məruzəsində də öz əksini tapmışdır. Müasir dövrdə İKT-nin gündəlik həyatın bütün sferalarına daha dərindən təmas etməsi və insanlar tərəfindən daha geniş istifadə olunması, digər tərəfdən də, buraxılan elektron izlərin artmasına gətirib çıxarmışdır. Bu hal

cinayətlərin törədilməsi zamanı buraxılan izlərə də aiddir. Buna görə də elektron sübutlar həm kibercinayətlərin, həm də İKT-dən istifadə etməklə törədilən digər cinayətlərin araşdırılması və müvafiq hökmün çıxarılması üçün əhəmiyyət daşıyır. Qeyd etmək lazımdır ki, elektron sübutlar cinayət işi başlama və ya işə başlamanı rəddetmə haqqında məsələnin həlli, ibtidai araşdırma zamanı hadisənin bütün mühüm hallarının tam, hərtərəfli və obyektiv araşdırılması, işdə mahiyyəti üzrə məhkəmə iclasında baxmaq üçün kifayətedici faktiki məlumatların və hüquqi əsasların olub-olmamasının yoxlanılması, daha sonra isə məhkəmə baxışı və hökmün çıxarılması mərhələsinin dəqiq və effektivliyinin əldə olunmasında həlledici rola malikdir. Bu mərhələlərin hər birinin prosessual qanunvericiliklə müəyyən olunmuş tələblərinə riayət olunması üçün elektron sübutların müəyyən olunması, əldə olunması, saxlanması, təhlili, məhkəmə baxışına təqdim edilməsi zəruridir. Bu isə hüquq mühafizə orqanlarından xüsusi texniki proqramlar, mexanizmlər, üsul və vasitələrin tətbiqini tələb edir. Bu tələblər İKT-nin istifadəsilə bağlı olduğuna görə hüquq mühafizə orqanlarının işinə bəzi aspektlərdən yardımçı olsa da, bir sıra hallarda çətinləşdirir.

1. İnformasiyanın həcmi və ötürülmə sürəti müasir kompyuter yaddaşlarında saxlanılan və şəbəkələr vasitəsilə ötürülən böyük həcmdə informasiyanın araşdırılması məqsədilə seçilməsi və

analiz olunması bu istiqamətdə əsas çətinliklərdən biridir. Onu da qeyd etmək lazımdır ki, müasir texnologiyalar və kompyuter sistemləri araşdırmanın sürətli və avtomatik həyata keçirilməsini təmin edə bildiyi üçün hüquq-mühafizə orqanlarına problemin texniki tərəfinin öhdəsindən nisbətən asanlıqla gəlmə imkanı yaradır. Məsələn, beynəlxalq təcrübədə uşaq pornoqrafiyasının dövriyyəsi ilə bağlı cinayətlərin araşdırılması zamanı bu cür araşdırma proqramlarından geniş istifadə olunur. Lakin axtarışın avtomatlaşdırılması prosesi araşdırılan informasiyanın məzmun və formatından asılı olduğu üçün məhdud xarakter daşıyır və məzmunun qiymətləndirilməsi araşdırmanı yenidən həyata keçirən şəxslərin üzərinə düşür. Hüquq mühafizə orqanları üçün vəziyyəti mürəkkəbləşdirən digər bir cəhət ondan ibarətdir ki, cinayətin elementlərini özündə daşıyan informasiyanın ötürülməsi, əsasən, çox qısa bir zamanda - cəmi bir neçə saniyə ərzində həyata keçirilir. Bu isə araşdırma məqsədilə zəruri sübutların toplanılması üçün həddən artıq məhdud zamanın olması deməkdir. Eyni zamanda, elektron sübutların çox qısa bir zaman ərzində asanlıqla dəyişdirilə, tamamilə məhv edilə bilməsi cinayət təqibi üzrə icraat prosesində operativ və daha diqqətli davranmanı tələb edir. Bu çeviklik İKT-nin tətbiqilə əldə oluna bilən sayılsa da, mövcud normativ-hüquqi mexanizmlər adekvat çevikliyin əldə olunmasını hər bir halda təmin edə bilmir və ya etmir. Çünki müvafiq qanunvericilik sübutların toplanılma-

sında istifadə olunan üsul və vasitələrin seçilməsi və tətbiqində bir sıra müddəalara riayət olunmasını tələb edir. Məsələn, sübutların müəyyən olunması və toplanılması zamanı şəxsi məlumatların toxunulmazlığı ilə bağlı məhdudiyyətlər buna misal ola bilər. Qanunvericiliyin tələblərini pozmaqla aparılan prosessual hərəkətlərin prosessual qanunvericiliyə görə hüquqi qüvvəsinin olmaması bu kimi hallarda çevikliyi istər-istəməz ikinci plana keçirir. Bundan başqa, maddi sübutların digər növlərindən fərqli olaraq, ən xırda diqqətsizliklə sübuti əhəmiyyətini tamamilə itirə biləcəyini nəzərə alaraq qeyd olunmalıdır ki, araşdırma zamanı əldə olunmuş elektron sübutların surətindən və ya şəklindən istifadə olunması onların orijinalının qorunması üçün, hər bir halda, daha məqsədəuyğundur. Əlavə olaraq, qeyd etmək lazımdır ki, bulud texnologiyalarına keçidin sürətlənməsi gələcəkdə kibercinayətlərin araşdırılması üçün zəruri olan elektron sübutların toplanması önündə əlyetərliliyin bir az da çətinləşməsi problemini yaradacaq və zəruri və mötəbər sübutların toplanmasını məhdudlaşdıracaq.

2. İnformasiyanın yeri, anonimlik və konfidensiallıq İKT elektron sübutlarla bağlı çətinliklərin texnoloji tərəfinin həllində müəyyən rola və imkanlara malik olsa da, problemin hüquqi aspektlərinin həlli müvafiq normativ-hüquqi mexanizmlərin tətbiqindən asılıdır. Kibercinayətlərin təhqiqatı və istintaqı özündə adekvat araşdırma alət və

vasitələrinin tətbiqi ilə yanaşı, elektron sübutlarla bağlı müvafiq prosessual qaydalara və qanunvericiliyə riayət olunmasını da tələb edir. Lakin sadəcə milli qanunvericiliyin təkmilləşdirilməsi kibercinayət-karlıqla mübarizənin effektivliyini və səmərəliliyini təmin etmir. Çünki cinayətin obyekti ilə subyekti arasındakı fiziki yaxınlığa və ya təmasa ehtiyac olmadan realizə olunan transmilli xarakterli kibercinayətlərin araşdırılması yurisdiksiya məsələləri ilə yanaşı, elektron sübutların da toplanmasında çətinlik yaradır. Belə ki, bir sıra hallarda kibercinayəti törədən şəxsin yerinin müəyyən olunma prosesində yaranan çətinlik həmin cinayət üçün əhəmiyyət daşıyan elektron sübutların əldə olunması önündə də əngəllər yaradır. Eyni zamanda, infrastrukturun böyük hissəsinin özəl və ya şəxsi mülkiyyətdə olması hüquq - mühafizə orqanlarından müxtəlif sektorlarla əməkdaşlığı tələb edir. Bu anlamda, daha bir diqqətəlayiq məqam isə kibermәkan üzərindən həyata keçirilən informasiya mübadilələrində anonimliyin və konfidensiallığın təmin olunması üçün imkanların geniş olmasıdır. Bu cür imkanların kibercinayətlərin realizəsi zamanı icraçılar tərəfindən geniş istifadə olunması cinayətlərin araşdırılması zamanı sübutların toplanması və qiymətləndirilməsi kimi hüquqi prosesləri mürəkkəbləşdirir. Qeyd olunduğu kimi, kibermәkan üzərindən törədilən bütün əməliyyatlar müəyyən izlər buraxır ki, bu da onların müvafiq metodlarla rahat izlənilə bilməsini mümkün edir.

Onlayn əməliyyatlarda tam anonimliyin təmin olunmasının "mif" olduğunu nəzərə alsaq, kiberməkanın yaratdığı bu İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il maneənin də aşılmasının texnoloji həllinin çətin olmadığını anlamaq olar. Bu, bütün hallarda araşdırma üçün lazımi informasiyaya limitsiz çıxışın əldə oluna bilməsi kimi qəbul edilməməlidir. Belə ki, informasiyanın yalnız sahibinə və ünvanlandığı şəxsə məlum olan alqoritmlərə əsasən şifrələnməsini həyata keçirərək daha yüksək səviyyəli konfidensiallıq təmin edən proqramların və texnologiyaların İnternet istifadəçiləri üçün əlyetərliliyi bu anlamda araşdırma qarşısında anonimlikdən daha böyük bir maneə yaradır. Açar şifrənin araşdırma orqanları tərəfindən şifrə sahibindən əldə edilə bilməsi məlumatların əlyetərliyinin mümkünsüzlüyünü aradan qaldırır. Lakin anonimliklə yanaşı, bu cür proqramlar vasitəsilə də şifrələnmiş bütün kommunikasiyalar və elektron sənədlər qanuni müdaxilələrə və axtarışlara qarşı immunitet qazanır, və bu cür həyata keçirilən elektron köçürmələr istənilən dövlət nəzarətindən kənarda qala bilir. Kibercinayətlərin törədilməsində son illərdə bu metodlardan istifadə hallarının sürətlə artmasını nəzərə alaraq anonim və şifrələnmiş informasiya və sənədlərin sübut qismində toplanması, yoxlanılması, qiymətləndirilməsi, saxlanması ilə bağlı həm normativ-hüquqi, həm də elmi-texniki bazanın təkmilləşdirilməsi

zəruridir. Beynəlxalq müstəviyə çıxış Müasir kompyuter şəbəkələri vasitəsilə həyata keçirilən əməliyyatlarda ərazi yurisdiksiyaları üzrə fəaliyyət göstərən milli ənənəvi cinayət-hüquqi mexanizmlərinin təsir dairələrindən rahatlıqla kənara çıxa bilməsi kibercinayətlərin törədilməsi üçün yeni imkanlar və hədəflər yaratmasına baxmayaraq, onların araşdırılması önünə bir sıra çətinliklər çıxarır. Çünki kiberməkan ərazilərə bölünərək yurisdiksiyalar üzrə fəaliyyət göstərmir və iş mexanizmi fiziki məkanda tətbiq olunan ərazi məhdudiyyətlərindən asılı deyil. Buna görə də, transmilli kibercinayətkarlığın araşdırılması və qarşısının alınmasında fiziki məkanın tələblərinə uyğunlaşdırılmış hüquqi mexanizmlər vasitəsilə effektivliyin təmini mümkün olmur. Kibercinayətkarlıqla hərtərəfli, səmərəli və effektiv şəkildə mübarizə aparılması və onların araşdırılması zamanı zəruri olan elektron informasiyanın toplanılması beynəlxalq əməkdaşlığı, xüsusilə də ölkələr arasındakı qarşılıqlı hüquqi və texniki yardımı şərtləndirir. Beynəlxalq əməkdaşlıq və qarşılıqlı yardımın əldə olunması bir sıra formal hüquqi qaydalara riayət olunmasını şərtləndirdiyi, habelə əməkdaşlığın təşkili müəyyən zaman tələb etdiyi üçün kibercinayətin araşdırılması üçün zəruri olan operativliyin əldə olunması bir sıra hallarda mümkün olmur və nəticədə araşdırmanın səmərəsizliyinə gətirib çıxarır. Araşdırmanın aparılması zamanı beynəlxalq əməkdaşlığın və yardımın əldə olunmasının sürətinin

artırılması məqsədilə Kibercinayətkarlıq haqqında Konvensiyanın 35-ci maddəsində müəyyən olunmuş, sutkada iyirmi dörd saat, həftədə yeddi gün fəaliyyət göstərən müvafiq əlaqələndirmə mərkəzlərinin yaradılması nəzərdə tutulmuşdur.

İKT-nin müasir həyatın və inkişafın bütün sferalarını geniş şəkildə əhatə etməsi, qlobal məkana və informasiyaya çıxışdakı sərhədləri aradan qaldırması, informasiya mübadilələrinin və əməliyyatların yüksək sürətini təmin etməklə yanaşı, ucuzluğu və əlyetərliliyi qısa bir zaman ərzində dünya əhalisinin təxminən yarısının istifadəçiyə çevrilməsi ilə nəticələnmişdir. Bütün bunlar isə kibercinayətlərin araşdırılmasının həyata keçirilməsi üçün yeni üsul və vasitələrlə yanaşı, onların realizəsində yeni metod və imkanların yaranmasına, habelə potensial kibercinayətkarlıq obyektlərinin sayının və miqyasının sürətlə artmasına gətirib cıxarmışdır. Kiberməkanın səciyyəvi xüsusiyətləri, habelə infrastrukturun, əsasən, özəl sektor və vətəndaşların əlində cəmlənməsi kibercinayətkarlıqla mübarizədə adekvat institutsional strukturların, elmi-texniki və normativ-hüquqi bazanın formalaşdırılması və təkmilləşdirilməsi ilə yanaşı, dövlət, özəl sektor və vətəndaşlar arasında, həmçinin beynəlxalq səviyyədə tərəfdaşlığın və əməkdaşlığın genişləndirilməsini tələb edir. Adekvat mexanizmlərin,

zəruri institutların, çoxtərəfli və beynəlxalq tərəfdaşlıq və əməkdaşlığın yerində olmaması isə kibercinayətkarlıqla mübarizəni daha da müəkkəbləşdirir və çətinləşdirir.

Beləliklə, kibercinayətlərin araşdırılmasının bəzi xüsusiyyətlərini qeyd edək:

- məlumatların mövcud olduğu kompyuterlərə giriş və çıxışın məhdudlaşdırılması;

- cinayətin araşdırılmasına yönəlmiş hərəkətlərə həddən artıq diqqəti cəlb etməmək üçün qlobal şəbəkədə fəaliyyətini davam etdirmək;

- cinayətin araşdırılmasinda istintaq hərəkətlərinin və əməliyyat-axtarış tədbirlərinin ardıcıllığının düzgün müəyyən edilməsini və vaxtında keçirilməsinin təmin edilməsi;

- məlumatların ələ keçirilməsi və ya tutulması ilə bağlı istintaq hərəkətlərinin aparılmasına məhdud sayda iştirakçiların cəlb edilməsi;

- kompyuter məlumatları sahəsində cinayətlərin araşdırılması prosesində eyni istiqamətdən daxil olan mesajların daimi monitorinqinin aparılması;

-zərərçəkmişə məxsus məlumatların qorunması, sistemindəki qüsurların müəyyən edilməsi;

- məlumatın dəyişdirildiyi və ya məhv edildiyi kompyuterdə saxlanılan informasiya sisteminə gizli təhdidlərin müəyyən edilməsi.

Eyni zamanda qeyd etmək lazımdır ki, kompyuter cinayətlərin araşdırılmasında rəqəmsal sübut və dəlillər müstəsna əhəmiyyət kəsb edir. Həmin sübutlar kompyuterin yaddaş qurğusu olan HARD DİSC-də (sərt disk) və ya RAM-da saxlanılır və kompyuterin tədqiqində aşağıdakı məlumatların əldə edilməsi məqsədəmüvafiqdir: gizli, silinmiş və şifrələnmiş fayl və qovluqların müəyyən edilməsi; sistemin hansı vaxtdan etibarən fəaliyyətdə olması; kompyuterin kimlərin istifadəsində olması; kmpüterin nə vaxt format olunması; kompyuterin iş rejimiini necə olması; internet keçmişi; hansı proqramların kompyuterə yüklənməsi; kompyuterin məsafədən idarə edilməsinin mümkün olub-olmaması; kompyuterə qoşulmuş USB cihazlarının olması; sənədlərin silinmə tarixləri; yaddaşda olan sosial şəbəkə haqqında məlumatlar; sosial şəbəkələrdəki yazışmaları; kopmüterin sonuncu dəfə kim tərəfindən istifadə olunması, söndürülmə tarixi, yaddaşda olan elekton poçt ünvanları; istifadə olunan İP məlumatları; ən son istifadə edilən sənədlər; CD və DVD disklərinin kompyuterdə olub-olmaması və s. Rəqəmsal dəlillər bir çox fayl növündə və ya ölçüdə ola bilər. Müxtəlif elektron cihazlarda saxlanılan sübutlar şifrələnə, mühafizə oluna və ya başqa şəkildə gizlənə bilər. Əgər bu kimi sübutları müəyyənləşdirmək və toplamaq üçün lazım olan qurğular, alətlər və ya xüsusi bir mütəxəssis yoxdursa,

bu halda bu sahə üzrə ixtisaslaşmış digər qurumlarla tərəfdaşlıq etmək vacibdir

Rəqəmsal sübutların toplanması zamanı rəqəmsal izlərin müəyyən edilməsi vacibdir. Rəqəmsal izlər - cinayətkarların əksəriyyətinin buraxdığı rəqəmsal izdir. Şübhəli şəxsin İP ünvanı, sosial şəbəkə ünvanı rəqəmsal izlərə misal ola bilər.

Rəqəmsal dəlillərin əsas mənbələrinə İnternet səhifələrini, personal (fərdi) kompyuterləri, mobil cihazları, məlumat banklarını, elektron qurğuları, yaddaş cihazlarını, internet linklərini misal gətirmək olar.

Bu dəlillərdən sübutetmə prosesində istifadə edilməsi aşağıdakı ardıcıllıqla həyata keçirilir: Rəqəmsal dəlilin müəyyən edilməsi - hadisə yerində ilk öncə rəqəmsal dəlillər müəyyən edilməlidir. Bu zaman "tez məhv oluna bilən dəlil"lərin mövcud olub-olmadığına xüsusi diqqət yetirilməlidir. Həmin dəlillərə əsasən kompyuterin müvəqqəti yaddaş qurğusunda saxlanılan və elektrik enerjisinin kəsilməsi ilə məhv olan sübutlar aid edilir və onlara aşağıdakılar aiddir: CPU yaddaş, mübadilə buferindəki məlumatlar, cihazın internetə və ya hansısa şəbəkəyə bağlılıq vəziyyəti, drarveryərin yaddaşı, internet brauzerinin tarixçəsi, ATM əməliyyat jurnallarını, elektron poçtları, rəqəmsal fotoşəkilləri və s.

Rəqəmsal dəlillərin toplanmasında dair bir sıra qaydalara riayət edilməsi məqsədəuyğun hesab edilir:

- orginal dəlillər ilk tapıldıqları vəziyyət və şərtlərə uyğun şəraitdə saxlanılmalıdır;

- orginal dəlillərin bütünlüyünü pozmamaqla mümkünsə bir kopyası çıxarılmalıdır;

- surəti çıxarılan verilənlər virus olmayan və içində hər hansı məlumat olmayan yaddaş qurğusuna köçürülməlidir;

- dəlillər paketə qoyulamlı, qablaşdırılmalı, möhürlənməli, qorunmalı və sənədləşdirilməlidir;

- əgər kopyuterdə və ya proqramlarda olan məlumatlar şifrələnmişdirsə və ya gizlidirsə bu halda kompyuter və ya digər texniki qurğunu götürülməli və labarator şəraitdə tədqiq edilməlidir.

Dəlillər toplandıqdan sonra qorunmalıdır. Qorunma iki formada həyata keçirilir:

- rəqəmsal qoruma – yəni verilənlərin dəyişdirilməməsi, bütünlüyünün qorunması ;

- fiziki qorunma – dəlillər götürlmə və saxlanılmalı şəraiti fiziki təsirlərdən mühfizə olunmalıdır.

Dəlillərin analizi – bu mərhələ mütəxəssislər tərəfindən həyata keçirilir. Bu mərhələdə adətə sübutun surəti çıxarılır və orginal nüsxəsi qorunur.

Son mərhələ dəlillərin məhkəməyə təqdim edilməsidir. Bu zaman hazırlanan bütün sənədlər

xüsusi qovluqda yerləşdirilməli, dəlillərin qorunması və tədqiqi prosesində istifadə olunan bütün sistemlər və onların sübutların tədqiqindəki rolu sənədləşdirilməlidir.

5. Kibercinayətkarlığla bağlı istintaq hərəkətlərinin aparılması.

Bu növ cinayətlər üzrə cinayət işlərinin araşdırılması və istintaq zamanı aşağıdakı hallar müəyyən edilməlidir.

Kompyuter informasiyası sisteminə və şəbəkəsinə qanunsuz daxil oluma faktlarını informasiya sistemindən istifadə edən subyektlər aşkar edirlər. Amma onlar müxtəlif səbəblərdən hüquq-mühafizə orqanlarına xəbər vermirlər. Maliyyə-kredit orqanları və banklar öz müştərilərinin etibarını itirməmək məqsədilə belə faktları gizlədirlər. Onlar yoxlamalardan sənədli təftişlərdən çəkinirlər ki, öz sirlərini başqaları bilməsindlər işdə olan çatışmamazlıqlar və digər nəqativ halların üzə çıxmaması üçün belə faktları gizlədirlər.

Firma-provayder internet şəbəkəsinə qanunsuz daxil olma faktını görülmüş xidmətlər barədə hesab göndərəndə də aşkar etmək olur. Hesabın məbləği göstərilən xidmətlərdən daha çox olması onu göstərir ki, kimsə qanunsuz şəbəkəyə daxil olub istifadə edir.

İnformasiya sisteminə qanunsuz daxil olma faktını sənədli təftişlər məhkəmə ekspertizaları, vergi və auditor yoxlamaları keçirilərkən də aşkar etmək olar.

Əməliyyat-axtarış tədbirləri keçirilərkən və araşdırma zamanı istintaq hərəkətlərinin keçirilməsində də belə faktları müəyyən etmək mümkündür.

Bu növ cinayətlərlə bağlı istintaq hərəkətlərinin özünəməxsus xüsusiyyətləri vardır.

***a).*Kibercinayətlər üzrə hadisə yerinə baxış.**

İstintaq baxışın növlərindən biri olan hadisə yerinə baxış müstəqil istintaq hərəkəti kimi cinayət işi üzrə sübutların toplanmasın da mühüm əhəmiyyət kəsb edir və Azərbaycan Respublikası CPM-nin 236-cı maddəsi ilə tənzimlənir.

Kibercinayətlər üzrə hadisə yerinə baxışın əsas vəzifələri aşağıdakılardır:

-kibercinayətin baş vermə şəraitinin, onun mexanizminin və digər halların aydınlaşdırılması;

- kibercinayətlərlə bağlı hadisə yerinə baxış protokolunda və protokola edilən əlavələrdə hadisə yerinin bütün vəziyyətini tam və dəqiq əks etdirilməsi;

-cinayət hadisəsinin baş verdiyi vəziyyəti canlandırmaq və istintaqı düzgün istiqamətə yönəltmək üçün zəruri fərziyyələrin müəyyənləşdirilməsi;

- kibercinayətlərlə bağlı digər sübutların aşkar edilməsi və ya yoxlanılması üçün istifadə oluna biləcək məlumatların müəyyənləşdirilməsi;

- kibercinayətkarın şəxsiyyətini və bir sıra hallarda isə cinayətin motivinin müəyyən edilməsi. Digər

cinayətlər kimi kibercinayətlər üzrə hadisə yerinə baxış hazırlıq, işçi və nəticə mərhələlərindən ibarət olmaqla həyata keçirilir.

Müstəntiq hadisə yerinə gedənə qədər mütəxəssisləri çağırmalı, hal şahidləri müəyyən etməli, götürüləcək məlumatları oxumaq və saxlamaq üçün müvafiq kompyuter texnikasını hazırlamalı, istintaq-əməliyyat qrupunun üzvlərini təlimatlandırmalı və mütəxəssisdən məsləhətlər almaqla digər baxış üçün zəruri texniki vasitələri hazırlamalıdır.

Müstəntiq hadisə yerinə gələnə qədər aşağıdakı hazırlıq tədbirlərini həyata keçirməlidir:

a) kibercinayət faktı üzrə hadisə yerinin toxunulmazlığını təmin etməli;

b) baxışda tətbiq edilənelmi-texniki vasitələrin yararlı olmasını yoxlamalı;

c) baxışa cəlb ediləcək şəxslərin dairəsini müəyyənləşdirməli və onların iştirakını təmin etməli. (xüsusilə kompyuter texnologiyası sahəsində mütəxəssisi)

Baxış aparılacaq sahənin sərhədinin müəyyən edilməsi hadisənin baş vermə şəraitindən və törədilmiş kibercinayətin xarakterindən asılıdır. O, elə müəyyənləşdirilməlidir ki, iş üçün əhəmiyyəti olan izlərin və digər maddi sübutların aşkar edilməsinə, qeydə alınmasına imkan versin. Konkret şəraitdən asılı olaraq, baxışı ilk müəyyən edilmiş sahədə deyil, daha geniş miqyasda aparmaq zərurəti qarşıya çıxa bilər. (Məsələn, baxışı təkcə kompyuter qurğularının

yerləşdiyi otaqlar deyi, həm də həmin yerdə, binada olan digər otaqlar da ola bilər). Bəzi hallarda isə ilkin müəyyən edilmiş baxış yerin sərhədi dəqiq müəyyən olunmadığından, bu sərhəd baxış prosesində dəyişilə bilər.

Hadisə yerinə gələndən sonra: Müstəntiq hadisə yerinə gəldikdən sonra baxışa başlamaq üçün aşağıdakı hazırlıq tədbirləri görməlidir:

a) baxışa maneçilik göstərə bilən şəxsləri hadisə yerindən (kompyuter texnologiyalarının yerləşdiyi otaqdan, binadan və s.) kənarlaşdırmalı;

b) hadisə haqqında məlumat toplamalı;

c) əgər hal şahidləri dəvət olunmayıbsa onları dəvət etməli, hüquq və vəzifələrini onlara izah etməli;

e) baxış yerinin sərhədlərini və baxışın aparılma metodunu müəyyənləşdirməli;

ə) hadisə yerinin toxunulmazlığını təmin etməli.

Müstəntiq kibercinayət barədə məlumat alan kimi mümkün qədər tez bir zamanda hadisə yerinə baxış keçirməyə başlamalıdır. Lakin o, hadisə yerinə nə qədər tez getsə də cinayət hadisəsinin baş vermə anından onun hadisə yerinə gəlmə anınadək müəyyən zaman keçir. Bu müddət ərzində hadisə yerinin vəziyyəti və ya orada olan kompyuter vasitələrinə müdaxilə oluna bilər, ayrı-ayrı izlər və maddi sübutlar qəsdən, bəzi hallarda isə heç bir marağı olmayan şəxslər tərəfindən dəyişilə və ya məhv edilə bilər. Belə halların qarşısını almaq məqsədi ilə müstəntiq hadisə

yerinin toxunulmazlığını təcili olaraq, təmin etmək üçün tədbirlər görməlidir.

Baxışda tətbiq edilən elmi-texniki vasitələrin yararlı olmasının yoxlanılması.

Kibercinayətlər üzrə hadisə yerinə baxış zamanı elmi-texniki vasitələrdən bacarıqla istifadə edilməsi onun keyfiyyətli aparılmasını təmin edən şərtlərdən biridir. Elmi-texniki vasitələrdən düzgün istifadə edilməməsi və eləcə də müstəntiqin təşəbbüssüzlüyü baxışın keyfiyyətsiz aparılmasına səbəb olur.

Hadisə yerində kiberizlərin və digər maddi sübutların götürülməsində, qeyd edilməsində istintaq çamadanında olan kriminalistik-texniki vasitələrdən geniş istifadə edilməli və onların yararlı halda saxlanılmasına xüsusi diqqət göstərilməlidir. Çünki, hər hansı alətin və ya vasitənin olmaması və yararsız olması müstəntiqin işini çətinləşdirir və baxışın keyfiyyətinə mənfi təsir göstərir. Müstəntiq hadisə yerinə gələrkən, istintaq çamadanındakı alət və vasitələrin tamlığını yoxlamalıdır.

Hal şahidlərinin dəvət edilməsi. Cinayət-prosessual qanunvericiliyi baxış aparılarkən, hal şahidlərinin mütləq iştirakını tələb edir. Müstəntiq hal şahidlərinin baxış zamanı nə kimi hüquq və vəzifələrə malik olmalarını, baxışın məqsədini onlara izah edir.

O, kibercinayətlər üzrə baxış zamanı hadisə yerində aşkara çıxarılan əşyaların əlamətləri ilə hal şahidlərini tanış etməli və törədilmiş cinayətlə bu əşyaların nə dərəcədə əlaqədar olmasını onlarla

birlikdə aydınlaşdırmalıdır. Bu baxışın dəqiq aparılmasını və eləcə də baxış protokolunun dolğun yazılmasını təmin edir. Nəzərə almaq lazımdır ki, hadisə yerinə baxış protokolu cinayət işləri üzrə sübut növlərindən biri sayılır.

Əgər hadisə yerindən baxış protokolunun dolğunluğu haqqında şübhə yaranarsa, onda hakim hadisə yerinə baxış zamanı iştirak edən hal şahidləri məhkəməyə dəvət edib onları dindirməklə yoxlaya bilər.

Kibercinayətlər üzrə baxış aparılarkən, hal şahidlərindən başqa, zərurət yarandıqda hadisə yerinə təqsirləndirilən və ya şübhəli, zərərçəkmiş şəxslər də iştirak edə bilər (CPM-nin 236.3-cü maddəsi).

Hadisə yerində mütəxəssislərin iştirakı.

Bir çox hallarda baxış zamanı müxtəlif elm, peşə və sənət sahələrinə aid olan məsələlərin aydınlaşdırılmasına ehtiyac yaranır. Belə hallarda baxışın obyektiv və tam aparalıması məqsədi ilə xüsusi biliyə malik olan şəxslərin dəvət edilməsi zəruridir. AR CPM-nin 236.5. maddəsində deyilir ki, müstəntiq baxışda iştirak etmək üçün mütəxəssislər dəvət edə bilər. Onlar izləri, əşyaları, sənədləri, habelə gələcəkdə iş üzrə sübut əhəmiyyəti kəsb edə biləcək digər əşyaları göturur, eyni zamanda xüsusi bilik tələb edən bu kimi başqa məsələlərin həllində müstəntiqə yaxından kömək edirlər.

Müstəntiq törədilmiş kibercinayətin xarakterindən asılı olaraq mütəxəssisin baxışa dəvət edilməsini müəyyənləşdirməli və iştirakını təmin etməlidir.

İlkin məlumatların toplanması.

Baxış üçün nəzərdə tutulmuş hərəkətlərindən biri də ilkin məlumatların toplanmasıdır. Müstəntiq kibercinayətlər üzrə hadisə yerinə gəlib, baxışa başlayana qədər hadisə haqqında məlumatı olan şəxsləri müəyyən etməli və onlardan baş vermiş hadisənin xarakteri haqqında məlumatlar toplamalıdır. Həmin məlumatlar hadisənin nədən ibarət olmasını aydınlaşdırmaq məqsədi ilə müvafiq tədbirlərin görülməsinə, hadisə yerinin qorunmasına, cinayətkarın müəyyənləşdirilməsinə, tutulmasına və bu kimi başqa mühüm halların aydınlaşdırılmasına şərait yaradır.

Müstəntiq kibercinayətlərlə bağlı hadisə haqqında məlumat toplayarkən, həm də hadisə yerinin ilkin vəziyyətində dəyişiklik baş verib-vermədiyini, dəyişiklik baş vermişsə bunun kim tərəfindən, nə vaxt və hansı məqsədlə edildiyini də müəyyənləşdirməyə çalışmalıdır.

Hadisə haqqında tam və dəqiq məlumat əldə edilməsi aparılan baxışın daha keyfiyyətli başa çatdırılması üçün zəmin yaradır.

Müstəntiq hadisə haqqında ilk məlumatları hadisəni görənləri, onu birinci dəfə müşahidə edənləri, zərərçəkmiş şəxsin qohumlarını və ya ona yaxın şəxsləri sorğu-sual etməklə alır.

Sorğu-sual nəticəsində alınan məlumatlar cinayət hadisəsi və bu cinayəti törətmiş şəxs və ya şəxslər haqqında düzgün fərziyyələrin irəli sürülməsinə imkan verir. Bu zaman cinayətkarın yoxlanılmasını təmin edən tədbirlərin görülməsinə və işin istintaqı üçün əhəmiyyəti olan məlumatların aydınlaşdırılmasına xüsusi diqqət yetirmək lazımdır. Bu şəxslər, xüsusilə, kibercinayətin törədilməsi şəraiti, cinayətkara xas əlamətlər və cinayətkar əməlinin yönəldilmiş olduğu obyektlərin əlamətləri barəsində ətraflı dindirilməlidir.

Lazım olani lkin məlumatlar alındıqdan sonra müstəntiq baxışın hansı ardıcıllıqla aparmaq məqsədi ilə hadisə yerini ümumi nəzərdən keçirir.

Hadisə yerinə baxış zamanı müsbət nətisə əldə etmək məqsədi ilə baxış prosesində müəyyən edilmiş aşağıdakı taktiki qaydalara riayət olunmalıdır:

a) kibercinayətlər üzrə hadisə yerinə baxışı yubanmadan vaxtında aparmaq;

b) hadisə yerində izlərə və digər maddi sübutlara baxış və qeydə alınması zamanı kriminalistik – texniki vasitələrdən və üsullardan bacarıqla istifadə etmək;

c) baxışı mütəşəkkil surətdə aparmaq.

Hadisə yerinə baxışın keyfiyyəti həmin qaydalara baxış zamanı hansı səviyyədə əməl edilməsindən çox asılıdır. Məsələn, kibercinayətlər üzrə hadisə yerində baxışın vaxtında aparılmaması onun keyfiyyətini olduqca aşağı sala bilər. Çünki bu hadisə yerində qalmış izlərin və digər maddi sübutların məhvi və bəzi hallarda isə keyfiyyətinin itirilməsi ilə nəticələnə bilər.

Hadisə yerinə vaxtında baxış keçirildikdə cinayətkarın qoyduğu izlərin və digər maddi sübutların əldə olunmasına, iş üzrə fərziyyələrin düzgün irəli sürülməsinə və s. Imkan yaradır.

Kibercinayətlər üzrə hadisə yerinin vəziyyətində dəyişikliklər edilə biləcəyi ehtimalı olduğu hallarda baxışın təxirəsalınmadan keçirilməsi xüsusilə vacibdir.

AR CPM-nin 236-cı maddəsinə müvafiq olaraq, hadisə yerində baxış təxirəsalına bilməyən hallardan başqa, gündüz aparılır. Baxış gecə aparıldıqda hadisə yeri işıqlandırılmalıdır. Lakin, bəzi hallarda süni işıq şəraitində hadisə yerində olan ayrı-ayrı izlərin və mikrohissəciklərin tam aşkar edilməsi mümkün olmur. Belə hallarda hadisə yerinə təkrar baxış keçirilməlidir.

Müstəntiq baxış zamanı taktiki qaydalara riayət etməklə yanaşı, elmi-texniki vasitələrdən də bacarıqla faydalanmalı və baxışı prosessual qaydada düzgün rəsmiləşdirməlidir.

Başqa sözlə ifadə etsək, müstəntiq hadisə yerinə baxış planını tutmalı və baxışı ardıcıl aparmalı, baxış prosesində müəyyən edilmiş halları aydınlaşdırmalı, cinayət hadisəsi haqqında olan fərziyyələrin hamısını yoxlamaqla baxışı ətraflı aparmalı, statik və dinamik baxışın ardıcıllığına ciddi riayət etməli, maddi sübutların cinayət hadisəsi ilə əlaqəli olub-olmamasını müəyyən etməli, cinayət izlərini aşkar edib və qeydə alaraq, əhəmiyyət kəsb edən əşyaların vəziyyətini və onların üzərindəki izlərin hansı qaydada yerləşmələrini dəqiqləşdirməli, iş üçün əhəmiyyət kəsb edən izlərin və

digər maddi sübutların fotoşəklini çəkməli, hadisə yerinin sxemini tərtib etməli, hadisə yerinə baxışı prosessual qaydada düzgün rəsmiləşdirilməli, cinayət alətlərinin axtarışını təmin etməlidr.

Hadisə yerinə baxışın işçi mərhələsi.

Bu mərhələ öz növbəsində statik və dinamik baxışa ayrılır. Statik baxışda sahənin sərhədini müəyyənləşdirmək məqsədi ilə hadisə yeri ümumi nəzərdən keçirilir. Baxışın hansı ardıcıllıqla aparılması aydınlaşdırılır, istiqamətləndirici və icmal fotoşəkillər çəkmək üçün yer seçilir və s. Bundan sonra müstəntiq baxışın iştirakçıları ilə birlikdə hadisə yerində hansı obyektlərin olmasını, bunların yerləşmə vəziyyətini və qarşılıqlı əlaqəsini müəyyən edir və həmin obyektlərin xarici görünüş və quruluşunu öyrənir.

Statik baxış zamanı hadisə yerinin vəziyyətində heç bir dəyişiklik aparılmır və hər şey olduğu kimi qalır. İstintaq təcrübəsindən məlumdur ki, bəzən təcrübəsi az olan müstəntiqlər hadisə yerində mühüm maddi sübut gördükdə (məsələn, cinayətin törədilməsində istifadə olunan silah) dərhal onu götürüb nəzərdən keçirirlər. Bu isə sonradan silahın hansı yerdə və vəziyyətdə yerləşməsi haqqında məsələni aydınlaşdırılmasında çətinlik törədir. Odur ki, baxışın statik mərhələsində iş üçün maddi sübut əhəmiyyətli halları planda qeydə almaq, hadisə yerinin və ətraf yerlərin fotoşəkillərini çəkmək, predmetlərin hansı vəziyyətdə olmasını ilk növbədə qeyd etmək lazımdır.

Hadisə yerinin vəziyyəti qeyd edildikdən sonra baxışın dinamik mərhələsi başlanır. Dinamik baxışın məzmunu hadisə yerindəki izlərə, kompyuter avadanlılarına və başqa maddi sübutlara hərtərəfli baxışın keçirilməsi və bunların kriminalistik elmi-texniki üsül və vasitələrdən istifadə edilərək möhkəmləndirilməsindən ibarətdir. (Məsələn, müxtəlif tozlar vasitəsilə kompyuter avadanlıqlarının və ya klaviaturalarının üzətində əl-barmaq izlərinin aşkar olunması və daktiloplyonkaya köçürülməsi və s.).

Ümumiyyətlə, dinamik baxışda obyektlərə mükəmməl və ətraflı baxış keçirilir və bu məqsədlə əşyalar yerindən tərpədilir, çevrilir və s. hərəkətlər edilir.

Hadisə yerində və onun ayrı-ayrı obyektlərində cinayətin və cinayətkarın izlərinin axtarışı və onların aşkar edilməsi üçün mümkün olan bütün tədbirlər görülür, üzərində iz qalmış obyektlər, yaxud obyektlərin qalmış hissələri götürülür. Obyektin baxılacaq sahəsinin sərhədi qabaqcadan müəyyənləşdirilməlidir. İstintaq təcrübəsi göstərir ki, müstəntiq baxış aparılacaq sahəsinin sərhəddini bəzən əvvəlcədən deyil, baxış aparan zaman müəyyən edir. Bunu düzgün hesab etmək olmaz. Çünki, baxış keçiriləcək sahənin sərhədi qabaqcadan müəyyən edilmədikdə onun mühafizəsini təşkil etmək mümkün olmur, bu isə cinayətin araşdırılması üçün əhəmiyyəti olan izlərin və digər maddi sübutların itməsi ilə

nəticələnə bilər.Kibercinayətlər üzrə hadisə yerinə baxiş zamani aşağidakı tıdbirlər həyata keçirilir:

- hadisə yerində olan mövcud şəraiti qeydə almaq;

- hadisə yerində olan texniki vasitələrə, proqram sisteminə hər hansı bir şəxsin müdaxilə edilməsinin qarşısını almaq üçün tədbirlər görmək;

- baxış keçirilən yerdə olan kompyuterlərin lokal hesablayıcı sistemə qoşulub-qoşulmamasını müəyyən etmək;

- baxış keçirilən yerdə olan kompyuterlərin digər otaqlarda olan vasitələrlə, hesablayıcı texnika ilə qoşulmasını yoxlamaq;

- kompyuterin telefona və ya teletayp sisteminə qoşulmasını yoxlamaq;

- EHM – proqramların yüklənməsi, əgər yüklənibsə onda hansı proqramlardır. Tədqiq olunan kompyuter sistem blokunun əməliyyat birləşmə yerləri kağızla tam örtərık möhürlənmək;

- maqnit daşıyıcılar yumşaq materiala bükülərək zərfə qablaşdırmaq və möhürlənərək üzərində zəruru qeydlər aparmaq;

- tədqiq olunan lazer disklər, disketlər, smartfonlar, mobil telefonlar və sair bu kimi obyektlər ayn-aynlıqda qablaşdırmaq;

Baxışın iş mərhələsində hər bir obyekt ayrı-ayrılıqda tədqiq olunmalıdır. Mütəxəssis kompyuter disklərində olan məlumatlara baxıb, analiz aparmalı, lazım gələrsə silinmiş faylları bərpa etməlidir. Baxış keçirərkən kompyuter texnikasının və maqnit

daşıyıcılarının üzərində zədələrin olub-olmamasını müəyyən etmək kifayət deyil, onların qapı və pəncərələrin, həm də bağlayıcı qurğuların vəziyyətini yoxlayıb qeyd etmək lazımdır. Proqramların hərəkətinə fikir vermək, faylların məzmununa və bazada olan məlumatlara da baxış keçirmək məqsədə müvafiqdir. Cinayətə münasibəti olan şəxsləri müəyyən etmək məqsədilə klaviaturada, EHM gövdəsinin, monitor və printerin üzərində olan əl-baqmaq izləri, mirkohissəçiklər aşkar edilərək götürülür.

Baxış zamanı kompyuter bütün hissələrinin neçə yerləşməsi, onların hissələrinin bir-birinə nisbətən vəziyyəti, model nömrəsi, hər bir detalın seriya nömrələri, mühasibatlıq tərəfindən qoyulan inventar nömrələri, fabrik yarlıqlarına olan digər məlumatlar protokolda qeyd edilməlidir.

Əgər kompyuterlər götürülürsə, onlarla işlənmiş şəbəkədən istifadə edən əməkdaşların adlarını, parollarını öyrənmək vacibdir. Kompyuterlərin hamısı, maqnit daşıyıcıları, işçilərin qaralama qeydləri götürülməlidir. Həmin kompyuterlərdə işləyən bütün şəxslərin, onlara xidmət göstərib təmir edənlərin, proqramlar hazırlayanların və s. mütəxəssislərin pasport qeydləri, ünvanları və daimi yaşadıqları yerləri göstərməklə siyahıları tərtib olunub götürülməlidir.

Hadisə yerinə baxış keçirib göstərilən sənədləri və məlumatları alandan sonra müstəntiq fakt əsasında cinayət işi başlayır və ibtidai istintaq aparır istintaq zamanı müstəntiq şahidləri dindirilir. Dindirmədən

əvvəl həmin istintaq hərəkətinin keçirilməsinə hazırlıq mərhələsində dindiriləcək şəxsin şəxsiyyətinin öyrənilməsi mühüm əhəmiyyət kəsb edir. Yadda saxlamaq lazımdır ki, bu kateqoriyalı cinayət işləri üzrə şahidlər yüksək intellektual səviyyəli, ali təhsilli, xüsusi terminologiyanı, kompyuter texnikasını, sistemini, şəbəkəsini və interneti mükəmməl bilən şəxslərdir.

b) Kibercinayətlər üzrə dindirmə və onun keçirilməsinin taktiki üsulları.

Kibercinayətlərlə bağlı dindirmənin həyata keçirilməsi bu növ cinayətlərin törədilməsi mexanizminin spesifikliyindən daha çox asılıdır. Kriminalistik nöqteyi nəzərdən dindirmə istintaq hərəkəti kibercinayəti törədən şəxsin ifşa olunmasında, həmçinin istintaqa qarşıdurmanın qarşısının alınması, fərziyyələrin qurulması istiqamətində vacib əhəmiyyət kəsb edir. Kibercinayətlərlə bağlı cinayət işlərinin təhlili göstərir ki, dindirmə və üzləşdirmə zamanı müstəntiq bir sıra çətinliklərlə rastlaşır. Məsələn, 71% respandetlər göstərir ki, kibercinayətlərlə dindirmə zamanı rast gəlinən əsas çətinliklərdən biri də bu sahədə mövcud terminologiyadan kifayət qədər bilməmələri ilə izah olunur. Bəzi hallarda müstəntiq bu sahədə kifayət qədər biliyə malik olmadığından onun dindirilən şəxslə intelektual qarşıdurmaya gətirib çıxarmasına səbəb olur. Ona görə də kibercinayətlərlə bağlı dindirmə zamanı xüsusi biliklərə malik mütəxəssislərin dəvət olunması məqsədəmüvafiq

olardı. Digər bir tərəfdən kibercinayətlər üzrə sübut və dəlillərin tez itməsi və məhv olması isə dindirmənin gedişatına məfi təsir göstərir.

Kibercinayətlərin araşdırılmasında dindirmə zamanı müsbət nəticələrin əldə olunması müstəntiqin dindirməyə hazırlıq zamanı həyata keçirdiyi tədbirlərdən xeyli dərəcədə aslıdır. Eyni zamanda kibercinayətin araşdırmasını həyata keçirən müstəntiqin məlumat təminatı və onun bu sahədə biliyi, köməkçi məlumatlarla davranışı isə dindirmənin təşkilati-taktiki məsələlərinə müsbət təsir göstərir. Dindirməyə hazırlıq dedikdə, kibercinayətlərin araşdırılması zamanı dindirilən şəxsəndən tam və düzgün ifadələrin alınmasını təmin edən kompleks ilkin hazırlıq tədbirləri başa düşülür. Kibercinayətlərlə bağlı dindirməyə hazırlıq tədbirlərinə aiddir :

1)cinayət işi materiallarının, həmçinin kibercinayətlərlə bağlı zəruri olan xüsusi ədəbiyyatların hərtərəfli öyrənilməsi;

2)kompyuter sahəsində istifadə olunan xüsusi terminologiyalarla tanış olmaq;

3)kibercinayəti törədən şəxsə sübutların təqdim olunma üsulunun müəyyən edilməsi;

4)bu sahə üzrə mütəxəssislərlə məsləhətlər aparmaq;

5)kompyuterin iş prinsipi ilə yaxından tanış olmaq; cinayətin törədilməsi mexanizmi, həmçinin istifadə olunankompyuter texniki vasitələr barədə məlumat əldə etmək;

6)iş üzrə əvvəlcə dindirilmiş şəxslərin ifadələrində qarşıdurmanın səbəbini və yalan ifadələri müəyyənləşdirmək;

7)cinayətlə bağlı əldə edilən dəlillər barədə məlumatları ətraflı təhlil etmək;

8)dindirilən şəxsin şəxsiyyətini xarakterizə edən məlumatların toplanması və öyrənilməsi;

9)dindirməyə çağırış qaydasının müəyyən edilməsi;

10) dindirmənin yerinin və vaxtının müəyyən;

11) dindirmə zamanı tətbiq ediləcək texniki vasitələrin hazırlanması.

Kibercinayətlərin araşdırılması zamanı dindirmədən əvvəl cinayət işinin materiallarının öyrənilməsi dedikdə, istintaq hərəkətləri protokollarının, maddi sübutların, ekspert rəyinin, sənədlərin, habelə əməliyyat axtarış tədbirləri vasitəsilə əldə olunmuş məlumatların, bir sözlə işdə mövcud olan sübutların təhlili və qiymətləndirilməsi başa düşülür. Materialları hərtərəfli öyrənməklə müstəntiq istintaq zamanı sübut edilməli olan halları, dindirilməli olan şəxslərin dairəsini, dindirmənin predmetini, dindirilən şəxsin hansı məlumatlara malik olduğunu, dindirmə zamanı şəxsə veriləcək sulları, dindirmə zamanı şəxsin yalan ifadə vermə hallarını asanlıqla müəyyən edə bilər.

Kibercinayətlər üzrə dindirmə zamanı psixoloji kontaktın yaradılması və dindirmənin düzgün taktikasının secimi uçun müstəntiq dindirilən şəxsin

şəxsiyyətini xarakterizə edən kifayət qədər məlumat toplamalı və öyrənməlidir. Belə məlumatlara aiddir: dindirilən şəxsin mənəvi simasını, psixoloji xüsusiyyətlərini, həyat tərzini, intellektual səviyyəsini, işdə iştirak edən digər şəxslərlə olan münasibətlərini və s. Dindirilən şəxs haqqında məlumatlar onun iş yerindən, təhsil aldığı müəssisədən xasiyyətnamələr almaqla; iş yoldaşlarının, qonşularının, yaxınların sorğusu; məhkəmə-psixoloji ekspertizasinin nəticələri əsasında, müxtəlif istintaq və əməliyyat axtarış tədbirlər həyata keçirməklə əldə olunur.

Kibercinayətlərlə bağlı dindirməyə hansı qaydada çağrılması dindirmənin nəticəsinə təsir göstərən əsas amillərdəndir. CPM 226-cı maddəsinə görə şəxs dindirməyə cağırış vərəqəsi, teleqram, telefonaqram, faksoqram vasitəsilə cağrıla bilər. Dindirməyə çağırış qaydasının müəyyən edilməsi kibercinayətlərin araşdırılmasında yaranmış konkret istintaq şəraitindən aslıdır. Şəxsi (barəsində həbs qətimkan tədbiri secilmiş şəxslər istisna olmaqla) dindirməyə çağırarkən müstəntiq calışmalıdır ki, bu barədə kənar şəxslər- iş yoldaşları, qonşular və s. xəbərdar olmasınlar. Bu tədbir ilk növbədə dindirilən şəxsə işdə marağı olan şəxslər tərəfindən qanunsuz təsirin qarşısını almaq üçün görülür.

Dindirmənin vaxtı kibercinayətlər üzrə dindirilən şəxsin prosessual vəziyyətindən, şəxsin törədilən kibercinayət barədə malik ola biləcək məlumatdan, habelə dindirilən şəxsin işdə iştirak edən digər

şəxslərlə münasibətindən aslıdır. AR CPM görə təqsirləndirilən şəxs ona ittiham elan edildikdən dərhal sonra; şübhəli şəxs isə onun tutulmasından və ya barəsində qətimkan tədbirinin tətbiq edilməsi barədə qərar ona elan edildikdən dərhal sonra dindirilməlidir. Şahid və zərərçəkmiş şəxsin dindirilməsi isə mümkün qədər tez aparılmalıdır. Çünki məhz onların ifadələri cinayətkarı ifşa etməyə, cinayət işi üzrə obyektiv həqiqəti müəyyən etməyə imkan verir.

Dindirmə bir qayda olaraq müstəntiqin otağında aparılır. Lakin bəzi hallarda dindirməni kibercinayətin törədildiyi hadisə yerində aparmaq daha məqsədəuyğundur. Çunki məhz hadisə yerində aparılan dindirmə şəxsə cinayət işi üçün əhəmiyyət kəsb edən halları yada salmağa kömək edir. Ahıl yaşlı şəxslər və xəstələr onların olduqları yer üzrə dindirilməsi daha məqsədəuyğudur..

Dindirmənin ümumi qaydaları cinayət-prosessual qanunvericiliklə müəyyən edilmişdir. Lakin onun prosessual qaydalarından fərqli olaraq taktiki üsullar qanunvericilik tərəfindən göstərilməmişdir. Qanun bununla da müstəntiqə kibercinayətlər üzrə də dindirmə zamanı müxtəlif taktiki üsullardan hər hansı birini seçməsinə və tətbiq etmək üçün geniş imkanlar verir.

Düzgün və tam ifadə almağı, habelə dindirmənin səmərəli qaydada təşkil edilməsini təmin edən taktiki üsullar dindirmənin taktikasını təşkil edir. Dindirmənin taktikası – konkret cinayət işinin hallarını,

dindirilən şəxsin xüsusiyyətlərini və dindirmə şəraitindən aslı olaraq tətbiq olunan taktiki üsulların məcmusudur. Kibercinayətlər üzrə dindirmə taktikasının məqsədi dindirilən şəxsdən obyektiv həqiqəti əks etdirən məlumatın alınmasıdır. Bu növ cinayətlər üzrə dindirmənin səmərəli nəticə verməsi hər bir halda düzgün taktikanın seçilməsindən aslıdır. Məhz bu səbəbdən taktiki üsul kibercinayətlər üzrə dindirilən şəxsin fərdi xüsusiyyətlərinə, müstəntiqin hansı informasiyaya malik olmasına və dindirmənin şəraitinə müvafiq olaraq müəyyən edilməlidir. Kibercinayətlər üzrə düzgün seçilmiş və səmərəli tətbiq edilmiş taktiki üsul tam və doğru ifadələrin alınmasına, şəxsin yalan ifadə vermək hallarının ifşa edilməsinə, habelə onların yoxlanılmasına imkan verir.

Dindirmənin taktiki üsulları müəyyən tələblərə cavab verməlidir. Taktiki üsullar cinayət-prosessual qanunvericiliyə, habelə mənəvi prinsiplərə uyğun olmalıdır. Bu baxımdan dindirilən şəxsin şərəf və ləyaqətini alçaldılması ilə müşayət olunan taktiki üsullardan istifadə etmək, habelə fiziki, yaxud mənəvi zor tətbiq olunması yolverilməzdir.

Kibercinayətlər üzrə dindirmənin taktiki üsulları onun növündən, dindirilən şəxsin prosessual vəziyyətindən aslı olaraq müəyyən edilməlidir.

Kibercinayətlərlə bağlı şahidin dindirilməsi taktikası. Şahid dedikdə, iş üzrə əhəmiyyət kəsb edən hallardan xəbərdar olan şəxs başa düşülür (CPM 95.1). Şahid cinayət təqibi üçün əhəmiyyət kəsb edən hər

bir hal üzrə, o cümlədən şübhəli, təqsirləndirilən, zərərçəkmiş şəxsin, digər şahidlərin şəxsiyyəti barədə dindirilə bilər (CPM 227). Kibercinayətlərin araşdırılmasında şahidin dindirilməsi zamanı müstəntiq cinayət işinin və şahidin spesifik cəhətləri nəzərə alınmaqla konkret taktiki üsullardan istifadə etməlidir. Bu taktiki üsulların əsas məqsədi şahidin iş üçün əhəmiyyət kəsb edən hallara dair doğru ifadə verməsinə nail olmaqdır.

Dindirmədən əvvəl müstəntiq kibercinayət üzrə üzrə çağrılan şahidlərin hansı ardıcıllıqla dindiriləcəyini taktiki cəhətdən düzgün müəyyən etməlidir. Bunun üçün şahidlərdən hansının hadisəni bilavasitə və hansı şəraitdə müşahidə etməsinə, şahidin işin nəticəsində maraqlı olub-olmamasına və s. bu kimi hallara fikir verilməlidir. İlk öncə istintaq üçün əhəmiyyət kəsb edən hallar və faktlar barəsində düzgün ifadə verməsi ehtimal olunan şahidlər dindirilməlidir. Habelə bu növ cinayətlər üzrə şahidlərin dindirilməsi ardıcıllığını müəyyən edərkən hadisələrin xronoloji axını da nəzərə alınmalıdır. Belə ki, əvvəlcə nisbətən uzaq keçmişə aid məlumat verə bilən şahidlərin dindirilməsi məqsədəmüvafiqdir. İşin nəticəsi ilə maraqlı olan şəxslərin əvvəlcə dindirilməsi taktiki cəhətdən düzgün deyildir. Çünki belə şəxslərin doğru ifadə verə bilməyəcəyi ehtimal olunur. Eyni fakta dair ifadə verən şahidlərin hamısı dindirilməlidir. Belə ki, şahidlərin hamısı eyni faktı heç də eyni dərəcədə qavramırlar.[4]

Müstəntiq hər bir şahidi digər şahidlərdən ayrı dindirməlidir və dindirmə qurtaranədək eyni iş üzrə çağrılmış şahidlərin öz aralarında ünsiyyətdə olmaması üçün tədbirlər görməlidir (A.R CPM 227.3). Qanunun bu tələbinin əsas məqsədi şahidlər arasında informasiya mübadiləsinin qarşısını almaqdır. Çünki şahidlər arasında informasiya mübadiləsi onların ifadələrinin obyektivliyinə təsir edə bilər. Ona görə də, müstəntiq mümkün qədər eyni iş üzrə olan şahidləri müxtəlif vaxtlarda dindirməlidir.

Kibercinayətlərin araşdırılmasında dindirmədən əvvəl müstəntiq şahidin şəxsiyyətini müəyyən edir, ona hansı iş üzrə cağrıldığı barədə məlumat verir və iş üzrə ona məlum olan bütün hallar barədə danışmaq vəzifəsi, habelə ifadə verməkdən imtina etməyə, boyun qaçırmağa, bilə-bilə yalan ifadə verməyə görə cinayət məsuliyyəti barədə xəbərdarlıq edir. Bundan sonra müstəntiq şahidlə şübhəli, təqsirləndirilən, zərərçəkmiş şəxslə münasibətlərini müəyyənləşdirir və dindirməyə başlayır. Dindirmə şahidə cinayət təqibi ilə bağlı bütün halları danışmaq təklifi ilə başlanılır və bundan sonra ona suallar verilə bilər (CPM 227).

Taktiki baxımdan şahidin ilk öncə sərbəst danışıq formasında ifadə vermənin nəzərdə tutulması həm şahid, həm də müstəntiq üçün mühüm əhəmiyyət kəsb edir. Belə ki, şahid öz fikrini cəmləşdirə, unutduğu halları yadına sala, onların ardıcıl danışa bilər. Bu zaman müstəntiq şahidin psixologiyası, xarakteri, yada salma qabiliyyəti barədə müəyyən nəticəyə gəlir, iş

üzrə istintaq məlum olmayan yeni halları da müəyyənləşdirir. Habelə, şahidin sərbəst danığı müstəntiqə ifadənin doğruluğu barədə nəticə çıxarmağa imkan verir. Şahid sərbəst danışarkən ona suallar vermək məqsəduyğun deyil, çünki bu şəxsə öz fikrini cəmləşdirə bilməsinə mane ola, bəzən hətta mənfi psixiloji təsir də göstərə bilər. Kibercinayətlər üzrə dindirmənin sərbəst danışıq formasında aparılması şahidin düzgün olmayan məlumat vermək və yaxud yalan ifadə vermə ehtimalını azaldır. Müstəntiq dindirmə zamanı şahidə sual verməyə tələsməməlidir. Belə ki, müstəntiq bir qayda olaraq şahidin hansı hallardan xəbərdar olduğunu bilmir, şahid isə müstəntiqin ondan soruşacağından daha çox informasiyaya malik ola bilər. Habelə sərbəst danışıq formasında dindirilən şahid bəzən müstəntiqin ümumiyyətlə məlumatı olmayan hallar barədə xəbər verə bilər.

Bəzən təcrübədə müstəntiqlər şahidin dindirilməsini sərbəst danışıq formasında deyil, suallar verməklə həyata keçirməyə üstünlük verirlər. Belə dindirmə forması taktiki cəhətdən düzgün deyildir: 1) müstəntiqin sualları və ona cavablar bir qayda olaraq hadisəni bütünlüklə əhatə edə bilmir və bu da şahid ifadələrində boşluqlar yaranmasına gətirib çıxarır 2) müstəntiqin öz sualları ilə arzuolunan cavabı şahidin beyninə yeridə bilər 3) müstəntiqin öz sualları ilə işdə olan sübutları vicdansız şahid qarşısında açıqlaya bilər.

Azərbaycan Respublikasının CPM-nin 227.1 maddəsinə görə dindirmə şahidə cinayət təqibi ilə bağlı bütün halları danışmaq təklif ilə başlanılır və bundan sonra ona sullar verilə bilər. Göründüyü kimi, şahidə sual vermək müstəntiqin vəzifəsi deyil, hüququ kimi nəzərdə tutulmuşdur. Lakin bu o demək deyil ki, müstəntiq həmişə bu hüquqdan istifadə etməlidir. Şahid sərbəst surətdə ifadə verdikdən sonra müstəntiq zərurət olduqda ona suallarla müraciət edir. Burada zərurət dedikdə, şahidin ifadələrinin natamamlığı, qeyri-müəyyənliyi və işdə olan materiallarla ziddiyyət təşkil etməsi başa düşülür. Ona görə də müstəntiq tərəfindən şahidə sual verməyin əsas məqsədi onun ifadələrini tamamlamaq, dəqiqləşdirmək və yaxud yoxlamaqdır. Şahidlərə verilən sualların vahid sxemini göstərmək çətindir, çünki bu suallar iş üzrə konkret hallardan irəli gələrək olduqca müxtəlif məzmunlu ola bilər. Bununla belə, şahidə dindirmənin predmetinə dair aydın və konkret suallar verilməli və elə formulə edilməlidir ki, onlara ətraflı cavab almaq mümkün olsun.

Dindirmə zamanı bəzən şahidlər dindirmənin predmeti ilə bağlı müəyyən fikir və mülahizələr irəli sürürlər: cinayətin konkret şəxs tərəfindən törədilməsini və s. Müstəntiq belə hallara ciddi yanaşaraq şahidin hansı faktlara əsaslanıb belə fikrə gəldiyini aydınlaşdırmalıdır. Belə ki, faktlara əsaslanmayan fikir və mülahizələr nəzərə alınmır və heç bir sübuti əhəmiyyət kəsb etmir.

Şahidlər düzgün və yaxud yalan ifadə verməkdən aslı olaraq vicdanlı və vicdansız şahidlərə bölünürlər. Buna uyğun olaraq onların dindirilmə taktikası da fərqlidir. Təqsirləndirilən şəxslə tanışlığın və işin nəticəsində marağın olmaması, düzgün ifadə vermək istəyi, habelə yüksək mənəvi keyfiyyətlər şahidin vicdanlı olmasına dəlalət edən faktorlardır. Düzgün ifadə verməyə çalışan vicdanlı şahidlərin dindirilmə taktikasının əsas məqsədi istintaq üçün əhəmiyyət kəsb edən halların onların yadına salmaq və düzgün ifadə verməyə kömək etməkdir.

Vicdansız şahidlər dedikdə bilə-bilə yalan ifadə verən və yaxud ifadə verməkdən imtina edən şəxslər başa düşülür. Vicdansız şahidlərin dindirilməsi zamanı müstəntiq onların yalan ifadə vermə hallarını ifşa edən taktiki üsullardan istifadə etməlidir. Yalan ifadə verən şahidlərin dindirilməsinin özünəməxsus taktiki üsulları vardır. Hər şeydən əvvəl müstəntiq şahidin yalan ifadə verməsinə əmin olmalıdır və bunun üçün ifadənin özündəki ziddiyyətlər, habelə onun digər sübutlarla təzad yaradan cəhətləri aydınlaşdırılmalıdır. Sonra isə müstəntiq şahidin yalan ifadə verməsinin səbəblərini müəyyənləşdirməli və onları aradan qaldırmağa çalışmalıdır. Bu səbəblər müxtəlif ola bilər: şahidin işin nəticəsində maraqlı olması, təqsirləndirilən və ya zərərçəkmişlə şəxslə razılaşması, qisas almaq arzusu, qorxaqlıq, yoldaşlıq borcunun düzgün dərk edilməməsi və s.

Şahidin doğru ifadə verməsinə nail olmaq üçün müstəntiq ilk növbədə mənəvi təsir vasitələrindən istifadə etməlidir. O, şahidə başa salmalıdır ki, doğru danışmaq onun vətəndaşlıq borcu olub, cinayətkarlığa qarşı mübarizə aparmaq vəzifəsindən irəli gəlir, doğru danışmaqla o, həqiqətin üzə çıxarılmasında istintaq orqanlarına yaxından kömək etmiş olur və s.

Müstəntiq vicdansız şahidləri ifşa etmək və düzgün informasiya verməyə məcbur etmək məqsədilə onlara digər şəxslərin ifadələri daxil olmaqla işdə olan sübutları təqdim edə; digər şahidlərlə və yaxud təqsirini boynuna almış təqsirləndirilən şəxslə üzləşdirmə apara bilər. Bəzən şahid təqsirləndirilən şəxsin və yaxud onun qohumlarının qisas alacağından qorxaraq ifadə vermir. Belə halda müstəntiq onun təhlükəsizliyinin təmin edilməsi üçün tədbirlər görməli və düzgün ifadə verməsinə nail olmalıdır.

Bütün bunlar müsbət nəticə vermədikdə isə müstəntiq şahidə yalan ifadə üstündə cinayət məsuliyyəti daşımasını bir daha xatırlatmalı və bu cinayətə hansı növ cəzanın tətbiq edilməsini bildirməlidir.

Zərərçəkmiş şəxsin dindirilməsi taktikası. Zərərçəkmiş cinayət qanununda nəzərdə tutulmuş əməl nəticəsində birbaşa mənəvi, fiziki və ya maddi ziyan vurulmuş şəxsdir (CPM 87.1). Azərbaycan Respublikası CPM-nin 231-ci maddəsinə görə zərərçəkmişin dindirilməsi şahidin dindirilməsi üçün nəzərdə tutulmuş qaydalara müvafiq aparılır. Habelə

zərərçəkmişin dindirilməsi zamanı şahidin dindirilməsinin taktiki üsullarından istifadə olunur. Buna baxmayaraq zərəçəkmiş şəxsin dindirilməsinin özünəməxsus cəhətləri də vardır. Bu isə ilk növbədə zərərçəkmişin prosessual vəziyyəti və əksər hallarda hadisəni bilavasitə müşahidə etməsi ilə əlaqədardır. Məhz zərərçəkmiş şəxsin ifadələri müstəntiqə hadisə ilə bağlı fərziyyələrin qurulmasına və sübutların aşkarlanmasına imkan verir. Ona görə də, bir qayda olaraq ibtidai araşdırma zərərçəkmiş şəxsin dindirilməsi ilə başlanılır.

Kibercinayələr üzrə zərərçəkmiş şəxs fiziki və hüquqi səxsin nümayəndələri ola bilər. Zərərçəkmiş şəxsin dindirilməsi müstəntiqin onu bilə-bilə yalan ifadə verməyə, ifadə verməkdən imtina etməyə və ya boyun qaçırmağa görə cinayət məsuliyyəti barədə xəbərdar etməklə başlanılır. Sonra isə müstəntiq zərərçəkmiş şəxsə ona qarşı törədilmiş hadisəsi ilə bağlı hər bir şeyi söyləməyi təklif edərək, sərbəst danışmaq imkanı yaradır. Zərərçəkmiş sərbəst surətdə ifadə verdikdən sonra, müstəntiq ifadəni dəqiqləşdirmək, onu tamamlamaq və yaxud onun düzgünlüyünü yoxlamaq məqsədilə sual verə bilər.

Ümumiyyətlə zərərçəkmiş şəxs işin nəticəsində maraqlı olması onun ifadələrinin obyektivliyinə təsir göstərir. Zərərçəkmiş şəxsin ifadələri əksər hallarda ittiham xarakterli olur. Lakin zərərçəkmiş şəxsin işin nəticəsində maraqlı olması özlüyündə heç də o demək deyildir ki, onun ifadəsi bütün hallarda şübhə altına

alınmalıdır. Buna görə də, zərərçəkmiş şəxsin ifadələrinə formal yanaşılmamalı və digər sübutlar ilə müqayisəli şəkildə, bərabər əsaslarla qiymətləndirilməlidir.

Bir sıra hallarda zərərçəkmiş şəxs müəyyən səbəblərdən doğru ifadə vermir, işın mühüm əhəmiyyət kəsb edən cəhətlərini demir, yaxud ifadə verməkdən yayınmağa çalışır. Bu müxtəlif səbəblərdən ola bilər: zərərçəkmiş şəxs özünün hər hansı qeyri-qanuni hərəkətinin ifşa olunmasından, onu nüfuzdan salan məlumatların yayılmasından, müəyyən faktı, etiraf etməkdən və s.

Ümumiyyətlə müstəntiq zərərçəkmiş şəxsə qarşı diqqətli olmalı, şəfqət göstərməli, onu cinayətin üstünün tezliklə açılmasına və cinayətkarın cəzalandırılmasına inandırmalıdır. Çünki məhz belə münasibət zərərçəkmişlə psixoloji kontaktın yaradılmasına imkan verir.

Kibercinayətlərin araşdırılması zamanı şübhəli şəxsin dindirilməsi onun tutulduğu andan və ya barəsində qətimkan tədbirinin tətbiq edilməsi barəsində qərar ona elan edildikdən dərhal sonra aparılır (CPM 232.1). Şübhəli şəxsin dindirilməsi təqsirləndirilən şəxs üçün nəzərdə tutulmuş prosessual qaydada həyata keçirilir (CPM 232.5). Lakin buna baxmayaraq, onların aparılma taktikası fərqlidir. Bu da onların prosessual vəziyyətindən və işdə olan sübutlarla təqsirinin müəyyən edilməsi dərəcəsindən irəli gəlir.

Ümumiyyətlə şübhəli şəxsin dindirilməsi müəyyən psixoloji xüsusiyyətlərə malikdir:1) dindirmə zamanı şübhəli şəxs özünü müdafiə etmək və həqiqətin gizlədilməsinə çalışması 2) şübhəli şəxsin müstəntiqə mənfi münasibət və apatiya bəsləməsi 3) şübhəli şəxsin psixi gərginlik və çaşqın vəziyyətdə olması 4) şübhəli şəxsin müstəntiqin hansı sübutlara malik olduğunu öyrənmək istəyi. Dindirmənin dərhal aparılması tələbi təkcə şübhəli şəxsin hüquqlarının pozulmaması üçün prosessual təminat deyil, həm də taktiki əhəmiyyət kəsb edir. Belə ki, kibercinayətlər üzrə dindirmə dərhal aparıldıqda şübhəli şəxs qanunsuz vasitələrlə özünü müdafiə etmək üçün tədbirlər görməyə vaxt tapmır və iş üçün əhəmiyyət kəsb edən hallara dair doğru ifadə verməyə məcbur olur.

Kibercinayətlər üzrə şübhəli şəxsin dindirilməsinin əsas xüsusiyyyətlərindən biri dindirməyə hazırlığın çox az müddətdə baş verməsidir. Buna görə də bir sıra hallarda müstəntiq şübhə edilən şəxsin şəxsiyyətini xarakterizə edən hallara dair məlumata malik olmur. Ona görə də müstəntiq bu halları bilavasitə dindirmə prosesində müəyyən etməli və buna müvafiq taktiki üsul seçməlidir.

Kibercinayətlər üzrə dindirməyə hazırlıq zamanı, şübhə edilən şəxsin cinayətdə iştirakının dərəcəsi, onun digər şübhəli şəxslərlə münasibəti, hansı əsasa görə tutulması da nəzərə alınmalıdır. Bu kimi hallara dair məlumatları iş üzrə toplanmış materiallar vasitəsilə

aydınlaşdırmaq olar. Göstərilən məlumatlar şübhəli şəxsə veriləcək sulların dairəsini, dindirmənin vaxtını, ardıcıllığını və s. müəyyənləşdirməyə imkan verir. Eyni zamanda bu növ cinayətlər üzrə şübhəli şəxsə verilən sualların dairəsi və ardıcıllığı isə həmin şəxsin kompyuter sahəsində hansı bilik və vərdişlərə malik olmasından asılıdır.

Müstəntiq dindirmədən əvvəl şübhəli şəxsi hansı faktlar barəsində xəbərdar edəcəyini, hansıları isə gizli saxlayacağını müəyyən etməlidir. Belə faktların qabaqcadan müəyyən edilməsi dindirmə zamanı mühüm rol oynayaraq, şübhəli şəxsin yalan ifadə vermə hallarının ifşa edilməsinə, habelə şübhəli şəxsin onun tərəfindən törədilmiş, lakin istintaqa məlum olmayan cinayətlərə dair ifadə verməsinə imkan vermış olur.

Müstəntiq dindirməyə şübhəli şəxsə şübhə barəsində və onun mülahizələrinə görə iş üçün əhəmiyyət kəsb edən bilən digər hallar barədə ifadə vermək təklifi ilə başlayır. Bu zaman müstəntiq şübhə edilən şəxsin cinayətin baş verdiyi yerə necə və nə üçün gəlməsi; həmin təşkilatda, idarədə, müəsissədə hansı müddət ərzində fəaliiət göstərməsi və fəaliyyət funksiyasının nədən ibarət olması; kompyuter sahəsində biliyi, bacarığı və proqramlara yiyələnmə dərəcəsi; hansı şəraitdə tutulması; hadisə yerində onu kimlərin görməsi; hansı cinayət alətlərinin onda olması və nə üçün bu alətləri əldə etməsi; onun özündə, iş yerində yaxud mənzilində cinayətin aşkar izlərinin

olduğunu nə ilə izah etməsi və s. aydınlaşdırılmalıdır. Yaranmış istintaq şəraitindən asılı olaraq kibercinayətlər üzrə dindirmədə şübhəli şəxsə verilən sualların dairəsi barədə məlumat xüsusi kriminalistik ədəbiyyatda kifayət qədər əks olunmuşdur

Şübhəli şəxsin dindirilməsi zamanı belə bir cəhət nəzərə alınmalıdır ki, şübhəli şəxs adətən müstəntiqdə onu ifşa etmək üçün kifayət qədər sübut olmadığını düşünür. Ona görə də həqiqəti müstəntiqdən gizlətməyə və bununla da şübhənin əsassızlığını sübuta yetirməyə çalışır. Belə hallarda müstəntiq sərəncamında olan ifşaedici sübutları ona elan etməlidir. Nəticədə şübhə edilən şəxs fakt qarşısında qalaraq həqiqəti etiraf etməli olur.

İstintaq şəraitindən asili olaraq kibercinayətlər üzrə dindirmədə müstəntiq daha çox inandırma metoduhdan istifadə edir.

İstintaq təcrübəsi göstərir ki, bu növ cinayətlər dindirmə daha çox münaqişəli olur, çünki kibercinayət törədən şəxs məsuliyətddən qaçmaq və ya onu müəyyən qədər yüngülləşdirmək məqsədilə qünahını ya qismən qismən etiraf edir və yaxud tamamilə inkar edir.

Əksər hallarda şübhəli şəxs məsuliyyətdən yaxa qurtarmaq üçün müxtəlif üsullardan istifadə edirlər: düzgün olmayan məlumatlar verir və yaxud müəyyən alibi irəli sürür. Hər bir halda onun ifadələri dəqiq yoxlanılmalıdır. Əsas yoxlama üsulu isə şübhəli şəxsin

ətraflı dindirilməsi və onun ifadələrinin işdə olan digər sübutlarla müqayisə edilməsidir.

Əgər dindirmə zamanı şübhəli şəxs cinayətin törədilməsini etiraf edirsə müstəntiq bununla kifayətlənməyib onu daha ətraflı dindirməli və işdə olan digər dəlillərlə yoxlamalı və sübutlarla əsaslandirmalıdır. Bəzi hallarda şübhəli şəxs daha ağır cinayətə görə məsuliyyətdən yaxa qurtarmaq üçün cinayətdə təqsirkar olduğunu etiraf edə bilər.

Dindirmə zamanı şübhəli şəxs bir qayda olaraq öz həyəcanını, əsəbi vəziyyətdə olmasını, nədənsə narahat olduğunu hərəkətlərində nümayiş etdirir. Müstəntiq şübhəli şəxsin davranışına fikir verməklə, dindirmə zamanı hansı məsələlərin onun üçün əhəmiyyət kəsb etdiyini müəyyən edə bilər. Şübhəli şəxsin belə davranışları sübut əhəmiyyət kəsb etməsə də dindirmənin hansı istiqamətdə həyata keçirilməsinə müəyyən etməyə imkan verir.[4] Lakin dindirmə zamanı şübhəli şəxsin bu və ya digər davranışı onun təqsirini sübut edən dəlil kimi qiymətləndirilməməlidir. Çünki belə davranış dindirmənin predmeti ilə bağlı olmayıb digər hallardan da irəli gələ bilər.

Kibercinayələr üzrə təqsirləndirilən şəxsin dindirilməsi.Təqsirləndirilən şəxsin dindirilməsi ona ittiham elan edildikdən sonra aparılmalıdır.

[4] Ратинов А. Р., Гаврилов О. А. Использование данных психологии в буржуазной криминалистике. В сб.: « Вопросы криминалистики ». № 8-9, М., 1963, s. 306-307

Təxirəsalınmaz hallar istisna olmaqla, təqsirləndirilən şəxsin dindirilməsi yalnız gündüz vaxtı mümkündür.

Kibercinayələrin araşdırılmasinin hərtərəfli, tam və obyektiv həyata keçirilməsi, habelə iş üzrə həqiqətin müəyyən edilməsində təqsirləndirilən şəxsin ifadələrinin böyük rolu vardır. [5] Bu da təsadüfü deyildir, çünki təqsirləndirilən şəxs cinayət hadisəsi barədə şahid və zərərçəkmiş şəxsdən fərqli olaraq daha cox məlumata malikdir. Təqsirləndirilən şəxs ona elan edilmiş ittihamın mahiyyətinə dair, habelə iş üzrə ona məlum olan bütün hallar haqqında ifadə vermək hüququna malikdir. O, dindirmə zamanı elan edilmiş ittihama münasibətini bildirir və bununla əlaqədar olaraq işdə olan sübutları izah edir və onların həqiqiliyi haqqında mülahizələrini bildirir.

Kibercinayələr üzrə təqsirləndirilən şəxsin dindirilməsinin özünəməxsus cəhətləri vardır. Bu da təqsirləndirilən şəxsin işin nəticəsində maraqlı olduğundan, ifadə verməkdən imtina etmək hüququnun və cinayət hadisəsi barədə şahid, zərərçəkmiş şəxsdən daha cox məlumata malik olmasından irəli gəlir.

Kibercinayələr üzrə təqsirləndirilən şəxsin dindirilməsinin əsas məqsədi ondan iş üçün əhəmiyyət kəsb edən hallar barədə düzgün ifadə almaqdır. Dindirmə zamanı müstəntiq təqsirləndirilən şəxsin nə zaman, harada və nəyin təsiri altında cinayəti törətməyə qərara gəldiyini; cinayətin hazırlıq

[5] Mövsümov C. Azərbaycan SSR Cinayət prosesi. Bakı, 1980, s. 203.

mərhələsində nə kimi hərəkətlər etdiyini və bu zaman ona kömək edən şəxslərin dairəsini; cinayət törədərkən hansı üsul, konpüter texniki vasitələrdən istifadə etdiyini; öz məqsədinə nail olub-olmadığını; cinayəti törətdikdən sonra kompyuterdə izlərin itirilməsi üçün hadisə yerində nə kimi hərəkətlər etdiyini; cinayət məsuliyyətinə cəlb olunduğu ana qədər kompyuter sahəsində yol verdiyi hərəkətləri aydınlaşdırmalıdır. Onu da qeyd etmək lazımdır ki, təqsirləndirilən şəxsin dindirilməsinin predmetini təkcə ittihamın formulası ilə məhdudlaşdırmaq olmaz. Təqsirləndirilən şəxs həmçinin cinayət təqibini istisna edən və məsuliyyəti yüngülləşdirən hallar barədə də dindirilməlidir.

Kibercinayələrin araşdırılmasında təqsirləndirilən şəxsin dindirilməsinin hazırlıq mərhələsində müstəntiq onu hansı ardıcıllıqla dindiriləcəyini aydınlaşdırmalır. Bu zaman aşağıdakı hallar nəzərə alınmalıdır: 1) təqsirləndirilən şəxs bu və ya digər cinayətin edilməsində nə kimi rol oynadığını; 2) toplanmış materiallar hansı təqsirləndirilən şəxsin təqsirini daha inandırıcı surətdə sübut edir; 3) təqsirləndirilən şəxslərin bir-birinə münasibəti; 4) təqsirləndirilən şəxsin öz hərəkətlərinə münasibəti; 5) təqsirləndirilənin şəxsiyyətini xarakterizə edən hallar. Taktiki baxımından cinayətin təşkilatçılarının, təhrikçilərinin və ya köməkçilərinin əvvəlcə dindirilməsi daha məqsədəmüvafiqdir. Çünki belə təqsirləndirilən şəxslər cinayətin edilməsində özlərini o qədər də təqsirkar

bilmədiklərinə görə çox vaxt yalan ifadə verməyə cəhd göstərmirlər.

Dindirmənin əvvəlində müstəntiq təqsirləndirilən şəxsin ona elan edilmiş ittiham üzrə özünün təqsirli bilib-bilmədiyini aydınlaşdırmalıdır. Sonra isə təqsirləndirilən əhəmiyyətli olan digər hallar üzrə ifadə vermək təklif etməlidir (CPM 233). Təqsirləndirilən şəxsin dindirilməsinin taktikası onun elan olunmuş ittihamla özünü təqsirli bilib-bilmədiyindən aslı olaraq müəyyən edilir.

Əgər təqsirləndirilən şəxs elan olunmuş ittihamla özünü tam təqsirli bilirsə, müstəntiq onu iş üçün əhəmiyyət kəsb edən bütün hallar barədə dindirməli və bu etirafın düzgünlüyünü yoxlamalıdır. İstintaq təcrübəsi göstərir ki, bir çox hallarda təqsirləndirilən şəxs ona yaxın şəxsləri cinayət məsuliyyətindən yayındırmaq məqsədilə; onu nüfuzdan salan məlumatın aşkar olunması qorxusu altında; maraqlı şəxslərdən mükafat almaq arzusu ilə; daha ağır cinayətdə ifşa olunmamaqdan ötrü və s. səbəblərdən cinayətin onun tərəfindən edilməsini yalandan etiraf edir.

Təqsirini etiraf etmiş təqsirləndirilən şəxsin dindirilməsi əsas taktiki üsullarından biri onun ifadələrinin dəqiqləşdirilməsidir. Bu üsul təqsirləndirilən şəxsin cinayət hadisəsilə əlaqədar hərəkətlərinin ardıcıllığını müəyyən etməyə imkan verir. Dindirmənin belə taktiki üsulla aparılması iş üçün əhəmiyyət kəsb edə bilən bütün faktların

aydınlaşdırmasına, habelə yalan ifadə vermə hallarının ifşa edilməsinə imkan verir.

Təqsirini boynuna almış təqsirləndirilən şəxsin dindirilməsinin digər taktiki üsulu onu ifadə verdiyi hallar barədə təkrar dindirilməsidir. Əgər təqsirləndirilən şəxs təkrar dindirmə zamanı əvvəlki ifadələri ilə ziddiyyət təşkil edən məlumat verirsə, bu onun yalan etiraf etdiyini dəlalət edir.

Kibercinayələr üzrə təqsirləndirilən şəxs elan olunmuş ittihamla özünü təqsirli bilmirsə, müstəntiq ona ittihamın mahiyyəti üzrə, habelə təqsirləndirilən şəxsin mülahizələrinə görə iş üçün əhəmiyyət kəsb edən hallar barədə ifadə verməyi təklif etməlidir. Təqsirləndirilən şəxsin öz təqsirini inkar etməsi doğru və yalan ola bilər.[6] Bir qayda olaraq təqsirini inkar edən təqsirləndirilən şəxslər öz mövqeyini tutarlı, inandırıcı olmayan dəlillər gətirməklə əsaslandırmağa çalışırlar. Bəzi hallarda isə təqsirləndirilən şəxs öz izahatlarında ittihamın əsaslandığı sübutların mövcud olduğunu inkar etməyərək, bunları başqa cür izah edir və ya istintaqa məlum olmayan yeni dəlillər gətirir. Lakin, kibercinayələrin araşdırılmasında təqsirləndirilən şəxsin verdiyi ifadənin xarakterindən aslı olmayaraq, hər bir halda, istər təqsirləndirilən şəxs təqsirini inkar edər əsaslı dəlillər gətirdikdə, istərsə də o, heç bir dəlil gətirmədən təqsirini əsassız inkar etdikdə müstəntiq həmin ifadələri işdə olan sübutlarla tam və mükəmməl yoxlamalıdır.

[6] Mövsümov C. Azərbaycan SSR Cinayət prosesi. Bakı, 1980, s. 204.

Əgər yoxlama nəticəsində təqsirləndirilən şəxsin yalan ifadə verdiyi məlum olarsa, bu zaman müstəntiq işdə olan sübutların ona elan olunması taktiki üsulundan istifadə etməlidir. Bu taktiki üsul təqsirləndirilən şəxsin yalan ifadə vermə hallarının ifşa etmək və onu düzgün məlumat verməyə məcbur etmək məqsədi daşıyır. Sübutlar təqsirləndirilən şəxsə elan etməzdən əvvəl onların həqiqiliyi yoxlanılmalı və təqsirləndirilən şəxsin bu sübutlara necə münasibət göstərəcəyi, öz ifadəsilə ilə həmin sübutlar arasındakı ziddiyyəti nə ilə izah edə biləcəyi nəzərə alınmalıdır. Əks təqdirdə bu sübutlarla təqsirləndirilən şəxsin ifadəsinin yalan olduğunu üzə çıxarmaq mümkün deyildir.

Kibercinayələr üzrə təqdim olunan sübutlar təqsirləndirilən şəxsdə müstəntiq işin hallarından tam xəbərdar olması barədə fikir yaratmalıdır. Ona görə də elə sübutlar elan edilməlidir ki, onlar təqsirləndirilən şəxs üçün tam gözlənilməz olsun. Əgər təqsirləndirilən şəxs cinayət hadisəsilə bağlı incəliklərin belə müstəntiqə məlum olduğunu gördükdə, yalan danışmağın mənasızlığını dərk edərək doğru ifadə vermiş olur. Təqsirləndirilən şəxsə şahid ifadələri elan olunmazdan əvvəl onun şahidə münasibətini aydınlaşdırmaq zəruridir. Əgər təqsirləndirilən şəxs şahidlə yaxın münasibətdə olduğunu təsdiq etsə, onda şahidin ittihamedici ifadəsini aralarındakı pis münasibətlə izah etmək imkanından məhrum olur.

Kibercinayələrin araşdırılmasında sübutlar təqsirləndirilən şəxsə aşağıdakı üsullarla təqdim edilir: 1) ifşaedici təsirin artan istiqaməti üzrə 2) dindirmənin ilk mərhələsində ən kəsərli sübutun təqdim edilməsi 3) birdəfəyə bütün sübutların təqdim edilməsi. Hər bir halda sübutların elan etmə üsulu işin konkret halından və təqsirləndirilən şəxsin xüsusiyyətlərindən aslı olaraq müəyyən edilməlidir. Təqsirləndirilən şəxsin ifşa etmək üçün sübutları epizodlarla elan olunması daha məqsəduyğundur. Ona görə ki, sübut təqsirləndirilən şəxsə tam məlum olduqda o, ifadəsinin sonrakı istiqamətini özü üçün əlverişli şəkildə tənzim edə bilər. Bu da çox zaman yalan ifadənin ifşa edilməsini çətinləşdirir.

Əgər kibercinayəti bir neçə təqsirləndirilən şəxs törətmişsə və onlardan heç biri təqsirini boynuna alaraq düzgün ifadə vermirsə, müstəntiq aşağıdakı taktiki üsuldan istifadə edə bilər. Müstəntiq təqsirləndirilən şəxslərin birindən iş üzrə az əhəmiyyət kəsb edən fakt barədə düzgün ifadə almağa çalışmalıdır. Sonra isə ondan digər təqsirləndirilən şəxslərlə üzləşdirmə zamanı bu fakt barədə ifadə verməк təklif olunur. Üzləşdirmə zamanı digər təqsirləndirilən şəxslərdə elə fikir yaranır ki, həmin şəxs cinayəti törədilməsini etiraf edərək, müstəntiqə cinayət hadisəsilə bağlı digər hallar barədə də məlumat verib. Məhz bu səbəbdən, onlar yalan ifadə verməyin mənasızlığını görüb, təqsirlərini boynuna alırlar. Lakin bu taktiki üsul təqsirləndirilən şəxslərə onlardan

birinin cinayəti etiraf etməsi barədə yalandan məlumat vermək kimi qiymətləndirilməməlidir. Çünki belə üsulla əldə edilmiş ifadə sübut əhəmiyyət kəsb edə bilməz (C PM 125.2.2).

Kibercinayələr üzrə şübhəli və təqsirləndirilən şəxsin dindirilməsi zamanı taktiki kombinasiyalardan da istifadə oluna bilər. Taktiki kombinasiyalar dedikdə, dindirilən şəxs tərəfindən mövcud istintaq şəraitini düzgün qiymətləndirilməməsi nəticəsində öz iradəsi əleyhinə doğru ifadə verməsinə yönəlmiş üsullar başa düşülür. İstintaq təcrübəsində aşağıdakı taktiki kombinasiyalar tətbiq olunur: 1) dindirilən şəxsdə müstəntiq "hər şeydən xəbərdar olması" təsəvvürünü yaratmaqla 2) dindirilən şəxsdən işin bu və ya digər halları haqqında müstəntiqin xəbəri olmasını gizlətmək 3) dolayı dindirmə- ikinci dərəcəli suallarla cinayət işi ilə əlaqədar əsas sualın maskalanması 4) cinayətlə əlaqədar müxtəlif halları təsdiqləyən ifadələrin alınması üçün şəraitin yaradılması.

Dindirmədə müstəntiq əsasən aşağıdakı sualları aydınlaşdırmalıdır:

- Potensial şübhəli kimlərdir?
- Hansı cinayət törədilib?
- Zərərçəkənlər kimlərdir ?
- Cinayət nə vaxt törədilib?
- Cinayət nə vaxt aşkar edilmişdir?
- Bu cinayətlərin hansı məkanı əhatə edir?

– Hansı dəlillər var və ya onları toplamaq mümkündürmü?
– Fiziki və rəqəmsal dəlillər harada yerləşə bilər?
– Cinayətlə bağlı hansı fiziki və rəqəmsal sübut növləri var? Cinayət nəticəsində vurulmuş ziyanın xarakteri və miqdarı?

***d).* Kiber cinayətlərin istintaqında axtarış və götürmə**

Kibercinayətlərin araşdırılmasında məlumatların əldə olunmasına yönəlmiş istintaq hərəkətləri zamanı axtarış və götürmənin keçirilməsinin özünəməxsus xüsusiyyətləri var. Sözügedən cinayətlərin istintaqı zamanı aparılan axtarış (götürmə) kompyuter avadanlığı və telekommunikasiya şəbəkələrinin istifadəsi zamanı cinayətin törədilməsi üsulu sübutların əldə edilməsi ilə əlaqədardır. Kibercinayətlərin araşdırılmasında axtarışın əsas məqsədi kibercinayətkarlığın izləri qalmış kompyuter texnikasının, həm də bu cinayəti törədənlər ilə əlaqəli kompyuter məlumatları, cinayətin izlərini daşıyan əşyalar və iş üçün vacib məlumatları ehtiva edən sənədlərin aşkar edilməsi və götürülməsidir.

Kibercinayətlərin araşdırılmasında axtarışın səmərəliliyi əsasən cinayətin hazırlanması və törədilməsi ilə əlaqədardır. Beləliklə, müstəntiq

axtarışın hazırlıq mərhələsində aşağıdakıları həyata keçirir:

1.Məlumatların mənbəyini təhlil etmək, cinayətkarın istifadə etdiyi kompyuter məlumatlarının növünü, məzmununu müəyyənləşdirmək; axtarılan məlumatın hansı qovluqda saxlanıla biləcəyini öyrənmək; törədilmiş cinayətlə əlaqədar hansı kompyuter avadanlığı axtarış yerində ola bilər.

2.Axtarış yeri (tutulma) barədə aşağıda qeyd olunan məlumatlar toplanılır: həmin yerin dəqiq ünvanı; struktur xüsusiyyətləri; telefon bağlantısı, işləyən modem varmı? yerli və ya qlobal şəbəkənin olub-olmaması; Wi-Fi şəbəkəsi işləmir; kompyuter avadanlıqlarının bir-birinə yerli şəbəkə ilə bağlı olub-olmaması; enerji təchizatı sistemi harada yerləşir; telekommunikasiya kabellərinin yerləşdiyi yer və s.

Bu məlumat cinayət işi materiallarından, eləcə də digər mənbələrdən, məsələn, telekommunikasiya xidmətlərindən (telefon şəbəkəsi, internet, simsiz Wi-Fi şəbəkəsi, lokal şəbəkə və s.) xəttə qoşulma barədə məlumat əldə etmək üçün şəbəkə operatorunuzla əlaqə saxlaya bilərsiniz.

3.Eyni otaqda axtarışda olan şəxsin və onunla birlikdə yaşayan və ya işləyən şəxslərin şəxsiyyətini öyrənmək. Eyni zamanda kompyuter avadanlığı və telekommunikasiya şəbəkələri ilə işləmə bacarıqları,

peşə bilikləri, iş yeri və vəzifəsi haqqında məlumat əldə etmək vacibdir.

4.Əvvəlcədən axtarışa kömək edəcək mütəxəssislərlə razılaşdırılmış logistika hazırlamaq.

5.Axtarışda iştirak edəcək şəxslərin dairəsini müəyyənləşdirmək. Kibercinayətlərin istintaqı zamanı axtarışın məcburi iştirakçıları müstəntiq, mütəxəssis və şahidlərdir. Müstəntiq axtarışın məqsədindən irəli gələrək, mütəxəssisi seçməlidir. Şahidlər kompyuter avadanlığı və telekommunikasiya şəbəkələri ilə işləmək bacarıqları nəzərə alınmaqla seçilməlidir. Belə vəziyyətdə riyaziyyat və kibernetika sahələri üzrə ixtisaslaşmış universitetlərin tələbələri də iştirak edə bilər.

Bütün hazırlıq tədbirlərini bitirdikdən sonra müstəntiq dərhal axtarışa (götürməyə) başlamalıdır.

Axtarış və götürmə aparılacaq yerə gəldikdə, binaya daxil olduqda müstəntiq axtarışa məruz qalmış ev sahibini məhkəmə qərarı ilə tanış etməli və axtarılan əşyaları könüllü verməyi təklif etməlidir. Şəxs axtarılan əşya və ya məlumat mənbələrini könüllü təhvil vermədiyi təqdirdə, müstəntiq axtarışda olan şəxslərin hamısını bir yerə toplamalı və dərhal kompyuter texnikasına girişi qadağan etməlidir.

Axtarış və götürmə aparılması zamanı tədbirlər iki mərhələyə bölünür: tam və qismən. Tam və

müfəssəl mərhələlərdə müstəntiq həm axtarış (götürmə) üçün ümumi taktiki müddəalara əməl etməli, həm də kibercinayətlərə xas olan müəyyən xüsusiyyətləri nəzərə almalıdır.

Kibercinayətlərin araşdırılması zamanı axtarış (götürmə) zamanı bir sıra xüsusiyyətlər nəzərə alınmalıdır:

Axtarışın işçi mərhələsində aşağıdakılara diqqət yetirilməlidir:

1.Otağın bütün sahələrini axtarmaq. İstədiyiniz obyektin kompyuter məlumatı şəklində olması səbəbi ilə ilk növbədə otaqda olan kompyuter avadanlığına, yerləşməsinə, vəziyyətinə, həmçinin telekommunikasiya şəbəkələrinin vəziyyətinə diqqət yetirmək lazımdır. Binada axtarış aparılarkən, məxfi olanlar da daxil olmaqla, portativ saxlama qurğularında da axtarış aparılmalıdır.

2.Kompyuterin yerli və telekommunikasiya şəbəkələrinə qoşulmasını müəyyən etmək lazımdır. Axtarılan otaqlarda bir neçə kompyuter varsa, mütəxəssisin köməyi ilə informasiya bazasını müəyyən edib, axtarışa başlamaq.

3. Kompyuterdə məlumatları mühafizə vasitələrinin, virus proqramlarının və məsafədən daxil olmanın mövcudluğunu yoxlamaq lazımdır. Əgər onlar mövcuddursa, ilk növbədə icazəsiz daxil olma

zamanı bütün məlumatları avtomatik olaraq məhv edən və məlumatların mühafizəsi üçün xüsusi vasitələrdən imtina etməlisiniz.

4.Kompyuterlərdən birini araşdırarkən aşağıdakılar müəyyənləşdirilir: hansı əməliyyat sistemi quraşdırılıb; kompyuter işə düşmədən öncə hansı əməliyyatlar yerinə yetirilib və hansı proqramlar istifadə olunub. Kompyuterin ekranındakı görüntü videoya çəkilməlidir (və ya ekranın görüntüsünü istifadə etməklə), lazım gəldikdə proqramları dayandırmaq lazımdır.

5.İşlək vəziyyətdə olan kompyuteri araşdırarkən: bir mütəxəssisin köməyi ilə kompyuter məlumatlarının məhv edilməsi təhlükəsi yoxdursa, araşdırılan kompyuterdə cinayətlə əlaqəli kompyuter məlumatlarını axtarılmalıdır. Axtarış, axtarılan obyekt barədə məlum məlumatlar əsasında aparılır.

Kompyuterə baxışdan sonra bütün qaydalara uyğun olaraq bağlanır, qablaşdırılır və götürülür.

İşlək vəziyyətdə olmayan kompyuteri araşdırarkən: yerini, eləcə də periferik cihazlarını düzəldin; telekommunikasiya şəbəkələri, periferik avadanlıqlar və digər qurğularla kompyuter əlaqələrini müəyyənləşdirmək və qeyd etmək; cihazı kompyuterdən ayırmaq onu qablaşdırma üçün hazırlamaq.

6. İstintaqı aparılan cinayətlə əlaqədar zəruri məlumatları axtarmaq üçün cib telefonu, smartfon və ya planşet kompyuteri mütəxəssisin iştirakı ilə götürmək.

Mobil cihazda məlumatları əvvəlcədən araşdırmaq mümkün olmadıqda, cihaz tədqiqat üçün götürülməlidir.

Axtarışdan (götürmədən) sonra istintaqı aparılan kibercinayətlər üçün axtarılan məlumatları ehtiva edən bütün aşkar edilmiş kompyuter avadanlıqları əvvəl düzgün qablaşdırılmalı və möhürlənməlidir. Axtarışın (götürmənin) sonunda istintaq hərəkətinin protokolu və ona əlavə edilən siyahı tərtib edilir.

e) İstintaq eksperimentinin xüsusiyyətləri

Cinayət Prosessual Məcəlləsinin 181-ci maddəsi cinayət işi ilə əlaqəli məlumatların dəqiqləşdirilməsi və onların etibarlılığının müəyyən edilməsi, habelə yeni sübutların alınması üçün müəyyən hadisənin vəziyyəti və ya digər hallarını təkrarlamaqla müstəntiq istintaq eksperimentini aparmaq hüququna malikdir. Eyni zamanda, hər hansı bir faktı dərk etmək, müəyyən hərəkətlər etmək, bir hadisənin baş vermə ehtimalı yoxlanılır, hadisənin ardıcıllığı və izlərin yaranma mexanizmi aşkar edilir.

Şübhəli (təqsirləndirilən) şəxsin informasiya sistemləri və kompyuter avadanlığı sahəsində

biliklərinə dair şübhələri aradan qaldırmaq üçün istintaq eksperimenti keçirilə bilər.

Kiber cinayətlərin istintaqı zamanı aparılan istintaq eksperimentinin növləri cinayətin törədilmə üsullarından asılıdır.

İstintaq eksperimenti aşağıdakı təcrübələr keçirilməklə aparıla bilər:

– cinayətkarın kompyuter texnologiyasından istifadə edərək onların birləşdirilməsi və hərəkətlərin həyata keçirilməsinin mümkünlüyünü yoxlamaq;

– parolların, eyniləşdirilməsi, kodlarının seçilməsini və bu seçim üçün bir müddət təyin olunmasını yoxlamaq;

– kompyuter şəbəkəsinə qoşulma və cinayət texnologiyalarından istifadənin mümkünlüyünü yoxlamaq;

– elektromaqnit dalğalarını tutma ehtimalını yoxlamaq;

– məlumatların qorunması, texniki vasitələrin işləməməsi üçün tələb olunan müddətləri və məlumatların dəyişdirilməsi;

– müəyyən vaxt təyin etməklə sənədlərin surətinin çıxarmaq imkanını yoxlamaq üçün;

– kiber məkanda müəyyən hərəkətlərin edilməsinin mümkünlüyünü yoxlamaq.

İstintaq eksperimentinin aparılmasından əvvəl aşağıdakı hazırlıq tədbirlərini aparmaq lazımdır:

1.Kibercinayətkarlıq və onların istirahəti zamanı texniki şərtlərin aydınlaşdırılması.

Cinayətkarlığın araşdırılmasında istintaq eksperimenti zamanı cinayətin törədildiyi anla oxşarlığın əsas şərti cinayətkarın istifadə edə biləcəyi orijinal və ya oxşar texniki vasitədən istifadə edilməsidir.

İstintaq eksperimentinin aparılması zamanı binaların ətraf mühitini bərpa etməyə ehtiyac yoxdur, çünki vəziyyət kiber sahəyə həqiqətən təsir göstərmir. Bununla birlikdə, cinayətkarın kompyuter avadanlıqlarının quraşdırıldığı otağa daxil olması ilə əlaqədar kompyuter məlumatlarına daxil olma ehtimalını yoxlamaq üçün istintaq eksperimenti aparmaq lazımdırsa, yenidənqurma lazımdır.

2. Cinayətin baş verdiyi informasiya texnologiyaları sahəsindəki bir mütəxəssislə hərəkətlərin məzmununu əlaqələndirmək. Mütəxəssis müsbət nəticələrə nail olmaq üçün istintaq eksperimenti zamanı hansı hərəkətlərin görülməli olduğunu düzgün izah edə biləcək.

3. Təcrübələrin keçirilməsi üçün lazım olan bütün elmi və texniki vasitələri, kompyuter avadanlıqlarını və digər texniki vasitələri əvvəlcədən hazırlamaq lazımdır. İstintaq eksperimentinin keçirilməsi üçün zəruri texniki vasitələr işin materiallarına və dindirilən şəxslərin verdiyi ifadələrə uyğun seçilir.

4. İstintaq eksperimentində iştirak edəcək şahidlərin dairəsini müəyyən etmək üçün onların kompyuter informasiyası sahəsində bilikləri olması yoxlanılmalıdır.

Müstəntiqin istəyi ilə təqsirləndirilən şəxs, zərərçəkmiş və şahid istintaq hərəkətində iştirak edə bilər, bu işdə bir mütəxəssisin iştirakı hərəkətin məzmununu aydınlaşdırmağa kömək edir. Bu şəxslərdən biri müstəntiqi yanıltmaq istəsə, mütəxəssis bu barədə xəbərdarlıq edə bilər.

Bu istintaq hərəkətinə hazırlıq prosesində işin xüsusiyyətlərini nəzərə almaq lazımdır. Bu baxımdan müstəntiq üçün aşağıdakı işlərin yerinə yetirməsi məcburidir:

– kompyuter avadanlığı və texnologiyaları sahəsindəki mütəxəssislərin istintaq araşdırılmasında iştirakının təmin edilməsi;

– yüksək texnologiyalar sahəsində cinayətlərə qarşı mübarizədə iştirak edən orqanların əməkdaşlarının iştirakını təmin etmək;

– kompyuter avadanlığı və texnologiyaları sahəsindəki bilikləri olan hal şahidlərin iştirakını təmin etmək;

– zəruri texniki (kompyuter) vasitələrinin hazırlanması.

Kiber cinayətlərin araşdırılması zamanı kompyuter avadanlığı və texnologiyaları sahəsində mütəxəssislərin iştirakının təmin edilməsi aksioma hesab edilməlidir Zəruri hallarda rabitə və ya şəbəkə xidmətlərinə mütəxəssis mühəndisləri cəlb etmək mümkündür. Yoxlama obyekti bir neçə kompyuterdirsə (yerli kompyuter şəbəkəsi), bu sahəyə bir neçə mütəxəssis cəlb etmək məsləhətdir.

Bir çox xarici ölkələrdə kiber cinayətlərin araşdırılmasında mütəxəssislərin köməyindən fəal istifadə olunur. Beləki ABŞ Senatının məhkəmə komitəsində etdiyi məruzədə kiber cinayətlərlə bağlı araşdırma bürosunun direktoru Louis Frich istintaq qruplarına kompyuter texnologiyaları sahəsindəki mütəxəssislərin məcburi şəkildə daxil edilməsini, lazımi texniki vasitələrin hamısını təmin etdiyini qeyd etmişdir.

Qeyd etmək lazımdır ki, mütəxəssislərin kiber cinayətlərin araşdırılmasında iştirakına ehtiyac Rusiyada aparılan tədqiqatların nəticələri ilə də təsdiqlənir. Belə ki A.V. Kasatkin, onun araşdırmalarının apardığı sorğunun nəticələrinə əsaslanaraq, respondentlərin 56 faizinin kompyuterin iş prinsipləri barədə heç nə bilmədiklərini qeyd etmişdir. Bununla yanaşı, müəllif tərəfindən sorğuda iştirak edən proqramçıların sayının 92% qeyd etmişdir ki, kompyuter texnologiyalarının hazırkı inkişaf səviyyəsində, peşəkarların iştirakı olmadan, kompyuterdə "gizli" məlumatları məhv etmək riski olmadan tapmaq çətindir. Müstəntiqlərin sorğusu zamanı "Bir mütəxəssisin iştirakı olmadan kompyuter avadanlıqlarını və ya kompyuter yaddaşında saxlanan məlumatları düzgün bir şəkildə çıxara bilərsinizmi?" Respondentlərin yalnız 17,3% -i müsbət cavab vermişdir

*l)*Məhkəmə kompyuter-texniki ekspertiza

Müasir dövrdə kompyuter və hesablama texnologiyalarının sürətli inkişafı, elmin, texnikanın, informasiya vasitələrinin elektron sistemlərdə tətbiqi bir çox işlərin araşdırılmasında kriminalistlərin qarşısına yeni sahələrin öyrənilməsi vəzifəsini qoyur. Hüquq-mühafizə orqanlarının qarşısında duran aktual problemlərdən birini də kompyuter texnologiyalarından, mobil rabitə vasitələrindən, bankomatlardan və s.-dən istifadə etməklə törədilən cinayətlərin qarşısını almaq, törədilmiş cinayətlərin tezliklə açılması və səmərəli istintaqının aparılması məqsədilə sübutların aşkar edilməsi, qeyd edilməsi və götürülməsi metodları, həmçinin xüsusi biliklərin tətbiqi təşkil edir. Kompyuter texnologiyalarından istifadə edilməklə törədilən cinayətlər bu sahədə xüsusi biliklərə malik olan ekspertlərin köməyi olmadan tam və obyektiv şəkildə araşdırıla bilməz. Bu onunla şərtlənir ki, yalnız kompyuter texnologiyaları sahəsində xüsusi biliklərə malik olan ekspertlər tərəfindən aparılan tədqiqatlar aparat vasitələrinin, proqram təminatının və kompyuter məlumatlarının tədqiqində mühüm sübut əhəmiyyəti olan nəticələrin əldə edilməsini təmin edir. Kompyuter texnologiyalarından istifadə edilməklə törədilən cinayətlər üzrə xüsusi biliklərin tətbiqinin əsas prosessual forması məhkəmə kompyuter-texniki ekspertizasıdır.

Məhkəmə kompyuter-texniki ekspertizası (MKTE)

məhkəmə ekspertizasının müstəqil növü kimi mühəndis-texniki ekspertizalar sinfinə daxildir və kompyuterin konstruktiv xüsusiyyətlərinin və vəziyyətinin, kompyuterə qoşulan periferik qurğuların, maqnit daşıyıcıların, kompyuterdə və maqnit daşıyıcılarda saxlanılan informasiyanın öyrənilməsi məqsədilə keçirilir. Onun hüquqi əsasını, təşkili prinsiplərini və əsas istiqamətlərini Azərbaycan Respublikası Cinayət Prosessual Məcəlləsı, Azərbaycan Respublikası Mülki Prosessual Məcəlləsı, "Dövlət məhkəmə ekspertizası fəaliyyəti haqqında", "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunları və digər normativ-hüquqi aktlar müəyyənləşdirir.

Azərbaycan Respublikasında kompyuter texnikasının və proqram təminatı vasitələrinin ekspert tədqiqatı 2003-cü ildən aparılmağa başlanmışdır. Məhkəmə texniki ekspertizaların yeni sahəsi olan kompyuter-texniki ekspertizalar Azərbaycan Respublikası Ədliyyə Nazirliyinin Məhkəmə Ekspertizası Mərkəzində keçirilir. "Məhkəmə ekspertizası mərkəzində məhkəmə eksperti ixtisasının verilməsi haqqında Əsasnamə"yə 1 nömrəli əlavədə - "Məhkəmə ekspertizası mərkəzində məhkəmə eksperti ixtisası verilən məhkəmə ekspertizası növlərinin və ekspert ixtisaslarının Siyahısı"nda məhkəmə kompyuter-texniki ekspertizası növü üzrə kompyuter-texniki obyektlərin tədqiqi ixtisası müəyyən

olunmuşdur.

MKTE-nin elmi əsasmı kompyuter sisteminin və kompyuter məlumatlarının hərəkətinin təşkili və öyrənilməsi qanunauyğunluqları təşkil edir.

Məhkəmə kompyuter-texniki ekspertizasının növləri

- ***Məhkəmə aparat-kompyuter ekspertizası*** - kompyuter sisteminin texniki (aparat) vasitələrinin
- tədqiq edilməsi məqsədilə təyin olunur;
- ***Məhkəmə proqram-kompyuter ekspertizası -*** kompyuter sisteminin proqram təminatının funksional təyinatının, xarakterinin və tələblərinin, alqoritm və quruluş xüsusiyyətlərinin öyrənilməsi məqsədilə təyin olunur;
- ***Məhkəmə məlumat-kompyuter ekspertizası —*** kompyuter sistemində istifadəçi tərəfindən hazırlanmış və yaxud yaradılmış proqramlarla məlumatların axtarışı, aşkar edilməsi, təhlili və qiymətləndirilməsi məqsədilə aparılır;
- ***Məhkəmə kompyuter-şəbəkə ekspertizası*** - şəbəkə texnologiyalarının həyata keçirilməsi zamanı kompyuter vasitələrinin funksional təyinatına əsaslanır.

İKT-nin və ETT-nin sürətlə inkişafı kompyuter-texniki ekspertizanın da yeni növlərinin formalaşmasını şərtləndirir ki, bunlardan məhkəmə tele- matik ekspertizanı misal göstərmək olar. Bu ekspertizanın predmetinə iş üçün əhəmiyyəti olan faktlar və hadisələr haqqında maddi məlumat daşı-

yıcıları kimi çıxış edən səyyar rabitə vasitələrinin tədqiqatı zamanı xüsusi elmi biliklərin köməyi ilə aşkar olunan faktiki məlumatlar daxildir.

Məhkəmə-kompyuter texniki ekspertizasının yuxarıda qeyd olunan növləri həll etdiyi məsələlərin dairəsinə görə fərqlənir. Belə ki, məhkəmə aparat-kompyuter ekspertizası aparılarkən əsasən aşağıdakı məsələlər həll edilir:

– ayrı-ayrı funksional tapşırıqların həll edilməsi üçün aparat vasitələrinin növlərinin (tip və markasının), əlamətlərinin, habelə onların texniki və funksional xüsusiyyətlərinin müəyyən edilməsi (məsələn, qrafik təsvirlərin yüksək səviyyədə işlənib hazırlanması);

– aparat vasitələrinin faktiki vəziyyətinin və yararlılığının müəyyənləşdirilməsi;

– həm ayrılıqda, həm də kompyuter sisteminin tərkibində kompleks şəkildə aparat vasitələrindən istifadə edərək hadisələrin quruluş mexanizminin və vəziyyətinin öyrənilməsi;

– aparat vasitələrinin konkret imkanları ilə onlardan istifadənin nəticələri arasındakı səbəbli əlaqənin aydınlaşdırılması;

– aparat vasitələrindən istifadənin xronoloji ardıcıllığını bərpa etməklə onların tətbiqi şərtlərinin, vəziyyətinin müəyyən edilməsi.

Məhkəmə proqram-kompyuter ekspertizasının vəzifələri:

• əməliyyat sisteminin əsas xarakterik

xüsusiyyətlərinin müəyyən edilməsi;

- proqram təminatının istiqamətlərinin funksional əlamətlərinin müəyyənləşdirilərək öyrənilməsi;
- proqram obyektinin faktiki vəziyyətinin, onun fayllarmın, parametrlərinin, məlumatın daxil və xaric olmasının müəyyənləşdirilməsi;
- proqram təminatının ümumi sistemlə əlaqə əlamətlərinin aydınlaşdırılması;
- proqram təminatının vəziyyətində baş vermiş dəyişikliklərin məqsəd və şərtlərinin müəyyənləşdirilməsi, proqramda dəyişikliklərin aradan qaldırılması üsullarının aşkar edilməsi;
- proqramın yüklənmiş informasiyanı saxlama qabiliyyətinin aydınlaşdırılması;
- proqram təminatına və əlavə edilmiş nəticəyə münasibətdə kompyuter sistemi istifadəçisinin hərəkətləri arasındakı səbəbli əlaqənin müəyyən edilməsi.

Məhkəmə məlumat-kompyuter ekspertizasının həll etdiyi məsələlər:

- tədqiq olunan kompyuter sisteminə daxil edilməli məlumatın növünün və əlamətlərinin öyrənilməsi;
- informasiya,daşıyıcılarındakı məlumatların ilkin vəziyyətinin öyrənilməsi;
- tədqiq olunan məlumatın xüsusiyyətlərinin dəyişməsi səbəblərinin müəyyənləşdirilməsi;
- hadisənin mexanizminin və ayrı-ayrı hallarının,

habelə məlumat daşıyıcılarında olan məlumatlara əsasən hadisənin ayrı-ayrı mərhələlərinin müəyyən edilməsi;

▪ məlumatın vaxtının, ona təsir edən halların xronoloji ardıcıllığının aydınlaşdırılması;

▪ hadisənin zənn edilən iştirakçılarının işlərinin məlumatı təşkil edən peşəkarlıq və istifadə bacarığından asılı olmaqla düşüncə, adətlər, səbəbin aşkar edilməsi kimi əlamətlərinin öyrənilməsi;

▪ başa çatmış hərəkətlərin zənn edilən nəticələrinin və onun hazırlanma imkanlarının aydınlaşdırılması.

Məhkəmə kompyuter-şəbəkə ekspertizasının vəzifələri:

– aparat vasitələrinin və proqram təminatının əlamət və xüsusiyyətlərinin müəyyən edilməsi;

– hesablayıcı şəbəkənin əlamət və xüsusiyyətlərinin, onun arxitekturasının, konfiqurasiyasının təyin edilməsi, şəbəkə hissələrinin, məlumatlara buraxılışın təşkilinin aydınlaşdırılması;

– şəbəkə texnologiyasının konkret qrupuna aid olan vasitələrin əlamətlərinin müəyyənləşdirilməsi;

– şəbəkə vasitələrinin faktiki vəziyyətinin və yararlılığının, fiziki de- fektlərin, sistem jurnalının və s.-nin müəyyən edilməsi;

– bütövlükdə hesablayıcı şəbəkənin və şəbəkə vasitələrinin ayrılıqda hər birinin ilkin vəziyyətinin öyrənilməsi;

– hesablayıcı şəbəkənin xüsusiyyətlərinin dəyişməsi səbəbinin aydınlaşdırılması;

– hadisənin şəbəkədəki nəticələrinə əsasən onun quruluş xüsusiyyətlərinin və əlamətlərinin müəyyənləşdirilməsi;

– hesablayıcı şəbəkənin konkret aparat-proqram vasitələrinin istifadəsi və onların tətbiqi arasındakı səbəbli əlaqənin təyin edilməsi.

Yuxarıda qeyd olunan vəzifələr məhkəmə kompyuter-texniki ekspertizasının qarşısında qoyulan sualların dairəsinin müəyyənləş-dirilməsinə imkan verir. Belə ki, məhkəmə kompyuter-texniki ekspertizasının qarşısında aşağıdakı təsnifləşdirici, eyniləşdirici və diaqnostik xarakterli suallar qoyula bilər:

•Təqdim edilən texniki kompleks vasitəsilə bu və ya digər funksional məsələlərin (İnternetə çıxış, başqa vasitələr kompleksinin idarə edilməsi üçün xüsusi mexanizmin yaradılması və s.) həyata keçirilməsi mümkündürmü?

•Təqdim edilən proqram təminatının əsas funksiyaları hansılardır və pozucu xarakter daşıyırım?

•Təqdim edilən proqram təminatı hansı hesablayıcı və proqram vasitələrinin köməyilə yaradılmışdır?

•Təqdim edilən maqnit daşıyıcılarda hər hansı bir fəaliyyətə aid olan sənədlərin faylları (pul nişanlarının təsviri, partlayıcı qurğuların sxemi, hüquqi şəxslərin blankları, möhür əksləri və s.) olan fayllar vardırım?

•Təqdim edilən məlumat bazasının təyinatını, onun istehlak xassələrini müəyyən etmək

mümkündürmü?

•Təqdim edilən obyektin yaddaşından silinmiş məlumatları bərpa etmək mümkündürmü? Əgər mümkündürsə, həmin məlumatlar hansı həcmdədir və məzmunu nədən ibarətdir? və s.

Məhkəmə kompyuter-texniki ekspertizanın obyektləri

Məhkəmə kompyuter-texniki ekspertizanın növlərini nəzərə alaraq onun obyektlərini aşağıdakı kimi təsnifləşdirmək olar:

Aparat obyektləri - fərdi kompyuterlər; periferik qurğular və hissələr; şəbəkə aparat vasitələri (serverlər, şəbəkə panelləri); mobil telefonlar və s.

Proqram obyektləri - kompyuterlərin sistemli proqram təminatı (əməliyyat sistemi). Əməliyyat sisteminin köməyilə istifadəçi-kompyuter dialoqu yaranır, əməli və daimi yaddaş qurğuları iş prosesinə qoşulur, kompyuter idarə edilir və istənilən proqram işə düşür. Beləliklə, əməliyyat sisteminin əsas funksiyası kompyuterin ehtiyatlarının (fiziki ehtiyatlar (mikroprosessor, monitor, disklər) və məntiqi ehtiyatlar (proqramlar, fayl- lar və s.)) və hesablama sistemləri proseslərinin idarə olunmasıdır. Əmə-liyyatlar sistemlərinə PC DOS, OS/2, MS DOS, UNIX, Windows-u misal göstərmək olar. Əməliyyat sistemləri yerinə yetirdikləri funksiyalarına görə üç qrupa bölünürlər:

1) Birməsələli (bir istifadəçidən ibarət) əməliyyat sistemləri;

2) Çoxməsələli (çox istifadəçidən ibarət) əməliyyat sistemləri;

3) Şəbəkə (lokal və qlobal kompyuter şəbəkələri üzrə) əməliyyatlar sistemləri.

İnformasiya obyektləri - kompyuter vasitələrindən istifadə etməklə mətn və qrafik sənədlərin hazırlanması (fayllar, mətn yığımı üçün formatlar (txt, doc), qrafik formatlar (bmp, jpg, bmp, cif, tiff, cdr), məlumat bazası formatları (dbf, mdb), elektron cədvəllər (xls, jal) və s.), multimedia formatmdakı məlumatlar, tətbiqi xarakter daşıyan məlumat bazası çərçivəsində informasiyalar .

Şəbəkə obyektləri **-** lokal və regional kompyuter şəbəkələri; simli və simsiz hesablama şəbəkələri; onların daxili struktur elementləri, qarşılıqlı əlaqələrinin interfeysləri və kanalları.

Məhkəmə kompyuter-texniki ekspertizasının obyektlərini həmçinin standart və qeyri-standart obyektlərə bölmək olar. Standart obyektlərə eyniləşdirilməsi heç bir çətinlik yaratmayan obyektləri aid etmək olar. Məsələn, kompyuterlər, noutbuklar, smartfonlar və s. Qeyri-standart obyektlərə kompyuter-texniki ekspertiza vasitəsilə eyniləşdirilməsi çətin olan zədələnmiş, sınmış, uyğunlaşdırılmış izləmə qurğuları, bankomatlara quraşdırılmış əldədüzəltmə kart oxuyucu- ları və yaddaşmda informasiya saxlayan digər qeyri-standart qurğular aiddir.

Kompyuter-texniki ekspertizanın obyektlərini daha müfəssəl şəkildə nəzərdən keçirək:

Bankomat **-** kompyuter-texniki ekspertizanın

qeyri-tipik obyektidir, çünki o, ənənəvi baxımdan klassik kompyuter deyil. Bankomat nağd pul vəsaitlərinin qəbul edilməsi və verilməsi, bank kartlarından istifadə etməklə əməliyyatlar üzrə sənədlərin tərtib edilməsi, bank hesabı üzrə məlumat verilməsi, nağdsız hesablaşmalar aparılması və s. üçün nəzərdə tutulmuşdur.

Bankomatlara çöx zaman əlavə qurğular quraşdırılır ki, bu da onların əhəmiyyətli dərəcədə bahalaşmasma səbəb olur: müşahidə üçün veb-kameralar, bank mütəxəssisləri ilə məsləhətləşmək üçün qurğu, kriptoprosessor, fasiləsiz elektrik cərəyam ilə təmin edilmək üçün qurğu və s. Bankomat istehsalçıları onun dəstinə xüsusi proqram təminatı - tətbiqi-sistemlər yaratmaq üçün baza proqram modullarının kitabxanasım da daxil edirlər.

Təyinatına görə bankomatlar aşağıdakı növlərə bölünürlər: ofis (bankların, mağazaların, metropolitenin və s. binalarının daxilində yerləşdirilir), küçə və yolkənarı (avtomobil yolları) bankomatlar.

Bankomatların əksər modelləri bank kartları vasitəsilə *online* rejimdə, eləcə də smartkartlar vasitəsilə isə *offline* rejimdə istifadə üçün nəzərdə tutulmuşdur.

Oyun avtomatları və maşınları - tez-tez xüsusi proqram vasitələrlə uduş alqoritmini dəyişməklə yüksək gəlir əldə etmək üçün istifadə olunur. Məsələn, avtomata müştərinin uduşunun orta statistik göstəricilərlə müqayisədə daha aşağı faizini ödəmək tapşırığı verilir. Nəzərə alsaq ki, bu maşınlar indi

elektron yolla proqramlaşdırılır, uduş faizini istənilən səviyyədə qoymaq olur. Oyun zallarının və kazinoların müdiriyyəti gün ərzində əldə olunan gəlirin miqdarından asılı olaraq onun bir hissəsini uduş faizi kimi ayırır.

Smartfonlar və mobil telefonlar - fərdi cib kompyuterlərinin funksiyaları əlavə edilmiş mobil telefonlardır. Hal-hazırda smartfonlar insan həyatının ayrılmaz atributuna çevrilmişdir.

Smartfonlar və mobil telefonlar məhkəmə kompyuter-texniki ekspertizasının ayrı-ayrı obyektləridir. Ona görə ki, "smartfonlar adi mobil telefonlardan kifayət qədər inkişaf etmiş, kənar proqramçılar tərəfindən proqram təminatının işlənməsi üçün açıq olan (adi mobil telefonların əməliyyat sistemi kənar proq- ramçılar üçün bağlıdır) əməlyyat sisteminin mövcudluğu ilə fərqlənir. Yardımçı əlavələrin quraşdırılması smartfonların funksional imkanlarını adi mobil telefonlarla müqayisədə əhəmiyyətli dərəcədə yaxşılaşdırmağa imkan verir.

Smartfonun tədqiqi üzrə təcrübədən götürülmüş ekspert rəyinin nümunəsini nəzərdən keçirək:

Ekspertiza qarşısında qoyulan suallar:

– Tədqiqata təqdim edilmiş İphone 6 markalı mobil telefon aparatının daxilində olan məlumatlar hansılardır?

– Tədqiqata təqdim edilmiş İphone 6 markalı mobil telefon aparatının yaddaşından silinmiş məlumatlan bərpa etmək mümkündürmü,

mümkündürsə həmin məlumatlar müəyyən edilsin.

Tədqiqat prosesinin təsviri:

Tədqiqata təqdim edilmiş mobil telefon çəhrayı və qara rəngli olub, arxa tərəfində "İphone 6S" yazısı vardır

1.Tədqiqata təqdim edilmiş bir ədəd arxa tərəfində "İphone 6S" yazısı olan mobil telefonun markasını, modelini, İMEİ kodunu, digər fərdi əlamətlərinin nədən ibarət olmasını və istifadəyə yararlı olub-olmamasını müəyyənləşdirmək üçün mobil telefonun texniki göstəriciləri, xarici görünüşünə baxış keçirilərək ekspert tərəfindən şərti olaraq müvafiq əməliyyatlar aparılaraq tədqiq olundu.

Aparılmış tədqiqata və texniki göstəricilərə əsasən belə nəticəyə gəlindi ki, tədqiqata təqdim edilmiş bir ədəd həssas (sensorlu) təzyiqlə çalışan "İPhone 6S" markalı "A1688" modelli "353317073788011" İMEİ kodlu mobil telefon olmaqla, xarici görünüşü çəhrayı və qara rəngli plastmas, metal kütlədən olması, arxa hissəsində "İphone S" sözünün yazılması müəyyənləşdirildi. Mobil telefonun yuxan hissəsi ekrandan, eşitmə mikrofonundan, kameradan, aşağı və yan tərəfi isə müvafiq düymələrdən və ötürmə mikrofonundan təşkil olunmuşdur. Mobil telefon əsas xüsusiyyətlərə, digər müvafiq köməkçi və əlavə xüsusiyyətlərə malik olmaqla, hal-hazırda işlək vəziyyətdə olub istifadə üçün yararlıdır.

2.Təqdim edilmiş "İPhone 6S" markalı "A1688" modelli mobil telefonun yaddaşında hər hansi bir

məlumatların və eləcə də həmin mobil telefonun yaddaşından pozulmuş məlumatlarının olub-olmaması müəyyən etmək üçün Ekspertiza Mərkəzində olan mobil telefonların və smartfon cihazların tədqiqatı üçün nəzərdə tutulmuş çox funksional "Cellebrite UFED" markah qurğuya qoşularaq tədqiq olundu.

Tədqiq olunan "İPhone 6S" markalı "A 1688" modelli mobil telefonda olan "File məlumat bazası" məlumatları çoxfiınksional "Cellebrite UFED" markah qurğu vasitəsilə xarici yaddaş qurğusuna köçürülərək "Analytics" proqramı vasitəsilə emal edildikdən sonra köçürülmüş fayllarm məzmununa xüsusi kompyuter proqramları vasitəsilə baxılaraq bir daha tədqiqat işləri aparıldı.

"Cellebrite UFED" markalı qurğunun vasitəsilə tədqiqata təqdim edilmiş "İPhone 6S" markalı "Al688" modelli mobil telefonun yaddaşında və həmin mobil telefonun yaddaşından pozulmuş 60.3 KB həcmdə məlumatlar müəyyən olundu ("Cellebrite UFED" markah qurğunun tərtib etdiyi hesabat (Report Tədqiq olunan "İPhone 6S" markalı "A 1688" modelli telefonun yaddaşında və həmin mobil telefonun yaddaşmdan pozulmuş və "Cellebrite UFED" markalı qurğunun tərtib etdiyi hesabat əsasında müəyyən olunmuş 60.3 KB həcmdə məlumatlar "Ekspertiza 2122" adlı iş çantasında üzərində "abv" yazısı olan DVD-R diskə köçürülərək ekspert rəyinə əlavə edildi.

Tədqiqatın nəticəsi:

– Təqdim edilmiş bir ədəd həssas (sensorlu)

təzyiqlə çalışan "İPhone 6S" markalı "A1688" modelli "353317073788011" İMEİ kodlu mobil telefon olmaqla, hal-hazırda işlək vəziyyətdə olub, istifadə üçün yararlıdır.

– "Cellebrite UFED" markalı qurğunun vasitəsilə tədqiqata təqdim edilmiş "İPhone 6S" markalı "Al688" modelli mobil telefonun yaddaşmda və həmin mobil telefonun yaddaşmdan pozulmuş 60.3 KB həcmdə məlumatlar müəyyən olundu ("Cellebrite UFED" markalı qurğ uçun tərtib etdiyi hesabat).

Tədqiq olunan "İPhone 6S" markalı "Al 688" modelli telefonun yaddaşmda və həmin mobil telefonun yaddaşmdan pozulmuş və "Cellebrite UFED" markah qurğunun tərtib etdiyi hesabat (Report-Отчет) əsasında müəyyən olunmuş 60.3 KB həcmdə məlumatlar "Ekspertiza 2122" adlı iş çantasında üzərində "abv" yazısı olan DVD-R diskə köçürülərək ekspert rəyinə əlavə edildi.

Bir çox müəlliflər məhkəmə kompyuter-texniki ekspertizasının yeni bir növünün - mobil rabitə vasitələrinin və smartfonlarm ekspertizasının müstəqil növ kimi ayrılmasını təklif edirlər. Onların fikrincə, bu, kompyuter-texniki tədqiqatların səmərələliyinə öz müsbət təsirini göstərər.

Yuxanda qeyd olunduğu kimi, kompyuter texnikasının sürətli inkişafı ilə əlaqədar olaraq, məhkəmə kompyuter-texniki ekspertizasının obyektlərinin daim genişlənməsi baş verir. Ona görə də bu növ ekspertizanın keyfiyyətli apanlması üçün

kompyuter texnologiyalan sahəsində baş verən yeniliklər, həmçinin yeni obyektlər üzrə müasir metodik tədqiqatlar daim izlənməlidir.

Məhkəmə kompyuter-texniki ekspertizası üçün materialların hazırlanması zamanı aşağıdakı qaydalara riayət edilməlidir:

-tədqiq olunan kompyuter sistem blokunun əməliyyat birləşmə yerləri kağızla tam örtülmüş və möhürlənmiş vəziyyətdə;

-maqnit daşıyıcılar yumşaq materiala bükülərək zərfə qablaşdırılmış və möhürlənmiş vəziyyətdə;

-tədqiq olunan lazer disklər, disketlər, smartfonlar, mobil telefonlar və sair bu kimi obyektlər ayn-aynlıqda qablaşdırılmış və möhürlənmiş vəziyyətdə ekspertizaya təqdim olunmalıdır.

Eyni zamanda, məhkəmə kompyuter-texniki ekspertizasının təyin olunması haqqında qərarda (qərardadda) tədqiq olunan obyektlərin göstəriciləri dəqiq qeyd edilməlidir.