AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ
MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

RƏHİMLİ ŞƏBNƏM CƏMİL qızı

«İQTİSADİ FƏALİYYƏT SAHƏSİNDƏ İNTERNET TEXNOLOGİYALARI VƏ KİBERCİNAYƏTLƏRƏ QARŞI MÜBARİZƏNİN HÜQUQİ ƏSASLARI»
mövzusunda

MAGİSTR DİSSERTASİYASI

İxtisasın şifri və adı: 060404 - "İqtisadiyyat"
İxtisaslaşma: "İqtisadiyyatın hüquqi tənzimlənməsi"

Elmi rəhbər:
hüquq üzrə fəlsəfə doktoru,
dosent F.E. HƏTƏMZADƏ

Magistr proqramının rəhbəri
iqtisad üzrə fəlsəfə doktoru,
dosent S.Z. İSAYEV

Kafedra müdiri:
iqtisad elmləri doktoru,
professor F.P. RƏHMANOV

BAKI-2015

MÜNDƏRİCAT

GİRİŞ

Mövzunun aktuallığı. Cəmiyyətin kompüterləşməsinin ən ciddi mənfi nəticəsi məhz kibercinayətlər hesab olunur. Kompüter sistemlərinin geniş yayılması, onların kommunikasiya sistemləri vasitəsilə əlaqələndirilməsi, bu sistemlərə elektron müdaxilə imkanını artırır. Bu cür cinayətlərin ənənəvi tipli cinayətlərdən tutmuş yüksək riyazi və texniki hazırlıq tələb edən cinayətlərə qədər çox geniş əhatə dairəsi mövcuddur. Fərdi kompüterlərin sayının sürətli artımı və inkişaf etmiş kommunikasiya sisteminin mövcudluğu hətta həvəskar-cinayətkarların belə kompüter sistemlərinə daxil olmasına imkan yaradır.

Əksər ölkələrdə mövcud olan cinayət qanunvericilikləri bu tip cinayətlərin təsnifləşdirilməsi baxımından kifayət qədər elastik olsalar da, sosial və texniki dəyişikliklər bu hüquq sistemi çərçivəsindən kənarda qalan yeni-yeni problemlər yaradır. Çünki dünya təcrübəsində mövcud olan bəzi kompüter cinayətlərinə cinayət qanunvericiliyi təsir göstərə bilmir. Belə ki, hüquqi baxımdan bu əməllər cinayət hesab edilə bilməz. Burada EHM-in bəzi əməliyyatlarının kriminallaşması problemi nəzərdə tutulur.

Kibercinayətkarlıq təhlükəsi bütün dünya ölkələri kimi Azərbaycan üçün də çox təhlükəli bir haldır və bu təhlükənin qarşısını almaq, həmçinin onunla effektli mübarizə aparmaq məqsədilə ölkəmiz Azərbaycan Respublikasının tarixli "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə 30.09.2009-cu il Qanunu ilə Avropa Şurasının "Kibercinayətkarlığa dair" Konvensiyasına qoşulmuşdur. Azərbaycan Avropa Şurasının "Kibercinayətkarlıq haqqında" 2001-ci il 23 noyabr tarixli Konvensiyasını imzalamış dövlətlər sırasına daxil olmasına baxmayaraq, beynəlxalq əməkdaşlıq özü də bu gün kibercinayətkarlıq problemi ilə mübarizənin yeni metodlarının axtarışı və vahid siyasətin işlənib hazırlanması prosesini yaşayır.

Tədqiqatın əsas məqsədi və vəzifələri. Bu tədqiqatın məqsədi kibercinayət-karlıq probleminin, onun ictimai təhlükəlilik dərəcəsinin qiymətləndirilməsi üçün zəruri olan kriminal əhəmiyyətli aspektlərin öyrənilməsi, bu hala qarşı mövcud

cinayət-hüquqi tədbirlərin təhlili və kibercinayətkarlıqla mübarizənin cinayət-hüquqi tənzimlənməsinin effektivliyinin artırılmasına yönəldilmiş təkliflərin işlənib hazırlanması təşkil edir. Bu məqsədə nail olmaq üçün aşağıdakı vəzifələrin həyata keçirilməsi nəzərdə tutulmuşdur:

- kibercinayətkarlığın vəziyyətinin, strukturu və dinamikasının dünya miqyasında kriminoloji təhlilini aparmaq;

- iqtisadi cinayətkarlıq, onun xüsusi bir forması olan kibercinayətkarlıq və eləcə də kibercinayət anlayışını formalaşdırmaq, kibercinayətlərin növlərini xarakterizə etmək;

- kibercinayətkarlıqla mübarizənin hüquqi təcrübəsini iki səviyyədə - beynəlxalq və milli səviyyədə təhlil etmək və eləcə də xarici ölkə qanunvericiliklərinin müqayisəli təhlilini aparmaq;

- kibercinayətkarlıqla mübarizə sahəsində beynəlxalq təcrübədən istifadə istiqamətlərini təhlil etməklə milli qanunvericiliyin təkmilləşdirilməsi imkanlarını müəyyən etmək.

Dissertasiya tədqiqatının obyektini kibercinayətkarlıqla mübarizə üzrə milli, eləcə də ayrı-ayrı xarici ölkələrin hüquq sistemləri təşkil edir. Tədqiqatın predmeti isə kibercinayətkarlığın kriminoloji aspektləri - onun vəziyyəti, strukturu, dinamikası və bu dinamikaya təsir göstərən amillər, onun cinayət-hüquqi mübarizə məsələləri, eləcə də kibermühitdə törədilən əməllərə görə məsuliyyəti müəyyən edən milli və beynəlxalq cinayət-hüquq normalarıdır.

Dissertasiya işinin elmi yeniliyi tədqiq olunan problemin respublikamızda son illər ərzində daha intensiv formada reallaşdırılmaqda olan internet texnologiyalarının tətbiqi ilə şərtlənir. Belə ki, tədqiq edilən sahənin kifayət qədər yeni olması, bu sahədəki elmi tədqiqatların aktuallığını və yeniliyini şərtləndirməkdədir.

Tədqiqatın informasiya bazasını mövzu ilə əlaqədar xarici tədqiqatçıların və ekspertlərin araşdırmaları, beynəlxalq təşkilatların işçi materialları və sənədləri, statistik və normativ – metodiki materiallar, o cümlədən kibercinayətkarlığa dair beynəlxalq təşkilatlar tərəfindən toplanmış məlumatlar, ayrı-ayrı ölkələrdə kompüter cinayətkarlığının vəziyyətinə dair məcmuələr, bir sıra seminar və konfransların

sənədləri, tədqiqat mövzusu üzrə elmi araşdırmalar və digər elmi ədəbiyyatlar təşkil edir.

İşin nəzəri – metodoloji bazasını kibercinayətkarlıq anlayışının, onun kompüter cinayətlərindən fərqinin, eləcə də bu halın mühüm kriminoloji əlamətləri və kibercinayətkarlıqla milli və beynəlxalq səviyyədə mübarizə istiqamətlərinin öyrənilməsi və tədqiqi ilə bağlı alimlərin tədqiqatları, onların əldə etdikləri nəticələr, eləcə də milli və ayrı-ayrı xarici ölkələrin hüquq yaratma orqanlarının səlahiyyətlərinə müvafiq formalaşdırdıqları qanunvericilik aktları sistemi (beynəlxalq qanunvericilik, o cümlədən Avropa Şurasının "Kibecinayətkarlıq haqqında" Konvensiyası, xarici ölkələrin kibercinayətkarlıqla mübarizə məsələlərinə istiqamətləndirilmiş milli qanunvericilikləri, Azərbaycan Respublikasının cinayət qanunvericiliyi) təşkil etmişdir. Tədqiqatda qarşıya qoyulan məsələlərin həllinə nail olmaq üçün müqayisəli təhlil, statistik təhlil, səbəb–nəticə, funksional, məntiqi, struktur, həmçinin, analiz və sintez və s. tədqiqat üsullarından istifadə edilmişdir.

Dissertasiyanın strukturu giriş, üç fəsil, nəticə və təklifdən ibarətdir. Dissertasiyada iqtisadi cinayətkarlıq, eləcə də onun xüsusi forması kimi kibercinayətkarlığın anlayışı, mahiyyəti açıqlanmış, kibercinayətlərin subyektlərinin təsnifatı aparılmış, kibercinayətkarlığınmiqyası, ictimai təhlükəsi təhlil edilmiş və ona qarşı mübarizənin formalaşdırılması istiqamətləri tədqiq edilmişdir. Bununla yanaşı tədqiqat işində Azərbaycan Respublikasının qanunvericilik sistemində iqtisadi cinayətkarlıq formalarının hüquqi təsbiti məsələləri və kibercinayətkarlığa qarşı mübarizənin hüquqi təminatının müasir vəziyyəti təhlil edilmiş, kibercinayətkarlıqla mübarizə sahəsində ayrı-ayrı ölkələrin qanunvericiliklərinin müqayisəli təhlili həyata keçirilmiş və Azərbaycanda kibercinayətkarlıqla mübarizə sahəsində beynəlxalq təcrübədən istifadə istiqamətləri geniş tədqiq edilmişdir.

Tədqiqatın sonunda nəticələr ümumiləşdirilmiş və təkliflər çıxarılmış, istifadə olunan ədəbiyyat siyahısı və internet resurslar təqdim edilmişdir.

FƏSİL I. İQTİSADİ SAHƏDƏ CİNAYƏTKARLIQĞIN SPESİFİK FORMASI KİMİ KİBERCİNAYƏTLƏRİN KONSEPTUAL ASPEKTLƏRİ

1.1 İqtisadi fəaliyyət sahəsində internet texnologiyalarının tətbiqi və bu sahədə cinayətkarlığın əsas təzahür formaları

İnformasiya texnologiyaları XX əsrin son on illiklərində informatikanın yaranması prosesində meydana gəlmişdir. İnformasiya texnologiyalarının özəllikləri ondan ibarətdir ki, orada əmək məhsulu və predmeti rolunu informasiya, əmək alətləri rolunu isə hesablama texnikası və rabitə vasitələri oynayır. İqtisadi və biznes proseslərinin müasir İKT əsasında idarə edilməsi istər konseptual, istərsə də tətbiq baxımından qlobal hadisədir. E-biznesin, E-kommersiyanın iqtisadiyyatın inkişafına təsiri artıq cəmiyyətin bütün sahələrini əhatə etməkdədir. Elektron kommersiya sifarişçi tələblərinin formalaşmasına radikal təsir edə bilmə imkanı təklif edir ki, bu da bazarları ya kökündən dəyişdirir, ya da tamamilə yeni tipli bazarlar yaradırlar. Cəmiyyətin ayrı-ayrı üzvləri malların və xidmətlərin əldə edilməsi proseslərinə, informasiya əlyetərliyinə və hökumət orqanları ilə qarşılıqlı əlaqələrin tamamilə yeni imkanlarına malik olur. Bu zaman seçim imkanı coğrafi və vaxt məhdudiyyətindən asılı olmayacaqdır. E-kommersiya texnologiyası alıcı və satıcılara aşağıdakı əlverişli imkanlardan eyni dərəcədə istifadə etməyə imkan verir.

- Biznesin qlobal miqyasda aparılması. E-kommersiya sistemi hətta xırda tədarükçü və sifarişçilərə də dünya miqyasında bizneslə məşğul olmaq imkanı verir.
- Satıcıların rəqabətqabiliyyətliliyinin yüksəlməsi. E-kommersiya tədarükçülərə "sifarişçiyə yaxınlaşma" hesabına rəqabətqabiliyyətliliyini yüksəltmək imkanı verir. Belə ki, bir çox şirkətlər satışqabağı və satışdan sonra geniş dəstək təklif edir.
- Satışın fərdiləşməsi. Elektron qarşılıqlı əlaqə vasitələrindən istifadə edərək şirkət hər bir fərdi sifarişçinin sorğuları haqqında müfəssəl informasiya ala bilər və avtomatik olaraq onun fərdi tələblərinə uyğun məhsulları və xidmətləri təklif edə bilər.
- Sorğuya operativ reaksiya. E-kommersiya tədarükçüdən sifarişçiyə göndərilən əmtəənin yolunu əhəmiyyətli dərəcədə qısaltmağa imkan verir. O həm

maliyyə, həm də vaxt məsrəflərini azaltmağa imkan verən optimal yol təklif edir. Xüsusi hallarda məhsullar və xidmətlər elektron üsullarla çatdırıldıqda yola maksimal qənaət olunur.

- Məsrəflərin azalması. Elektron yolla bağlanmış satış bir qayda olaraq xidmət xərclərinin dəyərini aşağı salır. İnsanlar arasında elektron qarşılıqlı əlaqədən istifadə edən hər hansı biznes-proses hər iki tərəfin xərclərini azaltmaq potensialına malikdir.
- Biznesin aparılmasının yeni imkanları. E-kommersiya texnologiyaları tamamilə yeni məhsulların və xidmətlərin meydana gəlməsinə şərait yaradır.

Ən yeni informasiya və telekommunikasiya texnologiyalarının tətbiqinə əsaslanan E-kommersiyanın əsas xüsusiyyəti alıcı ilə satıcı arasındakı bir çox əlaqələrin İnternet vasitəsilə həyata keçirilməsidir. Elektron kommersiyanın fərqləndirici xüsusiyyəti olaraq onun bütövlükdə təşkilatın daxili və xarici aləmini xarakterizə edən, o cümlədən təşkilatın əlverişli bazar mühitinin yaradılması ilə bağlı problemlərinin birləşdirilməsini hesab etmək olar. Bu isə elektron biznesin iqtisadi inkişafın mühüm mənbələrindən birinə çevrilməsinə şərait yaradır. İKT saziş iştirakçıları arasında kommersiya informasiyalarının interaktiv və sürətli mübadiləsini təmin edir ki, bu da nəticədə bir çox hallarda baş verə bilən anlaşılmazlıqları aradan qaldırır. Eyni zamanda əvvəlcədən qəbul edilmiş məsuliyyətli qərarın, bağlanan sazişin parametrləri haqqında tam, dəqiq və dürüst informasiya alanadək təxirə salmaq imkanı vardır. Elektron biznes iqtisadi mühiti əhatə edən problemlərin həllinin yeni üsullarını təqdim edir.

Elektron biznesdə (verilənlərin elektron mübadiləsi (EDİ), elektron poçtlar, kataloqlar, fondların elektron ötürülməsi və s.) müxtəlif texnologiyaların tətbiqi sahibkarlıq fəaliyyətində müəyyən rəqabət üstünlükləri yaradır. Aparılan əməliyyatların müxtəlifliyi malların və xidmətlərin reklam olunmasını və hərəkətini, bazarın konyukturasının öyrənilməsini, elektron ticarətləri və ödənişləri, tədarük olunan malların və xidmətlərin çatdırılmasını və satışdan sonrakı mühafizəsini təmin edir. Sifarişlərin rəsmiləşdirilməsi də daxil olmaqla məhsulun istehsalçıları və alıcıları arasında olan bütün kommersiya əməliyyatları - çatdırılma, hesabların açıqlanması və ödənilməsi İnternet şəbəkəsi vasitəsilə həyata keçirilir. Alıcılar, satıcılar, vasitəçilər İnternet

fəzada malların və xidmətlərin transmilli virtual bazarlarını yaradırlar. Elektron kommersiya firma və ticarətin digər iştirakçılarının keyfiyyətli təşkilati-iqtisadi, texniki və texnoloji təchizatını stimullaşdırır, həm də fəaliyyətin sonrakı artımını təmin edirlər. Bu xüsusilə ticarət iştirakçıları global bazara çıxdığı zaman nəzərə çarpır. Nəzərə almaq lazımdır ki, e-kommersiyanın inkişafı malların və xidmətlərin dünya bazarına asan daxil olmasını təmin edir, ənənəvi maneələri dağıdaraq korporasiya nümayəndələrinin qlobal sazişlərə qoşulmasına imkan yaradır.

İqtisadi yüksəlişin intensivləşməsində və keyfiyyətində E-kommersiya biznes-nailiyyətin başlıca amilinə çevrilərək daha böyük əhəmiyyət kəsb edir. E-kommersiya artıq istehsalın həyata keçirilməsinin və istehsal dövriyyəsinin avtomatlaşdırılmasının texniki və iqtisadi vasitəsidir. İnternet məkanda meydana gələn E-kommersiya ənənəvi sahibkarlıq qədər geniş və hərtərəflidir. E-kommersiyanın yaranmasının və eyni zamanda onun səciyyəvi xüsusiyyətlərinin və üstünlüklərinin əsas səbəbi təbii ki, istehsalın tranzaksiya xərclərinin aşağı salınmasıdır. Bununla belə, məqsəd təkcə tranzaksiya xərclərinin aşağı salınması deyildir. Əsas məsələ son məhsulun dəyərinin aşağı salınmasında iqtisadi effektin əldə edilməsi, yeni, daha effektli, yüksək dərəcəli istehlak dəyərinə malik məhsulların hazırlanmasında yeni texnologiyaların istifadə edilməsidir. Qiymətlərin ümumi aşağı salınması, bazarın genişləndirilməsi, rəqabətin güclənməsi mühüm şərtdir.

E-kommersiya texnologiyası biznesin aparılmasının ən yaxşı üsullarını meydana çıxartmağa imkan verir. O, müasir beynəlxalq münasibətlər sistemində makroiqtisadi aspektdə müsbət təsirə malikdir. Elektron kommersiyası beynəlxalq əmək bölgüsünə, kapitalın beynəlxalq hərəkətinə, işçi qüvvəsinin miqrasiyasına və s. kifayət qədər böyük təsir göstərir.

Təsərrüfat fəaliyyəti sferasında yeni münasibətlərin meydana gəlməsi və inkişafı, mülkiyyətin alternativ formalarının əmələ gəlməsi, idarə etmədə və bölgüdə bazar prinsiplərinin istifadə olunması iqtisadi cinayətlərlə bağlı vəziyyəti daha da ağırlaşdırmışdır. Mülkiyyət obyektlərinə qərəzli qəsdlər, iqtisadi proseslərin idarə edilməsində korrupsiya hallarının yayılması milli iqtisadiyyatların, eləcə də bütövlükdə dünya iqtisadiyyatının inkişafına ciddi təhlükə törədir.

Son dövrlərdə daha geniş vüsət alan bu vəziyyət uyğun olaraq iqtisadi cinayətkarlıqla mübarizə sahəsində də yeni elmi yanaşmaların işlənib hazırlanmasını zərurətə çevirmişdir. Hər şeydən əvvəl iqtisadi cinayətlər və həmçinin bu kateqoriyaya daxil olan konkret sosial halların dərindən təhlili aparılmalıdır.

İqtisadi cinayətkarlıq problemi bu fenomenin inkişafının bütün tarixi boyunca daima tədqiqatçıların diqqətini cəlb etmişdir. İqtisadi cinayətkarlığın ilkin anlamı faktiki olaraq mülkiyyət cinayətkarlığı anlamına gəlib çıxırdı.[1] Belə ki, kriminal təcrübənin bu yeni tendensiyaları hüquq elm və metodologiyasında öz adekvat əksini tapmırdı. Lakin artıq XIX əsrin 60-cı illərində bu problemin aparıcı fransız tədqiqatçılarından olan M.Paten özünün "Biznes sferasında cinayət hüququnun və cinayət qanunvericiliyinin ümumi hissəsi" (1861-ci il) işində iqtisadi cinayətkarlıq probleminin elmi tədqiqi məsələsinin vacibliyini qeyd edərək aşağıdakı suallara təcili cavab tapılmasını zəruri hesab edirdi:

- iqtisadi cinayətlər, o cümlədən sahibkarlıq fəaliyyəti səhəsində cinayətlər;
- bu sferada cinayət-hüquqi tənzimləmə, o cümlədən vergi-cinayət hüququ;
- sahibkarların, o cümlədən vergi ödəyicilərinin cinayət-hüquqi müdafiəsi;
- sahibkarların, o cümlədən vergi ödəyicilərinin cinayət məsuliyyəti.

O dövrün aparıcı mütəxəssisləri iqtisadi cinayətkarlıq problemini gələcəyin böyük sosial problemi kimi qiymətləndirərək, onun "yüksək artım" tempinə malik olduğunu və həllinin xüsusi müzakirə tələb edəcəyini qeyd edirdilər.

İqtisadi cinayətkarlıq probleminin tədqiqinin mühüm mərhələsi kimi kriminoloq E.Sazerlendin işi çıxış edir. Belə ki, onun ilk dəfə olaraq korporasiyaların cinayətkarlığının sistemli tədqiqini aparmaqla əsasını qoyduğu kriminoloji konsepsiya bu aktual problemin sonrakı dərk olunma üsullarına güclü ideoloji təsir göstərmişdir. E. Sazerlendin "Ağ yaxalıqlıların cinayətkarlığı" konsepsiyasının əsasında iqtisadi cinayətkarlığın korporasiyaların cinayətkarlığı kimi təyini formalaşmışdır. Q.İ.Şnayderin qeyd etdiyinə görə 80-ci illərin ortalarına yaxın Qərb ədəbiyyatında "ağyaxalıqlıların cinayətkarlığı" anlayışı yerinə daha çox "xidməti

[1]Г.А.Леман Экономические факторы преступности. М.: Издание, 2008

cinayətlər" və "korporativ cinayətkarlıq" termini istifadə olunmağa başladı. Bir çox tədqiqatçılar da iqtisadi cinayətkarlıq qismində məhz korporasiyaların cinayətkarlığını başa düşürdülər.[1] Q. Şnayderin sözlərinə görə, xidməti cinayətlər sırasına xidməti vəzifələrin həyata keçirilməsi prosesində törədilən bütün qanun pozuntuları daxildir. Lakin qeyd etmək lazımdır ki, iqtisadi cinayətlər sırasında yuxarıda qeyd olunmuş xidməti cinayətlər qrupunun ayırması, daha az sosial əhəmiyyətli, bəzəndə ümumiyyətlə əhəmiyyətsiz kriminoloji halların tədqiqinə yol açır. Bu isə ictimai diqqətin kiçik və orta sahibkarlıq subyektləri tərəfindən törədilən mühüm sosial miqyaslı cinayətlərdən yayınmasına səbəb olur.

E. Sazerlendin də mühüm rolu öz konsepsiyasında əsas diqqəti məhz yeni bir hal kimi qiymətləndirilən, təhlükəli iqtisadi cinayət əməllərinin subyektləri qismində biznes sferasında yüksək sosial duruma malik olan hüquqi şəxslərin, eləcə də öz şəxsi maraqları naminə professional fəaliyyət prosesində cinayət törədən şəxslərin çıxış etməsi məsələsinə yönəltməsindən ibarət olmuşdur. Onun tərəfindən elmə gətirilən "ağ yaxalıqlıların cinayətkarlığı" termini konsepsiyanın bu xüsusiyyətini daha dəqiq əks etdirir.

Analoji prinsipə əsaslanaraq amerika kriminoloqları R.Kuinni və M.Klaynard iqtisadi cinayətkarlıq çərçivəsində iki növ cinayətləri fərqləndirirlər. Birinci, məşğulluğun növünə görə cinayətkarlıq. Buraya şəxsi qazanc əldə etmək məqsədilə peşəkar fəaliyyət prosesində şəxslər tərəfindən törədilən cinayətlər, o cümlədən, işçilərin öz rəhbərlərinə qarşı törətdiyi cinayətlər daxildir. İkinci növ isə korporasiyaların cinayətləridir. Buraya isə hüquqi şəxs kimi korporasiyaların və eləcə də korporasiya idarə heyyəti üzvlərinin cinayətləri daxildir. Bütün bu yanaşmalar iqtisadi cinayətkarlığın "dar" şərhi olmaqla, problemli sahəni tam adekvat təsvir etmir. Belə yanaşmanın darlığı onunla izah olunur ki, iqtisadi cinayətlər yalnız müəssisələrin adından və onların maraqları naminə törədilmir. Sazerlendin konsepsiyasının inkişafı və kriminal təcrübədə yeni tendensiyaların mənimsənilməsi

[1] Винер И. Экономическая преступность: Теория экономического уголовного права. Будапешт. 1984

prosesində bu anlayışın geniş şərhləri təklif edilmişdir. Anlayışın genişləndirilmə tendensiyası iki qarşılıqlı əlaqəli aspektdə aşkara çıxır.

Birincisi, iqtisadi cinayətlərin subyekt dairəsinin genişlənməsi. Tədricən bu kateqoriyaya korporasiyaların yalnız ali rəhbərləri deyil, digər işçiləri də aid edilməyə başladı. Sonralar isə subyektlər üzrə məhdudiyyətlər tamamilə aradan götürüldü. Dəyişməz qalan isə bu cinayətlərin peşəkar fəaliyyət sahəsində törədilməsi əlaməti oldu.

İkincisi, iqtisadi cinayətlərin siyahısı dəyişdi. Sonralar bu cinayətlərə vergilərdən yayınma, kompüter cinayətləri həmçinin dövlət iqtisadiyyatına, onun ayrı-ayrı sahələrinə, sahibkarlıq fəaliyyətinə və eləcə də ayrı-ayrı qrup şəxslərin iqtisadi maraqlarına ziyan vuran digər cinayətlər də aid edilməyə başladı. Bu cinayətlərin siyahısı 20-30 tərkibə qədər genişləndi. Elm "xəritəsində" baş verən bu dəyişikliklər yalnız elmi biliyin inkişafının daxili məntiqi ilə deyil, eləcə də tədqiq olunan halın - iqtisadi cinayətkarlığın təkamülü ilə şərtlənir.

Problemə yeni yanaşma tədqiqatçılara iqtisadi cinayətkarlığın bu və ya digər əlamətlərlə bir-birindən fərqlənən çoxsaylı yeni şərhlərini təklif etməyə imkan verdi. Bunlardan bəzilərini nəzərdən keçirək.

Q.K.Mişin iqtisadi cinayətkarlığı yaşam uğrunda ümumi mübarizənin sosial həyatda təzahürü kimi nəzərdən keçirərək, onun mahiyyətini iqtisadi maraqların münaqişəsi kimi izah edir. Onun fikrincə, iqtisadi cinayətlər sırasına təsərrüfat cinayətləri ilə yanaşı həmçinin, bazar iqtisadiyyatı şəraitində bu və ya digər səviyyədə təsərrüfat fəaliyyəti ilə əlaqədar olan mülkiyyət əleyhinə törədilmiş bütün cinayətlər daxil edilməlidir.[1]

Rusiyada yeni cinayət məcəlləsinin yaradılması zamanı iqtisadi cinayətlərin təyin edilməsinə geniş yanaşma reallaşdırılmışdır. Qüvvədə olan Cinayət Məcəlləsində mülkiyyət əleyhinə, eləcə də iqtisadi fəaliyyət sahəsində törədilən cinayətləri özündə birləşdirən 3 fəsil və 47 maddədən ibarət "İqtisadi sahədə cinayətlər" adlı bölmə mövcuddur. Lakin buna baxmayaraq bu bölməyə ənənəvi

[1] Мишин Г.К. Проблема экономической преступности (опыт междисциплинарного изучения). - М.: ВНИИ МВД России, 1994, С. 33-34.

olaraq iqtisadi cinayətlər hesab olunan vəzifə cinayətləri (səlahiyyətdən sui-istifadə etmə, rüşvətxorluq və s.), kompüter cinayətləri, intellektual mülkiyyətə və müəlliflik hüququna qəsd etmə kimi cinayətlər daxil edilməmişdir. Digər tərəfdən, mülkiyyət əleyhinə cinayətlər (mülkiyyətə birbaşa qəsdlə əlaqədar olan cinayətlər (oğurluq, soyğunçuluq, quldurluq, əmlakın məhv edilməsi və ya israf edilməsi) və eləcə də iqtisadiyyatla əlaqədar olmayan digər mülkiyyət əleyhinə cinayətlər) iqtisadi cinayətlərə daxil deyildir.

V.V. Luneyevanın fikrincə dünya ədəbiyyatında mövcud bütün yanaşmaların rəngarəngliyinə baxmayaraq bazar iqtisadiyyatlı ölkələrdə iqtisadi cinayətkarlığın mahiyyətini korporasiyaların dövlət əleyhinə, digər korporasiyalar əleyhinə törətdiyi, eləcə də korporasiya işçilərinin korporasiya əleyhinə, korporasiyaların istehlakçılar əleyhinə törədiyi cinayətlər təşkil edir.[1]

E.E.Demetyeva ABŞ və Almaniya kriminoloqlarının təklif etdikləri tərifləri ümumiləşdirərək güman edir ki, "iqtisadi cinayətkarlıq – fiziki və hüquq şəxslər tərəfindən törədilən, bütövlükdə ölkənin iqtisadi maraqlarına, o cümlədən xüsusi sahibkarlıq fəaliyyətinə və ayrı-ayrı qrup şəxslərin maraqlarına qəsd edən həmçinin qanuni iqtisadi fəaliyyət çərçivəsində müntəzəm olaraq qazanc (fayda) əldə etməyə yönəldilmiş qeyri-qanunu fəaliyyətdir."[2]

E.İ.Petrov, R.N. Marçenko, L.V. Barinovanın fikrinə görə isə iqtisadi cinayətkarlıq şəxslərin iqtisadi sferada peşəkar fəaliyyət prosesində bu fəaliyyətlə əlaqədar olan və istehlakçıların, partnyorların, rəqiblərin və dövlətin mülkiyyət və digər maraqlarına, eləcə də müxtəlif təsərrüfat sahələrində iqtisadiyyatın idarə olunma qaydasına zidd olaraq törətdiyi qərəzli əməllərin məcmusu kimi nəzərdən keçirilməlidir.

İqtisadi cinayətkarlığın mahiyyətini daha dəqiq şərh edə bilmək üçün bu cinayətkarlığın hansı əlamətlərə malik olmasını müəyyən etmək mühüm əhəmiyyət kəsb edir. Xarici ölkələrdə baş verən iqtisadi cinayətlərin ciddi tədqiqini aparmış E.E.

---

[1] Лунеев В.В. Преступность XX века. - М.: 1997. - С. 257.

[2] Дементьева Е.Е. Экономическая преступность и борьба с ней в странах с развитой рыночной экономикой. - М.: ИНИОН РАН, 1992. - С. 12.

Demetyeva xarici kriminoloji ədəbiyyatın dərin təhlili nəticəsində iqtisadi cinayətkarlığın aşağıdakı əlamətlərini müəyyən etmişdir:

- Qərəzli xarakterə malik olması: Belə ki, bu cinayətlərin əsas məqsədini ekvivalentlik prinsipinin pozulması ilə iqtisadi resursların mənimsənilməsi nəticəsində mənfəətin əldə olunması təşkil edir. Bununla belə cinayətlər üçüncü şəxslərin və müəssisələrin maraqları çərçivəsində şəxsi fayda əldə etmək məqsədilə də törədilə bilər.

- Peşəkar fəaliyyət prosesində törədilməsi**:** 1982-ci ildə keçirilmiş beynəlxalq seminarda iqtisadi cinayətkarlığın şərhində bu əlamətin əhəmiyyəti xüsusi qeyd olunurdu.

- Subyektlərin dövlətlə və eləcə də öz aralarında yaranan və istehsal, təkrar istehsal, bölgü, mübadilə və istehlakın həyata keçirilməsi üçün zəruri olan müqavilə və öhdəliklərlə əlaqəli olması;

- Zərər çəkmiş şəxslərin kollektivliyi, cinayətlərin cəmiyyət üçün gizli xarakterə malik olması, cinayətkar və zərər çəkmiş şəxs arasında məsafənin böyüklüyü:Cinayət əməlinin obyekti qismində isə bütövlükdə iqtisadiyyat, onun ayrı-ayrı sektorları, fərdi sahibkarlıq fəaliyyəti və eləcə də şəxslər qrupu çıxış edir.

- Zərər çəkmiş şəxslərin məxfiliyi (anonimliyi);

- İki növ subyektin olması: hüquqi şəxslər (korporasiyaların cinayətkarlığı) eləcə də müəssisə adından və onun maraqları çərçivəsində fəaliyyət göstərən fiziki şəxslər (məşğulluğun növü üzrə cinayətkarlıq). Hüquqi şəxslər yalnız qanunvericiliklərində hüquqi şəxslərin cinayət məsuliyyətinin nəzərdə tutulduğu ölkələrdə cinayətin subyekti hesab olunur.(ABŞ, Fransa);

- Dövlətin, fərdi sahibkarların və eləcə də vətəndaşların iqtisadi maraqlarına vurulan əhəmiyyətli zərərin mövcudluğu;

- Xarakter müxtəlifliyi;

- İqtisadi cinayətin nəticəsi kimi maddi vəsaitlərin yenidən bölgüsünün baş verməsi;

- Davamlı, sistemli xarakterə malik olması.

Bütün sadalananlarla yanaşı iqtisadi cinayətlərin digər əlamətləri də mövcuddur ki, bunları aşağıdakı sxem 1.1-də daha aydın təsvir etmək olar.

İqtisadi istiqamətli cinayətlərin mühüm kateqoriyası iqtisadi münasibət subyektləri tərəfindən iqtisadi münasibətlərin hüquqi formalarının istifadəsi vasitəsilə törədilir. Lakin belə olan halda onlar peşəkar fəaliyyəti həyata keçirmirlər.

İqtisadi cinayətkarlığın ənənəvi şərhi dövlətin müasir iqtisadiyyatda rolunun artması nəticəsində iqtisadi cinayətlərin yeni subyektlərinin meydana gəlməsini nəzərə almır. Belə ki, dövlətin iqtisadiyyatda rolunun artması nəticəsində dövlət maliyyə fondları tərəfindən yenidən bölüşdürülən ÜDM-un həcmi artmışdır. Bunun nəticəsində isə maliyyə resurslarının formalaşdırılması, bölgü və yenidən bölgüsü ilə əlaqədar sui-istifadə hallarının yeni kateqoriyası meydana gəlmişdir.

Qərəzli xarakter	Əhəmiyyətli zərər	Zərər çəkmiş şəxslərin kollektivliyi	Xarakter müxtəlifliyi
Cinayətdən zərər çəkmiş şəxslərin anonimliyi	Cinayətin başvermə faktının qeyri-aşkarlığı	Fərdi məsuliyyətin müəyyən olunma çətinliyi	Öhdəlik münasibətlərinin istifadə olunması
Yüksək səviyyədə məxfilik	Peşəkar fəaliyyət prosesində törədilməsi	Cinayətkar və zərər çəkmiş şəxs arasında məsafənin böyüklüyü	Zor tətbiq edilmədən törədilməsi

Sxem 1.1 İqtisadi cinayətkarlığın əlamətləri

Beləliklə, cinayətin iqtisadi olub-olmamasının mühüm meyarı kimi nə cinayətin subyekti, nə də qəsdin obyekti deyil, hər şeydən öncə modus operandi, yəni cinayətin törədilmə üsulu çıxış edir. Bununla belə yuxarıda nəzərdən keçirilən iqtisadi cinayətkarlığın mühüm kriminoloji əlamətləri öz əhəmiyyətini itirmir. Lakin onların bəziləri iqtisadi yönümlü bütün cinayətlər üçün mühüm və ümumi deyildir.

İqtisadi cinayətkarlığın əlamətlərini aşağıdakı kimi də təsnifləşdirmək olar:

- sahibkarlıq fəaliyyəti və eləcə də biznes sferasında baş verməsi;
- bilavasitə iqtisadi fəaliyyət prosesində, onun sərhədləri və səlahiyyətləri çərçivəsində həyata keçirilməsi;
- sahibkarlıq fəaliyyəti subyektləri tərəfindən törədilməsi;
- qanuni iqtisadi fəaliyyətin həyata keçirilməsi prosesində iqtisadi nemətlərin mənimsənilməsinin kriminal üsullarının istifadə olunması;
- anonimlik, zərər çəkmiş şəxslərin fərdiləşməsinin mövcud olmaması;
- zərər çəkmiş şəxs ilə birbaşa əlaqənin olmaması;
- qəsd etmə obyektlərinin çoxluğu və spesifikliyi; Bu qəsd etmənin çoxlu və spesifik obyektləri qismində hər hansı bir ölkənin iqtisadiyyatı, onun ayrıca götürülmüş müəyyən bir seqmenti, təsərrüfatçılığın ayrı-ayrı subyektləri (mülkiyyət müxtəlifliyinə əsaslanan müəssisələr, hüquqi şəxs yaratmadan sahibkarlıq fəaliyyəti ilə məşğul olan sahibkarlar), ev təsərrüfatları və eləcə də qeyri-kommersiya müəssisələrin pul və digər vəsaitləri çıxış edir.[1]
- iqtisadi cinayətkarlıq subyektlərinin spesifikliyi;
- cinayətlərin kütləviliyi və səciyyəviliyi (tipikliyi): Cinayətlərin tipikliyi dedikdə, müxtəlif cinayətkarlar tərəfindən törədilməsinə baxmayaraq iqtisadi cinayətlərin bir növ şablon xarakterə malik olması yəni, eyni və ya oxşar sxem, mexanizm və üsullar vasitəsilə həyata keçirilməsi başa düşülür.
- cinayətlərin məxfiliyi: Bu cinayətlərin əsasən qanuni iqtisadi fəaliyyətin himayəsi altında törədilməsi onların dərhal aşkara çıxarılmasına və qanuni fəaliyyətdən fərqləndirilməsinə imkan vermir. Başqa sözlə, qanuni sahibkarlıq fəaliyyəti çərçivəsində törədilən əməlin cinayət xarakteri gizli qalır.
- cinayətlərin qərəzli xarakterə malik olması;
- qeyri-zorakı cinayət hesab olunması;

Дементьева Е. Е.Экономическая преступность и борьба с ней в странах с развитой рыночной экономикой... С. 11.

- iqtisadi cinayətlərə cəmiyyətin laqeyd münasibət göstərməsi fenomeninin mövcudluğu: Cəmiyyətin əksər üzvləri iqtisadi cinayətlərə laqeyd yanaşır. Belə laqeydliyin əsasında cəmiyyətə zərər vurulması faktının aşkara çıxarılma çətinliyinin mövcud olması, həmçinin iqtisadi cinayət törətmiş şəxsin, cinayətkarın cəmiyyətdə formalaşmış ənənəvi cinayətkar stereotipinə uyğun gəlməməsi faktı dayanır.

Cinayət əməllərinin çoxcəhətliliyi, onların təhlilinin ilkin addımı kimi bu əməllərin təsnifləşdirilməsi zərurətini ortaya çıxarır. Xüsusi ədəbiyyatda təsnifləşdirmənin müxtəlif variantları istifadə olunur. Cinayət əməlləri ya qanunverici əsasa görə, yəni bu cinayətlərin törədilməsi nəticəsində pozulan qanunlar üzrə, ya qəsd etmə obyektinə görə, ya da iqtisadi cinayətlərə aid edilən əməllərin sadəcə olaraq siyahısına görə təsnifləşdirilir.

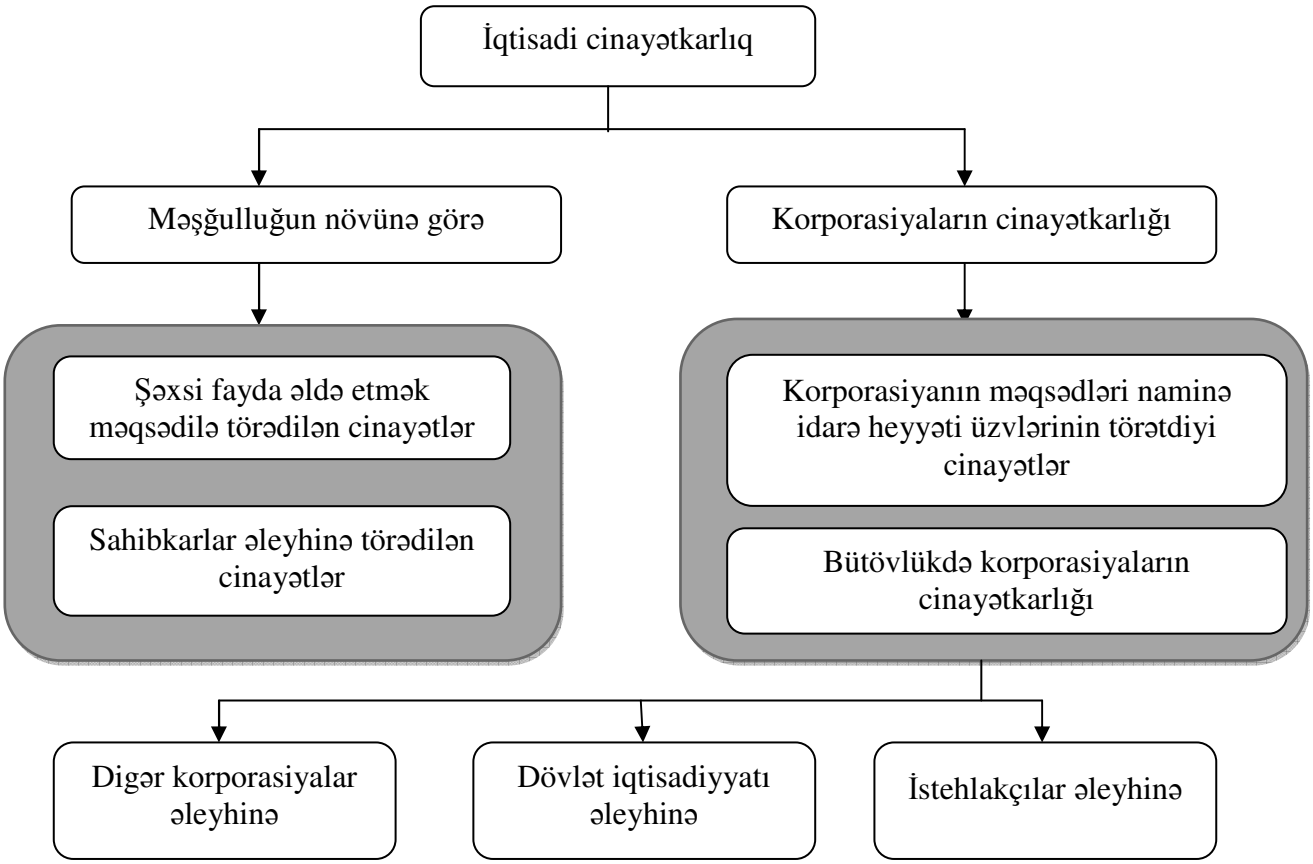
İqtisadi cinayətlərin ilkin təsnifatlarından biri 70-ci illərin sonunda BMT-nin Asiya və Yaxın Şərqdə Cinayətkarlığın qarşısının alınması və qanun pozucuları ilə davranış üzrə İnstitutu (UNAFEİ) tərəfindən təklif olunmuşdur. Bu təsnifata bazar iqtisadiyyatının təkmilləşdirilməsinə yönəldilmiş və bazar iqtisadiyyatını tənzimləyən qanunlar, eləcə də maliyyə və vergi qanunvericiliyinin pozulması, korrupsiya daxil edilmişdir.

Avropa Birliyinin mütəxəssisləri tərəfindən iqtisadi cinayətlərin aşağıdakı təsnifat sxemi qəbul edilmişdir:

- inhisar cinayətləri;
- dələduzluq (ələ alma, etibardan sui-istifadə etmə, alıcıların aldadılması);
- rəqəm maxinasiyaları;
- saxta müəssisələrin yaradılması;
- mühasibat sənədlərinin saxtalaşdırılması;
- erqonomik tələb və standartların pozulması;
- əmtəələrin yazılmasında bilərəkdən həyata keçirilmiş qeyri-dəqiqlik;
- haqsız rəqabət;
- maliyyə pozuntuları və vergi ödəməkdən yayınma;
- gömrük cinayətləri, pozuntuları;
- valyuta maxinasiyaları;

- birja və bank pozuntuları;
- ətraf mühitə zərər vuran pozuntular;
- çirkli pulların yuyulması.

Klinard və Kuini iqtisadi cinayətlərin strukturunda məşğulluq növlərinə görə cinayətkarlığı və korporasiyaların cinayətkarlığını fərqləndirərək onun daha geniş təsnifatını aşağıdakı sxem şəklində vermişlər.



Sxem 1.2 İqtisadi cinayətlərin təsnifatı

Marşal Klaynard və Peter Nigerin təsnifatına görə korporasiyaların cinayətlərinin aşağıdakı 6 növü var :

- inzibati aktların və qətnamələrin pozulması;
- təbiətin qorunması üzrə qanunvericiliyin pozulması (havanın və suyun çirkləndirilməsi, ərazilərin neft-kimya məhsullar ilə çirkləndirilməsi və s.);

- maliyyə pozuntuları (siyasi təşkilatlara subsidiyaların qanunsuz olaraq verilməsi, siyasətçilərin ələ alınması, valyuta əməliyyatları üzrə qanunvericiliyin pozulması və s.);

- əməyin qorunması və təhlükəsizliyi haqqında qanunvericiliyin pozulması (dininə, cinsinə, irqi əlamətlərinə görə muzdlu işçilərin diskriminasiyası);

- "istehsal cinayətləri" (zəruri keyfiyyət və təhlükəsizlik tələblərinə cavab verməyən, istehlakçıların sağlamlığına zərər vura bilən əmtəələrin istehsalı və satışı və s.)

- "haqsız ticarət təcrübəsi" (rəqabət şərtlərinin pozulması, razılaşma qiymətlərinin təyini, bazarın qeyri-qanuni bölüşdürülməsi və s.)

E.E. Demetyeva bazar iqtisadiyyatlı ölkələrin iqtisadi cinayətkarlığının əsasını təşkil edən korporativ cinayətlər üzrə tədqiqatının nəticələrini ümumiləşdirərək onun növlərinin aşağıdakı fərqli təsnifatını verir:

– kapital qoyuluşlarından sui-istifadə nəticəsində partnyorlara, səhmdarlara və s. zərər vurulması üzrə cinayətlər (mühasibat sənədləri, səhmlər üzrə müxtəlif maxinasiyaların həyata keçirilməsi);

– depozit kapitalının sui-istifadəsi nəticəsində kreditorlara, qarantlara zərərin vurulmasından ibarət olan cinayətlər (kreditorlara zərər vuran saxta müflisləşmə, sığorta sahəsində dələduzluq, subsidiyalarla əlaqədar maxinasiyalar);

– azad rəqabət qaydalarının pozulması ilə əlaqədar cinayətlər (sənaye cəsusluğu,qiymətlərin süni artırılması və azaldılması, saxta reklam);

– istehlakçıların hüquqlarının pozulmasından ibarət cinayətlər (istehlakçılara fiziki və eləcə də maddi zərər vura bilən keyfiyyətsiz məhsulun istehsalı);

– dövlətin maliyyə sisteminə qəsd edən cinayətlər (gəlirin gizlədilməsi, vergi ödəməkdən yayınma, istehsal və ticarətə nəzarətin pozulması);

– təbiətin qanunsuz istifadəsi və ətraf mühitə zərər vurulması ilə əlaqədar olan cinayətlər;

– sosial sığorta və pensiya təminatı sahəsində maxinasiyaların həyata keçirilməsi üzrə cinayətlər, o cümlədən işçilərə və qulluqçulara həm fiziki, həm də

maddi zərər vurulmasına səbəb olan texniki təhlükəsizlik qaydalarının qəsdən pozulması ilə əlaqədar cinayətlər;

– rüşvət alma;

– kompüter cinayətləri (kibercinayətlər).

Yuxarıda qeyd olunan təsnifatlardan göründüyü kimi iqtisadi cinayətlərin bir növü də məhz son dövrlər daha böyük təhlükə hesab olunan kibercinayətlərdir. İqtisadi cinayətkarlığın xüsusi forması kimi kibercinayətkarlığın mahiyyəti, xarakter və xüsusiyyətləri növbəti paraqrafda geniş izah olunacaq.

1.2 Kibercinayətkarlığın mahiyyəti və xarakterik xüsusiyyətləri

Cəmiyyətin kompüterləşməsinin ən ciddi mənfi nəticəsi məhz kibercinayətlər hesab olunur. Kompüter sistemlərinin geniş yayılması, onların kommunikasiya sistemləri vasitəsilə əlaqələndirilməsi, bu sistemlərə elektron müdaxilə imkanını artırır. Bu cür cinayətlərin ənənəvi tipli cinayətlərdən tutmuş yüksək riyazi və texniki hazırlıq tələb edən cinayətlərə qədər çox geniş əhatə dairəsi mövcuddur. Fərdi kompüterlərin sayının sürətli artımı və inkişaf etmiş kommunikasiya sisteminin mövcudluğu hətta həvəskar-cinayətkarların belə kompüter sistemlərinə daxil olmasına imkan yaradır.

Əksər ölkələrdə mövcud olan cinayət qanunvericilikləri bu tip cinayətlərin təsnifləşdirilməsi baxımından kifayət qədər elastik olsalar da, sosial və texniki dəyişikliklər bu hüquq sistemi çərçivəsindən kənarda qalan yeni-yeni problemlər yaradır. Çünki dünya təcrübəsində mövcud olan bəzi kompüter cinayətlərinə cinayət qanunvericiliyi təsir göstərə bilmir. Belə ki, hüquqi baxımdan bu əməllər cinayət hesab edilə bilməz. Burada EHM-in bəzi əməliyyatlarının kriminallaşması problemi nəzərdə tutulur.

"Kibercinayətkarlıq" termini hazırkı dövrdə "kompüter cinayətkarlığı" termini ilə yanaşı işlədilərək, bəzi hallarda hətta sinonim anlayışlar kimi qəbul edilir. Rus

dilli ədəbiyyatda da “kompüter cinayətkarlığı” terminində üstünlük verilir. Bununla yanaşı Azərbaycan Respublikası Cinayət Məcəlləsinin 1999-cu il 30 dekabr tarixli ilk redaktəsində də belə cinayət halları ilə əlaqədar yeganə bölmə də “Kompüter informasiyası sahəsində cinayətlər” adlanırdı. Həqiqətən də, bu terminlər bir-birinə çox yaxındırlar. Lakin onları sinonim ifadələr kimi qəbul etmək düzgün olmaz. Belə ki, “kibercinayətkarlıq” anlayışı (ingilis dilli variantda-cybercrime) “kompüter cinayətkarlığı” (computer crime) anlayışından daha geniş olmaqla informasiya mühitində törədilən cinayətlərin təbiətini daha aydın əks etdirir.

Oksford izahlı lüğətinə görə “cyber” sözü informasiya texnologiyaları, internet şəbəkəsi, eləcə də virtual reallığa aid olan mürəkkəb sözün bir hissəsi kimi izah olunur. Kembric izahlı lüğəti də buna yaxın izah verərək onu “kompüterlərin eləcə də internet şəbəkəsinin istifadəsi ilə əlaqədar” mənasını verən söz kimi təqdim edir. Bu lüğətdə “cybercrime” –kibercinayətkarlıq kimi tərcümə olunaraq, kompüterlərin, eləcə də informasiya texnologiyaları və qlobal şəbəkənin istifadəsi ilə əlaqədar olan cinayətkarlıq kimi izah edilir. Bununla yanaşı “computer crime” termini ancaq kompüter və kompüter məlumatları əleyhinə törədilən cinayətlərə aid edilir.

Yüksək texnologiyalar sferasında cinayətkarlıq haqqında xarici müəlliflərin işlərində də “cybercrime” - kibercinayətkarlıq terminə üstünlük verilir. Bu “kibercinayətkarlıq” terminin kompüter cinayətkarlığı və eləcə də informasiya texnologiyaları sahəsində cinayətkarlıq anlayışlarından daha geniş bir anlama sahib olması ilə izah olunur. Belə ki, amerika tədqiqatçıları Syuzan Brenner və Mark Qudmanın fikrincə kibercinayətkarlıq termini daha üstündür, çünki bu termin özündə kompüter vasitəsilə törədilən ənənəvi cinayətlərlə (oğurluq, dələduzluq, fırıldaqçılıq) yanaşı, cinayət obyekti qismində kompüter sistemləri və məlumatlarının çıxış etdiyi cinayətləri də birləşdirir. Beynəlxalq qanunvericilikdə də kibercinayətkarlıq termini istifadə olunur. Belə ki, 2001-ci ilin noyabr ayında Avropa Şurası tərəfindən qəbul olunmuş konvensiyanın adı da məhz “Kibercinayətkarlıq haqqında” Konvensiyadır.

Beləliklə, kibercinayətkarlıq dedikdə, kibermühitdə törədilən cinayətkarlıq başa düşülməlidir. Kibermühit termini isə ilk dəfə 1984-cü ildə Uilyam Qibson tərəfindən istifadə olunmuşdur. Daha sonra YUNESKO 2000-ci ildən etibarən

kibermühitin hüquqi aspektləri haqqında xüsusi nəşrlər çap etməyə başladı. Paris Universitetinin beynəlxalq hüquq və Avropa hüququ üzrə professoru və YUNESKO-nun informasiya cəmiyyətinin hüquqi aspektləri üzrə mütəxəssisi T. Fuentes-Kamaçonun yanaşmasına görə isə kibermühit özündə daima informasiya ilə təmin edən və onu axtaran bütün ölkələrin əhalisi, mədəniyyəti, dili, yaşı və peşələrini, eləcə də informasiyanın rəqəmsal işlənməsinə və göndərilməsinə xidmət edən və bir-birilə kommunikasiya vasitələri ilə bağlı olan ümumdünya kompüter şəbəkəsini birləşdirir.

T.Fuentes-Kamaçonun fikrincə "kibermühit" termininin sinonimi kimi "infosfera" çıxış edir. Kibermühiti həmçinin "virtual və ya alternativ reallıq", eləcə də "ümumdünya hörümçək toru" və "qlobal informasiya infrastrukturu" da adlandırırlar. K. V. Qryulix kibermühiti bütün dünyanı əhatə edən və hətta onun hüdudlarından kənara çıxa bilən siqnal, dalğa və informasiya elementlərinin məcmusu olan "elektron sfera" və "şəbəkə strukturlu vahid planet" fenomeni kimi izah edir. Bu fenomenin görünən tərəfi özündə elektron sistemlərini: kabel, peyk, kosmik gəmilər, telekommunikasiya qüllələri, kommutasiya mərkəzləri, eləcə də telefon, televizor və kompüterləri birləşdirir. Sadalananlarla sıx bağlı olan görünməyən tərəflər qismində isə proqram təminatının müxtəlif formaları, brauzerlər, elektron cizahlarda naviqasiya alətləri, baza sistemlərində insan biliklərinin saxlanması və "süni intellekt" çıxış edir.[1]

ABŞ Ali Məhkəməsinin şərhinə görə isə kibermühit - coğrafi məkanda yerləşməyən, lakin İnternet vasitəsilə dünyanın istənilən nöqtəsində hər kəs üçün əlçatan olan unikal bir mühitdir. Darrel Mentenin fikrinə görə də əksər hallarda sinonim kimi istifadə olunsalarda "kibermühit" termini həqiqətəndə "İnternet" anlamından daha geniş bir anlayışdır. Onun interpretasiyasında kibermühit bir-birilə qarşılıqlı əlaqədə olan bir neçə kompüterin birləşərək qlobal virtual əməkdaşlığa çevrildiyi konkret məkan kimi təqdim olunur.

[1] Грюлих, К.В. «Киберпространство»: специфическое регламентирование и конкурентные нормы в европейских телекоммуникациях // Право и информатизация общества: сб. науч. тр. – М.: ИНИОН РАН, 2002. – С. 189 – 193.

Rus hüquq elmində kibermühit anlayışı hələ formalaşmamışdır. Hüquq və informasiya texnologiyalarının qarşılıqlı əlaqəsi probleminin tədqiqi ilə məşğul olan mütəxəssislər kibermühit anlayışına məna baxımından oxşar olan digər terminlərdən istifadə edirlər.

Yuxarıda sadalananları nəzərə alaraq, kibercinayətkarlığa belə bir tərif vermək olar: Kibercinayətkarlıq – kompüter sistemi və şəbəkələrinin, həmçinin kibermühitə daxil olmağa imkan verən digər vasitələrin birbaşa və ya dolayı köməyi ilə kompüter sistemləri və şəbəkələri çərçivəsində, eləcə də onların əleyhinə olaraq kibermühitdə törədilən cinayətlərin məcmusudur. Bu şərh BMT mütəxəssislərinin məsləhətlərinə uyğun gəlir. Onların fikrincə "kibercinayətkarlıq" termini kompüter sistemləri və şəbəkələri vasitəsilə və ya kompüter sistemləri və şəbəkələri çərçivəsində, eləcə də onların əleyhinə törədilən istənilən cinayəti əhatə edir.

Beləliklə, kibercinayətlərə elektron mühitdə törədilən istənilən cinayət aid edilə bilər. Kompüter və onunla əlaqədar cinayətləri, məlumatların avtomatik işlənməsi və göndərilməsi ilə əlaqədar olan istənilən qanuna zidd, qeyri-etik davranış kimi müəyyən edən İqtisadi İnkişaf və Əməkdaşlıq Təşkilatı da bu yanaşmanı üstün tutur.

Təəssüflər olsun ki, kibercinayətkarlığın beynəlxalq sənədlərdə öz əksini tapmış rəsmi təyini yoxdur. Lakin bu, 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 məsləhətlər vermişdir. Kompüterlər, eləcə də kompüter şəbəkələri ilə əlaqəli cinayətkarlıq problemi üzrə simpoziumda BMT mütəxəssisləri tərəfindən kibercinayətlərin 2 cür - dar və geniş şərhi verilmişdir.

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

2. Kibercinayətlər geniş mənada (kompüterlərlə əlaqəli cinayətlər kimi): kompüter vasitəsilə və ya kompüterlər, kompüter sistemləri və şəbəkələri ilə əlaqəli olan, eləcə də kompüter 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-kompüterlərin, kompüter proqramlarının, kompüter şəbəkəsinin işinə müdaxilə, kompüter məlumatlarının sanksiyalaşdırılmamış (icazəsiz) modifikasiyası, eləcə də kompüterlərin, kompüter şəbəkə və sistemlərinin birbaşa və ya dolayı istifadəsi vasitəsilə törədilən digər qanunazidd ictimai təhlükəli və qanunla cəzalandırılan əməllərdir.

Kibercinayətkarlıq anlayışının şərh olunmasında mövcud mübahisəli məsələlərdən biri onun "ümumdünya hörümçək toru" çərçivəsində nəzərdən keçirilməsidir. A. Şetilovanın fikrinə görə kibercinayətkarlıq anlayışı yalnız qlobal internet şəbəkəsində törədilən cinayətləri əhatə etmir. O, informasiya, informasiya ehtiyatları və informasiya texnologiyalarının cinayət obyekti qismində çıxış edə biləcəyi informasiya-kommunikasiya sferasında törədilən bütün növ qanuna zidd əməlləri də kibercinayətkarlıq hesab edir.

Yuxarıda qeyd olunan BMT mütəxəssisləri tərəfindən müəyyən olunan şərhləri ümumiləşdirsək kibercinayətkarlıq termini informasiya texnologiyaları sferasında istər kompüterlər vasitəsilə törədilən, istərsə də cinayət obyekti qismində kompüterlərin, kompüter sistemləri və şəbəkələrinin, eləcə də onlarda saxlanılan informasiyanın çıxış etdiyi bütün cinayətlər spektorunu əhatə edir. Kompüter cinayətləri isə yalnız kompüterlərin, kompüter şəbəkələrinin, eləcə də onlar tərəfindən işlənilən məlumatların təhlükəsizliyinə qəsd edən cinayətlərdir. Beləliklə, kompüter cinayətləri kibercinayətlərin tərkibinə daxildir.

Avropa Şurasının "Kibercinayətkarlıq haqqında Konvensiyası"nda kompüter cinayətlərinin 4 növü müəyyən olunmuşdur:

- qanunsuz daxil olma, giriş - maddə 2;
- qanunsuz ələ keçirmə - maddə 3;

- məlumatlara müdaxilə - maddə 4;
- sistemə müdaxilə - maddə 5

Kibercinayətlərin məhz bu 4 növü "kompüter cinayətləri" hesab olunur. Digərləri ya kompüterlə əlaqəli olan (computer-related), ya da kompüter vasitəsilə törədilən (computer-facilitated) cinayətlərdir. Bu cinayətlərə isə aşağıdakılar daxildir:

- kompüterlərin silah qismində çıxış etdiyi cinayətlər (elektron oğurluqlar, dələduzluq və s.);
- törədilməsində kompüterin 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, İnternet vasitəsilə törədilən bir çox cinayətlər yeni növ qanuna zidd əməllər hesab olunmur. Məsələn, oğurluq 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.

Kompüter cinayətləri nəticəsində vurulan zərərin aşağıdakı növləri mövcuddur.[1]

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

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

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

– sistemin istifadəçilər üçün əlçatmazlığı;

– cihazların zədələnməsi (aradan qaldırıla bilən və bilinməyən);

– proqram təminatının pozulması (aradan qaldırıla bilən və bilinməyən).

2. Əhəmiyyətli resursların itməsi. Kompüter cinayətlərinin predmeti əsasən pul, əşya, xidmət, 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. Kompüter texnikasının məhv edilməsi:

– avadanlıqların məhv edilməsi;

– informasiya daşıyıcılarının məhv edilməsi;

– faylların məhv edilməsi (silinməsi);

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

2. Kompüter texnikası obyektlərinin dəyişdirilməsi:

– avadanlıqların zədələnməsi;

– faylların icazəsiz dəyişdirilməsi (modifikasiyası);

– kompüter sistemi informasiyasını icazəsiz müdaxilədən müdafiə edən vasitələrin icazəsiz dəyişdirilməsi;

– kompüter sistemlərinin işinin bloklanması;

– kompüter sisteminə kənar, yad proqram vasitələrinin icazəsiz quraşdırılması;

3. Kompüter texnikası obyektlərinin götürülməsi:

– avadanlıqların oğurlanması;

– hər hansı informasiya daşıyıcılarından informasiyanın oğurlanması;

– faylların sürətinin çıxarılması;

4. Oğurluq:

– maddi qiymətlilərin, pul və xidmətlərin oğurlanması;

– müxtəlif məqsədlər üçün informasiyanın oğurlanması;

5. Sanksiyalaşdırılmamış (icazəsiz) giriş:

– kompüter sisteminə icazəsiz giriş;

– icazəsiz olaraq maşın daşıyıcılarında saxlanan informasiyanın işlənməsi proqramının işə salınması;

Beləliklə, kibercinayətlərə aid edilən hücumların obyektlərini üç qrupa ayırmaq olar:

– kompüterlərin özləri;

– kompüterdən yalnız alət kimi istifadə edilərək hücum oluna bilən obyektlər;

– kompüterin silah 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 təşkilat işçiləri;

– öz vəzifə səlahiyyətlərindən sui-istifadə edən EHM-lərlə iş üzrə təşkilat işçiləri.

Mütəxəssislər kiberhücumlar törədən şəxs və təşkilatları şərti olaraq bir neçə kateqoriyaya ayırır. Bunlar aşağıdakılardır:

1. Xakerlər. Bu kateqoriyaya kompüter texnologiyaları sahəsində yüksək biliyə sahib olan və kompüter sistemlərinin zəif nöqtələrinin tapılması məqsədilə saatlarla kompüterlə məşğul olan şəxslər daxildir. Xakerləri əsasən özünü təsdiq və ya qərəzlilik kimi şəxsi motivlər idarə etsə də, onlar ciddi iqtisadi və sosial ziyan yetirmək üçün kifayət qədər motivə malik olmurlar.

2. Xaktivistlər. “Xaktivizm” termini elmi ədəbiyyata ilk dəfə kompüter cinayətkarlığı üzrə mütəxəssis D.Denninq tərəfindən gətirilib. “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 kompüterləşməsi "kiber-aktivistlərin" 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 edə bilmək üçün kompüter sistemlərinə hücum edirlər. Daha sonra isə bu şəxsi informasiyanın aşkara çıxarılması ilə təhdid edərək pul tələb edirlər. Fərdi kompüter sistemləri ilə yanaşı dövlət orqanlarının kompüter şəbəkələri də kibercinayətkarların hücumlarına məruz qala bilər.

4. Sənaye casusluğu ilə məşğul olan şəxslər. İnkişaf etmiş sənaye dövlətlərində sənaye casusluğu uzun tarixə malikdir və yeni texnologiyaların inkişafı ilə casuslar qarşısında yeni imkanlar açılmışdır. Casusluq dövlətin, təşkilatın eləcə də fərdi "sifarişçilərin" xeyrinə həyata keçirilə bilər.

5. İnsayderlər. "insider" - ingilis dilindən hərfi tərcümədə "daxildən yaxşı məlumatlandırılmış adam" mənasını verir. Kompüter 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 İnternet-

den istifadə etməklə ciddi təhlükə törədə bilərlər. FTB-nin kompüter 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 3 istiqamətdə iş aparılmalıdır.

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

2. kibercinayətlərin törədilməsinə görə cəza tədbirlərinin müəyyən edilməsi. (bu əslində kibercinayətlər haqqında normaların ayrılmaz hissəsi kimi çıxış edir)

3.İnformasiyanın qorunması məqsədilə kompleks tədbirlərin həyata keçirilməsi. Sadalanan bu istiqamətlər ictimai təhlükə hesab olunan kibercinayətlərinin qarışısının alınmasına yönəldilir.

Ən geniş yayılmış təsnifat daha öncə də qeyd edildiyi kimi kibercinayətlərin "kompüter cinayətlərinə" və "kompüter vasitəsilə törədilən cinayətlərə" bölgüsüdür. BMT mütəxəssisləri tərəfindən verilən bu təsnifat kibercinayətkarlığın "dar" və "geniş" şərhinə əsaslanır. Bu təsnifata uyğun olaraq kibercinayətlərin həm də "bir obyektli" və "çox obyektli" növlərə də bölgüsü mövcuddur. Kompüter cinayətləri, əsas obyektinin kompüter sistemi və verilənlərinin tamlığına, məxfiliyinə və təhlükəsiz fəaliyyətinə qəsddən ibarət olduğu cinayətlərdir. Digər kibercinayətlər əsasən digər obyektlərə qəsdlə bağlıdır ki, bu obyektlər qismində insanların və bütövlükdə cəmiyyətin təhlükəsizliyi (kiberterrorizm), mülkiyyət və mülkiyyət hüquqları (kompüter vasitəsilə və ya kibermühitdə törədilən oğurluq, dələduzluq), müəlliflik hüquqları (plagiat və piratçılıq) çıxış edir. Avropa Şurasının "Kibercinayətkarlıq haqqında" Konvensiyasında kibercinayətlər 5 qrupa bölünmüşdür. Bunlar aşağıdakılardır:

1. Kompüter sistemi və verilənlərinin tamlığı, məxfiliyi və istifadə imkanları əleyhinə törədilən cinayətləri: Bu qrup özündə aşağıdakı cinayət növlərini birləşdirir:

- qanunsuz daxil olma, giriş - kompüter və ya onun hər hansı bir hissəsinə qərəzli, qanuna zidd giriş (maddə 2);

- qanunsuz ələ keçirmə - ictimai mübadilə üçün nəzərdə tutulmayan kompüter verilənlərinin qərəzli və qanuna zidd ələ keçirilməsi (maddə 3);

- məlumatlara müdaxilə - kompüter verilənlərinin, məlumatların qərəzli və qanuna zidd olaraq törədilən zədələnməsi, silinməsi, pozulması (maddə 4);

- sistemə müdaxilə - kompüter sisteminin fəaliyyətinə mane olan qərəzli və qanunazidd əməl (maddə 5).

2. kompüter vasitələrinin istifadəsi ilə bağlı cinayətlər;

3. məlumatların məzmunu və tərkibi ilə əlaqəli cinayətlər;

4. müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər;

5. məsuliyyətin əlavə növləri və sanksiyaları.

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 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 təhlükəsinə birbaşa təhlükə hesab olunmayan cinayətlərin təsnifatı kimi xarakterizə etmək olar. Bu təsnifat cinayət obyekti qismində kompüterlər və onların fəaliyyəti, kompüter sistemləri və verilənləri, eləcə də mülkiyyət və müəlliflik hüquqlarının çıxış etdiyi cinayətlər baxımından daha uyğun hesab olunur.

Verilən təsnifatda kompüter cinayətlərini xarakterizə edən bütün kodlar Q hərfi ilə başlayan eyniləşdiriciyə malikdirlər. Bunlar özləri də qəsdin növündən asılı olaraq 6 qrupa bölünür (bunlar da hərflərlə işarə olunur məs: kompüter dələduzluğunun daxil olduğu qrup-QF ilə işarələnir (F-fraud). Növbəti təsnifat isə cinayətin törədilmə üsulundan asılı olaraq aparılır. Hər bir təsnifatda ardıcıllıq cinayətin ictimai təhlükəsinin azalması istiqamətində gedir.

Təsnifat aşağıdakı şəkildə təqdim olunur:

- QA – İcazəsiz (sanksiyalaşdırılmamış) giriş və ələ keçirmə
- QAH – kompüter abordajı
- QAİ - ələ keçirmə
- QAT – vaxtın oğurlanması
- QAZ – icazəsiz giriş və ələ keçirmənin digər növləri
- QD – kompüter verilənlərinin dəyişdirilməsi
- QDL – məntiqi bomba
- QDT – troya atı
- QDV – kompüter virusu
- QDW – kompüter soxulcanı
- QDZ – verilənlərin dəyişdirilməsinin digər növləri
- QF – kompüter dələduzluğu
- QFC – ATM-lərlə dələduzluq
- QFF – kompüter saxtalaşdırması
- QFG – oyun avtomatları ilə dələduzluq
- QFM – giriş-çıxış proqramları ilə manipulyasiyalar
- QFP – ödəmə vasitələri ilə dələduzluq
- QFT – telefon dələduzluğu
- QFZ –kompüter dələduzluğunun digər növləri
- QR – qanunsuz olaraq sürətin çıxarılması
- QRG – kompüter oyunları
- QRS – digər proqram təminatları

- QRT – yarımkeçirici məmulatların topoqrafiyası
- QRZ – digər növ qanunsuz sürət çıxarmalar
- QS – kompüter sabotajı
- QSH – avadanlıq təminatı ilə
- QSS – proqram təminatı ilə
- QSZ – sabotajın digər növləri
- QZ – digər kompüter cinayətləri
- QZB – kompüter elan lövhələrinin istifadəsi ilə həyata keçirilən cinayətlər
- QZE – kommersiya sirri hesab olunan məlumatların oğurlanması
- QZS – məxfi xarakterliinformasiyanın göndərilməsi
- QZZ – kompüter cinayətlərinin digər növləri

Amerika tədqiqatçısı D.L. Şinder "kiber" adlandırıla bilən və daha çox cinayətləri əhatə edən başqa bir təsnifat aparmışdır. Bütün digər xarici mütəxəssislərin təsnifatları içərisində D.L. Şinderin təsnifatı daha geniş və daha dəqiqdir. Belə ki, digər tədqiqatçılar əsasən «computer crimes», «computer-related crimes» və «computer-facilitated crimes» təsnifatı ilə kifayətlənirlər.

D.L.Şinderin tədqiqatında aşağıdakı təsnifat verilmişdir:

1. insanların fiziki təhlükəsizliyinə, həyatı və sağlamlığına qəsd edən zorakı və digər potensial təhlükə daşıyan kibercinayətlər;

2. məxfi informasiyaya qəsd edən cinayətlər - informasiyaya heç bir zərər törətmədən kompüter və kompüter sistemlərinə qanunsuz olaraq daxil olma;

3. dağıdıcı-destruktiv kibercinayətlər – bu cinayətlərin mahiyyəti kompüter verilənlərinin zədələnməsindən, eləcə də kompüter sistemlərinin tamlığına və təhlükəsiz fəaliyyətinə qəsd etmələrdən ibarətdir;

4. mülkiyyət, mülkiyyət hüquqları, eləcə də informasiya və müəlliflik hüquqlarına mülkiyyətçilik hüququna qəsd edən cinayətlər. D. Denninq bu cinayətləri şərti olaraq "oğurluq" adlandırdığı cinayətlər qrupuna daxil etmişdir.[1] Bu adın şərti olaraq verilməsi isə oğurluq halının ənənəvi qaydada törədilməməsindən, yəni

[1]Деннинг Д. Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику» URL:http://crime.vl.ru/docs/stats/stat_92.htm

oğurlanmış informasiyanın faktiki olaraq müəllifdə qalmasından və onun bu informasiyadan istifadə imkanının itməməsindən irəli gəlir.

5. ictimai dəyərlərə qəsd edən cinayətlər;

6. ictimai təhlükəsizliyə qəsd edən cinayətlər;

7. "computer-facilitated" adlandırılan digər kibercinayətlər – kompüter şəbəkəsi vasitəsilə törədilən və qanunla qorunan müxtəlif obyektlərə qəsd edən cinayətlər.

Beləliklə, aydın olur ki, kibercinayətlərin əhatə dairəsi çox genişdir. Bu isə kompüterlərin artıq həyatın bütün sferalarına daxil olmasından irəli gəlir. Kibercinayətkarlığın miqyası və onun hansı ictimai təhlükələr yaratması növbəti paraqrafda daha geniş şərh olunacaq.

1.3 İctimai təhlükəliliyi nöqteyi nəzərindən kibercinayətkarlığa qarşı mübarizənin zəruriliyi

Kibercinayətkarlığın vəziyyəti, dinamikası, miqyasından öncə kibercinayətkarlığın tədqiqi problemini təhlil etmək lazımdır. Belə ki, bu məsələnin öyrənilməsi müəyyən çətinliklər törədir. Bu çətinliklər kibercinayətkarlığın daha sonrakı tədqiqi üçün məlumatların alınmasından irəli gəlir. Cinayətkarlığın digər növlərinin tədqiqi üçün keçərli olan metodları kibercinayətkarlığın təhlili zamanı tətbiq etmək mümkün olmur.

Kibercinayətkarlıq təbiətinə görə transmilli bir haldır. Bu səbəbdən də kibercinayətkarlıq və onun növlərindən olan kompüter cinayətlərin bir ölkə və ya ölkələr qrupu çərçivəsində təhlil etmək əhəmiyyətli olsa da bu halın həqiqi miqyası haqqında təsəvvür yaratmağa imkan vermir. Kompüter və telekommunikasiya şəbəkələrinin transmilliliyi və qloballığı cinayətkarın bir qitədə, cinayət halının isə başqa bir qitədə törədilməsinə səbəb olur. Təəssüflər olsun ki, hazırki dövrdə heç bir kompleks xarakterli kriminoloji təhlil kibercinayətkarlığın qlobal miqyası haqqında tam təsəvvür yaratmaq iqtidarında deyildir. Bu heç də yalnız kibercinayətkarlıqla

mübarizə üzrə milli qanunvericiliklər və onun tətbiqi təcrübəsindəki fərqliliklərdən deyil, həmçinin burada cinayət statistikasının formalaşdırılması və müdafiə sisteminin xüsusiyyətlərində fərqlərin mövcud olmasından asılıdır.

Cinayətkarlığın kriminoloji təhlili ilk növbədə illər ərzində formalaşmış statistik göstəricilərin təhlilindən başlayır. A.İ.Dolqovanın fikrinə görə hal-hazırda kibercinayətkarlığın vəziyyəti və strukturu haqqında tam və dolğun məlumat verə bilən rəsmi statistika mövcud deyildir. Ən yaxşı halda bu halın baş vermə dinamikası və bu dinamikaya təsir edən səbəblərin təhlili aparıla bilər.[1] Kibercinayətkarlıq hallarının əksər hissəsi statistika çərçivəsindən kənarda qalır. Tam əminliklə demək olar ki, rəsmi statistikada ən yaxşı halda bu halların 20%-i öz əksini tapır.

ABŞ-ın FTB-nin Milli Şöbəsinin kompüter cinayətləri üzrə məlumatına görə elektron qəsdlərdən 85%-dən 97%-ə qədəri aşkara çıxarılmamış qalır. Digər mütəxəssislər isə hesab edirlər ki, kibercinayətkarlıq hallarının gizliliyi RF-də - 90%, ABŞ-da - 80%, Böyük Britaniyada – 85%, Almaniyada – 75%-ə qədər təşkil edir. Bununla yanaşı mütəxəssislərin iddialarına görə yoxlanışlar elektron oğurluqların yalnız 10%-ni aşkara çıxarmaq iqtidarındadır.

Mütəxəssislər gizlilik dərəcəsindən asılı olaraq kibercinayətlərin 4 növünü fərqləndirirlər:

1. Birinci qrupa baş vermə faktı haqqında nə hüquq mühafizə orqanlarının, nə də zərər çəkmişlərin heç bir məlumatının olmadığı cinayətlərin məcmusu daxildir. Cinayət halının baş verməsindən yalnız bu informasiyanın yayılmasında heç bir marağı olmayan günahkar şəxslər və onların əlbir olduqları şəxslər məlumatlı olurlar. Bu təbii gizlilikdir. Kibercinayətkarlığın tədqiqi ilə məşğul olan xarici mütəxəssislər kibercinayətkarlığın təbii gizliliyi problemini "aşkara çıxarma problemi" adlandırırlar. Məlumatlara görə törədilmiş kibercinayətlərin yalnız 1/10 hissəsi aşkara çıxarılır.

2. Gizli kibercinayətlərin ikinci növü xarici mütəxəssislər tərəfindən "məlumat verilməməsi problemi" kimi adlandırılan süni gizlilikdir. Bunun mahiyyəti cinayət

[1] Долгова, А.И. Преступность, ее организованность и криминальное общество. / А.И. Долгова. - М.: Рос.криминол. ассоц, 2003. – 575 с.

halının baş verməsi barədə hüquq mühafizə orqanlarına məlumat verilməməsindən ibarətdir. Bu hal zərər çəkmişlərin cinayət halının baş verməsi haqqında məlumatın hansı orqanlara verilməsi haqqında məlumatsız olmasından, bəzən isə bir çox müəssisə və təşkilatların yaranmış problemi öz gücləri hesabına həll eləməsindən irəli gəlir. Müəssisələrin belə həll yolu seçməsinin səbəbi tədqiqatın aparılması nəticəsində baş verən itkilərin cinayət nəticəsində dəymiş zərərdən çox olması halıdır.

3. Gizli kibercinayətlərin üçüncü növünü mütəxəssislər bəzən "sərhəd situasiyaları" adlandırırlar. Belə ki, bu qrupa törədilmiş cinayət faktı haqqında hüquq mühafizə orqanlarına məlumat verilsə də, işi tədqiq edən işçinin tam peşəkar hazırlığının olmaması nəticəsində ona düzgün hüquqi qiymət verməməsi və törədilmiş əməldə cinayət tərkibi əlamətlərini aşkar edə bilməməsi nəticəsində statistik uçotdan kənarda qalan cinayətlər daxildir. Bu hal əsasən kibercinayətkarlıqla mübarizə üzrə hüquq mühafizə orqanlarının maddi və maliyyə vəsaiti ilə zəif təmin olunduğu ölkələrdə rast gəlinir.

4. Dördüncü növ gizli kibercinayətlər baş vermə halı barəsində hüquq mühafizə orqanlarının məlumatının olduğu, lakin müxtəlif təsəvvürlərdən irəli gələrək qeydiyyatı aparılmayan cinayətlər (gizlədilən və ya üstü örtülən cinayətlər) hesab olunur. Bu hal ölkədə və ya şəhərdə əmin-amanlıq görüntüsü yaratmaq məqsədilə statistikanın manipulyasiya edilməsi səbəbindən irəli gəlir. Bununla yanaşı hüquq mühafizə orqanları tərəfindən kibercinayətin törədilməsi faktının gizlədilməsi səbəbi kimi şəxsi maraqlar və qərəzli meyllər çıxış edə bilər.

Kibercinayətkarlığın gizliliyinin yuxarıda sadalanan amilləri ilə yanaşı mütəxəssislər həmçinin informasiya amilini və bununla əlaqədar olan və informasiyanın texniki mühafizəsi, eləcə də hüquq mühafizə orqanları işçilərinin lazımı biliklərə sahib olmamasından irəli gələn qeyri-müəyyənlik halının mövcudluğu fikrini də irəli sürürlər. Beləliklə, digər cinayət növlərindən fərqli olaraq kibercinayətkarlığa yüksək gizlilik əlaməti xarakterikdir. Bu səbəbdən də kriminoloji təhlilin ilkin mərhələsi yəni rəsmi statistik məlumatların qiymətləndirilməsi kibercinayətkarlığın miqyası barəsində real təsəvvür yaratmağa imkan vermir. A.İ.Dolqovanın fikrinə görə cinayət və məhkəmə statistikası bu cinayətkarlıq halında

baş verən dəyişiklikləri yalnız bir neçə ildən sonra təsvir edə bilər.[1] Belə ki, artıq hüquq mühafizə orqanları yeni kriminoloji hala effektiv reaksiya verməyə başlamışlar. Lakin bununla belə kibercinayətkarlıq nisbətən yeni yaranmış hal olduğundan bu məsələnin tam statistik şərhinin formalaşması uzun zaman tələb edir.

Daha əvvəldə də qeyd olunduğu kimi kibercinayətkarlığın qlobal tendensiyasını təhlil və tədqiq etməyə imkan verən tam, dolğun statistika yoxdur. Yüksək texnologiyalar sferasında cinayətkarlıqla mübarizə problemi ilə uzun müddətdir məşğul olmasına baxmayaraq Avropa Şurası səviyyəsində də uyğun statistika mövcud deyildir. Lakin bununla belə kibercinayətlər haqqında müxtəlif ölkə vətəndaşlarından məlumat almaqla "qlobal" statistika aparan bəzi təşkilatlar fəaliyyət göstərir. Bu statistika kibercinayətkarlıqdan zərər çəkmişlərin məlumatları əsasında formalaşdırılır. Bir tərəfdən bu metodun tətbiqinin üstün cəhətləri mövcuddur ki, bu da rəsmi statistikaya nisbətən zərər çəkmişlərin məlumatı əsasında kibercinayətkarlığın vəziyyətinin daha real şəklinin formalaşmasından irəli gəlir. Xüsusilə, kibercinayətkarlığın yüksək gizlilik səviyyəsini, zərər çəkmişlərin bu hal barəsində hüquq mühafizə orqanlarına məlumat vermək istəməməsini və eləcə də bəzi ölkələrin rəsmi statistikalarında yalnız bir qisim cinayətlərin kibercinayət kimi qeydə alınmasını (digər cinayət əməlləri cinayətkarlığın başqa növləri adı altında – oğurluq, dələduzluq və s. statistikada öz əksini tapır.) nəzərə alsaq bu üsulun üstünlüyü bir daha öz təsdiqini tapacaq.

İnternet şəbəkəsində dələduzluq halları üzrə statistikanı National Fraud Information Center (Dələduzluq üzrə Milli İnformasiya Mərkəzi) və FTB-nin "ağyaxalıqlıların" cinayətkarlığını tədqiq edən Mərkəzinin nəzdində fəaliyyət göstərən İnternet Crime Complaint Center (IC3) adlı iki amerika təşkilatı toplayır.

İC3-ün məlumatına görə 2014-cü il ərzində Mərkəzə İnternet cinayətlər barəsində 300.000-dən çox şikayət daxil olmuşdur ki, bu da daha öncəki ilə nəzərən 3,4% daha çoxdur. Bu şikayətlərdən yalnız 36,9%-də maliyyə itkisi barəsində məlumat verilmişdir ki, bu da bütövlükdə 485,3 mln dollara bərabər olmuşdur.

---

[1]Долгова, А.И. Преступность, ее организованность и криминальное общество. / А.И. Долгова. - М.: Рос.криминол. ассоц, 2003. – 575 с.

2014-cü ilin məlumatlarına görə şikayətlərin böyük hissəsi ABŞ-dan (90,99%) daxil olmuşdur. Bununla belə Kanada (1,44%), Böyük Britaniya (0,97%), Avstraliya (0,66%), Hindistan (0,50%) və CAR-dan da (0,22%) çoxsaylı şikayətlər də daxil olmuşdur. Şikayətlərin çox hissəsini İnternet auksionlardakı dələduzluq halları təşkil edir (62,7 %). Şikayətlərin 15,7 %-ni sifariş olunmuş əmtəələrin ünvana çatdırılmaması və ya ödəmənin həyata keçirilməsi ilə bağlı cinayətlər, 6,8%-ni kredit və debit kartları ilə dələduzluq halları təşkil edir.

Zərərçəkmişlərin yaşına gəldikdə isə buraya əsasən 30-50 yaşlı kişi və qadınlar daxildir (61,2 %). Dələduz ilə zərərçəkmişin ilk əlaqəsi isə əsasən elektron poçt (73,9 %) və müxtəlif saytlar (36 %) vasitəsilə baş verir. National Fraud İnformation Center-in verdiyi məlumata görə də daxil olmuş şikayətlərin əksər hissəsi online auksionlarla əlaqəli cinayətlər (42%) və online şəkildə alınmış əmtəələrin çatdırılmaması (30%) (İnternet-dükandan alınmış əmtəə alıcıya çatdırılmır) ilə bağlı cinayətlər barəsindədir.

Daha bir statistik məcmuə Antivirus proqram təminatının istehsalçısı olan Symantec təşkilatının mütəxəssisləri tərəfindən hər yarım ildən bir çap olunan Internet Security Threat Report-dur. Aşağıda verilənbu məcmuə qlobal səviyyədə həyata keçirilən demək olar ki, yeganə məcmuə hesab olunur. Bu icmalda kompüter hücumlarının baş vermə tendensiyası və eləcə də virusların yaradılması və yayılması tendensiyası təhlil edilir. Bu haqda daha cədvəl 1.1-in materiallarından daha aydın təsəvvür yaranır.

Cədvəl 1.1

Avropa, Orta Asiya və Afrika regionu ölkələri
üzrə top hücumlar

Ölkələr	Sıra	Regiona nisbətən %-lə (2014)	Regiona nisbətən %-lə (2013)	Dəyişiklik %-lə
ABŞ	1	35.6%	36%	-0.4%
Çin	2	16.1%	9%	7.1%
Böyük Britaniya	3	7.5%	11%	-3.5%
Yaponiya	4	4.3%	-	-
Rusiya	5	3.6%	3%	0.6%
Almaniya	6	3.1%	3%	0.1%
İsveç	7	2.6%	5%	-2.4%

İsveçrə	8	1.9%	-	-
İtaliya	9	1.9%	-	-
İspaniya	10	1.5%	-	-

2014-cü ili əhatə edən icmalda ərazisində daha çox kompüter sistemləri və şəbəkələrinə hücumların törədildiyi ölkələrin siyahısı verilmişdir. Bu siyahıya ABŞ 35,6%-lə liderlik edir. ABŞ 2009 və 2010-cu illərdə də buna yaxın faizlə ərazisində ən çox kiberhücumların törədildiyi ölkə olmuşdur. Çində bu hücumların sayı 7,1% artmaqla ümumi hücumların 16,1%-i bu ərazidə törədilmişdir. Daha sonrakı yerlərdə isə Böyük Britaniya (7,5%), Yaponiya (4,3%), Rusiya (3,6%), Almaniya (3,1%), İsveç (2,6%), İsveçrə və İspaniya (hər biri 1,9%), İtaliya (1,5%) gəlir. Əgər 2003-cü ilə qədər ərazisindən daha çox kiberhücumların həyata keçirildiyi ölkələrin yarısı Asiya-Sakit okean regionuna daxil olan ölkələr idisə, son illər siyahıya bu regiondan cəmi 2 ölkə daxil olmuşdur. Lakin yuxarıda verilmiş məlumatlar heç də o demək deyil ki, xakerlərin çox hissəsi məhz bu 10 ölkənin ərazisində yaşayır. Belə ki, burada vasitəsilə cinayət törədilən kompüterin özü belə həmin hücumun predmeti ola bilər. Bu digər ölkə vətəndaşlarının kibercinayət törətmək məqsədilə həmin kompüter sistemlərinə qanunsuz daxil olmaları vasitəsilə törədilə bilir. Symantec şirkətinin mütəxəssisləri əsas diqqəti məhz bu məsələyə yönəltməyi məsləhət görürlər.

2014-cü il üçün Internet Security Threat Report-da qeyd olunur ki, 2014-cü il ərzində Symantec tərəfindən 5,5 mln-dan çox zərərli hücum qeydə alınmışdır ki, bu da 2010-cu ildəkindən 81% çoxdur. Gün ərzində 4500-dən çox "Web hücumlar" törədilmişdir ki, bu da keçən ilə nəzərən 36% artım deməkdir. Zərərverici proqramlara gəldikdə isə 2011-ci il ərzində 2010-cu ildəkindən 41% çox, yəni 403 mln belə proqram yaradılmışdır.[1]

Norton antivirus proqram təminatının istehsalçısı olan bu şirkətin "Norton 2011-ci il Kibercinayətkarlıq haqqında hesabat"-ında isə qeyd olunur ki, 2011-ci il ərzində 431 mln insan kibercinayətkarlığın qurbanı olmuş və bu cinayətlər 114 mlrd dollar zərər vurmuşdur. Belə ki, ABŞ-da qurbanların sayı 74 mln-dan artıq olmuşdur ki, onların birbaşa maliyyə itkisi 32 mlrd dollar təşkil etmişdir. Bu

[1]Internet Security Threat Report. URL: http://www.symantec.com/threatreport

kibercinayətkarlığın dəyəri Çində 25 mlrd dollar, Braziliyada 15 mlrd dollar, Hindistanda isə 4 mlrd dollar olmuşdur. Bununla yanaşı Symantec daha bir təhlükəli tendensiya olan mobil telefonlar üçün virusların yaradılmasına xüsusi diqqət yetirir. Lakin Symantec viruslarla əlaqədar vəziyyəti tədqiq edən yeganə proqram təminatı istehsal edən şirkət deyildir. Demək olar ki, virus əleyhinə proqram təminatı istehsalı ilə məşğul olan bütün iri şirkətlər zərərli proqramlar və onların törətdiyi nəticələrin tədqiqi ilə məşğul olurlar.

Ponemon İnstitutu tərəfindən HP üçün hazırlanan "Kibercinayətlərin İllik Maliyyə Zərərləri" hesabatında qeyd edilir ki, kompüter istifadəçilərinin virus proqramları haqqında məlumatları hər il daha da artsa da cinayətlərin sayı və zərərləri də əvvəlki illərlə müqayisədə artmaqdadır. Hesabata görə kibercinayətlərin illik orta hesabla vurduğu zərər 8,9 milyon dollardır. Bu cinayətlər nəticəsində itkilər və nəticələrin aradan qaldırılması üçün xərclənən vəsaitlərin həcmi isə illik olaraq 1,5 – 36,5 milyon dollar aralığında dəyişir. Kibercinayətkarlığın bu il üzrə göstəriciləri isə ötən ilkindən 56% çoxdur. Bu cinayətlərin qarşısı vaxtında alınmadıqda onun maliyyə zərərləri də xeyli artır. Belə ki, hesabata görə hücumların nəticələrinin aradan qaldırılması orta hesabla 24 gün çəkir və xərcləri 591,780 dollara bərabər olur. Ötən il isə 18 günlük bərpa xərcləri 415,748 dollar dəyərində idi. Əgər hücumlar şirkət daxilindən edilibsə o zaman onun nəticələrinin aradan qaldırılması orta hesabla 50 gün çəkir ki, 2011-ci ildə bu rəqəm 45 günə bərabər idi.[1]

Verilən bu statistik məlumatlar kibercinayətlərin sayının hər gün artdığını bir daha sübut edir. Təəssüflər olsun ki, demək olar ki, bütün tədqiqatçılar və mütəxəssislər kibercinayətkarlıqla əlaqədar vəziyyətin pisləşmə tendensiyasının mövcudluğunu etiraf edirlər. Daha bir təhlükəli tendensiya isə kibercinayətkarlıqla mütəşəkkil cinayətkarlığın bir-birinə daha da yaxınlaşması halıdır. Bütün bu deyilənlərdən bir daha aydın olur ki, müasir dünya üçün kibercinayətkarlıq çox ciddi bir problemdir. Ona qarşı dünyanın daha təsirli mübarizə üsullarına ehtiyacı var. Çünki dövlətlərin, iqtisadiyyatların və ayrı-ayrı şəxslərin fəaliyyətdə olan kiberməkandan asılılığı səbəbindən gələcəkdə baş verə biləcək fəlakət, bədbəxt

[1]201 3rdAnnual Cost of Cyber Crime StudyResultsURL:https://www.brighttalk.com/webcast/7477/57491

hadisə və ya cinayət nəticəsində kiberməkanda yarana biləcək genişmiqyaslı qəzalar əhalinin böyük bir qisminə dağıdıcı təsir göstərə bilər.

FƏSİL II. AZƏRBAYCANDA İQTİSADİ CİNAYƏTKARLIĞA QARŞI MÜBARİZƏNİN MÜASİR VƏZİYYƏTİ VƏ KİBERCİNAYƏTKARLIĞA QARŞI MÜBARİZƏNİN HÜQUQİ TƏMİNATI MEXANİZMİ

2.1 Azərbaycan Respublikasının qanunvericilik sistemində iqtisadi cinayətkarlıq formalarının hüquqi təsbiti

İqtisadi cinayətkarlığa qarşı mübarizənin mühüm həlqələrindən biri qanunvericilikdə iqtisadi cinayət hesab oluna biləcək cinayət formalarının hüquqi təsbiti məsələsidir. Azərbaycan Respublikasının qanunvericilik sistemində iqtisadi cinayətkarlıq formaları "iqtisadi fəaliyyət sahəsində olan cinayətlər" kimi nəzərdən keçirilir. İqtisadi fəaliyyət sahəsində olan cinayətlərə belə bir ümumi anlayış vermək olar: "İqtisadi fəaliyyət sahəsində olan cinayət dedikdə, iqtisadi sahədə qəsdən törədilən, öz qulluq mövqeyindən və ya hər kəsin öz bacarığından və əmlakından sahibkarlıq fəaliyyətindən və ya başqa iqtisadi fəaliyyətdən azad istifadə etmək hüququndan suiistifadənin bu və ya başqa formasında (qeydiyyatdan keçmədən sahibkarlıq fəaliyyəti ilə məşğul olma, yalançı sahibkarlıq, qanunsuz əldə edilmiş və ya saxlanmış əmlakdan, bazardakı inhisarçı mövqeyindən, məcburetmədən, özgənin əmtəə nişanından, yalan və ya qanunsuz yolla əldə edilmiş məlumatdan istifadə etmə və s.), yaxud da qanundan, ayrı-ayrı fəaliyyət növləri ilə məşğul olmadan və ya bağlanmış əqdlərdən irəli gələn müxtəlif öhdəliklərin icrasından yayınmada ifadə olunan, şəxsiyyətə, cəmiyyətə və ya dövlətə ziyan vuran və ya ziyan vurmaq təhlükəsi yaradan əməllər başa düşülür". Bu cinayətkarlıq formalarının qanunvericilikdə hüquqi təsbiti aşağıdakı təkmilləşmə yolunu keçmişdir.

Sovet cinayət qanunvericiliyi öz mövcudluğunun ilk illərindən iri müəsissələrin milliləşdirilməsi və xüsusi sahibkarlıq fəaliyyətinin mümkün olduğu sahələrin daraldılması yolu ilə getmişdir. Hələ Azərbaycan Respublikasının Cinayət Məcəlləsi (CM) qəbul edilənədək işə götürmə zamanı vasitəçilik funksiyaları, poçt göndərişlərinin

poçt idarələri ilə yanaşı daşınması, tünd spirtli içkilərinin hazırlanması və satışı, xaricdən malların alınması və s. cinayət hesab edilmişdi. Bütün bu qadağalar CM-də də öz əksini tapmışdır. Əvvəllər məlum olan əmlak qəsdlərindən isə sələmçiliyə görə, satılan malların saxtalaşdırılmasına görə, özgənin əmtəə, fabrik və ya əmtəə nişanından, özgə firma şəklindən, modelindən və ya özgənin adından istifadəyə görə məsuliyyət saxlanılmışdı. İdarəçilik qaydaları əleyhinə cinayətlərə müxtəlif növ dələduzluq, vergilərdən yayınma, habelə saxta pul və qiymətli kağızlar hazırlama daxil edilmişdi. Bununla yanaşı CM-nə "Təsərrüfat cinayətləri" fəsli daxil edilmişdir ki, həmin fəsildə əvvəllər praktiki olaraq məlum olmayan - əmək fərariliyi; əmək mükəlləfiyyəti qaydasında təqdim edilmiş işçi qüvvəsindən dövlət müəsissəsinin vəzifəli şəxsi tərəfindən təsərrüfatsızcasına istifadə etmə və s. kimi cinayətlər də nəzərdə tutulmuşdu.

Respublikanın 1927-ci il CM-də idarəçilik qaydaları əleyhinə olan cinayətlərin siyahısı müəyyən olunmuş və bu siyahıya qaydaları pozmaqla yerin təkinin işlənməsi, aksiz qaydalarına riayət etməmə kimi tərkiblər daxil edilmiş, habelə əvvəllər təsər-rüfat cinayəti hesab edilən bir sıra əməllərlə (ticarət qaydalarını pozma, spirti və spitli maddələri satış məqsədilə hazırlama və satma və s.) tamamlanmışdır.

Dövlət fərdi sahibkarlığı qadağan edərək, maddi nemətlərin, xüsusən də siyahısı getdikcə artmaqda olan yüksək tələbatlı malların və məhsulların ümumi bölgüsü və yenidən bölgüsü prinsipini də cinayət-hüquqi mühafizədən kənarda qoya bilməzdi. Bunun nəticəsində CM-nə dəfələrlə ticarət sahəsində pozuntulara görə məsuliyyət haqqında maddələr əlavə edilmiş, alqı-satqıya görə məsuliyyət ciddiləşdirilmişdir. Ölkəmizin 1999-cu il 30 dekabr tarixli yeni CM əvvəlki məcəllədə məlum olan təsərrüfat cinayətlərindən yalnız bir neçəsini saxlayaraq, bir sıra yeni tərkiblər nəzərdə tutmuşdur ki, onların da əksəriyyəti bu və ya başqa variantda XX əsrin əvvəllərində qüvvədə olmuş qanunvericiliyə məlum idi. Buna baxmayaraq yeni CM-nin "İqtisadi fəaliyyət sahəsində olan cinayətlər" adlanan fəslinə ekoloji xarakterli qəsdlər daxil edilməmişdir, çünki belə qəsdlərə "İctimai təhlükəsizlik və ictimai qayda əleyhinə olan cinayətlər" bölməsində müstəqil fəsil ayrılmışdır.

Hər kəsin sahibkarlıq və başqa iqtisadi fəaliyyətlə məşğul olmaq üçün öz bacarığından və əmlakından azad istifadə hüququnu təsbit edən Azərbaycan Respublikasının 1995-ci il Konstitusiyasının qəbul edilməsi bu hüququn cinayət-hüquqi mühafizənin müstəqil obyekti hesab edilməsini zəruri etmişdir. Azad sahibkarlığın vəzifə cinayətlərinə görə məsuliyyət haqqında ümumi normalar çərçivəsində cinayət-hüquqi müdafiəsini nəzərdə tutan çar Rusiyasının qanunvericiliyindən və belə müdafiəni, ümumiyyətlə, istisna edən sovet cinayət qanunvericiliyindən fərqli olaraq, Azərbaycan Respublikasının yeni CM ilk dəfə olaraq "qanuni sahibkarlıq fəaliyyətinə mane olma" adlı xüsusi cinayət tərkibi müəyyən etmişdir.

Sahibkarlıq və qanunla yol verilən başqa iqtisadi fəaliyyətlə məşğul olmaq üçün öz bacarığından və əmlakından istifadə etmək hüququnun cinayət-hüquqi müdafiəsi müəyyən növ vəzifələrin olmasını nəinki istisna etmir, hətta onların icra edilməməsinə görə məsuliyyət nəzərdə tutur. Bu baxımdan Azərbaycan Respublikasının yeni CM-nin həmin hüquqdan sui-istifadənin müxtəlif formalarına görə cinayət məsuliyyəti nəzərdə tutması tamamilə aydındır. Əgər bu mövqedən iqtisadi fəaliyyət sahəsində olan cinayətlərin başqa növlərinə yanaşılsa, onda bu cinayətlər arasında ilk növbədə həmin konstitusion hüquqdan müvafiq qaydada qeydiyyatdan keçmədən və ya xüsusi razılıq (lisenziya) almadan, habelə qadağan edilmiş fəaliyyəti gizlədərək istifadə etmə yolu ilə törədilən əməlləri göstərmək lazımdır. Azərbaycan Respublikası CM-nin "qanunsuz sahibkarlıq", "yalançı sahibkarlıq" əməllərinin əlamətlərini əks etdirən maddələrində məhz bu nəzərdə tutulur. Bir prinsipial faktı qeyd etmək lazımdır ki, sui-istifadənin belə forması yalnız o halda cinayət məsuliyyətinə cəlb etmə üçün əsas ola bilər ki, bu əməllərin nəticəsində vətəndaşlara, təşkilatlara və ya dövlətə xeyli miqdarda ziyan vurulsun.

Qanunsuz əldə edilmiş əmlakdan və ya əmlaka olan hüquqdan istifadə etmə, yəni bilə-bilə cinayət yolu ilə əldə edilmiş əmlakı alma və ya satma, qanunsuz kredit alma və ya kreditdən təyinatı üzrə istifadə etməmə, kreditor borclarını ödəməkdən qəsdən yayınma tərkiblərini yaradan əməlləri törətmə iqtisadi fəaliyyət sahəsində sui-istifadənin digər forması hesab edilə bilər. Sonuncu tərkibdə nəzərdə tutulan əmələ

görə cinayət məsuliyyətinin yaranması üçün zəruri şərtlərdən biri müvafiq məhkəmə aktının qanuni qüvvəyə minməsidir.

İqtisadi fəaliyyətdə iştirak hüququndan sui-istifadənin nisbi müstəqil növlərindən biri də hazırda "əmtəə nişanlarından qanunsuz istifadə etmə", "bilə-bilə yalan reklam etmə", "kommersiya və ya bank sirri olan məlumatları qanunsuz yolla əldə etmə və ya yayma" adlanan əməllərdir.

"Pul nişanlarının, qiymətli kağızların və müxtəlif növ ödəniş sənədlərinin" hazırkı cinayət hüquqi mühafizəsinin xüsusiyyəti ondan ibarətdir ki, bununla əlaqədar törədilən bütün qəsdlər, o cümlədən satış məqsədilə saxta pul, metal sikkələr, Azərbaycan valyutasında və ya xarici valyutada dövlət qiymətli kağızları və ya başqa qiymətli kağızlar və ya xarici valyutada qiymətli kağızlar hazırlama və ya satma iqtisadi sahədə törədilən cinayət hesab edilir. Bununla belə, artıq qeyd edildiyi kimi, saxta pul kəsmə bizim ölkəmizdə həmişə dövlət əleyhinə olan cinayət hesab edilmişdir. Həqiqətən də saxta pul hazırlamanın iqtisadi fəaliyyət sahəsində cinayət hesab edilməsi ilə razılaşmaq çətindir. Pulun hər bir emissiyasının fiziki və hüquqi şəxslərin mənafeləri ilə bağlılığı şübhəsizdir. Pulun köməyi ilə cəmiyyət həyatının iqtisadi sahəsinin tənzimlənməsi həyata keçirilir. Dövlətin pul hazırlamaq üzrə müstəsna hüququna müdaxilə edilməsi iqtisadi fəaliyyət sahəsində deyil, iqtisadiyyatın idarə edilməsi sahəsində törədilən cinayətdir.

Qeyd edilənlər iqtisadi fəaliyyət, o cümlədən kommersiya fəaliyyəti iştirakçısının hüququndan sui-istifadənin başqa formalarının xarakterizə edilməsi zamanı da prinsipial əhəmiyyətə malikdir. Onların arasında aşağıdakı əməllər nisbi müstəqil rol oynayır: 1) xarici iqtisadi fəaliyyət iştirakçısının hüquqlarından sui-istifadə (qaçaqmalçılıq, Azərbaycan Respublikasının və xarici ölkələrin incəsənət, tarixi, arxeoloji sərvəti olan əşyaları Azərbaycan Respublikasına qaytarmama); 2) valyuta dəyərləri ilə davranma qaydalarını pozma (xarici valyuta vəsaitlərini xaricdən qaytarmama); 3) yaranmış əmlak öhdəliklərini yerinə yetirilməməsinə yönəlmiş hərəkətlər (gömrük ödənişlərinin ödənilməsindən yayınma, müflisləşmə zamanı sui-istifadələr, vergi ödəməkdən yayınma, istehlakçıları aldatma).

AR-nın hal-hazırda qüvvədə olan 1999-cu il 30 dekabr tarixli CM-nin 24-cü fəsli "İqtisadi fəaliyyət sahəsində cinayətlər" adlandırılmaqla bu fəsildə iqtisadi cinayətkarlıq formalarının hüquqi təsbiti və onlara görə tətbiq olunacaq cəza tədbirləri əks olunmuşdur. 190-213-cü maddələri əhatə edən bu cinayət əməllərini aşağıdakı kimi təsnifləşdirmək olar:

1. Vəzifəli şəxslər tərəfindən törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Qanuni sahibkarlıq fəaliyyətinə mane olma (maddə 190);

– Torpaqla əlaqədar qanunsuz əqdlərin qeydiyyatı (maddə 191);

2. İqtisadi fəaliyyətin həyata keçirilməsi hüququndan qanunsuz olaraq istifadə etmək yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Qanunsuz sahibkarlıq (maddə 192);

– Yalançı sahibkarlıq (maddə 193);

– Cinayət yolu ilə əldə edilmiş pul vəsaitlərini və ya digər əmlakı leqallaşdırma (maddə 193-1);

3. Qanunsuz əldə edilmiş, alınmış və ya saxlanmış əmlakdan istifadə etməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Bilə-bilə cinayət yolu ilə əldə edilmiş əmlakı alma və ya satma (maddə 194);

– Qanunsuz kredit alma və ya kreditdən təyinatı üzrə istifadə etməmə;

– Kreditor borclarını ödəməkdən qəsdən yayınma (maddə 196);

4. Aldatmadan və ya ələ almadan istifadə etməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Əmtəə nişanlarından qanunsuz istifadə etmə (maddə 197);

– Bilə-bilə yalan reklam etmə (maddə 198);

– Kommersiya və ya bank sirri olan məlumatları qanunsuz yolla əldə etmə və ya yayma (maddə 202);

– İxrac nəzarətinə aid sənəd və məlumatları yayma (maddə 202-1);

5. Bazardakı inhisarçı mövqeyindən və ya məcburetmədən istifadə etməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– İnhisarçılıq hərəkətləri və rəqabəti məhdudlaşdırma (maddə 199);

– Əqdin bağlanmasına və ya onun bağlanılmasından imtinaya məcbur etmə;

6. Qiymətli kağızların buraxılması qaydalarınıpozmaqla, yaxud saxta pul, qiymətli kağızlar, kredit və ya hesab kartlarını və ya başqa ödəniş sənədlərini hazırlama və ya satma yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Qiymətli kağızların buraxılması (emissiyası) qaydalarını pozma (maddə 203);

– Saxta pul və ya qiymətli kağızlar hazırlama və ya satma (maddə 204);

– Saxta kredit və ya hesab kartlarını və ya başqa ödəniş sənədlərini hazırlama və ya satma (maddə 205);

7. Xarici iqtisadi fəaliyyətin iştirakçısının hüquqlarından istifadə edilməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Qaçaqmalçılıq (maddə 206);

– Azərbaycan Respublikasının və xarici ölkələrin incəsənət, tarixi, arxeoloji sərvəti olan əşyaları Azərbaycan Respublikasına qaytarmama (maddə 207);

8. Valyuta vəsaitləri ilə qanunsuz davranma yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– Xarici valyuta vəsaitlərini xaricdən qaytarmama (maddə 208);

9. Əmlak öhdəliklərindən yayınma yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

– İstehlakçıları aldatma və ya pis keyfiyyətli məhsul istehsal etmə və satma (maddə 200);

– Gömrük ödənişlərinin ödənilməsindən yayınma (maddə 209);

– Müflisləşmə zamanı qanunsuz hərəkətlər (maddə 210);

– Qəsdən müflisləşmə (maddə 211);

– Saxta müflisləşmə (maddə 212);

– Vergi ödəməkdən yayınma (maddə 213);

– Aksiz markası ilə markalanmalı olan məhsulları (malları) belə marka olmadan satma, satış məqsədi ilə saxlama, istehsal binasının hüdudlarından kənara çıxarma və ya idxal etmə (maddə 213-1);

Vəzifəli şəxslər tərəfindən törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1.Qanuni sahibkarlıq fəaliyyətinə mane olma: Bu cinayətin obyekti qanunvericiliklə təminat verilmiş sahibkarlıq fəaliyyəti ilə məşğul olmaq hüququna riayət edilməsini təmin edən ictimai münasibətlərdir.

Obyektiv cəhətdən cinayət bir sıra alternativ hərəkətlərin törədilməsi ilə xarakterizə olunur: a) fərdi sahibkarın və ya kommersiya təşkilatının qeydiyyatından qanunsuz olaraq imtina etmə; b) fərdi sahibkarın və ya kommersiya təşkilatının qeydiyyatından boyun qaçırma; c) müəyyən fəaliyyət növünü həyata keçirmək üçün xüsusi razılığın (lisenziyanın) verilməsindən qanunsuz olaraq imtina etmə; ç) müəyyən fəaliyyət növünü həyata keçirmək üçün xüsusi razılığın (lisenziyanın) verilməsindən boyun qaçırma; d) təşkilati-hüquqi və ya mülkiyyət formasından asılı olmayaraq fərdi sahibkarın və ya kommersiya təşkilatının hüquqlarını və ya qanuni maraqlarını məhdudlaşdırma; e) fərdi sahibkarın və ya kommersiya təşkilatının müstəqilliyini qanunsuz məhdudlaşdırma və ya onların fəaliyyətinə başqa cür müdaxilə etmə.

2.Torpaqla əlaqədar qanunsuz əqdlərin qeydiyyatı:Azərbaycan Respublikası Konstitusiyasının 14-cü maddəsinə müvafiq olaraq, təbii ehtiyatlar hər hansı fiziki və ya hüquqi şəxslərin hüquqlarına və mənafelərinə xələl gətirmədən Azərbaycan Respublikasına mənsubdur. Bunula əlaqədar torpaq mülkiyyəti sahəsində münasibətlərin dövlət tənzimi bir sıra qanunlarla, o cümlədən cinayət qanunu ilə həyata keçirilir.

Cinayətin obyekti mülkiyyət hüququnun obyekti kimi torpağın hüququ rejimini təmin edən ictimai münasibətlər, habelə torpaqla əlaqədar əqdlərin qeydiyyatının dövlət tərəfindən müəyyən edilmiş qaydasıdır.

Obyektiv cəhətdən cinayət müstəqil hərəkətlərlə xarakterizə olunur: torpaqla əlaqədar bilə-bilə qanunsuz əqdləri qeydiyyata alma; Dövlət kadastrının uçot məlumatlarını təhrif etmə; torpaq haqqının miqdarını azaltma.

Torpaqla əlaqədar əqd qanunun və ya başqa normativ aktların tələblərinə müvafiq olmadıqda, daha doğrusu, torpağın məqsədli təyinatı və mülkiyyət hüququnun obyekti kimi onun hüquq rejimi pozulduqda, qanunsuz hesab edilir.

İqtisadi fəaliyyətin həyata keçirilməsi hüququndan qanunsuz olaraq istifadə etmək yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1.Qanunsuz sahibkarlıq: Azərbaycan Respublikası Mülki Məcəlləsinin 13-cü maddəsinə əsasən, sahibkarlıq fəaliyyəti şəxsin müstəqil surətdə, öz riski ilə həyata keçirdiyi, əsas məqsədi əmlak istifadəsindən, əmtəə satışından, işlər görülməsindən, və ya xidmətlər göstərilməsindən mənfəət götürülməsi olan fəaliyyətidir. Bu fəaliyyətlə təkcə hüquqi şəxslər deyil, ayrı-ayrı vətəndaşlar da məşğul ola bilərlər.

Qanunvercilikdə müəyyən edilmiş məcburi, formal tələbə müvafiq olaraq, həm hüquqi, həm də fiziki şəxslər qanunla müəyyən olunmuş qaydada sahibkarlıq fəaliyyətini həyata keçirən şəxs kimi qeydiyyata alınmalıdırlar. Bir sıra fəaliyyət növləri (bank, birja, səhiyyə və s.) ilə məşğul olmaq üçün onlar lisenziya almalıdırlar.

Dövlət qeydiyyatından keçmədən və ya lisenziya almadan sahibkarlıq fəaliyyəti ilə məşğul olma qanunsuz hesab edilir, CM-nin 192-ci maddəsində göstərilmiş əlamətlər olduqda isə cinayət məsuliyyətinə səbəb olur.

Cinayətin obyektiv cəhəti hər biri bu cinayətkar qəsdin ayrıca növünü təşkil edən bir sıra alternativ əməllərdən ibarətdir. Aşağıdakı hallarda sahibkarlıq fəaliyyəti qanunsuz hesab edilir: Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş qaydada dövlət qeydiyyatına alınmayan; xüsusi razılıq (lisenziya) tələb olunduğu halda belə (lisenziya) alınmayan; lisenziyalaşdırma şərtlərinin pozulması ilə həyata keçirilən.

2.Yalançı sahibkarlıq: Sahibkarlıq fəaliyyətini həyata keçirmək niyyəti olmadan kommersiya təşkilatı yaratma, yəni yalançı sahibkarlıq qüvvədə olan qanunvericiliyə əsasən cinayət məsuliyyəti yaradır.

Cinayətin obyekti qanuni, təsis sənədlərinə müvafiq fəaliyyətin təmin edilməsinə yönəlmiş ictimai münasibətlərdir.

Cinayətin obyektiv cəhətini sahibkarlıq fəaliyyətini həyata keçirmək niyyəti olmadan müəssisə və ya digər hüquqi şəxsin yaradılmasından ibarət hərəkətlər təşkil

edir. Həmin hərəkətlər nəticəsində xeyli miqdarda ziyan vurulması, habelə CM-nin 103-cü maddəsinə Azərbaycan Respublikasının 26 dekabr 2000-ci il qanunu ilə əldə edilmiş əlavədən sonra həm də xeyli miqdarda gəlir əldə edilməsi obyektiv cəhətin məcburi əlamətidir.

Lakin şərh edilən cinayətin obyektiv cəhətini istənilən hüquqi şəxsin deyil, yalnız kommersiya hüquqi şəxslərinin yaradılması əmələ gətirə bilər, çünki qeyri-kommersiya hüquqi şəxslərinin əsas məqsədi, ümumiyyətlə sahibkarlıq fəaliyyətini həyata keçirmək deyildir (Azərbaycan Respublikası MM-nin 43.5-ci maddəsi). Ona görə də qeyri-kommersiya hüquqi şəxslərinin yaradılması, bu, başqa niyyətlə edilmiş olsa da belə, CM-nin 193-cü maddəsi ilə məsuliyyətə səbəb ola bilməz.

Qanunsuz əldə edilmiş, alınmış və ya saxlanmış əmlakdan istifadə etməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1.Bilə-bilə cinayət yolu ilə əldə edilmiş əmlakı alma və ya satma: Mülki dövriyyədən çıxarılmış, o cümlədən bilə-bilə cinayət yolu ilə əldə edilmiş əmlak vətəndaşların və hüquqi şəxslərin mülkiyyət hüququnun obyekti ola bilməz. Qabaq-cadan vəd edilmədən belə əmlakı əldə etmə və satma təkcə sahibkarlıq fəaliyyətinin əsas prinsiplərini pozmur, həm də şəxslərin əsassız olaraq varlanmasına şərait yaradır.

Obyektiv cəhətdən CM-nin 194-cü maddəsində nəzərdə tutulmuş cinayət bilə-bilə cinayət yolu ilə əldə edilmiş əmlakı xeyli miqdarda almadan və ya satmadan ibarətdir.

CM-nin 194-cü maddəsi üzrə məsuliyyət yalnız cinayətin icraçısına qabaq-cadan vəd edilməyən alma və ya satmaya görə yaranır. Qabaqcadan vəd etməklə (cinayət törədilən anadək və ya həmin anda) cinayət yolu ilə əldə edilmiş əmlakı alma və ya satmanı isə müvafiq cinayətin törədilməsində iştirakçılıq kimi nəzərdən keçir-mək lazımdır.

2.Qanunsuz kredit alma və ya kreditdən təyinatı üzrə istifadə etməmə: Təhlil edilən cinayətin obyekti təsərrüfat subyektlərinin kreditləşdirilməsini təmin edən

ictimai münasibətlərdir. Cinayətin predmetini isə kreditlər, güzəştli şərtlərlə kreditlər və ya məqsədli dövlət kreditləri təşkil edir.

Obyektiv cəhətdən cinayət təşkilatın rəhbəri və ya fərdi sahibkar tərəfindən təşkilatın, yaxud fərdi sahibkarın təsərrüfat və ya məliyyə vəziyyəti barədə bilə-bilə yalan məlumat verməklə aşağıdakı alternativ hərəkətlərdən birinin törədilməsində ifadə olunur: a) kreditin alınması; b) güzəştli şərtlərlə kreditin alınması; c) məqsədli dövlət kreditinin alınması; ç) məqsədli dövlət kreditindən təyinatı üzrə istifadə edilməməsi. Obyektiv cəhətin məcburi əlamətlərindən biri də yuxarıda göstərilmiş əməllər nəticəsində xeyli miqdarda ziyan vurulmasıdır.

3.Kreditor borclarını ödəməkdən qəsdən yayınma: Cinayətin obyekti təsərrüfat subyektlərinin kreditləşdirilməsini təmin edən ictimai münasibətlərdir. Əlavə obyekt kimi kreditorların əmlak mənafeləri çıxış edə bilər.

Cinayətin obyektiv cəhəti məhkəmənin qanuni qüvvəyə minmiş müvafiq qərarından sonra təşkilat rəhbərinin və ya vətəndaşın aşağıdakı əməllərini nəzərdə tutur: a) kreditor borclarını ödəməkdən qəsdən yayınma; b) qiymətli kağızları ödəməkdən qəsdən yayınma. Obyektiv cəhətin məcburi əlaməti göstərilən əməllər nəticəsində xeyli miqdarda ziyan vurulmasıdır. Kreditor borclarını ödəməkdən yayınma dedikdə, borcun müqavilədə və ya qanunla dəqiq müəyyən olunmuş müddətdə qaytarılmaması başa düşülür. Belə ki, Azərbaycan Respublikası Mülki Məcəlləsinin 739.1-ci maddəsinə müvafiq olaraq, borclunun aldığı kredit onun müqavilədə göstərilmiş miqdarda və şərtlərlə qaytarılması vəzifəsini nəzərdə tutur.

Aldatmadan və ya ələ almadan istifadə etməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1. Əmtəə nişanlarından qanunsuz istifadə etmə: Əmtəə nişanlarından qanunsuz istifadə etmə vicdansız rəqabətin formalarından biridir. Vicdansız rəqabət təsərrüfat subyektlərinin sahibkarlıq fəaliyyətində üstünlüklər əldə etməyə yönəlmiş və qüvvədə olan qanunvericiliyin müddəalarına, işgüzar dövriyyə adətlərinə, ədəblilik, məntiqlilik və ədalətlilik tələblərinə zidd olan, başqa təsərrüfat subyektlərinə ziyan vura bilən və ya onların işgüzar nüfuzuna zərər yetirə bilən hərəkətləridir.

Obyektiv cəhətdən CM-nin 197-ci maddəsində nəzərdə tutulmuş cinayət özgənin əmtəə və ya xidmət etmə nişanından, əmtəənin mənşə yerinin adından və ya əmtəələrin adına oxşar adlardan qanunsuz istifadə etmədən ibarətdir.

2. Bilə-bilə yalan reklam etmə: Son dövrlərdə reklam həyatımızın ayrılmaz hissəsinə çevrilmişdir. Reklam hesabına, konyukturadan istifadə etməklə, satışın artırılması və sürətləndirilməsi müəssisənin genişləndirilməsinə və işlərin daha da müvəffəqiyyətlə aparılmasına şərait yaradır.

Bununla yanaşı, bilə-bilə yalan reklam etmə cinayət-hüquqi məsuliyyət yaradır. Cinayətin obyekti əmtəə, xidmət və iş bazarında reklamın istehsalı, yerləşdirilməsi və yayılması ilə əlaqədar yaranan, normal sahibkarlıq fəaliyyətini təmin edən ictimai münasibətlərdir. Cinayətin obyektiv cəhəti əmtəələr, işlər və xidmətlər haqqında, habelə onların istehsalçıları (icraçıları, satıcıları) haqqında bilə-bilə yalan məlumatlardan reklamda istifadə etmədən ibarətdir. Belə reklamın köməyi ilə reklam verən (yayıcı, istehsalçı) istehlakçını qəsdən aldadır.

Bilə-bilə yalan reklam vicdansız rəqabətin növlərindən biridir. Reklamda verilən informasiya o halda yalan hesab edilə bilər ki, fiziki və ya hüquqi şəxslər, əmtəələr, ideyalar və yeniliklər haqqında məlumatlar ya onların məziyyətlərini (kəmiyyətini, keyfiyyətini, texniki göstəricilər və s.) azaldır, ya artırır, yaxud da ümumiyyətlə, həqiqətə uyğun deyildir.

3.Kommersiya və ya bank sirri olan məlumatları qanunsuz yolla əldə etmə və ya yayma: Hazırda vicdansız rəqabətin formalarından biri də kommersiya və ya bank sirri olan məlumatların yayılmasıdır. Sahibkarlıq fəaliyyəti xidməti və kommersiya məlumatının saxlanması prinsipinə bütün iqtisadi subyektlər və vətəndaşlar tərəfindən riayət edilməsinə əsaslanır. Hal-hazırda məlumat nəinki təkcə əmtəə xarakteri almış, həm də onun toplanması, saxlanması, yayılması, istifadəsi və s. ilə əlaqədar yaranan müqavilə münasibətlərinin obyekti olmuşdur.

Beləliklə, CM-nin 202-ci maddəsində nəzərdə tutulmuş cinayətin obyektini normal sahibkarlıq fəaliyyəti ilə əlaqədar ictimai münasibətlər təşkil edir. Cinayətin predmeti isə kommersiya və ya bank sirridir.

CM-nin 202.1-ci maddəsində nəzərdə tutulmuş cinayətin obyektiv cəhəti kommersiya və ya bank sirri olan məlumatların aşağıdakı alternativ üsullardan biri ilə toplanmasından ibarətdir: sənədləri oğurlamaqla, satın almaqla, hədələməklə, digər qanunsuz üsulla.

Bazardakı inhisarçı mövqeyindən və ya məcburetmədən istifadə etməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1.İnhisarçılıq hərəkətləri və rəqabəti məhdudlaşdırma: Mülkiyyət formalarının müxtəlifliyi şəraitində əmtəə bazarlarının səmərəli fəaliyyətinin, təsərrüfat subyektlərinin rəqabəti üçün münbit iqtisadi şəraitin hüquqi cəhətdən təmin edilməsi xüsusi əhəmiyyət kəsb edir. Ona görə də qanunvericiliklə inhisarçılıq fəaliyyətinin və vicdansız rəqabətin məhdudlaşdırılmasının və qarşısının alınmasının təşkilati və hüquqi əsasları müəyyən edilmişdir. Həmin qanunvericilik həm yerli və əcnəbi hüquqi şəxslərin, icra hakimiyyəti orqanlarının, yerli özünüidarə orqanlarının, fiziki şəxslərin iştirak etdiyi Azərbaycan Respublikasının əmtəə bazarlarındakı münasibətlərə, həm də həmin şəxslər tərəfindən Azərbaycan Respublikasından kənarda bağlanan əqdlərə və edilən hərəkətlərə şamil edilir.

Antiinhisar qanunvericiliyini pozan və cinayət hesab edilən əməllərə görə məsuliyyət CM-nin 199-cu maddəsində nəzərdə tutulmuşdur və cinayətin obyekti sahibkarların əmtəə bazarında qanuni rəqabəti ilə əlaqədar yaranan ictimai münasibətlərdir.

Təhlil edilən maddənin məzmununa əsasən, cinayətin obyektiv cəhəti antiinhisar qanunvericliyinin pozulmasının iki müstəqil növünü - inhisarçılıq hərəkətləri və rəqabəti məhdudlaşdırmanı özündə birləşdirir.

2.Əqdin bağlanmasına və ya onun bağlanılmasından imtinaya məcbur etmə: Mülki qanunvericiliyin əsas prinsiplərindən birini təşkil edən müddəaya əsasən, vətəndaşlar (fiziki şəxslər) və hüquqi şəxslər öz subyektiv mənafelərindən çıxış edərək mülki hüquqlar əldə edirlər və onları həyata keçirirlər. Əqdlər də mülki hüququn ən mühüm və əsas institutlarından biridir.

İstənilən iradi akt kimi, əqd də iradə və iradə ifadəsinin məzmunundan ibarətdir. Başqa şəxslərin hüquqazidd hərəkətlərinin təsiri altında bağlanmış əqd,

mülki qanunvericiliyə müvafiq olaraq, etibarsız hesab edilir (Azərbaycan Respublikası Mülki Məcəlləsinin 14-cü fəsli), CM-nin 201-ci maddəsində göstərilən əlamətlər olduqda isə cinayət məsuliyyəti yaranır.

Obyektiv cəhətdən təhlil edilən cinayət tərkibi iki hərəkətdən ibarət mürəkkəb cinayətdir: psixi zor; əqdin bağlanmasına və ya onun bağlanmasından imtinaya məcbur etmə. Hədənin istənilən növü zamanı psixi zorun başlıca funksiyası zərərçəkmişi əqdin bağlanmasına və ya onun bağlanmasından imtinaya məcbur etmək məqsədi ilə onun psixikasına təsir etməkdir. Əqd bağlamaq və ya onun bağlanmasından imtina etmək tələbi isə ilk növbədə mülki hüquq və vəzifələrin yaradılmasına, dəyişdirilməsinə və ya xitam edilməsinə məcbur etmədən ibarətdir. Təqsirkarın öz məqsədinə çatıb-çatmamasından asılı olmayaraq, məcbur etmə anında cinayət başa çatmış hesab edilir.

Xarici iqtisadi fəaliyyətin iştirakçısının hüquqlarından istifadə edilməklə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1.Qaçaqmalçılıq: Bu cinayət obyektiv cəhətdən malların və digər əşyalarınAR gömrük sərhədindən gömrük nəzarətindən kənar və ya ondan gizli, yaxud sənədlərdən və ya gömrük eyniləşdirilməsi vasitələrindən aldatma yolu ilə istifadə etməklə, yaxud bəyan etməməklə və ya düzgün bəyan etməməklə külli miqdarda keçirilməsindən ibarətdir.

Qaçaqmalçılığın predmeti kimi mallar dedikdə, Azərbaycan Respublikasının Gömrük Məcəlləsinin 17-ci maddəsinə əsasən. istənilən daşınan əmlak, o cümlədən valyuta, valyuta sərvətləri, elektrik və digər enerji növləri, nəqliyyat vasitələri (sərnişinlərin və malların beynəlxalq daşınmaları üçün nəzərdə tutulan nəqliyyat vasitələri istisna olmaqla) başa düşülür. Bundan başqa, şərh edilən cinayətin predmeti qismində gömrük sərhədindən keçirilərkən gömrük nəzarətindən keçməli, eyniləşdirilməli və bəyan edilməli əşyalar, məsələn, əlyazmalar. incəsənət əsərləri və s. də çıxış edə bilər.

2.Azərbaycan Respublikasının və xarici ölkələrin incəsənət, tarixi, arxeoloji sərvəti olan əşyaları Azərbaycan Respublikasına qaytarmama: Cinayətin obyekti Azərbaycan xalqının və xarici ölkə xalqlarının incəsənət, tarixi və arxeoloji sərvəti

olan əşyalara sahiblik, istifadə və sərəncam hüququnu təmin edən ictimai münasibətlərdir.

Cinayətin predmeti aşağıdakı yollarla əldə edilmiş mədəni sərvətlər ola bilər; Azərbaycan Respublikasının vətəndaşı olan şəxs və ya şəxslər qrupu tərəfindən, habelə AR ərazisində daimi yaşayan əcnəbilər və ya vətəndaşlığı olmayan şəxslər tərəfindən yaradılmış; AR ərazisində tapılmış; həmin sərvətlərin əldə edildiyi ölkənin səlahiyyətli orqanlarının razılığı ilə həyata keçirilmiş arxeoloji, etnoloji və təbii-elmi ekspedisiyalar nəticəsində tapılmış; azad mübadilə yolu ilə əldə edilmiş; bəxşiş olaraq əldə edilmiş və ya həmin sərvətin mənşə ölkəsinin səlahiyyətli orqanlarının razılığı ilə qanuni olaraq əldə edilmiş.

Cinayət obyektiv cəhətdən AR qanunvericiliyinə müvafiq olaraq qaytarılması məcburi olan AR hüdudlarından kənara çıxarılmış AR-in və xarici ölkələrin incəsənət, tarixi və arxeoloji sərvəti olan əşyaları müəyyən edilmiş müddətdə AR-ə qaytarmamada ifadə olunur.

Valyuta vəsaitləri ilə qanunsuz davranma yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1.Xarici valyuta vəsaitlərini xaricdən qaytarmama: Bu cinayətin obyekti valyuta tənzimi və valyuta nəzarəti ilə əlaqədar dövlətin maliyyə fəaliyyəti sahəsində yaranan ictimai münasibətlərdir.

Təhlil edilən cinayət obyektiv cəhətdən xarici iqtisadi fəaliyyətin həyata keçirilməsi nəticəsində əldə edilmiş və AR qanunvericiliyinə müvafiq olaraq AR-in müvəkkil edilmiş bankının hesabına məcburi qaydada köçürülməli olan xeyli miqdarda xarici valyuta vəsaitlərini xaricdən qaytarmamada ifadə olunur.

"Valyuta tənzimi haqqında" Azərbaycan Respublikası Qanununun 7-ci maddəsinə görə xarici valyuta vəsaitlərini xaricdən qaytarmama dedikdə, rezident müəssisə və təşkilatların xarici iqtisadi fəaliyyətdən əldə etdikləri xarici valyuta vəsaitlərini Azərbaycan Respublikasının müvəkkil bankındakı hesaba köçürməməsindən ibarət hərəkətsizlik başa düşülməlidir.

Xarici valyuta vəsaitlərinin bankın nəzarət sənədlərində (əqdin pasportunda, gömrük-bank nəzarəti uçotu vərəqində, dosyedə) müəyyən edilmiş müddətdə Azər-

baycan Respublikasının müvəkkil edilmiş bankdakı hesaba daxil olmadığı andan cinayət başa çatmış hesab edilməlidir.

Əmlak öhdəliklərindən yayınma yolu ilə törədilən iqtisadi fəaliyyət sahəsində olan cinayətlər:

1. İstehlakçıları aldatma və ya pis keyfiyyətli məhsul istehsal etmə və satma: CM-nin 200-cü maddəsində bir-birindən kifayət qədər fərqlənən iki cinayət tərkibi təsbit edilmişdir.

CM-nin 200.1-ci maddəsində nəzərdə tutulmuş cinayətin obyekti malların satışı (işlərin yerinə yetirilməsi, xidmətlərin göstərilməsi) zamanı istehlakçılarla mal satanlar və ya xidmət göstərənlər arasında yaranan münasibətlərdir. Əlavə obyekt qismində istehlakçıların həyat və sağlamlığı, habelə əmlak mənafeləri çıxış edir. Obyektiv cəhətdən cinayət mal satan və ya əhaliyə xidmət göstərən təşkilatlar, həmçinin ticarət (xidmət) sahəsində fərdi sahibkar qismində qeydə alınmış fiziki şəxslər tərəfindən malın (xidmətin) ölçüsünə, çəkisinə, hesabına, habelə istehlak xüsusiyyəti və ya keyfiyyətinə dair istehlakçıları xeyli miqdarda aldatmada ifadə olunmuşdur.

CM-nin 200.3-cü maddəsində nəzərdə tutulmuş cinayət çoxobyektlidir. Bu cinayətin əsas bilavasitə obyekti məhsulların lazımi keyfiyyətdə istehsalını və satışa buraxılmasını təmin edən ictimai münasibətlərdir. Cinayətkar qəsdin digər bilavasitə obyekti əhalinin sağlamlığıdır. Cinayətin predmeti isə pis keyfiyyətli məhsullardır.

Bu cinayət tərkibinin obyektiv cəhəti isə zərərçəmiş şəxsin sağlamlığına az ağır və ya ağır zərər vurulmasına səbəb olmuş aşağıdakı alternativ əməllərdə ifadə olunur: pis keyfiyyətli məhsulların istehsalı; satışa buraxılması; belə məhsulların satışı; onların keyfiyyətsiz olmasının gizlədilməsi.

Pis keyfiyyətli məhsulların keyfiyyətsiz olmasının gizlədilməsi həm istehsalçı və ya satıcı başqa məhsullar üçün verilmiş və ya bilə-bilə qanunsuz uyğunluq sertifikatından istifadə etdikdə, sertifikatlaşdırılmanı həyata keçirən orqan isə saxta sertifikat verdikdə təhlil edilən əlamət mövcud olacaqdır.

2.Gömrük ödənişlərinin ödənilməsindən yayınma: Azərbaycan Respublikasının xarici iqtisadi siyasətin və daxili əmtəə bazarının dövlət tənziminin mühüm vasitə-

lərindən biri Azərbaycan Respublikasının gömrük sərhədindən keçən mallara qoyulan gömrük ödənişlərinin müəyyən edilməsi və tətbiqi qaydalarıdır. Bu qaydaların və gömrük ödənişləri mexanizminin pozulması dövlət pul fondlarının təşkil olunması sahəsində ölkə iqtisadiyyatına ciddi ziyan vurur.

Cinayətin predmeti gömrük ödənişləridir. Cinayətin obyektiv cəhəti isə xeyli miqdarda gömrük ödənişlərinin ödənilməsindən yayınmada ifadə olunur. Bu halda yayınma aşağıdakı hərəkətlərdə ifadə oluna bilər: gömrük bəyannaməsində və ya gömrük məqsədləri üçün zəruri olan başqa sənədlərdə malın və nəqliyyat vasitələrinin gömrük rejimi; gömrük dəyəri, yaxud mənşə ölkəsi haqqında yalan məlumat verilməsi və ya gömrük ödənişlərindən azad etmək və ya onun miqdarını azaltmaq üçün əsas verən başqa yalan məlumatlar verilməsi; ödənilmiş gömrük ödənişlərinin qaytarılması hüququ, ödəniş və ya başqa əvəz almaq hüququ, yaxud alınmış əvəzin tam və ya qismən qaytarılmaması hüququ verən yalan daxil edilmiş sənədlərin AR-in gömrük orqanlarına təqdim edilməsi; ödəmə müddətlərinin pozulması.

3.Müflisləşmə zamanı qanunsuz hərəkətlər:Sahibkarlıq fəaliyyəti, eləcə də digər iqtisadi fəaliyyət təkcə sahibkarın özünə deyil, həm də onun kontragentlərinə ziyan vurulması riskinə malikdir. Ona görə də istənilən iqtisadi subyektin mülki dövriyyədə iştirakı ona və onun etdiyi əməliyyatlara etibar göstərilməsi şəraitində mümkündür. Kreditorların riskini minimuma endirmək üçün ölkəmizin qanunvericiliyində müflisləşmə institutu nəzərdə tutulmuşdur. Bu institutun əsasını "Müflisləşmə və iflas haqqında" Azərbaycan Respublikasının Qanunu, mülki hüququn müvafiq normaları, habelə bəzi başqa normativ hüquqi aktlar təşkil edir.

Müflis olmuş sahibkar qanunun tələb etdiyinin əksinə olaraq özünün iqtidarsız olmasını elan etməyərək, kontragentləri qarşısında əmlak öhdəliklərinin icrasından yayınmaq üçün öz vəziyyətini gizlətməyə cəhd etdikdə, CM-nin 210-cu maddəsi üzrə cinayət məsuliyyətinə cəlb edilə bilər.

Müflisləşmə zamanı qanunsuz hərəkətlər ayrıca cinayət məsuliyyəti yaradan iki növ əməlləri nəzərdə tutur. Obyektinə görə oxşar olan bu əməllər obyektiv cəhətinə, habelə subyektinə görə bir-birindən xeyli fərqlənir.

CM-nin 201.1-ci maddəsində nəzərdə tutulmuş cinayətin obyektiv cəhəti müflisləşmə zamanı və ya müflisləşmə güman edilən zaman törədilən bir sıra alternativ qanunsuz hərəkətdən ibarətdir: əmlakın və ya əmlak öhdəliklərinin, əmlak haqqında məlumatların, onun miqdarının, olduğu yerin, yaxud əmlak haqqında digər məlumatların gizlədilməsi; əmlakın digərinin sahibliyinə verilməsi, əmlakın özgəninkiləşdirilməsi və ya məhv edilməsi; iqtisadi fəaliyyəti əks etdirən mühasibat və ya digər hesabat sənədlərinin gizlədilməsi, məhv edilməsi və ya saxtalaşdırılması.

4.Qəsdən müflisləşmə: Nəzərdən keçirilən cinayətin obyekti dövlətin maliyyə fəaliyyəti sahəsində yaranan və sahibkarlıq fəaliyyətini təmin edən ictimai münasibətlərdir. Cinayət obyektiv cəhətdən ödəmə qabiliyyətsizliyinin yaradılmasından və ya artırılmasından ibarətdir.

Qəsdən müflisləşmə dedikdə, süni olaraq ödəmə qabiliyyətsizliyi yaradan və belə qabiliyyətsizliyi artıraraq bilə-bilə iflasa aparan sahibkarlıq fəaliyyəti (sərfəli olmayan əqdlər bağlanması, mühasibat və ya başqa maliyyə fəaliyyətinin səhlənkarcasına aparılması; iqtisadi kontragentlərin və ya işgüzar tərəfdaşların etinasızcasına seçilməsi, pul vəsaitlərinin müəssisənin mənafeyi ilə əlaqədar olmayan ehtiyaclara xərclənməsi və s.) başa düşülür.

5.Saxta müflisləşmə: Nəzərdən keçirilən cinayətin obyekti dövlətin maliyyə fəaliyyəti sahəsində yaranan və sahibkarlıq fəaliyyətini təmin edən ictimai münasibətlərdir.

Cinayətin obyektiv cəhəti kommersiya təşkilatının rəhbəri və ya mülkiyyətçisi, habelə fərdi sahibkar tərəfindən özünü bilə-bilə yalandan ödəmə qabiliyyəti olmayan elan etmədən ibarətdir. Obyektiv cəhətin daha bir məcburi əlaməti saxta müflisləşmənin xeyli miqdarda ziyan vurulmasıdır.

Saxta müflisləşmə dedikdə, özünü təşkilatın (fərdi sahibkar) həqiqi iqtisadi vəziyyətinin əksinə olaraq və kreditorlarla razılaşdırılmadan, bilə-bilə yalandan ödəmə qabiliyyəti olmayan elan etmə başa düşülür. CM-nin 212.1-ci maddəsi ilə cinayət məsuliyyəti həmin əməl nəticəsində xeyli miqdarda ziyan vurulduqda meydana gəlir. Saxta müflisləşmə nəticəsində kreditorlara xeyli miqdarda ziyan vurulduğu andan cinayət başa çatmış hesab edilir.

6.Vergi ödəməkdən yayınma: Müasir dövlətdə vergilər gəlirlərin əsas formasıdır. Azərbaycan Respublikası Konstitusiyanın 73-cü maddəsinə əsasən, qanunla müəyyən olunmuş vergiləri və başqa dövlət ödənişlərini tam həcmdə və vaxtında ödəmək hər bir şəxsin borcudur. Vergi ödəməkdən yayınma isə ölkə iqtisadiyyatının və maliyyə sisteminin sabitliyini pozulmasına səbəb olur.

İki növ əsas vergi ödəyicisi – fiziki və hüquqi şəxslər bir-birindən fərqləndiyindən CM-nin 213-cü maddəsində cinayət hesab edilən əməllərin iki müxtəlif növü təsbit olunmuşdur. Obyektinə görə oxşar olan bu cinayət tərkibləri obyektiv cəhətinə və subyektinə görə xeyli dərəcədə bir-birindən fərqlənir.

CM-nin 213.1-ci maddəsində nəzərdə tutulmuş cinayət tərkibinin obyekti dövlətin maliyyə fəaliyyəti sahəsində ictimai münasibətlərdir. Bu cinayətin obyektiv cəhəti isə fiziki şəxslər tərəfindən AR qanunvericliyində nəzərdə tutulmuş hallarda gəlirlər haqqında bəyannamə təqdim etməməklə, yaxud gəlirlər və ya xərclər barədə bilə-bilə təhrif olunmuş məlumatları bəyannamədə göstərməklə, yaxud digər üsulla xeyli miqdarda vergiləri və ya başqa icbari ödənişləri ödəməkdən yayınmadan ibarətdir.

CM-nin 213.3-cü maddəsində göstərilmiş cinayətin isə obyekti hüquqi şəxslərdən vergilərin yığılması ilə əlaqədar dövlətin maliyyə fəaliyyəti sahəsində yaranan ictimai münasibətlərdir.

CM-nin 213.3-cü maddəsində nəzərdə tutulmuş cinayətin obyektiv cəhəti gəlirlər və xərclər barədə bilə-bilə təhrif olunmuş məlumatları təşkilat mühasibat sənədlərində daxil etməklə, yaxud digər üsulla xeyli miqdarda vergiləri və ya başqa icbari ödənişləri ödəməkdən yayınmada ifadə olunmuşdur.

Beləliklə, Azərbaycan Respublikasının CM-nin "İqtisadi fəaliyyət sahəsində cinayətlər" adlandırılan 24-cü fəslində iqtisadi cinayətkarlıq formaları geniş şərh olunsa da iqtisadi cinayətkarlığın xüsusi forması olan kibercinayətkarlıq və eləcə də kompüter cinayətlərinə görə məsuliyyət bu fəsildə öz əksini tapmamışdır. Azərbaycanda Respublikasının cinayət qanunvericiliyində kibercinayətkarlığın hüquqi təsbiti məsələsi növbəti paraqrafda daha geniş şərh olunacaqdır.

2.2 Kibercinayətkarlıqla mübarizə sahəsində Azərbaycanın milli hüquq sisteminin müasir vəziyyəti

Külli miqdarda müxtəlif informasiyaların istifadəsinə əsaslanan müasir cəmiyyətin inkişafını cəmiyyətin bütün həyat sferalarına elektron hesablama maşınlarının geniş tətbiqi olmadan təsəvvür etmək mümkünsüzdür. EHM-lər yalnız ayrı-ayrı idarəetmə və eləcə də təsərrüfat vahidləri səviyyəsində informasiyanın işlənməsi, saxlanmasına və ya vətəndaşlar arasında əlaqənin yaradılmasına xidmət etmir, o həmçinin dövlətin daxili və xarici təhlükəsizliyinin təmin olunması məqsədilə geniş tətbiq edilir. Amma elmi-texniki inqilabın genişlənməsi ölkə iqtisadiyyatının inkişaf amillərinin tərkibində proqressiv dəyişikliklərə səbəb olmaqla yanaşı, kriminal dünyanın neqativ tendensiyalarının genişlənməsinə, cinayət əməllərinin yeni forma və növlərinin yaranmasına gətirib çıxarır. Bu isə özünü cinayətkar qrup və birliklərin öz fəaliyyətində elm və texnikanın yeni nailiyyətlərindən aktiv istifadə etmələrində daha aydın şəkildə göstərir.

Azərbaycanda kompüter texnikası vasitələrinin və informasiya emalı texnologiyalarının istifadəsi ilə əlaqəli olan, eləcə də yerli hüquq elminə və praktikasına məlum olmayan yeni növ cinayət əməllərinin – kompüter cinayətlərinin meydana gəlməsi faktı xüsusi həyəcan doğurur. Bu isə öz növbəsində ölkə qanunvericiliyində baş verən bu hala adekvat hüquqi təsir mexanizminin işlənib hazırlanmasını zəruri edir. Bu istiqamətdə əks olunmuş cinayət əməlləri mahiyyət etibarı ilə heç də cinayətin törədilməsi üçün vasitə kimi elektron hesablama texnikasının istifadəsini nəzərdə tutmur. Cinayət Məcəlləsinin 30-cu fəslinə informasiyanın və EHM-nın istifadəsi vasitəsilə informasiyanın işlənməsi sisteminin təhlükəsizliyinə qəsd edən ictimai-təhlükəli əməllər daxil edilmişdir.

İnformasiyanın qanunsuz istifadəsinin nəticələri çox müxtəlif ola bilər. Belə ki, informasiyadan qanunsuz istifadə intellektual mülkiyyətin toxunulmazlığının pozulması ilə yanaşı vətəndaşların şəxsi həyatları barədə məlumatlarının yayılmasına, birbaşa itkilər və əldə olunmamış mənfəət şəklində mülkiyyətə zərər vurulmasına,

müəssisələrin nüfuzunun itirilməsi və müəssisələrin normal fəaliyyətinin pozulmasına səbəb ola bilər. Bu səbəbdən də bu növ cinayətlərin Cinayət Məcəlləsinin "İctimai təhlükəsizlik və ictimai qayda əleyhinə olan cinayətlər" adlı X Bölməsində yerləşdirilməsi tamamilə doğrudur.

Azərbaycan Respublikası Cinayət Məcəlləsində Kompüter informasiya sferasındakı cinayətlərə aşağıdakılar daxildir:

1. Kompüter informasiyasına qanunsuz olaraq daxil olma (maddə 271);

2. Elektron-hesablayıcı maşınlar üçün ziyanverici proqramlar yaratma, onlardan istifadə etmə və ya onları yayma (maddə 272);

3. Elektron hesablayıcı maşınların (EHM), EHM sisteminin və ya onların şəbəkələrinin istismarı qaydalarını pozma (maddə 273).

Bu cinayət tərkiblərinin konstruksiyasının xüsusiliyi onların maddi tip üzrə formalaşdırılmasıdır. Yəni, bu tərkiblərdə EHM istifadəçilərinə zərər vurulması şəklində ictimai təhlükəli hücumlar nəzərdə tutulmuşdur. EHM istifadəçilərinə zərərin vurulması isə EHM-lərin və ya EHM şəbəkəsinin normal fəaliyyətinin pozulmasından ibarətdir.

Kompüter texnikasınının fiziki olaraq zədələnməsi və ya məhv edilməsi, qanunsuz ələ keçirilməsi isə maddi dəyərə malik predmetlər kimi AR CM-nin 23-cü "Mülkiyyət əleyhinə cinayətlər" fəslində nəzərdən keçirilir.

Bütövlükdə AR CM-nin 30-cu fəslinin əsas məqsədi informasiyanın qorunmasından və məhz buna əsasəndə bu informasiya ehtiyatlarının maddi daşıyıcıları olan aparat texniki vasitələrinin də təhlükəsizliyinin təmin olunmasından ibarətdir.

Kompüter cinayətlərinin obyektiv tərəfi hərəkətlə yanaşı hərəkətsizliklə də xarakterizə olunur. Hərəkət (hərəkətsizlik) kompüter informasiyasının istifadəsi ilə bağlı hüquq və maraqların pozulması ilə əlaqəlidir.

Daha öncə də qeyd olunduğu kimi kompüter 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 istina olaraq

formal tərkibə malik cinayət əməlləridir. Cinayətin nəticələri isə Cinayət Məcəlləsində kompüter cinayətlərinin növlərinə uyğun olaraq konkretləşdirilmişdir. Belə ki, cinayət əməlləri və onların nəticələri arasında səbəb-nəticə əlaqəsinin mövcudluğu məcburidir.

Kompüter 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 kompüter cinayətlərinin bəzi növlərinə aid edilməklə AR CM-nin Xüsusi hissəsinin 272.2 və 273.2-ci maddələrində öz əksini tapmışdır. Kompüter 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.

Kompüter informasiyası sferasında cinayətlər (kompüter cinayətləri) – bu cinayət qanunvericiliyi ilə nəzərdə tutulan məlumatların işlənməsinin avtomatlaşdırılmış sistemlərinə münasibətdə özgələrin hüquq və maraqlarının pozulması, eləcə də fiziki, hüquqi şəxslərin, cəmiyyət və dövlətin qanunla qorunan hüquq və maraqlarına zərər vurmaq məqsədilə törədilmiş təqsirdir.

1. Kompüter informasiyasına qanunsuz olaraq daxil olma (maddə 271 CM): Cinayətin bilavasitə obyekti qismində kompüter sistemi sahibinin bu sistemdə saxlanılan informasiyanın toxunulmazlığına olan hüququdur. Bu cinayət əməlinin obyektiv cəhəti isə qanunla qorunan kompüter 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:

- o, qanunsuz daxil olmanı həyata keçirən şəxs üçün yad olmalıdır;

- bu informasiya sürətinin sərbəst çıxarılmasından mühafizə olunmuş olmalıdır.

Qanunla qorunan kompüter 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 kompüter 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 kompüterin 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 kompüter 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 kompüter informasiyasına qanunsuz (sanksiyalaşdırılmamış) 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 (dolayı qəsd).

Bu cinayət əməlinin məqsəd və motivləri möxtəlif 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:

1. bu cinayət əməlinin qabaqcadan əlbir olan bir qrup şəxs tərəfindən törədilməsi;

2. 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;

3. bu cinayət əməlinin külli miqdarda ziyan vurmaqla törədilməsi.

İlk əlamətin təsviri AR CM-nin 34-cü maddəsində öz əksini tapmışdır. Həmin maddənin 2-ci hissəsində deyilir: "Qabaqcadan razılaşmaqla iki və ya daha çox şəxsin birgə iştirakı ilə törədilən cinayət qabaqcadan əlbir olan bir qrup şəxs tərəfindən törədilmiş cinayət hesab olunur." İkinci təsnifat əlamətini isə belə şərh etmək olar. Burada vəzifəli şəxslər qismində proqramçılar, EHM-nın operatorları, avadanlıqların sazlayıcıları, ixtisaslaşmış iş yerlərinin mütəxəssis-istifadəçiləri və s.

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 kompüter sistemində informasiya almağa, onu daxil etməyə və ya onda əməliyyatları həyata keçirməyə, həmçinin kompüter avadanlığının texniki xidmətini həyata keçirən və başqa qanuni əsaslarda kompüter sisteminə girişə malik olan şəxs başa düşülür. Kompüter sisteminə girişi olan şəxs bu cinayəti yalnız girişə malik olmadığı informasiyaya daxil olduğu halda törətmiş hesab olunur.

Üçüncü əlamət olan külli miqdarda ziyan dedikdə, CM-nin 190-cı maddəsinin qeydinə əsasən, ziyan şərti maliyyə vahidinin 7000 mislindən artıq məbləğə bərabər olmalıdır.

2. Elektron-hesablayıcı maşınlar üçün ziyan verici proqramlar yaratma, onlardan istifadə etmə və ya onları yayma (maddə 272): 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:

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

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

3. yuxarıda qeyd edilən hər iki növ proqramlardan istifadə etmə;

4. onları yayma;

5. belə proqramlarla yüklənmiş maşın daşıyıcılarından istifadə etmə;

6. 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.

Bütün bu əməllərin nəticəsi daha öncəki maddələrlə analojidir, fərq yalnız ondan ibarətdir ki, əməlin cinayət hesab olunması üçün proqramın işə salınması zəruri deyil. 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:

1. Cinayət əməlinin nəticələri sanksiyalaşdırılmamış (qanunsuz) olmalıdır;

2. Zərərverici proqramın özünün və ya proqramda belə dəyişikliyin mövcudluğu.

272-ci maddənin 2-ci hissəsində isə eyni əməllərin ehtiyatsızlıqdan ağır nəticələrə səbəb olması halı qeyd olunmuşdur. Cinayətin ehtiyatsızlıqdan törədilməsi CM-nin 26-ci maddəsində aşağıdakı şəkildə öz əksini tapmışdır:

Cinayətkarcasına özünəgüvənmə və ya cinayətkarcasına etinasızlıq nəticəsində törədilmiş əməl (hərəkət və ya hərəkətsizlik) ehtiyatsızlıqdan törədilmiş cinayət sayılır. (maddə 26.1. CM) Bunu 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 bilmiş, 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 cinayət törətmiş 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 şəklə salmaq üçün modifikasiya etdiyini dərk edir, bu proqramın digər EHM istifadəçiləri tərəfindən istifadəsi nəticəsində zərərli nəticələrə səbəb olacağını və ya səbəb olma ehtimalını öncədən 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. Azərbaycan Respublikası qanunvericiliyi ictimaiyyət üçün zərərli əməllər törətmiş, lakin cinayət məsuliyyətinə cəlb etmə yaşına çatmamış şəxslərə inzibati yolla tərbiyəvi xarakterli məcburi ölçülərin tətbiqini də nəzərdən keçirir.

3. Elektron hesablayıcı maşınların (EHM), EHM sisteminin və ya onların şəbəkələrinin istismarı qaydalarını pozma (maddə 273 CM): AR CM-nin 273-cü maddəsi EHM-lə, EHM sistemi ilə və ya onların şəbəkələri ilə işləməyə icazəsi olan şəxs tərəfindən EHM-in, EHM sisteminin və ya onların 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 kompüter sistemi və ya şəbəkəsi sahibinin bu sistem və ya şəbəkənin düzgün istifadəsi üzrə marağı çıxış edir.

Cinayətin obyektiv cəhəti kompüter sisteminin və ya şəbəkəsinin istifadə qaydalarının pozulması ilə əhəmiyyətli zərərin vurulmasına səbəb ola bilən hərəkət və hərəkətsizliklə xarakterizə olunur. Bu hal faktiki olaraq kompüter 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.

"Kompüter sistemindən istifadə qaydaları" dedikdə, səlahiyyətli dövlət orqanı tərəfindən, eləcə də texniki istifadə qaydaları, proqramlarla iş üzrə qaydalar, EHM və digər kompüter avadanlıqları istehsalçılarının müəyyən etdiyi qaydalar, həmçinin kompüter sistemi sahibi və ya onun göstərişi ilə qurulmuş olan qaydalar başa düşülür.

Kompüter 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 "Kompüter informasiyası sahəsində cinayətlər" adlı 30-cu fəsli kompüter 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 kompüterlər də sürətli templərlə insan fəaliyyətinin demək olar ki bütün sferalarını əhatə etmişdir. Bu dövr ərzində Azərbaycanda İnternet şəbəkəsi istifadəçilərinin sayında da əhəmiyyətli artım baş vermişdir. Belə ki, "İnternet World Stats"-ın məlumatına görə 2000-ci ildə bu rəqəm 12000 nəfər olduğu halda, 2012-ci ildə istifadəçilərin sayı 4,7 milyon nəfərə çatmışdır.[1] Bu isə o deməkdir ki, ölkə əhalisin 50 %-ə qədər internet istifadəçisidir. Kompüter cinayətlərinin mövcud tədqiqi metodları və bu cinayətlərin törədilməsinə görə məsuliyyəti müəyyən edən normaların müasir şərtlərə cavab verməməsi səbəbindən kompüter texnologiyalarının bu inkişafı ictimai təhlükəli əməllərin törədilməsinə şərait yaratmışdır. Kompüter informasiyası sferasında cinayətlərə görə məsuliyyət haqqında mövcud cinayət qanunvericiliyi isə kibercinayətkarlıq probleminin yalnız həlli görüntüsünü yaradır. Ən əsası isə bu normalar yalnız kompüter cinayətləri, yəni kompüterlər və kompüter informasiyası əleyhinə törədilən cinayətləri əhatə edir. Belə ki, bu normalarda kompüter vasitəsilə törədilən digər cinayətlərə görə məsuliyyət müəyyən olunmamışdır. Təbii ki, bu o demək deyil ki, qanunvericidən CM-nin kompüter cinayətlərinə həsr olunmuş fəslinə kompüter vasitəsilə törədilən lakin digər obyektlərə qəsd edən cinayətlər barəsində normaların əlavə edilməsi tələb olunur. Lakin bizim fikrimizcə, CM-də digər cinayət əməllərinin gizlədilməsi və ya onların törədilməsinin asanlaşdırılması məqsədilə kompüter və kompüter məlumatları ilə səlahiyyətsiz əməliyyatlara görə məsuliyyət nəzərdə tutulmalıdır. Beləliklə, qanunvericilikdə obyektini yalnız kompüter şəbəkələrinin fəaliyyətinin təhlükəsizliyi təşkil edən əməllər deyil, həmçinin digər kibercinayətlərdə əks olunacaq. Qeyd edək ki, MDB-ə üzv dövlətlərin Nümunəvi Məcəlləsi və onun kompüter informasiyası sahəsində cinayətlər barəsində fəsli

[1] Internet Usage in Asiahttp://www.internetworldstats.com/stats3.htm#asia

fikrimizcə kompüter cinayətlərinə münasibətdə AR CM-dən daha ətraflı sənəddir. Bu məcəllənin "informasiya təhlükəsizliyi əleyhinə cinayətlər" adlı XII fəslinə aşağıdakı 7 maddə daxildir.

- "Kompüter informasiyasına sanksiyalaşdırılmamış giriş";
- "Kompüter informasiyasının modifikasiya olunması";
- "Kompüter sabotajı";
- "Kompüter informasiyasının qanunsuz ələ keçirilməsi";
- "Kompüter sistemi və şəbəkəsinə qanunsuz girişi həyata keçirməyə imkan verən vasitələrin hazırlanması";
- "Zərərverici proqramların hazırlanması, istifadəsi və yayılması";
- "Kompüter 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 öncə qanunverici tərəfindən "EHM" termininin istifadəsi düzgün deyildir. Nəzərə alsaq ki, 271-ci maddədə "kompüter 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 "kompüter" sözünün tam sinonimi olaraq işlədilir. Lakin müasir zamanda texnologiyaların belə sürətli inkişafını nəzərə alsaq deyə bilərik ki, EHM və kompüterlər müasir mənalarına görə heç də sinonim sözlər deyildir. Bizim fikrimizcə "EHM" terminini daha universal və anlaşılan "kompüter" sözü ilə əvəz etmək daha məqsədə uyğun olardı. Onu da qeyd edək ki, MDB-ə üzv dövlətlərin Nümunəvi Cinayət Məcəlləsindədə "EHM" termini deyil, "kompüter" termini istifadə edilmişdir.

Onu da qeyd edək ki, qanunsuz olaraq daxil olma anlayışı alimlərin fikrincə, является оценочным, bu isə bir daha AR CM-nin 271-ci maddəsində hüquqi-texniki çatışmazlıqların mövcudluğunu sübut edir. 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, kompüterin ekranının şəklinin çəkilməsi. Kompüter 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, kompüter sistemlərinin normal fəaliyyətini, eləcə də informasiyanın saxlanması və göndərilməsini təmin etmək üçün cinayət qanunvericiliyi kompüter sistemlərinin müdafiə vasitələrini istifadə edən hər bir istifadəçinin kompüterini mühafizə etməlidir. Bununla belə, kompüter informasiyasının surətinin çıxarılmasına görə cinayət məsuliyyət MDB-ə üzv dövlətlərin Nümunə Məcəlləsində olduğu kimi ayrıca maddədə nəzərdə tutula bilər. Beləliklə, CM-nin 271-ci maddəsindən "kompüter informasiyasının sanksiyalaşdırılmamış ələ keçirilməsi", "informasiyanın sanksiyalaşdırılmamış modifikasiya edilməsi", "kompüter sabotajı" (kompüterlərin və kompüter 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 cinayətyaradan 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. Bizim fikrimizcə, 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 "kompüter dələduzluğu" – kompüter məlumatlarının daxil edilməsi, dəyişdirilməsi, silinməsi və ya təcrid olunması vasitəsilə özgənin əmlakının oğurlanması və ya özgəsinin əmlakına hüquqların ələ keçirilməsi və ya kompüter 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 kompüter texnologiyalarının 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, Rabitə və İnformasiya Texnologiyaları 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 Milli Təhlükəsizlik Nazirliyi əlaqələndirici qurum kimi müəyyənləşdirilib. Onlar 24/7

sistemində əlaqələndirici qurumlarla birgə işləyərək, real zaman ərzində müxtəlif ölkələrlə bu sahədə qanuna zidd əməllər baş verdikdə onunla mübarizə aparmaq üçün tədbirlər görməsi ilə bağlı mexanizm müəyyənləşdirə bilərlər. 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 "Kompüter 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:

- Kompüter sisteminə qanunsuz daxil olma (Maddə 271);
- Kompüter məlumatlarını qanunsuz ələ keçirmə (Maddə 272);
- Kompüter sisteminə və ya kompyuter məlumatlarına qanunsuz müdaxilə (Maddə 273);
- Kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (Maddə 273-1);
- Kompüter məlumatlarının saxtalaşdırılması (Maddə 273-2).

Qanuna əsasən kompüter sisteminə qanunsuz daxil olma, məlumatları qanunsuz ələ keçirmə, həmin məlumatları saxtalaşdırmaya, kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi, kompüter 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 tətbiqolunacaq. Əgər əməllər ictimai əhəmiyyətli infrastruktur obyektinin kompüter 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 "kompüter sistemi", "kompüter məlumatları" kimi anlayışların izahı verilmişdir. Belə ki, 271-ci maddənin qeydinə əsasən "kompüter 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. "Kompüter məlumatları" dedikdə isə, kompüter sistemində işlənməsi, emal edilməsi üçün yararlı olan istənilən informasiya (faktlar, məlumatlar, proqramlar və anlayışlar) başa düşülür.

Beləliklə, yeni yaranmış bir sahə olan kompüter 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.

FƏSİL III. MÜASİR ŞƏRAİTDƏ KİBERCİNAYƏTKARLIQLA MÜBARİZƏ SAHƏSİNDƏ XARİCİ TƏCRÜBƏDƏN İSTİFADƏ

İSTİQAMƏTLƏRİ

3.1 Kibercinayətkarlığa qarşı mübarizənin beynəlxalq hüquqi təminatı

Beynəlxalq təşkilatlar kibercinayətkarlığın təhlükəsini, transsərhəd xarakterə malik olduğundan bir tərəfli yanaşmanın məhdudluğunu, eləcə də bu problemin həlli üçün texniki tədbirlərlə yanaşı beynəlxalq qanunvericiliyin yaradılmasında beynəlxalq əməkdaşlığın zəruriliyini etiraf edirlər. İƏT, Avropa Şurası, Avropa Birliyi, BMT və İnterpol kimi təşkilatlar beynəlxalq səylərin koordinasiya olunmasında, eləcə də yüksək texnologiyalar sferasında cinayətlərlə mübarizədə beynəlxalq əməkdaşlığın qurulmasında mühüm rol oynayırlar. 1980-cı ildən Avropa Şurasının kibercinayətkarlıq haqqında Konvensiyasının qəbul olunmasına qədər kibercinayətkarlıqla mübarizə sahəsində beynəlxalq təşkilatların mühüm sənədlərinin qısa şərhi zəruridir. Bu sahədə beynəlxalq əməkdaşlığı daha yaxşı nümayiş etdirmək üçün məqsədə uyğun üsul xronoloji ardıcıllığın tətbiq edilməsidir. Belə ki, bu üsul sənədlərin hansı təşkilat tərəfindən qəbul edilməsindən asılı olmayaraq kibercinayətkarlıqla mübarizə məsələsinə vahid yanaşmanın formalaşdırılması üçün edilmiş səylərin inkişafını nümayiş etdirəcəkdir.

Kibercinayətkarlıq probleminin hərtərəfli tədqiqi və onunla beynəlxalq miqyasda cinayət-hüquqi mübarizə tədbirləri ilk dəfə İƏİT tərəfindən həyata keçirilmişdir. Bu təşkilat 1983-1985-ci illər ərzində kibercinayətlərə görə cinayət məsuliyyətini müəyyən edən normalarının harmoniyalaşdırılması imkanlarını tədqiq etmişdir. Bu təşkilatın gəldiyi nəticələr "Kompüterlərlə əlaqədar cinayətlər: hüquqi siyasətin təhlili" adlı məcmuədə qeyd olunmuşdur. Məcmuədə təşkilatın mövcud qanunvericiliyi təhlil edərək orada islahatların həyata keçirilməsi ilə bağlı təklifləri, eləcə də kriminal xarakterli hesab olunan əməllərin minimal siyahısını vermişdir. Buraya daxildir:

1. Maliyyə vəsaitlərinin və digər maddi nemətlərin qanunsuz yerdəyişməsi məqsədilə kompüter məlumatlarının və ya kompüter proqramlarının qəsdən dəyişdirilməsi, gizlədilməsi və silinməsi.

2. Kompüter məlumatlarının və ya kompüter proqramlarının saxtakarlıq edilməsi (niyyətilə) məqsədilə dəyişdirilməsi, gizlədilməsi və silinməsi.

3. Kompüterin və ya telekommunikasiya sisteminin fəaliyyətinə mane olmaq (niyyətilə) məqsədilə kompüter məlumatlarının və ya kompüter proqramlarının qəsdən dəyişdirilməsi, gizlədilməsi və silinməsi.

4. Kompüter proqramlarının kommersiya məqsədli istifadəsi və ya onun satışa buraxılması niyyətilə bu proqram sahiblərinin hüquqlarının pozulması.

5. Kompüter məlumatlarına və ya telekommunikasiya sistemləri məlumatlarına bu sistemin fəaliyyətinə görə məsul şəxsin icazəsi olmadan və ya təhlükəsizlik şərtlərinin pozulması ilə qəsdən törədilmiş giriş, eləcə də ələ keçirmə.

1985-ci ildən 1989-cu ilə qədər Avropa Birliyinin kompüterlərlə əlaqəli cinayətkarlıq məsələləri üzrə Xüsusi Komitəsi Avropa Birliyinin Nazirlər Komitəsi tərəfindən təsdiq edilmiş 13.09.1989-cu il tarixli 89 №-li Tövsiyəni işləyib hazırlamışdır.

Bu sənəddə kompüter cinayətləri ilə əlaqədar vahid cinayət-hüquqi strategiyanın hazırlanması üçün AB iştirakçı ölkələrinə tövsiyə edilən qanun pozuntularının siyahısı verilmişdir. Həmçinin burada kompüterlərlə əlaqədar bir sıra cinayətlərin kriminallaşdırılması məsələsində beynəlxalq konsensusun əldə edilməsi zəruriliyi də qeyd olunmuşdur. Tövsiyədə cinayətlərin 2 növ – "minimal" və "fakültativ (əlavə)" siyahısı öz əksini tapmışdır. "Minimal" siyahı özündə mütləq şəkildə beynəlxalq qanunvericiliklə qadağan edilməli olan və məhkəmə qaydasında təqibi həyata keçirilən əməlləri birləşdirir. "Əlavə" siyahıda isə həlli ilə bağlı beynəlxalq razılığa gəlinməsinin mürəkkəb olduğu qanun pozuntuları qeyd olunmuşdur.[1]

Qanun pozuntularının "minimal" siyahısına daxildir:

•kompüter dələduzluğu: Qeyri-qanuni iqtisadi xeyir əldə edilməsi niyyətilə üçüncü şəxslərə iqtisadi ziyan vurulmasına səbəb olan kompüter məlumatlarının və ya kompüter proqramlarının daxil edilməsi, dəyişdirilməsi, silinməsi, zədələnməsi, eləcə də məlumatlarının işlənməsi prosesinə digər müdaxilələr.

•kompüter informasiyasının saxtalaşdırılması: Kompüter məlumatlarının və ya kompüter proqramlarının daxil edilməsi, dəyişdirilməsi, gizlədilməsi, məhv edilməsi,

[1] URL:http://cm.coe.int/ta/rec/1989/89r9.htm

eləcə də müxtəlif üsullarla məlumatların işlənməsi prosesinə digər müdaxilələr, həmçinin milli qanunvericiliyə uyğun olaraq saxtalaşdırma hesab olunan qanun pozuntularına şərait yaradılması.

•kompüter məlumatlarının və proqramlarının zədələnməsi;

• kompüter sabotaji: Kompüter və telekommunikasiya sistemlərinin fəaliyyətinə mane olmaq məqsədilə kompüter məlumatlarının və proqramlarının sanksiyalaşdırılmamış (icazəsiz) məhvi, zədələnməsi, korlanması və digər müdaxilələr.

• icazəsiz giriş: Mühafizə vasitələrinin pozulması ilə kompüter sistemi və ya şəbəkəsinə sanksiyalaşdırılmamış icazəsiz giriş.

• icazəsiz ələ keçirmə;

• qorunan kompüter proqramlarının təkrar istehsalı;

• sxemlərin icazəsiz təkrar istehsalı.

"Əlavə" siyahı isə özündə aşağıdakıları birləşdirir:

• kompüter məlumatlarının və proqramlarının dəyişdirilməsi;

• kompüter cəsusluğu;

• kompüterlərin ixtiyarsız (icazəsiz) istifadəsi;

• Qorunan kompüter proqramlarının səlahiyyətsiz istifadəsi: İqtisadi xeyir əldə etmək və ya proqramın qanuni sahibinə zərər vurulması məqsədilə qanunla qorunan kompüter proqramının icazəsiz (səlahiyyətsiz) istifadəsi.

Tövsiyyələr ondan 10 il sonra qəbul edilmiş AŞ-nın "Kibercinayətkarlıq haqqında" Konvensiyasından fərqli olaraq Avropa ölkələrinin qanunvericiliklərinin inkişafına və dəyişdirilməsinə daha böyük təsir göstərmişdir. 1990-cı ildə BMT-nin cinayətkarlığın qarşısının alınması və qanun pozucuları ilə davranış üzrə VIII Konqressi BMT-yə üzv dövlətləri milli cinayət qanunvericiliyini müasirləşdirməklə, eləcə də kompüter cinayətkarlığı sahəsində məhkəmə təqibində və cəzalandırmada beynəlxalq standartların və prinsiplərin inkişafına yardım etməklə kompüter cinayətkarlığına qarşı mübarizədə səylərini artırmağa çağıran qətnamə qəbul etmişdir. Həmin ilin 14 dekabrında BMT-nin Baş Assambleyası tərəfindən üzv dövlətləri

1992-ci il 26 noyabr tarixində İƏİT Şurası informasiya sistemlərinin təhlükəsizliyinin təmin olunmasının rəhbər prinsipləri haqqında minimal standartların müəyyən olunduğu Tövsiyə qəbul etmişdir. Bu standartlar özündə cinayət qanunvericiliyinin informasiya sistemlərinin təhlükəsizliyinin pozulmasına görə məsuliyyəti müəyyən edən məcburi normalarını birləşdirir.

1995-ci ildə isə kompüter cinayətkarlığı halının tədqiqatının, eləcə də kompüter məlumatlarının və informasiyanın müdafiəsi haqqında mövcud cinayət qanunvericiliklərinin təhlilinin aparıldığı və bu sferada beynəlxalq əməkdaşlıq imkanlarının təhlil edildiyi "BMT-nin kompüterlərlə əlaqədar cinayətkarlığa nəzarət və bu cinayətlərinin qarşısının alınmasına dair Məlumat kitabçası" dərc edilmişdir.

Həmin ildə İnterpolun kompüter cinayətkarlığı üzrə ilk beynəlxalq konfransı keçirildi. Bu tədbir beynəlxalq aləmin kibercinayətkarlığın yayılması ilə bağlı narahatlığını bir daha təsdiq etdi. Konfrans iştirakçıları tərəfindən bu növ cinayətkarlığa qarşı istifadə oluna biləcək beynəlxalq rasional və effektiv mexanizmin yoxluğunun böyük narahatlığa səbəb olduğu vurğulanmışdır.

Sonrakı belə Konfranslar İnterpol tərəfindən 1995, 1996, 1998 və 2000-ci illərdə keçirilmişdir. İnterpolun kibercinayətkarlıqla mübarizəyə yanaşması "işçi qrupların" və "ekspert qrupların" fəaliyyətinin təşkili ilə konfrans iştirakçılarının informasiya texnologiyaları sferasındakı cinayətlərlə mübarizə təcrübəsinin istifadə olunmasından ibarətdir. İşçi qruplar regional təcrübənin öyrənilməsi məqsədilə yaradılmaqla Avropa, Asiya, Afrika və Şimalı və Cənubi Amerikada mövcuddur. İnterpolun informasiya texnologiyaları sferasındakı cinayətlər üzrə ilk işçi qrupu olan Avropa işçi qrupu 1990-cı ildə yaradılmışdır.

1997-ci ildə Böyük Səkkizliyin daxili işlər və ədliyyə nazirlərinin Vaşinqtondakı görüşündə "yüksək texnologiyalar sferasında cinayətlərlə mübarizənin 10 prinsipi" qəbul edilmişdir. 1999-cu ildə isə rəsmi beynəlxalq sənəd olmasa da mühüm əhəmiyyət kəsb edən Təhlükəsizlik və əməkdaşlıq Mərkəzinin (CİSAC) kibercinayətkarlıq haqqında Konvensiyası imzalanmışdır. Bu konvensiyada cinayət tərkiblərinin dəqiq xarakteristikası verilməsə də hansı əməllərin kriminal xarakterli olması müəyyən edilmişdir. Konvensiyada bu əməllərə aşağıdakılar aid edilir:

– kompüter sistemlərinə qanunsuz olaraq daxil olma;

– kompüter sistemlərinin fəaliyyətinin pozulması məqsədilə məlumatların idarə edilməsi;

– şəxsiyyətə və mülkiyyətə zərər vurulması məqsədilə məlumatların idarə edilməsi;

– kompüter təhlükəsizliyi tədbirlərinə müdaxilə;

– konvensiyada nəzərdən keçirilən cinayətlərin törədilməsi üçün zəruri olan avadanlıqların istehsalı və yayılması;

– qanunsuz fəaliyyətin həyata keçirilməsində kompüter texnologiyalarının istifadəsi;

– konvensiyaya tərəfdar olan dövlətlərin infrastrukturuna zərbələr vurmaq məqsədilə yuxarıda qeyd edilən pozuntulardan istənilən birinin törədilməsi.

2000-ci ilin mayında "Böyük Səkkizlik" dövlətləri əsas mövzusunun İnternet şəbəkəsində cinayətkarlıqla mübarizədə səylərin koordinasiya edilməsi məsələsinin təşkil etdiyi kibercinayətkarlıq üzrə Konfrans keçirmişdir. "Böyük Səkkizlik" dövlətlərinin bu məsələ ilə bağlı fikirləri qlobal informasiya cəmiyyətinin Okinavi Xartiyasında öz əksini tapmışdır. Bu xartiyanın 8-ci paraqrafında qeyd olunur: "Beynəlxalq əməkdaşlığın qlobal informasiya cəmiyyətinin inkişafına yönəldilmiş səyləri təhlükəsiz və cinayətlərdən azad olan kibermühitin yaradılması üzrə fəaliyyətlə müşayiət olunmalıdır. Bundan başqa kompüter şəbəkə və sistemlərinə icazəsiz daxil olma, eləcə də kompüter virusları kimi aktual problemlərin effektiv siyasi həllinin tapılması zəruridir.

2000-ci ilin iyun ayında AŞ-nın sammitində AŞ-na üzv 15 dövlətin başçıları 2002-ci ilin sonuna qədər kibercinayətkarlığa dair koordinasiyalaşdırılmış və ardıcıl bir yanaşmanın formalaşdırılmasına çağıran "Avropa elektron fəaliyyət planı"-nı qəbul etdilər. 1999-cu ilin oktyabrdan AŞ-nın gündəliyində olan bu məsələ çox illik səylərin məhsulu olaraq 2001-ci il 23 noyabr tarixində AŞ-nın kibercinayətkarlıq haqqında Budapeşt Konvensiyasının qəbul edilməsi ilə öz həllini tapdı. Bu qlobal

kompüter şəbəkəsində hüququ münasibətlərini tənzimləyən ən mühüm sənədlərdən biridir.

Bu gün Kibercinayətkarlıq haqqında Konvensiya telekommunikasiya hüquqları sferasının bazasını təşkil edən ən mühüm beynəlxalq-hüquqi aktlardan biridir. Onu qlobal informasiya cəmiyyətinin Okinavi Xartiyası ilə bir cərgəyə qoymaq olar. Lakin xartiyada informasiya kommunikasiya texnologiyalarının inkişafının ümumi konsepsiyasının qəbul edilməsindən söhbət gedirdisə, bu Konvensiyada real hüquqi tənzimləmə mexanizmləri öz əksini tapmışdır.[1]

Milli və beynəlxalq səylər bir-birini tamamlayaraq kibercinayətkarlıq probleminə qlobal diqqəti təmin edir, eləcə də bu problemin həllində atılacaq addımların koordinasiyasını və milli qanunvericiliklərin unifikasiyasını şərtləndirir. Dünyanın qırxdan çox dövləti kibercinayətkarlıqla beynəlxalq mübarizə strategiyasının formalaşdırılmasına cəlb edilmişlər. Onların bəziləri yüksək texnologiyalar sferasında cinayətlərlə mübarizə üzrə daha təkmil və praktikada istifadə olunan qanunvericiliyə malik olduğu halda, digərləri bu istiqamətdə hələ yeni-yeni addım atırlar. Beynəlxalq və üstmilli qurumların milli qanunvericiliklərdə islahatların keçirilməsində və kibercinayətlərin aşkara çıxarılmasının prosessual, texniki və digər vasitələrinin koordinasiya edilməsində böyük xidmətləri olmuşdur. Kibercinayətkarlıq sahəsində tədqiqatçı alim Ulrik Ziber belə bir qərara gəlmişdir ki, beynəlxalq səviyyədə həyata keçirilən tədbirlərlə milli cinayət qanunvericiliklərdə edilən islahatlar arasında sıx qarşılıqlı əlaqə mövcuddur.

Lakin milli qanunvericiliklərin formalaşdırılmasında və beynəlxalq səylərin koordinasiyasında müşahidə edilən bu inkişafa baxmayaraq, qlobal anlamda kibercinayətkarlıq haqqında qanunvericilik M. Qudman və S. Brennerin qeyd etdiyi kimi "yeni qanunlar, artıq mövcud olan qanunlar və qanunların olmamasından ibarət xaos" olaraq qalmaqdadır. Ekspertlər tərəfindən kibercinayətkarlıqla mübarizə üzrə qlobal strategiyaya uyğun olan, hərtərəfli milli startegiyanın inkişaf etdirilməsi zəruriliyi

[1]Окинавская Хартия глобального информационного сообщества – URL: http://www.internet-law.ru/intlaw/laws/okinava.htm

daim qeyd edilir. Belə ki, beynəlxalq səviyyədə həyata keçirilən səylər mütləq şəkildə ayrı götürülmüş dövlət səviyyəsində tədbirlərlə möhkəmləndirilməlidir.

Kibercinayətkarlıqla mübarizədə beynəlxalq əməkdaşlıq bu tip əməllərin bəzi ölkə qanunvericiliklərində kriminallaşdırıldığı halda, digərlərində cinayət əməli hesab olunmadığı şəraitdə mümkün deyildir. Faktiki olaraq, milli qanunvericiliklərdə mövcud bu fərqlər cinayətkarlar üçün xüsusi "baryer" rolu oynayaraq onların məsuliyyətdən yayına bilməsinə və cəzasız qalmasına xidmət edir.

İnformasiya cəmiyyətinin sərhədləri ilə yanaşı hətta getdikcə dövlətlərin fiziki sərhədlərinin silinməsinə səbəb olan qloballaşmadan öncə hər hansı bir əməlin kriminallaşdırılması qərarı yalnız dövlətə məxsus idi və bu beynəlxalq mühitə təsir göstərmirdi. Dövlətə yalnız öz vətəndaşlarına və onun ərazisində olan şəxslərə təsir göstərə bilmək vacib idi. Bununla yanaşı, 300-400 il bundan əvvəl hər hansı bir ölkə məsələn, İngitərə vətəndaşının digər bir ölkə məsələn, Çin ərazisində olması imkanı çox az idi. Lakin qlobal informasiya şəbəkəsinin meydana gəlməsi ilə ölkələr arasında mövcud "virtual" sərhədləri aşmaq üçün yalnız internetə çıxışı olan kompüter olması kifayətdir. Kibercinayətlər kibermühitin istənilən ərazisində, bu ərazinin hansı ölkənin yurisdiksiyasına aid olmasından asılı olmayaraq silahlana bilərlər. Onlar kompüter texnologiyalarının inkişafının bu sahədə münasibətləri tənzimləyən qanunvericiliyin inkişafını üstələməsi nəticəsində əmələ gələn hüquqi boşluqlardan uğurla istifadə edirlər. Bu problemin iki aspekti var: Birincisi, kibercinayət törətmiş şəxslər cəzalanmamış qalır, ikincisi, öz ölkəsində qanunlara riayət edən şəxslər kompüter texnologiyaları sferasındakı münasibətlərin cinayət-hüquqi tənzimlənməsindəki fərqlərə görə digər ölkədə məhkəmə təqibinə məruz qala bilərlər.

Daha əvvəl də qeyd edildiyi kimi qlobal informasiya şəbəkələrində sərhədlərin olmaması kibercinayətkarlıqla mübarizədə müəyyən ardıcıllığın olmasını və ölkələrin fəaliyyətinin koordinasiya edilməsini tələb edir. Amerika tədqiqatçıları S. Brenner və M. Qudman bu problemin iki həll yolunun mövcudluğunu iddia edirlər.

Birinci, kibercinayətlərə görə məsuliyyəti nəzərdə tutan universal vahid məcəllənin yaradılması. Bu halda kompüter texnologiyaları sferasında törədilən cinayətlər ayrı-ayrı milli qanunvericiliklə deyil, bu vahid beynəlxalq qanunla təqib ediləcək. Bu

isə kibercinayətkarlıqla mübarizənin cinayət-hüquqi tənzimlənməsinin milli qanunvericiliyin səlahiyyətindən çıxıb, beynəlxalq, üstmilli səviyyəyə qalxmasına, bununla da ayrı-ayrı dövlətlərin fəaliyyətindəki uyğunsuzluqların aradan qalxmasına səbəb olacaqdır. Lakin tədqiqatçıların fikrinə görə bu sistemin işləmə imkanı şübhəlidir. Belə ki, ölkələr öz səlahiyyətində olan idarəetmə funksiyasını beynəlxalq səviyyəyə qaldırmağa meyilli deyillər. Bu üsula alternativ variant isə yeni qanunların qəbulunda və ya mövcud qanunlarda islahatların həyata keçirilməsində dövlətlərin rəhbər tuta biləcəkləri müəyyən bir şablonun, prinsiplər dəstinin formalaşdırılmasıdır. Bu prinsiplər kibercinayətkarlıqla mübarizə üzrə milli qanunvericiliklərdə boşluqların və eləcə də hər hansı bir ölkə qanunlarının digərinin cinayət-hüquqi normaları ilə uyğunsuzluğunun olmamasının zəmanəti kimi çıxış edəcəklər. Avropa Şurası da məhz bu yolla gedərək "Kibercinayətkarlıq haqqında" Konvensiyanı qəbul etdi.

Cinayət-hüquqi tənzimləmənin funksiyası cəmiyyətdə sosial intizamın, dövlətin normal fəaliyyət göstərməsi və inkişafı üçün zəruri ictimai münasibətlərin qorunmasından ibarətdir. Hər bir ölkə hansı ictimai münasibətlərin cinayət-hüquqi mühafizəyə aid edildiyini özü müəyyən edir. Elə xüsusi əməllər var ki, onlar yalnız bir və ya bir neçə ölkədə cinayət hesab edilir. Bu isə ölkədə mövcud dini, etik normaların və ya siyasi rejimin mövcudluğundan irəli gəlir. Lakin elə cinayət növləri də var ki, onlar demək olar ki bütün dövlətlərin cinayət qanunvericiliklərində təsbit olunmuşdur. Bunlar:

1. şəxsiyyət əleyhinə cinayətlər (qətlə yetirmə, zorlama, sağlamlığa zərər vurma);

2. mülkiyyət əleyhinə cinayətlər (oğurluq, dələduzluq, mülkiyyətin məhv edilməsi);

3. dövlət hakimiyyəti əleyhinə cinayətlər (dövlətə xəyanət, casusluq, ədalət əleyhinə cinayətlər);

4. ictimai əxlaq əleyhinə cinayətlər.

İlk iki kateqoriya malum in se cinayətlər hesab olunurlar. Bu cinayətlərin mahiyyəti ictimai qanunlara və əxlaq normalarına ziddir. Onları qadağan etmədən cəmiyyət fəaliyyət göstərə bilməz. Ona görə də bu əməllərin həm

təsnifləşdirilməsində, həm də onların məhkəmə təqibində yüksək ardıcıllıq müşahidə olunur.

Milli qanunvericiliklərdə ən çox fərqlərin mövcud olduğu əməllər isə ictimai əxlaq əleyhinə cinayətlərdir. Belə ki, bunlar mənəvi və dini prinsiplərdən asılıdırlar.

Bütün yuxarıda sadalananlar yüksək texnologiyalar sahəsindəki cinayətlərə də tətbiq edilə bilər. Beynəlxalq tənzimləməyə daha çox insan həyatına, onun fiziki toxunulmazlığına, eləcə də hüquqi, fiziki şəxslərin və dövlətin mülkiyyətinə qəsd edən kibercinayətlər məruz qalır. Belə ki, bu cinayətlər də malum in se cinayətlər hesab olunurlar. Hətta belə cinayətlərin təyinində də müxtəlif ölkə qanunvericilikləri az və ya çox dərəcədə oxşardırlar. Lakin irqi və dini düşmənçiliyin təbliği ilə bağlı cinayətlərlə vəziyyət çox mürəkkəbdir. Çünki müxtəlif dövlətlərdə etik və dini prinsiplər o qədər güclü fərqlənirlər ki, bu məsələ ilə əlaqədar razılığın əldə olunması sadəcə mümkünsüz olur.

S. Brenner və M. Qudman kibermühitdə törədilən cinayətlərlə bağlı məsələlər üzrə ölkələr arasında razılığın əldə olunmasına həsr edilmiş "The Emerging Consensus on Criminal Conduct in Cyberspace" ("Kibermühitdə cinayət xarakterli davranışlarla bağlı formalaşan konsensus") adlı işində "barəsində konsensus əldə edilmiş kibercinayətlər" terminini təklif etmişlər. Bu növ kibercinayətlərə - barəsində kibercinayətlərlə mübarizə üzrə öz səylərini koordinasiya edən dövlətlərin həmin əməllərin cinayət hesab olunması məsələsində, eləcə də onların araşdırılması və məhkəmə təqibində razılıq əldə etdiyi və ya etməli olduğu cinayətlər aiddir. Onlar da ənənəvi cinayətlər kimi cinayət əməlinin obyekti olan cinayət qanunvericiliyi ilə qorunan ictimai münasibətlərin növündən asılı olaraq təsnifləşdirilirlər. M. Qudman və S. Brenner belə "barəsində konsensus əldə edilmiş kibercinayətlər"-in 4 növünü müəyyən edirlər. Bunlar şəxsiyyət əleyhinə, mülkiyyət əleyhinə, hakimiyyət əleyhinə və əxlaq əleyhinə olan cinayətlərdir.[1]

1. Şəxsiyyət əleyhinə cinayətlər: İstənilən bir dövlətin qanunvericiliyində şəxsiyyətin cinayət əməllərindən müdafiəsinə istiqamətlənmiş cinayət-hüquqi normalar mövcuddur. Lakin bununla belə şəxsiyyət əleyhinə cinayət törətmiş

[1] http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

kibercinayətkarlar qanunvericilikdəki boşluqlardan istifadə edərək məsuliyyətdən yayına bilərlər. Bu isə aşağıdakılarla əsaslandırılır:

– ölkədə kibermühitin əmələ gəlməsi ilə meydana çıxmış yeni cinayət növlərinə görə məsuliyyəti müəyyən edən normaların mövcud olmaması;

– şəxsiyyət əleyhinə cinayətlər üçün məsuliyyəti nəzərdə tutan cinayət qanununun tərifləri fiziki reallığa o qədər əsaslandırılmışdır ki, kompüter texnologiyalarının köməyi ilə virtual mühitdə törədilmiş cinayətlərə qanunun tətbiqi mümkünsüzdür.

Bununla belə kompüter texnologiyaları vasitəsilə törədilən və cinayət qurbanına fiziki zərərin vurulmasını nəzərdə tutan cinayətlərin araşdırılması və məhkəmə təqibi ilə bağlı ayrı-ayrı ölkə qanunvericiliklərində fərqlərin olması problem yaratmır. Belə ki, bu əməllər demək olar ki, bütün dövlətlərdə ənənəvi tərkiblərlə əhatə olunur. Şəxsiyyət əleyhinə olan və barəsində razılığa gəlinməsinin zəruri olduğu "problemli" cinayətlərə isə qeyri-fiziki, yəni izləmə və ya qorxutma kimi hallarla əlaqəli olan kibercinayətlər daxildir. İnternet öz anonimliyi ilə təhdid, qorxutma, şəxsi həyata müdaxilə, izləmə kimi bir çox cinayətlərə əlverişli şərait yaradır. Kibermühitdə törədilmiş belə cinayətlərə görə cinayət məsuliyyəti çox zaman ölkə cinayət qanunvericiliklərində öz əksini tapmır. Xüsusilə də çətinliklər cinayətkar və cinayət qurbanının müxtəlif dövlətlərin ərazisində olduğu hallarda meydana çıxır ki, belə situasiyaların da bəzən praktiki olaraq həll oluna bilməməsi qanunpozucusunun cəzasız qalmasına imkan yaradır.

2. Mülkiyyət əleyhinə cinayətlər: Şəxsiyyət əleyhinə cinayətlər kimi bu növ cinayətlər də hər bir dövlətin cinayət qanunvericiliyində mövcuddur. Bu cinayətlərin kibermühitdə kompüter texnologiyaları vasitəsilə törədilməsi belə əməllərin ixtisaslaşması və onların təqibi ilə bağlı problemlər yaradır. Əsas problem "mülkiyyət" anlayışının dərk olunması ilə bağlıdır. Belə ki, mülkiyyət münasibətlərinə qəsd edilməsi ilə bağlı qanunvericilik normalarında mülkiyyət əleyhinə cinayətlərin predmeti kimi həmişə hər hansı maddi bir şey, yəni fiziki, gözlə görünə bilən predmetlər nəzərdə tutulmuşdur. Bu isə öz növbəsində ənənəvi cinayət qanunlarının kibercinayətlərə də tətbiq olunması ilə bağlı problemlər yaradır. Belə ki, bu qanunlar informa-

siya, elektron məlumatlar və s. əleyhinə cinayətləri əhatə etmirlər. Mülkiyyətin qeyri-maddi obyektlərinə real həyatda xərclənilə bilən pul məbləğləri haqqında informasiyanın mövcud olduğu müəyyən məlumatlar, proqram təminatları və s. aid edilir. Lakin bəzi cinayətlərin ənənəvi qanunvericiliklə təqibi mümkün olu bilir. Məsələn, əgər xaker kompüter texnologiyalarından istifadə edərək özgənin bank hesabına daxil olub oradan öz hesabına külli miqdarda pul köçürmüşsə bu oğurluq əməli bəzi ölkələrdə mövcud cinayət qanunvericiliyi ilə təqib edilir. Pul vəsaitləri özgə hesabdan çıxarılıb cinayətkarın sərəncamına keçibsə cinayətkar onlara fiziki olaraq toxunmasa belə bu cinayət əməli bir çox ölkələrin oğurluq haqqında ənənəvi hüquqi normaları ilə əhatə olunur. Lakin əgər cinayətkar texnoloji tədqiqatlarla məşğul olan müəyyən şirkətin kompüter sisteminə daxil olmaqla gizli məlumatlarının sürətini əldə edib onlardan istifadə edirsə (satır və ya digər formalarda istifadə edir) bu əməl ənənəvi anlamda oğurluq hesab olunmur. Belə ki, cinayətkarın informasiyanı əldə etməsinə baxmayaraq şirkət bu məlumatdan məhrum olmur, yəni informasiya şirkətin mülkiyyətindən çıxmış hesab olunmur. Lakin bununla məlumatın dəyəri və məxfiliyi itir. Problemlər həmçinin əmlakın zədələnməsi kimi cinayətlərin təqibi prosesində də meydana çıxır. Ənənəvi hüquq normaları yalnız maddi əmlakın zədələnməsi və məhv edilməsi ilə bağlı məsuliyyəti müəyyən edir ki, bu səbəbdən də hər hansı bir saytı və ya qiymətli informasiyanı məhv edən cinayətkarı cinayət məsuliyyətinə cəlb etmək mümkün olmur.

Digər bir problem isə dələduzluğa dair normaların tətbiqi ilə bağlı meydana çıxır. Dələduzluq dedikdə, əmlakın oğurlanması, eləcə də yalan və ya etibardan sui-istifadə edilməsi yolu ilə özgənin əmlakına hüquqların əldə edilməsi başa düşülür. Lakin ənənəvi tərifl ər kompüter sistemlərinin "aldadılması" halını nəzərdən keçirmir.

Kompüter texnologiyalarının tətbiqi mülkiyyət əleyhinə yönələn, lakin cinayətlərin bütün mümkün tərkiblərindən heç biri ilə əhatə oluna bilməyən qanunpozuntuları doğurur. Məsələn, xaker hər hansı bir kommersiya müəssisəsinin saytına girişi bloklayır və sayta ziyarətçilərin daxil olması mümkünsüz olur. Təbii ki, bunun nəticəsində firma ziyan çəkir. Lakin bu əməl oğurluq hesab olunmur. Belə ki, xaker hücum etməklə müəssisənin gəlirini mənimsəmir və eləcə də əmlakın məhvinə səbəb

olmur. Çünki, sayta fiziki olaraq zərər vurulmamış və o məhv edilməmişdir. Bu hücum daxili kompüter sisteminə daxil olunmadan xaricdən törədildiyindən hətta kibermühitin sərhədlərinin aşılması halı kimi də nəzərdən keçirilə bilməz.

Bu səbəbdən də köhnə təriflərin müasirləşdirilməsi, yeni normaların qəbulu və onların müasir şəraitdə tətbiqi üçün yeni tərkiblərin – "konsensus əldə olunmuş kibercinayətlərin" tərkiblərinin yaradılması zəruridir.

3. Dövlət hakimiyyəti əleyhinə cinayətlər: Daha öncəki iki kateqoriyada olduğu kimi bu növ cinayətlərdə də kompüter texnologiyaları vasitəsilə törədilən əməlləri əhatə edən tərkiblər mövcuddur. Məsələn, dövlətə qarşı xəyanət və ya casusluq kimi ənənəvi tərkiblərdə cinayət əməlinin nəticəsindən danışılır və orada bu əməlin törədilmə üsulu nəzərdə tutulmur. Həmçinin sənədlərin saxtalaşdırılması halı da yeni tərkib yaratmır. Bununla belə problemlər mövcuddur və bu problemlər kütləvi qarışıqlığın yaradılması, dövlət hakimiyyətinin zorla dəyişdirilməsinə çağırışların edilməsi, milli düşmənçiliyinin qızışdırılması kimi cinayətlərin ixtisaslaşdırılması zamanı meydana çıxa bilər. Belə ki, bu cinayətlərin kompüter texnologiyaları vasitəsilə törədilməsi heç də həmişə ənənəvi tərkiblərdə əhatə olunmur. Bununla yanaşı ədalət əleyhinə cinayətlərlə mübarizə üzrə milli qanunvericilikdə islahatların keçirilməsi də zəruridir. Belə ki, bu cinayətlərin ənənəvi tərkiblərində məsələn, ədliyyə orqanlarının kompüter sistemlərinə hücumların edilməsi, məhkumlara dair məlumatların dəyişdirilməsi, eləcə də cinayətkarlar barəsində materialların məhv edilməsi və s. bu kimi cinayət əməlləri nəzərdə tutulmayıb. İlk baxışda bu məsələlərin yalnız milli səviyyədə həll olunmasının zəruriliyi və onların həlli ilə bağlı beynəlxalq səylərin koordinasiyasına ehtiyac olmadığı nəzərə çarpır. Lakin kibercinayətlərin transsərhəd xarakteri bu cinayətlərin tədqiqində dövlətlərin bu və ya digər səviyyədə bir-birindən asılı olduğunu aşkara çıxarır. Əgər kibermühitdə cinayət törədən şəxs hər hansı bir ölkədə ədalət əleyhinə cinayət üzrə milli qanunvericiliyində boşluqlar aşkar edib onlardan istifadə edərsə bu həmin ölkənin cinayət qurbanı olmuş vətəndaşlarına mənfi təsir göstərə bilər.

4. İctimai əxlaq əleyhinə cinayətlər:Konsensus əldə olunmuş kibercinayətlərin müəyyən olunması baxımından ictimai əxlaq əleyhinə cinayətlər kateqoriyasına aid

edilən əməllər daha problemli və mürəkkəb hesab olunur. Dünya ölkələrinin qanunvericilikləri bu məsələdə o qədər bir-birinə ziddir ki, bu əməllərdən hansılarının bütün dövlətlərdə təqib edilməsi üzrə beynəlxalq razılığın əldə oluna bilməsi şübhəlidir. Belə ki, bir dövlətdə ictimai əxlaq əleyhinə cinayət hesab olunan əməllər (avaralıq, qumar oyunları və s.) digər dövlətdə cinayət hesab olunmur.

İctimai əxlaq əleyhinə cinayətlər etik normalarla sıx bağlıdır. Bu normalar isə ayrı-ayrı dövlətlərdə əhəmiyyətli dərəcədə fərqlidirlər. Xüsusilə bu dini normalarla əlaqəli olan və milli qanunvericilikdə nəzərdə tutulan cinayətlərə aiddir. Konsensus əldə olunmuş əməllər kateqoriyasına həmçinin narkotik maddələr və spirtli içkilərin istifadə olunması kimi hallar da aid edilə bilmir.

Yuxarıda nəzərdən keçirilən 4 kateqoriya cinayət əməlləri ilə yanaşı elə cinayətlər də mövcuddur ki, eyni bir cinayət əməli ayrı-ayrı dövlətlərdə müxtəlif ictimai münasibət növlərinə qarşı qəsd hesab olunur. Məsələn, terrorizm bəzi ölkələrdə dövlət əleyhinə cinayət hesab olunduğu halda, digərlərində ictimai təhlükəsizlik əleyhinə, bir qrup ölkələrdə isə hətta insanın şəxsiyyəti və mülkiyyəti əleyhinə cinayət kimi nəzərdən keçirilir. Beləliklə "konsensus əldə edilmiş kibercinayətlərin" müəyyə edilməsi və bu cinayətlərlə mübarizə üzrə strategiyanın işlənib hazırlanmasında beynəlxalq səylərin koordinasiyası, eləcə də onların araşdırılması və cinayətkarların məhkəmə təqibi üzrə fəaliyyət aşağıdakıları nəzərdə tutur:

- şəxsiyyət əleyhinə cinayətlərin kiberizləmə kimi yeni növlərinin müəyyən edilməsi;

- mülkiyyət əleyhinə cinayətlər üzrə mövcud qanunvericilik normalarını yenidən nəzərdən keçirməklə bu normalarda qeyri-maddi mülkiyyət obyektlərinə qəsd olunması hallarının əhatə olunmasına nail olmaq;

- DNS-hücumları (Domain Name System) və informasiyanın zədələnməsinə görə məsuliyyəti nəzərdə tutan, mülkiyyət əleyhinə yeni cinayət növlərinin müəyyən edilməsi;

- ədalət əleyhinə cinayət üzrə normaların yenidən nəzərdən keçirilməsi ilə onlarda elektron dəlillərin dəyişdirilməsi, məhv edilməsi və ya saxtalaşdırılmasına yönəldilmiş əməllərin də öz əksini tapmasına nail olmaq;

- ədalətin təmin olunmasına maneələr yaradan cinayət növlərinin müəyyən edilməsi;

- ictimai əxlaq əleyhinə cinayətlər haqqında normalara yenidən baxmaqla kompüter texnologiyaları amilini də nəzərə almaq.

Ehtimal olunur ki, milli qanunvericilik normalarındakı uyğunsuzluqların aradan qaldırılması üzrə işlər məhz mülkiyyət əleyhinə kibercinayətlər kateqoriyası üzrə aparılacaq. Müəyyənedici amil kimi bu cinayət əməllərinin minimal xərclərlə böyük itkilər törətməyə qadir olması, eləcə də transmilli şirkətlərin, qlobal maliyyə bazarlarının işgüzar dairələrinin mülkiyyətlərinin təhlükəsizliyinin təmin olunmasında maraqlı olmaları çıxış edir. Lakin konsensusun əldə olunmasını ləngidən amillər də mövcuddur ki, bunlara bir çox kibercinayətkarlıq növlərinin milli qanunvericiklərdə artıq mövcud olan normaların istifadə olunması ilə araşdırıla bilməsi və eləcə də hansı əməllərin kriminal hesab olunması ilə əlaqədar dövlətlər arası razılığın əldə olunmasında çətinliklərin mövcud olmasıdır. Bununla yanaşı kibercinayətkarlıqla mübarizə üzrə effektli əməkdaşlığa nail olunması qanunvericiliyin və hüquqi terminlərin vahidliyini zəruri edir. Bu hal isə özü də konsensusun ələ olunması prosesini çətinləşdirə bilər. Lakin bütün bu çətinliklərə baxmayaraq, kibercinayətlərin təsnifləşdirilməsində və elektron əməllərin kriminallaşdırılması məsələsi üzrə ölkələr arasında razılığın əldə olunması kibercinayətkarlıqla effektli mübarizə üçün zəruridir.

Mütəxəssislər ümid edirlər ki, Avropa Şurasının "Kibercinayətkarlıq haqqında Konvensiyasının" qəbulu ilə başlanan bu proses nə vaxtsa uğurla tamamlanacaq və dünya dövlətləri kompüter texnologiyaları vasitəsilə törədilən əməllərdən hansılarının kriminal xarakterli olmasına dair razılığa gələ biləcəklər və bununla da kibercinayətlərlə mübarizə sferasında vahid cinayət-hüquqi qanunvericiliyin işlənib hazırlanmasına və istifadəsinə nail olacaqlar.

Qlobal kiberməkanın bir parçası olan Azərbaycanda iqtisadi cinayətkarlıq və onun xüsusi növü olan kibercinayətkarlıqla mübarizənin müasir vəziyyəti, eləcə də mübarizənin hüquqi təminat mexanizmi və təkmilləşmə istiqamətləri isə növbəti fəsildə daha ətraflı şərh olunacaqdır.

3.2 Kibercinayətkarlıqla milli hüquq çərçivəsində mübarizə sahəsində xarici ölkələrin təcrübəsi

Kibercinayətkarlıqla mübarizə üzrə müxtəlif ölkələrin milli qanunvericiliklərinin inkişaf tarixi kompüter cinayətkarlığının yaranması tarixi ilə bağlıdır və ətraflı təhlil edildikdə bəzi qanunauyğunluqlar aşkara çıxır. İnformasiya texnologiyalarının inkişafı və onların insan fəaliyyətinin getdikcə daha çox sferalarına daxil olması cinayət əməllərinin yeni formalarının yaranmasına səbəb olmuşdur. Bu isə öz növbəsində yeni-yeni əməllərin kriminallaşmasına, artıq mövcud cinayət qanunvericiliklərinə dəyişikliklərin edilməsinə və yeni normaların qəbul olunmasına gətirib çıxarmışdır.

Yüksək texnologiyalar sahəsində cinayətlərlə mübarizə sferasında cinayət qanunvericiliyinin dəyişdirilməsi yalnız texniki inkişafın deyil, eləcə də hüquq konsepsiyalarında baş verən fundamental dəyişikliklərin nəticəsidir. XX əsrin ortalarına qədər mövcud cinayət məcəllələri əsasən maddi obyektlərə mülkiyyət hüququnun qorunmasına xidmət edirdi. Lakin XX əsrin sonlarında informasiya cəmiyyətinin meydana gəlməsi qeyri-maddi obyektlərin və informasiyanın qorunması məsələsinin əhəmiyyətinin artmasına səbəb olmuşdur. Bu yeni obyektlər yeni hüquq normalarının qəbulunu tələb edirdi. Belə ki, onlar maddi nemətlərlə analoji qaydada müdafiə oluna bilmirdi. Cinayət əməllərinin yeni formalarının yaranması ilə dünya ölkələrinin cinayət qanunvericilikləri müxtəlif dəyişikliklərə məruz qalmışdır. Bu dəyişikliklər 5 istiqamətdə həyata keçirilmişdir. Kompüter cinayətkarlığının inkişafı tarixi ilə əlaqədar olan bu istiqamətlər kibercinayətkarlıqla mübarizə sahəsində cinayət-hüquqi, eləcə də cinayət-prosessual tənzimləmənin 5 sferasını əks etdirir. Həmin istiqamətlər aşağıdakılardır:

1. Məxfiliyin qorunması üzrə qanunvericilik. Cinayət qanunvericiliyində islahatların 1-ci istiqaməti məxfiliyin qorunması ilə əlaqədardır. Belə ki, 60-cı illərdə kompüterlər əsasən hərbi və elmi qurumlarda istifadə olunduğundan əsas təhlükə də məhz gizli məlumatlarının itirilməsi və onlara icazəsiz müdaxilənin baş verməsi idi. İlk islahatların həyata keçirilməsinə informasiya texnologiyalarının istifadəsi

vasitəsilə məlumatların toplanması, saxlanması və ötürülməsi üçün yeni imkanların meydana gəlməsi səbəb olmuşdur. Kompüter məlumatlarının müdafiəsi haqqında qanunvericilik aşağıdakı ölkələrdə meydana gəlmişdir: İsveç (1973), ABŞ (1974), Almaniya (1977), Avstriya, Danimarka, Fransa və Norveç (1978), Lüksemburq (1979 və 1982), İslandiya və İsrail (1981), Avstraliya və Kanada (1982), Böyük Britaniya (1984), Finlandiya (1987), İrlandiya, Yaponiya və Hollandiya (1988), Portuqaliya (1991), Belçika və İsveçrə (1992), İspaniya (1992 və 1995), İtaliya və Yunanıstan (1997). Braziliya, Hollandiya, Portuqaliya və İspaniyada hətta məlumatların qorunması ilə əlaqədar Konstitusiyaya dəyişikliklər də edilmişdir.

2. Kompüter şəbəkələrinin hücumlardan müdafiəsi və eləcə də iqtisadi cinayətlər üzrə qanunvericilik. Cinayət qanunvericiliyində dəyişikliklərin ikinci istiqaməti 70-ci illərdə kompüter texnologiyaları sferasında iqtisadi cinayətkarlığın (bankların kompüter şəbəkələrinə müdaxilələr, sənaye cəsusluğu və s.), 80-ci illərdə isə bir çox başqa sahələrdə də kompüter şəbəkələrinə qanunsuz müdaxilələrin artması ilə əlaqədar olmuşdur. Bütün bunlar 1980-ci ildən başlayaraq islahatların həyata keçirilməsinə gətirib çıxardı. İslahatların keçirilməsinə səbəb kimi həmin dövrdə mövcud olan cinayət-hüquq normalarının yalnız fiziki və maddi obyektlərin ənənəvi cinayət əməllərindən müdafiəsinə xidmət etməsi çıxış edirdi. Lakin iqtisadi kibercinayətkarlığın yeni formaları nəinki yeni qəsd etmə predmetlərinə, eləcə də yeni obyektlərə (kompüter proqramları, kompüter sistemləri) malikdirlər. Mövcud ənənəvi tərkiblər bu əməllərin təsnifi üçün uyğun deyildi, cinayət hüququnun analoji qaydada tətbiqi isə hüquq prinsiplərinə ziddir. Bu səbəbdən də mövcud normaların istifadəsi mümkün deyildi. Bütün bunlar bir çox ölkələrin iqtisadi kibercinayətkarlıqla və kompüter sistemlərinə qanunsuz müdaxilə ilə mübarizəni təmin edə biləcək yeni normalar qəbul etməsinə gətirib çıxardı. Cinayət qanunvericiliklərində dəyişikliklər İtaliya (1978), Avstraliya (1979), Böyük Britaniya (1981,1990), ABŞ (1980-ci illər), Kanada və Danimarka (1985), Almaniya (1986), Avstriya, Yaponiya və Norveç (1987), Fransa, Yunanıstan (1988), Finlandiya (1990,1995), Hollandiya (1992), Lüksemburq (1993), İsveçrə (1994), İspaniya (1995) və Malayziyada (1997) həyata keçirilmişdir.

3. İntellektual mülkiyyətin müdafiəsi. Cinayət-hüquqi islahatların 3-cü istiqaməti kompüter texnologiyaları sferasında intellektual mülkiyyətin müdafiəsi ilə əlaqədardır. Kompüter proqramları müəlliflərinin hüquqlarının qorunması üzrə normalar Filippin (1972), ABŞ (1980), Macarıstan (1983), Avstraliya, Hindistan və Meksika (1984), Çili, Almaniya, Fransa, Yaponiya, Böyük Britaniya (1985), Braziliya, Kanada, İspaniya (1987), Danimarka, İsrail (1988), İsveç (1989), Norveç (1990), Finlandiya (1991), Avstriya (1993), Lüksemburqda (1995) qəbul edilmişdir.

4. Qeyri-qanuni və zərərli informasiyadan müdafiə. Cinayət qanunvericiliyində islahatların 4-cü istiqaməti informasiya şəbəkələrində yerləşdirilmiş informasiyanın məzmunu ilə əlaqədar olmuşdur. Bu islahatlar öz başlanğıcını 1980-ci illərdən götürsədə, 1990-cı illərdə İnternet şəbəkəsinin yayılması ilə daha da sürətlənmişdir. Lakin qeyri-qanuni və zərərli informasiyanın İnternet şəbəkəsində yerləşdirilməsi problemi hələ də praktiki olaraq həll olunmaz xarakter daşıyır. Cinayət qanunvericiliyində bu istiqamətdə islahatlar həyata keçirən ölkələrə misal olaraq Böyük Britaniya (1994), ABŞ (1996) və Almaniya (1997) göstərilə bilər.

5. Cinayət-prosessual qanunvericilik. 1980-ci illərdən həyata keçirilməyə başlanılan cinayət-prosessual qanunvericilikdə dəyişikliklər Böyük Britaniya (1984), Danimarka (1985), ABŞ (1986), Kanada (1986, 1988, 1997), Almaniya (1989, 1996), Hollandiya (1992), və Avstriyada (1993) qəbul edilmişdir.

Təəssüflər olsun ki, milli qanunvericiliklərdə həyata keçirilən yuxarıda sadalanan bütün dəyişiklikləri hər bir ölkə fərdi şəkildə həyata keçirmişdir. Belə ki, bəzi ölkələr cinayət məcəlləsinə dəyişiklər edilməsini, digərləri isə kibercinayətkarlıqla mübarizəyə yönəlmiş xüsusi qanunların qəbul edilməsini üstün tutmuşlar. Ölkələrin bu sferada milli cinayət qanunvericilikləri olduqca müxtəlif və hətta bir-birinə ziddirlər. Daha əvvəl də qeyd edildiyi kimi milli cinayət qanunvericiliklərində eyniliklərin olmaması hətta bir region çərçivəsində - məsələn, Avropada, dövlət sərhədləri tanımayan bir hal olan kibercinayətkarlıqla effektiv mübarizə metodlarının inkişafını əhəmiyyətli dərəcədə ləngidir. Bununla belə aydındır ki, vahid normaların işlənib hazırlanması uzun bir prosesdir. Belə ki, 2001-ci ilin noyabr ayında qəbul olunmuş Avropa Şurasının "Kibercinayətkarlıq haqqında"

Budapeşt Konvensiyası qəbul olunmasından 3 il sonra qüvvəyə minmişdir. Lakin hələ də Avropa dövlətlə rinin qanunvericiliklərində unifikasiya istiqamətində ciddi dəyişikliklər baş verməmişdir. Çünki Konvensiyanın qüvvəyə minməsi üçün onun 5 dövlət tərəfindən ratifikasiya olunması zəruri idi ki, bu dövlətlərdən də minimum 3-ü Avropa Şurasının üzvü olmalı idi. Budapeşt Konvensiyası 2003-cü ildə imzalansa da 37 dövlətdən yalnız 4-ü - Albaniya, Xorvatiya, Macarıstan və Estoniya tərəfindən ratifikasiya olundu. 2004-cü ilin 18 mart tarixində Litvanın da bu siyahıya daxil olması ilə həmin ilin 1 iyul tarixində Konvensiya qüvvəyə mindi.

Yuxarıda sadalanan problemlərə baxmayaraq ABŞ, İtaliya, Almaniya və s. kimi ölkələr də var ki, kibercinayətkarlıq haqqında qanunvericilikləri kifayət qədər yaxşı formalaşdırılmış, həmçinin praktikada da tətbiq edilir.

Avropa, Asiya və Amerika dövlətlərinin cinayət qanunvericiliklərinin növbəti müqayisəli təhlili ayrı-ayrı ölkələrin kibercinayətkarlıqla mübarizə problemini milli səviyyədə necə həll etdiklərini ətraflı nümayiş etdirir.

Ölkə qanunvericiliklərinin müqayisəli təhlili yuxarıda qeyd olunmuş milli qanunvericiliklərdə edilmiş dəyişikliklərin təsnifatı əsasında formalaşdırılmışdır. Lakin burada hüquq normaları törədilmiş qəsdin obyektinə görə təhlil edildiyindən daha ətraflı xarakter daşıyır.

Təhlilin bu üsulu daha məqsədə uyğun hesab olunur. Belə ki, bu üsul aşağıdakıları ayrı-ayrılıqda ətraflı təhlil etməyə imkan verir:

- məlumatların məxfiliyinin qorunması haqqında normalar;
- kompüter və kompüter şəbəkələrinə səlahiyyətsiz daxil olmağa görə məsuliyyət haqqında normalar;
- kommersiya sirrinin qorunması haqqında normalar;
- kompüter və kompüter şəbəkələrinin sabotajdan müdafiəsi haqqında normalar;
- iqtisadi kibercinayətlər haqqında normalar; (xüsusilə kompüter dələduzluğu);
- göstərilən normalarda öz əksini tapmış və kibercinayətkarlığın müxtəlif növlərinin qarşısının alınmasına yönəlmiş digər hallar.

Təhlilin əsası kimi digər kriteriyalarda götürülə bilər. Məsələn: ölkələrin kibercinayətkarlıqla mübarizəyə yönəlmiş cinayət hüquq normalarının həcminə görə aşağıdakı bölgüsü aparıla bilər.

- kifayət dərəcədə yaxşı formalaşdırılmış və həcmli xüsusi qanunvericiliyi olan dövlətlər;

- kibercinayətkarlıqla mübarizəyə yönəldilmiş az saylı normalara malik dövlətlər və ya göstərilən əməllərin cinayət təqibinin "köhnə", artıq mövcud normalar əsasında həyata keçirildiyi dövlətlər;

- kibercinayətlər və kompüter cinayətləri haqqında xüsusi cinayət qanunvericiliyinə malik olmayan, həmçinin kibercinayətlərə görə inzibati məsuliyyətin nəzərdə tutulduğu dövlətlər;

Milli cinayət qanunvericiliklərinin müqayisəli təhlilini çətinləşdirən hal isə məhz bəzi dövlətlərdə kibercinayətkarlıq haqqında xüsusi normaların olmamasıdır. Lakin mütəxəssislər qeyd edirlər ki, həmin dövlətlərdə bu cinayət əməllərinin araşdırılması "köhnə" normalar əsasında aparılır. Məsələn, kibercinayətkarlıqla mübarizə sahəsində qanunvericiliyin tədqiqi ilə məşğul olan Avropa mütəxəssisləri hesab edirlər ki, Finlandiyada xidmətdən imtina və ziyanverici proqramların yayılması kimi kriminal əməllərin cinayət təqibi "Rabitənin pozulması haqqında Akt"-a (1894) uyğun olaraq həyata keçirilir. Bu akt çox köhnə olsa da onun kommunikasiya sistemlərinin işinin qəsdən pozulmasına görə cəza tədbirini (2 ilə qədər azadlıqdan məhrumetmə) nəzərdə tutan normaları indiki dövrdə də aktualdır. Qanunvericiliyin təhlilində belə normaların mövcudluğu da nəzərə alınmalıdır.

Qlobal telekommunikasiya sistemlərində məlumatların məxfiliyinin müdafiəsi haqqında qanunvericilik: Maddi obyektlərdən fərqli olaraq informasiya obyektlərinin qorunması zamanı cinayət qanunvericiliyi yalnız informasiya sahibinin maraqlarını deyil, həmçinin informasiyanın məzmununun bilavasitə toxunduğu üçüncü şəxslərin maraqlarını da müdafiə etməlidir. Lakin ənənəvi cinayət qanunvericiliyində əsasən şəxsi həyat haqqında məxfi informasiyanın toxunulmazlığının müdafiəsi nəzərdə tutulurdu və bu qanunvericilik informasiya texnologiyaları vasitəsilə məlumatların yeni saxlanma, toplanma və göndərilmə üsulları şəraitində informasiyanın qorunması

üçün yetərli deyildi. Bu isə 1970-ci ildən başlayaraq ölkələrin milli qanunvericiliklərində dəyişikliklər etməsinə gətirib çıxardı. Bu dəyişikliklərin çox hissəsi inzibati qanunvericilikdə olsa da, telekommunikasiya şəbəkələrində və kompüterlərdə saxlanılan məlumatların məxfiliyinin pozulmasına görə cinayət məsuliyyətini müəyyən edən qanunlar da qəbul edilmişdir. Müxtəlif dövlətlərin bu cinayət qanunvericilikləri bir-birindən kəskin şəkildə fərqlənirlər. Buna isə ayrı-ayrı dövlətlərdə məxfiliyin pozulması üzrə cinayət məsuliyyətinə səbəb olan əməllərin fərqli qiymətləndirilməsi və cinayət qanunvericiliyin bu məxfiliyin müdafiə olunmasında oynamalı olduğu roldan asılıdır. Məsələn, Almaniyada elektron və eləcə də digər daşıyıcılarda saxlanılan məlumatların məxfiliyinin pozulmasına görə məsuliyyət üçün ayrıca olaraq CM-nin 202a maddəsi nəzərdə tutulmuşdur. Bu maddədə açıq aydın onun yalnız bu növ məlumatlara aid edildiyi göstərilmişdir. Bu maddə şəxsi həyata dair sirrlərin və toxunulmazlıqların pozulmasını nəzərdə tutan 15 №-li bölməyə daxil olmaqla qeyri-qanuni şəkildə onlar üçün nəzərdə tutulmayan və xüsusi qorunan məlumatları əldə etmiş şəxslər üçün məsuliyyəti müəyyən edir.

Finlandiyanın CM-sində elektron məlumatların qorunmasına yönəldilmiş üç maddə (CM, fəsil 28, maddə 1,2,3) nəzərdə tutulmuşdur. 3-cü maddə birbaşa olaraq kompüter məlumatlarının, o cümlədən elektron poçtların, kompüter şəbəkələri ilə göndərilən məlumatların məxfiliyinin pozulmasına görə məsuliyyəti müəyyən edir. Digər 2 maddə isə ümumi xarakter daşıyaraq informasiyanın məxfiliyinin pozulması halında praktiki olaraq tətbiq edilir. Əksər ölkələr elektron məlumatların qorunmasını cinayət qanunvericiliyində ayrıca maddə kimi qeyd etməyərək onu rabitə sirrinin saxlanmasının və ya şəxsi həyatın toxunulmazlığının bir aspekti kimi nəzərdən keçirir. Belə ki, İspaniya CM-sində bu hal şəxsi məlumatların, o cümlədən elektron şəkildə - məsələn, elektron poçtda saxlanılan məktubların, telekommunikasiya və digər kommunikasiya sistemləri vasitəsilə ötürülən məlumatların aşkara çıxarılması və yayılmasına görə məsuliyyət şəklində öz əksini tapır. Bundan başqa İspaniya CM-nin 200-cü maddəsi göstərilən vəziyyətləri hüquqi şəxslərin informasiyasına da aid edir. Ümumiyyətlə, məlumatların məxfiliyi və onun qanunsuz ələ keçirilmədən qorunması haqqında normalar elə formalaşdırılmışdır ki, onlar telekommunikasiya,

eləcə də digər rabitə sistemləri vasitəsilə göndərilən məlumatların məxfiliyinin müdafiəsinə istiqamətlənmişlər.

Kompüter və kompüter şəbəkələrinə səlahiyyətsiz daxil olma:Daha öncə də qeyd edildiyi kimi ölkələrin cinayət qanunvericiliklərində edilən islahatların ikinci istiqaməti (1980-ci ildən başlayaraq) olmaqla həyata keçirilməsinin əsas səbəbi yüksək texnologiyalar sferasında iqtisadi cinayətlərinin miqyasının genişlənməsi olmuşdur. Cinayət qanunvericiliyinə bu dəyişikliklərin edilməsini kibercinayətkarlığın yeni formalarının yalnız cinayət-hüquqi müdafiənin ənənəvi obyektlərinə deyil, elektron hesablar, kompüter proqramları, elektron sənədlər kimi yeni "duyulmayan" obyektlər üçün də təhlükə yaratması zəruri etmişdir.

Kibercinayətkarlığın yeni formaları həmçinin ənənəvi cinayət əməllərinin törədilməsinin yeni formalarını - məsələn, insanların aldadılması yerinə kompüter sistemlərinin "aldadılması"nı da nəzərdə tuturdu. Dəyişikliklər 2 yolla həyata keçirilmişdir: 1-ci bir sıra dövlətlər "köhnə", yəni artıq mövcud normaların fəaliyyət dairəsini genişləndirmiş, digərləri bilavasita və ya dolayısı ilə kompüter vasitəsilə törədilən iqtisadi cinayətlər haqqında xüsusi qanunlar qəbul etmişlər. 1980-ci illərin əvvəllərində bu qanunlar əsasən kompüter dələduzluğu haqqında qanunlar olsa da, daha sonralar bu cinayətlərin siyahısı kompüter sabotajı, casusluq, kompüter və kompüter sistemlərinə qanunsuz daxil olma kimi əməllər hesabına genişlənmişdir. Nəticədə məhz kompüter sistemlərinə və kompüterlərə qanunsuz daxil olmaya görə məsuliyyəti nəzərdə tutan qanunvericilik iqtisadi kibercinayətlərin qarşısının alınması üçün "baza" hesab olunmağa başladı. Buna səbəb isə iqtisadi kibercinayətlərin çox hissəsinin "kənardan", səlahiyyətsiz şəxslər tərəfindən qeyri-qanuni daxil olmaqla törədilməsi oldu.

Kompüterlərin kəşf olunmasına qədər də cinayət qanunvericiliyinin yazışmaların, telefon və teleqraf əlaqəsinin məxfiliyini qoruyan normaları mövcud idi. Yüksək texnologiyaların inkişafı ilə kompüterlərin bazasında saxlanılan məlumatların qorunması zəruriliyi, "rabitə sirri, məxfiliyi" anlayışını genişləndirməyi tələb etdi. Bir çox dövlətlərdə kompüter və kompüter şəbəkələrini mövcud cinayət-hüquq normaları vasitəsilə hücumlardan müdafiə etmək qeyri-mümkün idi. Belə ki, bir çox dövlətlərin,

məsələn, Almaniya, İtaliya, Hollandiya, ABŞ-ın məlumatların ələ keçirilməsi haqqında ənənəvi qanunları yalnız şifahi əlaqənin ələ keçirilməsinə və daha çox rabitə sirrinin cinayət-hüquqi mühafizəsinə istiqamətləndirilmişdir. Bununla yanaşı xüsusi mülkiyyətin sərhədlərinin pozulmasına görə məsuliyyət haqqında normalar da istifadə oluna bilmirdi. Beləliklə, kompüter məlumatlarına qanunsuz daxil olma hallarının getdikcə artması kompüter, kompüter məlumatları və sistemlərinə səlahiyyətsiz daxil olma və ya onların qanunsuz istifadəsi haqqında yeni qanunların qəbul olunmasına gətirib çıxardı. Bu qanunlar Avstraliya, Kanada, Danimarka, Almaniya, Finlandiya, Fransa, Hollandiya, Norveç, İspaniya, İsveç, Böyük Britaniya, İsveçrə, ABŞ-da qəbul edilmişdir. Sonralar qanunsuz olaraq daxil olmaya görə məsuliyyəti müəyyən edən belə qanunlar Belçika və Yaponiyada da qəbul olundu.

Lakin bəzi ölkələrdə belə əməllər kriminallaşdırılmamışdır. Məsələn Avstriya. Avstriyanın 2000-ci ildə qəbul olunmuş "Məxfi məlumatlar haqqında Akt"-nın 52-ci maddəsində məlumatlara qanunsuz daxil olmaya görə inzibati məsuliyyət müəyyən olunmuşdur. Qanunsuz daxil olma halını kriminallaşdıran normalar isə mahiyyət etibarı ilə fərqlidirlər. Belə ki, Danimarka, İngiltərə, Yunanıstan, ABŞ-ın bir çox ştat-larında məlumatlara istənilən qanunsuz daxil olma kriminal xarakter daşıyır. Digər ölkələrdə - Almaniya, Hollandiya, Norveçdə cinayət məsuliyyətini müəyyən edən normalar yalnız təhlükəsizlik tədbirləri ilə qorunan və ya xüsusi nəzarət altında olan, o cümlədən qanunla qorunan məlumatlara qanunsuz daxil olma halı baş verdikdə tətbiq edilir. Məlumatlara səlahiyyətsiz daxil olma halının cinayət hesab olunmasının şərtlərinə aşağıdakılar aid edilir:

- cinayətkarın zərər vurmaq niyyəti (Kanada, Fransa, İsrail, Yeni Zellandiya, Şotlandiya);
- informasiyaya zərərin vurulması, dəyişdirilməsi və ya daha sonrakı istifadəsi məqsədilə informasiyanın ələ keçirilməsi (ABŞ-ın bəzi ştatları);
- informasiyaya istənilən minimal zərərin vurulması (İspaniya).

Bəzi ölkələr – məsələn Böyük Britaniya bu yanaşmaları kombinasiya edib "sadə" qanunsuz daxil olma və ixtisaslaşdırılmış qanunsuz daxil olmanı kriminal-laşdırır. Misal kimi Böyük Britaniyanın 1990-cı il tarixli "Kompüterdən sui-istifadə

halları haqqında Akt”-nı göstərə bilərik. Bu aktın 1-ci paraqrafında “kompüter məlumatlarına səlahiyyətsiz daxil olma”-ya görə məsuliyyət müəyyən edilmişdir. Bu paraqrafda kompüterlərdən onların hər hansı funksiyasını yerinə yetirmək, hər hansı proqrama daxil olmaq və ya məlumatı əldə etmək məqsədilə qanunsuz istifadə etmə nəzərdə tutulur. Bu “sadə” daxil olma hesab olunur. “Kompüterdən sui-istifadə halları haqqında Akt”-ın 2-ci paraqrafı “digər cinayətləri törətmək məqsədilə səlahiyyətsiz daxil olma”-ya görə məsuliyyəti nəzərdə tutur. Bu isə ixtisaslaşdırılmış tip daxil olma hesab olunur. Bu məsuliyyət həm cərimə şəklində, həm də 6 aya qədər azadlıqdan məhrum etmə şəklində tətbiq edilir. Daha ciddi cinayətlərdə hətta 5 ilə qədər azadlıqdan məhrum etmə müəyyən edilə bilər.[1]

Ticarət və sənaye sirrinin mühafizəsi: Qanunvericilikdə informasiya mülkiyyət hesab olunsa da ənənəvi normalarda mülkiyyətin oğurlanması halı kimi əmlakın və ya əmlaka olan hüququn cinayətkarın və ya üçüncü şəxsin xeyrinə geri qaytarılmamaq şərtilə ələ keçirilməsi nəzərdə tutulur. Bununla yanaşı mülkiyyətçini əmlakdan məhrum etmə və onu öz xeyrinə istifadə etmə mütləq hal kimi nəzərdən keçirilir. Kommersiya və sənaye sirrlərinin oğurlanması halının fərqli cəhəti isə onun kommersiya sirrinin mövcud olduğu informasiyanın sadəcə olaraq sürətinin çıxarılması ilə həyata keçirilə bilməsidir. Məsələn, bu informasiyanın cinayətkar və ya üçüncü şəxs tərəfindən oxunması onun sahibkarın mülkiyyətindən çıxmasına səbəb olmur. Lakin bununla belə informasiya öz dəyərini – qiymətlilik və məxfiliyini itirir.

Ölkələrin kommersiya sirrinin elektron daşıyıcılara daxil olmaqla oğurlanmasından qorunması haqqında milli qanunvericiliklərdə müxtəlif terminlərdən istifadə olunur. Bu cinayətlər həm “iqtisadi cəsusluq”, “işgüzar cəsusluq”, həm də “ticarət sirlərinin oğurlanması” kimi adlandırıla bilər. Normaların konstruksiyası və yerləşməsi də müxtəlifdir. Bu normalar daha çox biznes və ya bazar əleyhinə cinayətlər bölməsində (Finlandiya, İspaniya) və ya kompüter və telekommunikasiya cinayətləri bölməsində qeyd edilirlər. Cəsusluq və kommersiya sirrinin elektron qəsdlərdən qorunmasına xidmət edən qanunvericiliyə ən yaxşı nümunə istehsal sirrlərinin cinayət hüquqi mühafizəsi haqqında ABŞ qanunvericiliyidir. Bu normalar ABŞ

[1] URL:http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm.

qanunvericiliyinə 11 oktyabr 1996-cı ildə daxil edilmişdir. İstehsal sirrlərinin mühafizəsinə ABŞ Məcəlləsinin 90-ci fəslinin 18-ci bölməsi, xüsusilə "İqtisadi cəsusluq" adlı 1831-ci və "Ticarət sirrlərinin oğurlanması" adlı 1832-ci maddələri həsr olunmuşdur.[1]

ABŞ-dan fərqli olaraq Avropa ölkələrində kommersiya sirrini təşkil edən məlumatların istənilən ələ keçirilməsi "cəsusluq" termini ilə ifadə edilir. Belə ki, Finlandiya CM-nin 30-cu fəslinin "Kommersiya cəsusluğu" adlı 4-cü maddəsi kommersiya sirrinin oğurlanmasına görə məsuliyyəti müəyyən edir. İspaniya CM-nin 278-ci maddəsi isə kommersiya sirrinin mövcud olduğu elektron məlumat və informasiyaya kompüterlərlə səlahiyyətsiz daxil olmaya görə məsuliyyəti müəyyən edir.

İsveçrənin CM-də "sənaye cəsusluğu" və "ticarət sirri" terminləri istifadə olunmur. Bu məcəllənin kommersiya və digər sirrlərin mühafizəsinə həsr olunmuş 143-cü maddəsi "Məlumatların qanunsuz əldə edilməsi" adlanır və qərəzli şəkildə gəlir əldə etmək məqsədilə elektron və digər bu kimi vasitələrlə məlumatların səlahiyyətsiz toplanması və göndərilməsi hallarını cinayət hesab edir.

Kompüter sabotajı və zərərverici proqramların yayılması: 1980-ci illərə qədər kompüter məlumatlarının və saytların zədələnmələrdən və xuliqanlıqdan müdafiəsi əmlaka zərərin vurulması və vandalizm haqqında normalar vasitəsilə təmin edilirdi. Lakin bu normalar maddi obyektlərin müdafiəsinə yönəldiyindən yalnız hər hansı daşıyıcılarda saxlanılan informasiyanın, yəni daşıyıcının tamlığını müdafiə edə bilirdi. Bəzi dövlətlərdə Avstraliya, Belçika cinayət-hüquqi normalarında informasiya daşıyıcısını məhv etmədən informasiyanın məhv edilməsi halı əmlaka zərərin vurulması kimi qiymətləndirilmir və bu normaların təsir dairəsinə daxil edilmirdi. Digər dövlətlərdə vandalizm və ya əmlaka zərərin vurulması haqqında normalar kompüter məlumatlarına və saytlara da tətbiq edilməklə yanaşı, informasiyaya zərər vurulması halının qəbul edilməsi üçün informasiya daşıyıcısına da zərərin vurulması halının mövcudluğu tələb edilmirdi. Xarici alimlərin fikrincə, bu normalardan bəziləri hazırda da uğurla tətbiq edilir. Bu normalar Danimarka CM-nin özgənin mülkiyyətinin yerdəyişməsi və məhv edilməsinə görə məsuliyyəti müəyyən edən 291-ci

[1] http://www4.law.cornell.edu

maddəsi, İsveç CM-nin maddi ziyan vuran cinayətlərə (həmçinin informasiyaya zərərin vurulması halında da tətbiq edilir) həsr olunmuş 12-ci fəsli, Yapon CM-nin 258-ci (rəsmi sənədlərə zərər vurulması) və 259-cu (şəxsi sənədlərə zərər vurulması) maddələridir. [1] Lakin bununla belə göndərilən, amma yaddaşda saxlanılmayan məlumatların göndərilmə prosesində məhv edilməsi kimi problemlər ortaya çıxırdı. Bu problemi həll edən yeni qanunvericilik Kanada, Danimarka, Almaniya, Finlandiya, Fransa, Yaponiya, Hollandiya, İspaniya, İsveç, Böyük Britaniya, ABŞ-da formalaşdırıldı. Bununla belə ayrı-ayrı dövlətlərdə bu proses müxtəlif üsullarla həyata keçirildi. Bəzi ölkələrdə - məsələn Finlandiyada artıq mövcud olan vandalizm və əmlaka zərər vurulması haqqında normalarda dəyişiklik edildi. Digərlərində (xüsusilə Yaponiyada) yeni nomalar bütün növ məlumat və sənədləri əhatə edir. Almaniya, Fransa, Hollandiya, İspaniya, Böyük Britaniyada isə kompüter məlumatlarının tamlığının müdafiəsi haqqında xüsusi normalar qəbul edilmişdir.

Virusların yayılması haqqında normaların yaradılmasında ölkələr daha irəliyə gedərək virus proqramlarının yaradılması və yayılması haqqında normalar qəbul etmişlər. Bu normalarda əməlin cinayət hesab olunması üçün onun müəyyən bir kompüterə qəsdən istiqamətlənməsi, eləcə də zərərin vurulması mütləq şərt kimi tələb edilmir. Məsələn, Böyük Britaniyada belə bir qəsdin müəyyən bir kompüterə istiqamətlənmiş olmasının təsdiqi zəruri deyil. O, istənilən bir kompüterə zərər vurulmasına yönəldilə bilər və bu hal artıq cinayət hesab edilir.

ABŞ-ın 6 ştatı (Kaliforniya, Nebraska, İllinoys, Men, Minnesota, Texas) ilk dəfə virus probleminə yanaşaraq kompüter və ya kompüter sistemlərinə virus və ya zərərverici proqramların yeridilməsinə görə məsuliyyəti müəyyən edən qanunlar qəbul etmişlər.

Problemə belə yanaşma Avropa ölkələrində də müşahidə olunmaqdadır. Məsələn, İtaliya CM-nə kompüter sistemlərinə zərərin vurulması və ya onların məhv edilməsi üçün nəzərdə tutulan proqramların yayılmasına görə məsuliyyəti – cərimə və ya 2 ilə qədər azadlıqdan məhrum etməni nəzərdə tutan 615d maddəsi əlavə edilmişdir.

[1] http://www.isc.meiji.ac.jp/~sumwel_h/Co-des/comp-crim.html

Hollandiyanın CM-nin 350b maddəsi isə çoxaldılması ilə sistemə zərər vurulması üçün nəzərdə tutulan məlumatların heç bir icazə olmadan yayılması halını qanunsuz hesab edir. İsveçrədə 1995-ci il 1 yanvar tarixində qəbul edilmiş normalar yalnız zərərverici proqramların yaradılması, yayılması, reklamının deyil, eləcə də bu proqramların yaradılması üçün təlimatlar verilməsini də cinayət hesab edir. (İsveçrə CM maddə 144bis)[1]

Əgər kompüter və kompüter sistemlərinə daxil olma, kompüter sabotajı, məlumatların məxfiliyinin pozulması, kompüter dələduzluğu haqqında məsuliyyəti müəyyən edən qanunvericiliyi bütövlükdə nəzərdən keçirsək, əksər inkişaf etmiş dövlətlərin cinayət qanunvericilikləri bu və ya digər səviyyədə bütün sadalanan əməlləri nəzərdə tutur. Bununla belə bir çox kibercinayətlərin başlanğıcını götürdüyü məlumatlara qanunsuz daxil olmaya görə məsuliyyəti müəyyən edən normaların eyni vəziyyətləri, yəni vurduğu ziyanın ağırlığından asılı olmayaraq məlumatlara istənilən səlahiyyətsiz girişin qanunsuz hesab olunmasını əks etdirmələri vacibdir. Əks halda kibercinayətkarlığın transsərhəd xarakteri belə qanuna zidd əməlləri törədən şəxslərin qanunvericiliklərdəki bu fərqlərdən istifadə edərək məsuliyyətdən yayına bilməsinə imkan verəcəkdir. Bundan başqa terminologiyada, qanunverici konstruksiyalarda və kibercinayətlərin tərkib əlamətlərində ciddi fərqlərin mövcudluğu cinayətlərin araşdırılmasında və cinayətkarın məhkəmə təqibində problemlər yaradır. Beləliklə, kibercinayətkarlıqla, xüsusilə böyük maliyyə itkilərinə səbəb olan iqtisadi kibercinayətkarlıqla, kompüter sabotajı, zərərverici proqramların yayılması ilə effektli mübarizə üçün kompüter və kompüter sistemlərinə qanunsuz olaraq daxil olma, kompüter dələduzluğu, kompüter sistemlərinin işinə müdaxilə haqqında normaların unifikasiya edilməsi zəruridir.

[1] http://www.admin.ch/ch/d/sr/311_0/a143.html

NƏTİCƏ VƏ TƏKLİFLƏR

Tədqiqat işində beynəlxalq əməkdaşlıq üçün nisbətən yeni bir problem olan kibercinayətkarlıq problemi və ona qarşı mübarizənin hüquqi təminatının həm milli həm də beynəlxalq səviyyədə tədqiq edilmişdir. Yarım əsr bundan əvvəl meydana gəlmiş kibercinayətkarlıq insan fəaliyyətinin demək olar ki, bütün sahələrini əhatə etməsi və sürətli artım tempinə malik olması bu hala qarşı vaxtında adekvat münasibət göstərilməsini tələb edir.

Kibercinayətkarlıq informasiya proseslərinin qloballaşmasının qaçılmaz nəticəsidir. İnformasiya texnologiyalarını bəşəriyyət üçün cəlbedici edən sadəlik, asanlıq, anonimlik, əl çatanlılıq və vaxta qənaət kimi keyfiyyətlər qeyri-qanuni hərəkətlər törədən şəxslərin də diqqətini cəlb etməyə bilməzdi.

İnsan fəaliyyətinin müxtəlif sahələrində informasiya texnologiyalarının istifadəsinin artması ilə bu texnologiyaların cinayətlərin törədilməsi məqsədilə istifadəsini də artır. İnformasiya texnologiyaları sahəsindəki münasibətlərin qanunvericiliklə

tənzimlənməsi də bu texnologiyaların inkişafını nəinki üstələmir hətta bu inkişafdan geri qalır.

Kibercinayətkarlıq problemi bir dövlət sərhədləri ilə məhdudlaşmadığına və qlobal xarakterə malik olduğuna görə ciddi və miqyaslı tədqiqatların aparılmasını, həmçinin vahid beynəlxalq standartların işlənib hazırlanmasını zəruri edir.

Tədqiqat işində "kibercinayətkarlığın" beynəlxalq standartlara cavab verən şərhi verilmişdir. Kompüter texnologiyalarının tətbiqi ilə törədilən qanunsuz əməlləri adlandırmaq üçün istifadə olunan "Kompüter cinayətkarlığı" termini son dövrlər geniş yayılan bu halın təbiətini təqiq əks etdirmir. Belə ki, kibercinayətkarlıq mahiyyət etibarı ilə kompüter cinayətlərindən daha geniş anlayışdır. Bu tədqiqat işində kibercinayətkarlıq dedikdə, kompüter sistemləri və şəbəkələri, həmçinin kibermühitə daxil olma vasitələrinin köməyi ilə kibermühitdə kompüter sistemləri və şəbəkələri çərçivəsində, kompüter sistemləri və şəbəkələri və məlumatları əleyhinə törədilən cinayətlərin məcmusu başa düşülür. Uyğun olaraq, kibercinayətkarlıq-kompüterlərin, kompüter proqramları və şəbəkələrinin işinə qanunazidd müdaxilə, həmçinin kompüter məlumatlarının sanksiyalaşdırılmamış modifikasiya olunması və digər qanunazidd ictimai təhlükəli əməllərdir.

Kibercinayətkarlığa minimal xərclərlə və aşağı risklə böyük zərər vura bilmə imkanına görə yüksəl ictimai təhlükəyə malikdir. Bundan başqa, kibercinayətkarlıq yüksək məxfiliklə xarakterizə olunduğuna görə hüquq mühafizə orqanlarının statistikası kibercinayətkarlığın həqiqi vəziyyətini nə dövlət səviyyəsində, nə də bütövlükdə dünya səviyyəsində dəqiq əks etdirmir. Bu səbəbdən də kibercinayətkarlığın vəziyyətini qiymətləndirmək üçün məlumatların toplanmasının və bu halın qiymətləndirilməsinin digər üsullarından istifadə etmək zəruridir.

Kibercinayətkarlığın son illərdə baş verən artımını dövlətin hüquq mühafizə orqanlarının mütəxəssisləri, həmçinin alternativ üsullarla statistik məlumatları toplamaqla tədqiqat aparan təşkilat işçiləri də təsdiq edir. Kibercinayətkarlıq nəticəsində dəyən maliyyə itkiləri isə milyon dollarla ölçülür. Lakin kibercinayətkarlıq nisbətən "yeni" növ cinayət əməli olduğundan və kibercinayətkarlığın transsərhəd xarakterindən asılı olaraq onun araşdırılmasının çətinləşməsindən irəli gələrək bu cina-

yətlərlə bağlı statistik məlumatlar hələ uzun müddət bu qəsdlərin real vəziyyətini dəqiq əks etdirməyəcək. Kibercinayətkarlıqla bağlı bir çox dövlətlərin rəsmi statistikasında göstəricilərin reallıqdan fərqli olaraq bir o qədər də yüksək olmamasına baxmayaraq kibercinayətkarlıq problemi ilə bir çox dövlətlərlə yanaşı beynəlxalq təşkilatlarda narahatdırlar. Bu halın transsərhəd xarakterindən irəli gələrək onunla cinayət-hüquqi mübarizə məsələsi də qlobal problemə çevrilmişdir.

Kibercinayətkarlıqla effektiv mübarizə üçün milli səviyyədə cinayət-hüquqi normaların qəbulu ilə yanaşı, vahid beynəlxalq standartların işlənib hazırlanması zəruridir.

Kibercinayətkarlığın meydana gəlməsi və onunla mübarizə üzrə effektiv mübarizə tədbirlərinin işlənib hazırlanması ilə dünya ölkələrinin milli cinayət qanunvericiliklərində ciddi dəyişikliklər baş vermişdir. Bu dəyişikliklər kibercinayətkarlıqla mübarizə sahəsində beynəlxalq sənədlərin qəbulu ilə paralel baş vermişdir. Lakin ölkələrin milli qanunvericiliklərində bütün bu dəyişikliklər müəyyən bir beynəlxalq sənədin qəbulu ilə şərtlənməsinə baxmayaraq, ölkələr səviyyəsində "avtonom" şəkildə qəbul edilir, dəyişdirilir və inkişaf edirdi. Belə ki, bəzi ölkələr cinayət məcəlləsində dəyişikliklərin edilməsinə, digərləri kibercinayətkarlıqla mübarizəyə yönəlmiş xüsusi qanunların qəbul edilməsinə üstünlük vermişlər.

Ölkələrin milli cinayət qanunvericilikləri kifayət qədər müxtəlif və ziddiyyətlidir. Ayrı-ayrı ölkələrin, hətta bir region çərçivəsində milli cinayət qanunvericiliklərində eyniliyin olmaması kibercinayətkarlıqla effektli mübarizə metodlarının inkişafını ləngidir. Bununla yanaşı bəzi dövlətlərdə - məsələn, ABŞ, İtaliya, Almaniya,- kibercinayətkarlıqla bağlı qanunvericilik kifayət qədər yaxşı formalaşdırılmış və müvəffəqiyyətlə praktikada tətbiq edilir. Bu dövlətlərin təcrübəsi beynəlxalq strategiyanın işlənib hazırlanması, eləcə də hər hansı konkret bir ölkənin qanunvericiliyində islahatların həyata keçirilməsində müsbət rol oynaya bilər.

Həm ayrı-ayrı fərdlər, həm də cinayətkar qrupların qanunazidd fəaliyyəti üçün geniş imkanlar yaradan informasiya texnologiyalarının istifadə sferasının genişlənməsi ilə sözsüz artmaqda olan kibercinayətkarlıq təhlükəsiylə mübarizə üçün daima beynəlxalq əməkdaşlıq zəruridir. Kibercinayətkarlığa nəzarət etmək və onunla

mübarizə aparmaq müəyyən bir dövlət səviyyəsində demək olar ki, mümkünsüzdür. Beynəlxalq norma və standartların qəbulu dövlətlərin milli qanunvericiliklərinə uyğun dəyişikliklərin edilməsi ilə müşaiət olunmalıdır.

Kompüter texnologiyalarının inkişafına təcili reaksiya vermə bilmək və uyğun normaların qəbulu üçün dövlət səylərinin koodinasiyası zəruridir. Hazırki zamanda kibercinayətkarlıqla mübarizə üzrə beynəlxalq strategiyanın formalaşdırılması ilə 40-dan çox dövlət məşquldur və bu prosesin uzunmüddətli olacağı gözlənilir. Lakin bütün bu çətinliklərə baxmayaraq, beynəlxalq əməkdaşlığın qanunvericiliyin unifikasiyası problemi ilə bağlı bir qərara gəlmələri zəruridir. Əks halda kibercinayətkarlığın transsərhəd xarakterini nəzərə alaraq, qanunvericilikdə müəyyən uyğunsuzluqlar və ölkələrin cinayətkarlıq üzrə siyasətlərinin koordinasiya olunmaması ictimai təhlükəli əməl törədən şəxslərə məsuliyyətdən yayınmağa imkan verəcək və cinayətlərin araşdırılması, həmçinin qanunpozucularının təqibini çətinləşdirəcəkdir.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYATLAR

Nəzəri materiallar:

1. Грюлих К.В. «Киберпространство: специфическое регламентирование и конкурентные нормы в евопейских телекоммуникациях”, сборник научных трудов ИНИОН РАН, Москва, 2008
2. Авчаров И.В. Борьба с киберпреступностью / Информатизация и информационная безопасность правоохранительных органов. XI межд. конф.
3. Антонос Г. А. Международные изменения права киберпространства. / Право и информатизация общества: сб. науч. Тр.
4. Быков В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями / В. Быков, А. Нехорошев, В. Черкасов.

5. Вехов, В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского - М.:
6. Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации / А.Г. Волеводз // Российский судья.
7. Дрёмин, В. Н. Глобализация информационных систем как фактор глобализации преступности / В.Н. Дрёмин // Інформаційні технології та безпека.
8. Завидов, Б.Д. Комментарий действующего законодательства о защите объектов интеллектуальной собственности и сферы высоких технологий / Б.Д. Завидов // Библиотечка Российской газеты.
9. Кашлев, Ю. Б. Становление глобального информационного общества и место России / Ю.Б. Кашлев. // Информация. Дипломатия. Психология. – М.: Издательство «Известия».
10. Козлов, В. Е. Теория и практика борьбы с компьютерной преступностью / Е.В. Козлов. - М.: Горячая линия
11. Компьютерная преступность и информационная безопасность // Под ред. Леонова А. П.
12. Ляпунов, Ю., Ответственность за компьютерные преступления. / Ю.Ляпунов, В. Максимов //
13. Мазуров, В.А. Компьютерные преступления: классификация и способы противодействия/ В.А. Мазуров.

Normativ-hüquqi aktlar:

1. Azərbaycan Respublikasının Konstitusiyası
2. Azərbaycan Respublikasının Cinayət Məcəlləsi 30.12.1999
3. “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanunu 03.04.1998;

4. “Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında” Azərbaycan Respublikası Qanunu 29.06. 2012
5. Müstəqil Dövlətlər Birliyinə üzv dövlətlərin Nümunəvi Cinayət Məcəlləsi.
6. Qlobal informasiya əməkdaşlığının Okinav Xartiyası. http://www.internet-law.ru/intlaw/laws/okinava.htm
7. BMT-nin cinayətkarlığın qarşısının alınması və qanunu pozanlarla davranış üzrə X Konqresi. http://www.un.org/russian/topics/crime/docs10.htm

İnternet resursları:

1. http://www.setevoi.ru
2. http://www.lenta.ru/internet
3. http://www.crime-research.ru
4. http://www.crime-research.ru
5. http://www.socio.ru/wr/00-1/Cadtells.htm.
6. http://www.vesti.ru/news
7. http://www.cyberpol.ru/cybercrime.shtml.
8. http://www.crime-research.ru/articles/Mirosh1
9. http://www.supcourt.ru
10. http://www1.ifccfbi.gov/strategy
11. http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php
12. http://dictionary.cambridge.org
13. http://all.net
14. http://4law.co.il
15. http://www.coe.int/T/E/Com/Files/Themes
16. http://www.nautilus.org/info-policy/workshop
17. http://www.askoxford.com/
18. http://www.mosstingrett.no/index.html

АННОТАЦИЯ

В диссертационной работе отмечается, что одним из важных отраслей регулирования является регулирование информационных технологии. Информационная система являясь необходимым елементом современной жизни тесно взаимасвязано с другими отраслями экономики, постоянно оперативно обнавляется и развивается. Информационные технологии составляют органическую часть факторов развития цивилизации.

Информационные технологии являются важным средством положительно ваздействующем на развитие обшества. Она влияет на ряду государственными органами, институтами гражданского обшества, экономического бизнеса, социалного сектора, так же науке, образования, отраслей культуры и повстедневной жизни. Во многих развитых и развивающихся странах вслетствии применения информационных коммуникационных технологий были

достигнуты большие достижения, и таким образом ни укого не взывает сомнение что информационные технологии ведут будешщуму мировую цивилизацию.

В диссертационной работе отмечается, что преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, так и распространение противоправной информации через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Широкое применение информационных технологии даёт силный толчок обшему социально-экономическому развитию страны, имеет действенные средства снижения бедности. По этому с целью усиления развития использования потенциала страны, подготовка стратегии своей национальной информационной технологии является решаюшим. А это осебенно необходимо для такой страны как Азербайджан каторое переживает перемены сосиально-экономического развития и стримится интеграции мировое сообшество.

ANNOTATION

In dissertational work it is noticed, that one of the important branches of regulation is regulation of information technologies and telecommunications. Information system being necessary a modern life it is close with other branches of economy, constantly operatively and develops. Information technologies make an organic part of factors of development of a civilisation.

Information communication technologies are the important means positively on development. It influences on a number the state bodies, institutes civil, economic business sectors, as to a science, formations, branches and lives. In many developed and developing countries applications of information communication technologies have been reached the big achievements, and thus the doubt does not appeal that information and communication technologies conduct a world civilisation.

The thesis points out that computer crime include both the propagation of malicious viruses, hacking passwords, steal credit card numbers and other bank details, and the spread of illegal information via the Internet, as well as harmful interference through computer networks of various systems work.

Wide application information and communication to technology gives a push to social and economic development of the country, has effective means of decrease in poverty. On it for the purpose of strengthening of development of use of potential of the country, preparation of strategy of the national information and communication technology. And it is necessary for such country as Azerbaijan worries changes of economic development and integration world comuniti.

REFERAT

İqtisadiyyatın kompüterləşməsinin ən ciddi mənfi nəticəsi məhz kibercinayətlər hesab olunur. Kompüter sistemlərinin geniş yayılması, onların kommunikasiya sistemləri vasitəsilə əlaqələndirilməsi, bu sistemlərə elektron müdaxilə imkanını artırır. Bu cür cinayətlərin ənənəvi tipli cinayətlərdən tutmuş yüksək riyazi və texniki hazırlıq tələb edən cinayətlərə qədər çox geniş əhatə dairəsi mövcuddur.

Fərdi kompüterlərin sayının sürətli artımı və inkişaf etmiş kommunikasiya sisteminin mövcudluğu hətta həvəskar-cinayətkarların belə kompüter sistemlərinə daxil olmasına imkan yaradır. Əksər ölkələrdə mövcud olan cinayət qanunvericilikləri bu tip cinayətlərin təsnifləşdirilməsi baxımından kifayət qədər elastik olsalar da, sosial və texniki dəyişikliklər bu hüquq sistemi çərçivəsindən kənarda qalan yeni-yeni problemlər yaradır. Çünki dünya təcrübəsində mövcud olan bəzi kompüter cinayətlərinə cinayət qanunvericiliyi təsir göstərə bilmir. Belə ki, hüquqi baxımdan bu əməllər cinayət hesab edilə bilməz. Burada EHM-in bəzi əməliyyatlarının kriminallaşması problemi nəzərdə tutulur.

Kibercinayətkarlıq təhlükəsi bütün dünya ölkələri kimi Azərbaycan üçün də çox təhlükəli bir haldır və bu təhlükənin qarşısını almaq, həmçinin onunla effektli mübarizə aparmaq məqsədilə ölkəmiz Azərbaycan Respublikasının tarixli "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə 30.09.2009-cu il Qanunu ilə Avropa Şurasının "Kibercinayətkarlığa dair" Konvensiyasına qoşulmuşdur. Azərbaycan Avropa Şurasının "Kibercinayətkarlıq haqqında" 2001-ci il 23 noyabr tarixli Konvensiyasını imzalamış dövlətlər sırasına daxil olmasına baxmayaraq, beynəlxalq əməkdaşlıq özü də bu gün kibercinayətkarlıq problemi ilə mübarizənin yeni metodlarının axtarışı və vahid siyasətin işlənib hazırlanması prosesini yaşayır.

Tədqiqatın məqsədi kibercinayətkarlıq probleminin, onun ictimai təhlükəlilik dərəcəsinin qiymətləndirilməsi üçün zəruri olan kriminal əhəmiyyətli aspektlərin öyrənilməsi, bu hala qarşı mövcud cinayət-hüquqi tədbirlərin təhlili və kibercinayətkarlıqla mübarizənin cinayət-hüquqi tənzimlənməsinin effektivliyinin artırılmasına yönəldilmiş təkliflərin işlənib hazırlanması təşkil edir. Bu məqsədə nail olmaq üçün aşağıdakı vəzifələrin həyata keçirilməsi nəzərdə tutulmuşdur:

- iqtisadi cinayətkarlıq, onun xüsusi bir forması olan kibercinayətkarlıq və eləcə də kibercinayət anlayışını formalaşdırmaq, kibercinayətlərin növlərini xarakterizə etmək;

- kibercinayətkarlıqla mübarizənin hüquqi təcrübəsini iki səviyyədə - beynəlxalq və milli səviyyədə təhlil etmək və eləcə də xarici ölkə qanunvericiliklərinin müqayisəli təhlilini aparmaq;

- kibercinayətkarlıqla mübarizə sahəsində beynəlxalq təcrübədən istifadə istiqamətlərini təhlil etməklə milli qanunvericiliyin təkmilləşdirilməsi imkanlarını müəyyən etmək.

Dissertasiya tədqiqatının obyektini kibercinayətkarlıqla mübarizə üzrə milli, eləcə də ayrı-ayrı xarici ölkələrin hüquq sistemləri təşkil edir. Tədqiqatın predmeti isə kibercinayətkarlığın kriminoloji aspektləri - onun vəziyyəti, strukturu, dinamikası və bu dinamikaya təsir göstərən amillər, onun cinayət-hüquqi mübarizə məsələləri, eləcə də kibermühitdə törədilən əməllərə görə məsuliyyəti müəyyən edən milli və beynəlxalq cinayət-hüquq normalarıdır.

Dissertasiya işinin elmi yeniliyi tədqiq olunan problemin respublikamızda son illər ərzində daha intensiv formada reallaşdırılmaqda olan internet texnologiyalarının tətbiqi ilə şərtlənir. Belə ki, tədqiq edilən sahənin kifayət qədər yeni olması, bu sahədəki elmi tədqiqatların aktuallığını və yeniliyini şərtləndirməkdədir.

Tədqiqatın informasiya bazasını mövzu ilə əlaqədar xarici tədqiqatçıların və ekspertlərin araşdırmaları, beynəlxalq təşkilatların işçi materialları və sənədləri, statistik və normativ materiallar, o cümlədən kibercinayətkarlığa dair beynəlxalq təşkilatlar tərəfindən toplanmış məlumatlar, ayrı-ayrı ölkələrdə kompüter cinayət-

karlığının vəziyyətinə dair məcmuələr, bir sıra seminar və konfransların sənədləri, tədqiqat mövzusu üzrə elmi araşdırmalar və digər elmi ədəbiyyatlar təşkil edir.

İşin nəzəri – metodoloji bazasını kibercinayətkarlıq anlayışının, onun kompüter cinayətlərindən fərqinin, eləcə də bu halın mühüm kriminoloji əlamətləri və kibercinayətkarlıqla milli və beynəlxalq səviyyədə mübarizə istiqamətlərinin öyrənilməsi və tədqiqi ilə bağlı alimlərin tədqiqatları, onların əldə etdikləri nəticələr, eləcə də milli və ayrı-ayrı xarici ölkələrin hüquq yaratma orqanlarının səlahiyyətlərinə müvafiq formalaşdırdıqları qanunvericilik aktları sistemi təşkil etmişdir. Tədqiqatda qarşıya qoyulan məsələlərin həllinə nail olmaq üçün müqayisəli təhlil, statistik təhlil, səbəb–nəticə, funksional, məntiqi, struktur, həmçinin, analiz və sintez və s. tədqiqat üsullarından istifadə edilmişdir.

Dissertasiyanın strukturu giriş, üç fəsil, nəticə və təklifdən ibarətdir. Dissertasiyada iqtisadi cinayətkarlıq, eləcə də onun xüsusi forması kimi kibercinayətkarlığın anlayışı, mahiyyəti açıqlanmış, kibercinayətlərin subyektlərinin təsnifatı aparılmış, kibercinayətkarlığınmiqyası, ictimai təhlükəsi təhlil edilmiş və ona qarşı mübarizənin formalaşdırılması istiqamətləri tədqiq edilmişdir. Bununla yanaşı tədqiqat işində Azərbaycan Respublikasının qanunvericilik sistemində iqtisadi cinayətkarlıq formalarının hüquqi təsbiti məsələləri və kibercinayətkarlığa qarşı mübarizənin hüquqi təminatının müasir vəziyyəti təhlil edilmiş, kibercinayətkarlıqla mübarizə sahəsində ayrı-ayrı ölkələrin qanunvericiliklərinin müqayisəli təhlili həyata keçirilmiş və Azərbaycanda kibercinayətkarlıqla mübarizə sahəsində beynəlxalq təcrübədən istifadə istiqamətləri geniş tədqiq edilmişdir.

Tədqiqatın sonunda nəticələr ümumiləşdirilmiş və təkliflər çıxarılmış, istifadə olunan ədəbiyyat siyahısı və internet resurslar təqdim edilmişdir.