Səkinəxanım RZAYEVA,
Bakı Dövlət Universitetinin Hüquq fakültəsinin
Cinayət hüququ və kriminologiya kafedrasının
dosenti, hüquq üzrə fəlsəfə doktoru
sakinaxanim_rzayeva@mail.ru

Vüqar SADİQLİ,
Bakı Dövlət Universitetinin Hüquq fakültəsinin
Cinayət hüququ və kriminologiya kafedrasının
"Transmilli cinayət hüququ" ixtisası üzrə
I kurs magistrantı
woogalle@gmail.com

CİNAYƏTİN KİBER ÜSULLA TÖRƏDİLMƏSİ – CƏZANI AĞIRLAŞDIRAN HAL KİMİ

Açar sözlər: kiber üsul, kiber mühit, kiber cinayət, informasiya texnologiyaları, ağırlaşdırıcı hal, cinayət tərkibi.

Key words: cyber way, cyber environment, cybercrime, information technology, aggravating circumstance, criminal composition.

Ключевые слова: киберспособ, киберсреда, киберпреступление, информационные технологии, отягчающее обстоятельство, состав преступления.

Mühafizəedici tənzimetmə mexanizminə malik olan cinayət qanunvericiliyinin müddəalarının müasir dövrün obyektiv gerçəkliyinə uyğunlaşdırılması cinayətkarlıqla hərtərəfli və daha səmərəli mübarizə aparılması, törədilən əməllərə tam və düzgün hüquqi qiymətin verilməsi, habelə ədalətli və humanist cəza siyasətinin həyata keçirilməsi məqsədilə vacib əhəmiyyət daşıyır.

İnformasiya texnologiyalarının istifadəsi təkcə fəaliyyətimizin müxtəlif sahələrində yox, həm də cinayətkar məqsədlər üçün ictimai təhlükəli əməllərin törədilməsində "səmərə" verdiyindən, bu istifadənin cinayət-hüquqi münasibətlər ilə tənzimlənməsi qaçılmazdır. Daim inkişaf edib təkmilləşməkdə olan informasiya texnologiyalarının hər keçən gün həyatımızın ayrılmaz tərkib hissəsinə çevrilməsi hüquq elminin bütün sahələrinə (mülki hüquq, əmək hüququ və s.), xüsusən də, cinayət hüququna təsirsiz ötüşmür. Təəssüf hissilə bildirməliyik ki, müasir dövrün texnologiyaları özlüyündə böyük elmi-texnoloji və tibbi nailiyyətlərə səbəb olsa da, həm də şəxsiyyətə, cəmiyyətə, habelə dövlətə qarşı qanunla qadağan olunan əməllərin törədilməsində böyük ölçüdə istifadə edilir.

XX əsrin sonlarından və XXI əsrin əvvəllərindən başlayaraq "İnternet" qlobal şəbəkəsinin dünya miqyasında əlçatanlığının artması [14,s.6] və "yeni ictimai münasibətlər" kimi qiymət-ləndirilməsi ilk vaxtlar milli hüquq sistemlərini formalaşdırmaqda olan ölkələrdə tənzim edilməz bir hal kimi səciyyələndirilirdi. Məhz milli hüquq sistemləri üçün "boşluq" sayılan bu halların birbaşa və ya dolayı yolla ictimai təhlükəli əməllər və nəticələr doğurması cinayət hüququnda "klassik yanaşma və prinsipləri" sorğu altına almış oldu.

Günümüzdə hələ də beynəlxalq-hüquqi (mühafizəedici) tənzimlənməsi mövcud olmayan, yalnız ayrı-ayrı qitə, region, siyasi-iqtisadi və s. təşkilatlar (Afrika Birliyi Təşkilatı**,** Avropa Şurası, "Şanxay" ƏT və s.) səviyyəsindəki aktlarda işlənib hazırlanan və kiber mühitdə törədilən cinayətlərin (kibercinayətlərin) transmilli xarakteri onlara spesfik yanaşmanı məcburi edir.

Azərbaycan Respublikasının 29 iyun 2004-cü il tarixli "Milli təhlükəsizlik haqqında" Qanu-nu-

nun 20-ci maddəsinin məzmununa əsasən, kiber mühitdə törədilən hüquq pozuntularına milli təhlükəsizlik konteksindən yanaşan dövlətimiz [3, m.20] kibercinayətlərə qarşı hüquqi mübarizədə hazırkı dövr üçün müfəssəl akt hesab olunan və kibercinayətləri əsas təsnifat kimi beş növə ayıraraq hüquqi təsbitini üzv dövlətlərə tövsiyyə edən Avropa Şurasının 23 noyabr 2001-ci il tarixli "Kiber-cinayətkarlıq haqqında" Budapeşt Konvensiyasını 30 iyun 2008-ci il tarixində imzalayıb, 30 sentyabr 2009-cu il tarixində ratifikasiya etmiş və 29 iyun 2012-ci il tarixli "Azərbaycan Respublikasının Cinayət Məcəlləsinə dəyişiklik edilməsi haqqında" Qanunun qəbulu ilə Cinayət Məcəlləsinin XXX fəslində kibercinayətləri əhatə edən yeni müddəaları təsbit etmişdir.

Milli qanunvericiliyimiz Cinayət Məcəlləsinin XXX fəsli üzrə "Budapeşt" Konvensiyasının maddi cinayət hüququna dair müddəalarını özünəməxsus tərzdə − yalnız bu Konvensiyanın I Altfəslini (normaları) müstəqil və birləşdirici (iki ayrı növdən əməli bir maddə üzrə) tərkibdə tam (konvensiyon müddəaları bütöv həcmdə), II Fəslini (normaları) isə müstəqil tərkibdə qismən (konvensiyon müddəaları məhdud həcmdə) təsbit etmişdir.

Ancaq qeyd etməliyik ki, "Budapeşt" Konvensiyasının qəbul edilməsindən keçən onilliklər ərzində kiber mühitdə törədilən cinayətlərin ictimai təhlükəliliyi olduqca artmış [9, s.70], bu qəbildən olan cinayətlər yönəldiyi qəsd obyektləri təyinatını böyük ölçüdə dəyişmiş (ictimai əhəmiyyətli infrastruktur obyektləri və d.) və onların mürəkkəb törədilmə formaları çoxsaylı dəyişikliyə məruz qalaraq yeni növlərinin meydana çıxmasına səbəb olmuşdur.

Bütün bu deyilənləri nəzərə alaraq, kiber mühitdə törədilən cinayətləri iki kateqoriya üzrə təsnifləşdirə bilərik: a) ictimai təhlükəli əməlin yönəldiyi qəsd obyektinə və b) obyektiv cəhətin elementlərinə görə − kibercinayətlər və kiberləşən (kiber xarakterli) cinayətlər.

Azərbaycan Respublikasının cinayət qanunvericiliyində kibercinayətlər dedikdə, Cinayət Məcəlləsinin XXX fəslində təsbit edilən və cinayətin bilavasitə obyektinə görə beş növdə müəyyən edilən cinayətlər başa düşülür. Buraya: kompüter sisteminə qanunsuz daxil olma; kompüter məlumatlarını qanunsuz ələ keçirmə; kompüter sisteminə və ya kompüter məlumatlarına qanunsuz müdaxilə; kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi və kompüter məlumatlarının saxtalaşdırılması aid edilir [7, s.282-293].

Kiber xarakterli cinayətlər dedikdə isə, Cinayət Məcəlləsinin Xüsusi hissəsinin ayrı-ayrı fəsillərində nəzərdə tutulan cinayət növləri üzrə kiberləşmə əlamətinə malik olan cinayətlər başa düşülür. Burada kiberləşmə (yaxud bu və ya digər cinayətin kiberləşməyə aid edilməsi) dedikdə, insan və cəmiyyətin kiber mühitdə sosial və psixoloji təbiət qanunayğunluqlarının və kriminoloji ünsürlərin qarşılıqlı təsiri ilə hüquqazidd ictimai təhlükəli əməllərin müstəqil formalaşması imkanı nəzərdə tutulur.

Kibercinayətlər ilə kiber xarakterli cinayətlərin ictimai təhlükəlilik meyarlarını müqayisə etsək, deyə bilərik ki, kibercinayətlər bu və ya digər formada kompüter sistemi, məlumatları və bu sahədəki texniki vasitələrin təyinatı ilə bağlı (ümumi) kiber təhlükəsizlik, habelə, ictimai əhəmiyyətli infrastruktur obyektlərinə münasibətdə (xüsusi) təhlükəsizliklə bağlı ictimai münasibətlərə qəsd etsə də, kiber xarakterli cinayətlərin törədilməsi ilə cinsi obyekt daxilində istənilən ictimai münasibətlər qəsd obyektinə çevrilə bilər.

Hazırda Cinayət Məcəlləsində kiber xarakterli cinayətlər kiberləşmə əlaməti üzrə əməlin ictimai təhlükəliliyinin dərəcəsi ilə müəyyən edilən əsas tərkiblərdə və cinayət məsuliyyətini ağırlaşdıran və xüsusilə ağırlaşdıran halı ehtiva edən tərkiblər kimi təsbit olunur. Bu spesifik əlamət, bir qayda olaraq, cinayətin törədilmə üsulu ilə müşayiət olunur ki, bu da "adi" növdən olan eyni cinayət əməlini onun kiber xarakterli növündən fərqləndirmədə əsas kimi çıxış edir.

Əvvəlki məqaləmizdə də qeyd etdiyimiz kimi, əməllə sıx surətdə əlaqəli olan və onun tərkib hissəsini əmələ gətirən üsul çox vaxt törədilən əməlin ictimai təhlükəli xarakterinə və dərəcəsinə o qədər əhəmiyyətli təsir göstərir ki, o, hətta bir çox cinayətlərin əsas və ya tövsifedici tərkiblərinə də zəruri əlamət kimi daxil edilir. Əksər hallarda məhz cinayətin edilmə üsulu bütövlükdə

həmin cinayətin mahiyyətini ifadə edir [8, s.96].

Digər tərəfdən, Azərbaycan Respublikası Ali Məhkəməsinin 5 iyun 2003-cü il tarixli "Məhkəmələr tərəfindən cinayət cəzalarının təyin edilməsi təcrübəsi haqqında" Plenum Qərarında göstərilir ki, cinayətin ictimai təhlükəlilik dərəcəsi onun törədilmə hallarına (məsələn, cinayətkar niyyətin həyata keçirilmə dərəcəsi, üsulu, vurulmuş zərərin həcmi və baş vermiş nəticələrin ağırlığı, iştirakçılıqla törədilmiş cinayətlərdə təqsirli şəxslərin rolu və s.) əsasən müəyyən edilir [5, s.231].

Məhz yuxarıda qeyd edilənlərə əsasən hesab edirik ki, kiberləşmə əlaməti obyektiv cəhətin bir elementi kimi cinayətin edilmə üsulunu təşkil edib müvafiq cinayət tərkibinin tövsifedici əlaməti qismində təsbit edildikdə, törədilmiş əmələ cinayət-hüquqi qiymətin verilmə əsası kimi çıxış edir. Ancaq bu əsasın müvafiq cinayət-hüquq normasında obyektiv cəhətin zəruri əlaməti kimi və ya cinayət tərkibinin tövsifedici və ya xüsusilə tövsifedici əlamətləri kimi təsbit edilməməsi, lakin cinayətin törədilməsində bilavasitə mövcud olması onun cəza təyin etmədə ağırlaşdırıcı hal qismində nəzərə alınmasını istisna etməməlidir.

Çünki, hər bir halda cinayətin edilmə üsulu cinayətkarın şəxsiyyətinin ictimai təhlükəliliyinə qiymət verilməsi, habelə cinayət məsuliyyətinin və cəzanın diferensiallaşdırılması nöqteyi-nəzərindən vacib əhəmiyyətə malikdir [10, s.189]. Bu qeyd edilənlər isə ümumilikdə Cinayət Məcəlləsinin 58.3-cü maddəsinin göstərişindən irəli gəlir. Həmin maddədə deyilir ki, cəza təyin edilərkən törədilmiş cinayətin xarakteri və ictimai təhlükəlilik dərəcəsi, təqsirkarın şəxsiyyəti, o cümlədən cəzanı yüngülləşdirən və ağırlaşdıran hallar, habelə təyin olunmuş cəzanın şəxsin islah olunmasına və onun ailəsinin həyat şəraitinə təsiri nəzərə alınır [1, s.62].

Cinayət Məcəlləsinin ayrı-ayrı ictimai münasibətləri mühafizə edən bir sıra normalarında informasiya texnologiyalarından istifadə etməklə ictimai təhlükəli əməllərin kiber mühitdə törədilməsinin əsas tərkiblərdə təsbit edilməsi həyata keçirilmişdir. Bura Cinayət Məcəlləsinin 147.1, 148, 148-1, 323.1, 323.1-1-ci və s. maddələrində nəzərdə tutulan alternativ cinayət tərkibləri daxildir.

Cinayət təqibi xüsusi ittiham qaydasında həyata keçirilən Cinayət Məcəlləsinin 147 (Böhtan) və 148-ci (Təhqir) maddələri, habelə, bu maddələrə münasibətdə xüsusi norma kimi çıxış edən 148-1-ci maddəsində [4, s.518-523] (İnternet informasiya ehtiyatında saxta istifadəçi adlar, profil və ya hesablardan istifadə edərək böhtan atma və ya təhqir etmə) nəzərdə tutulan cinayət əməllərinin kiberləşmə əlaməti obyektiv cəhətdən sadalanan hərəkətlərin "internet informasiya ehtiyatı"nda törədilməsini ehtiva edir. İlk baxışda bu əlamət cinayətin törədilmə yerinə bənzəsə də, bu belə deyildir, çünki cinayət qanunvericiliyimizdə cinayətin törədilmə yeri dedikdə, konkret coğrafi (məkan) anlayışlar (qitə şelfi, atmosfer və s.) başa düşülür. Belə olan halda isə, bu anlayış cinayətin törədilmə üsulunu əhatə edir, yəni əməlin "internet informasiya ehtiyatında" törədilməsi elə cinayətin informasiya texnologiyalarından istifadə etməklə törədilmə üsulunu bildirir. Qeyd edilən məsələ indi də cinayət hüquq nəzəriyyəsində öz problematikliyini qoruyur. Belə ki, klassik cinayət hüquq nəzəriyyəçilərinə münasibətdə yeni nəsil (kiber) hüquqşünaslar məhz kiber mühiti cinayətin edildiyi yerə aid digər komponentlərlə bərabərləşdirirlər [15,s. 211].

Cinayət Məcəlləsinin 148-1-ci maddəsinin qeyd hissəsində "saxta istifadəçi adlar, profil və ya hesablar"a anlayış verilmişdir. Burada deyilir ki, "saxta istifadəçi adlar, profil və ya hesablar" dedikdə, internet informasiya ehtiyatlarında, o cümlədən sosial şəbəkələrdə istifadəçinin şəxsiyyətini eyniləşdirməyə imkan verməyən, yəni ad, soyad və ya ata adına dair yalan məlumat yerləşdirilmiş və ya belə məlumatlar gizlədilmiş, habelə digər şəxsə aid məlumatlardan onun razılığı olmadan istifadə edilməklə yaradılmış istifadəçi adlar, profil və ya hesablar başa düşülür [13, s.378-379]. Qeyd hissənin təhlilinə əsasən ilkin olaraq hesab edirik ki, "internet informasiya ehtiyatı" termini "informasiya texnologiyaları" terminin alt kateqoriyasını təşkil etdiyindən, həm qeyd hissə, həm də obyektiv cəhətdə sadalanan əməllər məhz sonuncu terminlə müşaiyət edilmiş olsa, daha məqsədəmüvafiq olardı. Çünki "informasiya texnologiyaları" dedikdə, informasiyanın yaradılması, emalı, saxlanması, istifadəsi, ötürülməsi və idarə olunması ilə bağlı texnologiyaları

(həm kompüter texnikasını, həm də proqramlaşdırmanı ehtiva edən) adlandırmaq üçün istifadə olunan ümumi termin başa düşülür [6, s.397]. Normativ mövqe olaraq bunu da qeyd etməliyik ki, 3 aprel 1998-ci il tarixli "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununun 1-ci maddəsində informasiya texnologiyalarına anlayış verilmişdir. Burada deyilir ki, informasiya prosesləri zamanı, o cümlədən hesablama və rabitə texnikasının tətbiqi ilə istifadə edilən üsul və vasitələr sistemi başa düşülür. Qanunun həmin maddəsində həmçinin "internet informasiya ehtiyatı" terminə də qanunverici anlayış verərək bildirmişdir ki, bu termin internet şəbəkəsində yaradılan, informasiyanın yayılması üçün istifadə olunan, müraciət edilməsi üçün domen adına və sahibi tərəfindən müəyyənləşdirilmiş digər işarələnməyə malik olan informasiya ehtiyatını ehtiva edir [2, m.1]

Digər tərəfdən hesab edirik ki, internet informasiya ehtiyatında saxta istifadəçi adlar, profil və ya hesablardan istifadə etməni (xüsusi kiberləşmə əlamətinin) həm böhtan, həm də təhqir cinayəti üzrə xüsusi törədilmə üsulu kimi ayrıca normada təsbit edilməsi hüquqi texnika baxımından Cinayət Məcəlləsinə əlavə yüklülük gətirir. Yaxşı olardı ki, qanunverici "elektron informasiya mühiti"ndə saxta istifadəçi adlar, profil və ya hesablardan istifadə etməni tövsifedici və ya xüsusilə tövsifedici hal kimi həm böhtan, həm də təhqir cinayəti üzrə onların təsbit olunduğu cinayət tərkiblərinin tövsifedici halı kimi təsbit etsin.

Yuxarıda təklifini verdiyimiz nüans, bir maddə üzrə ancaq iki əsas tərkibdə Cinayət Məcəlləsinin 323-cü maddəsində də öz əksini tapmışdır. Belə ki, qanunverici 323.1-ci maddə üzrə Azərbaycan dövlətinin başçısının-Azərbaycan Respublikası Prezidentinin şərəf və layaqətini kütləvi çıxışda, kütləvi nümayiş etdirilən əsərdə, kütləvi informasiya vasitəsində və ya kütləvi nümayiş etdirildiyi halda internet informasiya ehtiyatında ləkələmə və ya alçaltma əməlini əsas tərkibdə kriminallaşdırmışdır. Xüsusi kiberləşmə əlaməti isə Cinayət Məcəlləsinin 323.1-1-ci maddəsi üzrə birinci əsas tərkibdə nəzərdə tutulmuş əməllərin internet informasiya ehtiyatında saxta istifadəçi adlar, profil və ya hesablardan istifadə edərək kütləvi nümayiş etdirməklə törədilmə halını ehtiva edir. Bu cinayət-hüquq normasının təhlilindən də bu qənaətə gəlirik ki, qanunvericinin 323.1-1-ci maddədə təsbit etdiyi cinayət tərkibinin əsas tərkib kimi yox, tövsifedici hal kimi nəzərdə tutulması daha məqsədəuyğun olardı. Çünki, hüquqi texnika baxımından qanunverici, bir qayda olaraq, əsas tərkibdə nəzərdə tutulan ictimai təhlükəli əməllərin sosial təhlükəliliyini artıran və əsas tərkiblə müqayisədə daha ağır nəticələrə səbəb olan halları tövsifedici əlamət kimi qiymətləndirir (məsələn, 120.1. və 120.2.11.mad.). Burada nəzərdə tutulan xüsusi kiberləşmə əlamətinin (saxta istifadəçi adlar, profil və ya hesablar) cinayətin ictimai təhlükəlilik dərəcəsini artırması (bunu deməyə CM-nin həm 323.1-1-in, həm də 148-1-ci maddəsinin sanksiyası əsas verir.) bu mövqeni haqlı hesab etməyə imkan yaradır.

Bunu da xüsusi olaraq qeyd etməliyik ki, qüvvədə olan cinayət qanunvericiliyimiz üzrə kiberləşmə əlaməti əməlin təkcə "elektron informasiya mühiti"ndə törədilməsini yox, həm də müvafiq (kiber) qurğularla törədilməsini ehtiva edir. Bu əlamətə Cinayət Məcəlləsində həm əsas tərkiblərdə (CM-nin 233-4.1-ci maddəsi − telekommunikasiya operatorunun və ya provayderinin telekommunikasiya şəbəkəsinə müvafiq qurğu vasitəsilə qoşulmaqla qanunsuz beynəlxalq telekommu-nikasiya xidmətlərinin təşkil edilməsi əhəmiyyətli zərər vurulmasına səbəb olduqda), həm tövsifedici (CM-nin 302.2-ci maddəsi − gizli qaydada informasiya alınması üçün nəzərdə tutulmuş texniki vasitələrdən istifadə edilməklə törədildikdə), həm də xüsusilə tövsifedici (CM-nin 234.4.4−kütləvi informasiya vasitələrindən, o cümlədən internet informasiya ehtiyatlarından və ya informasiya-telekommunikasiya şəbəkələrindən istifadə etməklə törədildikdə) tərkiblərdə rast gəlmək mümkündür. Burada da, yenə hesab edirik ki, qanunverici "müvafiq qurğu", yaxud "texniki vasitələr" terminə münasibətdə informasiya texnologiyaları" terminindən istifadə etmiş olsa, eyni məzmunu ifadə edən fərqli anlayışlara ehtiyac qalmaz.

Kiberləşmə əlaməti qüvvədə olan Cinayət Məcəlləsinin ayrı-ayrı normalarında tövsifedici hal

kimi də nəzərdə tutulmuşdur. Burada əsas problemli məsələ müxtəlif cinayət hüquq normalarında məsuliyyəti ağırlaşdıran kiberləşmə əlamətlərinin müxtəlif adlarla təsbit olunmasıdır. Misal olaraq, Cinayət Məcəlləsinin 177.2.3-1-ci maddəsində özgə əmlakını gizli talamanın (oğurluq) elektron məlumat daşıyıcılarından, yaxud informasiya texnologiyalarından istifadə edilməklə törədilmə forması təsbit edilmişdir. Eyni məzmunda Cinayət Məcəlləsinin 244-1.2.2-ci maddəsindəqumar oyunlarının təşkili və ya keçirilməsinin internet informasiya ehtiyatlarından və ya informasiya-telekommunikasiya şəbəkələrindən istifadə etməklə törədilməsi öz əksini tapmışdır. Hər iki cinayət-hüquq normasında ağırlaşdırıcı halı ehtiva edən, məzmunca eyni kiberləşmə əlamətinin müxtəlif formalarda təsbit edilməsini hüquqi müəyyənlik prinsipi baxımdan məqsədəmüvafiq hesab etmirik. Yaxşı olardı ki, qanunverici istər əsas tərkiblər, istərsə də tövsifedici tərkiblərdə təsbit edilən ümumi kiberləşmə və ya xüsusi kiberləşmə əlamətlərini eyni məzmunda müəyyən etsin. Cinayət Məcəlləsinin 244-1.2.2-ci maddəsində təsbit olunan "informasiya-telekommunikasiya şəbəkələri" termini xüsusi bir termin kimi "informasiya texnologiyaları (IT)" terminin genişlənməsini bildirir [6, s.383]. Hesab edirik ki, müvafiq norma üzrə cinayətin törədilmə üsulunda bu qədər texniki xüsusiləşməyə ehtiyac yoxdur. Bu halda təklif edirik ki, qanunvericinin Cinayət Məcəlləsinin 244-1.2.2-ci maddəsində nəzərdə tutulan cinayət hüquq normasını həmin Məcəlləsinin 177.2.3-1-ci maddəsində nəzərdə tutulan kiberləşmə əlamətinə uyğun şəkildə təsbit etməsi daha məqsədə-müvafiq olardı.

Cinayətin kiber üsulla törədilməsi ilə bağlı digər bir məsələ isə, bəzi cinayətlərin bu üsulla törədilməsində yüksək göstəricilərin olmasına baxmayaraq, hələ də konkret cinayət-hüquq normalarında kiberləşmə əlamətlərinin təsbit olunmamasıdır. Buna misal olaraq, mülkiyyət əleyhinə törədilən cinayətlər sırasında "dələduzluq" cinayətini xüsusi vurğulamalıyıq. Son vaxtlar ictimaiyyətdə və KİV-də "kiber dələduzluq", "kiber dələduzlar" ifadələrinə tez-tez rast gəlinməsi məhz dələduzluq cinayətinin törədilməsində kiber üsulların geniş istifadəsini sübut edir. AR-nin Daxili İşlər Nazirliyinin məlumatına görə, son dövrlər dələduzluqla məşğul olan bəzi şəxslər tərəfindən vətəndaşlara xüsusilə saxta xarici nömrələrdən zənglər edilməklə, onların şəxsi bank kart məlumatlarının əldə edilməsi hallarına rast gəlinməkdədir. Həmin dələduzlar tətbiq edilən xüsusi gizli sosial kiber üsullar vasitəsilə bu haqda məlumatsız olan, əsasən yaşlı nəslin nümayəndələrinə zəng etməklə özlərini hansısa bankın əməkdaşı kimi təqdim edirlər. Daha sonra onlar müxtəlif həvəsləndirici təkliflər vasitəsi ilə vətəndaşların bank kartlarındakı məlumatları əldə etməyə çalışırlar. Həmin məlumatları əldə edəndən sonra kiber dələduzlar tərəfindən kart sahiblərinin xəbərləri belə olmadan onların hesablarından qanunsuz olaraq onlayn ödənişlər həyata keçirilir [11]. Bu zaman dələduzluq həm də kiber üsulla törədildiyi üçün əməlin ictimai təhlükəlilik dərəcəsi də artmış olur. Daha çox yaşlı nəsilə münasibətdə törədilən və xarici ölkələrin qanunvericilik praktikasında kiber xarakterli ayrıca cinayət əməli (məs., Türkiyə Cəza Qanunun 245-ci maddəsi və s.) qəbul edilən [12, s.66] "kiber dələduzluq" cinayətinə münasibətdə milli qanunvericimizin Cinayət Məcəlləsinin 178-ci maddəsi üzrə qeyd edilən əsasda tövsifedici tərkibi qurması, həmin cinayətlərə görə məsuliyyətin dəqiq müəyyən edilməsi üçün olduqca böyük əhəmiyyət kəsb edir.

Hər bir halda qəbul ediləndir ki, cinayətin kiber üsulla törədilməsi əsası kimi çıxış edən kiberləşmə əlamətinin qısa müddət ərzində Cinayət Məcəlləsinin əksər maddələrində qurulması hüquqi və texniki cəhətdən imkansızdır. Ancaq hər bir halda Cinayət Məcəlləsinin 2-ci maddəsində də müəyyən edildiyi kimi cinayət-hüquq normaları qanunla qorunan müvafiq ictimai münasibətləri cinayətkar qəsdlərdən qorumalı və cinayətlərin qarşısını almalıdır. Bu əsasda cinayətin kiber üsulla törədilməsi meyarının cəzanı ağırlaşdıran hallar sırasına daxil edilməsi qaçılmazdır.

Azərbaycan Respublikası Cinayət Məcəlləsinin 61-ci maddəsində cinayət tərkibindən kənarda qalan, ancaq bilavasitə törədilən cinayətin və cinayəti törədənin şəxsiyyəti ilə bağlı olan cəzanı ağırlaşdıran hallar təsbit edilmişdir. Həmçinin, qanunverici müəyyən etmişdir ki, Cinayət Məcəlləsinin 61-ci maddəsinin müvafiq bəndlərində

göstərilməmiş hallar cəzanı ağırlaşdıran hal qismində cəza təyin etmədə nəzərə alına bilməz. Eyni zamanda cinayət qanununun Xüsusi hissəsinin müvafiq maddəsində cinayət tərkibinin əlaməti kimi nəzərdə tutulmuş cəzanı ağırlaşdıran hallar olduqda, cəza təyin edilərkən təkrarən CM-nin 61-ci maddəsinə istinad edilə bilməz. Belə olan halda hesab edirik ki, törədilən bir sıra hüquqazidd əməllərin ictimai təhlükəliliyini artıran, onun vurduğu ziyanı genişləndirib şaxələndirən kiber üsulların, yəni "cinayətin informasiya texnologiyalarından istifadə edilməklə, yaxud da elektron informasiya mühitində törədilməsi" halının müvafiq olaraq Cinayət Məcəlləsinin 61-ci maddəsində təsbit olunması zəruridir. Yalnız bu halda, törədilən ictimai təhlükəli əməlin təsbit olunduğu cinayət-hüquq normasında informasiya texnologiyalarından istifadə edilməklə, yaxud da elektron informasiya mühitində – kiber üsulla törədilmə halı birbaşa göstərilmədiyi halda, ədalət mühakiməsini həyata keçirən orqan Cinayət Məcəlləsinin 61-ci maddəsinə istinad edərək əmələ tam, obyektiv və düzgün hüquqi qiymət verə bilər.

Onu da qeyd etmək istərdik ki, transmilli xarakterə malik olan kibercinayətlərin və kiber xarakterli (kiberləşən) cinayətlərin Cinayət Məcəlləsində təsbit olunması Məcəllə üçün yeni olan və daha öncə istifadə edilməyən terminlərin cinayət-hüquq normalarına daxil edilməsini zəruri edir. Lakin hər bir halda ümumişlək olmayan bu sözlər və terminlərin Cinayət Məcəlləsinə əlavə edilməsi Məcəlləni həm hüquq-mühafizə orqanlarının əməkdaşları, həm də cəmiyyətin digər üzvləri üçün mürəkkəb və başa düşülməyən ifadələr toplusuna çevirməməlidir. Bu səbəbdən əlavə edilən yeni terminlərin izah edilməsi və onların aydınlaşdırılması olduqca böyük əhəmiyyət daşıyır. Bu baxımdan hesab edirik ki, CM-nin normalarında nəzərdə tutulan və ya gələcəkdə əlavə ediləcək yeni terminlərin hər biri üçün ayrıca olaraq müvafiq cinayət tərkiblərinin ehtiva olunduğu maddələrdə (ənənəvi olaraq) qeyd verilərək izah edilməsi Cinayət Məcəlləsi üçün əlavə yüklülüyə səbəb olar. Fikrimizcə, gələcəkdə həm kibercinayətlərin, həm də kiber xarakterli (kiberləşən) cinayətlərin ehtiva olunduğu dispozisiyalarda işlədilən xüsusi terminlərin (yəni kiber üsula aid olan) başa düşülən olması və təvsifdə çətinlik yaratmaması üçün Cinayət Məcəlləsinin konkret fəslində (əhatə etdiyi ictimai münasibətlər baxımından XXX Fəsil daha məqsədəuyğundur) və ya Xüsusi hissənin kiber üsullarla törədilən hansısa normasından birinin Qeydində bu sahədə işlədilən konkret terminlərə sistemli anlayışın verilməsi məqsədəmüvafiq olardı.

İstifadə edilmiş ədəbiyyat:

1. Azərbaycan Respublikasının Cinayət Məcəlləsi. Bakı, "Hüquq yayın evi" nəşriyyatı, 2021, 767
2. Azərbaycan Respublikasının "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunu, https://e-qanun.az/framework/3525
3. Azərbaycan Respublikasının "Milli təhlükəsizlik haqqında" Qanunu, https://e-qanun. az/framework/5455
4. Azərbaycan Respublikası Cinayət Məcəlləsinin Kommentariyası. CM-in 1-189-1-ci maddələrinin şərhi (prof. F.Y. Səməndərovun redaktorluğu ilə). "Hüquq Yayın evi" nəşriyyatı. Bakı, 2019, 704 s.
5. Azərbaycan Respublikası Ali Məhkəməsi Plenumunun Qərarlar Məcmuəsi, "MSV NƏŞR", Bakı, 2017,479 s.
6. İsmayıl Calallı, İnformatika Terminlərinin İzahli Lüğəti, "İnformasiya Texnologiyaları" və "Bakı" nəşriyyatı, Azərbaycan Milli Elmlər Akademiyası İnformasiya Texnologiyaları İnstitutu, 2017, s. 997 https://ict.az/uploads/Informasiya_terminlerinin_izahli_lugeti.pdf
7. Məcidli S.T. Kibercinayətlər. "Avropa İnteqrasiya Mərkəzi" Bakı: 2019, 315 s.
8. Rzayeva S.N. Cinayətin edilmə üsulu obyektiv cəhətin əlaməti kimi. Heydər Əliyev və Azərbaycanda hüquqi dövlət quruculuğu mövzusunda Beynəlxalq Elmi-Praktiki Konfransın materialları, Bakı, 2016, s.95-97.

9. Rzayeva S.N., Sadiqli V.A., Transmilli cinayət kimi kibercinayətlərin anlayışı və ictimai təhlükəliliyi, Qanun 10 (324), 2021, s.65-72.
10. Səməndərov F.Y. Cinayət hüququ. Ümumi hissə. Dərslik. Bakı, "Hüquq Yayın Evi" nışriyyatı, 2018, 724 s.
11. AR-nin DİN-nin məlumatı. https://mia.gov.az/?/az/news/view/1581/
12. Türkiye Cumhuriyyeti Türk Ceza Kanunu, https://www.mevzuat.gov.tr/Mevzuat Metin / 1.5.5237.pdf
13. Самедова Ш.Т. Уголовное право Азербайджанской Республики. Особенная частъ в двух томах. Учебник. Баку, Айдыноглу, 2020, том I, 824 с.
14. K.G.Coffman and A.M.Odlyzko, "Growth of the Internet", July 6, 2001. P.44 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjLtZK139L3AhVgRPEDHZbpATcQFnoECA4QAQ&url=http%3A%2F%2Fwww.dtc.umn.edu%2F~odlyzko%2Fdoc%2Foft.internet.growth.ps&usg=AOvVaw0BwC4ChJPxihsNDFaTE0mH
15. Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage, Cyber Crime, Cyber Space and Effects of Cyber Crime, Punyashlok Ahilyadevi Holkar Solapur University Solapur, Maharashtra, India. − Volume 7, Issue 1, 210-214, January-February-2021,,pp.210-214. https://www.researchgate.net/publication/349352653_Cyber_Crime_Cyber_Space_and_Effects_of_Cyber_Crime

Sakinakhanum Rzayeva
Vugar Sadigli

Committing a crime in a cyber way - as an aggravating circumstance of penalty

At a time when global digitalisation trends are accelerating, the abuse of information technology for criminal purposes is becoming more widespread. In this case, it has become necessary to give a correct criminal assessment of cybercrime.

The article examines cases of cyber ways that increase the public danger of illegal actions, expand and diversify its damage, ie "crime committed using information technology or in the electronic information environment", and this feature is specified in the Special Part of the Criminal Code as a new aggravating circumstance. It is proposed to include both the criminal compositions and Article 61 of the Criminal Code of the Republic of Azerbaijan.

Сакинаханум Рзаева
Вугар Садигли

Совершение преступления киберспособом - как отягчающее наказание обстоятельства

В то время, когда в мире ускоряются глобальные тенденции цифровизации, все большее распространение получает злоупотребление информационными технологиями в преступных целях. В связи с этим возникает необходимость дачи надлежащей криминальной оценки киберпреступности.

В статье рассматриваются дела о киберспособах, повышающих общественную опасность противоправных действий, расширяющих и разветвляющих его ущерб, то есть исследуются обстоятельства «совершения преступления с использованием информационных технологий или в электронной информационной среде» и предлагается включить этот признак как новое отягчающее обстоятельство в конкретные составы Особенной части Уголовного кодекса, а также в статью 61 УКАзербайджанской Республики.