DİN-in Polis Akademiyası "DİO-da idarəetmənin təşkili" kafedrasının rəisi, polis polkovniki, f-r.e.ü.f.d., dosent, əməkdar müəllim
Səməd Hümbətov

Kibercinayətkarlığın transmilli xarakteri və onun hüquqi məzmununa dair

İnformasiya cəmiyyətinin formalaşması nəticəsində fiziki əməyin azaldılması ilə müşayiət olunan insanların rahatçılığını təmin edən yeni imkanlar yaranır. Lakin bu prosesdə müəyyən problemlər də meydana çıxır.Təbii ki, bunlar diqqətdə saxlanılmaqla aidiyyatı araşdırmaların aparılmasını və bundan irəli gələrək həyata keçirilməli olan fəaliyyəti şərtləndirir.

Lakin hazırda hüquq-mühafizə orqanları qarşısında duran aktual problemlərdən biri də informasiya texnologiyaları sahəsində törədilən və məzmun baxımından şəxsiyyətin, cəmiyyətin və dövlətin maraqlarına qəsd edən hüquqa zidd əməllərin qabaqlanmasıdır. Son zamanlar kibercinayətlər, xüsusən də kiberterrorizm daha təhlükəli xarakter alır ki, bu da təhlil edilən sosial-neqativ təzahürün qarşısının alınması üzrə hüquq-mühafizə fəaliyyətinin təkmilləşdirilməsi zərurətini artırır.

Qeyd edilməsi vacibdir ki, kibertəhdidlərə qarşı mübarizə imkanlarının təkmilləşdirilməsi və qabaqcıl dövlətlərin təcrübəsinin öyrənilməsi Azərbaycan Respublikasının hüquq-mühafizəsinin siyasətinin tərkib hissəsidir.

"Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının qanununun 20-ci maddəsində informasiya sahəsində milli təhlükəsizliyin təmin edilməsinin anlayışı verilmişdir. Qanunvericinin mövqeyindən aydın olur ki, dövlət, cəmiyyət və fərdi informasiya resurslarının mühafizəsinə, həmçinin informasiya sahəsində milli maraqların qorunmasına yönəlmiş tədbirlər kompleksinin həyata keçirilməsi milli təhlükəsizliyin təmin edilməsidir. [1].

Nəzərə almaq lazımdır ki, virtual məkanda sərhəd (dövlət sərhədi) yoxdur. Onun yoxluğu virtual məkanda kibercinayətlərin miqyasını təsəvvür etməyə imkan verir. Kibercinayətkarlıq anlayışı beynəlxalq müstəviyə daha çox aiddir. O, məz-

munca informasiya texnologiyalarından cinayətkar məqsədlərlə istifadəni özündə ehtiva edir.

BMT yurisdiksiyasına aid olan sənədlərdə istifadə olunan anlayışa görə kibercinayətkarlıq dedikdə, kompyuter sistemi və ya şəbəkəsinin köməyi ilə, həmin sistem və ya şəbəkə çərçivəsində, yaxud kompyuter sistemi və ya şəbəkəsi əleyhinə törədilə bilən istənilən cinayət başa düşülür. Beləliklə, kiberməkanda törədilən hüquqa zidd əməllər kibercinayətlərə aid edilə bilər. Kibernetik məkan dedikdə, EHM-nin köməyi ilə emal olunan informasiyanın elektron kompyuter şəbəkəsində istifadə prosesində yaranan ictimai münasibətlər məcmusu başa düşülür [2,səh 9].

Bu növ cinayətlərin inkişaf səviyyəsi bilavasitə informasiya texnologiyalarının və qlobal şəbəkələrin inkişaf dərəcəsindən və istifadə açıqlığından asılıdır. Kibercinayətkarlıq bütövlükdə kompyuter cinayətkarlığını və onunla bağlı bütün hadisələri də əhatə edir. Kompyuter məlumatlarının dəyişdirilməsi məqsədilə şəbəkəyə, kompyuter sistemləri və proqramlarının işinə icazəsiz (sanksiyasız) və cinayət təqibi ilə cəzalandırılan müdaxilə kibercinayət hesab edilir. Klassik anlamda bu zaman həmin kompyuter (avadanlıq kimi) cinayətin predmeti, informasiya təhlükəsizliyi isə cinayət obyekti qismində çıxış edir. Kompyuter vasitəsi ilə müəllif hüquqlarının, ictimai təhlükəsizliyin, mülkiyyət hüququnun, əxlaq qaydalarının pozulması məqsədilə törədilən əməllər törədilən cinayətlə bağlı hadisələrə aid olunmalıdır.

Müasir dövrdə kibercinayətkarlıq kütləvi xarakter daşıyır və bir çox istifadəçilər cinayətkar qrupların girovuna çevrilir. Diqqət çəkən məqam budur ki, cinayət hüquqi tənzimləmənin yeni obyekti kimi kibercinayətkarlıq qlobal kompyuter şəbəkəsinin istifadəçilərinin sayına proporsional artır. Ekspertlərin proqnozlarına görə internet texnologiyalarının dinamik inkişafı və genişlənməsi ilə cinayətkarların sayı artmağa davam edəcək ki, bu da mütəşəkkil qlobal qruplaşmanı yaradılması prosesinə gətirib çıxara bilər. Məhz bu kimi xüsusiyyətlərinə görə təhlil edilən cinayətlərin qabaqlanması mürəkkəb sayılır.

Hüquqtətbiqetmə təcrübəsinin təhlili göstərir ki, bu sahənin təkmilləşdirilməsinin rezervləri hələ tükənməyib. Bundan başqa, kibercinayətkarlığın vəziyyə-

tinin təhlilinə görə mövcud cinayət-hüquqi normalar insan və vətəndaşların konstitusiya hüquq və azadlıqlarının cinayətkar qəsdlərdən müdafiəsinin lazımi effektivliyini təmin etmədiyi üçün təkmilləşdirməyə ehtiyac vardır.

Hesab edirik ki, kibercinayətkarlıqla effektiv mübarizə üçün onun spesifikasını və yayılma növlərini detallaşdırılmış şəkildə öyrənmək lazımdır. Hər bir ölkənin güc və hüquq mühafizə sisteminin fəaliyyətində koordinasiyanı təmin etmək və zəruri sayılacaq bütün səyləri birləşdirmək tələb olunur.Zənnimcə bu hal ayrılıqda hər bir ölkənin informasiya məkanının təhlükəsizliyini artırmağa yardım edə bilər.

Kompyuter informasiyası sahəsində cinayətkarlıqla effektiv mübarizəni təmin etmək üçün və hüquq-mühafizə, məhkəmə orqanlarının əməkdaşlığının hüquqi əsaslarını yaratmaq niyyəti ilə 01.06.2001-ci il tarixdə Minsk şəhərində "Kompyuter informasiyası sahəsində cinayətlərə mübarizədə MDB üzvü olan dövlətlərin əməkdaşlığı haqqında Sazişin ratifikasiyası haqqında"Qanun qəbul edilmişdir [3].

Kibercinayətkarlıqla mübarizədə beynəlxalq təcrübə göstərir ki, müasir cinayətkar fəaliyyətə qarşı effektiv əks-təsir məsələlərinin həllində prioritet istiqamətlərindən biri də HMO tərəfindən profilaktik xarakterli müxtəlif tədbirlərin həyata keçirilməsidir. Yüksək texnologiyalar sahəsində cinayətkarlığa qarşı mübarizədə beynəlxalq səviyyədə ən böyük nailiyyətlərdən biri də 23.11.2001-ci ildə "Kibercinayətkarlıq haqqında Konvensiyanın" qəbul edilməsi olmuşdur. Burada cinayətkar fəaliyyətin növləri, hüquq-mühafizə orqanlarının əməkdaşlığının prinsipləri və onu imzalamış ölkələrin qanunvericilik təkmilləşdirilməsi tələbləri müəyyən edilmişdir [4].

Cinayət hüququ sahəsində cəmiyyətin kibercinayətkarlıqdan müdafiəsinə yönəlmiş ümumi siyasət olmaqla, qeyd olunan konvensiya kompyuter sistemləri, şəbəkələri və kompyuter məlumatlarının konfidensiallığı, bütövlüyü və əlyetərliyinə qarşı, həmçinin sadalanan sistemlərdən, şəbəkə və məlumatlardan sui-istifadəyə qarşı yönələn hərəkətlərin qarşısını almaq üçün zəruridir.

Kibercinayətkarlıq haqqında Konvensiyada həmçinin virtual məkanda baxılan cinayətlər barəsində milli – hüquqi tənzimləmə səviyyəsini də görülməli

tədbirlər müəyyən edilib. Bunlar ilk növbədə maddi cinayət hüquqi və cinayət prosessual qanunvericiliyə dair ölçülərdir. Azərbaycan Respublikası Kibercinayətkarlıq haqqında Konvensiyanı ratifikasiya etdikdən sonra milli qanunvericiliyimizin tərkib hissəsi olan cinayət məcəlləsində zəruri olan dəyişikliklər edilmişdir.

Qeyd edilməsi vacib olan fikirlərdən biri də budur ki, hüquqpozmaların miqyası və dərəcəsinə, həmçinin dövlət təhlükəsizliyinə qarşı təhdidlərə baxmayaraq bəzi dövlətlər müəyyən prinsiplərə görə "Kibercinayətkarlıq haqqında" Konvensiyaya qoşulmayaraq virtual məkanda təşkilati-texniki mübarizə tədbirlərinin təkmilləşdirilməsi ilə kifayətlənmişlər. Bu da öz növbəsində kibercinayətkarlıqla mübarizənin effektiv mübarizəsi üçün hüquq-mühafizə orqanlarının işbirliyini məhdudlaşdırır.

İstifadə edilən mənbələrin siyahısı:

1. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının 29.06.2004-cü il tarixli 712-IIQ №-li Qanunu.

2. Kibercinayətkarlığa qarşı mübarizə üzrə Avropa Konvensiyası (9.11.2001).

3. Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности.

4. Приходько Ю.П., 2014 информационных отношений. Автореферат дисс.кан.юрид.наук.-Екатеринбург, 2003. – с.9.3. Закон «О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01.06.2001 года.