AZƏRBAYCAN RESPUBLİKASI DAXİLİ İŞLƏR NAZİRLİYİ

POLİS AKADEMİYASI

"DİO-nun İNZİBATİ FƏALİYYƏTİ" KAFEDRASI

İxtisasartırma fakültəsinin dinləyiciləri üçün

M Ü H A Z İ R Ə

Mövzu № 2: "Kibercinayətkarlıq haqqında" Konvensiya

Vaxt – 2 saat
Mühazirə – 2 saat

Bakı - 2019

AZƏRBAYCAN RESPUBLİKASI DAXİLİ İŞLƏR NAZİRLİYİ

POLİS AKADEMİYASI

"DİO-nun İNZİBATİ FƏALİYYƏTİ" KAFEDRASI

İxtisasartırma fakültəsinin dinləyiciləri üçün

M Ü H A Z İ R Ə

Mövzu № 2: "Kibercinayətkarlıq haqqında" Konvensiya

Vaxt – 2 saat
Mühazirə – 2 saat

Tərtib etdi:

Kafedranın baş müəllimi,
polis polkovnik-leytenantı **Heydərov H.M.**

Mühazirənin mətni kafedranın iclasında müzakirə olunmuş və təsdiq edilmişdir.
Protokol №*11* "*30*" *iyun* 2019-cu il.

Bakı - 2019

Mövzu № 2: ″Kibercinayətkarlıq haqqında'' Konvensiya

PLAN:

1. Kibercinayətlərin təşəkkül tarixi və inkişaf mərhələləri
2. Transmilli kibercinayətlərlə mübarizədə "Kibercinayətkarlıq haqqında" Konvensiya
3. Kibertəhlükəsizlik konvensiyasinin əhəmiyyəti

Ə D Ə B İ Y Y A T :

1. ″İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında″ Azərbaycan Respublikasının 03.04.1998-ci il tarixli Qanunu.
2. "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə milli strategiya″ (2003-2012-ci illər) haqqında Azərbaycan Respublikası Prezidentinin 17.02.2003-cü il tarixli Sərəncamı.
3. Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası. 23.05.2017-ci il.
4. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının 29.06.2004-cü il tarixli Qanunu.
5. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının 30.09.2009-cu il tarixli Qanunu.
6. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə" DİN-in 693 nömrəli 23.11.2009-cu il tarixli əmri.
7. Kərimov S. İnformasiya sistemləri. Bakı 2012.
8. Məcidli S.T. İnternet hüququ və etikası. Dərs vəsaiti. Bakı: "Elm və təhsil" nəşriyyatı, 2013.115-24 səh.
9. Məcidli S.T. "Kibercinayətlər". Bakı: 2019. 315 səh.
10. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı 2009.
11. Balacanov E. Kibercinayətlərlə mübarizə: çətinliklər və imkanlar/ İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14.05.2015-ci il. Bakı. 56-58 s.
12. Məmmədova K. Kibercinayətkarlığa qarşı mübarizənin prioritet istiqamətləri/ Azərbaycan Respublikasının Konstitusiyasında təsbit edilmiş dəyərlərin müdafəiəsi sahəsində müasir nəzəri və praktiki yanaşmalar mövzusunda Elmi-nəzəri konfrans/ Bakı, 2017. 118-120 s.
13. Əlizadə M.N., Bayramov H.M., Məmmədov Ə.S. İnformasiya təhlükəsizliyi. Dərslik, İqtisad universiteti nəşriyyatı, Bakı, 2016.
14. Wall D. S. The Transformation of Crime in the Information Age, 2007, Wiley, 2007, 288 p.
15. Convention on Cybercrime, Budapest, 21 November 2011, http://conventions.coe.int/ Treaty/en/Treaties/Html/185.htm
16. http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
17. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu. http://www.cert.az/konvensiya.html

GİRİŞ

İnformasiyalaşdırma müasir cəmiyyətin həyatında xarakterik cəhətlərdən biri hesab olunur. Elmi-texniki inqilab nəticəsində informasiya cəmiyyətinin yaranması informasiyanı ən mühüm resursa və başlıca amilə çevrilmişdir. Cəmiyyət tədricən öz informasiya infrastrukturunun vəziyyətindən müəyyən asılılıq vəziyyətinə düşür. Müasir dövrdə şəxsiyyətin, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması milli təhlükəsizliyin təmin olunması sistemində informasiya təhlükəsizliyi məsələlərini ön plana çıxarır. XXI əsrdə vətəndaşların, cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması milli təhlükəsizliyin təmin olunması sistemində informasiya təhlükəsizliyi məsələlərini ön plana çıxarır.

İnformasiya təhlükəsizliyinə istər təşkilati, istərsə də texniki metod və vasitələrin köməyi ilə nail olmaq olar. Təşkilati tədbirlər kompleksi, proqram, texniki və informasiya təhlükəsizliyini təmin edən digər metod və vasitələr informasiyanın mühafizə sistemini təşkil edir.

Elmi texniki tərəqqinin inkişafı artdıqca şəxsiyyətin, cəmiyyətin, dövlətin informasiya təhlükəsizliyi artmaqdadır və onun təhlükəsizliyi dövlət siyasətində müvafiq yeri tutmalıdır. İnformasiya irimiqyaslı qəzalara, hərbi konfliktlərə, dövlət idarəçiliyi, maliyyə sistemi və elmi mərkəzlərin fəaliyyətinin pozulmasına səbəb ola bilən faktora çevrilmişdir. Cəmiyyətin informasiyalaşdırılması və intellektuallaşdırılması səviyyəsinin artması onun informasiya təhlükəsizliyini daha etibarlı edir.

İnformasiya cəmiyyətinin çoxsaylı risklər qarşısında müdafiəsizliyi cinayət hüququ sistemini yeni çətinliklərlə üz-üzə qoymuşdur. Sərhədsiz kiberməkan fərdlərə və qruplara dövlətlərin yurisdiksiyalarındakı boşluqlardan cinayətkar məqsədlər üçün istifadə etməyə şərait yaradır. Transmilli fenomen olan kibercinayətkarlıq əksər hallarda cinayətkar və zərərçəkənin müxtəlif yurisdiksiyalarda yerləşməsi səbəbindən hüquq-mühafizə orqanları tərəfindən bu cür cinayətlərin istintaqı və mühakimə olunmasına maneə törədir. Dövlətlər daxili qanunvericiliyin lazımi səviyyədə olmaması və ya zəruri texniki resursların çatışmazlığı ilə əlaqədar kibercinayətlərin hədəfinə çevrilirlər. Bu sahədə ölkələr arasında beynəlxalq əməkdaşlığın qənaətbəxş olmaması isə həmin çətinliklərin aradan qaldırılmasına əngəl törədir. Bu səbəbdən kibercinayətkarlıqla mübarizədə beynəlxalq əməkdaşlıq, əlaqələndirmə və minimum harmonizasiya zəruridir. Beynəlxalq əməkdaşlıq dövlətlərin qanunvericiliklərində kiberməkandakı risklərin və təhdidlərin cinayət əməli kimi təsbit olunmasını və bu qanunvericiliklərin uyğunlaşdırılmasını tələb edir. Qloballaşma prosesi muasir cəmiyyətlərə musbət və mənfi təsirləri ilə xarakterizə olunur. Əksər hallarda bu proses rəqəmsal texnologiyalardan istifadə etməklə hər kəsin rifahına pozitiv təsir etsə də, bir sıra məqamlarda isə İKT inkişaf etdikcə adekvat olaraq virtual məkanda kriminal elementlər də aktivləşir. Daha doğrusu, bu prosesdən oz cinayətkar məqsədləri ucun yararlanmaq və ya sui-stifadə etmək istəyən xüsusi kateqoriya şəbəkə kriminalları formalaşır.

Ona gorə də, internetdən, elektron və rəqəmsal texnologiyalardan istifadənin, habelə kiberməkanın cinayət hüquqi tənzimlənməsi məsələsinin beynəlxalq və milli hüquqi aspektlərinin öyrənilməsi dövrün tələbi kimi çıxış edir.

Cəmiyyətdə yaranan yeni virtual münasibətlər sistemində, İnternetin, informasiya-kommunikasiya texnologiyalarının tərəqqisi beynəlxalq hüquqda beynəlxalq xarakterli və ya transmilli cinayətlərin yeni növünü – kibercinayətləri cəmiyyətin və hüququn mühüm elementinə cevirmişdir.

Avropa Şurasının (AŞ) 2001-ci ildə Budapeştdə imzalanmış və 2004-cü ildə qüvvəyə minmiş Kibercinayətkarlıq və ya Budapeşt Konvensiyası kibercinayətkarlıqla mübarizədə tarixi nailiyyət hesab oluna bilər və bu günə qədər müvafiq sahədə aparıcı və ən çox istinad olunan beynəlxalq sənəddir.

Bu mənada kibercinayətlərin elmi cəhətdən araşdırılması, virtual xarakterli münasibətlərin beynəlxalq və milli cinayət hüquqi nöqteyi-nəzərindən oyrənilməsi xususi aktuallıq kəsb edir.

Sual 1. Kibercinayətlərin təşəkkül tarixi və inkişaf mərhələləri

Cəmiyyətin informasiyalaşdırılmasının mənfi cəhətlərindən biri də kompüter cinayətkarlığıdır. Bəzi ədəbiyyatlarda müasir dövrə qədər hansı əməllərin kompüter cinayətləri kateqoriyasına aid edilməsi ilə bağlı mübahisələr gedir. Sualın həllinin mürəkkəbliyi ondan ibarətdir ki, kompüter texnikası vasitələrindən istifadə etməklə törədilən qeyri-qanuni əməllərin dairəsi (ənənəvi növlərdən başlayaraq yüksək riyazi və texniki hazırlıq tələb edən səviyyəyə qədər) olduqca genişdir.

1974-cü ildə fərdi kompüterlərin ilk dəfə olaraq kütləvi şəkildə bazara çıxarılması böyük informasiya massivlərinə məhdudiyyətsiz olaraq istifadəçilərin qoşulmasına imkan yaratdı. İnformasiyaya buraxılış nəzarəti, onun saxlanılması və tamlığı haqqında sual meydana çıxdı. İnformasiyanın mühafizəsi sahəsində həyata keçirilən təşkilati tədbirlər, eləcə də proqram və texniki vasitələr kifayət qədər effektiv olmamışdır.

Kompüter sistemlərinə qanunsuz daxil olma problemləri informasiya texnologiyalarının inkişaf etmiş ölkələrində özünü daha qabarıq surətdə büruzə vermişdir. Əlavə təhlükəsizlik tədbirlərinə əl atmağa məcbur olan bu ölkələr aktiv şəkildə hüquqi və eləcə də cinayət-hüquqi mühafizə vasitələrindən istifadə etməyə başladılar. Belə ki, Fransanın cinayət məcəlləsində 1992-ci ildə mülkiyyət əleyhinə olan cinayətlər sisteminə "Verilənlərin avtomatlaşdırılmış emalı sisteminə qəsd" adlı xüsusi başlıq əlavə olunmuşdur. Burada verilənlərin avtomatlaşdırılmış emalı sisteminə tam və ya qismən icazəsiz daxil olmaya, sistemin işinə mane olma və ya sistemin işinin pozulmasına, saxta üsul ilə informasiyanın daxil edilməsinə, verilənlər bazasının məhv edilməsi və ya dəyişdirilməsinə görə məsuliyyət nəzərdə tutulmuşdur.

Kompüter cinayətkarlığı Sovet İttifaqı məkanında da inkişaf edirdi. Belə ki SSRİ-də ilk kompüter cinayətkarlığı 1979-cu ildə Vilnyus şəhərində 78584 manat pulun oğurlanması ilə qeydə alınmışdır.

Müstəqillik əldə etdikdən sonra Azərbaycanda idarə və təşkilatlarda informasiyanın avtomatlaşdırılmış emalı vasitələrinin tətbiqi və sürətlə yayılması bu sahədə yaranan hüquq münasibətlərinin tənzimlənməsini ön plana çıxartdı. 1998-ci ildə kompüter informasiyaları ilə bağlı bir sıra normaları özündə əks edən ″İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında″ Azərbaycan Respublikasının Qanunu qəbul edilmişdir. İnformasiyanın avtomatlaşdırılmış emalı təhlükəsizliyini təmin edən hüquqi sistemin məntiqi inkişafı kimi 2000-ci ildə Azərbaycan Respublikasının Cinayət Məcəlləsinə kompüter informasiyası sahəsində əməllərinə görə cinayət məsuliyyətini nəzərdə tutan bir qrup maddələrin daxil edilməsi olmuşdur.

Əksər ölkələrdə və o cümlədən də Azərbaycanda qüvvədə olan cinayət qanunvericiliyi bu tip hüquqpozmaları təsnif etmək üçün kifayət qədər yumşaqdır. Sosial və texniki dəyişiklər yeni-yeni problemlər yaratmaqdadır. Buna görə də dünya təcrübəsindən məlum olan bəzi kompüter təcavüzləri cinayət qanunvericiliyi əməllərinə daxil olmur və beləliklə də hüquqi baxımdan cinayət kimi hesab edilmir. Belə bir nəzər nöqtəsi mövcuddur ki, kompüter cinayətləri xüsusi və hüquqi baxımdan cinayət kimi mövcud deyil və burada yalnız cinayətlərin kompüter cəhətlərindən danışmaq lazımdır.

Öz növbəsində mütəxəssislər belə bir nəticəyə gəldilər ki, kompüter cinayətləri kateqoriyasına o cinayətlər aid edilməlidir ki, burada cinayət qəsdinin obyekti qismində kompüter sistemlərində saxlanılan və emal olunan informasiya olsun, qəsd aləti qismində isə kompüter çıxış etsin.

Qeyd etmək lazımdır ki, cinayət qanunvericiliyi nöqteyi-nəzərdən maşın daşıyıcılarında, kompüterlərdə və ya onların şəbəkələrində olan və ya telekommunikasiya kanalları ilə kompüter üçün qəbul oluna bilən formada ötürülən

kompüter *informasiyası mühafizə* olunur. Kompüter informasiyası termini əvəzinə maşın daşıyıcısı terminini də istifadə etmək olar ki, bu da kompüter informasiyasının olduğu texnoloji vasitələri əks etdirir. Cinayətin predmeti və ya aləti qismində qanunvericiliyə müvafiq olaraq kompüter informasiyası, kompüter, kompüter sistemi və kompüter şəbəkəsi çıxış edə bilər.

Kompüter cinayətlərinin təsnifatları və onların kriminalistik xüsusiyyətləri suallarını nəzərdən keçirərkən kompüter cinayətləri tərifindən çıxış etmək məqsədəmüvafiqdir. Bu halda kompüter cinayətləri dedikdə kompüter texnikası vasitələrindən istifadə etməklə törədilən, qanunla ictimai təhlükəli əməl kimi nəzərdə tutulan hallar başa düşülür. Sosial kateqoriya kimi "kompüter cinayətləri" termininin istifadə olunması da həmçinin qanunauyğundur.

Kompüter cinayətlərinin təsnifatı müxtəlif əsaslara görə aparıla bilər. Belə ki, məsələn, bütün kompüter cinayətlərini şərti olaraq iki böyük kateqoriyaya bölmək olar:

- kompüterin işinə müdaxilə etməklə bağlı cinayətlər;
- kompüterləri vacib texniki vasitələr kimi istifadə edən cinayətlər.

Kompüter cinayətlərinin ümumi təsnifatlarından biri 1983-cü ildə İqtisadi Əməkdaşlıq Təşkilatı ekspertlər qrupu tərəfindən təklif olunmuşdur. Ona müvafiq olaraq kompüter cinayətlərinin aşağıdakı kriminoloji qrupları müəyyənləşdirilmişdir:

- iqtisadi cinayətlər;
- şəxsi hüquq və şəxsi dairə əleyhinə cinayətlər;
- dövlət və ictimai maraqlar əleyhinə cinayətlər.

İqtisadi kompüter cinayətləri daha geniş yayılmış hesab olunurlar. Onlar tamah məqsədi ilə törədilir və kompüter dələduzluğu, proqramların oğurlanması ("kompüter piratlığı"), xidmətlərin oğurlanması, iqtisadi casusluq kimi halları özündə birləşdirir.

Şəxsi hüquq və şəxsi dairə əleyhinə kompüter cinayətləri şəxs haqqında verilənlərin qanunsuz yığılması, şəxsi informasiyanın yayılması (məsələn, bank və ya tibbi sirlər), xərcləri haqqında informasiyanın qanunsuz alınması və s. özündə birləşdirir.

Dövlət və ictimai maraqlar əleyhinə kompüter cinayətləri dövlət və ictimai təhlükəsizlik əleyhinə yönəlmiş, dövlətin müdafiə qabiliyyətinə təhlükə yaradan və eləcə də avtomatlaşdırılmış səsvermə sistemlərindən sui-istifadə və s. cinayətləri özündə birləşdirir.

Kompüterlərin işinə müdaxilə ilə bağlı əsas cinayət növlərini sadalayaq:

♦ ***Tamah məqsədi ilə informasiya-hesablama şəbəkəsində və ya kompüterdə saxlanılan informasiyaya icazəsiz daxil olma.***

İcazəsiz daxil olma bir qayda olaraq özgə adı istifadə etməklə, texniki qurğuların fiziki ünvanlarını dəyişməklə, tapşırığın həllindən sonra qalan informasiyanın istifadə olunması, informasiya daşıyıcısında saxlanılan proqram və informasiya təminatının modifikasiyası, verilənlərin ötürülməsi kanalına qoşulmaqla aparat yazısının işə salınması ilə yerinə yetirilir.

Bəzi hallarda naməlum bir şəxs kompüter sisteminə daxil olaraq özünü qanuni istifadəçi kimi qələmə verir. Autentik identifikasiya vasitələrinə malik olmayan sistemlər (məsələn, fizioloji xarakteristikaları üzrə: əl-barmaq izlərinə görə, göz qişasının rənginə görə, səsə və s.), bu üsula qarşı aciz qalırlar. Qanuni istifadəçilərin kod və digər identifikasiya şriftlərinin alınması, sisteminə daxil olmaq üçün ən sadə yol hesab olunur.

İcazəsiz daxil olma sistemin sıradan çıxması nəticəsində də baş verə bilər. Məsələn, əgər bir istifadəçinin bəzi faylları açıq vəziyyətdə qalırsa, onda digər istifadəçilər onlara aid olmayan verilənlər bankının hissələrinə buraxılış əldə edə bilərlər.

♦ ***Kompüter viruslarının hazırlanması və yayılması.***

Virus proqramları bir sistemdən digərinə kommunikasiya şəbəkələrindən keçməklə virus xəstəliyi kimi yayılma xüsusiyyətlərinə malikdirlər.

♦ ***Proqram təminatına "məntiqi bombalar"ın daxil edilməsi.***

"Məntiqi bomba" proqramları müəyyən şərtlər yerinə yetirdikdən sonra işə düşür və tam və ya qismən kompüter sistemini sıradan çıxarırlar.

♦ ***Kompüter şəbəkəsinin proqram-hesablama kompleksinin yaradılması və istismarı zamanı ağır nəticələrə səbəb olan səhlənkarlıq.***

Kompüter sisteminin xüsusiyyəti ondan ibarətdir ki, heç də qüsursuz proqram prinsip etibarı ilə mövcud deyildir. Əgər layihə istənilən texnika sahəsində böyük etibarlıqla yerinə yetirirsə, proqramlaşdırma sahəsində bu etibarlıq olduqca şərtidir, bəzi hallarda isə demək olar ki, mümkün deyildir.

♦ ***Kompüter informasiyasının saxtalaşdırılması.***

Bu növ kompüter cinayətkarlığı daha geniş miqyas almaqdadırlar. Bu cinayət kompüter sisteminə qanunsuz daxil olmanın növlərindən biridir, yalnız o fərqlə ki, bu cinayəti törədən qanuni istifadəçinin özü olur.

♦ ***Proqram təminatının oğurlanması.***

Adi oğurluqlar mövcud cinayət qanunvericiliyinə düşüyü halda proqram təminatının oğurlanması problemi xeyli dərəcədə çətinliklər yaradır. Əksər ölkələrdə proqram təminatının xeyli hissəsi oğruluq və oğruluğun mübadiləsi yolu ilə yayılır.

♦ ***İnformasiyanın icazəsiz köçürülməsi, dəyişdirilməsi və məhv edilməsi.***

İnformasiyaya qanunsuz müraciət edərkən maşın informasiyası fonddan çıxarılmadan köçürülür. Buna görə də maşın informasiyası cinayət-hüquqi mühafizənin müstəqil predmeti kimi qeyd olunmalıdır.

♦ ***Verilənlər bankından, verilənlər bazasından informasiyaya icazəsiz baxış keçirilməsi və ya informasiyanı məhv olunması.***

İnformasiyanın qorunub-saxlanılması kompüterlərin ən vacib funksiyalarından biridir. Belə qorunub saxlanmanın ən çox yayılmış növü verilənlər bazasıdır. Verilənlər bazası müəyyən şəkildə strukturlaşdırılmış informasiyadan təşkil olunmuş xüsusi formatlı fayldır.

Verilən – predmet sahəsinin obyektlərini, proseslərini və gerçəkliklərini xarakterizə edən ayrı-ayrı cəhətlər, atributlardır. Verilən – bazaya daxil ediləcək informasiya vahidləridir. Verilən – verilənlər bazasının elementləridir.

Baza dedikdə kompüterin köməyi ilə tapılan və emal oluna bilən verilənlərin təqdim edilməsi və təşkili formasının sistemləşdirilmiş məcmusu (məsələn: maddələr, hesabatlar) başa düşülür.

Kompüter cinayətlərinin törədilmə üsulları. Qeyd etmək lazımdır ki, kompüter vasitəsilə müəyyən işlərin görülməsində elektron maşınlarından geniş istifadə edən təşkilatlar və ya fiziki şəxslər kompüter cinayətkarlığından sığorta olunmamışlar. Kompüter cinayətkarlığının əsas yönəldiyi obyektlərin siyahısına nəzər yetirək:

a) Hərbi və kəşfiyyat, əks-kəşfiyyat idarələrinin kompüterləri.
b) Ticarət və biznes təşkilatları (rəqabət məqsədi ilə).
c) Bank və maliyyə məsələləri ilə məşğul olan bank filialları.
d) Hökumət və bələdiyyələrin kompüterləri.
e) İstənilən fiziki və hüquqi şəxslərin kompüterləri.

Hərbi və kəşfiyyat, əks-kəşfiyyat idarələrindən casusluq məqsədi ilə onların kompüterlərindən lazımi informasiyaların oğurlanması əsas başa düşülməlidir. Beynəlxalq aləmdə dövlətlərin milli təhlükəsizliyinin təmin olunmasında kompüterlərin rolunun böyüklüyü danılmazdır. Belə ki, kompüterlərdə müxtəlif növ məlumatlar saxlanılır. Bu növ məlumatlar aşağıdakılardır:

1. Peyk vasitəsilə təşkil olunmuş hərbi hava qüvvələrinin orbit parametrləri.
2. Təhlükəsizlik departamentinin kəşfiyyat məlumatları və s.

Yuxarıda adları göstərilən kompüter cinayətkarlığının əsas obyektləri olan sahələrə kompüter cinayətkarlarının müdaxilə etməsi, bu sahələrdə maliyyənin olması ilə birbaşa bağlıdır.

Bu cinayətkarlıq barədə müxtəlif alimlər öz əsərlərində bu növ cinayətlərin baş vermə səbəblərini şpionluq, xobbi, maliyyə hərisliyi və asan yolla qazanc əldə etmə kimi açıqlamış, izah etmiş və pisləmişlər.

Amerika alim Kliff Stoll öz yazdığı əsərində, ″The Cuckoo Egg″ kitabında nəşr etdirmiş və izah etmişdir ki, Qərbi Almaniyadan olan bir nəfər ″xaker″ (kompüter cinayətkarı) ondan artıq dövlətin hərbi kompüter sistemlərindən məlumatlar çıxarmış və bununla da o, məlumatlar aid olan məsələnin hərbi sirrinin açılması üçün real təhlükəyə çevrilmişdir. Daha sonra 1988-ci ildə xaker olan Kevin (″Kondor″ təxəllüslü) Müdafiə Nazirliyinin kompüter şəbəkəsinə daxil olmuş və oradan VMS v 5.0 Digital Equipment Corporation-a məxsus olan hərbi əməliyyatın ilkin versiyasının layihəsini çıxarmış və Pataksent bazasında hərbi-dəniz qüvvələrinin kompüterlərinin yaddaşına salmışdır. Ölkə rəsmilərinin dediklərinə görə, bu insidentdə heç bir hərbi sirrin açılmasından danışmaq olmaz. Sonrakı əməliyyat-axtarış tədbirləri nəticəsində Kevin Mitnik yoxlanılmış və cinayət qanunu ilə nəzərdə tutulmuş əsaslarla cinayət məsuliyyətinə cəlb olunaraq azadlıqdan məhrum edilmişdir.

Amerika Birləşmiş Ştatlarının Müdafiə Nazirliyinin kompüter sistemlərinin müdafiəsinin inkişaf etdirilməsinə baxmayaraq, heç bir stabillik əldə olunmur. Bu narahatlıq təkcə müdafiə sahəsində deyil, eləcə də bütün hökumət sahələrinə də aid olunur.

Məsələn, 1990-cı ildə 3 nəfər şəxs hökumət orqanlarının kompüterlərinə, həm də özəl telefon kompaniyalarının kompüter sistemlərinə daxil olmuş və sabiq Filippin prezidenti F.Markosa və onun yaxın qohumları barədə məlumatlar əldə etmişlər. Bu məlumatlar ″Məxfi″ qrifinə malik olan və açıqlanması mümkünsüz hesab edilən informasiyalara aid olunur.

Başqa bir misalda, məsələn, 1990-cı ildən başlayaraq ABŞ-ın Energetika sahəsində baş verən kompüter cinayətkarlığı. Lakin xakerlərə imkan verilməməlidir ki, hansısa məlumatı əldə edə bilsinlər. Tezliklə onlar tapılmış və hüquq mühafizə orqanları tərəfindən qanunvericiliyə əsasən, məsuliyyətə cəlb olunmuşlar.

XX əsrin axırlarında ABŞ ilə keçmiş SSRİ arasında gedən soyuq müharibənin başa çatmasına baxmayaraq, yeni era – qlobal iqtisadi rəqabət dövrü başlanmışdır. Bu sahədə yaranan rəqabət isə özlüyündə istehsal casusluğunun meydana gəlməsinə ən böyük zəmin yaradır. Belə ki, dost ölkələr də bir-birinə qarşı bu cür casusluğu işə salıblar. Buna misal olaraq göstərmək olar ki, bu yaxınlarda ″Boeing″ firması Fransanın ″Airbus″ firmasına qarşı casusluq hərəkətləri törətmişdir.

″Boeing″ firmasının ixtisaslaşdırılmış əməkdaşları ″Airbus″ firmasının təyyarələrində oturacaqların altına və bu firmanın əməkdaşlarının qaldıqları mehmanxana otaqlarında telefon danışıqlarına qulaq asılması üçün telefon aparatlarına xüsusi ″juçok″lar quraşdırmışlar. Bu hərəkətin əsasında isə ″Airbus″ firmasına aid olan korporativ xarakterli informasiyanın əldə edilməsi dayanır. Bu məsələyə aid öz subyektiv fikrimi bildirsəm, onu qeyd etməliyəm ki, ″Boeing″ kimi dünya şöhrətli firma istənilən rəqibinə qarşı bu hərəkəti etməsi onun dünyada olan işgüzar nüfuzunun aşağı enməsinə zəmin yaradır və bu cür iqtisadi casusluğa məruz qalan firmalar isə özlərində bu insindentlə əlaqədar tutarlı faktları vardırsa, mütləq hüquq-mühafizə orqanlarına müraciət etməlidirlər.

Sual 2. Transmilli kibercinayətlərlə mübarizədə "Kibercinayətkarlıq haqqında" Konvensiyası

Cəmiyyətin idarə olunması, əsasən, zaman və məkan sərhədləri daxilində fəaliyyət göstərməsi üçün yaradılmış mexanizmlər vasitəsilə həyata keçirilmişdir. Kiberməkanda tənzimləmə isə məkan və zaman məhdudiyyətlərinin aradan qalxması ilə əlaqədar olaraq ənənəvi yanaşma və mexanizmlər vasitəsilə həyata keçirildikdə lazımi effekti vermir. Bu hal analoji olaraq kiberməkanda törədilmiş cinayətlərlə mübarizə üsul və mexanizmlərinin effektivliyi və səmərəliliyinə də aid edilə bilər. Müasir cəmiyyətin və dövlətin davamlı inkişafını şərtləndirən İKT-nin geniş tətbiqinin limitsiz və azad informasiya axınını təmin etməsi bu imkanlardan cinayətkar məqsədlər üçün istifadə olunmasını istisna etmir. Rəqəmsal texnologiyaların yaratdığı mühit cinayətlərin törədilməsi və miqyasının genişlənməsi üçün münbit məkan rolunu oynayır.

Kiberməkan və fiziki məkan arasındakı kəmiyyət və keyfiyyət göstəricilərindəki fərqlər bu iki müxtəlif məkanda törədilmiş cinayətlərdə də öz əksini tapır. Kibercinayətkarlıqla mübarizənin effektivliyi və səmərəliliyinin təmin olunması bu fərqlərdən irəli gələn çətinlik və problemlərin ətraflı araşdırılması, onların həlli zamanı nəzərə alınması, həmçinin İKT-nin kibercinayətkarlıqla mübarizədə yaratdığı imkanların müəyyən olunması və tətbiqindən asılıdır. Belə ki, kiberməkan cinayətlərin törədilməsi üçün şərait yaratmaqla yanaşı, həm də onların araşdırılması və ya qarşısının alınması üçün yeni imkanları və çətinlikləri özündə birləşdirir.

Cəmiyyətin və dövlətin həyatında və inkişafında İKT-dən geniş istifadə olunması ölkənin beynəlxalq müstəvidə rəqabət qabiliyyətini və davamlı inkişafını təmin etməklə yanaşı, ondan asılılığını da artırır. İKT-nin geniş tətbiqindən asılılıq isə öz növbəsində informasiya infrastrukturlarına edilən hər hansı hücum və müdaxilənin zərər vurma potensialını və həcmini yüksəldir. Son illərdə Azərbaycan Respublikasında e-hökumət, e-təhsil, e-səhiyyə, e-ticarət və s. sahələrə ayrılmış investisayalar sayəsində ölkənin informasiya infrastrukturunun əhəmiyyətli dərəcədə genişləndirilməsi, eyni zamanda, potensial kibercinayətkarlıq obyektlərinin də sayının artması kimi qəbul edilə bilər. İnformasiya infrastrukturuna edilmiş hücumlar, əsasən, kompüter sistemlərinin və ya məlumatlarının qəsdən zədələnməsi, silinməsi, korlanması, dəyişdirilməsi, bloklanması, saxtalaşdırılması, yaxud ələ keçirilməsi yolu ilə həyata keçirilir ki, bunlar da həm Kibercinayət haqqında Konvensiyaya, həm də Azərbaycan Respublikası Cinayət Məcəlləsinə əsasən kibercinayətkarlıq sayılan əməlləri təşkil edir.

Symantec Korporasiyası tərəfindən hazırlanmış kibercinayətkarlıqla bağlı hesabatda dünya üzrə İnternetdən istifadə edən yetkin insanların 50%-nin kibercinayətkarlıqla və ya digər neqativ onlayn vəziyyətlərlə üzləşməsi ilə bağlı məlumatlar, ümumilikdə, kibercinayətkarlıqla mübarizə mexanizlərinin zəifliyinin göstəricisi kimi qəbul oluna bilər]. Hal-hazırda dünya əhalisinin 73%-nin (3 milyarddan artıq), Azərbaycan Respublikası əhalisinin 73%-nin İnternetə çıxışla təmin olunması, İKT-nin inkişafı sahəsində qarşıya qoyulmuş məqsədə əsasən isə yaxın illərdə 85%-nin sürətli İnternetlə təmin olunacağını nəzərə alsaq, zəruri mexanizmlərin yerində olmamasının potensial zərərləri daha da aydın görünə bilər. Həcmindən və hədəf obyektlərin sayından asılı olmayaraq yalnız bir və ya eyni anda bir neçə mənbədən, avtomatlaşdırılmış formada idarə oluna bilən, transmilli xarakterli kibercinayətkarlıqla mübarizə daha intensiv və adekvat mühafizə tədbirlərinin və mexanizmlərinin tətbiqini zəruriləşdirir. Buna görə də, informasiyalaşdırmaya yatırılmış invesitisiya ilə

informasiya infrastrukturunun və vətəndaşların mühafizəsinə ayrılmış resurslar arasındakı mütənasibliyin asılılıqla risk arasındakı mütənasibliyə əsasən müəyyən olunması vacibdir. 2007-ci ilin aprel və may aylarında Estoniya Respublikasının bir sıra dövlət, media, bank və digər mühüm veb-saytlarının məruz qaldığı kiber hücumlar da məhz zəruri mühafizə tədbir və mexanizmlərinin çatışmazlığı səbəbindən əhəmiyyətli zərərlə nəticələnmişdir. Həmin hücumların arxasındakı motiv bu gün Azərbaycan Respublikasının inkişafını istəməyən qüvvələr üçün də yad deyil. Üzvü olduğu Kibercinayətkarlıq haqqında Konvensiya və ya digər hüquqi mexanizmlərin Estoniya Respublikasına qarşı olan kiber hücumları istisna etməməsi, bunu deməyə əsas verir ki, Azərbaycan Respublikasının da kritik informasiya infrastrukturuna edilə biləcək cinayətkar motivli və ya düşmən xarakterli oxşar hücumlardan effektiv qorunması üçün həmin kritik informasiya infrastrukturlarının müvafiq mühafizə sistemləri ilə paralel təşkili və inkişaf etdirilməsi vacibdir.

İKT-nin geniş istifadəsi və yaratdığı imkanlar həmçinin cinayət əməllərinin törədilməsindəki müxtəlifliklərlə müşayiət olunur. Bu texnologiyalardan istifadə etməklə törədilən cinayətlərin qarşısının alınması üçün güclü mühafizə, cinayətlərin təhqiqatı və istintaqı üçün isə adekvat araşdırma alət və vasitələri tələb edilir. Araşdırma vasitələrinin adekvatlığı isə özündə həm texniki, həm də hüquqi cəhətləri birləşdirir. Kibercinayətkarlıqla effektiv mübarizə üçün cinayət hüququ ilə yanaşı, cinayət - prosessual hüquqi mexanizmlərin və müvafiq araşdırma texnikalarının inkişaf etdirilməsi zərurəti Kibercinayət haqqında Konvensiyanın izahedici məruzəsində də öz əksini tapmışdır.

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

A. İnformasiyanın həcmi və ötürülmə sürəti.

Müasir kompüter yaddaşlarında saxlanılan və şəbəkələr vasitəsilə ötürülən böyük həcmdə informasiyanın araşdırılması məqsədilə seçilməsi və analiz olunması bu istiqamətdə əsas çətinliklərdən biridir. Onu da qeyd etmək lazımdır ki, müasir texnologiyalar və kompüter sistemləri araşdırmanın sürətli və avtomatik həyata keçirilməsini təmin edə bildiyi üçün hüquq-mühafizə orqanlarına problemin texniki tərəfinin öhdəsindən nisbətən asanlıqla gəlmə imkanı yaradır. Məsələn, beynəlxalq təcrübədə uşaq pornoqrafiyasının dövriyyəsi ilə bağlı cinayətlərin araşdırılması

zamanı bu cür araşdırma proqramlarından geniş istifadə olunur. Lakin axtarışın avtomatlaşdırılması prosesi araşdırılan informasiyanın məzmun və formatından asılı olduğu üçün məhdud xarakter daşıyır və məzmunun qiymətləndirilməsi araşdırmanı yenidən həyata keçirən şəxslərin üzərinə düşür.

Hüquq mühafizə orqanları üçün vəziyyəti mürəkkəbləşdirən digər bir cəhət ondan ibarətdir ki, cinayətin elementlərini özündə daşıyan informasiyanın ötürülməsi, əsasən, çox qısa bir zamanda - cəmi bir neçə saniyə ərzində həyata keçirilir. Bu isə araşdırma məqsədilə zəruri sübutların toplanılması üçün həddən artıq məhdud zamanın olması deməkdir. Eyni zamanda, elektron sübutların çox qısa bir zaman ərzində asanlıqla dəyişdirilə, tamamilə məhv edilə bilməsi cinayət təqibi üzrə icraat prosesində operativ və daha diqqətli davranmanı tələb edir. Bu çeviklik İKT-nin tətbiqi ilə əldə oluna bilən sayılsa da, mövcud normativ-hüquqi mexanizmlər adekvat çevikliyin əldə olunmasını hər bir halda təmin edə bilmir və ya etmir. Çünki müvafiq qanunvericilik sübutların toplanılmasında istifadə olunan üsul və vasitələrin seçilməsi və tətbiqində bir sıra müddəalara riayət olunmasını tələb edir. Məsələn, sübutların müəyyən olunması və toplanılması zamanı şəxsi məlumatların toxunulmazlığı ilə bağlı məhdudiyyətlər buna misal ola bilər. Qanunvericiliyin tələblərini pozmaqla aparılan proses-sual hərəkətlərin prosessual qanunvericiliyə görə hüquqi qüvvəsinin olmaması bu kimi hallarda çevikliyi istər-istəməz ikinci plana keçirir. Bundan başqa, maddi sübutların digər növlərindən fərqli olaraq, ən xırda diqqətsizliklə sübuti əhəmiyyətini tamamilə itirə biləcəyini nəzərə alaraq qeyd olunmalıdır ki, araşdırma zamanı əldə olunmuş elektron sübutların surətindən və ya şəklindən istifadə olunması onların orijinalının qorunması üçün, hər bir halda, daha məqsədəuyğundur. Əlavə olaraq, qeyd etmək lazımdır ki, bulud texnologiyalarına (Cloud Computing) keçidin sürətlənməsi gələcəkdə kibercinayətlərin araşdırılması üçün zəruri olan elektron sübutların toplanması önündə əlyetərliliyin bir az da çətinləşməsi problemini yaradacaq və zəruri və mötəbər sübutların toplanmasını məhdudlaşdıracaq.

B. İnformasiyanın yeri, anonimlik və konfidensiallıq

İKT elektron sübutlarla bağlı çətinliklərin texnoloji tərəfinin həllində müəyyən rola və imkanlara malik olsa da, problemin hüquqi aspektlərinin həlli müvafiq normativ-hüquqi mexanizmlərin tətbiqindən asılıdır. Kibercinayətlərin təhqiqatı və istintaqı özündə adekvat araşdırma alət və vasitələrinin tətbiqi ilə yanaşı, elektron sübutlarla bağlı müvafiq prosessual qaydalara və qanunvericiliyə riayət olunmasını da tələb edir. Lakin sadəcə milli qanunvericiliyin təkmilləşdirilməsi kibercinayətkarlıqla mübarizənin effektivliyini və səmərəliyini təmin etmir. Çünki cinayətin obyekti ilə subyekti arasındakı fiziki yaxınlığa və ya təmasa ehtiyac olmadan realizə olunan transmilli xarakterli kibercinayətlərin araşdırılması yurisdiksiya məsələləri ilə yanaşı, elektron sübutların da toplanmasında çətinlik yaradır. Belə ki, bir sıra hallarda kibercinayəti törədən şəxsin yerinin müəyyən olunma prosesində yaranan çətinlik həmin cinayət üçün əhəmiyyət daşıyan elektron sübutların əldə olunması önündə də əngəllər yaradır. Eyni zamanda, infrastrukturun böyük hissəsinin özəl və ya şəxsi mülkiyyətdə olması hüquq - mühafizə orqanlarından müxtəlif sektorlarla əməkdaşlığı tələb edir.

Bu anlamda, daha bir diqqətəlayiq məqam isə kibermәkan üzərindən həyata keçirilən informasiya mübadilələrində anonimliyin və konfidensiallığın təmin olunması üçün imkanların geniş olmasıdır. Bu cür imkanların kibercinayətlərin realizəsi zamanı icraçılar tərəfindən geniş istifadə olunması cinayətlərin araşdırılması zamanı sübutların toplanması və qiymətləndirilməsi kimi hüquqi prosesləri mürəkkəbləşdirir. Qeyd olunduğu kimi, kibermәkan üzərindən törədilən bütün əməliyyatlar müəyyən

izlər buraxır ki, bu da onların müvafiq metodlarla rahat izlənilə bilməsini mümkün edir. Onlayn əməliyyatlarda tam anonimliyin təmin olunmasının “mif” olduğunu nəzərə alsaq, kiberməkanın yaratdığı bu maneənin də aşılmasının texnoloji həllinin çətin olmadığını anlamaq olar.

Bu, bütün hallarda araşdırma üçün lazımi informasiyaya limitsiz çıxışın əldə oluna bilməsi kimi qəbul edilməməlidir. Belə ki, informasiyanın yalnız sahibinə və ünvanlandığı şəxsə məlum olan alqoritmlərə əsasən şifrələnməsini həyata keçirərək daha yüksək səviyyəli konfidensiallıq təmin edən proqramların və texnologiyaların İnternet istifadəçiləri üçün əlyetərliliyi bu anlamda araşdırma qarşısında anonimlikdən daha böyük bir maneə yaradır. Açar şifrənin araşdırma orqanları tərəfindən şifrə sahibindən əldə edilə bilməsi məlumatların əlyetərliyinin mümkünsüzlüyünü aradan qaldırır. Lakin anonimliklə yanaşı, bu cür proqramlar vasitəsilə də şifrələnmiş bütün kommunikasiyalar və elektron sənədlər qanuni müdaxilələrə və axtarışlara qarşı immunitet qazanır, və bu cür həyata keçirilən elektron köçürmələr istənilən dövlət nəzarətindən kənarda qala bilir.

Kibercinayətlərin törədilməsində son illərdə bu metodlardan istifadə hallarının sürətlə artmasını nəzərə alaraq anonim və şifrələnmiş informasiya və sənədlərin sübut qismində toplanması, yoxlanılması, qiymətləndirilməsi, saxlanması ilə bağlı həm normativ-hüquqi, həm də elmi-texniki bazanın təkmilləşdirilməsi zəruridir.

C. Beynəlxalq müstəviyə çıxış

Müasir kompüter şəbəkələri vasitəsilə həyata keçirilən əməliyyatlarda ərazi yurisdiksiyaları üzrə fəaliyyət göstərən milli ənənəvi cinayət-hüquqi mexanizmlərinin təsir dairələrindən rahatlıqla kənara çıxıla bilməsi kibercinayətlərin törədilməsi üçün yeni imkanlar və hədəflər yaratmasına baxmayaraq, onların araşdırılması önünə bir sıra çətinliklər çıxarır. Çünki kiberməkan ərazilərə bölünərək yurisdiksiyalar üzrə fəaliyyət göstərmir və iş mexanizmi fiziki məkanda tətbiq olunan ərazi məhdudiyyətlərindən asılı deyil. Buna görə də, transmilli kibercinayətkarlığın araşdırılması və qarşısının alınmasında fiziki məkanın tələblərinə uyğunlaşdırılmış hüquqi mexanizmlər vasitəsilə effektivliyin təmini mümkün olmur. Kibercinayətkarlıqla hərtərəfli, səmərəli və effektiv şəkildə mübarizə aparılması və onların araşdırılması zamanı zəruri olan elektron informasiyanın toplanılması beynəlxalq əməkdaşlığı, xüsusilə də ölkələr arasındakı qarşılıqlı hüquqi və texniki yardımı şərtləndirir.

Beynəlxalq əməkdaşlıq və qarşılıqlı yardımın əldə olunması bir sıra formal hüquqi qaydalara riayət olunmasını şərtləndirdiyi, habelə əməkdaşlığın təşkili müəyyən zaman tələb etdiyi üçün kibercinayətin araşdırılması üçün zəruri olan operativliyin əldə olunması bir sıra hallarda mümkün olmur və nəticədə araşdırmanın səmərəsizliyinə gətirib çıxarır. Araşdırmanın aparılması zamanı beynəlxalq əməkdaşlığın və yardımın əldə olunmasının sürətinin artırılması məqsədilə Kibercinayətkarlıq haqqında Konvensiyanın 35-ci maddəsində müəyyən olunmuş, sutkada iyirmi dörd saat, həftədə yeddi gün fəaliyyət göstərən müvafiq əlaqələndirmə mərkəzlərinin yaradılması nəzərdə tutulmuşdur.

Sual 3. Kibertəhlükəsizlik konvensiyasinin əhəmiyyəti

Avropa Şurasının (AŞ) 2001-ci ildə Budapeştdə imzalanmış və 2004-cü ildə qüvvəyə minmiş Kibercinayətkarlıq və ya Budapeşt Konvensiyası kibercinayətkarlıqla mübarizədə tarixi nailiyyət hesab oluna bilər və bu günə qədər müvafiq sahədə aparıcı və ən çox istinad olunan beynəlxalq sənəddir. 2014-cü ilin fevral ayına qədər Budapeşt Konvensiyası 49 ölkə tərəfindən imzalanmış, 41 ölkə tərəfindən ratifikasiya edilmişdir. Azərbaycan da Budapeşt Konvensiyasını 30 iyun 2008-ci ildə imzalamış, 30 sentyabr 2009-cu ildə ratifikasiya etmişdir. Milli qanunvericiliyin Konvensiyaya uyğunlaşdırılması məqsədilə Azərbaycan Respublikası Cinayət Məcəlləsinə və digər normativ hüquqi aktlara müvafiq əlavə və düzəlişlər edilmişdir. Layihəsinin hazırlanması və qəbul edilməsi AŞ tərəfindən həyata keçirilməsinə baxmayaraq, Budapeşt Konvensiyası AŞ üzvü olmayan ölkələr üçün də açıqdır və regional saziş hesab olunmur. AŞ üzvü olmayan ABŞ, Kanada, Yaponiya və Cənubi Afrika onu imzalamış, ABŞ və Yaponiya, Avstraliya, Dominikan Respublikası və Mavriki Respublikası isə ratifikasiya etmişdir.

Budapeşt Konvensiyası kibercinayətkarlıqla mübarizədə ən geniş əhatə dairəsinə malik sənəddir. Belə ki, bu Konvensiya bütün dünya üzrə İnternet istifadəçilərinin üçdə bir hissəsini əhatə edir. Bu sənəddə kibercinayətkarlıq üzrə maddi və prosessual hüquqlar, yurisdiksiya sahəsində qabaqcıl təcrübə öz əksini tapıb. Ən vacib cəhətlərindən biri odur ki, Konvensiyanın müddəaları əksər üzv ölkələr tərəfindən milli qanunvericiliyə tətbiq edilmişdir.

Budapeşt Konvensiyasının ən mühüm çatışmazlığı kimi onun Avropa sərhədlərindən kənara çıxmaması göstərilir. Belə ki, Konvensiyanı ratifikasiya etmiş 41 dövlətdən yalnız 5-i (ABŞ, Yaponiya, Avstraliya, Dominikan Respublikası və Mavriki Respublikası) AŞ üzvü deyildir. Bu səbəbdən regional səviyyədə (Karib hövzəsi, Qərbi Afrika və s.) kibercinayətkarlıq üzrə qanunvericilik formalaşdırılmağa başlanmışdır. Lakin 2014-cü ilin yanvar ayında Afrika Birliyi tərəfindən hazırlanmış Kibertəhlükəsizlik Konvensiyası İnternetdə ifadə azadlığını məhdudlaşdıracağı, qitə ölkələrinin iqtisadiyyat və mədəniyyətinə mənfi təsir göstərə biləcəyi səbəbindən qəbul edilmədi. Bundan başqa, Budapeşt Konvensiyasına qoşulma tələblərinin BMT konvensiyaları ilə müqayisədə daha sərt olması ona daha çox ölkələrin qoşulması üçün maneə hesab olunur. Konvensiyaya üzv olmaq üçün ona üzv olan bütün ölkələrin yekdil razılığı vacibdir. Budapeşt Konvensiyasının 37-ci maddəsinə görə, AŞ Nazirlər Şurası konvensiya üzrə razılığa gəlmiş tərəflərlə məsləhətləşmələrdən və onların anonim razılığını aldıqdan sonra Şuranın üzvü olmayan və ya Konvensiyanın hazırlanmasında iştirak etməyən istənilən dövləti Konvensiyaya qoşulmağa dəvət edə bilər.

Bundan başqa, inkişaf etməkdə olan ölkələr Konvensiyanın layihəsinin hazırlanmasında iştirak etməmişdir. Hazırda inkişaf etməkdə olan ölkələrin İnternet istifadəçilərinin sayı inkişaf etmiş ölkələrinkindən daha çoxdur və birincilərin kiberməkandakı risklərə məruz qalması ehtimalı daha böyükdür. Bu səbəbdən, kibercinayətkarlıqla mübarizəyə inkişaf etməkdə olan ölkələrin cəlb edilməsi zəruridir.

Konvensiyanın müasir və gələcək texnologiyaları əhatə etməsi məqsədilə texnoloji baxımdan neytral dildə tərtib olunmasına baxmayaraq, ən mühüm arqumentlərdən biri onun kiberməkandakı müasir cinayət və riskləri əhatə etməməsidir. Bundan əlavə, elektron sübutların məhkəmə tərəfindən qəbul edilməsi qaydaları və İnternet provayderlərinin məsuliyyəti, təşkilati məsələlər, dövlət və özəl sektor əməkdaşlığı Konvensiyada öz əksini tapmamışdır.

Konvensiyasının 32b maddəsinin beynəlxalq hüququn hamılıqla tanınmış prinsiplərindən olan milli suverenlik prinsipi ilə ziddiyyət təşkil etməsi narahatlıq doğurur. Belə ki, Konvensiyanı ratifikasiya edən dövlət digər dövlətlərə öz ərazisində təhqiqat aparmağa icazə verməklə milli suverenlik prinsipindən qismən imtina etmiş olur. Həmin maddəyə görə, hüquq-mühafizə orqanları məxsus olduqları ölkənin sərhədləri xaricində yerləşən, ictimaiyyətə açıq olmayan kompüter məlumatlarını bu cür məlumatları açıqlamaq üçün qanuni icazəsi olan şəxsin qanuni və könüllü icazəsi ilə əldə edə bilərlər.

Kibercinayətkarlıqla mübarizədə ümumi hüquqi çərçivənin təsbit olunmasında AŞ son dövrlərə qədər mühüm rol oynasa da, artıq bu təşəbbüsün istər qanunvericilik, istərsə də təcrübə baxımından Avropa Birliyinə (AB) keçdiyi iddia olunur. İstənilən halda kibercinayətkarlıqla mübarizədə Avropa mübarizə modeli dəyərlidir və gələcək qlobal inkişaf üçün baza rolunu oynaya bilər. Lakin ümumilikdə, kibercinayətkarlığın qlobal xarakteri ilə əlaqədar Avropa qitəsində həyata keçirilən tədbirlər qənaətbəxş hesab edilmir. Bu səbəbdən bir sıra dövlətlər BMT çərçivəsində yeni qlobal kibertəhlükəsizlik konvensiyasının işlənib hazırlanmasını zəruri hesab edir.

On ildən artıq bir müddətdə kibertəhlükəsizlik məsələlərinə öz gündəliyində geniş yer ayıran BMT bu rolu 1949-cu ildən telekommunikasiya və İKT sahəsində ixtisaslaşmış quruma çevrilmiş BTİ vasitəsilə həyata keçirir. BTİ kiberməkandakı təhdid və zəif nöqtələrə qarşı şəbəkə, xidmət və mexanizmlər işlənib hazırlanmasında dövlət və özəl sektor üçün qlobal mərkəz hesab olunur. BMT kibertəhlükəsizlik məsələləri ilə əlaqədar öz mövqeyini Baş Assambleya çərçivəsində qəbul edilmiş qətnamələrlə ifadə etmişdir.

İnformasiya Cəmiyyəti üzrə Ümumdünya Sammitinin ikinci - Tunis mərhələsində iştirak edən dövlətlər İKT-nin istifadəsinə inam və etibarı formalaşdırmaq üzrə vahid moderator rolunu BTİ-yə həvalə etmiş, 2006-cı ildə BTİ-nin yeni Baş katibi seçilmiş H.Ture BMT çərçivəsində qəbul edilmiş sənədlər arasında ən geniş əhatə dairəsinə malik olan və ən perspektivlisini - Qlobal Kibertəhlükəsizlik Gündəliyi və Qlobal Strateji Hesabatı təqdim etmişdir. BMT çərçivəsində kibertəhlükəsizlik üzrə qlobal konvensiyanın layihəsinin hazırlanmasında qeyd edilən sənədlərin danışıqlar üçün baza rolu oynayacağı gözlənilir.

Bundan başqa, bir sıra tədqiqat institutları və alimlər kibercinayətkarlıqla mübarizə üzrə mühüm layihələr işləyib hazırlamışlar. Amerika Huver İnstitutu tərəfindən 2001-ci ildə hazırlanmış və bu günə qədər kibercinayətkarlığa qarşı beynəlxalq sənəd üçün aparıcı akademik təklif hesab edilən “Kibercinayətdən və terrorizmdən müdafiəni gücləndirmək üçün Beynəlxalq Konvensiyanın Stanford Layihəsi 2000”dir. Layihə kiberməkanda əsas cinayətlərin beynəlxalq səviyyədə tanınması, təhqiqatı, cinayətkarların ekstradisiyası və mühakiməsi sahəsində əməkdaşlıq edilməsi üçün universal sazişi təşviq etmək məqsədilə yaradılmışdır.

2014-cü ilin yanvar ayında Afrika Birliyi tərəfindən hazırlanmış Kibertəhlükəsizlik Konvensiyası İnternetdə ifadə azadlığını məhdudlaşdırmaq, qitə ölkələrinin iqtisadiyyat və mədəniyyətinə mənfi təsir göstərə bilmək ehtimalı səbəbindən Birlik üzvləri tərəfindən qəbul edilmədi. Bu hadisə hətta regional səviyyədə konvensiya layihəsi üzrə ölkələr arasında razılığın əldə edilməsinin asan olmadığını və mövcud alətlərin təkmilləşdirilərək istifadə edilməsinin məqsədəuyğunluğunu bir daha sübut edir.

Qlobal kibertəhlükəsizlik konvensiyasının tərəfdarları və əleyhdarları.

Kibercinayətkarlıqla mübarizə sahəsində yeni beynəlxalq konvensiyanın hazırlanması təşəbbüsü ilə bir neçə dəfə çıxış etmiş Rusiyanın bu məsələdə əsas

arqumenti Budapeşt Konvensiyasının köhnəlmiş olması və dövlətlərin suverenliyini pozan müddəaları ehtiva etməsidir. Qeyd edək ki, Rusiya AŞ üzvü olmasına baxmayaraq, Konvensiyaya qoşulmamışdır. Konvensiyanın kiberterrorizmi tənzimləməməsi də Rusiyanı narahat edən məsələlərdəndir. Lakin Rusiya yeni Konvensiyanın AB və ya NATO deyil, məhz BMT çərçivəsində hazırlanmasının tərəfdarıdır. 2011-ci ilin sentyabr ayında Rusiya, Çin, Tacikistan və Özbəkistan bu məsələ ilə bağlı BMT Baş Assambleyası çərçivəsində müvafiq qətnamənin qəbul edilməsi təşəbbüsü ilə çıxış etmişdir. Budapeşt Konvensiyasının qlobal standart kimi qəbul edilməsinin əleyhinə olan BTİ Baş katibi H. Turenin mövqeyi bu səbəbdən Rusiya tərəfindən dəstəklənir.

Lakin qeyd edilən məsələ ilə bağlı Rusiya ilə Qərb dövlətləri, xüsusilə, ABŞ arasında ortaq məxrəcə gəlinməsi real görünmür. İki dövlət arasında fikir ayrılığının əsas səbəbi onlar üçün müxtəlif mənalar daşıyan "informasiya təhlükəsizliyi" anlayışıdır. Kiberməkanın fiziki infrastrukturunu təşkil edən naqillər, serverlər, routerlər və s. kimi rəqəmsal informasiyadan hazırlanmış proqram təminatı informasiya texnologiyaları hesab olunur. Bu mənada, böyük ziyan vurmaq iqtidarında olan Stuxnet kimi proqram təminatı "informasiya silahı"dır. ABŞ informasiya təhlükəsizliyinin bu cür məhdud şərhinə üstünlük versə də, Rusiya informasiya, ideya və komminikasiya platformalarının hakimiyyət əleyhinə istifadə edilməsindən ehtiyat edərək, bu cür platformaların da "informasiya təhlükəsizliyi" termini ilə əhatə olunmasının tərəfdarıdır.

Hələ 1998-ci ildə Rusiya BMT Baş Assambleyasına "informasiya silahları"nın müəyyənləşdirilməsi və günahkarların cəzalandırılması ilə bağlı qətnamə layihəsi təklif edərkən ABŞ mövcud qanunların kiberməkandan hərbi məqsədlərlə istifadəni kifayət qədər tənzimləməsi səbəbindən Rusiyanın mövqeyini dəstəkləməmişdir. Ehtimal olunur ki, o dövrdə ABŞ-ın bunu etməsi üçün üç səbəb var idi. Birincisi, ABŞ digər dövlətlər tərəfindən özünə qarşı kibermüharibəni real hesab etməyərək, kiberməkanda milli təhlükəsizliyi üçün əsas təhlükəni terroristlərdən gözləyirdi. İkincisi, ifadə azadlığının məhdudlaşdırılması Amerika dəyərləri və rəsmi xarici siyasətlə bir araya sığa bilməzdi. Üçüncüsü, ən güclü kiberhücum imkanlarına malik olması ehtimal edilən bir dövlət kimi kibersilahların məhdudlaşdırılması ABŞ-ın maraqlarına uyğun olmazdı.

Lakin 2010-cu ildə Rusiya və bir sıra digər dövlətlərlə birgə BMT Baş Assambleyasında qlobal səviyyədə kibertəhlükəsizliyi genişləndirən beynəlxalq normaların işlənib hazırlanması zəruriliyini bəyan edən qətnamə layihəsini dəstəkləyən ABŞ-ın mövqeyində dəyişiklik baş verdi.

Siyasi kursda bu cür kəskin dəyişikliyin baş verməsi səbəbləri tam aydın olmasa da, bunun ABŞ siyasətçiləri tərəfindən kiberməkanda öz ölkələrinin zəifliyinin dərk etmələri ilə əlaqələndirmək olar.

Ağ Evin kibertəhlükəsizlik üzrə keçmiş müşaviri R.Klarke ölkənin milli kibertəhlikəsizliyi üçün güclü kiberhücum imkanlarına malik olmağı üç vacib faktordan yalnız biri hesab edir. Kibermüdafiə imkanları və ölkənin kiberməkandan asılılığı dərəcəsi də milli kibertəhlükəsizlik üçün vacib elementlərdir. Rusiya, Çin və İran ABŞ-dan daha zəif kiberhücum imkanlarına malik olmasına baxmayaraq, daha güclü kibermüdafiə imkanlarına malikdirlər və kiberməknadan daha az asılıdırlar. Hər üç faktoru vəhdət şəklində nəzərdən keçirən R.Klarke ABŞ-ın milli kibertəhlükəsizliyinin adıçəkilən dövlətlərdən daha zəif olması qənaətinə gəlir.

Lakin qeyd edilən cəhətlərin ABŞ-ın kibertəhlükəsizliklə bağlı dövlət siyasətində dəyişikliyə səbəb olması beynəlxalq kibersiyasətdə digər dövlətlər, o cümlədən Rusiya

ilə ortaq məxrəcə gəlməsinə kömək etmədi. Belə ki, Rusiyanın yuxarıda adıçəkilən qətnamə layihəsi ABŞ və əsas Qərb dövlətləri tərəfindən ifadə azadlığını məhdudlaşdırması səbəbindən dəstəklənmədi. Qətnamə layihəsi informasiyanın axtarılması, əldə edilməsi və yayılması hüquqlarının milli qanunlar əsasında tənzimlənməsini təklif etsə də, təşəbbüskar dövlətlərin (Rusiya, Çin, Tacikistan və Özbəkistan) nəşr, yayım və İnternet azadlığı sahəsində hüquqları məhdudlaşdıran ölkələr arasında ilk yerləri tutması Qərb dövlətlərinin qətnamə layihəsini qəbul etməməsi ilə nəticələndi.

Bundan başqa, siyasi məqsədlər üçün kibercinayətkarlığın müxtəlif növlərini maliyyələşdirməkdə ittiham olunan Rusiya və Çinin kibercinayətlərin istintaqı və mühakiməsi üzrə beynəlxalq əməkdaşlığın yüksək standartları ilə razılaşaraq öz üzərilərinə öhdəlik götürmələri şübhə ilə qarşılanır. Belə ki, Rusiya 2007-ci ilin aprel ayında Tallində Bürünc əsgər heykəlinin yerinin dəyişdirilməsindən sonra Estoniya və Rusiya arasında diplomatik qalmaqal yaranmışdır. Bu hadisədən sonra Rusiya Estoniyanın dövlət qurumlarına, banklarına, KİV-lərinə məxsus saytlara edilən DDoS hücumlarına görə məsuliyyət daşımadığını bəyan etmişdir. Lakin həmin insidentlərin araşdırılması üçün Estoniya hökuməti ilə əməkdaşlıq etməkdən imtina etməsi hücumların arxasında məhz Rusiyanın dayanmasını ehtimal etməyə əsas vermişdir.

Budapeşt Konvensiyasının Asiya-Sakit Okean İqtisadi Əməkdaşlığı, AB, İnterpol, Amerika Dövlətləri Təşkilatı tərəfindən dəstəkləndiyini və kibercinayətkarlıqla mübarizədə aydın və hərtərəfli çıxış yolları təklif etdiyini bəyan edən AŞ Budapeşt Konvensiyasının layihəsinin hazırlanmasında iştirak etməmiş dövlətlərin siyasi səbəblərdən ona qoşulmaqdan imtina etmələrini anlayışla qarşılayır. Bununla belə, Konvensiyaya qoşulan ölkələrin Budapeşt Konvensiyasının Komitəsinə üzvlük əldə edərək onun gələcəkdə yenilənməsində iştirak edə biləcəyini bəyan edir. AŞ kibercinayətkarlıqla mübarizə üzrə yeni konvensiya layihəsinin hazırlanmasının deyil, BMT çərçivəsində Budapeşt Konvensiyasının təmin etdiyi prosessual hüquqlar və əməkdaşlıq imkanları üzrə konsensusun əldə edilməsini təklif edir.

Kibercinayətkarlıqla effektli mübarizə aparmaq və kiberməkanda təhlükəsizliyə nail olmaq üçün Budapeşt Konvensiyasına daha çox ölkənin qoşulması vacibdir. Yeni qlobal konvensiya layihəsinin hazırlanması illərlə davam edə, diplomatik mübahisələrlə müşayiət oluna və müsbət sonluqla nəticələnməsi qeyri-müəyyən olan bir proses ola bilər. Bu həm də üzv dövlətlər tərəfindən Budapeşt Konvensiyası əsasında artıq həyata keçirilməkdə olan qanunvericilik islahatlarını ləngidə, qanunvericilik və digər tədbirlərin həyata keçirilməsinin təxirə salınmasına səbəb ola bilər. Bundan başqa, artıq mürəkkəb qanunvericilik islahatları həyata keçirmiş və Konvensiyanı tətbiq etmiş ölkələr bu cəhdlərini yenidən təkrarlamaq məcburiyyətində qala bilərlər.

Budapeşt Konvensiyasının üzv ölkələr tərəfindən tətbiqinin effektli olması və onlara kibercinayətkarlıqla mübarizədə mühüm təcrübə qazandırması faktı inkar edilə bilməz.

Konvensiyanın yenilənməyə ehtiyacı olduğunu etiraf etmişdir və bu sənəd təşkilata üzv olmayan ölkələrin qoşulması və Konvensiyanın təkmilləşdirilməsində iştirak etməsi üçün açıqdır.

Yeni qlobal konvensiyanın Budapeşt Konvensiyasından fərqli tənzimləmə predmeti və istinad edəcəyi standartlar vacib aspektlərdir. Bu cür konvensiyanın inkişaf etməkdə olan ölkələr üçün daha aşağı standartlar təsbit edərək rəqəmsal uçurumu daha da dərinləşdirmək və effektli beynəlxalq əməkdaşlığa əngəl yaratmaq ehtimalı vardır. Bundan başqa, daha aşağı və daha az spesifik prosessual hüquq

müddəalarının daha aşağı təhlükəsizlik tədbirləri nəzərdə tutması kiberməkanda mövcud vəziyyətin daha da gərginləşməsinə səbəb ola bilər.

İndiki mərhələdə artıq bir çox ölkələrdə başlanmış harmonizasiya prosesini və maliyyə imkanlarının çatışmazlığını nəzərə alaraq, harmonizasiya proseslərini təkrarlamaqdansa, resursları artıq mövcud olan alətlərin tətbiqinə yönəltmək, ölkələrə Budapeşt Konvensiyasının və əlaqədar tədbirlərin tətbiqi üçün texniki yardım göstərməyin kibertəhlükəsiziliyin təmin edilməsi üçün daha effektli olduğu hesab edilir.

Qeyd olunanları nəzərə alaraq, mövcud Konvensiyanın kiberməkandakı müasir risklərə uyğun şəkildə yenilənməsi və ona daha çox ölkənin cəlb edilməsi daha rasional hesab olunur. Budapeşt Konvensiyası artıq 10-cu ildir ki qüvvədədir. Onun qlobal standarta çevrilə bilməsi üçün daha çox dövlət tərəfindən imzalanması və ratifikasiya edilməsi məqsədilə AŞ və BMT tərəfindən birgə tədbirlər həyata keçirilməli və Konvensiyaya qoşulma tələbləri yumşaldılmalıdır.

Kibercinayətlərin anlayışı: fərqli tendensiyalar və konseptual baxışlar. Müasir dövrdə informasiya cəmiyyətinin inkişafı, qloballaşmanın daha geniş məkanlara, o cümlədən informasiya mühitinə sirayət etməsi bu sahədə transmilli cinayətlərə və dünya ölkələrinin milli hüququnda yeni cinayətlər kateqoriyasının formalaşmasına, bu cinayətlərlə mübarizəyə və cəza sisteminə öz əhəmiyyətli təsirini göstərmişdir. Beynəlxalq sistemdə İKT-nin inkişafı ilə əlaqədar fəaliyyətlər və səmərəli idarəetmə bu sistemin hüquqi cəhətdən nizamlanmasını zəruri etmişdir. Bu mənada beynəlxalq birliyi qlobal informasiya mühitinin hüquqi tənzimləməsi, xüsusilə bu məkanın cinayətkar qəsdlərdən mühafizəsi olmadan təsəvvür etmək mümkün deyil və bu, sosial tənzimetmənin mühüm vasitəsi kimi çıxış edərək, orada fəaliyyət göstərən subyektlərin qanuni maraqlarının reallaşdırılmasını təmin etməklə ictimai münasibətlərin nizamlanmasına xidmət edir. Kompüter sistemləri, şəbəkə və proqramlarının, İKT, habelə internetin fəaliyyəti ilə əlaqədar meydana çıxan ictimai münasibətlərin effektli şəkildə tənzimlənməsi üçün bu cür mexanizmlərin seçilməsi və tətbiqi olduqca mühüm əhəmiyyət kəsb edir. Virtual məkanın inkişafı, kompüterlər şəbəkəsinin geniş istifadəsi detallı hüquqi reqlamentasiya tələb edir. Hüquqi tənzimləmənin zəifliyi nəticəsində bu gün kompüter cinayətləri cinayətkar qəsdlərin ən təhlükəli növünə çevrilmişdir.

Hazırda beynəlxalq praktikada kompüter sistemlərinin və şəbəkələrinin, o cümlədən internetin tənzimlənməsi sahəsində tətbiq edilən hüquqi mexanizmlər bunlardır: qanunvericilik normaları, sosial normalar, özünütənzimləmə, məhkəmə təcrübəsi, beynəlxalq hüquq.

Bu mexanizmlər isə hazırda internet hüquqlarının və insan haqlarının inkişafı ilə əlaqədar olaraq biri-biri ilə daha da sıx bağlı fəaliyyət göstərir. Burada ilk növbədə ümum məcburi hüquq normalarına cəmiyyət daxili zərurət və ya ehtiyac yaranır. Elmi-texniki tərəqqi bəzi hallarda neqativ ictimai təzahürlərlə, xüsusilə bir sıra cinayətlərlə müşayiət olunur. Daha sonra, buna adekvat olaraq dövlətlərin hüquq normaları yaratma fəaliyyətləri inkişaf edir. Hazırda qlobal şəbəkədə və informasiya kommunikasiyalarının inkişafı ilə əlaqədar mövcud olan texnoloji fəaliyyətin prioritet sahələrində əsas insan hüquq və azadlıqlarının, söz və ifadə azadlığının, şəxsi həyatın, şəbəkə istifadəçiləri haqqında məlumatların, habelə onların əqli mülkiyyət hüquqlarının qorunması, xüsusilə müasir informasiya cəmiyyəti üçün daha aktual olan problem – kibercinayətkarlıqla mübarizə məsələləri ön planda çıxış edir.

Ona görə də kibercinayətlərin anlayışı və əsas xüsusiyyətlərinə nəzəri və normativ yanaşma bu günkü dönəm üçün olduqca vacibdir.

Bu problemlə bağlı çoxsaylı elmi əsərlər yazılmış və kibercinayətlərin anlayışının ilə bağlı cəhdlər edilərək, nəzəri cəhətdən araşdırılmış, xarici ölkələrin milli hüquq normalarının qarşılıqlı təhlili əsasında məsələyə akademik münasibət sərgilənmişdir.

İnternet istifadəçilərinin hüquqazidd davranışları bəzən cinayət tərkibi yaradan əməllərin törədilməsinə səbəb olur. Buna görə də, müasir beynəlxalq hüquqda mövcud sosial-iqtisadi inkişaf, elmi-texniki tərəqqi və İKT üzrə yeniliklərdən asılı olaraq beynəlxalq xarakterli cinayətlərin də diapazonu dəyişir və genişlənir. Bu mənada hazırda veb-məkan üçün aktual olan cinayət tərkiblərindən biri kibercinayətkarlıqdır (kompüter cinayətkarlığı). Bu əməllər müasir dövrdə rəqəmsal texnologiyaların, kompüter və internet şəbəkələrinin, bankomatların, ödəniş kartlarının, ödəmə terminallarının və s. cinayətkar məqsədlərlə istifadəsi ilə əlaqədar cinayət xarakteri kəsb etmişdir. İctimai qayda əleyhinə yönələn bu cinayətlər həm milli, həm də beynəlxalq hüquqi tənzimetmənin predmetini təşkil edir. Müasir beynəlxalq hüquqda isə bu məsələlər internet hüququ və beynəlxalq cinayət hüququ kontekstində nəzərdən keçirilir.

İctimai həyatın müasir qlobal inkişaf şəraiti informasiya texnologiyaları, telekommunikasiyalar, yaxud bütövlükdə kiberməkan olmadan təsəvvür edilə bilməz. Müasir dövrdə İKT o qədər sürətlə inkişaf edir ki, bəzən qanunvericilik və hüquq-mühafizə orqanları bu inkişafa adekvat reaksiya vermək imkanından uzaq olurlar. Bu xüsusilə özünü kiberməkanın tənzimlənməsində daha bariz şəkildə göstərir.

Yeni yaranan qlobal sistemlər, informasiya texnologiyaları, bütövlükdə hüquq sistemləri, xüsusilə əsas insan hüquq və azadlıqlarına hörmət prinsipi əsasında insan və vətəndaş hüquqlarına münasibətdə zəruri qanunvericilik və təşkilati mexanizmlərin yaradılması üzrə mühüm addımların atılmasını tələb edir. Dünya proseslərinin qloballaşması insan hüquqlarına yeni yanaşmalar müəyyən edir, lakin onların ümumi başlanğıc prinsiplərini dəyişdirmir. Bununla yanaşı insan hüquq və azadlıqlarına yeni situasiyalarla əlaqədar bir sıra düzəlişlərin edilməsi də qaçılmazdır.[1]

Qeyd etmək lazımdır ki, informasiya kommunikasiya texnologiyaları proseslərinin dünya hüquq sisteminə təsiri bir sıra çətinliklərlə xarakterizə olunmuşdur. Bu səbəbdən ölkənin real təhlükəsizliyinin qorunması üçün müxtəlif texnologiyalar, sərhədlər var. Amma virtual mühit artıq müəyyən məkanla bağlı deyil. Burada dünyanın istənilən ölkəsi bizim qonşumuzdur və ya əksidir. Belə bir şəraitdə virtual məkanın təhlükəsizliyinin təmin olunması çox çətindir. Müasir dünyamızın sakinləri ictimai münasibətlərin, demək olar ki, bütün sahələrində istifadə edilən informasiya texnologiyalarından bu və ya digər dərəcədə asılıdır. İnkişaf etmiş dövlətlər informasiya texnologiyalarından fəal istifadə etməklə məlumat mübadiləsini sürətləndirir və insan resurslarına qənaət edirlər. Fəal məlumat mübadiləsi prosesləri cəmiyyətin şəffaflığına təsir göstərir, dövlət idarəçiliyini daha səmərəli edir, vətəndaş cəmiyyətinin formalaşmasına xidmət edir. İctimai həyatda "elektron demokratiya", "elektron dövlət" adlandırılan müasir idarəetmə formaları meydana gəlir. Bu proses qarşısıalınmazdır və o, dövlət hakimiyyətinə bu prosesi necə idarə etmək, ədalətin, insan hüquqlarının və sosial bərabərliyin təmin olunması, dövlət hakimiyyətinə inam və digər demokratik dəyərləri qorumaqla elektron aləmi necə tarazlaşdırmaq kimi konkret sxemlər təqdim edir. Alimlərin fikrincə, yaxın zamanlarda orta şəxsi kompüterlər insan beyninin imkanlarını ötüb keçəcək, 2029-cu ildə elektron intellekt insanın əqli qabiliyyətindən 1000 dəfə artıq olacaq. Əlli milyonluq auditoriyanı əhatə etmək üçün radioya 38, televiziyaya isə 13 il lazım olmuşdur. 1993-cü ildə qlobal

[1] Əliyev. Ə. Müasir beynəlxalq hüquqda insan hüquqları, əhali və miqrasiya problemləri. Dərslik, Bakı- 2007. Səh 14. 488 s.

şəbəkədə yalnız 50 səhifə olduğu halda, bu gün onların sayı milyardlarladır. Ötən il dünyada internet istifadəçilərinin sayı 3,8 milyardı keçib. Bu da dünya əhalisinin yarıdan çoxunu təşkil edir. İnternet istifadəçilərinin 53%-i Asiya-Sakit Okean, 15%-I Avropa, 13%-i Afrika və Orta Şərq, 10%-i Latın Amerika, 9%-i Şimali Amerika, 21%-i Cin, 12%-I Hindistan və ABŞ-ın payına düşüb. İnternetdən istifadə edən dünya əhalisinin göstəricisi 2009-cu ildə 24 faiz idisə, keçən il bu rəqəm 51 faizədək artıb.[2] Bu isə İKT-nin dinamik inkişafını və ictimai münasibətlərə, o cümlədən milli və beynəlxalq hüquqa da təsirini şərtləndirir.

Bütün cəmiyyətlərdə cinayətlər həmin cəmiyyətin inkişaf tendensiyasına uyğun paylanır. XX əsrin 80-90-cı illərinə qədər kompüter texnologiyasının istifadəsi ilə bağlı cinayətlərin payı çox da böyük olmamışdır. Lakin zəhmətsiz qazanc məqsədilə və əyləncə naminə kompüter şəbəkələrindən qanunsuz istifadə, uşaq pornoqrafiyasının yayılması, kompüter və informasiya sistemlərinın dağıdılması təhlükəsi, habelə kompüter şəbəkəsindən dələduzluq məqsədilə istifadə olunması kompüter cinayətlərinin adi formalarından hesab olunur.

Bir sıra əlamətlərinə görə kibercinayətlərin beynəlxalq və milli hüquq prizmadan aşağıdakı növləri fərqləndirilir: kompüter məlumatlarının və sisteminin konfidensiallığı, bütövlüyü və əlverişliliyi əleyhinə cinayətlər, kompüterlə əlaqəli cinayətlər, məzmununu kompüter informasiyası təşkil edən hüquq pozuntuları, uşaq pornoqrafiyası ilə əlaqəli materiallarla bağlı hüquqazidd əməllər, müəlliflik və əlaqəli hüquqların pozulması ilə bağlı cinayətlər.

Qeyd etmək lazımdır ki, kibercinayətlərin anlayışı məsələsində beynəlxalq təşkilatların, o cümlədən Birləşmiş Millətlər Təşkilatının xüsusi yanaşması da elmi araşdırma baxımından əhəmiyyətli hesab olunur. Bu məsələyə BMT səviyyəsində münasibət bildirilməsi ona görə zəruridir ki, kibercinayətlər müasir dövrdə yalnız bir dövləti və onun milli sərhədlərini əhatə etməyərək, eləcə də bütövlükdə dünya birliyinin narahatlıq mövzusuna çevrilmişdir. BMT tərəfindən kibercinayətlərin standart tərifi Cinayətlərin qarşısının alınması və cinayətkarlıqla mübarizə üzrə BMT-nin X Konqresində müəyyən olunmuşdur. Həmin Konqresin bir seminarı kompüter şəbəkələrinə dair cinayət problemlərinə həsr olunmuş, kibercinayətlərin iki əsas növü fərqləndirilərək, onun anlayışı aşağıdakı kimi müəyyən edilmişdir:

1. Dar mənada kibercinayətlər (kompüter cinayətləri). Bu o deməkdir ki, elektron əməliyyatlar vasitəsilə yönəldilən hər hansı qeyri-qanuni hərəkət və hərəkətsizliyin məqsədi kompüter sistemlərinin təhlükəsizliyinə və onlarda olan məlumat (verilənlər) bazasına xələl gətirməkdir.

2. Geniş mənada kibercinayətlər (kompüter ilə əlaqədar cinayətlər). Bu isə o deməkdir ki, hər hansı qeyri-qanuni hərəkət və hərəkətsizlik kompüter sistemləri və ya şəbəkələri, o cümlədən belə cinayətlər informasiyaların kompüter sistemləri və ya şəbəkələrindən qanunsuz olaraq əldə edilməsi, təklif olunması və yayılması vasitəsilə və ya onlarla əlaqəli şəkildə törədilir.

Lakin bir məsələni xüsusi vurğulamaq lazımdır ki, “kompüter cinayəti” anlayışının beynəlxalq hüquq müstəvisində ilk dəfə istifadəsi İnterpola məxsusdur. Belə ki, İnterpolun 11-13 dekabr 1979-cu ildə keçirilmiş Üçüncü Beynəlxalq Dələduzluq üzrə Simpoziumunda “kompüter dələduzluğu” haqqında prezentasiya təqdim olunmuş və vurğulanmışdır ki, müxtəlif ölkələr arasında telefonlar, peyklər və s. vasitəsilə davamlı şəkildə artan kommunikasiyalar səbəbindən kompüter cinayətlərinin təbiəti artıq

[2] Dünyada internet istifadəcilərinin sayı 3,8 milyardı kecib. https://report.az/i-kt/dünyada-internet-istifadecilerinin-sayi-3-8-milyardi-kecib/

beynəlxalq xarakter kəsb edir. Beləliklə də, beynəlxalq hüquq tarixində ilk dəfə kompüter cinayətləri lokal səviyyəli kriminal aktlar çərçivəsindən çıxmaqla, İnterpol tərəfindən transmilli mahiyyətli əməllər olaraq hələ XX əsrin ikinci yarısından başlayaraq tanınmış və faktiki surətdə dövlətlərin milli cinayət qanunvericiliyi üçün tövsiyə olunan "kompüter cinayətləri" terminindən istifadə olunmağa başlanmışdır.

Kibercinayətlərə internetdən istifadə etməklə törədilən dələduzluq, insanların narahat edilməsi və ya onlara qarşı xuliqanlıq, qanunsuz pornoqrafiyanın yüklənilməsi, musiqilərin oğurlanması, milli təhlükəsizliyin pozulması kimi əməllər aiddir.

"Kibercinayətlər, internet şəbəkəsindən qanunsuz istifadə nəticəsində kompüter və informasiya sistemlərinın dağıdılması və virtual məkanda qəsdən törədilən digər cəzalandırılmalı, hüquqazidd ictimai təhlükəli əməllər başa düşülür".[3] Bu tərifdən göründüyü kimi, "kibercinayət" anlayışı təkcə bir kompüterdə və ya lokal informasiya məkanında törədilən qanunsuz əməl olmayıb, eyni zamanda, bu fəzada bütün texnoloji vasitələr arasında əlaqələndirici rolunda çıxış edən internet vasitəsilə törədilən çoxsaylı hüquqazidd əməlləri də əhatə edir.

Bütün bunları nəzərə alaraq qeyd olunan tərifl ərin Kembric lüğətində verilən tərifl müqayisəsindən kibercinayət anlayışına bir daha aydınlıq gətirmiş olarıq. Belə ki, həmin lüğətdə kibercinayətə aşağıdakı kimi anlayış verilmişdir: "Kibercinayət" – həm kompüterlərin istifadəsi, həm də informasiya texnologiyalarının və qlobal şəbəkələrin istifadəsi ilə bağlı olan cinayətdir. Bu anlayışların yekun təhlilindən isə belə bir nəticəyə gəlmək mümkündür ki, əslində "kompüter cinayəti" termini əsas etibarilə konkret hər hansı kompüterə qarşı və ya həmin kompüterdə mövcud olan məlumat bazasına yönəlmiş cinayəti özündə ehtiva edir.

Bu səbəbdən də BMT-nin kibercinayətlər üzrə mütəxəssisləri Kibercinayətkarlıq haqqında Konvensiyanı şərh edərkən haqlı olaraq qeyd edirlər ki, "kibercinayət" termini ən yaxşı halda kompüter və informasiyalarla əlaqədar hərəkət və ya

Kibercinayətlərin təsnifatı: yeni cinayət modelləri. Kibercinayətlərin təsnifatı məsələsi də müasir beynəlxalq hüquqda və xarici ölkələrin milli qanunverciliklərində geniş müzakirə olunan problemlərdəndir.

Ümumilikdə bu qeyri-qanuni əməlləri aşağıdakı kimi qruplaşdırmaq olar:

1) Kompüterə qanunsuz daxil olma;
2) Kompüter məlumatına və ya proqramlarına ziyan vurma;
3) Kompüter sabotajı;
4) Kommunikasiyaların qanunsuz olaraq dayandırılması və ya kəsilməsi;
5) Kompüter casusluğu.

Bu qeyd olunan məsələlər kibercinayətlərin anlayışı, növləri və cinayət tərkibi ilə bağlı təfsilatı əks etdirə bilməz. Birincisi, bu cinayətlərin xarakteri elədir ki, bunlar daim inkişafdadır və texnoloji innovasiyalara həmişə uyğun gəlməlidir. İkincisi isə bunun üçün kibercinayətlərin universal əsasda müvafiq ayrıca tərifinin müəyyən edilməsi daha məqsədəuyğun olardı.

Kibercinayətlər beynəlxalq cinayətlərin surətlə inkişaf edən sahəsidir. Əksər cinayətkarlar heç bir fiziki və ya virtual sərhədlər tanımadan cinayətkar fəaliyyətlərinin müxtəlif diapazonunu genişləndirmək üçün sürət, rahatlıq və internetin anonimliyini axtarırlar.

İnterpolun mövqeyinə əsasən, kontent təsnifatı həyata keçirilərək, bu cinayətlər üç geniş sahəyə bölünür:

[3] Məcidli S.T. "İnternet hüququ və etikası". Dərs vəsaiti. Bakı: "Elm və təhsil" nəşriyyatı, 2013. s 114.

- Kompüter aparat vasitələrinə və proqram təminatına qarşı hücumlar;
- Maliyyə cinayətləri, onlayn dələduzluq, onlayn maliyyə xidmətlərinə nüfuzetmə;
- Xüsusilə gənclərin alçaldıcı hərəkətləri və ya "seksplotasiya" formalarından sui-istifadə etməsi.[4]

Kibercinayətlərin müxtəlif qəsd obyektlərinə, predmetlərinə və törədilmə xüsusiyyətlərinə münasibətdə müxtəlif növləri fərqləndirilir. Qeyd olunmalıdır ki, əslində kibercinayətlərlə bağlı yetkin elmi anlayışın verilməsi üçün onun növləri məsələsinə diqqətin ayrılması və bu əməllərin tərkib elementlərinin qruplaşdırılması mühüm təcrübi və elmi əhəmiyyətə malikdir. Müxtəlif ədəbiyyatlarda, beynəlxalq və milli hüquqi normalarda bununla bağlı fərqli bölgülərin aparılmasını nəzərə alaraq, onların bəzilərini araşdırmağa cəhd edəcəyik.

Xüsusi vurğulanmalıdır ki, beynəlxalq təcrübi və elmi hüquqi əhəmiyyəti və Avrasiya regionunda hüquqi qüvvəsinə görə kibercinayətlərin Kibercinayətkarlıq haqqında 2001-ci il Budapeşt Konvensiyasına müvafiq olaraq aparılan bölgüsü daha mükəmməl və məqsədəmüvafiqdir. Həmçinin, bu Konvensiya əsasında aparılan təsnifat əksər beynəlxalq hüquq mütəxəssisləri və alimləri tərəfindən təqdir olunmaqla, müasir beynəlxalq hüquqda və hətta bu sənədi ratifikasiya etməyən xarici ölkələrin milli hüquq sistemlərində də etalon kimi qəbul edilməkdədir. Kibercinayətkarlıq haqqında Konvensiyaya (və ona Əlavə Protokola) görə kibercinayətləri *beş əsas qrupa* bölmək olar:

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

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

3) Kontentlə, yəni kompüter şəbəkəsində yerləşdirilmiş verilənlərin məzmunu ilə əlaqədar kibercinayətlər.

Qeyd etmək lazımdır ki, bu qrup cinayətlər ictimai təhlükəlilik dərəcəsinə görə və praktiki nöqteyi-nəzərindən daha ciddi xarakteri ilə diqqəti cəlb edir. Belə ki, bütün dövlətlər tərəfindən xüsusi önəm verilən uşaq pornoqrafiyası və ümumilikdə internetdə yayılan porno-materiallar ilə bağlı cinayətlər bu qrupa aid edilə bilər. Ümumiyyətlə vurğulanmalıdır ki, hazırda kompüter şəbəkələrində, İnternetdə, Facebook, Twitter, İnstagram və digər sosial şəbəkələrdə kontent məsələsində ciddi problemlər yaşanmaqdadır. Bu mənada kontent cinayətlərinin elmi baxımdan daha dəqiq və müasir beynəlxalq hüquqa uyğun şəkildə balanslaşdırılmış qaydada araşdırılması zəruridir. Çünki, bu zaman kibercinayətlərlə mübarizə məsələsində insan hüquqları amili, o cümlədən şəxsi həyata, ifadə azadlığına müdaxilə problemləri xüsusilə aktual olacaqdır.

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

[4] Cybercrime, http://www.interpol.int

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

Yuxarıda qeyd olunan təsnifatdan bir daha aydın olur ki, müasir dövrdə kibercinayətlərin diapazonu doğurdan da özünün geniş əhatəliliyi ilə diqqəti cəlb edir və bu hüquqazidd əməllərlə mübarizə aparılması əslində bütün digər cinayətlərin də qarşısının alınması və profilaktikasına özünün müsbət təsirini göstərə bilər. Çünki, biz bu cinayətləri qəsd obyektlərinə görə qruplaşdırsaq görərik ki, çoxsaylı əməllərin törədilməsi məhz kompüter şəbəkələri və digər İKT vasitələri ilə həyata keçirilir.

Qeyd olunmalıdır ki, kibercinayətlərin təsnifatı məsələsi hələ də formalaşmaqda olan elmi prosesdir. Kibercinayətlərin təkamülü ilə bağlı "Cybercriminal Activity" ("Kiberkriminal fəaliyyət") adlı məqalədə xarici ölkə tədqiqatçıları bu cinayətin texniki və kontent əlamətləri baxımından müxtəlif növlərini – kompüter servisinin dağıdılması, informasiya oğurluğu, uşaq pornoqrafiyası, reputasiyaya zərər vurulması, spamlar, informasiya saxtakarlığı cinayətlərini fərqləndirirlər.

Göründüyü kimi, kibercinayət termini o qədər geniş anlayışdır ki, onun cinayət tərkibi ilə bağlı müddəalarının müasir informasiya texnologiyalarının inkişafına müvafiq olaraq və sürətli texnoloji tərəqqi nəzərə alınmaqla genişlənməsi ehtimalı böyükdür. Onların bəziləri elmi dairələrdə mübahisəli məsələ kimi hələ də acıq qalmaqdadır.

Ümumiyyətlə, Kibercinayətkarlıq haqqında Konvensiyaya görə kibercinayətlərin beş əsas qrupa bölgüsü müasir beynəlxalq hüquq normaları baxımından və xarici ölkələrin milli hüquq sistemlərinə nəzərən optimal və təcrübi əhəmiyyətli təsnifat kimi qəbul edilir. Törədilən hər hansı istənilən dağıdıcı cinayətkar fəaliyyət məhz kompüter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməl kibercinayətlər kateqoriyasına aid edilir. Kompüter sistemləri və ya şəbəkəsindən, o cümlədən internetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən danışmaq mümkündür. Məsələn, "kiberterrorizm" anlayışı bu kateqoriyaya aid edilə bilər.

Kiberterrorizm və kibercinayətlər: müqayisəli təhlil. Müasir beynəlxalq hüquqda terrorçuluq ayrıca cinayət tərkibi kimi xüsusi statusa malikdir. Belə olan təqdirdə kiberməkandan terrorist məqsədləri ilə istifadə olunması, şəbəkə istifadəçilərinin də həm obyekti, həm də subyekti olduğu bu cinayət əməlinin terrorçuluq, yoxsa kibercinayətlərin xüsusi növü olması məsələsi bir qədər problemlərə yol acmış olacaqdır. Əlbəttə, bu kimi mübahisəli elementlərin aradan qaldırılması üçün bu sahədə unifikasiya olunmuş beynəlxalq cinayət hüquqi konsepsiyanın ortaya qoyulması və bu cinayət əməlləri ilə mübarizədə yeni tendensiyaların ortaya qoyulması zəruridir.

Qeyd etmək lazımdır ki, bu cinayətlərlə mübarizədə xüsusi proqram və layihələrin hazırlanması üzrə "Evropol"un xidmətləri danılmazdır. Həmin layihənin məqsədlərindən də göründüyü kimi, internet üzərindən həyata keçirilən qeyri-qanuni fəaliyyətlərə aid olan ictimai və özəl dialoq təşəbbüsləri xüsusi olaraq terrorçu fəaliyyətlərin fokuslanmasına gətirib çıxarır. Bu mənada onlayn terrorizmlə mübarizənin bilavasitə kibercinayətkalıqla mübarizə ilə qarşılıqlı əlaqə və asılılıqda

nəzərdən keçirilməsi fikrimizcə, faydalı olardı. Lakin, bu iki ayrı-ayrı cinayətlər öz tərkibləri etibarilə fərqləndiyindən, internet şəbəkəsi yalnız terror cinayətinin həyata keçirilməsinin vasitəsi olaraq qalacaqdır. Çünki, bu zaman terror cinayətinin törədilməsində əsas məqsəd kompüter sistemləri və ya məlumatları deyil, terror cinayətinin qəsd obyekti olan ictimai təhlükəsizlik olacaqdır. Burada dövlətlərin səyi ondan ibarət olacaqdır ki, terrorçuluq cinayətinin qarşısının alınmasında yalnız məhdudlaşdırıcı İT vasitələrinin köməyindən istifadə etməklə, onlayn terrorizmin fəsadları minimuma endirilsin.

Bu məsələdə daha müfəssəl yanaşmanın ortaya qoyulması üçün "kiberterrorizm" termininin yaranma tarixinə də diqqətin ayrılması zəruridir.

XX əsrin 80-ci illərinin sonlarında Amerika Təhlükəsizlik və Kəşfiyyat İnstitutunun böyük elmi işçisi Berri Kollin virtual fəzada terrorçuluq fəaliyyətini ifadə etmək üçün ilk dəfə "kibernetik terrorçuluq" terminindən istifadə etmişdir. Qeyd olunmalıdır ki, o zaman bu termin praktiki əhəmiyyət kəsb etmirdi və yalnız gələcək üçün proqnoz verməkdən ötrü istifadə olunurdu. Berri Kollinin özü isə kiberterrorçuluqdan yalnız XXI əsrin ilk onilliyində danışmağın real olduğunu qeyd etmişdir. Lakin real vəziyyətlə əlaqədar olaraq, FTB-in xüsusi agenti Mark Pollit 1996-cı ildə kiberterrorçuluq termininin tərifini təklif etmişdir. Həmin tərifə görə, kiberterrorizm informasiya, kompüter sistemləri, kompüter proqramları əleyhinə yönələn, milli qruplara və mülki hədəflərə qarşı zorakılıqla nəticələnən siyasi motivli qəsdən törədilən hücumdur.

Kiberməkanda terrorizm həm kibercinayət, həm də terrorizmin əlamətlərini özündə ehtiva edir. Kiberməkanda terrorist hücumları kibercinayətin kateqoriyası və informasiya texnologiyalarından kriminal sui-istifadə kimi çıxış edir.

Qeyd olunduğu kimi, kiberterrorçuluq və informasiya təhlükəsizliyi müasir dövrün real vəziyyətinə əsaslanaraq, hüquq və informatika mütəxəssislərinin məşğul olduğu ciddi bir problemə çevrilmişdir. Kiberterrorçuluqla bağlı hərəkət və hərəkətsizlik artıq real olaraq baş verməkdədir. Bu, həm digər cinayətlərin, xüsusilə terrorun və təcavüzün törədilməsi üçün hərəkətverici vasitə olaraq, həm də müstəqil cinayət tərkibi olaraq artıq dunya birliyi tərəfindən cəzalandırılmalı olan əməllər kateqoriyasına aid edilmişdir. Bununla yanaşı, bu günkü Azərbaycan reallığında kibermuharibənin, kibertəcavüzün və digər beynəlxalq cinayətlərin qurbanı kimi artıq bu əməllərə görə cinayət hüquqi yurisdiksiyanın həyata keçirilməsi labüd və zəruridir. Səmərəli cinayət hüquqi yurisdiksiyanın tətbiqi üçün isə kiberməkanda baş verən hərəkət və hərəkətsizlikləri özündə ehtiva edən hüquqi terminlərin istər nəzəri, istərsə də normativ hüquqi müəyyənliyə malik olması danılmazdır.

Beləliklə, kiberterroçuluğa belə bir anlayış verilə bilər: ***Kiberterrorçuluq dedikdə*, kompüterdə** emal olunan informasiyaya, kompüter sisteminə və şəbəkəsinə düşünülmüş, siyasi motivlərə əsaslanmış hücum başa düşülür. Əgər belə hərəkətlər ictimai təhlükəsizliyin pozulması, əhalinin qorxudulması, hərbi konfliktlərin, təxribatlarının törədilməsi məqsədilə həyata keçirilmiş olarsa, onda bu hücum insanların həyatı və sağlamlığı və ya digər ağır fəsadların baş verməsi üçün daha böyük təhlükə yaradır.

Kiberterrorizm siyasi, dini və ideoloji motivlər əsasında dağıdıcı, təxribatçı və qorxu aşılayan nəticələrə səbəb olan, terroristlər tərəfindən informasiya infrastrukturuna edilən hücumlar kimi müəyyən edilir.[5]

Kiberterrorçuluq cinayətkar niyyətlərin əldə olunması məqsədilə əhalinin, hakimiyyət orqanlarının məhz kibervasitələrlə qorxudulması kimi qəbul edilir. Bu,

[5] International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, page 14.

müəyyən siyasi və ya digər məqsədlərin əldə olunması, şəxslərin, təşkilatların və ya hakimiyyət strukturlarının müəyyən hərəkətlərə məcbur edilməsi, kiberterrorçunun şəxsiyyətinə və terrorçu təşkilata diqqətin yönəldilməsi məqsədilə əhalinin təhlükəyə məruz qoyulması, daimi qorxu vəziyyətində saxlanması şəklində özünü göstərə bilər.

Transmilli mütəşəkkil cinayətkar qrupların müasir İKT-dən geniş miqyasda istifadə etməsi labüd faktdır. Beynəlxalq terrorçu təşkilatlar elmi-texniki nailiyyətlərdən yararlanmağa, kompüter, rabitə, İKT və s. sahələrdə mütəxəssisləri öz sıralarına cəlb etməyə çalışırlar. Bu terrorçu təşkilatlar tərəfindən daim yeni üzvlərin daxil edilməsi, törədilmiş terror aktlarına bəraət qazandırılması, potensial terrorçulara təlimlərin keçirilməsi, üzvlər arasında müntəzəm əlaqələrin saxlanılması və s. məqsədlərlə internet şəbəkəsindən fəal istifadə edilir.

Bəzi ədəbiyyatlarda belə kateqoriya əməllər kibercinayətkarlığın bir növü kimi elektron vandalizm də adlandırılır. Orada bu cinayət növü çox ciddi problem kimi səciyyələndirilərək, qeyd olunur ki, bu gün iqtisadiyyat, idarəetmə, hətta dünyanın əksər ölkələrinin ayrı-ayrı vətəndaşları kompüter şəbəkə və sistemlərinin normal fəaliyyətindən asılıdır. Bu tipli cinayətlərin motivi ya öz iradəsini reallaşdırmaq, ya qisas və ya intiqam almaq istəyi, ya da rəqiblə hesablaşmaq istəyi ola bilər. Belə olan təqdirdə kompüter sistemləri zədələnir və onların işinə olan müdaxilələr daha ciddi və bəzən də daha faciəvi nəticələrə səbəb ola bilər.[6] Məsələn 1992-ci ildə kompüter sisteminə edilən müdaxilənin nəticəsi idi ki, Litvada İqnalinsk atom elektrostansiyasında böyük bir nüvə partlayışlarına səbəb ola biləcək hadisələrin yaşanma ehtimalı yaranmışdı. Göründüyü kimi, kompüterlərə edilən hətta təsadüfi müdaxilələr belə ağır fəsadları ilə xarakterizə olunan digər beynəlxalq cinayətlərin törədilməsinin əsas səbəbi kimi çıxış edə bilər. Bu səbəbdən də qeyd olunan cinayət növlərini kompüter cinayətləri ilə əlaqəli cinayətlər kimi adlandırmaq fikrimizcə daha məqbul olardı. Lakin əsas məqsədini və hədəfini məhz kompüter sistemləri və ya kompüter şəbəkələri təşkil edən cinayətləri isə birbaşa kibercinayətlər kateqoriyasına aid etmək olar. Məsələn, 1999-cu ildə Belqradın bombalanması zamanı NATO-nun kompüter sistemlərinin hədəflənməsi və onların işinin iflic edilməsi ilə bağlı həyata keçirilmiş cəhdlər kibercinayət kimi tövsif oluna bilər. Bu mənada kibercinayətlərdə əsas kriminal məqsədin məhz İKT-yə qarşı yönəldilməsi faktoru onun növlərə bölgüsündə əsas təsnifat meyarı kimi götürülməsi qəbul edilməlidir.

Buradan belə nəticəyə gəlmək mümkündür ki, əgər törədilən vandalizm və hər hansı istənilən dağıdıcı cinayətkar fəaliyyət məhz kompüter sistemlərinin və şəbəkələrinin, habelə onlarda mövcud olan informasiyaların məhv edilməsinə yönəlmişdirsə, həmin əməlin törədilmə miqyasından və zahiri əlamətlərindən asılı olmayaraq, onları kibercinayətlər kateqoriyasına aid etmək olar. Digər tərəfdən, əgər kompüter sistemləri və ya şəbəkəsindən, o cümlədən internetdən vasitə kimi istifadə olunaraq, mütəşəkkil cinayətkar qruplar və ayrıca şəxslər konkret cinayət məqsədlərini reallaşdırmağa cəhdlər etmişlərsə, bu zaman qeyd olunan vasitələr həmin cinayət əməllərinin törədilməsi üçün yalnız köməkçi alət qismində çıxış edəcəkdir. Burada ayrıca növ kimi təsnifləşdiriləcək hansısa kibercinayətdən yox, konkret tərkibi olan müstəqil cinayət əməlindən gedəcəkdir.

Beləliklə, “kibercinayət” və “kiberterrorizm” anlayışları fərqləndirilməklə hər biri müstəqil cinayət tərkibi olaraq təsnif edilir və kompüterlər, kompüter şəbəkələri, internet, sosial şəbəkələr yalnız “kiberterrorizm”in törədilməsində yardımçı vasitələr kimi qəbul edilir.

[6] Тимошкина Ю.М. Компьютерные преступления. Москва 2010. S. 11.

Kibercinayətkarlıqla mübarizənin istiqamət və formaları. Müasir dövrdə kibercinayətkarlıqla mübarizə sahəsində dövlətlərarası münasibətlərin istər universal, istərsə də regional tənzimlənməsi məsələsi özünəməxsus xüsusiyyətləri ilə diqqəti cəlb edir. Birincisi, bu sahədə həm beynəlxalq, həm də ölkədaxili maddi hüquq normalarının və bununla əlaqədar prosessual normaların yaradılması yeni və inkişafda olan prosesdir. İkincisi, kibercinayətkarlıq sahəsində ictimai münasibətlərin tənzimlənməsinə və beynəlxalq hüquq normalarının harmonizasiyasına təsir göstərmək iqtidarında olan beynəlxalq əməkdaşlıq formaları özünün ilkin təzahür dövrünü yaşayır. Yəni, bu sahədə beynəlxalq konfranslar, forumlar, elmi-nəzəri və praktiki əməkdaşlıq, habelə kibertəhlükəsizliyin tənzimlənməsinin müxtəlif aspektlərinə dair (hüquqi, təşkilati, texniki və s.) əlaqələr nəticə etibarilə bu sahədə normativ bazanın da formalaşmasında əvəzsiz rol oynayır. Üçüncüsü, bu sahədə daha çox regional əməkdaşlığın aktivliyi və dünyanın müxtəlif regionlarında formalaşmaqda olan ölkələrarası razılaşma nümunələri (məsələn, Avropa Şurası çərçivəsində qəbul olunmuş Kibercinayətkarlıq haqqında 23 noyabr 2001-ci il Budapeşt Konvensiyası, Afrika qitəsində Afrikada kibertəhlükəsizlik fəaliyyətinin hüquqi çərçivəsinin yaradılması haqqında 2012-ci il tarixli Konvensiya layihəsi, Ərəb Şərqində Ərəb Dövlətləri Liqası tərəfindən qəbul olunmuş İnformasiya texnologiyaları cinayətləri ilə mübarizə haqqında 2010-cu il tarixli Ərəb Konvensiyası, MDB məkanında 2001-ci il tarixli Kompüter informasiyası sferasında cinayətlərlə mübarizədə MDB iştirakçı-dövlətlərin əməkdaşlığı haqqında Müqavilə, habelə bu qurum çərçivəsində 17 fevral 1996-cı il tarixdə qəbul edilmiş Model Cinayət Məcəlləsi və s.) daha çox hüquqi müstəvidə müşahidə olunur.

Kibercinayətlərlə mübarizə üzrə əməkdaşlığa dair yeni tendensiyalar BMT-nin İqtisadi və Sosial Şurasının 26 fevral 2014-cü il tarixli yuxarıda qeyd etdiyimiz Cinayətlərin xəbər verilməsi və cinayət mühakiməsi üzrə Komissiyası tərəfindən xüsusi qərar qəbul edilmişdir. Həmin sənədin E bölməsinin (Cinayətkarlığın yeni və yaranmaqda olan növləri ilə mübarizədə beynəlxalq əməkdaşlıq) 57-ci bəndində qeyd olunur: "Kibercinayətlər şübhəsiz ki, qlobal əks-tədbirlərin görülməsini tələb edən birinci cinayət növləri deyildir. Qeyd olunmalıdır ki, müasir kibercinayətlər, habelə elektron daşıyıcılarla əlaqədar cinayətlər beynəlxalq əməkdaşlıq sahəsində unikal çağırışlar səsləndirir. Elektron daşıyıcıların qısamüddətli xarakterini nəzərə alaraq, kibercinayətlərlə mübarizə işində beynəlxalq əməkdaşlıq öz növbəsində dərhal reaksiya verilməsini və xüsusi araşdırma tədbirlərinin görülməsi barədə sorğu göndərmək xüsusiyyətini tələb edir.

Baxmayaraq ki, hüquq-mühafizə orqanları arasında əməkdaşlığın bir sıra qeyri-rəsmi metodları, o cümlədən "24/7" şəbəkəsi mövcuddur, ölkədən elektron sübutların alınması üçün əhəmiyyətli dərəcədə əvvəlki ənənəvi məhkəmə kanalları vasitəsindən, xüsusilə qarşılıqlı yardım haqqında ikitərəfli sənədlərdən istifadə olunur."[7] BMT-nin Cinayətlərin xəbər verilməsi və cinayət mühakiməsi üzrə Komissiyasının qeyd olunan sənədinin 58-ci bəndi isə qarşılıqlı hüquqi yardımın bəzi prosedur məsələlərinə aydınlıq gətirmişdir. Orada bildirilir ki, kibercinayətlərin araşdırılmasına dair qarşılıqlı hüquqi yardım haqqında belə sorğuya cavabın alınması müddəti adətən 150 gün təşkil edir. Komissiyanın hazırladığı sənədin 59-cu bəndi isə elektron informasiyalardan istifadə ilə əlaqədar şəxsi məlumatların əldə edilməsi üzrə hüquq

[7] Организация Объединенных Наций E/CN.15/2014/12, Экономический и Социальный Совет, Distr.: General 26 February 2014, V.14-01305 (R) 240314 250314, Комиссия по предупреждению преступности и уголовному правосудию, Двадцать третья сессия, Вена, 12-16 мая 2014 года.

pozuntusu törədən şəxslər barədə tədbirlərin görülməsi ilə bağlı beynəlxalq əməkdaşlıq məsələlərinə həsr edilmişdir.

İkitərəfli müqavilələrdə kibercinayətlərlə mübarizə məsələləri. Müasir beynəlxalq hüquqda kibercinayətlərin qarşısının alınması, istintaqı, hüquqi yardım, habelə informasiya mübadiləsi baxımından ikitərəfli müqavilələr olduqca mühüm əhəmiyyət kəsb edən beynəlxalq əməkdaşlıq formasıdır. Əslində ikitərəfli əməkdaşlıq dövlətlər arasında hüquqi proseduraların daha da konkretləşməsinə xidmət edir, eyni zamanda kibercinayətlərə qarşı mübarizə üzrə qüvvədə olan beynəlxalq və regional konvensiyaların səmərəli icra və ya tətbiq olunmasına yardımçı funksiya daşıyır. Əgər kibertəhlükəsizlik və kibercinayətlər sahəsində beynəlxalq konvensiyalar bu cinayətə dair ümumi məsələləri (universal anlayışların verilməsi, ümumi prosedur məsələlərini, mühakimə icraatının ümumi prinsiplərini və s.) tənzim edirsə, ikitərəfli müqavilələr isə kibercinayətlərlə mübarizənin konkret elementlərini (qarşılıqlı hüquqi yardım, texniki yardım, qarşılıqlı informasiya mübadiləsi, kibercinayət törətməkdə şübhəli şəxslərin ekstradisiyası, kibercinayətkarların verilməsi və s.) məsələlər üzrə xüsusi rol oynayır.

Kibercinayətlərə qarşı əməkdaşlıq üzrə konkret ikitərəfli müqavilələr müasir beynəlxalq hüquqda çox az saydadır. Bunun iki mühüm səbəbi var: birincisi, bu cinayət əməlləri beynəlxalq əməkdaşlıq müstəvisində innovativ xarakter daşıyır və bununla əlaqədar ikitərəfli müqavilə münasibətləri yeni yaranmaqda olan davamlı proses kimi səciyyələnir. İkincisi, bu sahədə mövcud ikitərəfli münasibətlər yalnız ümumi hüquqi yardım və iki dövlət arasında bağlanan əməkdaşlıq memorandumlarının tərkib hissəsi olaraq formalaşmaqdadır. Ona görə də, bu istiqamətdə ikitərəfli müqavilə bazası günümüzün reallıqları baxımından daha çox dəyişən texnoloji yeniliklərə münasibətdə günbəgün təzələnir.

Məzmununu kibercinayətlər üzrə əməkdaşlıq və qarşılıqlı münasibətlər təşkil edən ikitərəfli müqavilələri şərti olaraq aşağıdakı qruplara ayırmaq olar:

Cinayət işləri üzrə hüquqi yardım haqqında ikitərəfli müqavilələr. Bu müqavilələrin ayrıca müddəaları kibercinayətlərə dair qarşılıqlı yardıma, o cümlədən texniki yardım və digər qarışlıqlı anlaşma, kömək və s. hərəkətlər tələb edən məsələləri əhatə edir. Misal olaraq, Azərbaycan Respublikası ilə Hindistan Respublikası arasında cinayət işləri üzrə qarşılıqlı hüquqi yardım haqqında Nyu Dehli şəhərində 04 aprel 2013-cü il tarixdə imzalanmış Müqaviləni, Azərbaycan Respublikası və Birləşmiş Ərəb Əmirlikləri arasında cinayət işləri üzrə qarşılıqlı hüquqi yardım haqqında Əbu-Dabi şəhərində 20 noyabr 2006-cı il tarixində imzalanmış Müqaviləni göstərmək olar.

Ekstradisiya, təslimetmə və məhkumların verilməsi ilə bağlı ikitərəfli müqavilələr. Bu müqavilələrdə isə daha çox iki ölkənin cinayət axtarış, istintaq və cinayət mühakimə orqanları, habelə hökmün icrasını həyata keçirən orqanlar arasında kibercinayət törətməkdə şübhəli olan şəxslərin ekstradisiyası və bu cinayətlərə görə məhkum olunmuş şəxslərin verilməsi üzrə mövcud olan əlaqələr öz əksini tapır. Buna misal olaraq, Azərbaycan Respublikası və Birləşmiş Ərəb Əmirlikləri arasında ekstradisiya haqqında Abu-Dabi şəhərində imzalanmış 20 noyabr 2006-cı il tarixli Müqaviləni, Azərbaycan Respublikası və Cin Xalq Respublikası arasında Təslimetmə haqqında Pekin şəhərində 17 mart 2005-ci ildə imzalanmış Müqaviləni, Azərbaycan Respublikası və Litva Respublikası arasında azadlıqdan məhkum olunmuş şəxslərin cəzanın qalan hissəsinin çəkilməsi üçün verilməsi haqqında Vilnüs şəhərində imzalanmış 23 oktyabr 2001-ci il tarixli Müqaviləni göstərmək olar.

İki dövlət arasında dostluq və əməkdaşlıq haqqında memorandumlar. Bu xüsusdan olan sənədlərdə də iki dövlət arasında münasibətlərin daha yüksək

səviyyədə inkişafına nail olmaq üçün kibercinayətlər üzrə öz qanunvericilikləri nöqteyi-nəzərindən çıxış edərək, bu sahədə geniş informasiya mübadiləsi, hər iki tərəfin qeyd olunan sahədə elmi-praktiki əməkdaşlığı məsələlərini özündə ehtiva edir. Məsələn, Azərbaycan Respublikası Ədliyyə Nazirliyi və Slovakiya Respublikası Ədliyyə Nazirliyi arasında 12 may 2009-cu il tarixdə imzalanmış Əməkdaşlıq haqqında Memorandumun 1-ci maddəsində qeyd olunur: "Tərəflər aşağıdakı sahələr üzrə əməkdaşlığı, məlumat və təcrübə mübadiləsini dəstəkləyəcəklər:

a) daxili qanunvericilik və hüquqi xarakterli məlumatlar;

b) məhkəmə sisteminin idarəetməsi;

c) elektron ədliyyə və s.

"Eyni zamanda, həmin sənədin 2-ci maddəsində yuxarıda göstərilən sahələr üzrə əməkdaşlığın həyata keçirilməsi məqsədilə Tərəflərin normativ aktlar, hüquqi sənəd və rəylərlə bağlı mübadilə aparacağı, birgə seminar və məsləhətləşmələr təşkil edəcəkləri ilə bağlı müddəalar vardır. Göründüyü kimi, son dövrlər elektron ədliyyə, o cümlədən kibercinayətlər üzrə əməkdaşlıq məsələləri ölkəmizin bağladığı müqavilələrin predmetini təşkil edir.

Kibercinayətkarlıqla mübarizə üzrə beynəlxalq hüquq normalarının Azərbaycan Respublikasının milli qanunvericiliyinə daxil edilməsi məsələləri

Artıq qloballaşma və informasiya dövrünün tələblərinə müvafiq olaraq milli qanunvericilik sistemləri də əhəmiyyətli dərəcədə modern dəyişikliklərə məruz qalmaqdadır. Bu gün dünyanın əksər ölkələri surətlə inkişaf edən müasir İKT sistemlərinə nüfuz etdikcə milli qanunvericiliklərdə də müasir beynəlxalq hüquq norma və prinsiplərinin tələblərinə uyğun rasional dəyişiklik və inkişaf müşahidə olunur.

Kibercinayətkarlığın qarşısının alınması, bu sahədə profilaktik, habelə digər təşkilatı-hüquqi mexanizmlərin müəyyən olunması istiqamətində ölkəmizdə kompleks işlər görülərək, bu cinayətlə mübarizə tədbirlərini əhatə edən normativ-hüquqi aktlar, Dövlət Proqramları, xüsusi layihələr qəbul edilməklə və icra olunmaqla digər sahəvi qanunvericilik normalarının inkişafına dövlətimiz tərəfindən əlavə dəstək verilir, müvafiq qurumlar tərəfindən maarifləndirici fəaliyyət həyata keçirilir.

Müasir dövrdə kompüter sistemləri, bütün dünyanı vahid informasiya məkanında birləşdirən internet şəbəkəsi, virtual kitabxanalar, elektron jurnallar və bu qəbildən olan digər vasitələr Azərbaycanda cəmiyyət həyatının ayrılmaz hissəsinə çevrilib. Lakin bu informasiya axınından və sosial şəbəkələrdən heç də hamı mütərəqqi məqsədlər üçün faydalanmır, bundan bəzən cinayətkar mənafe naminə istifadə olunur, ictimai qaydalara zərər vurulur və cəmiyyətin sosial-mənəvi əsasları zərbə altında qalır. Bəzən hətta ölkəmizin milli təhlükəsizliyi, dövlətimizin ərazi bütövlüyü cinayətkar təhdid altında qalır. Dünyada cinayətkarlığın vəziyyətinin təhlili sübut edir ki, o görünməmiş səviyyəyə çatmış və dövlətlərin təhlükəsizliyi üçün real hədəyə çevrilmişdir.

Buna görə də dövlət tərəfindən kibercinayətkarlıqla mübarizə məsələlərinin respublikamızın ayrı-ayrı sahəvi qanunvericiliyinə daxil edilməsi zərurəti yaranmışdır. Daha doğrusu, bu gün kibercinayətlər bütövlükdə qlobal dünya üçün real təhlükə olduğundan və Azərbaycan Respublikası da dünya birliyinin müstəqil və ayrılmaz tərkib hissəsi olaraq bu məkana sıx inteqrasiya etdiyi üçün mili hüququn bütün sahələri üzrə beynəlxalq hüquq normalarının implementasiyası (milli qanunvericiliyə daxil edilməsi) dövlətimizin prioritet vəzifələrindən birini təşkil edir.

Qeyd olunmalıdır ki, ölkəmiz digər sahələrdə olduğu kimi, cinayətkarlıqla mübarizə, o cümlədən kibercinayətkarlığa qarşı mübarizə sahəsində də siyasi iradə nümayiş etdirir. Son dövrlərin İKT-nin sürətli inkişafı beynəlxalq hüquqi əlaqələrin müxtəlif sahələrində, o cümlədən kibercinayətlər üzrə beynəlxalq əməkdaşlığı, bu

sahədə normativ hüquqi mübadiləni zərurətə çevirmişdir. Ona görə də ölkəmiz də daxil olmaqla yuxarıda qeyd olunan problemləri nəzərə alaraq, kompüter cinayətkarlığı ilə mübarizə sahəsində dövlətlər öz səylərini birləşdirməyə və bu məsələlərlə bağlı hüquqi müstəvidə BMT, Avropa Şurası, Avropa İttifaqı, ATƏT, MDB və digər beynəlxalq qurumlar çərçivəsində addımlar atmağa başlamışdır. Bu həm qarşılıqlı hüquqi yardım, həm də universal və regional təhlükəsizliyin qorunması və təhdidlərin qarşısının alınması sahələrinə aid edilə bilər.

Bu sahədə maddi və prosessual normaları unifikasiya edən və kibermünasibətləri tənzimləyən ən mühüm sənədlər Avropa Şurası çərçivəsində qəbul edilmişdir. Artıq qeyd etdiyimiz kimi, qurumun 23 noyabr 2001-ci il tarixli Kibercinayətkarlıq haqqında Konvensiyası kiberməkanda baş verən cinayətlər və onlarla mübarizə məsələlərinə həsr olunmuşdur. Bu Konvensiyada beynəlxalq təcrübədə analoqu olmayan bir sıra cinayətlər – kompüter məlumatlarının və sisteminin konfidensiallığı, bütövlüyü və əlverişliliyi əleyhinə cinayətlər, kompüterlə əlaqəli cinayətlər, habelə, məzmununu kompüter informasiyası təşkil edən hüquq pozuntuları, uşaq pornoqrafiyası ilə əlaqəli materiallarla bağlı hüquqazidd əməllər, müəlliflik və əlaqəli hüquqların pozulması ilə bağlı cinayətlər təsbit olmuşdur.

Bundan başqa, Konvensiya kibercinayətkarlıqla mübarizədə əməkdaşlığın prinsiplərini də müəyyən edir. Bunlara aiddir: bir-biri ilə geniş əməkdaşlıq prinsipi, ekstradisiya prinsipi, qarşılıqlı yardımın ümumi prinsipləri, müvafiq beynəlxalq sazişlərin istisna etdiyi hallarda yardım haqqında sorğuların yönləndirilməsi və yerinə yetirilməsi prinsipi, konfidensiallıq və məhdud istifadə prinsipi, müvəqqəti tədbirlərin görülməsi üzrə yardım prinsipi, istintaq xidmətlərinin fəaliyyətlərinə yardım prinsipi.

Kibercinayətkarlıq üzrə prinsiplərin həyata keçirilməsi fikrimizcə müasir dövr üçün daha aktual hüquqi problem olaraq araşdırılmalı və riayət olunmalıdır. Çünki, özünün transmilli mahiyyətinə və nəticələrinin ağırlığına görə bu kateqoriyaya daxil olan əməllərin təhlükəsizliyi heç də digər beynəlxalq və beynəlxalq xarakterli cinayətlərdən geri qalmır.

Ölkəmizdə kibertəhlükəsizliyin təmin olunması sahəsində mühüm addımlar atılmış və bu siyasət hazırda ölkə Prezidenti cənab İlham Əliyev tərəfindən uğurla davam etdirilməkdədir. Kibercinayətkalıqla mübarizə üzrə beynəlxalq hüquq normalarının ölkəmizin sahəvi qanunvericiliyinə tətbiqi sahəsində ilk qanunvericilik tədbiri kimi ölkəmizin Kibercinayətkarlıq haqqında Budapeşt Konvensiyasına qoşulmasını qeyd etmək olar.

Azərbaycan Respublikasının Cinayət Məcəlləsində kibercinayətlərin anlayışı və tərkibi. Ölkəmizdə kibertəhlükəsizliyin təmin olunması və kibercinayətkalıqla mübarizə ilə bağlı yuxarıda qeyd etdiyimiz kimi, çoxsaylı normativ-hüquqi aktlar qəbul olunmuşdur ki, onların da əsas məqsədini bu sahəyə aid olan beynəlxalq hüquqi norma və prinsiplərin effektiv dövlətdaxili tətbiqinə nail olunması təşkil edir. Bunların qəbulu nəticəsində isə əksər milli hüquq normalarında, o cümlədən Azərbaycan Respublikasının Cinayət Məcəlləsində müvafiq dəyişikliklər həyata keçirilmişdir.

Cinayət əməlinin obyekti kompüter sisteminin, kompüter məlumatlarının mühafizəsi sahəsində yaranan ictimai münasibətlərdir. Bu cinayətin predmeti kompüter məlumatlarıdır. Cinayətin obyektiv cəhəti kompüter sisteminə və ya onun hər hansı bir hissəsinə daxil olmaq hüququ olmadan həmin sistemə və ya saxlanılan kompüter məlumatlarını ələ keçirmək və ya başqa şəxsi niyyətlə daxil olmada ifadə olunur.

“Kibercinayətkarlıq haqqında” konvensiyaya görə kompüter məlumatları dedikdə kompüter sistemində işlənməsi, emal edilməsi üçün yararlı olan istənilən informasiya (faktlar, məlumatlar, proqramlar və anlayışlar) başa duşulur.

Kompüter informasiyasının predmeti informasiya ehtiyatlarıdır. Informasiya ehtiyatları dedikdə informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda məlumat banklarında və s.) sənədlər və sənəd massivləri, habelə ayrıca mövcud olan sənədlər və onların massivləri başa duşulur ("İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Qanunun 2-ci maddəsi).

Kompüter informasiyasının xüsusiyyəti onun nisbətən asan göndərilməsinin, yenidən yaradılmasının, artırılmasının mümkünlüyündə ifadə olunur.

CM-in 271-ci maddəsinin qeydinin 1-ci, "Kibercinayətkarlıq haqqında" Konvensiyanın 1-ci maddəsinin "a" bəndinə görə kompüter sistemi dedikdə müvafiq proqramlara uyğun olaraq verilənlərin avtomatik işlənməsini həyata keçirən hər hansı qurğu və ya bir-birinə qoşulmuş və ya əlaqələndirilmiş qurğular qrupu başa duşulur. Kompüter sistemi verilənlərin işlənməsi üçün nəzərdə tutulan aparat vasitələrinin və proqram təminatının toplusudur.

Kompüter şəbəkəsi dedikdə öz aralarında rabitə kanalı ilə birləşdirilmiş və bu rabitənin həyata keçirmə yə imkan verən iki və daha çox kompüterin məcmusu başa duşulur.

CM-in 271-ci maddəsinin tərkibinin olması üçün kompüter informasiyası işlənmə, emal edilmə üçün yararlı olmalıdır. Informasiyanın yararlı olması ondan istifadəsinin mümkünlüyü dərəcəsindən asılıdır. Kompüter sistemində olan informasiyanın bütövlükdə yararlı olması tələb olunmur: kifayətdir ki, ələ keçirilən informasiya onu ələ keçirən şəxsə lazım olan səviyyədə yararlı olsun. Məsələn, belə informasiyadan istifadə etməklə informasiya sahibinə zərər vurula bilsin, ictimai təhlükəsizliyə və ictimai qaydaya təhlükə yaransın.

Bu gün Azərbaycan Respublikasında kibertəhlükəsiziliyin təmin olunması istiqamətində qanunvericiliyin təkmilləşdirilməsi ilə yanaşı, təşkilati mexanizmlərin inkişafı istiqamətində dövlətimiz tərəfindən informasiya təklüləsizliyi baxımından müxtəlif təbirlər həyata keçirilir.

"E-hökumət" layihəsi "Elektron Azərbaycan" proqramı çərçivəsində "Azərbaycan Respublikasının inkişafı naminə informasiya-kommunikasiya texnologiyaları üzrə Milli Strategiyaya (2003-2012-ci illər)" əsasən işlənib hazırlanmış və "Elektron Azərbaycan" Dövlət Proqramı çərçivəsində həyata keçirilir. Layihə İKT-nin geniş tətbiqi ilə dövlət orqanlarının fəaliyyətinin səmərəliliyinin və operativliyinin yüksəldilməsini, əhali, biznes qurumları, həmçinin öz aralarında əlaqələrin asanlaşdırılması və sərbəstləşdirilməsinə yönəldilmiş fəaliyyəti nəzərdə tutur, vətəndaş-məmur münasibətlərinin yeni müstəvidə qurulmasına, şəffaflığın təmin olunmasına və informasiya tələbatının dolğun ödənilməsinə şərait yaradır.[8] Bütün bunlar isə əlbəttə kiberməkanda yeni yanaşmaları, xüsusilə bu sahədə neqativ təzahürlərlə mübarizə aparacaq yeni strukturların yaradılmasını da özündə ehtiva edir.

Müasir mərhələdə Azərbaycanın davamlı və dayanıqlı inkişafı siyasətinin prioritet istiqamətlərindən elan olunan İKT (İKT) sosial-iqtisadi sistemin bütün sahələrinə və insanların gündəlik fəaliyyətinə surətlə nüfuz edərək, ictimai-iqtisadi münasibətlərin ayrılmaz tərkib hissəsinə çevrilmişdir. Son illərdə ölkədə informasiya cəmiyyətinin bərqərar olması və bunun tərkib hissəsi kimi İKT-nin geniş tətbiq edilməsi istiqamətində sistemli fəaliyyət aparılır. Bu baxımdan, "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003-2012-ci illər)", Azərbaycan Respublikası Prezidentinin 2010-cu il 11 avqust tarixli, 1056 nömrəli Sərəncamı ilə təsdiq edilmiş Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan) və həyata keçirilən genişmiqyaslı işlər qeyd edilə bilər.

[8] Elektron hökumət, http://www.mincom.gov.az/layiheler/elektron-hokumet

Bu gün artıq ölkəmizdə "Azərbaycan 2020: gələcəyə baxış" İnkişaf Konsepsiyası"na əsasən İKT sahəsi üzrə vəzifələr müəyyənləşdirilmiş, "Azərbaycan Respublikasında 2013-cü ilin "İnformasiya-kommunikasiya texnologiyaları ili" elan edilməsi ilə bağlı Tədbirlər Planı"nın təsdiq olunmuş və icra edilmiş, habelə "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya"[9] təsdiq edilmişdir. Yuxarıda qeyd etdiyimiz bütün sənədləri üzrə əlaqələndirici qurum qismində məhz Azərbaycan Respublikasının Rabitə və Yüksək Texnologiyalar Nazirliyi müəyyən olunmuşdur. Bu sənədlərdə irəli sürülən ideyalar və həyata keçirilən tədbirlər informasiya cəmiyyətinin inkişafına yönəlmiş addımlardandır və respublikamızda kibertəhlükəsizliyin təmin olunması əhalinin bu istiqamətdə daha müasir və modern texnologiyalardan istifadə mədəniyyətinin yüksəldiləsi ilə bağlı müasir beynəlxalq birliyin qəbul etdiyi normaların ölkəmizdə səmərəli tətbiqinə hesablanmışdır.

Azərbaycan Respublikasında kibercinayətkarlıqla mübarizənin təşkilati-hüquqi əsasları

Kibercinayətkarlıqla mübarizə, o cümlədən informasiya təhlükəsizliyi məsələsi bir çox dövlət orqanlarının birgə əlaqəli işini tələb edir. Bu sahədə fəaliyyətin həyata keçirilməsinin müxtəlif aspektləri ölkəmizdə Rabitə və Yüksək Texnologiyalar Nazirliyi, Dövlət Təhlükəsizlik Xidməti və Ədliyyə Nazirliyinə şamil edilmişdir.

Rabitə və İnformasiya Texnologiyaları Nazirliyi 2005-ci ildə Azərbaycan Respublikasının "Kibercinayətkarlıq haqqında" 23 noyabr 2001-ci il tarixli Budapeşt şəhərində imzalanmış Konvensiyaya qoşulmasının təşəbbüskarı kimi çıxış etmiş, Prezident İlham Əliyevin Sərəncamı ilə ölkəmiz 2008-ci ildə bu konvensiyaya qoşulması haqqında Avropa Şurasında, Strasburqda sənəd imzalamışdır. Sözügedən Konvensiya 2009-cu il sentyabrın 30-da Azərbaycan Respublikasının Milli Məclisi tərəfindən müvafiq bəyanatlar və qeyd-şərtlərlə təsdiq olunmuşdur.[10] 2010-cu il iyulun 1-də nəzərdə tutulan müvafiq prosedurlar həyata keçirildikdən sonra ölkəmiz adı çəkilən Konvensiyaya qoşulmuşdur. Bu, kibertəhlükəsizliyin təmin olunması və onun ayrılmaz hissəsi olan kibercinayətkarlığa qarşı mübarizə sahəsində istifadə olunan beynəlxalq mexanizmlərdən biridir.[11]

Xüsusi vurğulamaq lazımdır ki, yuxarıda da qeyd olunduğu kimi, Azərbaycan Respublikası "Kibercinayətkarlıq haqqında" Konvensiyanı 5 bəyanat və 4 qeyd-şərtlə ratifikasiya etmişdir. Bunlar həmin Konvensiyanın ölkəmizdə implementasiya şərtlərini və imkanlarını diktə etməklə, müvafiq olaraq kibercinayətkarlıq üzrə ekstradisiya, qarşılıqlı yardım, səmərəliliyin təmin edilməsi, cinayətlərin istintaqı və ya digər icraatın aparılması məqsədilə və ya cinayətlərə dair subutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsi və s. məsələlərə aiddir.

Kibercinayətkalıqla mübarizənin həyata keçirilməsi və bu sahəyə aid beynəlxalq hüquq normalarının implementasiyası ilə bağlı praktiki əhəmiyyət kəsb edən problemlərdən biri ekstradisiyadır. Bununla əlaqədar olaraq, ölkəmiz Konvensiyaya qoşularkən Bəyanat verərək bildirmişdir ki, "Azərbaycan Respublikası, Konvensiyanın 24-cü maddəsinin 7-ci bəndinin "a" yarımbəndinə uyğun olaraq, ekstradisiya müqaviləsi olmadığı hallarda ekstradisiya və müvəqqəti həbsə dair sorğuları qəbul edən səlahiyyətli orqan qismində Ədliyyə Nazirliyini təyin edir". Ümumiyyətlə qeyd etmək lazımdır ki, cinayətlərə münasibətdə ekstradisiya üzrə sorğuları qəbul etmək və

[9] "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" İlham Əliyev Azərbaycan Respublikasının Prezidenti Bakı şəhəri, 2 aprel 2014-cü il.

[10] "Kibercinayətkarlıq haqqında" konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, http://www.eqanun.az

[11] Kibercinayətkarlıqla bağlı ayrıca qanunun qəbul olunmasına ehtiyac görülür. http://www.paritet.az/layihe/5863.html

vermək səlahiyyətinə malik qurumların dairəsi Azərbaycanda bir qədər mürəkkəb xarakter daşıyır və elmi dairələrdə mübahisəli sayılır.

Ölkəmizdə mövcud olan praktikaya uyğun olaraq, bu ekstradisiya ilə bağlı sorğu məsələsi ilə iki orqan – Ədliyyə Nazirliyi və Azərbaycan Respublikasının Baş Prokurorluğu məşğul olur. Respublikamızda kibercinayətkalıq sahəsində sorğu məsələlərinin həllinin Ədliyyə Nazirliyinə həvalə olunmasının əsas səbəbi isə ondan ibarətdir ki, bir qayda olaraq, Avropa konvesiyaları, ikitərəfli müqavilələr və milli qanun çərçivəsində sorğu məsələsinə məhz Ədliyyə Nazirliyi baxır. Mövcud praktikaya uyğun olaraq, MDB konvensiyaları çərçivəsində isə bu məsələ Baş Prokurorluğun səlahiyyətinə aid edilir.

Kibercinayətlərlə bağlı ölkəmiz tərəfindən verilən növbəti bəyanat qarşılıqlı yardım üzrə sorğularla bağlıdır. Bu məsələdə isə səlahiyyətli orqan Dövlət Təhlükəsizlik Xidməti müəyyən edilmişdir. Sənəddə qeyd olunur ki, "Azərbaycan Respublikası, Konvensiyanın 27-ci maddəsinin 2-ci bəndinin "c" yarımbəndinə müvafiq olaraq, qarşılıqlı yardım üçün sorğu göndərmək, sorğuları icra etmək və onların icra edilməsi üçün məsul olan səlahiyyətli orqan qismində Dövlət Təhlükəsizlik Xidmətini təyin edir". Göründüyü kimi, bu məsələ də sorğu ilə bağlı olsa da qanunda buna səlahiyyətli qurum daha fərqli mərkəzi icra hakimiyyəti orqanı müəyyən edilmişdir.

"Kibercinayətkarlıq haqqında" Konvensiya üzrə verilən digər Bəyanatda Konvensiyanın 27-ci maddəsinin 9-cu bəndinin "e" yarımbəndinə uyğun olaraq Azərbaycan Respublikası baş katibi məlumatlandırır ki, səmərəliliyin təmin edilməsi məqsədilə bu bənd əsasında edilmiş sorğular onun mərkəzi hakimiyyət orqanına göndərilməlidir. Konvensiyanın 27-ci maddəsinin 9-cu bəndinin "e" yarımbəndinə qeyd olunur ki, hər bir Tərəf hazırkı Konvensiyanı imzalayarkən və ya ratifikasiya fərmanını yaxud qəbul etmə, bəyənilmə və ya qoşulma haqqında öz sənədini saxlanılması üçün təhvil verərkən səmərəliliyin təmin edilməsi məqsədilə hazırkı bəndin müddəalarına uyğun olaraq göndərilən sorğuların onun mərkəzi orqanlarına ünvanlanmalı olduqları barədə Avropa Şurasının Baş katibini məlumatlandıra bilər. 9-cu bəndə müvafiq olaraq, kibercinayətlərlə bağlı qarşılıqlı yardım haqqında sorğular və ya bu sorğularla bağlı məlumatlar həm sorğu edən Tərəfin cinayət prosesini həyata keçirən orqanları tərəfindən birbaşa sorğu edilən Tərəfin müvafiq orqanlarına göndərilə bilər, həm də sorğu və ya məlumat Beynəlxalq Cinayət Polisi Təşkilatı (İnterpol) vasitəsilə göndərilə bilər. Göründüyü kimi, kibercinayətkarlıqla bağlı Konvensiyada nəzərdə tutulan prosedurlar müvafiq qaydada ölkəmizin milli hüquq sisteminə transformasiya olunmaqla, onun müddəalarının səmərəli şəkildə həyata keçirilməsi üçün əlverişli şərait yaradır.

Konvensiyanın ölkədaxili implementasiyası ilə bağlı mühüm və maraqlı məsələlərdən biri də kibercinayətlərlə bağlı istintaqın və digər icraatların aparılması ilə əlaqədardır. Bu, öz həllini Konvensiyanın 35-ci maddəsinin 1-ci bəndi üzrə ölkəmizin verdiyi Bəyanatda tapmışdır. Orada qeyd olunur ki, Azərbaycan Respublikası, Konvensiyanın 35-ci maddəsinin 1-ci bəndinə müvafiq olaraq, kompüter sistemləri və kompüter verilənləri ilə əlaqədar cinayətlərin istintaqı və ya digər icraatın aparılması məqsədilə və ya cinayətlərə dair subutların elektron formada toplanması üçün təxirəsalınmaz yardımın göstərilməsini təmin etmək məqsədilə sutkada iyirmi dörd saat, həftədə yeddi gün (7/24) ərzində fəaliyyət göstərən əlaqələndirici qurum qismində Dövlət Təhlükəsizlik Xidmətini təyin edir.

Azərbaycan milli qanunvericiliyində kibercinayətlərə görə məsuliyyət məsələləri. Azərbaycan Respublikasının qanunvericiliyində kibercinyətkarlıqla mübarizə və bu hüquqazidd əməllərə görə məsuliyyət məsələlərinə diqqət yetirilir, milli qanunlara beynəlxalq konvensiyaların tələblərindən irəli gələn əlavə və dəyişikliklər

edilir. Bununla əlaqədar 30 sentyabr 2009-cu il tarixli "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu[12] qəbul edilmiş, müvafiq bəyanatlar və qeyd sərtlərlə bu sənəd təsdiq olunmuşdur.

Eyni zamanda, kompüter informasiyası sahəsində cinayətlər Cinayət Məcəlləsində ayrıca fəsildə (otuzuncu fəsil) qruplaşdırılmaqla, 29 iyun 2012-ci ildə qəbul edilmiş Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Qanunla[13] Məcəllənin həmin fəsli daha da təkmilləşdirilmiş, "Kibercinayətlər" adlandırılmış, buraya kibercinayətkarlıqla mübarizəni şərtləndirən yeni müddəalar əlavə olunmuşdur.

Qeyd edək ki, Məcəllənin müvafiq fəslinin "Kibercinayətlər" adlandırılması müasir beynəlxalq hüquq normaları ilə tam uyğunluq təşkil edir və yeni müddəalar ölkəmiz tərəfindən ratifikasiya edilmiş AŞ-nın 23 noyabr 2001-ci il tarixli Kibercinayətkarlıq haqqında Konvensiyasından implementasiya olunmuşdur.

Məcəllənin 271-ci maddəsinə görə, kompüter sisteminə və ya onun hər hansı bir hissəsinə daxil olmaq hüququ olmadan həmin sistemə və ya onun hər hansı bir hissəsinə mühafizə tədbirlərini pozmaqla, yaxud burada saxlanılan kompüter məlumatlarını ələ keçirmək və ya başqa şəxsi niyyətlə qəsdən daxil olma cinayət sayılır və cəzalandırılır.

272-ci maddədə kompüter məlumatlarını qanunsuz ələ keçirmə cinayət hesab edilir: Kompüter sisteminə, kompüter sistemindən və ya bu sistem daxilində ötürülən ümumi istifadə üçün nəzərdə tutulmayan kompüter məlumatlarının, o cümlədən bu cür kompüter məlumatlarının daşıyıcısı olan kompüter sistemlərinin elektromaqnit şüalanmasının, buna hüququ olmayan şəxs tərəfindən texniki vasitələrdən istifadə etməklə qəsdən ələ keçirilməsi iki ilədək müddətə müəyyən vəzifə tutma və ya müəyyən fəaliyyətlə məşğul olma hüququndan məhrum edilməklə min manatdan iki min manatadək miqdarda cərimə və ya iki ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır.

Qanuna əsasən qeyd olunan cinayətlər üzrə, habelə kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsi (273-1-ci maddə), kompüter məlumatlarının saxtalaşdırılması (273-2-ci maddə) cinayətləri ilə bağlı yeni yanaşmalar ortaya qoyulmuş, cəzalar sərtləşdirilmişdir.

Bundan əlavə, qanunla Məcəlləyə yeni – 171-1-ci maddə əlavə olunmuşdur. "Uşaq pornoqrafiyasının dövriyyəsi" adlandırılan bu müddəada "uşaq pornoqrafiyası" anlayışına aydınlıq gətirilir. "Uşaq pornoqrafiyası" dedikdə, yetkinlik yaşına çatmayan şəxsin və ya yetkinlik yaşına çatmayan təsəvvürünü yaradan şəxsin aşkar seksual xarakterli hərəkətlərdə real və ya simulyasiya edilmiş iştirakını əks etdirən, yaxud seksual məqsədlərlə yetkinlik yaşına çatmayanların cinsi orqanlarını əks etdirən istənilən əşyalar və ya materiallar, o cümlədən aşkar seksual hərəkətlərdə iştirak edən yetkinlik yaşına çatmayan şəxsi əks etdirən realistik təsvirlər başa düşulur.

Cinayət Məcəlləsinin 171-1.1-ci maddəsinə görə uşaq pornoqrafiyasını yayma, reklam etmə, satma, başqasına vermə, göndərmə, təklif etmə, əldə edilməsinə şərait yaratma, yaxud yaymaq və ya reklam etmək məqsədilə hazırlama, əldə etmə və ya saxlama səkkiz min manatdan on min manatadək miqdarda cərimə və ya beş ilədək müddətə azadlıqdan məhrum etmə ilə cəzalandırılır. Ağırlaşdırıcı hallarda isə bu əmələ görə azadlıqdan məhrum etmə cəzası maksimum 8 il müəyyən olunmuşdur.

---

[12] "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, № 874-IIIQ, http://www.meclis.gov.az

[13] Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişikliklər edilməsi haqqında Azərbaycan Respublikasının Qanunu, 29 iyun 2012-ci il, № 408-IVQD.

Göründüyü kimi, informasiya əsrinin tələbləri baxımından qanunvericiliyə edilmiş bu dəyişikliklər mütərəqqi xarakter daşımaqla, ictimai qaydanın qorunmasına, İnternet cinayətkarlığının azaldılmasına, dövlətin, cəmiyyətin və ya ayrı-ayrı şəxslərin qanunla qorunan maraqlarına zərər vurulmasının qarşısının alınmasına xidmət edir.

Beləliklə, internetdə kibercinayəkarlıq ən geniş yayılmış beynəlxalq xarakterli qeyri-hüquqi əməllərdən hesab edildiyindən, bu cinayətlərin xarakteri və diapazonu sosial-iqtisadi inkişafdan və İKT üzrə yeniliklərdən asılı olaraq dəyişir və genişlənir. Eyni zamanda, bu cinayətlərlə mübarizə müasir beynəlxalq hüquqda daha aktual əhəmiyyət kəsb edir. Müasir dövrdə "elektron hökumət", "elektron imza", "elektron ticarət" strategiyalarının inkişafını nəzərə alaraq, telekommunikasiyaların, rəqəmsal texnologiyaların, kompüter və internet şəbəkələrinin, bankomatların, ödəniş kartlarının və s. cinayətkar məqsədlərlə istifadəsinin mümkünlüyü baxımından bu cinayətlər həm milli hüquqi, həm də beynəlxalq hüquqi tənzimetmənin predmetini təşkil edir.

İKT-lərin inkişafı qanunvericiliyin bütün sahələrinin təkmilləşdirilməsini şərtləndirir, milli və beynəlxalq normalarda yeni hüquq pozuntusu tərkiblərinin təsbit olunmasını ehtiva edir. Ona görə də, elektron informasiyaların yayılması ilə əlaqədar inzibati xətalar digər hüquq pozuntularından, xüsusilə yaranan məsuliyyət baxımından cinayətlərdən tamamilə fərqlənir. Bu fərq başlıca olaraq ondan ibarətdir ki, cinayət inzibati xətaya nisbətən daha böyük ictimai təhlükəyə malikdir.

Şəxsin inzibati məsuliyyətə cəlb edilməsi zərurəti ondan yaranır ki, həmin hüququ pozan şəxs tərəfindən törədilmiş əməl dövlətə və cəmiyyətə ziyan vurmaqla, müəyyən ictimai münasibətlərə qəsd etmiş olur.

İnzibati hüquqpozmaların qarşısının alınmasına və onlarla mübarizəyə dair münasibətləri nizamlayan sistemləşdirilmiş qanunvericilik aktı Azərbaycan Respublikasının İnzibatı Xətalar Məcəlləsidir. Həmin Qanunun 16-cı fəsli İnformasiyadan istifadə edilməsi, onun yayılması və mühafizəsi qaydaları əleyhinə olan inzibati xətalara həsr edilmişdir.

Qanuna əsasən bilavasitə informasiya ehtiyatlarından düzgün istifadə edilməsi ilə bağlı fiziki və hüquqi şəxslər, habelə vəzifəli şəxslər üçün konkret məsuliyyətin hüdudları müəyyən olunaraq, müvafiq cərimə cəzası müəyyən edilmişdir. Bu kateqoriya inzibati hüquq pozuntularına aiddir: informasiya ehtiyatlarından istifadə qaydalarının pozulması (maddə 181), ətraf mühitə dair informasiyanın verilməsinin qanuna zidd məhdudlaşdırılması (maddə 181-1), məxfiləşdirilmiş məlumatların məxfiliyinin açılması haqqında sorğuya mahiyyəti üzrə baxmaqdan boyun qaçırılması (maddə 181-2), informasiya əldə etmək haqqında qanunvericiliyin pozulması (maddə 181-3) Fərdi məlumatlar haqqında qanunvericiliyin pozulması gizli qaydada informasiya alınması üçün nəzərdə tutulmuş texniki vasitələri satış məqsədi olmadan qanunsuz əldə etmə (maddə 181-4).

Digər tərəfdən, informasiyanın mühafizəsi qaydalarının pozulması və informasiya sistemlərinin sertifikatlaşdırılmaması da qanuna görə inzibati məsuliyyətə səbəb olur.

Bundan əlavə, Məcəllənin 183-1-ci maddəsi sertifikatlaşdırılmamış elektron imza və elektron sənəd dövriyyəsi vasitələrindən istifadə edilməsinə görə fiziki şəxslər üçün iyirmi manatdan iyirmi beş manatadək miqdarda, vəzifəli şəxslərə əlli beş manatdan yetmiş manatadək miqdarda, hüquqi şəxslərə isə iki yüz manatdan iki yüz əlli manatadək miqdarda cərimə nəzərdə tutur. Eyni zamanda, elektron sənədlərin saxlanmasında, ötürülməsində, qəbulunda vasitəçinin informasiya sistemindən etibarlı istifadəni təmin edən texnika və texnologiyalara, bilikli, təcrübəli və sərişləli işçi heyətə, xidmət göstərilmiş elektron sənədlərin vaxtını və mənbəyini teyin etməyə imkan verən şəraitə, həmin elektron sənədlərin vaxtı və mənbəyi haqqında informasiyanın saxlanması üçün etibarlı sistemə malik olmamasına görə də, inzibati məsuliyyət müəyyən edilərək inzibati tənbeh tədbirləri nəzərdə tutulmuşdur.

NƏTİCƏ

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

Kibercinayətkarlıqla effektiv mübarizənin aparılması və bu sahədə mövcud ola biləcək problemlərin aradan qaldırılması üçün ilk növbədə dövlət orqanları, idarə müəssisə və təşkilatların informasiya sistemləri, habelə bu sistemlərin mühafizə vasitələri Azərbaycan Respublikası Prezidentinin 02.09.2002-ci il tarixli “Bəzi fəaliyyət növlərinə xüsusi razılıq (lisenziya) verilməsi qaydalarının təkmilləşdirilməsi haqqında” Fərmanı ilə müəyyənləşdirilmiş qaydada sertifikatlaşdırılmalıdır.

Müasir dövrdə hər bir dövlətin milli informasiya infrastrukturu qlobal sistemdə birləşmiş internet şəbəkəsi ilə sıx bağlıdır. Məhz buna görə də bu növ cinayətkarlıq dövlətin milli təhlükəsizliyi üçün ciddi təhlükəyə çevrilib. Belə ki, heç bir dövlət bu növ cinayətkarlıqla ayrılıqda mübarizə aparmaq iqtidarında deyil. Bu cinayətkarlıqla səmərəli mübarizə aparmaq üçün beynəlxalq əməkdaşlıq çərçivəsində hüquqi tənzimləmə mexanizmləri hazırlanmalı və dünya birliyinin heç bir dövləti bu sahədə qəbul olunmuş standartlardan kənarda qalmamalıdır.

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