Aytəkin İbrahimova, Gülnaz Rzayeva. Virtual məkanda kibertəhlükələr və insan hüquqlarının müdafiəsi: beynəlxalq və milli-hüquqi tənzimetmə // Azərbaycan Hüquq Jurnalı. 2021 (№1), s.48-70

İNSAN HÜQUQLARI

VİRTUAL MƏKANDA KİBERTƏHLÜKƏLƏR VƏ İNSAN HÜQUQLARININ MÜDAFİƏSİ: BEYNƏLXALQ VƏ MİLLİ-HÜQUQİ TƏNZİMETMƏ

Aytəkin İbrahimova[*], Gülnaz Rzayeva[**]

Xülasə

Müasir cəmiyyətdə dünyagörüşünün dəyişməsi və inkişafı eyni zamanda hüquqazidd davranışlara da öz təsirini göstərir. Ənənəvi üsulların dövrün tələblərinə cavab verməd̈iyi bir şəraitdə insan hüquqlarına qəsd edən əməllərin törədilməsində yeni üsul və vasitə kimi İKT-dən daha çox istifadə olunur. Bu da "kibercinayət" aktuallaşmasına gətirib çıxarmışdır və kibercinayətlərlə mübarizənin gücləndirilməsini tələb edir. Məqalədə kibertəhlükələrin qanuni və qeyri-qanuni təsnifatları müqayisəli şəkildə təhlil edilmiş, virtual məkanda kibercinayətlərlə pozulan insan hüquqlarının müdafiəsi mexanizmlərinin işlənib hazırlanmasına dair təklif və tövsiyələr irəli sürülmüşdür.

Açar sözlər: *qlobal informasiya cəmiyyəti, kiberməkan, kibertəhlükə, kibermüharibə, ifadə azadlığı, şəxsi toxunulmazlıq hüququ, informasiya siyasəti.*

Giriş

Qlobal informasiya cəmiyyətinin sürətlə inkişafı insan hüquqlarının müdafiəsi mexanizmlərinin, eləcə də onlara qarşı yönəlmiş pozuntularla mübarizənin də dünya miqyasında müzakirəsinə gətirib çıxarmışdır. Qlobal informasiya cəmiyyəti yeni tip cəmiyyətdir ki, burada informasiya dövriyyəsi zaman, məkan, siyasi sərhədlər tanımır və məhz biliklərin emalı nəticəsində cəmiyyətin həyatının bütün aspektlərdə yaxşılaşdırılması üçün əsaslı qərarlar verilə bilər. Bu cəmiyyətin əsas tələbi hər kəsin informasiya mübadiləsində iştirakının təmin edilməsi olduğu üçün hal-hazırda internet şəbəkəsi həyatımızın ayrılmaz hissəsinə çevrilmişdir. Təbii ki, İKT-nin imkanlarından məqsədyönlü istifadə ilə yanaşı, qeyri-qanuni əməllərin törədilməsi də qaçılmaz haldır. Hətta, ənənəvi cəmiyyətdə mövcud olan cinayətlərin də kiberməkanda yeni törədilmə üsulları formalaşmışdır ki, bu da "kibertəhlükə" problemini gündəmə gətirmişdir. İnformasiya cəmiyyətinin ilkin dövrlərində kiberməkanda törədilən pozuntular yalnız informasiya hüquqlarına qəsd edirdisə, artıq bu gün İKT-dən istifadə etməklə törədilən cinayətlər müxtəlif insan hüquqlarını pozur. Bu da kibertəhlükələrə qarşı mübarizənin həm beynəlxalq, həm də milli səviyyədə gücləndirilməsini zəruri edir.

[*] hüquq üzrə fəlsəfə doktoru, Bakı Dövlət Universitetinin Hüquq fakültəsinin dekan müavini, Konstitusiya hüququ kafedrasının müəllimi

[**] hüquq üzrə fəlsəfə doktoru, Bakı Dövlət Universitetinin Hüquq fakültəsinin İnsan hüquqları və informasiya hüququ" UNESCO kafedrasının müəllimi, Azərbaycan Respublikası Dövlət Gömrük Komitəsi Akademiyasının müəllimi

Kiberməkan, yoxsa virtual məkan?

İnformasiya cəmiyyətinin qloballaşması ***"kiberməkan"*** termininin yaranmasına gətirib çıxarmışdır. "Kiberməkan" anlayışı ilk dəfə 1982-ci ildə Uilyam Qibson tərəfindən "Yanan xrom" (Burning Chrome) [14], az sonra isə 1984-cü ildə "Neuromancer" [15] əsərində istifadə edilmişdir.

ABŞ Ali Məhkəməsinin verdiyi anlayışa görə: "Kiberməkan konkret ərazisi olmayan, lakin dünyanın istənilən nöqtəsində internet vasitəsilə hər kəs üçün açıq və əlyetər olan unikal daşıyıcıdır." Darrel Ment "internasional məkanlar nəzəriyyəsi"ni şərh edərək, üç belə məkan olduğunu yazır: Antarktika, kosmos və açıq dəniz. Müəllif dördüncü belə məkan qismində kiberməkan olduğunu qeyd edir və bu məkana dövlət suverenliyinin şamil olunmadığını vurğulayır [9, s.70]. Maraqlı cəhət ondadır ki, kiberməkanda yurisdiksiya məsələlərini araşdıran tədqiqatçı yalnız müəlliflik hüququ və böhtanla bağlı tərəfləri izah edir. Bu zaman belə bir sual ortaya çıxır: Əgər kiberməkana heç bir dövlətin suverenliyi şamil olunmursa, onda bir dövlətin qanunvericiliyinin hər hansı bir məlumatın internetə yerləşdirilməsini qadağan etməsi nə dərəcədə qanunauyğun hesab oluna bilər? Və yaxud dövlət öz vətəndaşlarının istənilən informasiyaya çıxışını məhdudlaşdıra bilərmi? - Bütün bu kimi sualların cavablandırılması üçün kiberməkanın əsaslandığı prinsiplər normativ təminata malik olmalıdır. Təsadüfi deyil ki, 22 iyul 2000-ci il tarixdə "Böyük Səkkizlik"[1] dövlətləri tərəfindən qəbul edilmiş "Qlobal İnformasiya Cəmiyyətinin Okinava Xartiyası"nda dövlətlər siyasi, normativ və şəbəkə təminatını İKT-nin sonrakı inkişafı üçün zəruri tədbirlər sırasında qeyd etmişlər.

Müasir dövrdə kiberməkanın müstəqilliyinə dair çıxışlar səsləndirilir. Məsələn, 1996-cı ildə Davos forumunda Elektron Sərhəd Fondunun yaradıcısı Con Perri Barlou özünün məşhur "Kiberməkanın müstəqilliyi" adlı Bəyannaməsini elan etdi. Bəyannamədə bütün dövlətlərə belə bir müraciət ünvanlanır: "Kiberməkan sizin sərhədlərinizə aid deyil. Elə düşünməyin ki, onu siz yaratmısınız. Kiberməkan ictimai layihədir. Bizim aramızda sizə yer yoxdur. Siz kiberməkanda üstün hakimiyyətə malik deyilsiniz. Bizim üzərimizdə hökmranlıq etməyə sizin nə mənəvi haqqınız, nə də məcburetmə metodlarınız var. Biz kiberməkanda sizin qurduğunuzdan daha ədalətli və humanist olan cəmiyyət yaradacağıq…" [19] Belə çıxışların səslənməsinə baxmayaraq, kiberməkanla bağlı məsələlər hələ də hər bir dövlətin öz yurisdiksiyası çərçivəsində həll olunur. Təbii ki, bu zaman beynəlxalq hüquq normaları və prinsipləri nəzərə alınır.

"Kiberməkan" anlayışının təhlili məqsədilə "informasiya məkanı", "İnternet" və s. bu kimi terminlərin məzmununa aydınlıq gətirilməsi, onların arasında fərqin müəyyən edilməsi məqsədəmüvafiqdir. ***İnternet*** - informasiyanın saxlanması və ötürülməsi üçün yaradılmış kompüter şəbəkələrinin ümumdünya sistemidir. Ona görə də əksər hallarda İnternet "qlobal şəbəkə", "ümümdünya

[1] Almaniya, ABŞ, Böyük Britaniya, Fransa, Yaponiya, Kanada, Rusiya, İtaliya.

şəbəkəsi" kimi adlandırılır. Bu şəbəkəni kiberməkanla eyniləşdirmək olmaz. Darrel Ment yazır ki, biz İnternetin haradan başlandığını bilirik, amma kibermə-kanın sərhədlərini və məhz hardan başlandığını müəyyənləşdirmək qeyri-mümkündür. Ona görə də kiberməkan anlayışı İnternetlə eyniləşdirilə bilməz [9, s.69-70]. Tədqiqatçının mövqeyini məqbul saymaq olar, yəni kompüter şəbəkələrinin vahid sistemi olan İnternetdən fərqli olaraq, kiberməkan metaforik abstrakt, virtual reallıq kimi qiymətləndirilməlidir. Qısa sözlə desək, kiberməkan ümumdünya kompüter şəbəkəsinin içində sərhədləri bilinməyən bir "aləmdir". Ona görə də əksər hallarda bu aləmi xarakterizə etmək üçün ***"virtual məkan"***[2] anlayışından istifadə edilir. Məsələ burasındadır ki, beynəlxalq normalarda hüquqi termin olaraq, "kiberməkan" anlayışına müraciət olunur. Lakin milli hüquqda isə "virtual" terminina bir çox normativ aktlarda rast gəlmək olar. Həmin normativ aktların məzmununa əsasən, deyə bilərik ki, dövlətdaxili hüquqda "virtual" adı altında İnternet vasitəsilə qurulan münasibətlər başa düşülür. Hətta, Virtual Azərbaycan [16], Virtual Qarabağ [18] və s. bu kimi saytlar yaradılmış və fəaliyyət göstərir. Hətta, "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016-2020-ci illər üçün Dövlət Proqramı"nda "Azərbaycan həqiqətlərinin virtual məkanda təbliği və yayılmasının genişləndirilməsi üzrə tədbirlər görülməsi" milli kontentin inkişaf etdirilməsi üzrə tədbirlər sırasında qeyd olunmuşdur. Eyni zamanda, azərbaycandilli mənbələrdə "virtual cəmiyyət" "İnternet cəmiyyət"lə eyniləşdirilərək, elektron fəzada yaranan və fəaliyyət göstərən yeni tip cəmiyyət kimi şərh olunur.

Ədəbiyyatda hər iki terminlə bağlı yanaşmalardan açıq-aydın görünür ki, məna baxımından həm kiberməkan, həm də virtual məkan kompüter şəbəkəsindən istifadə edilməklə qurulan və gözlə görülə bilməyən bir aləmdir. İngilisdilli ədəbiyyatlarda kiberməkan anlayışına daha çox rast gəlinir. Lakin bununla belə, "virtual mühit", "virtual aləm", "virtual dünya" kimi anlayışlardan da istifadə edilir və verilən anlayışlardan bunların hamısının kiberməkanla eyni məzmuna malik olması nəticəsinə gələ bilərik. Lakin fərqli şərhlər də vardır. Belə ki, bəzi tədqiqatçılar kiberməkan və virtual reallığın hər ikisinin İnternet şəbəkəsi, KİV-lə bağlı olduğunu qeyd edərək yazırlar: "Hipermediya[3] iki funksiya icra edə bilər: obyektiv aləmdə pəncərə funksiyası və subyektiv aləmin güzgüsü funksiyası. Birinci funksiya virtual reallığı, ikinci isə kiberməkanı əhatə edir. Yəni virtual reallıq dəqiq qavranılan aləmi əks etdirirsə, kiberməkan həmin aləmin

[2] Ümumi anlamda, "virtual" termini xəyali, fiziki baxımdan reallıqda mövcud olmayan, lakin müəyyən şəraitdə meydana çıxa bilən mənasını verir. Virtual reallıq isə süni üsullarla və interaktiv multimedia vasitələri ilə yaradılan elektron gerçəklik, gerçəkliyin kompüter modelidir.

[3] Hipermediya - audio, video, qrafik və mətn formasında məlumatların Web sisteminə inteqrasiyasını xarakterizə edir.

dəqiq konseptual əsasını müəyyən edir. [29]" Rusdilli ədəbiyyatlarda isə "virtual məkan" ya "cyberspace" kateqoriyasının tərcüməsi kimi qiymətləndirilir [6, s.742], ya da bu anlayışların sinonim olduğu iddia edilir [5, s.6]. Fikrimizcə, "kiberməkan" və "virtual məkan" hər ikisi abstrakt və sinonim anlayışlardır. Sadəcə olaraq, nəzəri yanaşmadan asılı olaraq bəzi müəlliflər birinci, bəzi müəlliflər isə ikinci termindən istifadə edirlər. Yəni daha çox texniki və idarəetmə aspektindən yanaşdıqda, kiberməkan, sosial-humanitar movqedən yanaşdıqda isə virtual məkan anlayışına müraciət olunur. Nəzərə alsaq ki, hal-hazırda dünyada internetdən başqa, alternativ şəbəkə yoxdur, virtual məkan və kiberməkan anlayışları sırf internet müstəvisində şərh olunmalıdır.

Kibercinayətlər kibertəhlükələrin bir növü kimi

İKT-nin sürətli inkişafı nəticəsində formalaşan anlayışlardan olan ***"kibercinayətkarlıq"*** çox geniş məzmuna malikdir. Ədəbiyyatda həmçinin "kompüter cinayətkarlığı" terminindən də istifadə olunur. Fikrimizcə, ikinci anlayış texniki aspektdən yanaşmanın nəticəsidir və birinci anlayış daha geniş olduğu üçün məqbul hesab olunmalıdır. Təsadüfi deyil ki, Azərbaycan Respublikasının Cinayət Məcəlləsində əvvəllər "Kompüter informasiyası sahəsində cinayətlər" ifadəsi nəzərdə tutulmuşdusa, hal-hazırda kibercinayətlərə görə məsuliyyət müəyyənləşdirən fəsil "Kibercinayətlər" adlanır. Maraqlı məqam ondan ibarətdir ki, kiberməkan çox geniş əhatə dairəsinə malikdir və burada yalnız kompüter informasiyası ilə bağlı cinayətlər törədilmir, eyni zamanda kibermühitdən istifadə edərək, digər qeyri-qanuni əməllər (dələduzluq, müəlliflik hüquqlarını pozma, təhqir, böhtan və s.) icra olunur, yəni kiberməkanda mövcud əlaqələr və texniki vasitələr ənənəvi cinayətlərin törədilməsinin yeni üsulları qismində çıxış edə bilir. Bəs belə olan halda "kibercinayət" anlayışının hədləri artmırmı? Cinayət Məcəlləsində yalnız kompüter informasiyası ilə bağlı cinayətlərin kibercinayətlər qismində tanınmasında qanunvericinin mövqeyi doğrudurmu? - "Kibercinayətkarlıq haqqında" 23 noyabr 2001-ci il tarixli Budapeşt Konvensiyasına nəzər salsaq, burada kibercinayətlər fərqli qaydada qruplaşdırılır:

1. Kompüter verilənləri və sistemlərinin məxfiliyi, tamlığı və istifadə imkanlarına qarşı cinayətlər - qanunsuz daxil olma, qanunsuz ələ keçirmə, verilənlərə müdaxilə, sistemlərə müdaxilə, qurğulardan qanunsuz istifadə;

2. Kompüter vasitələrindən istifadə ilə bağlı cinayətlər - kompüter texnologiyalarından istifadə etməklə saxtalaşdırma, kompüter texnologiyalarından istifadə etməklə dələduzluq;

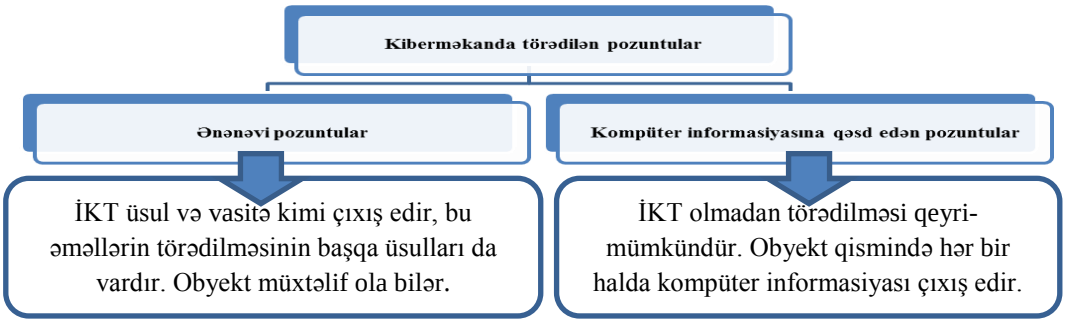
3. Məlumatların məzmunu ilə bağlı cinayətlər - uşaq pornoqrafiyası ilə bağlı cinayətlər;

4. Müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər - müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər.

Göründüyü kimi, Konvensiya kibercinayətləri kompüter cinayətlərinə və kompüter vasitəsilə törədilən cinayətlərə bölür. Əslində Konvensiyanın möv-

qeyi ilə razılaşmaq olar. Çünki yuxarıda sadalanan cinayətlərin hamısı kibermәkanda törədilir. Təbii ki, Azərbaycan Respublikasının cinayət qanunvericiliyində həmin əməllərin hamısı sanksiyalaşdırılmışdır. Sadəcə olaraq onlar kibercinayətlər fəslində deyil, müxtəlif fəsillərdə nəzərdə tutulmuşdur. Müasir dövrdə İKT-nin bütün insan həyatını əhatə etdiyini və onlardan kriminal məqsədlər üçün istifadənin geniş vüsət aldığına əsaslansaq, informasiya texnologiyaları cinayət əməllərinin törədilməsi üçün ən asan üsul kimi qiymətləndirilməlidir. Belə olan təqdirdə kibermühitdən istifadə etməklə törədilən bütün cinayətlərin kibercinayət kimi qəbul olunması bir qədər məntiqi sayılmır. Çünki cinayət əməllərinin obyekti və motivi (məqsədi) fərqli olur. Digər tərəfdən isə kiberməkanda törədilən bir çox əməllərin ənənəvi üsullarla da törədilməsi mümkündür. Məsələn, Azərbaycan Respublikası Cinayət Məcəlləsinin 171-1-ci maddəsində nəzərdə tutulan uşaq pornoqrafiyasının dövriyyəsi - 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 ilə müşayiət olunur. Belə pornoqrafik məhsullar isə yalnız kiberməkanda deyil, müxtəlif nəşrlər, əşya və materiallar formasında da yayıla bilər. Bütün bunlara istinad edərək, Azərbaycan Respublikasının qanunvericiliyinin yanaşmasını məqbul saymaq olar. Sadəcə olaraq İKT-nin inkişaf etdiyi mühitin xüsusiyyətlərini nəzərə alıb, bir çox ənənəvi cinayətlərin törədilməsi üsulları ilə bağlı dəyişikliklərin edilməsi məqsədəmüvafiqdir. Digər bir məsələ isə ondan ibarətdir ki, terrorizm və s. bu kimi təhlükəli cinayətlər Konvensiyanın normalarından kənarda qalmışdır. Tvitter, Youtube və digər şəbəkələrdə müxtəlif terrorçuluğa açıq çağırışların (məsələn, İŞİD) yayılması kompüter vasitəsilə törədilən cinayətlərin siyahısının artırılmasını tələb edir.

Qeyd olunanlar əsasında belə bir nəticəyə gəlmək olar:



Adı çəkilən Konvensiya ilə yanaşı, başqa rəsmi təsnifatlar da vardır. Belə təsnifatlardan biri 1991-ci ildə İnterpolun işçi qrupu tərəfindən hazırlanmışdır. Bu təsnifatda bütün kodlar "Q" hərfi ilə başlayan eyniləşdiriciyə (identifikatora) malikdir. Onlar özləri də qəsdin növündən asılı olaraq 6 qrupa bölünür

ki, burada da "A", "F", "D", "R", "S", "Z" hərflərindən istifadə olunur. Məsələn, "QA" hərf birləşməsindən ibarət kod - İcazəsiz (sanksiyalaşdırılmamış) giriş və ələ keçirməni, "QF" birləşməsindən ibarət kod - kompüter dələduzluğunu, "QR" kodu - qanunsuz surətçıxarmanı (piratçılığı) əks etdirir və s. Bu kodların hər birinin cinayətin törədilmə üsulundan asılı olaraq öz təsnifatı aparılır. Hər bir təsnifatda ardıcıllıq cinayətin ictimai təhlükəsinin azalması istiqamətində gedir.

Kibercinay ətlərin	**İNTERPOL təsnifatı və kodları**
QA – İcazəsiz (sanksiyalaşdırılmamış) giriş və ələ keçirmə	• QAH – kompüter abordajı • QAİ – ələ keçirmə • QAT – vaxtın oğurlanması • QAZ – icazəsiz giriş və ələ keçirmənin digər növləri
QD – kompüter verilənlərinin dəyişdirilməsi	• QDL – məntiqi bomba • QDT – troya atı • QDV – kompüter virusu • QDW – kompüter soxulcanı • QDZ – verilənlərin dəyişdirilməsinin digər növləri
QF – kompüter dələduzluğu	• QFC – ATM-lərlə dələduzluq • QFF – kompüter saxtalaşdırması • QFG – oyun avtomatları ilə dələduzluq • QFM – giriş-çıxış proqramları ilə manipulyasiyalar • QFP – ödəmə vasitələri ilə dələduzluq • QFT – telefon dələduzluğu • QFZ – kompüter dələduzluğunun digər növləri
QR – qanunsuz olaraq surət çıxarılması (piratçılıq)	• QRG – kompüter oyunları • QRS – digər proqram təminatları • QRT – yarımkeçirici məmulatların topoqrafiyası • QRZ – digər növ qanunsuz surət çıxarmalar
QS – kompüter sabotajı	• QSH – avadanlıq təminatı ilə • QSS – proqram təminatı ilə • QSZ – sabotajın digər növləri

QZ – digər kompüter cinayətləri	• QZB – kompüter elan lövhələrinin istifadəsi ilə həyata keçirilən cinayətlər • QZE – kommersiya sirri hesab olunan məlumatların oğurlanması • QZS – konfidensial informasiyanın ötürülməsi • QZZ – kompüter cinayətlərinin digər növləri

Avtomatlaşdırılmış axtarış-informasiya sisteminə daxil edilmiş İnterpol kodlaşdırması bir çox kibercinayətlərin aşkar edilməsində geniş imkanlara malikdir.

Qeyri-rəsmi təsnifatlardan isə Debra Littlejon Şinderin verdiyi təsnifatı daha geniş şərh kimi qiymətləndirmək olar. Belə ki, D.L.Şinder kibercinayətlərin iki kateqoriyasını [10, s.19-33] fərqləndirir: zorakılıqla törədilən və zorakılıqla müşayiət olunmayan (qeyri-zorakı) cinayətlər. Müəllif zorakılıqla törədilən cinayətlərə kiberterrorçuluğu, hədə-qorxu ilə (təhdidlə) hücumu,[4] kibertəcavüzü,[5] uşaq pornoqrafiyasını daxil edir. Zorakılıqla müşayiət olunmayan kibercinayətləri isə D.L.Şinder müxtəlif subkateqoriyalara ayırır: qanunsuz daxil olma,[6] kiberoğurluq, kiberdələduzluq, dağıdıcı kibercinayətlər[7] və digər kibercinayətlər.

D.L.Şinder hər subkateqoriyanın tərkibində müxtəlif cinayətləri qruplaşdırır. Məsələn, kiberoğurluğun plagiat, qanunsuz mənimsəmə, piratçılıq, fərdi məlumatların ələ keçirilməsi və s. növlərini fərqləndirir [10, s.24]. Digər kibercinayətlərə isə internet-qumarxanaların təşkili, internet qaçaqmalçılığı, internet vasitəsilə narkotik vasitələrin dövriyyəsi və s. əməllər daxil edilir. Müəllif tərəfindən digər kibercinayətlərin ayrıca bir subkateqoriya kimi göstərilməsi cəmiyyət inkişaf etdikcə kiberməkanda meydana çıxan yeni cinayət əməllərinin də təsnifata daxil edilməsinə imkan verir (Qeyd etmək lazımdır ki, kibercinayətlər

[4] D.L.Şinderin verdiyi anlayışa görə, **hədə-qorxu ilə (təhdidlə) hücum (assault by threat)** – e-mail vasitəsilə həyata keçirilə bilər. Bu kibercinayət insanların özü və onların yaxınlarının həyatı ilə bağlı hədələməklə törədilir və həmçinin müəssisələrə və ya dövlət qurumlarına e-poçtla göndərilən bomba təhdidlərini də əhatə edə bilər.

[5] D.L.Şinderin verdiyi anlayışa görə, **kibertəcavüz (cyberstalking)** – cinayətin qurbanında mütəmadi şəkildə qorxu yaradan və real həyatda mövcud olan fiziki təcavüz və digər şiddətli davranışa səbəb ola biləcək ifadə və təhdidləri əks etdirən elektron təcavüz formasıdır.

[6] D.L.Şinderin verdiyi anlayışa görə, **özbaşına (qanunsuz) müdaxilə (cyber trespass)** – zamanı cinayətkar kompüter və şəbəkə resurslarını qanunsuz əldə edir, lakin burada informasiyanın zədələnməsi və korlanması məqsədi olmur. Məsələn, yetkinlik yaşına çatmayan hakerlərin "özünü yaşıdlarına sübut etmək" və ya müxtəlif "fərdi çağırışlar" məqsədilə törətdiyi əməllər.

[7] D.L.Şinderin verdiyi anlayışa görə, **dağıdıcı kibercinayətlər (destructive cybercrimes)** – şəbəkənin dağıdılması və məlumatların zədələnməsi və ya məhv edilməsi ilə müşayiət olunur. Bu növ əməllərə şəbəkəyə müdaxilə və məlumatların və proqramların silinməsi, veb-server və veb-səhifələrə müdaxilə, şəbəkə və kompüterlərə viruslar və digər ziyanverici proqramlarla ziyan vurulması, Dos hücumlar daxildir.

haqqında cinayət hüquq elmində ətraflı məlumat verildiyi üçün bu məsələyə cinayətlərin adını qeyd etməklə toxunmağa üstünlük veririk).

Kibercinayətlərin törədilməsinin müxtəlif üsulları vardır. 2016-cı ilin məlumatına görə [2], informasiya təhlükəsizliyinin ən zəif nöqtəsi insan faktorudur və ona qarşı yönəlmiş hücumların geniş yayılan 4 növünə Azərbaycanda çox təsadüf edilir:

1. Sosial mühəndislik (Social engineering, Human hacking). Sosial mühəndislik - insanlarla qarşılıqlı əlaqədə olaraq onlardan məlumat toplamaqdır. Bu növün əsas amillərindən biri saxta profillərdən (başqa adla və ya hər hansı bir saxta şirkət, kampaniya və s.), virtual dostluq və tanışlıqdan istifadə edib istifadəçini aldatmaqdan ibarətdir. Əsas məqsədi tanışlıq, virtual dostluq və ya hər hansı digər etibar qazanmış mənbədən sui-istifadə etməklə məlumatın toplanmasıdır. Ona görə də istifadəçilərin onlara gələn məktubların ünvanına xüsusi diqqət yetirməsi vacibdir. Hətta bir hərf dəyişməklə belə saxta sayt yaradıla bilər. (məsələn, www.facebook.com saytı əvəzinə www.facabook.com və s.)

2. "Brute-forcing". "Brute-force" - istifadəçinin hər hansı e-mail hesabına və ya digər hesabındakı şifrələr toplusuna edilən hücumdur. Bu zaman istifadəçiyə aid olan məlumatlardan (məsələn, ad, soyad, valideyn və ya övladın adı və doğum tarixləri, maşın nömrəsi, telefon nömrəsi və s.) istifadə edərək manual (əl ilə bir-bir) və ya avtomatik şəkildə müxtəlif vasitələrlə hesabdakı şifrlər yoxlanılır və şifrə (parol) tapılır. Bəs brute-force hücumunun məqsədi nədir? - Social engineering kimi bu hücumlar da istifadəçi haqqında məlumatların toplanması və sonradan həmin məlumatların qeyri-qanuni məqsədlərlə istifadəsi məqsədini daşıyır. Elektron təhlükəsizlik Mərkəzinin tövsiyələrinə görə, belə hücumlardan qorunmaq üçün şifrələrin təhlükəsizliyi qaydalarına riayət olunmalıdır. Məsələn, sosial şəbəkələrdə, maillərdə və ya digər hesablarda eyni şifrə istifadə olunmaması [2]. Çünki belə hal bir hesabdakı şifrənin sındırıldığı halda digər hesabların da "ələ keçməsi"nə gətirib çıxara bilər. Eyni zamanda, yaxşı olar ki, şifrələrin qoyulması zamanı istifadəçi özünə aid məlumatlardan istifadə etməsin. Məsələn, bir qayda olaraq, şifrə qismində ad və ona bitişik formada doğum tarixinin ili, ayı və ya günü istifadə olunur. Belə tip şifrələrin aşkar olunması daha asan olduğu üçün cinayətkarın işi də asanlaşmış olur. Ona görə də istifadəçilərin bu cür şifrələrdən uzaq olması daha məqsədəmüvafiq hesab edilir. Bundan əlavə, istifadəçiyə məxsus şifrənin bədniyyətlinin əlinə keçməməsi üçün ikiqat autentifikasiyadan[8] istifadə olunması müasir və uğurlu bir vasitə kimi qiymətləndirilir. İlkin dövrlərdə daha çox şifrənin yığılması və sonradan mobil qurğuya sms (mesaj) gəlməsi üsulu tətbiq edilirdisə, 2015-ci ildən etibarən ikiqat autentifikasiya üçün ikiqat biometrik şifrələrdən

[8] **İkiqat autentifikasiya (two-factor authentication – 2FA)** – multi-faktor autentifikasiyanın bir növüdür, eyniləşdirmə üçün eyni anda iki müxtəlif komponentdən istifadə edilməsini nəzərdə tutur. Məsələn, şifrənin yığılması + mobil telefona daxil olan zəng və ya sms.

istifadəyə başlandı. Bu o deməkdir ki, yalnız bioloji markerə çevrilmiş barmaq izi deyil, eyni zamanda gözün torlu qişası da identifikasiya üçün istifadə olunur. Mobil bankçılıqda geniş yayılmış bu üsul artıq yeni telefonların son modellərində tətbiq edilir. Hesab edirik ki, biometrik məlumatlar eyniləşdirmə üçün daha "etibarlı" xarakterə malikdir və bu sahədə tədqiqatların davam etdirilməsi və təcrübəyə tətbiqi informasiya təhlükəsizliyinin təminatında əvəzsiz rola malik ola bilər. Digər tərəfdən isə müxtəlif şifrələrin yadda saxlanmasına nisbətdə biometrik məlumatlardan istifadə etməklə eyniləşdirmə daha asan və rahat olar.

3. Ziyanverici proqramlar (malware) vasitəsilə yoluxdurma. Zərərverici yoluxdurma texnikası istifadəçiyə video, şəkil, musiqi, kino, hər hansı fayl, link göndərməklə kompüterə ziyanverici proqram (troyanlar, casus proqramları, soxulcanlar, viruslar və botnetlər) yüklənməsinə nail olmaqdır. Bu proqramların əsas məqsədi hədəfdən informasiyanın oğurlanmasıdır.

Qeyd etmək lazımdır ki, istifadəçilərin internetdən normal istifadəsinə mane olan ziyanverici proqramlar artmaqda davam edir və onlara qarşı mübarizə tədbirləri gücləndirilməkdədir. Məsələn, Elektron Təhlükəsizlik Mərkəzi botnetlərdən qorunmaq üçün firewall quraşdırmaq, əməliyyat sistemini, brouzerləri və digər proqram təminatlarını istehsalçıların rəsmi veb səhifəsindən mütəmadi şəkildə yeniləmək, naməlum istifadəçilərdən faylları qəbul etməmək, tanınmayan resurslara malik əlavələri (faylları) qəbul etməmək, faylları endirərkən ehtiyatlı olmaq və s. bu kimi tövsiyələr verir.

4. Fişinq (Phishing). Fişinq - ingilis dilindən tərcümədə "balıq ovu" deməkdir və qlobal şəbəkədə balıq ovunu xatırladan fırıldaqçılığın bir növüdür. Belə ki, fırıldaqçı (fişer) internetdə "tələ" quraraq, bu tələyə düşən internet istifadəçilərini aldatmaqla məşğul olur. Fişer müxtəlif üsullarla internet istifadəçilərindən bank hesablarını, kredit kartlarını və internetə çıxış üçün lazım olan informasiyaları öyrənir. Fişinq kiberdələduzluğun xüsusi növüdür, istifadəçiləri aldatma yolu ilə adətən maliyyə xarakterli fərdi məlumatların təqdim olunmasına məcbur etməyə yönəlir. Dələduz bank saytı kimi görünən (və ya maliyyə əməliyyatları aparılan istənilən digər sayt kimi, məsələn, eBay) saxta veb-sayt yaradır. Sonra cinayətkarlar istifadəçiləri bu sayta aldadıb aparmağa cəhd edirlər ki, bu saytda onlar login, parol və ya PIN-kod kimi konfidensial məlumatları daxil etsinlər. Çox zaman dələduzlar bunun üçün həmin saytlara istinadları spamın köməyilə yayırlar. Bəs belə saxta veb-saytları qanuni veb-səhifələrdən necə ayırmaq olar? - Bununla bağlı, Elektron Təhlükəsizlik Mərkəzinin istifadəçilər üçün hazırladığı tövsiyələrdə fişinq təhlükəsini müəyyən etmə və ondan müdafiə üsulları sadalanır [2]. Məsələn, istifadəçiyə gələn məktubda "Dəyərli müştərilərimiz" şəklində ifadələrin olması məktub göndərənin istifadəçini tanımadığını göstərir. Hətta veb-ünvanları yazarkən kiçik bir hərf səhvi belə istifadəçini "tələ"yə sala bilər. Açılan səhifə onun daxil olmaq istədiyi veb-sayta çox bənzəyə bilər. Ona görə də istifadəçi diqqətli və ehtiyatlı

olmazsa, müəyyən mərhələyə qədər məlumatlar çoxdan oğurlanmış ola bilər (məsələn, www.microsoft.com əvəzinə, www.micrsoft.com daxil etdiyiniz zaman qarşınıza axtardığınız sayta çox bənzəyən səhifə çıxa bilər və s.).

İKT inkişaf etdikcə kibercinayətlərin törədilmə üsulları da artır və buna adekvat olaraq onlarla mübarizə tədbirləri də gücləndirilməlidir. Çünki bu növ cinayətlər yüksək latentlik səviyyəsi ilə xarakterizə olunur və bu latentlik onların törədilmə üsullarının xüsusiyyətlərindən irəli gəlir. Demək olar ki, əksər tədqiqatçılar latentlik dərəcəsindən asılı olaraq kibercinayətlərin 4 növünü fərqləndirir [4, s.171-176; 3]:

Birinci qrupa baş vermə faktı haqqında nə hüquq mühafizə orqanlarının, nə də zərər çəkmiş şəxslərin heç bir məlumatının olmadığı cinayətlər daxildir. Buna "təbii latentlik" deyilir. Bu növ cinayətlərdə "aşkara çıxarma problemi" hökm sürür.

İkinci qrupa kibercinayətin baş verməməsi barədə məlumat vermək vəzifəsi daşıyan şəxslərin hüquq mühafizə orqanlarını məlumatlandırmaması ilə bağlı cinayətlər daxildir. Bu isə "süni latentlik" kimi qiymətləndirilir və "məlumat verilməməsi problemi" mövcud olur.

Üçüncü qrupa törədilmiş kibercinayət barəsində hüquq mühafizə orqanlarına məlumat verilsə də, istintaqı aparan şəxslərin peşəkarlıq səviyyəsinin aşağı olmasından irəli gələrək, əmələ düzgün qiymət verilməməsi və əməldə cinayət tərkibi əlamətlərinin aşkar edilməməsi nəticəsində latent qalan cinayətlər daxildir. Bu isə ədəbiyyatda "sərhəd və ya hissəvi latentlik" adlandırılı

Dördüncü qrup kibercinayətlər baş vermə halı barəsində hüquq mühafizə orqanlarının məlumatının olduğu, lakin müxtəlif təsəvvürlərdən irəli gələrək qeydiyyatı aparılmayan cinayətlər (gizlədilən və ya ört-basdır edilən cinayətlər) hesab olunur.

İnformasiya müharibələri kibertəhlükələrin növü kimi

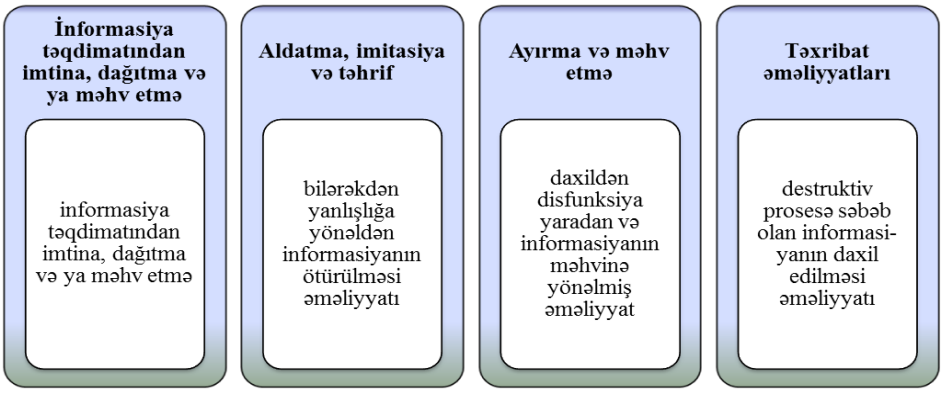
İnformasiya qarşıdurması - tərəflərin xüsusi metodlardan, informasiya ehtiyatlarına təsir üsulları və vasitələrindən istifadə etməklə qarşı tərəfin informasiya ehtiyatlarının məhvinə və ya nəzarətdə saxlanmasına yönəlmiş informasiya əməliyyatlarıdır. ***İnformasiya hücumu*** - icazə olmadan istənilən formada informasiyanın köçürülməsi, dəyişdirilməsi və məhvinə, həmçinin proqram təminatlarına, məxfi informasiyanın saxlandığı texniki qurğulara və insan psixologiyasına yönəlmiş əməliyyatlardır. ***İnformasiya müharibəsi*** isə özündə informasiya hücumu və informasiya qarşıdurması kimi əməliyyatları birləşdirən daha təhlükəli informasiya təsiri forması olub, qarşı tərəfin informasiyasına, informasiya proseslərinə və sistemlərinə zərər vurmaqla informasiya üstünlüyü əldə etmək, qarşı tərəfin iqtisadi, hərbi potensialını ələ keçirmək, ictimai şüura informasiya təsiri göstərməklə insanların davranışlarını dəyişmək uğrunda həyata keçirilən məqsədyönlü fəaliyyətdir. İnformasiya müharibəsində informasiya həm silah, həm də məqsəd, həm də müdafiə obyekti

kimi çıxış edir. Mənbələrdə informasiya müharibəsi kombinə edilmiş kibercinayətlərə aid olunur [28, s.57].

Ədəbiyyatda "şəbəkə müharibəsi" və "kibermüharibə" terminlərini irəli sürən mövqelər də vardır ki, bu qrup müəlliflər şəbəkə müharibəsini daha çox ictimai səviyyəli konseptual münaqişə kimi qiymətləndirərək, onun iqtisadi, siyasi və sosial sferaları əhatə etdiyini, kibermüharibənin isə əksinə hərbi məqsəd daşıdığını iddia edirlər [21, s.27-30].

İnformasiya müharibəsinin iki istiqamətdə aparılması ilə bağlı fikirlərə də rast gəlinir: informasiya-texniki müharibə və informasiya-psixoloji müharibə. İnformasiya-texniki müharibədə müxtəlif növ informasiya sistemlərinə (verilənlər bazası, analitik sistemlər və s.), telekommunikasiya vasitələrinə, kompüter şəbəkəsinə və s. texniki vasitələrə hücum əməliyyatları nəzərdə tutulur. Nəticədə informasiya sistemlərinin ələ keçirilərək nəzarətdə saxlanması və ya məhv edilməsi əməliyyatları reallaşdırılır. İnformasiya-psixoloji müharibədə isə hədəf ayrı-ayrı insanlar, sosial qruplar, təşkilatlar, bir və ya bir neçə dövlətin vətəndaşları, dünya ictimaiyyətidir. Əslində belə bölgünün aparılması bir qədər məntiqi ziddiyyət doğurur. Bir tərəfdən informasiya müharibəsinin məqsəd və strategiyasının (siyasi, hərbi, iqtisadi və s.) vacib məqam olmasını nəzərə alsaq, bu cür təhlükəli əməliyyatlar sisteminin yalnız texniki istiqamətdə xarakterizə olunması onun əsl mahiyyətini açmağa imkan vermir. Çünki hər bir halda həyata keçirilən fəaliyyətin məqsədi əsas faktor hesab olunur. Digər tərəfdən isə müasir dövrdə psixoloji informasiya müharibəsinin özü belə informasiya sistemlərindən istifadə etmədən mümkün deyil və burada da texniki əməliyyatlar həyata keçirilir. Ona görə də informasiya müharibəsinin məqsəd və strategiya aspektindən fərqləndirilməsi daha düzgün olar. İnformasiyanın ələ keçirilməsi, korlanması, dəyişdirilməsi, məhv edilməsi və s. bu kimi texniki əməliyyatlar isə informasiya müharibəsinin həyata keçirilməsinin üsulları kimi qəbul olunmalıdır.

İnformasiya müharibəsinin fundamental paradiqmasının aşağıdakı informasiya əməliyyatlarından ibarət olması qeyd edilir:



İnformasiya müharibəsini daha çox texniki istiqamətdə izah edən yuxarıdakı bölgü informasiya-hüquqi aspektdən qarşıya çıxan sualları cavablandırmaq üçün yetərli deyil. Fikrimizcə, bu məsələ ilə bağlı ABŞ tədqiqatçısı Martin Libikinin təsnifatı daha dolğun səciyyə daşıyır. Belə ki, o, informasiya müharibəsinin 7 formasını fərqləndirir [22, s.7-8]:

1. Komanda-nəzarət müharibəsi (Command and Control Warfare) - komandanlıq və icraçılar arasındakı əlaqə kanallarına istiqamətlənmiş informasiya müharibəsidir. Bu növ müharibədə əvvəlki dövrlərdə geniş yayılmış anti-rəhbər (anti-head) və müasir dövrdə inkişaf etmiş, İKT-dən istifadə etməklə icra olunan antineek əməliyyatlardan istifadə olunur.

2. Kəşfiyyat müharibəsi (Information Based Warfare) - mühüm informasiyanın toplanması və bu zaman hücum edən tərəfin öz informasiya resurslarını mühafizə etməsi prosesidir.

3.Elektron müharibə (Electronic Warfare) - elektron kommunikasiya vasitələrinə qarşı yönəlmiş müharibədir. Elektron kommunikasiya vasitələri dedikdə, radio əlaqə, radarlar, kompüter şəbəkəsi nəzərdə tutulur. Elektron dövlətin formalaşdırılmasından sonra geniş vüsət alan bu növ müharibələrin əsas obyektini kriptoqrafik istiqamətlər təşkil edir. Məhz belə növ müharibələrin artmasının nəticəsidir ki, respublikamızda da dövlət əhəmiyyətli informasiya resurslarının mühafizəsi üçün xüsusi qaydalar müəyyənləşdirilmişdir.

4. Psixoloji müharibə (Psychological Warfare) - insanların psixologiyasına təsir edən müharibə növüdür. M.Libiki psixoloji müharibənin 4 kateqoriyasını fərqləndirir: milli iradəyə qarşı yönəlmiş əməliyyatlar, rəhbərliyə (komandanlığa) qarşı yönəlmiş əməliyyatlar, hərbi qüvvələrdə əsgərlərə qarşı yönəlmiş və buna oxşar digər əməliyyatlar, mədəniyyətlərin müharibəsi [22, s.35].

5. Haker müharibəsi (Hacker Warfare) - qarşı tərəfin mülki obyektlərinə yönəlmiş diversiya əməliyyatlarıdır. Hakerlərin silahı viruslardır.

6. İqtisadi informasiya müharibəsi (Economic Info-Warfare) - M.Libiki bu müharibəni iki formada təsvir edir: informasiya blokadası və informasiya imperializmi. Tədqiqatçı informasiya blokadasını iqtisadi blokadanın bir versiyası kimi qiymətləndirərək, informasiyanın kəsilməsini iqtisadi sahənin - ticarət əlaqələrinin də kəsilməsi ilə nəticələnəcəyini əsaslandırır. İnformasiya imperializmini isə müəllif ümumi iqtisadi imperializm siyasətinin bir hissəsi kimi şərh edir və ticarətin özünü də bir müharibə kimi qiymətləndirir. O iddia edir ki, ticarət sahəsində üstünlüyün əldə olunması nəticə etibarilə həmin dövlətlərdə bilik üstünlüyünə gətirib çıxarır və belə hakim mövqeni əldən verməmək üçün bu dövlətlər daima "zəif" dövlətlərə "təzyiq göstərməyə" cəhd edirlər [22, s.67-74].

7. Kibermüharibə (Cyberwar). Sonuncu təsnifat olan kibermüharibə müasir dövrümüzün ən aktual probleminə çevrilmişdir. Xüsusilə, informasiya

terrorizmi təhlükəli xarakteri ilə fərqlənir. Məlum olduğu kimi, bütün dövlətlər elektron dövlət quruculuğuna keçdiyi üçün bütün informasiyalar informasiya sistemlərində yerləşdirilir. Artıq hər hansı bir dövlətin informasiya sahəsinə "hücum" etməklə, həmin dövləti yalnız siyasi, hərbi deyil, həmçinin iqtisadi, sosial və digər istiqamətlərdə də "iflic" etmək olar. Qeyd etmək lazımdır ki, tədricən dünya üzrə virtuallaşmanın sürətlənməsi insanları bir çox real varlıqlardan uzaqlaşdırır və bu da simulyasiya müharibələrinin formalaşmasını şərtləndirmişdir. Belə müharibələrdə real döyüş meydanındakı hərbi əməliyyatlar kompüter modeli ilə əvəz olunur. Hadisələrin gedişatına əsasən israrla deyə bilərik ki, yaxın gələcəkdə simulyasiya müharibəsi real müharibə ilə eyni məna kəsb edəcəkdir. Bütün bunlar həqiqətən də real müharibədən qat-qat təhlükəlidir. Hesab edirik ki, 2003-cü ildə yaradılan və virtual aləm kimi bir milyondan çox aktiv istifadəçisi olan "Second life" mövqeyimizi əsaslandırmaq üçün bariz nümunə kimi götürülə bilər. İnsanları tədricən real aləmdən uzaqlaşdıran bu şəbəkə "güclü" dövlətlər üçün "zəif" dövlətlərə asan və operativ psixoloji təsir vasitəsi rolunu oynaya bilər. Eyni zamanda, bu məsələ ilə bağlı müxtəlif virtual oyunların təsiri də az deyil. Məsələn, son dövrlərdə geniş yayılmış "Mavi balina" oyununun nə qədər intihar faktlarına səbəb olması göz qabağındadır. Bütün bunlar bir daha göstərir ki, "informasiya müharibəsi" nəzəri anlayış olmaqdan daha çox, təcrübi istiqamətdə təhlil olunmalı, onunla mübarizə tədbirləri yalnız beynəlxalq deyil, milli səviyyədə də aparılmalıdır. Hal-hazırda dövlətlər öz informasiya sistemlərinin məxfiliyini elektron vasitələrlə yetərincə qorumağa nail olurlar və bu da siyasi, hərbi və iqtisadi sahədə törədilən kiberhücumların sayını azaltmışdır. Lakin psixoloji hücumların necə təhlükəli olması və daha ağır nəticələrə gətirib çıxarması Dünya ictimaiyyətinin diqqətindən bir qədər kənarda qalmışdır. Hesab edirik ki, belə psixoloji hücumlar xalqların mənəviyyatının pozulması nəticəsində sonda bütün sahələrə (hərbi, siyasi, iqtisadi) öz mənfi təsirini göstərə bilər. Bu istiqamətdə respublikamızda aparılan işləri təqdirəlayiq hal kimi qiymətləndirmək lazımdır. Elektron Təhlükəsizlik Mərkəzinin gördüyü işlər vətəndaşlarda psixoloji təsir vasitələrindən qorunmaq üçün "immunitet" formalaşdırmış olur.

Kibertəhlükələrlə pozulan insan hüquqlarının müdafiəsi

Müasir cəmiyyətdə məlumatların yayılması, ötürülməsində başlıca vasitəyə çevrilmiş kiberməkanda şəxsi toxunulmazlıq hüquqlarının pozulmasına və şəxsi həyata dair məlumatların qeyri-qanuni üsullarla və qeyri-qanuni məqsədlər üçün istifadəsinə də az rast gəlinmir. Ona görə də bu problemin həlli dünya ictimaiyyətinin qarşısında dayanan vacib məsələlərdən biridir.

Kiberməkanda şəxsi toxunulmazlığın qorunması problemi hələ XIX əsrin sonlarından ABŞ-da irəli sürülməyə başlanmışdı. Belə ki, 1890-cı ildə Harvard Hüquq İcmalında dərc olunan Samuel Uorren (1852-1910) və Luis Brendaysın (1856-1941) dərc etdirdiyi "Şəxsi həyatın toxunulmazlığı" adlı məqalədə şəxsi

həyata dair bir çox vacib məqamlar öz əksini tapmışdır. Məqalədə deyilir: "Şəxsi həyatın və mülkiyyətin toxunulmazlığı əslində əvvəlki dövrlərdən ümumi hüquqda tanınmışdır. Belə ki, əvvəllər qanun (hüquq) daha çox fiziki müdaxilələrin qarşısının alınması vasitələrini nəzərdə tuturdu və "vi et armis" (silahın gücü ilə) prinsipi rəhbər tutulurdu. Lakin tədricən baş verən sosial, siyasi və iqtisadi dəyişikliklər insanın intellektinin ön plana çəkilməsinə və nəticə etibarilə, şəxsi həyatın və mülkiyyətin toxunulmazlığı kimi hüquqların əhatə dairəsinin genişlənməsinə gətirib çıxardı. Bununla da, şəxsi toxunulmazlıq hüququ bir sıra imtiyazları ehtiva etməyə başladı və artıq mülkiyyət toxunulmazlığı yalnız maddi deyil, həmçinin qeyri-maddi formada sahibliyi əhatə etdi... [27, s.193-220]"

Deməli, artıq əvvəllər olduğu kimi, şəxsi həyatın toxunulmazlığı məsələsi hər hansı bədən xəsarətləri ilə bağlı meydana gəlmirdi və intellekt, informasiya özü şəxsi həyatın toxunulmazlığında əsas element kimi qiymətləndirilirdi. Bununla yanaşı, şəxsi toxunulmazlığın insanın fiziki bədənindən asılı olmayaraq müəyyənləşdirilməsi insanın ailə münasibətlərini şəxsi həyatın toxunulmazlığı konsepsiyasının bir hissəsinə çevirdi. S.Uorren və L.Brendaysın öz məqaləsini yazmaqda əsas məqsədi məhz belə bir yeni şəraitdə şəxsi həyatın toxunulmazlığı, təhqir, böhtan və s. bu kimi məsələlərin qanunla necə tənzimlənməsini və təcrübi tərəfləri təhlil etməkdən ibarət idi. Məqalənin maraqlı tərəfi ondadır ki, müəlliflər bir çox Roma hüququnun prinsiplərinə (postulatlarına) müraciət edirlər. Məsələn, "damnum absque injuria"[9] prinsipini rəhbər tutan tədqiqatçılar xüsusi vurğulayırlar ki, hətta formal olaraq qanuni və leqal görünən hər hansı bir hərəkət insanın şəxsi həyatına qəsd edə bilər.

Müəlliflər Prins Albert v. Strencin və Vilsonun məhkəmə işlərini misal göstərərək, Lord Kottenhamın "III Georginin xəstəliyi zamanı onun ətrafında olmuş həkimlərin öz gündəliklərindəki qeydləri çap etməyin düzgün olmadığı" iddiasını xüsusi qeyd edirlər [11].

S.Uorren və L.Brendays öz məqaləsində həmçinin şəxsi toxunulmazlıq hüququnun Fransa qanunvericiliyində əks olunan tərəflərinə də nəzər salırlar: şəxsi toxunulmazlıq hüququ dövlət və ictimai maraq kəsb edən hər hansı bir məsələ üzrə nəşri qadağan etmir; şəxsi toxunulmazlıq hüququ müxtəlif formalarda kommunikasiyanı (rabitəni) qadağan etmir; şəxsi toxunulmazlıq hüququ faktın dərc olunmasına icazə verildiyi və ya onun dərc olunduğu andan başa çatmış hesab olunur və sair.

Şəxsi həyatın toxunulmazlığı problemi sonralar Uilyam Lloyd Prosserin (1898-1972) 1960-cı ildə dərc etdirdiyi məqaləsində daha geniş təhlil olunmuşdur. Belə ki, müəllif şəxsi həyatın toxunulmazlığının pozulması ilə müşayiət olunan dörd növ delikti fərqləndirirdi:

[9] **Damnum absque injuria** – latın dilindən götürülüb, delikt hüququnun prinsiplərindən biridir və şəxsə fiziki zərər yetirmədən hər hansı bir itkiyə məruz qoymanı ifadə edir.

1. Şəxsin həyatına və mənzilinə irrasional müdaxilə;
2. Şəxsi məlumatların açıqlanması;
3. Şəxs haqqında məlumatların təhrif olunması, yəni yalan məlumatların yayılması;
4. Şəxsin adı, soyadı və portretinin gəlir əldə etmək məqsədilə qanunsuz əldə olunması və ya istifadəsi [30, s.389].

Göründüyü kimi, ilkin olaraq, gənc tədqiqatçılar tərəfindən irəli sürülmüş şəxsi həyatın toxunulmazlığı hüququ müasir dünyada fundamental insan hüquqlarından biri kimi həm beynəlxalq səviyyədə, həm də ayrı-ayrı dövlətlərin milli hüququnda tanınmışdır.

Hal-hazırda Azərbaycan Respublikasında fərdi məlumatların qorunması sahəsində həm hüquqi istiqamətdə, həm də təcrübi baxımdan böyük uğur əldə olunmuşdur. Hüquqi baza barəsində fərdi məlumatların təhlili zamanı yetərincə məlumat verilmişdir. O ki qaldı təcrübi tərəflərə, ölkə daxilində elektronlaşdırma proseslərinin sürətlə həyata keçirilməsi, elektron imzanın tətbiqi və digər müxtəlif kriptoqrafik üsullardan istifadə hal-hazırda şəxsi həyatın toxunulmazlığı hüququna müdaxilələrin sayını xeyli aşağı salmışdır.

Şəxsi toxunulmazlıq hüququndan fərqli olaraq, əqli mülkiyyət hüquqlarının virtual məkanda müdafiəsində çoxsaylı ziddiyyətlər mövcuddur. Kibermə-kanda əqli mülkiyyət hüquqlarının qorunması ilə bağlı ən başlıca problem ondan irəli gəlir ki, İnternetin açıqlığı, yəni məlumatların asan əldə edilməsi əqli mülkiyyət hüquqlarının pozulması hallarını daha da artırır. Hətta, müəlliflər bu cür ziddiyyəti "İnternet - Copyright" konflikti kimi adlandırırlar [13, s.197-213].

İnternetdə əqli mülkiyyət hüquqlarının qorunmasına dair iki yanaşma mövcuddur. Birinci yanaşmaya görə, İnternetdə əqli mülkiyyət hüquqlarının qorunmasına ehtiyac yoxdur, bu İnternetin inkişafına mane ola bilər. Ən yaxşı halda şəxsin qeyri-əmlak hüquqlarının tanınması kifayət edir. İkinci yanaşma isə əksinə, İnternetdə əqli mülkiyyət hüquqlarının qorunmasını zəruri sayır, bu məqsədlə "hüquqların kollektiv idarə edilməsi" üsulunu təklif edir. Bu üsul o vaxt tətbiq edilir ki, müəlliflik və əlaqəli hüquqların fərdi qaydada müdafiəsi çətin olur. Belə halda əqli mülkiyyətin obyektlərindən istifadə olunur, əvəzində hüquq sahiblərinə müəyyən olunmuş qaydada haqq ödənilir [12, s.238-252].

Kibermə̇kanda əqli mülkiyyət hüquqlarının qorunması ilə bağlı YUNESKO-nun fəaliyyəti xüsusi qeyd olunmalıdır. 2006-cı ilin yanvarında təşkilat "Rəqəmsal əsrdə hüquq və cəmiyyət" tədqiqat layihəsinə start verdi. Layihənin əsas məqsədi əqli mülkiyyət sahibləri və istifadəçilər arasında kompromisin əldə olunması idi. İlkin fəaliyyət rəqəmsal formada ifadə olunan əqli mülkiyyət obyektlərinə dair hüquqlarla bağlı sorğunun keçirilməsi ilə başlandı. Sorğunun nəticələrinə əsasən, bir çox maraqlı faktlar üzə çıxarıldı. Məsələn, sorğuda iştirak edən hüquq sahiblərinin 51%-i hesab edirdi ki, piratçılığın artmasında əsas səbəb qismində yalnız qanunvericilikdəki boşluqlar deyil, həmçinin istehlakçıların hüquq düşüncəsinin aşağı səviyyədə olması çıxış edir. Həmçinin

başqa bir misal: İstifadəçilərin 46%-i və hüquq sahiblərinin 44%-i qeyri-kommersiya məqsədləri üçün pirat məhsulların yayılmasının ümumiyyətlə cəzaya məruz qalmamasının tərəfdarı kimi çıxış edirdilər. Əksinə kommersiya məqsədilə pirat məhsul istehsalına görə daha sərt cəzalar müəyyən olunmasını zəruri sayırdılar [7, s.9-12].

Kiberməkan informasiyanın dövr etdiyi bir məkan olduğu üçün burada ifadə azadlığından sui-istifadə halları da insan hüquq və azadlıqlarına qəsd edir. Belə ki, sırf ifadə azadlığının realizə olunması ilə törədilən cinayətləri şərti olaraq iki qrupda ayırmaq olar:

1. Kiberməkandan cinayətin törədilməsi vasitəsi kimi istifadə olunan, müxtəlif obyektə - ictimai münasibətlərə qəsd edən cinayətlər. Məsələn, təcavüzkar müharibəni başlamağa açıq çağırışlar (Cinayət Məcəlləsinin 101-ci maddəsi) sülh və insanlıq əleyhinə cinayətlərə, milli, irqi, sosial və ya dini nifrət və düşmənçiliyin salınması isə (Cinayət Məcəlləsinin 283-cü maddəsi) dövlətin konstitusiya quruluşunun əsasları və təhlükəsizliyi əleyhinə olan cinayətlərə daxildir. Lakin hər iki cinayətin törədilməsində kütləvi informasiya vasitələrindən istifadə olunarsa, daha ağır cəza tətbiq edilir. Təbii ki, kiberməkandan istifadə edilməklə, bu cinayətlərin törədilməsi ifadə azadlığının qeyri-qanuni formada realizəsi deməkdir.

2. Hər bir halda kiberməkandan istifadə edilməklə törədilən şərəf və ləyaqətə qəsd edən cinayətlər. Bu cinayətlər fikir və söz azadlığının həm şifahi, həm də yazılı formada həyata keçirilməsi zamanı icra edilə bilər. Məsələn, təhqir (Azərbaycan Respublikası Cinayət Məcəlləsinin 148-ci maddəsi), böhtan (Azərbaycan Respublikası Cinayət Məcəlləsinin 147-ci maddəsi) və Azərbaycan dövlətinin başçısının - Azərbaycan Respublikası Prezidentinin şərəf və ləyaqətini ləkələmə və ya alçaltma (Azərbaycan Respublikası Cinayət Məcəlləsinin 323-cü maddəsi) cinayətləri.

İfadə azadlığından kiberməkanda sui-istifadə halları son illərdə ***nifrət nitqi*** ilə bağlı məsələləri gündəmə gətirmişdir. Avropa Şurasının Nazirlər Komitəsinin Tövsiyəsinin 97(20) verdiyi anlayışa görə: "Nifrət nitqi dedikdə, irqi nifrət, ksenofobiya, anti-semitizm və ya aqressiv millətçilik və etnosentrizmlə ifadə olunan dözümsüzlük, azlıqlara, miqrantlara və immiqrant mənşəli şəxslərə ayrıseçkilik və düşmənçilik də daxil olmaqla, dözümsüzlüyə əsaslanan nifrətin digər formalarını yayan, təhrik edən, təşviq edən və ya əsaslandıran ifadənin bütün formaları başa düşülür. [24]"

Son dövrlərdə fikir və söz azadlığının normal şərtlər altında həyata keçirilməsi məqsədilə həm beynəlxalq, həm də milli səviyyədə bir sıra tədbirlər icra olunur. Belə ki, 47 ölkəni birləşdirən Avropa Şurası tərəfindən Gənclər Sektorunda 2012-2017-cü illər üzrə prioritet təşəbbüs kimi *"No Hate Speech Movement" - "Nifrət Nitqinə Yox Hərəkatı"* kampaniyası reallaşdırılmağa başlanmışdır. Bu kampaniya bərabərliyi, ləyaqəti, insan hüquqlarını, müxtəlifliyi müdafiə edir və dəstəkləyir. Kampaniyanın məqsədi gəncləri və gənclər təşkilatlarını bu cür insan haqları pozuntularını üzə çıxarmaq və belə hallara qarşı çıxış etmək

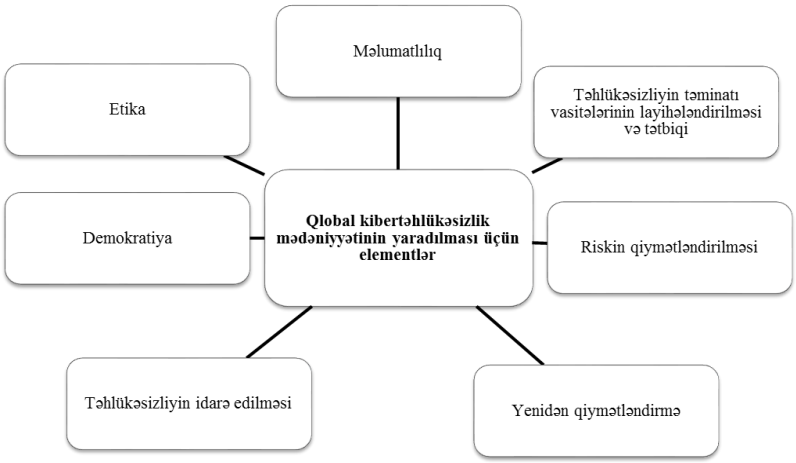
üçün zəruri bacarıqlarla təmin etməklə, irqçilik və ayrı-seçkilik məzmunlu nifrət nitqinin onlayn ifadəsinə qarşı mübarizə aparmaqdır.

Azərbaycanı Avropa Gənclər Forumunda tam hüquqlu üzv olaraq təmsil edən, Avropa Şurasının Gənclər üzrə Məşvərət Şurasının üzvü seçilmiş Azərbaycan Respublikası Gənclər Təşkilatları Milli Şurası bu kampaniyanın Azərbaycan üzrə milli əlaqələndiricisi olaraq, 2013-cü ilin may ayından etibarən "Nifrət Nitqinə Yox Hərəkatı"-na qoşulmuş və bu çərçivədə bir sıra tədbirlər həyata keçirmişdir. Bunlar sırasına Beynəlxalq Gənclər Gününə həsr edilən Gənclər Həftəsi, "Nifrət Nitqinə Yox Hərəkatı" fotosərgisi, Qəbələ rayonunda "Nifrət Nitqinə Yox Hərəkatı" Beynəlxalq Gənclər Forumu, "Nifrət Nitqinə Yox Hərəkatı" adlı beynəlxalq forumu, "Qərbdən - Şərqə Nifrət Nitqinə Yox" regional forumu və bir sıra müxtəlif tədbirlər aiddir.

Kibertəhlükələrin qarşısının alınması üzrə tədbirlər

Kibertəhlükələrin qarşısının alınması üzrə tədbirləri şərti olaraq ümumi və xüsusi tədbirlərə bölmək olar. Xüsusi tədbirlərə insanların özünün həmin təhlükələrdən qorunması üzrə aktivlik dərəcəsini daxil etmək olar. Bu mənada, informasiya təhlükəsizliyi mədəniyyətinin mövcudluğu xüsusi əhəmiyyətə malikdir.

İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması istiqamətində əsas mənbə - BMT Baş Məclisinin 20 dekabr 2002-ci il tarixli 57/239 saylı qətnaməsi ilə təsdiq edilmiş ***"Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması"*** və ona əlavə olan ***"Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər"***dir. Qlobal kibertəhlükəsizlik mədəniyyəti bütün iştirakçılardan - informasiya sistemləri və şəbəkələrini yaradan, onlara sahib olan, idarə edən, xidmət edən və istifadə edən dövlət orqanlarından, müəssisələrdən və digər təşkilatlardan, fərdi istifadəçilərdən bir-birini tamamlayan aşağıdakı doqquz elementə əməl etmələrini tələb edəcək:



"Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər"ə görə, iştirakçılar informasiya sistemlərinin və şəbəkələrin təhlükəsizliyinin zəruriliyi haqqında və təhlükəsizliyin yüksəldilməsi üçün onların nə edə biləcəkləri barədə məlumatlı olmalıdırlar, eləcə də onlar informasiya sistemlərinin və şəbəkələrin təhlükəsizliyi üçün öz rollarına uyğun olaraq cavabdehlik daşıyırlar. İştirakçılar təhlükəsizliyə aid insidentlərin qarşısının alınması, onların aşkarlanması və onlara cavab verilməsi üzrə vaxtında və birgə tədbirlər görməlidirlər. Onlar lazımi hallarda təhdidlər və boşluq faktorları haqqında məlumat mübadiləsi etməli və belə insidentlərin qarşısının alınması, onların aşkarlanması və onlara cavab verilməsi işində operativ və səmərəli əməkdaşlığı nəzərdə tutan prosedurlar tətbiq etməlidirlər. Bu transsərhəd informasiya mübadiləsini və əməkdaşlığı nəzərdə tuta bilər. Təhlükəsizlik elə təmin edilməlidir ki, bu fikir və ideyaların mübadiləsinin sərbəstliyi, azad informasiya axını, informasiya və kommunikasiyanın konfidensiallığı, şəxsi xarakterli informasiyanın lazımi şəkildə qorunması, açıqlıq və aşkarlıq daxil olmaqla demokratik cəmiyyətdə qəbul edilən dəyərlərə uyğun olsun [8].

Göründüyü kimi, "Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər" yalnız istifadəçilər üçün deyil, konkret dövlətlər üçün bir sıra vəzifələr müəyyənləşdirir. Bu da informasiya təhlükəsizliyi mədəniyyətinin dövlətin marağında olan problem olmasını bir daha təsdiq edir. Məhz ona görə də Azərbaycan Respublikası Prezidentinin 6 dekabr 2016-cı il tarixli Fərmanı ilə təsdiq edilmiş "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"ndə informasiya təhlükəsizliyi üzrə ümummilli hazırlıq və maarifləndirmə səviyyəsinin artırılması strateji məqsədlər sırasında əks olunmuşdur. Milli strategiyalarda isə informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi belə maarifləndirmə işi üzrə gözlənilən nəticələrdən biri kimi nəzərdə tutulmuşdur.

Kibertəhlükələrin qarşısının alınması üzrə ümumi tədbirlər isə dövlət tərəfindən həyata keçirilir. Birinci növbədə, müxtəlif pozuntulara görə məsuliyyətin müəyyən olunması və sanksiyaların təyin edilməsi qeyd olunmalıdır. Ənənəvi olaraq, hüquq pozuntularının xarakterindən asılı olaraq dörd növ - cinayət, inzibati, mülki və intizam məsuliyyəti fərqləndirilir. Lakin müasir dövrdə beynəlxalq-hüquqi məsuliyyət, konstitusiya-hüquqi məsuliyyət kimi anlayışlara da rast gəlinir. Bəs informasiya hüquqi məsuliyyət hansı növə aiddir və necə tənzimlənir? - Məsələ burasındadır ki, informasiya sahəsində münasibətlərin realizəsi zamanı törədilən hüquq pozuntularına görə sanksiyalar informasiya qanunvericilik aktlarında təsbit olunmamışdır. İctimai təhlükəli olan informasiya-hüquq pozuntuları cinayət qanunvericiliyində, inzibati xətanın əlamətləri ilə səciyyələnən pozuntular inzibati qanunvericilikdə, müxtəlif deliktlər mülki qanunvericilikdə nəzərdə tutulmuşdur və s. Belə olan halda, informasiya-hüquqi məsuliyyətin ayrıca bir institut kimi fərqləndirilməsinə ehtiyac varmı? - Leqal aspektdən yanaşsaq, xeyr. Lakin informasiya sahəsinin sərhədsiz olmasını, informasiya-

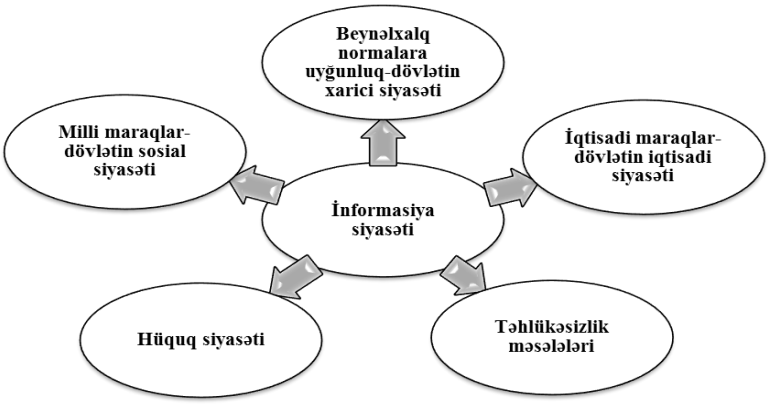
hüquq pozuntuları ilə bağlı problemlərin və kolliziyaların mövcudluğunu nəzərə alsaq, həmin problemlərin cinayət, mülki və inzibati hüquq sahələri üzrə şərhi mümkün deyil. Məsələn, kibertəhlükələr, informasiya təhdidləri nəinki konkret vətəndaşa qarşı yönəlir, hətta böyük bir xalqın mənəviyyatına mənfi təsir göstərir. Belə təhlükələrin qarşısının alınması üzrə təklif və tövsiyələrin işlənməsi isə yalnız informasiya hüquq elmi çərçivəsində mümkün ola bilər. Bütün bunları rəhbər tutaraq, informasiya-hüquqi məsuliyyətin müstəqil bir hüquqi institut kimi təhlilini məqsədyönlü hesab edirik.

Digər bir ümumi tədbirlər planı milli informasiya siyasətinin istiqamətləri sırasında informasiya təhlükəsizliyinin təminatı qeyd olunmalıdır. YUNESKO-nun İnformasiya hamı üçün (İnformation for All) Proqramı Milli İnformasiya Cəmiyyəti Siyasətində (MİCS) beş prioritet müəyyənləşdirir: İnformasiya inkişaf üçün; İnformasiya mədəniyyəti; İnformasiyanın saxlanması; İnformasiya etikası; İnformasiya əlyetərliyi [23].

Göründüyü kimi, milli informasiya siyasəti bütövlükdə cəmiyyət üçün informasiyanın əlyetərliyinin təminatına yönəlmiş tədbirlər və qaydalar sistemini özündə birləşdirir. Həll onunan məsələlərin xarakterindən asılı olaraq informasiya siyasəti 2 yerə bölünür: ***informasiya strategiyası*** **və** ***informasiya taktikası.*** ***İnformasiya strategiyası*** böyükhəcmli informasiya problemlərinin həllinə yönəlmiş planlı fəaliyyət modelidir ki, bu model nəticə etibarilə informasiyalaşdırma proseslərinin uğurla başa çatmasına və informasiya hüquq və azadlıqlarının maneəsiz təminatına yönəlmişdir. ***İnformasiya taktikası*** isə informasiya strategiyasının əsasında formalaşır, qarşıya qoyulan məqsəd və vəzifələrə çatmaq üçün icra olunan konkret tədbirləri əhatə edir. Bu o deməkdir ki, informasiya strategiyası "nə" və "niyə" suallarını cavablandırırsa, informasiya taktikası "necə" sualına cavab verir. Strategiyadan fərqli olaraq, informasiya taktikası çevikliyi ilə xarakterizə olunur. Məsələn, Azərbaycan Respublikası Prezidentinin 17 fevral 2003-cü il tarixli 1146 nömrəli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003-2012-ci illər)"nın icrası məqsədilə bir sıra dövlət proqramları - "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan)" və s. qəbul edilmişdir ki, bu proqramlar dövlətin informasiya taktikasını əks etdirir.

Milli informasiya siyasətinin həyata keçirilməsi dövlətin fəaliyyətinin digər aspektləri nəzərə alınmadan qeyri-mümkündür. Belə ki, iqtisadi baxımdan səmərəsiz bir şəraitdə informasiyalaşdırma və elektronlaşdırma proseslərindən, informasiya əlyetərliyinin təminatından danışmaq bir qədər məntiqsiz olar. Digər tərəfdən milli maraqları nəzərə almayan informasiya siyasəti uğurla icra oluna bilməz. Həmçinin beynəlxalq normalara riayət etmədən həyata keçirilən və hüquqi bazası olmayan informasiya siyasəti nəticədə maraqların toqquşmasına gətirib çıxaracaqdır. Başqa bir tərəf onda özünü büruzə verir ki, milli

təhlükəsizlik qorunmadığı bir şəraitdə informasiya siyasətinin normal icrasına nail olmaq mümkünsüzdür. Təsadüfi deyil ki, "Milli təhlükəsizlik haqqında" 29 iyun 2004-cü il tarixli Azərbaycan Respublikası Qanununda informasiya sahəsində milli təhlükəsizliyin təmin olunması ayrıca bir sahə kimi nəzərdə tutulmuşdur: "Azərbaycan Respublikasının milli təhlükəsizliyi siyasi, iqtisadi, hərbi, sosial, informasiya, ekologiya, elm, mədəniyyət, mənəviyyat və digər sahələr üzrə təmin olunur" (maddə 15.1). Ona görə də dövlətin informasiya siyasəti beynəlxalq və milli maraqlar nəzərə alınmaqla, milli təhlükəsizlik təmin olunmaqla, iqtisadi və hüquqi tədbirlərlə qarşılıqlı əlaqəli formada həyata keçirilir:



Yuxarıdakı sxemdən açıq-aydın görünür ki, milli informasiya siyasəti dedikdə, dövlət orqanları tərəfindən həyata keçirilən kompleks tədbirlər sistemi başa düşülür. Belə bir sual ortaya çıxır: Milli informasiya siyasətinin yalnız dövlət hakimiyyət orqanlarında çəmləşməsi insan hüquq və azadlıqlarının məhdudlaşdırılması anlamına gətirə bilərmi? - Xeyr. Əslində, hüquq və azadlıqların təminatı, hüquq pozuntularının qarşısının alınması və s. bu kimi vəzifələrin icrası üçün dövlət hər bir zaman idarəedici təsisat olaraq mövcud olmuşdur. Hüquqi dövlət ideyasının geniş vüsət aldığı bir dövrdə dövlətin rolu olmadan qarşıya qoyulan məqsədlərə nail olmaq mümkün deyil. Təbii ki, dövlət orqanlarının özünün də fəaliyyətinə nəzarət olunması vacib faktorlardan sayılır. Məhz ona görə də hüquqi dövlətin əsas prinsiplərindən biri kimi "qarşılıqlı məsuliyyət, yəni şəxsin dövlət qarşısında və dövlətin şəxs qarşısında məsuliyyəti" hər zaman rəhbər tutulur. Bununla yanaşı, açıq hökumət, ictimai nəzarət, vətəndaş cəmiyyəti və digər ideyaların ön plana çəkilməsi dövlətin milli informasiya siyasətinin həyata keçirilməsinə mühüm təsirini göstərir.

Nəticə

Cəmiyyətin bütün sferalarının qloballaşması, kiberməkanın formalaşması qanuna riayət edən vətəndaşlarla yanaşı, hüquq pozucuları üçün də asan üsullarla pozuntuların törədilməsi üçün imkanlar açır. Müasir dövrün ən aktual

problemlərindən olan "kibertəhlükələr"lə mübarizə dünya miqyasında aparılır. Sərhədləri bilinməyən bir məkanda cinayətkarın axtarılması son dərəcə çətin olduğu üçün həm milli səviyyədə, həm də beynəlxalq səviyyədə kibermühitdə törədilən cinayətlərə "həssaslıqla" yanaşılmalıdır. Hətta, onu deyə bilərik ki, kibercinayətlər ənənəvi üsulla törədilən cinayətlə müqayisədə daha ağır nəticələrə səbəb ola bilir. Bu baxımdan, kibertəhlükələrin qarşısının alınması üzrə məkdaşlıq prinsipi rəhbər tutulmalıdır. Bu, iki isitqamətdə aparılsa, daha operativ nəticələr əldə etmək olar: dövlətlərin əməkdaşlığı - beynəlxalq səviyyədə və vətəndaşla dövlət orqanlarının əməkdaşlığı - milli səviyyədə.

İKT-nin sürətlə inkişaf etdiyi bir dövrdə ənənəvi cinayətlərin də İKT-dən isitfadə edilməklə törədilməsinə daha çox üstünlük verilir. Bu günkü dövrdə şəxsin üzərinə silah çəkməklə pulunu almağa gərək yoxdur, texnologiyanın köməyilə daha asan yollarla (bank dələduzluğu və s.) varlanmaq olur. Hətta, məsafədən virtual aləmdə insanı öünü öldürməyə məcbur etmək belə mümkündür. Ona görə də kibertəhükələrlə bağlı hüquqi mənbələrdə "kibercinayət" anlayışına yenidən baxılmasını məqsədəmüvafiq hesab edirik. Bu zaman nəzəri ədəbiyyatda kibercinayətlərin müxtəlif təsnifatlarından istifadə etmək olar.

Beləliklə, kiberməkanda insan hüquqlarının təminatı və müdafiəsi üçün informasiya ekologiyasının aradan qaldırılması, informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması və inkişaf etdirilməsi, fərdi məlumatların mühafizəsi üzrə tədbirlərin gücləndirilməsi, kibermühitin insan psixologiyasına mənfi təsir üsullarının aradan qaldırılması və s. bu kimi tədbirlər planlaşdırılmalı və icra olunmalıdır.

İstinadlar:

1. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: Nurlar, 2019, 448 s.

2. İnformasiya təhlükəsizliyi və ona qarşı yönəlmiş hücumlar. // Elektron Təhlükəsizlik Mərkəzinin rəsmi saytı. https://www.cert.az/news/2016/informasiya-tehlukesizliyi-ve-ona-qarsi-yonelmis-hucumlar

3. К вопросу о латентности киберпреступлений. https://infourok.ru/statya-k-voprosu-latentnosti-kiberprestupleniy-1460496.html

4. Платошин Ю.А.Сущность латентной преступности. // Право и образование, 2011, №5, с. 171-176

5. Рассолов И.М. Право и Интернет: Теоретические проблемы. Москва: Норма, 2009, 383 с.

6. Телешина Н.Н. Виртуальная пространства как новая юридическая конструкция: к постановке проблемы. // Юридическая техника, 2013, №7 (Ч.2), с.740-747.

7. Туликов А. Интеллектуальная собственность в киберпространстве: правообладатели и общество готовы к диалогу. // Интеллектуальная собственность в киберпространстве: Сборник аналитических материалов проекта "Право и общество в цифровую эпоху". МОО ВПП ЮНЕСКО "Информация для всех". Составитель: Евгений Альтовский, 2006, с. 9-12.

8. Creation of a global culture of cybersecurity: resolution / United Nations General Assembly (UNGA) Resolution 57/239, 31 January 2003. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unga-creation-global-culture-cybersecurity

9. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. // Michigan Telecommunications and Technology Law Review, 1998, Volume 4, Issue 1, p. 69-103.

10. Debra Littlejohn Shinder. Scene of the Cybercrime: Computer Forensics Handbook. Canada: Syngress Publishing, Inc., 2002, 749 p.

11. Dorothy J. Glancy. The invention of the right to privacy. // Arizona Law Review, 1979, Volume 21 (1), http://law.scu.edu/wp-content/uploads/Privacy.pdf

12. Dutfield G. Global intellectual property law: commentary and materials / Graham Dutfield [and others]. Northampton, MA: Edward Elgar Pub., 2005, pp. 238-252.

13. Fiordalisi E. The Tangled Web: Cross-Border Conflicts of Copyright Law in the Age of Internet Sharing. // Loyola University Chicago International Law Review, 2015, Vol. 12, İssue 2, pp. 197-213.

14. Gibson W. Burning chrome. Canada, 1982. http://project.cyberpunk.ru/lib/burning_chrome/

15. Gibson W. Neuromancer. First edition, 1984, 271 p.

16. http://virtualaz.org/

17. http://www.dictionary.com/browse/virtual-environment

18. http://www.virtualkarabakh.az/index.php?lang=3

19. https://www.eff.org/cyberspace-independence

20. Human Rights in the Global Information Society (Information Revolution and Global Politics). Edited by Rikke Frank Jorgensen, London: The MIT Press Cambridge, Massachusets, 2006, 323 p.

21. John Arquilla and David Ronfeldt. Cyberwar is coming! // National Security Research Division. https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

22. Martin C. Libicki. What Is Information Warfare? Washington, 1995, 104 p.

23. National information society policy: A template. Developed by The Information For All Programme of UNESCO. Paris November 2009, 143 p.

24. Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech". / Adopted on 30 October 1997 by Committee of Ministers of Council of Europe. https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-97-20-of-the-committee-of-ministers-to-member-states-on-hate-speech-?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/

25. Recommendations of the Electronic Security Center for the prevention and elimination of the consequences of information security incidents. // Electronic Security Center, 2014. https://www.cert.az/s/u/document/tovsiye.pdf,

26. Richard R. Bartle. Designing Virtual Worlds. New Riders, 2003, 741 p.

27. Samuel D. Warren, Louis D. Brandeis. The Right to Privacy. // Harvard Law Review, 1890, Vol. 4, No. 5, p. 193-220.

28. Understanding Cybercrime: A Guide For Developing Countries. ICT Applications and Cybersecurity Division Policies and Strategies Department, ITU Telecommunication Development Sector Draft April 2009, 225 p.

29. W.Lambert Gardiner. Virtual Reality/Cyberspace: Challenges to Communication Studies//Canadian Journal of Communication, 1993, Vol 18 (3). http://www.cjc-online.ca/index.php/journal/article/view/762/668

30. William L.Prosser. Privacy. // California Law Review, 1960, Volume 48 (3), p. 383-423.

КИБЕР УГРОЗЫ И ЗАЩИТА ПРАВ ЧЕЛОВЕКА В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ: МЕЖДУНАРОДНОЕ И НАЦИОНАЛЬНОЕ ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Айтекин Ибрагимова[*], Гюльназ Рзаева[**]

Резюме

Изменение и развитие мировоззрения в современном обществе также оказывает влияние на незаконное поведение. Поскольку традиционные методы не соответствуют требованиям времени, ИКТ все чаще используются в качестве нового метода и инструмента для нарушения прав человека и совершения различных преступлений. Это также требует усиления борьбы с киберпреступностью. В статье проводится сравнительный анализ легальной и нелегальной классификаций киберугроз, а также предлагаются предложения и рекомендации по развитию механизмов защиты прав человека, нарушаемых киберпреступностью в киберпространстве.

Ключевые слова: *глобальное информационное общество, киберпространство, киберугроза, киберпреступность, кибервойна, свобода выражения мнений, право на неприкосновенность частной жизни, информационная политика.*

CYBER THREATS AND PROTECTION OF HUMAN RIGHTS IN VIRTUAL SPACE: INTERNATIONAL AND NATIONAL LEGAL REGULATION

Aytekin Ibrahimova[*], Gulnaz Rzayeva[**]

Abstract

Changing and developing world outlook in modern society also has an impact on illegal behavior. As traditional methods do not meet the requirements of the time, ICTs are increasingly being used as a new method and tool for violating human rights and committing different offences. This also requires strengthening the fight against cybercrimes. In the article were analyzed in detail the legal and illegal classifications of cyber threats, were put forward suggestions and recommendations for the development of human rights protection mechanisms that have been violated by cybercrimes in cyberspace.

Keywords: *global information society, cyberspace, cyberthreat cybercrime, cyber war, freedom of expression, right to personal privacy, information policy.*

[*] Доктор философии по праву, заместитель декана юридического факультета Бакинского государственного университета, преподаватель кафедры конституционного права.

[**] Доктор философии по праву, преподаватель кафедры прав человека и информационного права ЮНЕСКО юридического факультета Бакинского государственного университета, преподаватель Академии Государственного таможенного комитета Азербайджанской Республики

[*] Doctor of Philosophy in Law, Deputy Dean of the Faculty of Law of Baku State University, Teacher of the Department of Constitutional Law

[**] Doctor of Philosophy in Law, Teacher of the UNESCO Department of Human Rights and Information Law, Faculty of Law, Baku State University, Lecturer of the Academy of the State Customs Committee of the Republic of Azerbaijan