İnformasiya təhlükəsizliyi, hüquqi əsasları, müqayisəli yanaşma

Xalid Niyazov
AMEA Hüquq və İnsan Haqları İnstitu, Bakı, Azərbaycan
xalid-555@mail.ru

***Xülasə*— Dünya ölkələrinin təcrübəsində də informasiyanın müdafiəsi haqqında ilk qanunlar dövlət sirrinin müdafiəsi haqqında qanunlar olmuşdur. Informasiya təhlükəsizliyinin hüquqi cəhətdən təmin olunması sahəsində vacib məsələlərdən biri kimi şəxsi məlumatların müdafiəsi çıxış edir. Fransa, İtaliya, İspaniya, Portuqaliya, Danimarka, Hollandiya və s. ölkələrdə hər kəsin hakimiyyət orqanlarının fəaliyyəti ilə bağlı informasiya ilə, ABŞ, Kanada, Avstraliya və Yeni Zelandiyada isə vətəndaşların birbaşa idarəetmə məlumatları ilə tanış olma imkanını təmin edən qanunlar qəbul edilmişdir. İnformasiya təhlükəsizliyinin təmin olunması istiqamətində zəruri tədbirlərin həyata keçirilməsi üçün beynəlxalq hüquqi mexanizmlərin, milli normativ-hüquqi bazanın formalaşdırılması mühüm əhəmiyyət daşıyır və bu məsələ ayrı-ayrı ölkələr kontekstində deyil, beynəlxalq qlobal informasiya təhlükəsizliyi kontekstində nəzərdən keçirilməlidir. Azərbaycan Respublikası informasiya təhlükəsizliyi sahəsində MDB dövlətləri ilə sıx beynəlxalq əməkdaşlıq tədbirlərini həyata keçirir. Müasir inkişaf meylləri və tendensiyaları onu deməyə əsas verir ki, informasiya təhlükəsizliyinin milli təhlükəsizliyin təmin edilməsi sistemində yeri və rolu gələcəkdə daha da artacaqdır.**

Açar sözlər*— *milli təhlükəsizlik, informasiya təhlükəsizliyi, informasiya hüququ, informasiya cəmiyyəti, informasiya qanunvericiliyi, kompyuter texnologiyaları, informasiya məkanı

I. GİRİŞ

Bəşəriyyətin keçib gəldiyi bir yol var və həmin yolu müşahidə edərkən görürük ki, təbii-elmi mədəniyyətin nailiyyətləri bir qayda olaraq humanitar mədəniyyət üçün problemlər yaradıb. Burada elə bir sirr yoxdur da... yüksək insan zəkasının məhsulu sayılan texnika onun imkan və qabiliyyətini gücləndirməklə yanaşı həm də hüquqa, belə deyək, meydan oxuyub. Belə ki, informasiya fenomeninin şəxsiyyət-cəmiyyət- dövlət üçbucağının rifahına xidməti ilə yanaşı, dağıdıcı effekti də məlumdur. İki mədəniyyətin vəhdət və mübarizəsi bəşəriyyətin keçid mərhələsində – insanın energetika sektorundakı fiziki imkanlarının informasiya sahəsindəki zəka qabiliyyətinə transformasiyası prosesində daha da güclənir. Belə bir keyfiyyət sıçrayışı nəticə etibarilə cəmiyyətdə qüvvələr palitrasını dəyişir; postsənaye cəmiyyətini informasiya cəmiyyəti əvəz edir, cəmiyyətdə hökmran sosial qrup, həqiqi güc və söz sahibi qismində artıq bankirlər, sənaye maqnatları, oliqarxlar deyil, informasiya və nou-xau texnologiyalarının sahibləri çıxış edirlər

XX əsrin sonu XXI əsrin əvvəli bəşəriyyətin yeni bir cəmiyyətə, yeni sosiofəlsəfi düşüncə müstəvisinə, paradiqmal dəyər və meqaideyaların önə keçdiyi ictimai münasibətlər coğrafiyasına qədəm qoyduğu zaman miqyasıdır. Yeni cəmiyyət hər bir halda yeni insan tipi, transformasiyaya açıq dəyərlər sistemi və bir də mütləq çoxvektorlu ictimai münasibətlər şəbəkəsi ilə səciyyələnir.

Bu gün bir çoxları “Üçüncü dünya müharibəsi” təhlükəsindən danışır. Siyasətşünaslar, hərbi ekspertlər danışırlar. Nostradamusun, Vanqanın, Qlobanın, başqalarının öncəgörmələrində sətiraltı mənalar axtaranlar çoxalıb. Amma hamı bir ortaq fikirlə həmrəydir ki, razılaşır ki, “Üçüncü dünya müharibəsi” artıq başlayıb. Belə ki, müasir hibrid müharibə hər şeydən əvvəl elə informasiya müharibəsidir. Əgər müharibə varsa, apriori təhlükəsizlik tədbirlərləri də aktuallaşmalıdır. Fəaliyyət varsa, deməli, konkret münasibətdən danışa bilərik. Hər bir münasibət isə ilk növbədə hüquqi tənzimləmə aparatı tələb edir. Hələ tam formalaşmamış Azərbaycan informasiya hüququ sistemində informasiya təhlükəsizliyinin hüquqi nizamlanması məsələsi həm elmi-nəzəri, həm də praktiki əhəmiyyət kəsb edir.

II. MEYDAN MÜHARİBƏSİNDƏN KİBERMÜHARİBƏYƏ

Bu gün ictimai-siyasi-iqtisadi fəaliyyətin elə bir sahəsini tapmaq mümkün deyil ki, orada informasiya təhlükəsizliyi məsələsi öz aktuallığını diktə eləməsin: hərbi-müdafiə, dövlət idarəçiliyi, hüquq-mühafizə, E-hökumət, milli təhlükəsizlik, elmi, humanitar, İKT və s.

Buna görə də informasiyanın ictimai həyatdakı rolunun, iştirak və yerinin yüksəlməsi ilə sıx bağlı olan informasiya təhlükəsizliyi məsələsi də müasir cəmiyyətin qarşılaşdığı ən müstəsna problemlərdən birinə çevrilmişdir. İnformasiya təhlükəsizliyi lokal məsələ olmadığına görə onun hüquqi təminatı sahəsində sistemli iş aparılmalıdır və bu ilk növbədə beynəlxalq informasiya təhlükəsizliyinin, həmçinin milli maraqların qorunması və möhkəmləndirilməsini nəzərdə tutan beynəlxalq norma və prinsipləri diqqətə alan normativ aktların elmi əsaslandırılmasını tələb edir.

2001-ci ildə Avropa Şurası tərəfindən “Kibercinayətkarlıq haqqında” Budapeşt konvensiyası qəbul olunmuşdur. Azərbaycan Respublikası da həmin konvensiyaya qoşulub.

Kibercinayət hər hansı bir informasiya sisteminə icazəsiz və hüquqa zidd şəkildə daxil olunması və sonradan həyata keçirilən əməldir. Bu halda ixtiyari bir insan, ona məxsus əmlak, eyni zamanda istifadə olunan sistemin özü hədəf seçilə bilir. Məsələn, bir sistemə daxil olmaqla zərər vermək, bazanı, informasiya ehtiyatını silmək, şifrələmək, ələ keçirmək, yad

DOI: 10.25045/NCInfoSec.2018.04

informasiya yükləmək, sistemin iş prinsipini dayandırmaq, şəxsi həyatın toxunulmazlığını pozmaq, əlaqəni əngəlləmək, əlaqəni icazəsiz izləmək, qeydə almaq kimi hərəkət və əməllərin törədilməsi kibercinayət faktlarıdır.

Kibercinayətlərdən bəziləri özünü adi cinayət kimi büruzə verir, yəni maddi vəsaitin mənimsənilməsinə yönəlir. Məsələn, kibervasitələrlə başqalarının bank hesablarından pulun çıxarılması və oxşar istiqamətlərdə cinayət əməllərinin törədilməsi buna misaldır. Digər bir qrup da var ki, o, mövcud informasiya ehtiyatlarını sıradan çıxarmağa yönəlib. Məsələn, bəzi gənclər kompyuter sistemləri üzrə ixtisaslaşır və özlərini təsdiq etmək üçün bu və ya digər informasiya ehtiyatını sıradan çıxarmağa cəhd edir. Yəni informasiya ehtiyatlarında müəyyən boşluqlar axtarır və ondan sonra müxtəlif şəkillər, müxtəlif bəyanatlar qeyd edir və özlərini bu formada təsdiq etməyə cəhd göstərirlər. Bundan əlavə, məqsədyönlü şəkildə informasiya ehtiyatlarının sıradan çıxarılması təcrübəsi də var ki, bu, adətən mürəkkəb münasibətlərdə olan dövlətlər arasında da baş verir [1].

Elmi ədəbiyyatda internetdəki informasiya müharibəsininin kompyuter cinayətkarlığından fərqləndirilməsinin zəruriliyi vurğulanaraq göstərilir ki, istənilən kompyuter cinayəti birbaşa qanunun pozulması faktıdır. Kompyuter cinayəti təsadüfi də ola bilər, qəsdən planlaşdırılmış da, ayrıca törədilə və ya geniş hücum planının tərkib hissəsi də ola bilər. İnformasiya müharibələri isə heç vaxt təsadüf üzündən, yaxud birtərəfli şəkildə baş vermir (və əksər hallarda qanunu pozmur), istər əsil müharibə meydanında, istərsə də iqtisadiyyatda, yaxud siyasətdə döyüş əməliyyatları aparmaq üçün informasiyadan razılaşdırılmış şəkildə silah kimi istifadəni nəzərdə tutur. Informasiya mübarizəsi sırf internet vasitələrilə nadir hallarda aparılır. Bir qayda olaraq, bu mübarizədə şüurlara və mənəviyyata təsir vasitələrinin bütöv bir spektri işə salınır [2, 98].

Kompyuter cinayətkarlığı ilə mübarizəni çətinləşdirən amillərdən biri bu sahədə normativ bazanın kifayət qədər mükəmməl olmamasıdır. Bu problem əksər dünya ölkələrində mövcuddur. Respublikamızda hələ də bu sahədə çox mühüm normativ akt olan “EHM və məlumat bazaları üçün yaradılmış proqramların hüquqi mühafizəsi haqqında” qanun qəbul edilməmişdir. Bu sahədəki münasibətlər “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” 19 iyun 1998-ci il, “Müəlliflik hüququ və əlaqəli hüquqlar haqqında” 5 iyun 1996-cı il, “Dövlət sirri haqqında” 15 noyabr 1996-cı il qanunları (bir sıra digər qanunlar da dolayı yurisdiksiyaya malikdir), habelə CM-nin 271, 272 və 273-cü maddələri ilə tənzimlənir [3,15]. Beləliklə, EHM-lərin fəaliyyətini nizamlayan birbaşa qanun yoxdur.

“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun 3-cü maddəsində isə informasiyanın mühafizəsinin aşağıdakı məqsədləri müəyyən olunmuşdur:

- informasiyanın məhvinin, itməsinin, saxtalaşdırılmasının qarşısının alınması;
- dövlətin, ictimaiyyətin, vətəndaşların təhlükəsizliyinin təmin edilməsi;
- informasiyanın məhvi, modifikasiyası, surətinin çıxarılması, təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması;
- dövlət sirri təşkil edən və konfidensial informasiyanın qorunması;
- informasiya proseslərində və informasiya sistemlərinin, texnologiyalarının və onların təminat vasitələrinin işlənməsi, istehsalı, tətbiqi zamanı fiziki və hüquqi şəxslərin hüquqlarının təmin olunması [4].

Göründüyü kimi, burada dövlət sirri təşkil edən informasiyanın qorunması məqsədi xüsusi olaraq göstərilmişdir. “Dövlət sirri haqqında” Azərbaycan Respublikası Qanununda dövlət sirri dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti ilə bağlı olub, dövlət tərəfindən mühafizə edilən və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlar kimi müəyyən edilir. Bu Qanunun müddəaları Azərbaycan Respublikasının ərazisində və onun hüdudlarından kənarda Azərbaycan Respublikasının dövlət hakimiyyəti və yerli özünüidarə orqanları, təşkilati-hüquqi formasından və mülkiyyət növündən asılı olmayaraq bütün müəssisə, idarə və təşkilatları, dövlət sirri haqqında Azərbaycan Respublikası qanunvericiliyinin tələblərini yerinə yetirmək öhdəliyi götürmüş və ya statusuna görə buna borclu olan Azərbaycan Respublikasının vəzifəli şəxsləri və vətəndaşları, əcnəbilər və vətəndaşlığı olmayan şəxslər tərəfindən hökmən icra edilməlidir [5]

III. BEYNƏLXALQ TƏCRÜBƏ VƏ MİLLİ HÜQUQ MƏKANI

Dünya ölkələrinin təcrübəsində də informasiyanın müdafiəsi haqqında ilk qanunlar dövlət sirrinin müdafiəsi haqqında qanunlar olmuşdur. Dövlət sirrinin müstəsna əhəmiyyəti və onun müdafiəsi zərurəti nəzərə alınaraq bütün inkişaf etmiş dövlətlərdə xüsusi ictimai təhlükəli əməllər kimi casusluq və dövlətə xəyanət ən ağır cinayətlər sırasına aid edilmişdir.

ABŞ-ın “İnformasiya təhlükəsizliyinin idarə edilməsi haqqında” 2002-ci il tarixli Qanununda informasiya təhlükəsizliyi aşağıdakı kimi xarakterizə edilir:

- informasiyanın və informasiya sistemlərinin icazəsiz girişdən, istifadədən, açıqlamandan, yayılmadan, dəyişdirilmədən və ya məhv edilmədən müdafiəsi;
- həqiqiliyinin təminatları da daxil olmaqla, informasiyanın tamlığının qanunsuz dəyişdirilmədən və ya məhv edilmədən qorunmasının təmin edilməsi;
- şəxsi həyat və mülkiyyət haqqında məlumatların gizliliyi də daxil olmaqla, tanış olma və yayılma imkanları məhdudlaşdırılmış informasiyanın konfidensiallığının təmin olunması;
- informasiya ilə tez və etibarlı şəkildə tanış olma imkanını ifadə edən əlçatanlıq.

Informasiya təhlükəsizliyinin hüquqi cəhətdən təmin olunması sahəsində vacib məsələlərdən biri kimi şəxsi məlumatların müdafiəsi çıxış edir.Ümumdünya İnsan Hüquqları Bəyannaməsinin 12-ci maddəsinə görə, heç kim

şəxsi və ailə həyatına müdaxiləyə, evinin toxunulmazlığına, məktublaşmasının gizliliyinə, şərəf və nüfuzuna özbaşına qəsdə məruz qala bilməz. Hər bir şəxsin belə müdaxilə və qəsddən qanun tərəfindən müdafiə olunmaq hüququ var [6].

ABŞ-ın “Telekommunikasiya haqqında” (1984), “Polis haqqında” (1997), “Təqibdən müdafiə haqqında” (1997) və bir sıra digər qanunlarında da şəxsi həyatın toxunulmazlığı ilə bağlı müddəalar öz əksini tapmışdır.

Fransa, İtaliya, İspaniya, Portuqaliya, Danimarka, Hollandiya və s. ölkələrdə hər kəsin hakimiyyət orqanlarının fəaliyyəti ilə bağlı informasiya ilə, ABŞ, Kanada, Avstraliya və Yeni Zelandiyada isə vətəndaşların birbaşa idarəetmə məlumatları ilə tanış olma imkanını təmin edən qanunlar qəbul edilmişdir. İspaniya, Portuqaliya, Rumıniya, Hollandiya, Avstriya, Macarıstan, Estoniya, Belçika kimi Avropa ölkələrində vətəndaşların rəsmi informasiya ilə tanış olmaq hüququ konstitusion səviyyədə, Fransa, Yunanıstan və İtaliyada isə qanunla təsbit olunmuşdur. İsveç və Finlandiyada bu tendensiyanın əksinə olaraq rəsmi informasiya ilə tanış olmaq hüququ məhdudlaşdırılmışdır. Bolqarıstanın “Məxfi informasiyalar haqqında” 2002-ci il tarixli Qanunu istənilən məmura istənilən sənədə məxfilik qrifi tətbiq etmək imkanı verməklə geniş ictimaiyyətin informasiya ilə tanış olmaq hüququnu məhdudlaşdırır [7, 45-48].

Müasir dövrdə planetin vahid informasiya resurslarının formalaşması prosesi gedir. Yer kürəsinin bütün əhalisinin informasiyanı mənimsəməsi üçün zəmin yaranır [8, 5]. Qlobal informasiya cəmiyyəti formalaşır. Qlobal informasiya cəmiyyətinin qurulması isə qlobal informasiya təhlükəsizliyinin aktuallığını daha da artırır.

Cəmiyyətin informasiya təhlükəsizliyinin təmin olunması üçün zəruri olan tədbirlər kimi beynəlxalq hüquqi mexanizmlərin ciddi araşdırılması, milli normativ-hüquqi bazanın formalaşdırılması, təhlükəsizlik siyasətinin işlənilməsi və reallaşdırılması, xüsusi texnologiyaların tətbiqi, ölkə və korporativ səviyyədə informasiya təhlükəsizliyinin monitorinqi və menecmentinin aparılması, kadr hazırlığı, əhalinin maarifləndirilməsi və vətəndaşlarda informasiya mədəniyyətinin tərkib hissəsi kimi informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması məsələləri aktuallıq kəsb edir. Ümumiyyətlə, informasiya təhlükəsizliyinin təmin olunması istiqamətində zəruri tədbirlərin həyata keçirilməsi üçün beynəlxalq hüquqi mexanizmlərin, milli normativ-hüquqi bazanın formalaşdırılması mühüm əhəmiyyət daşıyır və bu məsələ ayrı-ayrı ölkələr kontekstində deyil, beynəlxalq qlobal informasiya təhlükəsizliyi kontekstində nəzərdən keçirilməlidir[9, 3-9].

Informasiya məkanında həyata keçirilən fəaliyyət növlərindən bəziləri dövlətlərin informasiya təhlükəsizliyinə ciddi surətdə mənfi təsir göstərə bilər. Ona görə də bu sahə həssas olmaqla, yüksək diqqət, dəqiqIilk və əməkdaşlıq tələb edir. İnformasiya- kommunikasiya sahəsini də əhatə edən qloballaşma dövründə dövlətlər arasında əlaqələrin informasiya texnologiyalarına əsaslanan infrastrukturlardan asılılığı daha çox artır. Yalnız ikitərəfli, regional və beynəlxalq səviyyədə əlaqələndirilmiş və bir-birini qarşılıqlı tamamlayan tədbirlər informasiya sahəsində müasir təhdidlərə adekvat reaksiya göstərməyə imkan verir [10, 104-106]. Lakin informasiya sahəsində beynəlxalq əməkdaşlıq sülh və təhlükəsizliyin təmin olunması, dövlətlərin suverenliyinə, daxili işlərinə müdaxilənin yolverilməzliyi və insan və vətəndaş hüquq və azadlıqlarına hörmət kimi prinsiplər əsas götürülməklə həyata keçirilməlidir. Bu əməkdaşlığın həyata keçirilməsində birgə informasiya sistemlərinin və vahid informasiya banklarının yaradılması, habelə operativ, statistik, elmi-metodiki və digər informasiyaların mübadiləsi barədə müddəaları özündə əks etdirən sazişlər xüsusi rol oynayırlar.

BMT Baş Assambleyasının 23 dekabr 1999-cu il tarixli Qətnaməsində (A/RES/54/49) göstərilir ki, müasir informasiya texnologiyalarının və vasitələrinin yayılması və istifadəsi beynəlxalq sülh və təhlükəsizliyin təmin edilməsi vəzifələrinə zidd ola bilməz. BMT BA-nın beynəlxalq informasiya təhlükəsizliyi barədə 56/19 №-li qətnaməsində göstərilir ki, İKT beynəlxalq stabillik və təhlükəsizliyin təmin edilməsi vəzifələri ilə bir araya sığmayan məqsədlərlə istifadə oluna, habelə ayrı-ayrı dövlətlərin həm mülki, həm də hərbi sahədə təhlükəsizliyini pozmamaqla, onların infrastrukturlarının bütövlüyünə mənfi təsir göstərə bilməz. Həmçinin, qeyd edilən qətnamədə cinayət və ya terror məqsədilə informasiya resurslarından və ya texnologiyalarından istifadə edilməsinin qarşısının alınmasının zəruriliyi vurğulanırdı.

7-9 noyabr 2002-ci il tarixində informasiya məsələləri ilə bağlı Buxarestdə keçirilmiş Ümumavropa konfransında qəbul olunan yekun sənəddə öz əksini tapan prinsiplərdən birini İKT-dən istifadə zamanı etimad və təhlükəsizliyin möhkəmləndirilməsi prinsipi təşkil edirdi. Həmin prinsip qlobal kibertəhlükəsizlik mədəniyyətinin formalaşdırılmasını nəzərdə tutur.

15 iyun 2006-cı il tarixdə keçirilən Şanxay Əməkdaşlıq Təşkilatı (ŞƏT) Şurasının iclasında təşkilata daxil olan dövlət başçılarının beynəlxalq informasiya təhlükəsizliyi barədə qəbul etdikləri bəyanatda İKT-dən hüquq bərabərliyi və qarşılıqlı hörmət, dövlətlərin daxili işlərinə qarışmama, münaqişələrin dinc yolla həll edilməsi və güc tətbiq etməmək prinsipləri pozulmaqla insanın, cəmiyyətin və dövlətin təhlükəsizliyi maraqları əleyhinə istifadə edilməsi üçün real təhlükənin mövcudluğu etiraf edilirdi. Göstərilən təşkilat çərçivəsində 16 iyun 2009-cu il tarixdə qəbul edilən “Beynəlxalq informasiya təhlükəsizliyinin təmin edilməsi sahəsində əməkdaşlıq haqqında” Sazişin 2-ci maddəsində beynəlxalq informasiya təhlükəsizliyinin təmin edilməsi sahəsində əsas təhdidlər göstərilmişdir.

Azərbaycan Respublikasında informasiya təhlükəsizliyinin qorunması stiqamətində hüququn əsas mənbəyi ölkə Konstitusiyasıdır.

Konstitusiyaya əsasən:

- hər kəsin şəxsi toxunulmazlıq hüququ vardır (maddə 32, I-VIII his.);
- hər kəsin ətraf mühitin əsl vəziyyəti haqqında məlumat toplamaq və ekoloji hüquqpozma ilə əlaqədar onun sağlamlığına və əmlakına vurulmuş zərərin əvəzini almaq hüququ vardır (maddə 39);
- hər kəsin istədiyi məlumatı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır (maddə 50);

Ölkədə informasiya sferasındakı münasibətləri tənzimləyən əsas normativ akt “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanunudur. Həmin hüquqi aktın tənzimlədiyi predmet informasiya müstəvisində yaranan münasibətlərin geniş spektridir.

Bütövlükdə isə, informasiya münasibətləri sferasında tənzimləmə mexanizminin hüquqi mənbəyi kimi aşağıdakıları göstərmək mümkündür:

- Prezident fərmanları;
- AR Konstitusiyası;
- sahəvi qanunlar;
- AR tərəfdar çıxdığı beynəlxalq müqavilələr.

Azərbaycan Respublikası informasiya təhlükəsizliyi sahəsində MDB dövlətləri ilə sıx beynəlxalq əməkdaşlıq tədbirlərini həyata keçirir. Bu əməkdaşlığın normativ hüquqi əsasları kimi aşağıdakıları qeyd etmək olar:

1) 2004-cü il fevralın 6-da Moskva şəhərində imzalanmış "Azərbaycan Respublikası Hökuməti və Rusiya Federasiyası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında" Saziş;

2) 2004-cü il martın 4-də Bakı şəhərində imzalanmış "Azərbaycan Respublikası Hökuməti və Gürcüstan Hökuməti arasında informasiya sahəsində əməkdaşlıq haqqında" Saziş;

3) 2005-ci il aprelin 21-də Kişinyov şəhərində imzalanmış “Azərbaycan Respublikasının Hökuməti və Moldova Respublikasının Hökuməti arasında informatizasiya və informasiya texnologiyaları sahəsində əməkdaşlıq haqqında” Saziş;

4) 2006-cı il iyunun 24-də Astana şəhərində imzalanmış Azərbaycan Respublikası, Qazaxıstan Respublikası, Qırğız Respublikası, Rusiya Federasiyası, Tacikistan Respublikası, Türkmənistan və Özbəkistan Respublikası arasında "Narkotik vasitələrin, psixotrop maddələrin və onların prekursorlarının qeyri-qanuni dövriyyəsi ilə mübarizə üzrə Mərkəzi Asiya Regional İnformasiya və Əlaqələndirmə Mərkəzinin yaradılması haqqında" Saziş;

5) 1 oktyabr 2007-ci il tarixli (№ 402-IIIQ) Azərbaycan Respublikası Qanunu ilə təsdiq edilmiş "Azərbaycan Respublikası Hökuməti və Belarus Respublikası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi haqqında" Saziş;

6) 2008-ci il sentyabrın 11-də Bakı şəhərində imzalanmış "Azərbaycan Respublikası Hökuməti və Özbəkistan Respublikası Hökuməti arasında məxfi informasiyanın qarşılıqlı mühafizəsi-haqqında" Saziş və s.

IV. İNFOTƏHDİD VƏ HÜQUQİ TƏNZİMLƏMƏ MƏSƏLƏLƏRİ

Ölkənin firavanlığı və dünya sivilizasiyasında layiqli yeri informasiya texnologiyaları sahəsində siyasətin praqmatikliyindən, konstruktivliyindən və çevikliyindən asılıdır. İnformasiya məkanın qloballaşması və kütləvi kommunikasiya vasitələri şəbəkəsinin təsiri altında cəmiyyətdə baş verən dəyişikliklər təkcə müəyyən üstünlüklər və mənfəətlərlə məhdudlaşmayıb, həm də sosial-siyasi sahədə informasiya mübarizəsi aparmaq üçün geniş imkanlar açır ki, bu da öz növbəsində milli və beynəlxalq təhlükəsizliyə təhdid doğurur. Bu vəziyyət milli təhlükəsizlik və ilk növbədə, informasiya təhlükəsizliyi kimi mühüm sahənin problemlərinə ənənəvi yanaşmaların ciddi transformasiyasına gətirib çıxarmışdır. Formalaşmaqda olan yeni informasiya-kommunikasiya mühiti istənilən ölkənin siyasi, iqtisadi və müdafiə təhlükəsizliyinə fəal təsir göstərir [11, 8-9].

Son illər kompyuter texnologiyalarının inkişafı ilə bağlı insanların düşüncələrinə, siyasi əqidəsinə, dövlət və cəmiyyət həyatında baş verən hadisə və proseslərə dair baxışlarına təsir göstərən, süni şəkildə müəyyən dairələrin maraqlarına uyğun rəy formalaşdıran vasitələr artmışdır. Məsələn, sosial şəbəkələr vasitəsilə insanlar dövlət çevrilişlərinə, inqilablara çağırılır və s. Bu isə şəxsiyyət-cəmiyyət-dövlət sisteminin bütün ünsürlərinə mənfi təsir göstərməklə, şəxsiyyətin hüquq və azadlıqlarını, cəmiyyətin sabitliyini, dövlətin isə suverenliyini böyük təhdid altında qoymuş olur.

Hər bir dövlətdə informasiya təhlükəsizliyi siyasətinin əsas təyinatı cəmiyyətin maneəsiz, sabit və azad inkişafıdır. Bu isə milli maraqların reallaşması üçün müvafiq əlverişli şəraitin olmasını nəzərdə tutur və informasiya təhlükəsizliyi bütün mümkün vasitələrlə milli maraqların daha səmərəli şəkildə reallaşdırılmasına xidmət edir. Burada informasiya təhlükəsizliyi siyasətini həyata keçirən dövlət orqanlarının operativ və effektli fəaliyyəti mühüm rol oynayır.

Milli maraqlar, onlara təhdidlər və milli təhlükəsizliyin bütün sahələrində həmin təhdidlərdən müdafiənin təmin olunması informasiya və informasiya sahəsi vasitəsilə həyata keçirilir. Müəlliflərdən İ.L.Bəçilo bu məsələ ilə bağlı olaraq qeyd edir ki, informasiya sahəsində milli maraqlara nail olunması və onların təhlükəsizliyinin təmin edilməsi ilə bağlı münasibətlərin tənzimlənməsi üçün müxtəlif hüquq sahələrinin metod və vasitələrindən, o cümlədən intensiv şəkildə inkişaf edən yeni hüquq sahəsi olan informasiya hüququnun metod və vasitələrindən istifadə olunur [12, 21].

İnsan və onun hüquqları, informasiya və informasiya sistemləri və onlara olan hüquqlar yalnız informasiya təhlükəsizliyinin əsas obyekti deyil, həm də bütün sahələrdə bütün təhlükəsizlik obyektlərinin əsas elementləri kimi çıxış edir.

Azərbaycanın qanunvericilik və normativ-hüquqi aktlarına müvafiq olaraq, milli təhlükəsizlik insanların, cəmiyyətin və dövlətin həyati əhəmiyyətli mühüm maraqlarının, həmçinin milli dəyərlərin və həyat tərzinin daxili və xarici təhdidlərdən etibarlı müdafiəsidir. Milli təhlükəsizlik sistemi ilə milli təhlükəsizliyin təmin olunması sistemi öz məzmununa görə bir-birindən fərqlənir. Birincisi, maraq və təhdidlərin qarşılıqlı təsiri prosesini əks etdirən funksional-nəzəri (konseptual) sistemdirsə, ikincisi, milli təhlükəsizliyin təmin olunmasının praktiki məsələlərini həll etməyi nəzərdə tutan orqanlar, vasitələr, müxtəlif təşkilatlar (institusional) sistemidir [13, 93].

Milli təhlükəsizliyin bütün tərkib elementləri çərçivəsində, yəni, siyasi, iqtisadi, hərbi, ekoloji və s. sahələrdə informasiya faktorunun rolu getdikcə daha çox artır. Müasir inkişaf meylləri və tendensiyaları onu deməyə əsas verir ki, informasiya təhlükəsizliyinin milli təhlükəsizliyin təmin edilməsi

sistemində yeri və rolu gələcəkdə daha da artacaqdır. Hüquq ədəbiyyatında bu yanaşma konkret arqumentlərlə əsaslandırılır.

İnternetin hüquqi tənzimlənməsi məsələsi də informasiya təhlükəsizliyi ilə bağlı müasir dövrün aktual məsələlərindən birinə çevrilmişdir.

Hazırda bütün dünya üzrə insan fəaliyyətinin ən zəif hüquqi tənzimetməyə məruz qalan sahələrindən biri İnternetdir. Müasir dövrdə dünyanın heç bir ölkəsində İnternet şəbəkəsi ilə bağlı yaranan hüquq münasibətlərini tənzim edən məcəllələşdirilmiş qanunvericilik yoxdur. Bu sahədə mövcud olan normativ hüquqi aktlar Şəbəkənin fəaliyyətinin ayrı-ayrı aspektlərini tənzim edir. Onlara ilk növbədə şəbəkəyə təchizatçılar vasitəsilə qoşulma, müvafiq əlaqə xətləri və ayrıca xidmətlər təqdim edilməsi məsələləri aiddir [14, 16-19].

Aparılan statistik təhlillər və İnterpolun müvafiq məlumatları göstərir ki, hazırkı şəraitdə İnternet planetdə cinayətkarlığın ən sürətli templə artdığı bir məkana çevrilmişdir.

İnternetin qlobal xarakteri milli qanunvericilik sistemləri ilə beynəlxalq praktika arasında ziddiyyət yaradır. Internetdə yerləşdirilən informasiya bir qrup dövlətlərin maraqlarına xidmət etdiyi halda digər dövlətlərin maraqlarına və qanunvericiliyinə zidd ola bilər. Bu isə virtual məkanda milli təhlükəsizliyin təmin edilməsi məsələsinin aktuallığını artırır

NƏTİCƏ

Beləliklə, qeyd edilənləri aşağıdakı kimi ümumiləşdirmək mümkündür:

Milli informasiya təhlükəsizliyinin daha səmərəli və dolğun təmin edilməsi baxımından aşağıdakıları zəruri hesab edirik:

- “İnformasiya təhlükəsizliyi haqqında“ qanunun qəbul edilməsi;
- informasiya təhlükəsizliyinin idarə edilməsi mexanizminin təkmilləşdirilməsi;
- şəxsi həyatın toxunulmazlığının daha dolğun təmin edilməsi;
- dövlət orqanlarının fəaliyyətində şəffaflığın təmin edilməsi;
- elektron sənəd dövriyyəsinin və elektron imzadan istifadənin genişləndirilməsi;
- postneft dövründə qeyri-neft sektorunun inkişafı fonunda rəqabətədavamlı, dünya standartlarına və ən son tələblərə cavab verən informasiya texnologiyalarının istehsalı üzrə fəaliyyətin ön palana çəkilməsi;
- sosial mediada təhqir, böhtan, işgüzar nüfuza xələl gətirilməsi, cəmiyyətin və dövlətin maraqlarına zidd, xaosa səbəb ola biləcək çağırışlarla və digər bu kimi mənfi və arzuolunmaz hallarla adekvat mübarizə imkanının təmin olunması üçün İnternet resurslarının məzmununun yoxlanılması üzrə mükəmməl və qabaqcıl dünya dövlətlərinin mütərəqqi təcrübəsinə uyğun gələn texniki və hüquqi mexanizmlərin tətbiqi və s.

ƏDƏBİYYAT

[1] İnternetdə və informasiya cəmiyyətində insan hüquqları/ http://azerbaycaninfo.az/ iqtisadiyyat/print:page,1,1214-dnternetdj-vj-informasiya-cjmiyyjtindj-insan-hgquqlard.html.

[2] Əsgərbəyov Y. İnternetdə informasiya müharibələri / Informasiya müharibələri və kompyuter cinayətkarlığı. Bakı: Elm və təhsil, 2011, 120 s.

[3] Xəlilov Q., Eminov F. Kompyuter cinayətkarlığı ilə mübarizə və milli qanunvericilik / Informasiya müharibələri və kompyuter cinayətkarlığı. Bakı: Elm və təhsil, 2011, 120 s.

[4] “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu. Bakı: Qanun, 2013.

[5] “Dövlət sirri haqqında” Azərbaycan Respublikası Qanunu / http://e-qanun.az/framework/5526.

[6] İnsan hüquqları haqqında Beynəlxalq bill. Bakı: “Azərbaycan” nəşriyyatı, 1998, 54 s.

[7] Асланов Р.М. Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и общество, 2012, № 2 (86), с. 45-48.

[8] Камышев Э.Н.Информационная безопасность и защита информации. Учебное пособие. Томск: ТПУ, 2009, 95 с.

[9] Əliquliyev R.M., İmamverdiyev Y.N., Yusifov F.F. Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar // İnformasiya cəmiyyəti problemləri, №2 (4), 2011, s. 3-9.

[10] Асланов Р.М. Международное правовое регулирование в сфере обеспечения информационной безопасности // Закон и право, 2012, № 3, с. 104-106.

[11] Мехтиев Р. Общие подходы к укреплению международной информационной безопасности / Informasiya müharibələri və kompyuter cinayətkarlığı. Bakı: Elm və təhsil, 2011, s. 8-9.

[12] Исполнительная власть Российской Федерации. Проблемы развития / Под ред. И.Л.Бачило. М.: Юрист, 1998, 432 с.

[13] Həsənov Ə.M. Azərbaycan Respublikasının milli inkişaf və təhlükəsizlik siyasətinin əsasları. Bakı: Zərdabi LTD, 2016, 700 s.

[14] Танимов О.В., Кудашкин Я.В. Перспективы правового регулирования отношений в сети Интернет // Информационное право, 2010, № 4, с. 16-19.

FUNDAMENTAL LEGAL PRINCIPLES OF INFORMATION SECURITY: A COMPARATIVE APPROACH

Kh. Niyazov
Institute of Law and Human Rights of ANAS
xalid-555@mail.ru

Abstract – It should be emphasized that in the experience of the **countries** across the world there were the first laws on the information protection and national security information too.
In France, Italy, Spain, Portugal, Denmark, the Netherlands and other countries, laws were passed which allowed everyone to get acquainted with information on the activities of government agencies and in the United States, Canada, Australia and New Zealand, in accordance with these laws, citizens have the opportunity to obtain information directly about management.
Particular emphasis should be put on that, in order to take the necessary measures to ensure information security, the issue of the formation of international legal mechanisms and the national legal and regulatory framework is of special importance and should be considered not in the context of individual countries but in international global information security. The Republic of Azerbaijan in the field of information security carries out measures for international cooperation with the CIS countries, as substantive legal frameworks. Current trends in development create the opportunity to assert that the place and role of information security in the system of ensuring national security will be strengthened, which is specifically argued in the law books.

Keywords – national security, information security, information law, information society, information legislation, computer technology, information space