UOT 004.056 DOI: 10.25045/jpis.v11.i1.01

Əliquliyev R.M.[1], İmamverdiyev Y.N.[2], Mahmudov R.Ş.[3]
[1,2,3]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]r.alguliev@gmail.com, [2]yadigar@iit.science.az, [3]rasimmahmudov@gmail.com

İNFORMASİYA TƏHLÜKƏSİZLİYİ MİLLİ TƏHLÜKƏSİZLİYİN MÜHÜM KOMPONENTİ KİMİ

Daxil olmuşdur: 25.11.2019. Düzəliş olunmuşdur: 29.12.2019. Qəbul olunmuşdur: 07.01.2020.

Məqalədə milli təhlükəsizliyin mahiyyətinə, məzmununa dair müxtəlif yanaşmalar araşdırılır. Milli təhlükəsizliyin vəzifələri, təmin olunması metodları şərh olunur. Milli təhlükəsizliyin obyekti olan həyati vacib maraqlar, müxtəlif sahələr təsnif edilir. Bu təsnifata uyğun olaraq milli təhlükəsizliyin ictimai-siyasi təhlükəsizlik, hərbi təhlükəsizlik, informasiya təhlükəsizliyi, qida təhlükəsizliyi, enerji təhlükəsizliyi, təhsil sisteminin təhlükəsizliyi, elmi-texnoloji təhlükəsizlik, səhiyyə sisteminin təhlükəsizliyi, nəqliyyat sisteminin təhlükəsizliyi, ekoloji təhlükəsizlik, KİV-in təhlükəsizliyi, mədəni-mənəvi təhlükəsizlik kimi komponentləri fərqləndirilir. İKT-nin inkişafı, informasiya təhlükəsizliyinin formalaşması ilə əlaqədar milli təhlükəsizlik sistemində informasiya cəmiyyətinin artan rolu və vəzifələri göstərilir. Həmçinin informasiya təhlükəsizliyi ilə milli təhlükəsizliyin digər komponentləri arasında qarşılıqlı münasibətlər analiz edilir. Hər bir milli təhlükəsizlik komponentində İKT-nin tətbiq sahələri, informasiya təhlükəsizliyi təhdidləri müəyyən edilir və onların aradan qaldırılması yolları göstərilir.
İşin yerinə yetirilməsində analiz və sintez, müqayisə, ümumiləşdirmə, sistemli yanaşma metodlarından istifadə edilmişdir.
Məqalədə əldə edilən nəticələr informasiya cəmiyyəti şəraitində milli təhlükəsizlik üzrə yeni konsepsiyaların, strategiyaların və digər normativ sənədlərin hazırlanması üçün istifadə edilə bilər.

Açar sözlər: *milli təhlükəsizlik, informasiya təhlükəsizliyi, hərbi təhlükəsizlik, iqtisadi təhlükəsizlik, enerji təhlükəsizliyi.*

Giriş

Təhlükəsizlik həmişə ayrı-ayrı insanların, cəmiyyətin və bütövlükdə, dövlətin ən mühüm məqsədlərindən və tələbatlarından biri olub. İnsan sivilizasiyasının formalaşması və inkişafı həmişə təbiətdən, cəmiyyətdən, düşmən ölkələrdən, texnoloji obyektlərdən və s. qaynaqlanan müxtəlif təhlükələrin dəf edilməsi ilə bağlı olub. Başqa sözlə, cəmiyyətin və dövlətin mövcudluğunun və inkişafının ən mühüm şərtlərindən biri təhlükəsizlikdir.

"Təhlükəsizlik" (ing. safety) termini ilk dəfə 1190-cı ildə ingilis filosofu Robert Grossetestenin (1175–1253) lüğətində "özünü istənilən təhlükədən qorunmuş hesab edən insan ruhunun sakit vəziyyəti" kimi istifadə edilib [1]. Təhlükəsizliyin təmin olunması problemi bir çox filosof, politoloq, tarixçi və hüquqşünasların diqqət mərkəzində olub.

Cəmiyyətin dövlət quruluşu, təhlükəsizliyin təmin edilməsi sahəsində dövlətin vəzifələri və funksiyaları haqqında bir sıra mütəfəkkirlər maraqlı fikirlər irəli sürmüşlər [2]. Platon hesab edirdi ki, dövlət əsas diqqətini onun təhlükəsizliyini təmin edən hərbçilərə yönəltməlidir. Aristotel cəmiyyətdə və dövlətdə təhlükəsizliyin təmin edilməsinin yolunu vətəndaşlar arasında ictimai-siyasi mədəniyyətin formallaşdırılmasında görürdü. İtalyan ictimai-siyasi mütəfəkkiri Makiavelli dövlətə daxildən (vətəndaşlar tərəfindən) və xaricdən (güclü qonşu dövlətlər tərəfindən) təhlükələrin mövcud olduğunu bildirirdi. Hesab edirdi ki, xarici təhlükələri yaxşı ordu və etibarlı müttəfiqlərin köməyi ilə dəf etmək olar. Onun fikrincə, xarici təhlükələr aradan qalxarsa, daxildə təhlükəsizilyi qorumaq mümkündür. Fransız filosofu Russo "cəmiyyətin inkişafı" nəzəriyyəsinə "xalq suverenliyi" anlayışını daxil etmişdir. Həmin anlayışda xalqın azad və müstəqil inkişafı ilə yanaşı, həm də cəmiyyətin təhlükəsizliyi məsələsi nəzərdə tulur.

Ötən əsrin 50-ci illərində Amerika psixoloq-alimi Maslou tərəfindən "motivasiya nəzəriyyəsi" işlənib hazırlanmışdır [3]. Həmin nəzəriyyədə insanın əsas tələbatlarının iyerarxiyasını quran müəllif təhlükəsizlik məsələsini ikinci pilləyə qoymuşdur. Yəni Maslouya görə, insanın həyat motivasiyasında fiziki tələbatlardan sonra onun təhlükəsizliyə olan tələbatı dayanır.

"Milli təhlükəsizlik" termini ilk dəfə 1904-cü ildə ABŞ prezidenti Teodor Ruzveltin ölkə Konqresinə göndərdiyi məktubda istifadə edilmişdir. Lakin bu termin yalnız 1947-ci ildə rəsmi status almışdır. Belə ki, həmin il ABŞ-da "Milli təhlükəsizlik haqqında" qanun qəbul edilmişdir. Məhz həmin qanun əsasında ilk dəfə olaraq ABŞ-ın Milli Təhlükəsizlik Şurası və Mərkəzi Kəşfiyyat İdarəsi təşkil olunmuşdur [4].

1994-cü ildə BMT XXI əsr üçün "təhlükəsizlik" anlayışına yeni yanaşmanı təklif etdi [5]:

- təhlükəsizlik yalnız ölkəyə deyil, həm də xalqa aiddir;
- təhlükəsizlik, sadəcə, hərbi gücə malik olmaqla deyil, həm də inkişafa nail olmaqla əldə edilir;
- təhlükəsizlik yalnız dövlətə deyil, həm də öz evində və iş yerində olan insana aiddir;
- təhlükəsizlik yalnız dövlətlər arasında deyil, həm də xalqlar arasında münaqişələrdən qorunma vəziyyətidir.

Ənənəvi olaraq, "təhlükəsizlik" anlayışı "təhlükənin olmaması, sabitlik, qorunma, əmniyyət, etibarlılıq" kimi izah olunur.

Azərbaycan Respublikasının qanunvericiliyinə görə, təhlükəsizlik – dövlətin müstəqilliyinin, suverenliyinin, ərazi bütövlüyünün, konstitusiya quruluşunun, xalqın və ölkənin milli maraqlarının, insanın, cəmiyyətin və dövlətin hüquq və mənafelərinin daxili və xarici təhdidlərdən qorunmasının təmin edilməsidir [6]. Lakin bəzi tədqiqatçıların fikrincə, təhlükəsizliyə yalnız hər hansı bir vəziyyət kimi baxılmamalıdır. Bu mövqedən çıxış edənlər hesab edirlər ki, təhlükəsizlik həm də konkret sistemin münasibətləri və xüsusiyyətləri, həmçinin müvafiq strukturların müəyyən təhlükəsizlik səviyyəsinin təmin olunmasına yönəlmiş fəaliyyətinin şərtləri və nəticələridir.

Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyasında qeyd edilir ki, Azərbaycan Respublikasının təhlükəsizlik mühiti onun suverenliyi, ərazi bütövlüyü, sərhədlərinin toxunulmazlığı, milli maraqları, davamlı inkişafı, əhalisinin rifah və dəyərlərinin qorunmasına təsir edən amillərin məcmusudur [7].

Müasir konsepsiyalarda təhlükəsizlik şəxsiyyətin, cəmiyyətin və dövlətin həyati vacib maraqlarının daxili və xarici təhdidlərdən qorunma səviyyəsi kimi xarakterizə olunur. Həyati vacib maraqlara şəxsiyyətin, cəmiyyətin və dövlətin fəaliyyətini və inkişafını səmərəli şəkildə təmin edən tələbatlarının məcmusu aid edilir [8].

Şəxsiyyətin maraqları konstitusiya hüquqlarının, azadlıqlarının reallaşdırılmasından, şəxsi təhlükəsizliyin təmin edilməsindən, həyat səviyyəsinin yüksəldilməsi, fiziki, mənəvi və intellektual inkişafdan ibarətdir.

*Cəmiyyətin maraqları*nı demokratiyanın təmin edilməsi, hüquqi və sosial dövlətin yaradılması, ictimai həmrəyliyə nail olunması və onun dəstəklənməsi, mənəvi ab-havanın sağlamlaşdırılması kimi məsələlər təşkil edir.

*Dövlətin maraqları*na konstitusiya quruluşunun toxunulmazlığı, suverenlik və ərazi bütövlüyü, ictimai-siyasi, iqtisadi və sosial sabitlik, qanunçuluq və hüquqi nizam-intizamın təmin edilməsi, bərabərhüquqlu və qarşılıqlı faydalı beynəlxalq əməkdaşlığın inkişaf etdirilməsi aid edilir. Hər üç tərəfin bütün maraqlarının tam şəkildə təmin edilməsi "milli təhlükəsizlik" anlayışı ilə ifadə olunur.

İstənilən dövlətin suverenliyinin əsasını onun milli təhlükəsizliyi təşkil edir. Ona görə də milli təhlükəsizliyin təmin edilməsi dövlətin ən vacib funksiyalarından biri sayılır. Milli təhlükəsizliyini təmin edə bilməyən ölkələr öz suverenliyini itirir, onların daxili və xarici siyasəti

digər, güclü ölkələr tərəfindən müəyyən olunur. Hər bir dövlətin milli təhlükəsizliyi həm də beynəlxalq təhlükəsizliyin tərkib hissəsidir [9].

Təhlükəsizliyin təmin edilməsinin aşağıdakı metodları mövcuddur [1, 10]:

- risklərin idarə edilməsi;
- dağıdıcı (destruktiv) təsirlərə qarşı müqavimətin artırılması (məsələn, sağlamlığın qorunmasında immunitetin gücləndirilməsi, dağıdıcı təsirlərin nəticələrinin aradan qaldırılması sisteminin yaradılması);
- təhlükələrdən qorunma sisteminin və vasitələrinin yaradılması;
- təhlükə mənbələrinin məhv edilməsi.

Təhlükəsizliyin miqyasına görə üç səviyyəsi fərqləndirilir:

- qlobal təhlükəsizlik;
- regional təhlükəsizlik;
- milli təhlükəsizlik.

Təhlükəsizliyi aşağıdakı müəyyən əlamətlərə görə təsnifatlandırmaq olar:

- obyektinə görə - insan, cəmiyyət, dövlət;
- istiqamətlərinə görə - iqtisadi, sosial, ictimai-siyasi, informasiya və s.
- zərərin miqyasına görə - həddindən artıq, əhəmiyyəti, əhəmiyyətsiz;
- baş vermə ehtimalına görə - böyük ehtimallı, ehtimallı, az ehtimallı;
- baş vermə səbəbinə görə - təbii, qəsdən;
- iyerarxik prinsipə görə - planetlərarası, qlobal, regional, dövlətlərarası, milli, ölkədaxili regional, korporativ, lokal, şəxsi.

Milli təhlükəsizlik mürəkkəb və çoxsəviyyəli sistem olaraq bütün fəaliyyət sahələrini əhatə edir. O, hər birinin özünün məxsusi strukturu olan bir sıra altsistemlərin məcmusunu əks etdirir.

Fəaliyyət sahələrinin, həyati vacib maraqların hər biri ən müxtəlif təhlükələrin təsirinə məruz qalır. Ona görə də təhlükəsizlik obyektlərinin fəaliyyət sahələrinə uyğun olaraq komponentlərə bölünməsi praktiki əhəmiyyət daşıyır. Məhz bu prinsip üzrə həyati vacib maraqlar, təhdidlər və milli təhlükəsizliyin təmin edilməsi istiqamətlərini aşağıdakı kimi təsnif etmək olar (Şəkil 1):

- ictimai-siyasi təhlükəsizlik;
- iqtisadi təhlükəsizlik;
- hərbi təhlükəsizlik;
- informasiya təhlükəsizliyi;
- elmi-texnoloji təhlükəsizlik;
- təhsil sisteminin təhlükəsizliyi;
- səhiyyə sisteminin təhlükəsizliyi;
- qida təhlükəsizliyi;
- enerji təhlükəsizliyi;
- nəqliyyat sisteminin təhlükəsizlyi;
- KİV-in təhlükəsizliyi;
- ekoloji təhlükəsizlik;
- mədəni-mənəvi təhlükəsizlik.

Milli təhlükəsizliyin ayrı-ayrı sahələri bir-biri ilə bağlıdır və biri digəri olmadan təmin edilə bilməz. Bu məqalədə informasiya cəmiyyəti şəraitində milli təhlükəsizlik sistemində informasiya təhlükəsizliyinin artan rolu göstərilir. Milli təhlükəsizliyin ayrı-ayrı komponentlərinin informasiya təhlükəsizliyi ilə qarşılıqlı əlaqəsi araşdırılır. Milli təhlükəsizliyin ayrı-ayrı komponentlərini təşkil edən müxtəlif fəaliyyət sahələrində İKT-nin tətbiqinin, informasiyalaşdırmanın xüsusiyyətləri, həmin sahələrdə informasiya təhlükəsizliyi ilə bağlı əsas təhdidlər və onların qarşısının alınması yolları araşdırılır.

Şəkil 1. Milli təhlükəsizliyin komponentləri

Milli təhlükəsizlik sistemində informasiya təhlükəsizliyinin yeri və rolu

İnformasiya təhlükəsizliyi dedikdə, konfidensiallığı, tamlığı və əlyetərliyi təmin etmək üçün informasiyanın və informasiya sistemlərinin icazəsiz girişlərdən, istifadədən, açıqlanmaqdan, modifikasiyadan və ya məhv edilməkdən mühafizəsi başa düşülür [11].

Başqa sözlə, informasiya təhlükəsizliyi – informasiya sferasında ölkənin milli maraqlarının (şəxsiyyətin, cəmiyyətin və dövlətin həyati vacib maraqlarının balanslaşdırılmış əsasda) daxili və xarici təhdidlərdən qorunma səviyyəsini əks etdirir [12].

Digər prizmadan yanaşsaq, informasiya təhlükəsizliyi – obyektin vəziyyətinin (xüsusiyyətlərinin) və inkişaf istiqamətlərinin bötövlüyünü, idarəçiliyini, mahiyyətini, müxtəlif növ potensialının, reputasiyasının qorunmasını təmin edən keyfiyyət göstəricilərinin məcmusudur [13].

İnformasiya sferasında şəxsiyyətin maraqları onun informasiyanın əlyetərliliyi, informasiyadan qanunla qadağan olunmayan fiziki, mənəvi və intellektual inkişaf məqsədləri ilə istifadəsi, həmçinin şəxsi təhlükəsizliyi təmin edən informasiyanın, fərdi məlumatların mühafizəsi kimi məsələləri əhatə edir.

İnformasiya sferasında cəmiyyətin maraqları bu sahədə şəxsiyyətin maraqlarının təmin olunması, demokratiyanın möhkəmləndirilməsi, hüquqi dövlətin formalaşdırılması və ictimai həmrəyliyə nail olunmasından ibarətdir.

İnformasiya sferasında dövlətin maraqlarına ölkənin informasiya infrastrukturunun davamlı və harmonik inkişafı, vətəndaşların informasiya sahəsində konstitusion hüquqlarının reallaşdırılması üçün şəraitin yaradılması, dövlətin informasiya resurslarının qanunsuz

müdaxilələrdən qorunması, ölkənin informasiya və telekommunikasiya sistemlərinin təhlükəsizliyinin təmin edilməsindən ibarətdir.

Milli təhlükəsizliyin informasiya sferasında əsas vəzifələri aşağıdakılardan ibarətdir [1, 5, 7, 10]:

- vətəndaşların informasiya hüquqlarının reallaşdırılması və informasiya təhlükəsizliyi məsələləri arasında həssas balansın yaradılması;
- informasiya infrastrukturunun təkmilləşdirilməsi, yeni informasiya texnologiyalarının inkişafının, yayılmasının və bütün zəruri sahələrə tətbiqinin dəstəklənməsi, informasiyanın axtarılması, toplanması, saxlanması, emalı və analizi vasitələrinin qlobal informasiya infrastrukturunun tələblərinə uyğun unifikasiyası;
- informasiya təhlükəsizliyinin təmin olunması sahəsində hüquqi bazanın təkmilləşdirilməsi, müvafiq dövlət orqanlarının fəaliyyətinin koordinasiyası;
- milli telekommunikasiya və informasiya texnologiyaları sənayesinin inkişafı;
- dövlət orqanlarında və digər strateji sahələrdə dövlət informasiya resurslarının etibarlı mühafizəsi.

İKT-nin sürətlə inkişaf etdiyi, cəmiyyətin bütün sahələrinə, bütün fəaliyyət sferalarına dərin nüfuz etdiyi və bunun nəticəsi olaraq informasiya cəmiyyətinin formalaşdığı müasir dövrdə informasiya təhlükəsizliyi milli təhlükəsizlik və onun ayrı-ayrı komponentləri ilə sıx qarşılıqlı əlaqədədir.

Dövlətçiliyin, cəmiyyətin inkişafının müasir mərhələsində milli təhlükəsizlik problemi son dərəcə mürəkkəb, kompleks və çoxaspektlidir, onun tərkibində informasiya komponentləri özünü daha qabarıq şəkildə büruzə verməkdədir. Belə ki, İKT milli təhlükəsizliyin və sabitliyin təmin olunmasında getdikcə daha çox rol oynamağa başlayır. Ona görə də bütün inkişaf etmiş ölkələr milli təhlükəsizliyi yüksək səviyyədə təmin etmək üçün müxtəlif təyinatlı informasiya infrastrukturlarının, sistemlərinin yaradılmasına və inkişafına xüsusi diqqət ayırırlar.

Cəmiyyətin informasiyalaşdırılması səviyyəsi, iqtisadi, ictimai-siyasi və sosial proseslərin vəziyyəti və inkişafı haqqında mötəbər informasiyanın mövcudluğu və əlyetərliliyi hakimiyyət strukturlarının və cəmiyyətin, bütövlükdə, ictimai-siyasi, hərbi, iqtisadi, ekoloji sosial və mədəni sferalarda səmərəli qərarların hazırlanması və reallaşdırılması üzrə imkanlarını müəyyən edir. Bu baxımdan, hazırda informasiya cəmiyyətin dayanıqlı inkişafı və təhlükəsizliyi üçün həlledici əhəmiyyət daşıyır.

Yeni dövrdə informasiya təhlükəsizliyi öz əhəmiyyətinə görə milli təhlükəsizlik sistemində digər komponentlərlə müqayisədə daha böyük əhəmiyyət daşımağa başlayır. Belə ki, artıq informasiya bəşəriyyətin ən qiymətli resursuna çevrilib və elmdə, təhsildə, idarəetmədə, iqtisadiyyatda, biznesdə, cəmiyyətdə bütün mütərəqqi yeniliklər, əhəmiyyətli hadisələr informasiya və bilik istehsalı ilə bağlıdır. İnformasiya cəmiyyətində insan fəaliyyətinin bütün sferaları informasiya fəzasına daşınır, informasiya prosesləri sosial, ictimai-siyasi, hüquqi, iqtisadi, psixoloji, kulturoloji və digər münasibətləri də əhatə edir. Bununla yanaşı, informasiya proseslərinin neqativ təsirləri özünü daha qabarıq göstərir, kibercinayətkarlıq, kiberterrorizm, informasiya müharibəsi təhlükələri artır [12].

İKT sürətlə inkişaf etdikcə informasiya təhlükəsizliyi çətiri (*hypernym*) altında müxtəlif təhlükəsizlik anlayışları meydana gəlir (*hyponym*) :

- kibertəhlükəsizlik;
- elektron təhlükəsizlik;
- kompüter təhlükəsizliyi;
- şəbəkə təhlükəsizliyi;
- telekommunikasiya təhlükəsizliyi;
- Big data təhlükəsizliyi;
- bulud təhlükəsizliyi;
- kiberfiziki sistemlərin təhlükəsizliyi;

- radio-efir məkanının təhlükəsizliyi;
- mobil sistemlərin təhlükəsizliyi;
- virtual təhlükəsizlik;
- informasiyanın mühafizəsi;
- kriptoqrafiya;
- e-imza texnologiyası;
- informasiya azadlığı;
- uşaqların kibertəhlükəsizliyi;
- İnternet azadlığı;
- fərdi məlumatların mühafizəsi;
- steqanoqrafiya;
- proqram sistemlərinin təhlükəsizliyi;
- və s .

Bütün bu istiqamətlər milli təhlükəsizliyin ayrı-ayrı sahələri üzrə həyati vacib maraqların qorunması sahəsində mühüm elementlər kimi çıxış edir. İKT-nin yeni inkişaf istiqamətləri, tətbiq sahələri meydana gəldikcə informasiya təhlükəsizliyinin əhatə dairəsi genişlənir və buna müvafiq olaraq vəzifələri də artır.

Big data analitikasının, bulud hesablamalarının, ucuz və təkmilləşdirilmiş sensorların, genişzolaqlı mobil rabitənin meydana gəlməsi ilə bütün istehsal və xidmət sahələrində "4-cü sənaye inqilabı" adlanan köklü dəyişikliklər baş verdi [13]. Bu texnologiyaların əsas xüsusiyyəti insanların iştirakı olmadan və qərarların avtonom qəbulu sisteminin fəaliyyəti növbəti – 5-ci sənaye inqilabi üçün zəmin yaradır [14]. "Sənaye 5.0" robototexnika və süni intellektə əsaslanacaq. Lakin bu texnologiyaların informasiya təhlükəsizliyi ilə bağlı təhdidləri hələlik yaxşı öyrənilməyib və onların tətbiqi ilə bağlı müvafiq risklərin qiymətləndirilməsinə ehtiyac vardır [15, 16].

İctimai-siyasi təhlükəsizlik və informasiya təhlükəsizliyi

Milli təhlükəsizliyin mühüm komponentlərindən biri ictimai-siyasi təhlükəsizlikdir. İctimai-siyasi təhlükəsizlik səviyyəsi bilavasitə dövlət hakimiyyətinin fəaliyyətinin göstəricisidir. Yəni ictimai-siyasi təhlükəsizliyin pozulması ölkədə idarəetmənin iflic vəziyyətə düşməsi, xaotik vəziyyətin yaranması deməkdir. Milli təhlükəsizliyin digər komponentlərinin vəziyyəti də məhz ictimai-siyasi təhlükəsizlik səviyyəsindən asılıdır. Hər hansı bir ölkədə ictimai-siyasi təhlükəsizlik, sabitlik təmin olunmazsa, hərbi, iqtisadi, sosial və digər sahələrdə təhlükəsizlik mövcud ola bilməz.

Daxili şərtlər baxımından, ictimai-siyasi təhlükəsizlik, cəmiyyətdə, ölkədə ictimai-siyasi sistemin dayanıqlılığının, bütün sosial qurupların əsas maraqlarının, əsas insan hüquq və azadlıqlarının təmin olunması, sosial-ictimai-siyasi konfliktlərin olmaması deməkdir [17].

Xarici şərtlər baxımından isə, ictimai-siyasi təhlükəsizlik - dövlət hakimiyyəti tərəfindən beynəlxalq arenada ölkənin konstitutusiya quruluşunun, suverenliyinin, ərazi bütövlüyünün, milli maraqlarının qorunma səviyyəsidir.

İctimai-siyasi təhlükəsizlik həm də cəmiyyətdə sosial ədalət prinsiplərinin reallaşdırılması, vətəndaşların minimum sosial rifah səviyyəsi və yüksək həyat standartları ilə təmin olunması vəziyyətidir. İctimai-siyasi təhlükəsizliyin təmin olunması, əslində, ictimai sabitliyin qarantı sayılır.

Müasir dövrdə ictimai-siyasi təhlükəsizliyin həm təmin olunmasında, həm də pozulmasında İKT böyük rol oynayır. Məsələn, bir sıra əsas insan hüquq və azadlıqlarının, o cümlədən təhsil hüququnun, fikir və söz azadlığının, məlumat azadlığının, yaradıcılıq azadlığının, dövlətin idarə olunmasında iştirak etmək hüququnun, müraciət hüququnun, şəxsi toxunulmazlıq hüququnun, təhlükəsiz yaşamaq hüququnun, bərabərlik hüququnun, mülkiyyət hüququnun, mənzil hüququnun, nikah hüququnun, əmək hüququnun, istirahət hüququnun, sosial təminat hüququnun və s. təmin olunmasında İKT əvvəllər mövcud olmayan geniş imkanlar yaradır. Eyni zamanda, İKT vasitəsi

ilə ölkədə ictimai-siyasi sabitliyi pozmaq üçün informasiya müharibəsi texnologiyalarından istifadə imkanları mövcuddur [18].

Qeyd edilən hüquq və azadlıqların təmin edilməsi üçün yaradılan texnoloji mühitin dayanıqlığını qorumaq, eləcə də, ictimai-siyasi sabitliyin pozulmasına yönələn ideoloji-texnoloji təsirlərdən sığortlanmaq üçün informasiya təhlükəsizliyi tədbirlərinə böyük ehtiyac vardır.

İctimai-siyasi təhlükəsizliyin ən mühüm obyekti isə dövlətin idarəetmə orqanlarıdır. İKT-nin tətbiqi ilə formalaşan və inkişaf edən müasir dövlət idarəetmə sistemi – elektron dövlət informasiya təhlükəsizliyinin ən məsuliyyətli sahəsidir. E-dövlət platformasında texnoloji infrastrukturun, elektron sənəd dövriyyəsinin, e-imzaya əsaslanan autentifikasiya sisteminin, dövlət sirri daşıyan məlumatların, fərdi məlumatların qorunması, dövlətin açıq informasiya resurslarının vətəndaşlar üçün əlyetərliliyinin təmin edilməsi və s. informasiya təhlükəsizliyinin mühüm vəzifələrindəndir.

Hərbi təhlükəsizlik və informasiya təhlükəsizliyi

Dövlətin hərbi təhlükəsizliyi – konstitusiya quruluşunun, ictimai-siyasi, iqtisadi və sosial sabitliyin və cəmiyyətin dayanaqlılığının hərbi təhlükə və təhdidlərdən, hərbi təcavüzdən qorunma səviyyəsidir [19].

Azərbaycan Respublikasının müstəqilliyinin, suverenliyinin, ərazi bütövlüyünün, konstitusiya quruluşunun, xalqın və ölkənin milli maraqlarının, insanın, cəmiyyətin və dövlətin hüquq və mənafelərinin hərbi və ictimai-siyasi, habelə digər təhdidlərdən qorunması dövlətin hərbi təhlükəsizliyin təmin edilməsi sahəsində başlıca vəzifələrindən biridir [7].

İnkişaf etmiş ölkələrin hərbi təhlükəsizlik strukturlarında informasiya faktorunun rolu getdikcə artmaqdadır. Həmin ölkələr öz hərbi güclərini artırmaq, müdafiə sistemlərini möhkəmləndirmək üçün informasiya resursları və texnologiyalarının imkanlarından effektli şəkildə istifadə edirlər [20].

Dövlətin informasiyanı mühafizə sistemi mürəkkəb bir struktur kimi digər komponentlərlə yanaşı, hərbi informasiyanın qorunması vəzifəsini də daşıyır. Hərbi sahədə qorunması vacib olan əsas informasiya obyektləri bunlardır: mərkəzi hərbi idarəetmə, ayrı-ayrı qoşun növlərinin, birləşmələrinin, hərbi hissələrin idarəetmə orqanlarının informasiya infrastrukturu; qoşunların, hərbi texnika və silahların avtomatlaşdırılmış idarəetmə sistemləri.

Bundan başqa, mühəndis qoşunlarında informasiya yükü daha artıq olan bir sıra spesifik vəzifələr həyata keçirilir: döyüş üçün istehkamların hazırlanması, müşahidə, mühəndis kəşfiyyatı, şəxsi heyətin, texnikanın və mövqelərin gizlədilməsi, hərəkət yollarının müəyyənləşdirilməsi, maneələrin aradan qaldırılması və s. Müasir dövrdə bu cür döyüş vəzifələrinin həyata keçirilməsi üçün informasiya texnologiyalarının imkanlarından geniş istifadə edilir [21].

Mühəndis qoşunlarının idarə edilməsi zamanı informasiyanın ötürülməsi və emalı aşağıdakı prosesləri əhatə edir: cari vəziyyət haqqında hərbi-mühəndis informasiyasının toplanması və onun mətndən qrafik formaya keçirilməsi (kriptoqrafiya), qrafik informasiyanın yuxarı idarəetmə orqanlarına göndərilməsi, qrafik informasiyanın yenidən mətnə çevrilməsi, informasiyanın emalı, qiymətləndirilməsi və müvafiq qərarların qəbulu, qəbul olunmuş qərarların qrafik formaya keçirilərək yerli hərbi bölmələrə göndərilməsi və orada yenidən mətnə çevrilməsi [22].

Əsas döyüş sənədlərindən biri olan hərbi xəritələrin operativ şəkildə hazırlanması və dəyişdirilmisi prosesləri də bilavasitə informasiya texnologiyaları vasitəsi ilə həyata keçirilir. Bu xəritələr cari taktiki vəziyyətin çevik və dəqiq vizuallaşdırılmasına imkan verir.

Müasir ordularda kəşfiyyat və digər məqsədlər üçün məsafədən idarə edilən robototexnika qurğularından, pilotsuz uçuş aparatlarından geniş istifadə edilir.

Bu cür proseslərin uğurla həyata keçirilməsi isə, ilk növbədə, informasiya təhlükəsizliyinin yüksək səviyyədə təmin edilməsini tələb edir. Bu məqsədlə bir sıra ölkələrdə xüsusi hərbi bölmələr – kiberqoşunlar formalaşdırılır [23].

Hərbi təhlükəsizliklə sıx bağlı olan məsələlərdən biri də informasiya müharibəsidir [24]. Tarixə ekskurs etsək, müəyyən etmək olar ki, hər bir dövrdə hərbi əməliyyatlarla yanaşı, informasiya silahlarından, informasiya hücumlarından da istifadə edilib. Bu üsuldan daha uğurla istifadə edən tərəf hədəfə çatmaq üçün əlavə imkanlar qazanıb.

XX əsrin ikinci yarısından etibarən həyata keçirilən hərbi əməliyyatlar zamanı informasiya müharibəsi texnologiyaları daha aktiv şəkildə və uğurla tətbiq edilməkdədir. Bu da İKT-nin inkişafı və yaratdığı yeni imkanlar hesabına baş verir.

Hərbi əməliyyatlarla paralel şəkildə aparılan informasiya müharibəsinin əsas hədəflərindən biri qarşı tərəfin ordusu və ya bötövlükdə, əhalisi arasında təxribat xarakterli dezinformasiya yaymaq, onları çaşqın, ümidsiz vəziyyətə salmaq, döyüş ruhunu sarsıtmaqdır. Sürətlə inkişaf edən İKT bu cür psixoloji təsirlərin həyata keçirilməsi üçün böyük imkanlar yaradır. Bu baxımdan, informasiya təhlükəsizliyinin əsas vəzifələrindən biri informasiya müharibəsinə qarşı hazırlıqlı olmaq və real təhlükələr baş verdikdə onların qarşısını alamaq üçün adekvat tədbirlərin görülməsidir.

İqtisadi təhlükəsizlik və informasiya təhlükəsizliyi

İqtisadi təhlükəsizlik – ölkənin müstəqil şəkildə yaşaması və inkişafı üçün iqtisadiyyatın və onun müxtəlif sahələrinin (maliyyə, bank, investisiya, vergi və s.) milli məhsulun minimal zəruri həcmini təmin etmə vəziyyətidir. Həmçinin ölkənin strateji təsərrüfat resurslarının düşmən və kriminal qüvvələrin təsirindən və nəzarətindən qorunması, əsas iqtisadi hüquqların və azadlıqların qorunması səviyyəsidir [25].

İqtisadi təhlükəsizliyin təmin olunması – ölkənin suverenliyinin təmin olunmasının qarantı, cəmiyyətin sabitliyinin və normal fəaliyyətinin, müvəffəqiyyətə nail olmanın əsas şərtlərindən biridir. Bu, onunla izah olunur ki, iqtisadiyyat dövlətin, cəmiyyətin və şəxsiyyətin fəaliyyətinin ən mühüm istiqamətlərindən biridir. İqtisadi təhlükəsizliyin təmin olunmadığı şəraitdə milli təhlükəsizlikdən söhbət gedə bilməz. Ona görə də iqtisadi təhlükəsizlik dövlətin ən vacib prioritetlərindən biri sayılır [26].

Son zamanlar informasiya texnologiyaları, o cümlədən İnternet-texnologiyalar idarəetmə, maliyyə, texniki infrastruktur, istehsal, xidmət, məişət və s. sahələrə geniş tətbiq edilməkdədir. Bu texnologiyaların təsiri ilə bank işi, dövlət idarəetməsi, səhiyyə, təhsil, kütləvi informasiya vasitələri, nəqliyyat, rabitə kimi ənənəvi fəaliyyət sahələri ciddi transformasiyaya uğrayır. İqtisadi sahələrdə informasiyanın, informasiya texnologiyalarının rolu artdıqca informasiya təhlükəsizliyi məsələləri də iqtisadi sektor üçün mühüm əhəmiyyət kəsb etməyə başlayır.

Yeni iqtisadiyyatın əsasını informasiya və biliklər təşkil edir. Artıq informasiya və biliklər əsas istehsal və xidmət amilləri sırasında xüsusi əhəmiyyət kəsb etməyə başlayır. İnformasiya iqtisadiyyatında ənənəvi resurs növlərinə informasiya resursu da əlavə olunur. Maddi istehsal sahələrində də yüksək səmərəlilik yalnız informasiya resurslarının toplanması, emalı, istifadəsi hesabına mümkündür. İnformasiya resursları sənədlər, verilənlər bazaları, alqoritmlər, kompüter proqramları, ədəbiyyat, incəsənət və elmi əsərlər şəklində maddiləşir. Ölkənin, regionun, müəssisənin informasiya resursları öz əhəmiyyətinə görə xammal, material, enerji, faydalı qazıntılar və s. kimi strateji resurs sayılır.

İnformasiya və biliklər iqtisadiyyatının əsas texnologiyaları isə bunlardır [27]:

- Big data;
- neyrotexnologiyalar və süni intellekt;
- nanotexnologiyalar;
- paylanmış reyestr sistemləri (blokçeyn);
- kvant texnologiyaları (kvant informatikası, kvant kompüterləri, kvant kriptoqrafiyası və s.);
- Əşyaların İnterneti;
- robototexnika;
- virtual və əlavə reallıq texnologiyaları;

- 3D printer;
- və s.

İnformasiya və biliklərə əsaslanan iqtisadiyyatın formalaşdırılması və inkişafına dair müasir konsepsiyalarda, əsasən, aşağıdakı məsələlərin həlli nəzərdə tutulur [28]:

– hüquqi-normativ tənzimləmə;
– təhsil və kadr məsələləri;
– elmi-tədqiqatların aparılması;
– yeni texnologiyaların yaradılması və tətbiqi;
– informasiya infrastrukturunun yaradılması;
– informasiya təhlükəsizliyinin təmin edilməsi.

İqtisadi təhlükəsizliyin ən mühüm istiqamətlərindən biri onun infrastrukturunun təhlükəsizliyidir [26]. İnfrastruktur təhlükəsizliyi – milli iqtisadiyyat infrastrukturunun fasiləsiz və maneəsiz fəaliyyətinin təmin edilməsi vəziyyətidir. Bu sahədə fasiləsizliyin təmin edilməsi ilə ictimai istehsal proseslərinin dayanıqlı və effektli şəkildə reallaşdırılması həyata keçirilir. İnfrastruktur təhlükəsizliyinin təmin edilməsinin məqsədi istehlakçılara infrastruktur xidmətlərinin göstərilməsi və təqdim olunan məhsulların mühafizəsi üçün təminatın yaradılması, həmçinin vacib iqtisadi maraqlara daxili və xarici təhdidlərin mövcudluğu şəraitində ölkənin iqtisadi sisteminin dayanıqlı fəaliyyət göstərməsi üçün zəruri ilkin infrastruktur şərtlərinin təmin olunmasıdır.

İqtisadi infrastrukturun təhlükəsizliyinə əsas təhdidlər aşağıdakılardır:

- infrastruktur kompleksinin maddi-texniki bazasının köhnəlməsi və texnoloji geriliyi;
- infrastrukturun inkişafının onun xidmət etdiyi xidmət və istehsal sahələri ilə müqayisədə geridə qalması;
- infrastruktur mühitinin strukturunun deformasiyası;
- infrastruktur kompleksinin yüksək material tutumluluğu;
- daxili bazarda milli infrastruktur komplekslərinin xarici analoqları tərəfindən sıxışdırılıb çıxarılması.

Son vaxtlar İKT-nin geniş və hərtərəfli tətbiqi ilə iqtisadi infrastruktur sahələrində ciddi keyfiyyət dəyişiklikləri baş verir. Bu prosesdən kənarda qalan mikro və makro iqtisadi subyektlər rəqabətdə uduzmağa məhkumdurlar. Məhz buna görə də infrastruktur kompleksinin maddi-texniki bazasının köhnəlməsi və texnoloji geriliyi infrastruktur təhlükəsizliyinə təhdidlər sırasında ən mühüm faktor sayılır. Qeyd edilən maddi-texniki bazanın köhnəlməsinin və texnoloji geriliyin aradan qaldırılması isə məhz İKT-nin effektli tətbiqi ilə mümkün ola bilər. İnfrastruktur kompleksinin yüksək material tutumluluğu da infrastruktur təhlükəsizliyinə təhdidlər sırasında yer alır. Bu təhlükənin aradan qaldırılması üçün infrastruktur kompleksinin yüksək material tutumluluğunu əhəmiyyətli dərəcədə azaltmaq tələb olunur. Bu isə yalnız informasiya və elmtutumlu texnologiyaları tətbiq etməklə reallaşdırıla bilər.

İqtisadi təhlükəsizliyin daha bir mühüm istiqaməti istehsal təhlükəsizliyidir [26]. İstehsal təhlükəsizliyi – istehsal sferasında iqtisadi maraqların qorunma səviyyəsidir. İstehsal təhlükəsizliyinin təmin olunmasının məqsədi istehsal strukturlarının stabil fəaliyyət göstərmələri və bütün mövcud resurslardan maksimum səmərəli istifadə etməklə rəqabətədavamlı məhsulların buraxılması üçün şəraitin yaradılmasıdır.

Son dövrlərdə ənənəvi istehsal və xidmət sahələrinin sürətlə informasiyalaşdırılması prosesi gedir [29]. Müəssisələrin idarə edilməsində, istehsal və xidmət proseslərində informasiya texnologiyaları, o cümlədən e-sənəd dövriyyəsi tətbiq edilir. Kağız daşıyıcılarında olan bütün sənədlər, informasiya elektron formaya keçirilir. Həmçinin müəssisələrdə müxtəlif informasiya bazaları yaradılır, informasiya sistemləri formalaşdırılır. Bütün bunlar həm də informasiya təhlükəsizliyinin obyektləri kimi çıxış edir. Ona görə də istehsal və xidmət müəssisələrində informasiya təhlükəsizliyinin əhəmiyyəti ön plana çıxır.

İnformasiya texnologiyalarının, xüsusilə İnternetin təsiri ilə iqtisadiyyatda baş verən əsas tendensiyalardan biri məhz rəqəmsallaşma proseslərdir [30]. Yəni insan müasir texniki vasitələrin köməyi ilə real obyektlərlə deyil, onların təsvirləri, simvolları ilə qarşılıqlı əlaqədə olur. Rəqəmsallaşma prosesi daha çox maliyyə, pul-kredit sistemlərində müşahidə olunur. O cümlədən kağız, metal pulları elektron pullar, nağd ödənişləri nağdsız ödənişlər əvəz edir, elektron ödəniş sistemləri meydana gəlir və inkişaf edir.

Maliyyə təhlükəsizliyi iqtisadi təhlükəsizliyin ən vacib tərkib hissələrindən biridir [31]. Maliyyə təhlükəsizliyi praktiki olaraq ölkənin istər makroiqtisadi, istərsə də mikroiqtisadi səviyyədə bütün iqtisadi fəaliyyət sahələrinə təsir göstərir. Yəni maliyyə təhlükəsizliyi ölkənin bütün iqtisadi münasibətlər sisteminin stabil fəaliyyət göstərməsi üçün mühüm faktordur. Ölkənin maliyyə təhlükəsizliyinin təmin edilməsi büdcə-vergi, pul-kredit, həmçinin valyuta tənzimlənməsi siyasətinin düzgün həyata keçirilməsi ilə bağlıdır [30, 31].

Elektron pulların, elektron ödəniş sistemlərinin meydana gəlməsi ilə iqtisadi təhlükəsizliyin mühüm istiqaməti olan maliyyə təhlükəsizliyi həm də informasiya təhlükəsizliyi kimi çıxış etməyə başlayır.

Bütövlükdə, iqtisadiyyat sahəsində informasiya təhlükəsizliyi ilə bağlı əsas təhdidlər aşağıdakılardır [32, 33]:

- dövlətin statistika sistemi;
- maliyyə-kredit sistemi;
- iqtisadiyyat sahəsində cəmiyyətin və dövlətin fəaliyyətini təmin edən intellektual informasiya sistemləri və bazaları;
- mülkiyyət formasından asılı olmayaraq, müəssisə və təşkilatların mühasibat uçotu sistemi;
- dövlətin, eləcə də, mülkiyyət formasından asılı olmayaraq, ayrı-ayrı müəssisə və təşkilatların maliyyə, birja, vergi, gömrük, xarici iqtisadi fəaliyyətlə bağlı informasiyanın toplanması, emalı, saxlanması və ötürülməsi sistemləri.

İnformasiyalaşdırma, telekommunikasiya, informasiyanın mühafizəsi vasitələrinin xaricdən alınması da ölkənin texnoloji cəhətdən idxaldan asılı vəziyyətə düşməsinə gətirib çıxarır. Bu da iqtisadi sahədə ciddi informasiya təhdidlərindən biri sayılmalıdır. İqtisadiyyatın normal fəaliyyətinə əsas təhdidlər sırasında kibercinayətkarlıq da mühüm yer tutur.

Həmçinin təsərrüfat subyektlərinin öz kommersiya fəaliyyətləri barəsində qeyri-mötəbər informasiya vermələri, yaxud informasiyanı gizlətmələri, eləcə də, istehsal etdikləri məhsulların istehlak xüsusiyyətləri ilə bağlı məsuliyyətini müəyyən edən normativ-hüquqi bazanın yetərli olmaması da informasiya təhlükəsizliyi sahəsində ciddi təhdidlərdən biridir.

Bütövlükdə, iqtisadi sahədə informasiya təhlükəsizliyinin təmin edilməsi üçün dövlət səviyyəsində aşağıdakı tədbirlərin görülməsi zəruridir [32, 33]:

- statistik, maliyyə, birja, vergi, gömrük və s. informasiyanın toplanması, emalı, saxlanması və ötürülməsi sistemlərinin və vasitələrinin yaradılması, inkişafı və mühafizəsinə dövlət nəzarətinin təşkili və həyata keçirilməsi;
- intellektual kart, elektron pul və elektron ticarət sistemləri bazasında mühafizə olunan milli elektron ödəniş sistemlərinin işlənməsi və tətbiqi;
- iqtisadiyyat sahəsində informasiya münasibətlərini tənzimləyən normativ-hüquqi bazanın təkmilləşdirilməsi;
- iqtisadi informasiyanın toplanması, emalı, saxlanması və ötürülməsi sahəsində kadr hazırlığının təkmilləşdirilməsi.

Enerji təhlükəsizliyi və informasiya təhlükəsizliyi

Enerji təhlükəsizliyi, ölkənin, vətəndaşların, cəmiyyətin, dövlətin və iqtisadiyyatın etibarlı yanacaq-enerji təminatına təhdidlərdən qorunma səviyyəsidir [34]. Bu təhdidlər xarici (geo, ictimai-siyasi, makroiqtisadi, konyuktur və s.) amillərlə, həmçinin ölkənin energetika sektorunun vəziyyəti və fəaliyyəti ilə bağlı müəyyən edilir.

Enerji təhlükəsizliyinin təmin olunmasının əsas prinsipləri aşağıdakılardır [35]:

- strateji və mühüm obyektlərin enerji ilə etibarlı təmin olunması;
- sərf edilmiş yanacaq ehtiyatlarının yerinin doldurulması;
- yanacağın və enerji növlərinin diversifikasiyası (şaxələndirilməsi);
- ekoloji tələblərin nəzərə alınması;
- enerji ehtiyatlarından səmərəsiz istifadənin qarşısının alınması;
- daxili və xarici bazarlarda enerji ehtiyatlarının lazımi gəlir gətirməsi və səmərəli ixrac üçün azad iqtisadi şəraitin yaradılması;
- və s.

Energetika sisteminə aid müəssisələr, qurğular kritik obyektlər sırasına aid edilir [36]. Çünki müasir dövrdə məişət həyatının, bütün xidmət və istehsal sahələrinin, dövlət idarəetmə orqanlarının fəaliyyəti energetika sisteminin təhlükəsiz, stabil fəaliyyətindən asılıdır. Ona görə də bu sahənin informasiya təhlükəsizliyi kritik əhəmiyyət daşıyır [37].

Hazırda elektrik enerjisinin istehsalı, vahid sistemə qoşulması, ötürülməsi və istehlakçılara çatdırılması işləri də olduqca geniş və mürəkkəb proseslər kompleksini əhatə edir. Bütün bu proseslər İKT-nin tətbiqi ilə həyata keçirilir.

4-cü sənaye inqilabının – intellektual sensorlar şəbəkəsinin, kiberfiziki sistemlərin, superkompüter texnologiyalarının imkanlarından istifadə edərək mövcud enerji mənbələrinin bərpası və alternativ mənbələrin tapılması, başqa sözlə "yaşıl" iqtisadiyyatın bir qolu olan "yaşıl" smart-energetikanın inkişaf etdirilməsi bəşəriyyət qarşısında dayanan ən vacib çağırışlardan biridir [38].

Müasir dövrdə enerji təhlükəsizliyi milli təhlükəsizliyin ən mühüm istiqamətlərindən biri kimi çıxış edir. Bütün fəaliyyət sahələrində İKT-nin tətbiqi, informasiya cəmiyyətinin formalaşması prosesləri elektrik enerjisindən "qidalanır". Aqrar və sənaye cəmiyyətlərindən fərqli olaraq, informasiya cəmiyyəti elektrik enerjisindən tam asılı olan bir inkişaf mərhələsidir. Ona görə də "minilliyin ideologiyası"nda bəyan edilən informasiya cəmiyyəti quruculuğunun ən mühüm məsələlərindən biri də dayanıqlı və təhlükəsiz enerji təminatıdır. Elektrik enerjisi verilişinin dayanması nəticəsində dövlət, istehsal və xidmət sektorunun fəaliyyəti iflic vəziyyətə düşə bilər, böyük həcmdə maliyyə itkiləri yaranar [39].

Ümumiyyətlə, energetika informasiya təhlükəsizliyinin təmin edilməsi üçün xüsusi kompleks tədbirlərin həyata keçirilməsi tələb edilən strateji sahələrdən biridir. Energetika sahəsində əsas mühafizə obyekti informasiya deyil, texnoloji proses və idarəetmə sistemidir [40]. Bu mühitdə təhlükəsizlik sistemi texnoloji prosesin bütövlüyünü və idarəetmənin fasiləsizliyini, operativliyini təmin etməlidir [41, 42]. Energetika sahəsində informasiya təhlükəsizliyinin əhəmiyyəti müvafiq kiber-təhdidlərin reallaşdırılmasının nəticələri ilə müəyyən edilir. Bu, yalnız maddi itki və ya reputasiyanın aşağı salınması deyil, həm də vətəndaşların sağlamlığına ziyan vurulması, ekologiyanın korlanması, hərbi, iqtisadi, nəqliyyat, rabitə və sosial infrastruktura ciddi ziyan vurulması, bütün sahələrdə fəaliyyətin iflic vəziyyətə düşməsidir.

Qida təhlükəsizliyi və informasiya təhlükəsizliyi

Qida təhlükəsizliyi, əsas insan hüquqlarından biridir. Ona görə də bu hüququn təmin edilməsi hər bir dövlətin mühüm vəzifələrindən sayılır. Qida təhlükəsizliyi hər bir insanın sağlam və məhsuldar həyat tərzi üçün qida ilə kifayət qədər təmin edilməsi səviyyəsidir. Bu məsələnin həlli, ilk növbədə, yoxsulluğun azaldılması, qida təminatının və qida məhsullarından istifadənin səmərəliliyinin artırılması ilə bağlıdır [43].

Başqa bir yanaşmaya görə, qida təhlükəsizliyi – müharibə və ya hərbi münaqişələrdən asılı olmayaraq, milli istehsalçıların əhalini lazımi həcmdə və kaloridə, müvafiq tibbi normalara uyğun qida ilə təminetmə qabiliyyətidir.

Qida təhlükəsizliyinin aşağıdakı bir sıra sahələrlə bağlılığı mövcuddur:

- istehsal;
- xammal;
- maliyyə;
- elmi-texniki;
- sosial-demoqrafik;
- əmək bazarının təhlükəsizliyi;
- ictimai;
- informasiya təhlükəsizliyi;
- və s.

Hazırda qida təhlükəsizliyini təmin etmək üçün İKT-nin imkanlarından geniş istifadə edilir. Fermer fəaliyyətini həyata keçirmək üçün bütün zəruri informasiyanın İKT vasitəsi ilə ələtərliliyi təmin olunur: aqrobiznes modelləri, real zaman rejimində hava haqqında məlumatlar, kənd təsərrüfatı və aqrotexniki xidmət üzrə məlumatlar, təqvimlər və s. [44].

Kənd təsərrüfatı obyektlərinin, orada baş verən proseslərin real zaman rejimində müşahidəsi və monitorinqi, sensorlar vasitəsi ilə həmin obyektlərdən operativ və dəqiq informasiyanın toplanması, analizi və idarəetmə qərarlarının qəbulu kimi imkanlar qida məhsullarının və içməli su resurslarının təhlükəsizliyinin təmin edilməsi üçün mühüm əhəmiyyət daşıyır. Bu cür analitik informasiya sistemləri həm qida təhlükəsizliyinin, həm də informasiya təhlükəsizliyinin ortaq obyekti kimi çıxış edir [45].

Qida ehtiyatlarının sistemli şəkildə monitorinqi qida təhlükəsizliyinin təmin edilməsinin ən zəruri tədbirlərindən biri hesab olunur. Müasir dövrdə İKT və kosmik peyklər vasitəsi ilə həyata keçirilən bu cür monitorinqlər aşağıdakıları əhatə edir [46]:

- kənd təsərrüfatı və su resurslarının məsafədən zondlaşdırılması;
- qida təhlükəsizliyinə aid olan informasiyanın toplanması, analizi və istifadəsi üçün kompüterlərin, şəbəkələrin, verilənlər bazalarının, proqram təminatının, Big Data, CİS texnologiyalarının tətbiqi;
- fermerlərin və istehlakçıların məlumatlandırılması üçün şəbəkə infrastrukturlarından istifadə.

Qida təhlükəsizliyi sahəsində informasiya təhlükəsizliyinin əsas vəzifəsi müvafiq idarəetmə strukturları, qərar qəbul edən şəxslər və istehlakçılar üçün zəruri olan informasiyanın tamlığının, konfidensiallığının və əlyetərliliyinin təmin edilməsidir [47].

Qida təhlükəsizliyi və informasiya təhlükəsizliyi üçün ortaq olan digər mühüm problemlər də mövcuddur: qida məhsulları haqqında məlumatların qanunsuz ələ keçirilməsi və açıqlanması, yararsız hala salınması, məhv edilməsi və ya itirilməsi, saxtalaşdırılması, bu cür məlumatlarla manipulyasiya edilməsi və s. Bu cür təhlükələri reallaşdıranlar xarici agentlər, kibercinayətkar, narazı əməkdaş, rəqib şirkətin casusu da ola bilər [47].

Elektron kənd təsərrüfatının formalaşması və inkişafı qida sektorunda informasiya təhlükəsizliyinin rolunu daha da artırır. Elektron kənd təsərrüfatı bitkiçilik, heyvandarlıq, balıqçılıq, meşə və su təsərrüfatlarında İKT-dən istifadənin yenilikçi metodlarının planlaşdırılması, işlənməsi və tətbiqini nəzərdə tutur. Daha geniş mənada, elektron kənd təsərrüfatı - müvafiq texnologiyaların tətbiqi, fəaliyyət istiqamətləri, norma və standartların işlənməsi və reallaşdırılmasının dəstəklənməsi, potensialın inkişafı, kadrların yetişdirilməsi və biliklərin yayılması kimi məsələləri əhatə edir [48].

Elmi-texnoloji təhlükəsizlik və informasiya təhlükəsizliyi

İnformasiya cəmiyyətinin inkişaf etdiyi, biliklər iqtisadiyyatının formalaşdığı müasir dövrdə milli təhlükəsizlik üçün elmi-texnoloji sahənin əhəmiyyəti daha da yüksəlir. İstənilən dövlətin iqtisadi və hərbi qüdrəti onun elmi-texnoloji potensialı ilə bağlıdır [49]. Dahi fransız alimi L.Paster yazırdı ki, "elm ölkədə ən yüksək dəyərə malik olmalıdır, intellektual fəaliyyət sahəsində başqalarından öndə olan xalqlar, digər sahələrdə də həmişə lider olacaqlar". Həqiqətən də, bu gün elmi-texnoloji cəhətdən daha çox inkişaf etmiş ölkələr qlobal miqyasda siyasi, iqtisadi, hərbi, mədəni və s. sahələrdə də qabaqcıl mövqe tuturlar, digər ölkələrə həmin sahələr üzrə əhəmiyyətli dərəcədə təsir göstərmək imkanına malikdirlər.

Elm və texnologiya bütün sahələrdə həm milli təhlükəsizliyin təmin olunması üçün bazis rolunu oynayır, həm də onların özlərinin təhlükəsizliyinin təmin olunmasına ehtiyac vardır. O cümlədən müasir dövrdə elmi-texnoloji fəaliyyətin informasiya təhlükəsizliyi aspektindən mühafizəsinə çox böyük ehtiyac vardır.

Dövlətin elmi-texnoloji təhlükəsizliyinin əsas obyektləri aşağıdakılardır [50]:

- ölkənin elmi-texnoloji, sosial-iqtisadi inkişafı üçün vacib olan fundamental və tətbiqi elmi tədqiqatların nəticələri;
- kəşflər, patentləşdirilməmiş texnologiyalar, sənaye nümunələri, faydalı modellər və eksperimental avadanlıqlar;
- elmi-texnoloji kadrlar və onların hazırlanması sistemi;
- mürəkkəb tədqiqat komplekslərinin idarəetmə sistemləri;
- və s.

Elmi-texnoloji fəaliyyət sahəsində informasiya təhlükəsizliyinə olan xarici təhdidlərə aiddir [51, 52]:

- inkişaf etmiş xarici ölkələr tərəfindən milli elmi-texnoloji resurslara qanunsuz şəkildə çıxış əldə etmək cəhdləri;
- yerli bazarda xarici elmi-texnoloji məhsullar üçün güzəştli şərtlərin təmin edilməsi yolu ilə milli elmi-texnoloji potensialın inkişafının məhdudlaşdırılması;
- xarici dövlət və kommersiya təşkilatları tərəfindən ölkə daxilində sənaye casusluğunun həyata keçirilməsi;
- ölkənin strateji əhəmiyyətli sahələrdə çalışan perspektivli alim və mütəxəssislərinin sosial-iqtisadi motivasiya üsulu ilə xarici ölkələrə cəlb edilməsi.

Daxili təhdidlərə isə aşağıdakıları aid etmək olar:

- elmi-texnoloji fəaliyyətin maliyyələşmə səviyyəsinin aşağı düşməsi;
- elmi-texnoloji sferalarda prestijin azalması nəticəsində gənclərin həmin sahələrə marağının azalması;
- ölkənin texnoloji müstəqilliyini təmin edən informasiya texnologiyaları və digər yüksək texnologiyalar sahəsində rəqabətədavamlı məhsulların istehsal qabiliyyətinin olmaması;
- elmi-texnoloji fəaliyyətin nəticələrinin patent müdafiəsi sahəsində ciddi problemlərin mövcudluğu.

Dövlətin elmi-texnoloji təhlükəsizliyinin təmin edilməsi üçün aşağıdakı məsələlərin həll edilməsi vacibdir [53]:

- milli elmi-texnoloji potensialın reallaşdırılması;
- milli iqtisadiyyatın beynəlxalq rəqabətədavamlılığını təmin edən elmi tədqiqat və texnoloji işləmələrin prioritet istiqamətlərinin inkişaf etdirilməsi;
- dövlət sirrinin obyekti olan strateji əhəmiyyət daşıyan müəssisə və təşkilatlarda, yüksək təhlükəli istehsal sahələrində, elmi-tədqiqat qurumlarında konfidensiallığın və mühafizənin təmin edilməsi;
- texnologiya və elmi işləmələrin ixracına nəzarətin həyata keçirilməsi;

- xarici iqtisadi fəaliyyət və elmi-texnoloji əməkdaşlıq sahələrində intellektual mülkiyyət hüququnun qorunması;
- strateji əhəmiyyət daşıyan texnoloji və elmi işləmələr sahəsində kəşfiyyat və əks-kəşfiyyat fəaliyyəti;
- xarici ölkələrə fiziki və virtual "beyni axını"nın tənzimlənməsi.

Təhsil sisteminin təhlükəsizliyi və informasiya təhlükəsizliyi

Təhsil sistemi milli təhlükəsizlik üçün mühüm əhəmiyyətə malikdir [54]. Yəni təhlükəsizliyin təmin olunmasında insan faktoru ön plana çıxır. Təhsil sistemi isə insan resurslarının, şəxsiyyətin yetişdirilməsində, onun dünyagörüşünün, intellektinin, milli-mənəvi dəyərlərinin, vətənpərvərlik ruhunun formalaşmasında müstəsna rol oynayır.

Beləliklə, milli təhlükəsizlik sisteminin strateji əsaslarından biri də təhsilə bağlıdır. Təhsil milli təhlükəsizliyin hər üç səviyyəsi: şəxsiyyət, cəmiyyət və dövlət üçün eyni dərəcədə vacibdir [55].

Təhsil sisteminin və prosesinin informasiya komponentinin xüsusi çəkisi çox yüksəkdir. Belə ki, dərsliklərin, dərs vəsaitlərinin, müəllimlərin tədris etdikləri dərslərin məzmunu milli təhlükəsizliyin və onun mühüm komponenti olan informasiya təhlükəsizliyinin tələblərinə cavab verməlidir. Təhsil prosesi qanunla qadağan edilmiş istənilən mövzuda təbliğatdan və reklamdan qorunmalıdır.

Dərsliklərin, dərs vəsaitlərinin və kitabxanaların rəqəmsallaşması, elektron dərsliklərin meydana gəlməsi, İnternet mühitində şagird və tələbələrin istifadə etdikləri, təhsil sisteminin nəzarətindən kənar olan əlavə bilik və informasiya mənbələrinin mövcudluğu müvafiq təhlükəsizlik məsələlərini daha da çətinləşdirir. Ona görə də təhsil sistemi ilə bağlı informasiya təhlükəsizliyinin üzərinə çox məsuliyyətli vəzifələr düşür [56].

Təhsil sistemində informasiya təhlükəsizliyinə mühüm təhdidlərdən biri də konfidensial informasiyanın ələ keçirilməsi ilə bağlıdır. Məsələn, praktikada buna misal olaraq elektron bazalarda saxlanılan imtahan suallarının ələ keçirilməsi hallarını göstərmək olar. Bundan başqa, test üsulu ilə keçirilən onlayn imtahan proseslərinin, eləcə də, distant tədris proseslərinin təhlükəsizliyinin təmin edilməsi məsələsi də çox aktualdır [57].

Təhsil sistemində informasiya təhlükəsizliyinin təmin edilməsi üçün aşağıdakı tədbirlərin görülməsi vacibdir [57, 58]:

- tədris prosesində istifadə olunan kompüterlərin icazəsiz müdaxilələrdən (viruslar, haker hücumları və s.) qorunması;
- təhsil müəssisələrinə verilən İnternet trafikinin filtirasiya olunması;
- dərsliklərin və dərs vəsaitlərinin çap və elektron versiyalarının ciddi ekspertizasının həyata keçirilməsi, onların tamlığının qorunması;
- müəllim, şagird və tələbələrin informasiya təhlükəsizliyinin əsasları barədə məlumatlandırılması, onlara informasiya təhlükəsizliyi mədəniyyətinin aşılanması.

İnformasiya təhlükəsizliyinin etibarlı təmin edilməsində əsas elementlərdən biri bu sahədə yüksək ixtisaslı, öz biliklərini real şəraitdə tətbiq etməyə və yeni meydana çıxan kibertəhdidlərə çevik cavab verməyə qabil mütəxəssislərin hazırlanmasıdır. Hazırda qlobal əmək bazarında informasiya təhlükəsizliyi mütəxəssislərinə böyük tələbat vardır [59].

Səhiyyə sisteminin təhlükəsizliyi və informasiya təhlükəsizliyi

Səhiyyə sahəsində milli təhlükəsizliyin təmin edilməsinin strateji məqsədləri bunlardır [60]: ömür müddətinin uzadılması, əlillik və ölüm səviyyəsinin aşağı salınması; vaxtında ilkin tibbi-sanitar və yüksəktexnoloji tibbi yardımın göstərilməsi və profilaktikasının təkmilləşdirilməsi; tibbi yardım standartlarının təkmilləşdiririlməsi; dərman vasitələrinin keyfiyyətinin, effektivliyinin və təhlükəsizliyinə nəzarətin artırılması, pasiyentlərin hüquqlarının etibarlı şəkildə qorunması və s.

Səhiyyə sahəsində aşağıdakılar milli təhlükəsizliyə əsas təhdidlər hesab olunur [61]:

- genişmiqyaslı epidemiyaların və pandemiyaların yayılması;

- immunçatışmazlığı virusunun, vərəmin, narkomaniyanın və alkoqolizmin yayılması;
- psixoaktiv və psixotrop maddələrin əlyetərliliyinin artması.
- və s.

Səhiyyə sahəsində milli təhlükəsizliyin möhkəmləndirilməsi üçün İKT-dən istifadə etməklə tibbi xidmətin keyfiyyətini və əlyetərliliyini yüksəltmək, əczaçılıq, biotexnologiya və nanotexnologiya sahəsində perspektivli tədqiqatlara dövlət dəstəyinin verilməsi, bu sahənin inkişafı üçün iqtisadi mexanizmləri təkmilləşdirmək və maddi-texniki bazanı möhkəmləndirmək tələb olunur [62].

Klinikalar, tibb mərkəzləri və digər səhiyyə müəssisələrində pasiyentlərin qanunla qorunan böyük həcmdə fərdi məlumatları toplanır. Bir çox sənədlər "həkim sirri" hüquqi kateqoriyasına aid edilir. Həmin məlumatlar və sənədlər hazırda elektron formada, müxtəlif informasiya sistemlərində dövr edir, müəyyən bazalarda saxlanılır və analiz olunur. Tibb müəssisələri elektron sənəd dövriyyəsi sisteminə keçir, pasiyentlərin elektron qeydiyyat sistemi formalaşır. Nəzərə almaq lazımdır ki, tibbi məlumatlar fərdi məlumatlar arasında ən həssas kateqoriya hesab olunur [63].

Tibbi fəaliyyət sahələrində İKT-nin tətbiqi ilə e-tibb, kiberfiziki və kiberbioloji sistemlər formalaşır. O cümlədən məsafədən tibbi xidmətlər göstərilir, vətəndaşlara e-sağlamlıq kartları verilir, müayinə-diaqnostika proseslərində, bir sıra cərrahiyyə əməliyyatlarının aparılmasında İKT-nin imkanlarından geniş istifadə edilir.

Həmçinin bir çox tibbi cihazda geniş yayılmış əməliyyat sistemləri tətbiq olunur, bu baxımdan, onlar da adi kompüterlər kimi hücumlara həssasdırlar. Lakin xüsusi əməliyyat sistemləri olan cihazlar da kiber hücumlara məruz qala bilər, çox zaman bunun üçün proqram təminatının yenilənməsi mexanizmi istifadə edilir [64].

Səhiyyə sisteminin sürətlə informasiyalaşdırılması, elektron tibbin formalaşması nəticəsində tibb sisteminin İKT-dən, informasiya təhlükəsizliyindən asılılıq səviyyəsi də yüksəlir [65].

Nəqliyyat sisteminin təhlükəsizliyi və informasiya təhlükəsizliyi

Nəqliyyat sistemi təhlükəsizlik baxımından çox kritik sahədir. Nəqliyyət infrastrukturunun və vasitələrinin təhlükəsizliyi böyük həcmdə maliyyə və insan resurları tələb edir. Çünki bu sahə insanların şəxsi həyatının, qiymətli xammal və hazır məhsulların təhlükəsizliyi ilə bağlıdır, bu sahədə baş verən qəzalar, adətən, kütləvi insan tələfatına, böyük həcmdə maliyyə itkisinə səbəb olur [66].

Nəqliyyat sistemi insanların nəqliyyat tələbatlarını ödəmək üçün nəzərdə tutulur və nəqliyyat vasitələrini, nəqliyyat obyektlərini (infrastrukturunu), nəqliyyat müəssisələrini, nəqliyyat sisteminin idarəetmə iyerarxiyasını, həmçinin ətraf mühiti əhatə edir.

Nəqliyyat infrastrukturuna avtomobil yolları, dəmir yolları, hava dəhlüzləri, su yolları, kanallar, tunellər, körpülər, boru xətləri, nəqliyyat qovşaqları və ya terminalları (aeroportlar, avtomobil və dəmir yolu vağzalları, dəniz limanları və s.) daxildir.

Nəqliyyat vasitələrinə isə konveyerlər, gəmilər, liftlər, kanatlar, yükqaldırma kranları, raketlər, avtomobillər, velosipedlər, motosikllər, avtobuslar, tramvaylar, trolleybuslar, qatarlar, təyyarələr və s. aiddir.

Nəqliyyat və kommunikasiya bir-birinə sıx bağlı olan sahələrdir. Müasir dövrdə nəqliyyat sahələrinin və xidmətlərinin sürətli inkişafı da məhz telekommunikasiya sahəsindəki sürətlə artan imkanlarla bağlıdır.

Eyni zamanda, müasir nəqliyyat sistemini informasiya texnologiyalarından kənarda təsəvvür etmək qeyri-mümkündür. Bu gün bütün dünyada nəqliyyatın intellektual idarəetmə sistemləri uğurla tətbiq edilir, bu sahədə məhsuldarlığın artırılması, keyfiyyətli xidmətin göstərilməsi, optimal idarəetmənin, təhlükəsizliyin təmin edilməsi bilavasitə informasiya texnologiyalarının imkanları hesabına reallaşdırılır [67].

O cümlədən sərnişinlərin, nəqliyyat vasitələrinin və avadanlıqlarının avtomatik identifikasiyası həyata keçirilir. Eləcə də, nəqliyyatın, sərnişinlərin, yüklərin hərəkətinin onlayn montorinqi reallaşdırılır. Nəqliyyat infrastrukturunun (yollar, körpülər, tunellər, boru xətləri,

kanallar və s.) etibarlı mühafizəsi üçün onlayn videomüşahidə sistemlərindən, sensor şəbəkələrindən istifadə edilir. Nəqliyyat trafikinin tənzimlənməsi üçün intellektual sistemlər tətbiq edilir. Eyni zamanda, bütün növ nəqliyyat vasitələrinin özləri də intellektuallaşır, "ağıllı" nəqliyyat vasitələrinə çevrilir.

Həmçinin nəqliyyat sistemində sərnişinlərə, xidmət personalına aid böyük həcmdə fərdi məlumatlar, dövlət sirri, kommersiya sirri daşıyan məlumatlar dövr edir.

Bunlardan başqa, elektron poçt sistemi nə qədər inkişaf etsə də, təhlükəsizlik, konfidensiallıq baxımından bəzi rəsmi məktubların, sənədlərin kağız daşıyıcılarda və fiziki poçtla daşınması məqsədəuyğun sayılır.

Nəqliyyat sistemində İKT-nin tətbiqi ilə reallaşdırılan bütün proseslər infrastruktur obyektləri, nəqliyyat vasitələri, bu sistemdə dövr edən informasiya, o cümlədən fiziki poçt məlumatları informasiya təhlükəsizliyinin obyektinə çevrilir [68].

Ekoloji təhlükəsizlik və informasiya təhlükəsizliyi

Ekoloji təhlükəsizlik – təbii mühitin və normal həyat şəraitinin insanın mənfi təsərrüfat fəaliyyətinin nəticələrindən, həmçinin təbii fəlakətlərdən və s. müdafiə olunmuş vəziyyətidir.

Azərbaycan Respublikasının müvafiq qanunvericiliyində ekoloji təhlükəsizlik "insanın və cəmiyyətin həyati vacib maraqlarının, ətraf mühitin ona antropogen və təbii təsirlər nəticəsində yaranan təhlükələrdən qorunmasının təmin edilməsi" kimi xarakterizə olunur.

Ekoloji təhlükəsizliyin təmin edilməsi ilə bağlı dövlətin üzərinə bir sıra vəzifələr düşür. Həmin vəzifələrdən biri də informasiya təminatını təşkil etmək və həyata keçirməkdir. Müvafiq informasiya təminatı ətraf mühitin və təbii ehtiyatların monitorinqini aparmaq, zəruri informasiyanı toplamaq, analiz etmək, adekvat qərarlar qəbul etmək və tədbirlər görmək, habelə ətraf mühitin vəziyyətinə, ətraf mühitə ziyan vurulmasına və təhlükəli ekoloji təsirlərə dair məlumatları qanunvericiliklə müəyyən edilmiş üsullarla açıqlamaqdan ibarətdir.

Müasir dövrdə bütün bu proseslər informasiya texnologiyalarını tətbiq etməklə həyata keçirilir. Belə ki, ekoloji obyektlərdən dəqiq və operativ informasiya əldə etmək üçün Əşyaların İnterneti texnologiyalarından, sensor şəbəkələrindən istifadə edilir. Bu informasiya sistemlərinin təhlükəsizliyi bilavasitə ekoloji təhlükəsizlik baxımından kritik əhəmiyyətə malikdir. Hər hansı bir ekoloji fəlakət haqqında vaxtında dəqiq və etibarlı informasiya əldə edilməlidir ki, qabaqlayıcı tədbirlər görmək mümkün olsun [69].

İKT-nin inkişafı ilə əlaqədar ekoloji təhlükəsizliyin yeni bir istiqaməti – elektron tullantıların təhlükəsizliyi aktuallıq kəsb etməkdədir [70]. Son illər elektron tullantıların həcmi sürətlə artmaqdadır. Bu cür tullantılar insan sağlamlığına və ətraf mühitə ciddi ziyan vurur. Elektron tullantıların bir qismi informasiya daşıyıcılarından ibarətdir. Praktika göstərir ki, tullantı kimi atılmış informasiya daşıyıcılarında müxtəlif xarakterli konfidensial məlumatlar da olur. Yaxud bu cür informasiya daşıyıcılarında, ilk baxışda, əhəmiyyətsiz görünən məlumatlardan Big data texnologiyaları vasitəsi ilə çox qiymətli konfidensial informasiya əldə edilə bilər. Ona görə də müvafiq elektron tullantılar informasiya təhlükəsizliyinin obyekti kimi çıxış edir. Bu sahədə informasiya təhlükəsizliyinin əsas vəzifəsi həmin elektron daşıyıcılarda olan məlumatların etibarlı şəkildə məhv edilməsidir [71].

KİV-in təhlükəsizliyi və informasiya təhlükəsizliyi

Milli təhlükəsizlik sistemində KİV-in təhlükəsizliyinin təmin edilməsi məsələsi xüsusi əhəmiyyətə malikdir. Belə ki, vətəndaşların informasiya təminatı funksiyasını yerinə yetirən KİV-də yayılan hər hansı qeyri-obyektiv, qərəzli, təxribat xarakterli məlumat milli təhlükəsizlik, ölkədəki ictimai-siyasi sabitlik üçün ciddi problemlər yarada bilər [72].

KİV-in fəaliyyətinin obyekti informasiya olduğu üçün bu sahənin fəaliyyəti bilavasitə informasiya təhlükəsizliyinin əhatə dairəsinə düşür. KİV-lə bağlı informasiya təhlükəsizliyinin əsas vəzifəsi milli maraqların qorunmasıdır.

KİV-in informasiya təhlükəsizliyi səviyyəsinin əsas göstəricilərindən biri informasiya müharibəsi əməliyyatlarına qarşı dayanıqlılığıdır. Bu istiqamətdə dayanıqlılığı təmin etmək üçün zəruri texnoloji baza və insan resurları tələb olunur [73].

Xüsusilə, fövqəladə vəziyyətlər zamanı KİV-in funksiyası və əhəmiyyəti dəfələrlə artır, vətəndaşlara, ictimaiyyətə operativ, dolğun və mötəbər informasiya təqdim etmək lazım gəlir ki, insanlar arasında çaşqınlıq, ümidsizlik və s. kimi neqativ tendensiyalar yaranmasın. Bu baxımdan, informasiya təhlükəsizliyinin KİV sahəsində əsas vəzifələrindən biri də müvafiq informasiya mənbələrinə əlyetərliliyin təmin edilməsidir [74].

İKT-nin təsiri ilə KİV-in transformasiyası və konvergensiyası, İnternet-medianın meydana gəlməsi və inkişafı, insanların informasiya tələbatının onlayn rejimdə, operativ şəkildə ödənilməsi imkanının yaranması, vətəndaş jurnalistikasının formalaşması bu sahənin informasiya təhlükəsizliyinin təmin edilməsini daha da mürəkkəbləşdirir. Belə bir şəraitdə müxtəlif informasiya cinayətlərinin reallaşdırılması imkanları da artır [75].

Mədəni-mənəvi sferanın təhlükəsizliyi və informasiya təhlükəsizliyi

Mədəni-mənəvi təhlükəsizlik – ictimai şüurun və xalqın mənəvi sağlamlığının, ənənəvi əxlaqi dəyərlərinin və həyat tərzinin daxili və xarici neqativ təsirlərdən qorunma səviyyəsidir. Dövlətin bu sahədə vəzifəsi əxlaqi normaların, ənənəvi konfessiyaların və milli-mədəni ənənələrin, tarixi ənənələrin və dəyərlərin mühafizəsini təmin etməkdir [76].

Dövlətin mədəni-mənəvi sahədə informasiya təhlükəsizliyinin əsas obyektləri aşağıdakılardır:

- şəxsi ləyaqət;
- vicdan azadlığı;
- dini və digər etiqadı sərbəst şəkildə seçmək və yaymaq azadlığı;
- söz və fikir azadlığı;
- ədəbi, bədii, elmi, texniki və digər yaradıcılıq azadlığı;
- şəxsi həyatın toxunulmazlığı, şəxsi və ailə sirri;
- ölkənin əsas ünsiyyət dili və milli azlıqlarının dili, əxlaqi dəyərləri və tarixi-mədəni irsi;
- intellektual mülkiyyət obyektləri.

Mədəni-mənəvi sferada milli təhlükəsizliyə olan əsas təhdidlərə aşağıdakıları aid etmək olar [77]:

- müxtəlif əhali qruplarının mənəvi tələbatlarına yönəlmiş kütləvi mədəni məhsulların (geyim, davranış, həyat tərzi və s.) neqativ təsirləri;
- mədəniyyət obyektlərinə qarşı qanunsuz təcavüzlər;
- milli dəyərlərin aşılanması istiqamətində qanunsuz təbliğat-təşviqat işləri;
- ölkənin, xalqın tarixinə, tarixi şəxsiyyətlərinə qarşı neqativ rəyin formalaşdırılması;
- irqi, milli, dini ayrıseçkiliyin və dözümsüzlüyün təbliği;
- dövlət dilinin və ya əsas ünsiyyət dilinin ədəbi normalarının pozulmasına yönəlmiş fəaliyyət.

Mədəni sferada milli təhlükəsizlik təhdidlərinə qarşı milli azlıqların öz mədəniyyətlərini inkişaf etdirmələri üçün dövlət tənzimlənməsinin effektivliyinin artırılması, cəmiyyətdə tolerantlığın və qarşılıqlı hörmətin aşılanması, millətlərarası mədəni əlaqələrin gücləndirilməsi, ölkə xalqlarının, milli azlıqların mədəniyyətlərinin, vətəndaşların mənəvi dəyərlərinin qorunması və inkişaf etdirilməsi, mədəniyyət və istirahət müəssisələrinin maddi texniki bazalarının gücləndirilməsi, milli-mənəvi dəyərlər aşılayan kinematoqrafiya və çap məhsullarının, tele-radio verilişlərinin, İnternet kontentinin kütləviləşdirilməsi, inkişafı, əhali üçün əlyetərliliyinin təmin edilməsi, bu cür məhsulların həcminin və keyfiyyətinin artırılması üçün dövlət sifarişlərinin təşkili, mədəni-maarifçilik (etno) turizminin inkişaf etdirilməsi və s. tədbirlərin görülməsi zəruridir.

Mədəni-mənəvi sferaya ekspansiya məqsədilə müxtəlif ölkələrdə istehsal olunan teleseriallar, televiziya verilişləri, İnternet vasitəsi ilə yayılan video-materiallar, elektron kitablar, digər rəqəmsal resurslar bilavasitə informasiya təhlükəsizliyinin obyekti kimi çıxış edir.

Mədəni-mənəvi sahələrdə ölkənin informasiya təhlükəsizliyinin təmin edilməsi şəxsiyyətin inkişafı, formalaşması və davranışları ilə bağlı bir sıra konstitusiya hüquq və azadlıqlarından – informasiya hüquqlarından, mədəni və mənəvi-əxlaqi dəyərlərdən, tarixi ənənə və normalardan istifadə ilə əlaqədardır.

Göründüyü kimi, yuxarıda qeyd edilən mədəni sahə üzrə strateji dövlət məqsədlərinin, bu sahədəki təhlükələrin və onların aradan qaldırılması tədbirlərinin hər biri informativ xarakterlidir, yüksək dərəcədə informasiya yükünə malikdir. Yəni mədəni sferada baş verən həm pozitiv, həm də neqativ proseslər müasir dövrdə İKT-nin, elektron informasiya vasitələrinin vasitəsi ilə həyata keçirilir.

Mədəni-mənəvi sahədə informasiya təhlükəsizliyini təmin etmək üçün dövlətin üzərinə aşağıdakı vəzifələr düşür:

- yaradıcılıq fəaliyyəti və mədəniyyət müəssisələrinin fəaliyyəti üçün sosial-iqtisadi şəraitin yaradılması;
- müasir paylanmış informasiya fondlarının yaradılması yolu ilə geniş əhali təbəqələrinin ən yaxşı milli və xarici mədəniyyət və incəsənət nümunələri ilə tanış olmaq imkanının yaradılması;
- mədəni-maarifçilik işlərinin təkmilləşdirilməsi yolu ilə əhali üçün yaradıcılıq sahəsində özünüreallaşdırma imkanlarının yaradılması;
- əhali üçün asudə vaxtın və uşaqlar üçün məktəbdənkənar kütləvi yaradıcılıq təhsilinin təşkili;
- regionların və milli azlıqların mədəni irsinin qorunması və bu sahədə təşəbbüslərin dəstəklənməsi.
- cəmiyyətdə ölkənin milli maraqlarına cavab verən mənəvi dəyərlərin formalaşmasına və inkişafına ictimai nəzarətin sivil forma və üsullarının tətbiqi;
- ictimai şüura təsir edən neqativ informasiya-psixoloji təsirlərin qarşısını almaq, mənəvi-əxlaqi və tarixi dəyərlərin qorunması üçün hüquqi-təşkilati mexanizmlərin işlənməsi;
- zorakılığı, qəddarlığı, ictimai əxlaqa zidd digər davranışları təbliğ edən teleradio proqramlarının, İnternet resurslarının qarşısının alınması;
- əcnəbi missioner təşkilatlarının ölkədəki fəaliyyətinin qarşısının alınması.
- və s.

Nəticə

İKT-nin sürətlə inkişaf edərək insan fəaliyyətinin bütün sahələrinə uğurla tətbiq edildiyi, elektron dövlətin, informasiya cəmiyyətinin formalaşdığı müasir dövrdə milli təhlükəsizliyin təmin olunması məsələsinə də yeni baxışlar, yanaşmalar, metodologiyalar tələb edilir. Artıq ənənəvi üsul və vasitələrlə milli təhlükəsizliyi təmin etmək mümkün deyil. Ənənəvi cəmiyyət informasiya cəmiyyəti ilə əvəz olunduğu kimi, onun təhlükəsizliyi məsələsi də informasiya və informasiya texnologiyaları amillərindən yüksək dərəcədə asılı vəziyyətə düşür.

Milli təhlükəsizliyin ayrı-ayrı komponentlərinin informasiyalaşdırılmasının xüsusiyyətlərinin və onların informasiya təhlükəsizliyi ilə qarşılıqlı əlaqələrinin analizi də göstərir ki, artıq "milli təhlükəsizlik" və "informasiya təhlükəsizliyi" anlayışları məzmun və mahiyyət baxımından bir-birlərindən o qədər də fərqlənmir. Milli təhlükəsizliyin bütün komponentləri informasiya təhlükəsizliyinin obyektinə çevrilir.

Bütün bunlar milli təhlükəsizliklə bağlı mövcud doktrina, konsepsiya və strategiyalara, bu sahədəki hüquqi-normativ aktlara yenidən baxılmasını, onların İKT-nin, informasiya cəmiyyətinin formalaşdırdığı virtual mühitin diktə etdiyi müasir şərtlərə uyğunlaşdırılmasını tələb edir.

Minnətdarlıq: *Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir* ***– Qrant № EİF-BGM-4-RFTF-1/2017-21/8/1***

Ədəbiyyat:

1. Sidorkin A.I., Iroshnikov D.V. Theoretical issues of "security" concept // Journal of Politics and Law, 2019, Vol. 12, No. 3; pp. 34-39.
2. Peou S. Human Security Studies: Theories, Methods and Themes. World Scientific Publishing Company, 2014, 516 p.
3. Maslow A. H. Motivation and Personality. New York, Harpaer & Row, 1954, 395 p.
4. Smith S., Hadfield A., Dunne T., Dunne T. Foreign policy: Theories, actors, cases. OUP Oxford, 2008, 442 p.
5. Alkire S. A conceptual framework for human security. . CRISE working paper No. 2. University of Oxford: Queen Elizabeth House, 2003, 53 p.
6. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanunu, http://mfa.gov.az/files/file/39.pdf
7. Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası, http://www.e-qanun.az/framework/13373
8. Zelikow Ph. The transformation of national security: Five redefinitions // The National Interest, 2003, no. 71, pp. 17–28.
9. Donohue L. K. Limits of national security // American Criminal Law Review, 2011, Vol. 48, No. 4, pp.1573-1756.
10. DCAF, National Security Policy, 2005, https://issat.dcaf.ch/download/17202/201862/bg_national-security%20(1).pdf
11. İmamverdiyev Y.N. İnformasiya təhlükəsizliyi terminlərinin izahlı lüğəti, Bakı, "İnformasiya Texnologiyaları" nəşriyyatı, 2015, 160 s.
12. Əliquliyev R.M., İmamverdiyev Y.N., Mahmudov R.Ş. İnformasiya təhlükəsizliyinin multidistiplinar elmi-nəzəri problemləri // İnformasiya cəmiyyəti problemləri, 2017, №2, s.32-43.
13. Hofmann E., Rüsch M. Industry 4.0 and the current status as well as future prospects on logistics // Computers in Industry, 2017, Vol. 89, pp. 23-34.
14. Özdemir V., Hekim N. Birth of industry 5.0: Making sense of big data with artificial intelligence, "the internet of things" and next-generation technology policy // Omics: a journal of integrative biology, 2018, Vol. 22, No. 1, pp. 65-76.
15. Lu Y. Industry 4.0: A survey on technologies, applications and open research issues // Journal of industrial information integration, 2017, Vol. 6, pp. 1-10.
16. Ataç C., & Akleylek S. A survey on security threats and solutions in the age of IoT // European Journal of Science and Theology, 2019, Vol.15, pp. 36-42.
17. Margolis J. E. Understanding political stability and instability // Civil Wars, 2010, Vol. 12, No. 3, pp. 326-345.
18. Beskow D. M., Carley K. M. Social cybersecurity: an emerging national security requirement // Military Review, Vol. 99, No. 2, pp. 117-127.
19. Brooks R. A. The military and homeland security // Public Administration and Management, 2005, Vol. 10, No. 2, pp. 130-152
20. Szpyra R. Military security within the framework of security studies: Research results // Connections: The Quarterly Journal, 2014, Vol. 13, No. 3, pp. 59-82.
21. Kramer F.D., Starr S.H., Wentz L.K. (Eds.). Cyberpower and national security. Potomac Books, Inc.. 2009, 664 p.
22. İmamverdiyev Y.N. İnformasiya cəmiyyətində milli kriptoqrafiya siyasətinin formalaşdırılması problemləri // İnformasiya cəmiyyəti problemləri, 2015, №1, s. 12-23.
23. İmamverdiyev Y.N. Kiberqoşunlar: funksiyaları, silahları və kadr potensialı // İnformasiya cəmiyyəti problemləri, 2015, №2, s. 15-25.
24. Ələkbərova İ.Y. İnformasiya müharibəsi texnologiyalarının analizi və təsnifatı // İnformasiya cəmiyyəti problemləri, 2010, № 2, s. 80-91.

25. Əliquliyev R.M., Mahmudov R.Ş. İqtisadi təhlükəsizliklə informasiya təhlükəsizliyinin qarşılıqlı əlaqəsi / Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı", 17-18 may, 2013, s. 7-10.
26. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya iqtisadiyyatının təhlükəsizliyinin təmin edilməsi məsələləri // İnformasiya cəmiyyəti problemləri, 2013, № 1, s. 3-13.
27. Hadad S. Knowledge economy: Characteristics and dimensions // Management dynamics in the Knowledge economy, 2017, Vol. 5, No. 2, pp. 203-225.
28. Tang S. M. Rethinking economic security in a globalized world // Contemporary Politics, 2015, Vol. 21, No. 1, pp. 40-52.
29. Petrenko S. Cyber security innovation for the digital economy. River Publishers, 2018, 492 p.
30. Ozili P. K. Impact of digital finance on financial inclusion and stability // Borsa Istanbul Review, 2018, Vol. 18, No. 4, pp. 329-340.
31. Li Y., Qiu J.P., Xie Q. FinSec 3.0: Theory and practices in financial enterprise / International Symposium on Security in Computing and Communication, 2018, pp. 443-454.
32. Abbosh O., Bissell K. Securing the digital economy. Reinventing the Internet for trust. Accenture, 2019, 49 p.
33. Teoh C.S., Mahmood A.K. National cyber security strategies for digital economy / International Conference on Research and Innovation in Information Systems (ICRIIS), 2017, pp. 217-221.
34. Ang B. W., Choong W. L., & Ng T. S. Energy security: Definitions, dimensions and indexes // Renewable and sustainable energy reviews, 2015, vol. 42, pp. 1077-1093.
35. Bompard E., Carpignano A., Erriquez M., Grosso D., Pession M., Profumo F. National energy security assessment in a geopolitical perspective // Energy, 2017, Vol. 130, pp. 144-154.
36. Cai T. Energy infrastructure security in the digital age // International Journal of Public Administration in the Digital Age (IJPADA), 2018, Vol. 5, No. 2, pp. 12-22.
37. Onyeji I., Bazilian M., Bronk C. Cyber security and critical energy infrastructure // The Electricity Journal, 2014, Vol. 27, No. 2, pp. 52-60.
38. Biresselioglu M.E., Nilsen M., Demir M.H., Røyrvik J., Koksvik G. Examining the barriers and motivators affecting European decision-makers in the development of smart and green energy technologies. // Journal of Cleaner Production, 2018, Vol. 198, pp. 417-429.
39. Venkatachary S. K., Prasad J., Samikannu R. Economic impacts of cyber security in energy sector: a review // International Journal of Energy Economics and Policy, 2017, Vol. 7, No. 5, pp.250-262.
40. Yadav G., Paul K. Assessment of SCADA system vulnerabilities / The 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp.1737-1744.
41. Khan R., Maynard P., McLaughlin K., Laverty D., Sezer S. Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid / The 4th International Symposium for ICS & SCADA Cyber Security Research, 2016, pp. 53-63.
42. Pourbeik P., Kundur P. S., & Taylor C. W. The anatomy of a power grid blackout - Root causes and dynamics of recent major blackouts // IEEE Power and Energy Magazine, 2006, Vol. 4, No. 5, pp. 22-29.
43. Godfray H.C.J., Beddington J.R., Crute I.R., Haddad L., Lawrence D., Muir J.F., Pretty J., Robinson S., Thomas S.M., Toulmin C. Food security: The challenge of feeding 9 billion people // Science, 2010, 327, pp. 812–818.
44. Aker J.C., Ghosh I., Burrell J. The promise (and pitfalls) of ICT for agriculture initiatives // Agricultural Economics, 2016, Vol. 47, No. S1, pp. 35-48.
45. Mohanraj I., Ashokumar K., Naren J. Field monitoring and automation using IoT in agriculture domain // Procedia Computer Science, 2016, Vol. 93, pp. 931-939.

46. Gebbers R., Adamchuk V.I. Precision agriculture and food security // Science, 2010, No. 327(5967), pp. 828-831.
47. Cooper, C. 2015. Cybersecurity in food and agriculture. Kirjassa Leclair, J. (ed.): Protecting Our Future, Volume 2: Educating a Cybersecurity Work Force. Albany NY: Excelsior College. 234 s.
48. Fernando E., Assegaff S., Rohayani A.H. Trends information technology in E-agriculture: A systematic literature review / 3rd International Conference on Information Technology, Computer, and Electrical Engineering, 2016, pp. 351-355.
49. Əliquliyev R.M., İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya cəmiyyəti problemləri, 2010, №1, s. 3-13.
50. Mowery D.C. National security and national innovation systems // The Journal of Technology Transfer, 2009, Vol. 34, No. 5, pp. 455.
51. Halbert D. Intellectual property theft and national security: Agendas and assumptions // The Information Society, 2016, Vol. 32, No. 4, pp. 256-268.
52. Mayers A.M. A study on how cyber economic espionage affects US national security and competitiveness. Doctoral dissertation, Northcentral University, 2018, 120 p.
53. Tabansky L. Towards a theory of cyber power: The Israeli experience with innovation and strategy / 8th IEEE International Conference on Cyber Conflict (CyCon), 2016, pp. 51-63.
54. Klein J.I., Rice C. US education reform and national security. Council on Foreign Relations. 2014, No. 68, 121 p.
55. Orikpe E.A. Education and national security: Challenges and the way forward // Journal of Educational and Social Research, 2013, Vol. 3, No. 10, pp. 53-59.
56. Dai N.H.P., András K., Zoltán R. E-learning security risks and counter measures // Engineering Research and Solutions in ICT, 2016, Vol. 1, pp. 17-25.
57. Bialaszewski D. Information security in education: are we continually improving? // Issues in Informing Science and Information Technology, 2015, Vol. 12, pp. 45-54.
58. Pires E., Moreira F. The integration of information and communication technology in Schools: Online Safety // Procedia Technology, 2012, Vol. 5, pp. 59–66.
59. Thomson K.L., Futcher L.A., Gomana L. Towards a framework for the integration of information security into undergraduate computing curricula // South African Journal of Higher Education, 2019, Vol. 33, No. 3, pp. 155-175.
60. Feldbaum H., Patel P., Sondorp E., Lee K. Global health and national security: the need for critical engagement // Medicine, conflict and survival, 2006, Vol. 22, No. 3, pp. 192-198.
61. Fidler D. P. Public health and national security in the global age: infectious diseases, bioterrorism, and realpolitik // Geo. Wash. Int'l L. Rev., 2003, Vol. 35, pp. 787-856.
62. Blaya J.A., Fraser H.S., Holt B. E-health technologies show promise in developing countries // Health Affairs, 2010, Vol. 29, No. 2, pp. 244-251.
63. Chenthara S., Ahmed K., Wang H., Whittaker F. Security and privacy-preserving challenges of e-health solutions in cloud computing // IEEE Access, 2019, Vol. 7, pp. 74361–74382.
64. Pandey A., Singh B., Saini B.S., Sood N. Medical data security tools and techniques in e-health applications / Medical Data Security for Bioengineers, 2019, pp. 124-131.
65. İmamverdiyev Y.N. E-səhiyyə: informasiya təhlükəsizliyinin aktual problemləri / "Elektron tibbin multidissiplinar problemləri" I respublika elmi-praktiki konfransı, Bakı, 24 may 2016-cı il, c.31-38.
66. Theoharidou M., Kandias M., Gritzalis D. Securing transportation-critical infrastructures: Trends and perspectives. Global Security, Safety and Sustainability & e-Democracy, 2011, pp. 171-178.
67. Thomopoulos N., Givoni M., Rieltveld P. (Eds.). ICT for transport: Opportunities and threats. Edward Elgar Publishing, 2015, 336 p.

68. Dellios K., Papanikas D., Polemi D. Information security compliance over intelligent transport systems: is IT possible?.// IEEE Security & Privacy, 2015, Vol. 13, No. 3, pp. 9-15.
69. Popović, T., Latinović, N., Pešić, A., Zečević, Ž., Krstajić, B., & Djukanović, S. (2017). Architecting an IoT-enabled platform for precision agriculture and ecological monitoring: A case study. Computers and Electronics in Agriculture, 140, 255-265.
70. Alghazo J. Ouda O.K.M., El Hassan A., E-waste environmental and information security threat: GCC countries vulnerabilities // Euro-Mediterranean Journal for Environmental Integration, 2018, 3:13, https://doi.org/10.1007/s41207-018-0050-4
71. Ağayev B.S., Əliyeva K.T. Elektron tullantılar və məlumat daşıyıcılarının informasiya təhlükəsizliyinin bəzi aspektləri // İnformasiya cəmiyyəti problemləri, 2013, №1, 67-74.
72. McLeod D.M., Shah D.V. News frames and national security. Cambridge University Press. 2014, 232 p.
73. Taylor R. The need for a paradigm shift toward cybersecurity in journalism // National Cybersecurity Institute Journal, 2015, Vol. 1, No. 3, pp. 45-47.
74. Henrichsen J.R., Betz M., Lisosky J.M. Building digital safety for journalism: A survey of selected issues. UNESCO Publishing, 2015, 104 p.
75. Thakur K., Hayajneh T., Tseng J. Cyber security in social media: Challenges and the way forward // IT Professional, 2019, Vol. 21, No.2, pp. 41-49.
76. Giles K. "Information troops" - A Russian Cyber Command? / 3rd International Conference on Cyber Conflict, 2011, pp. 45-60.
77. Colarik A., Janczewski L. Establishing cyber warfare doctrine. In Current and Emerging Trends in Cyber Operations. Palgrave Macmillan, London, 2015, pp. 37-50.

УДК 004.056

Алгулиев Расим М.[1], Имамвердиев Ядигар Н.[2], Махмудов Расим Ш.[3]
[1,2,3]Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]r.alguliev@gmail.com, [2]yadigar@iit.science.az, [3]rasimmahmudov@gmail.com

Информационная безопасность как важный компонент национальной безопасности

В статье исследуются различные подходы к сути и содержанию национальной безопасности. Интерпретируются задачи и методы обеспечения национальной безопасности. Классифицируются жизненно важные интересы, различные сферы, являющиеся объектом национальной безопасности. В соответствии с этой классификацией различают такие компоненты национальной безопасности, как общественно-политическая безопасность, военная безопасность, информационная безопасность, пищевая безопасность, энергетическая безопасность, безопасность системы образования, научно-технологическая безопасность, безопасность системы здравоохранения, безопасность транспортной системы, экологическая безопасность, безопасность СМИ, культурно-духовная безопасность. В системе национальной безопасности в связи с развитием ИКТ, формированием информационной безопасности демонстрируются растущая роль и задачи информационного общества. Также анализируются взаимоотношения между информационной безопасностью и другими компонентами национальной безопасности. В каждом компоненте национальной безопасности определяются области применения ИКТ, угрозы информационной безопасности и указываются пути их устранения. При научном исследовании по данной теме были использованы методы анализа и синтеза, сравнения, обобщения, системного подхода. Результаты, полученные в статье, могут быть использованы для разработки новых концепций, стратегий и других нормативных документов по национальной безопасности в условиях информационного общества.

Ключевые слова: *национальная безопасность, информационная безопасность, военная безопасность, экономическая безопасность, энергетическая безопасность.*

Rasim M. Alguliyev[1], Yadigar N. İmamverdiyev[2], Rasim Sh. Mahmudov[3]
[1,2,3]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]r.alguliev@gmail.com, [2]yadigar@iit.science.az, [3]rasimmahmudov@gmail.com

Information security as a national security component

The essence and different approaches to the national security are explored in the article. The article interprets the duties and provision methods of the national security. Different areas and vital interests that are the objects of the national security are classified. According to this classification, the components of the national security, such as socio-political security, military security, information security, food security, energy security, education system security, scientific and technological security, health system security, transport system security, environmental security, Mass Media security, and cultural-moral security are differentiated. The development of ICT, the growing role and responsibilities of the information society in the national security system in connection with the formation of information security are described. The article also analyzes the relationship between the information security and other components of the national security. Application areas of ICT in each national security component and information security threats are identified. Their solution ways are described.

The article uses analysis and synthesis, comparison, generalization and systematic approach.

The results obtained in the article can be used for the development of new security concepts, strategies and other regulatory documents for the national security in the context of the information society.

Keywords: *national security, information security, military security, economic security, energy security.*