

UOT 004.9:351

Əliquliyev R.M.¹, İmamverdiyev Y.N.², Yusifov F.F.³

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹secretary@iit.ab.az, ²yadigar@lan.ab.az, ³farhadysuifov@gmail.com

CƏMIYYƏTİN İNFORMASIYA TƏHLÜKƏSİZLİYİNƏ DAİR BƏZİ KONSEPTUAL BAXIŞLAR

İnformasiya təhlükəsizliyinin təmin olunması üzrə beynəlxalq təcrübədə mövcud olan mexanizmlər tədqiq olunmuş, bu sahədə milli normativ-hüquqi bazanın formalaşdırılması istiqamətində görülən işlər araşdırılmış və təkliflər verilmişdir. Cəmiyyətin təhlükəsizliyinin mühüm komponenti kimi informasiya təhlükəsizliyinin vəzifələri müəyyənləşdirilmiş, mövcud təhlükələr və onların hədəfləri araşdırılmış, cəmiyyətin informasiya təhlükəsizliyinin təmin olunmasına dair təklif və tövsiyələr verilmişdir.

Açar sözlər: informasiya təhlükəsizliyi, informasiya cəmiyyəti, elektron elm.

Giriş

Müasir dövr sənaye cəmiyyətinin informasiya cəmiyyətinə (İC) transformasiyası ilə xarakterizə olunur. İnformasiya cəmiyyətinin qurulmasının əsas vəzifələrinə İC-nin hüquqi əsaslarının yaradılması, insan resurslarının inkişafı, vətəndaşların məlumat almaq və istifadə etmək hüquqları, elektron dövlətin, elektron ticarətin formalaşması, xüsusən, ölkənin intellektual potensialının möhkəmləndirilməsi, informasiya və biliklərə əsaslanan iqtisadiyyatın qurulması, müasir informasiya-kommunikasiya infrastrukturunun yaradılması, milli elektron informasiya fəzasının formalaşdırılması və informasiya təhlükəsizliyinin təmin edilməsi kimi məsələlər daxildir. İnformasiya cəmiyyəti sivilizasiyanın inkişafının müasir mərhələsi kimi cəmiyyətdə informasiya və biliyin rolunun artması, ümumi daxili məhsulun tərkibində informasiya sektorunun payının artması, insanların səmərəli informasiya mübadiləsini və onların qlobal informasiya resurslarına çıxışını təmin edən qlobal informasiya fəzasının yaradılması ilə xarakterizə olunur. Hal-hazırda cəmiyyətin müxtəlif sferalarında, o cümlədən, iqtisadi, enerji, ekologiya və s. sahələrdə informasiya-kommunikasiya texnologiyalarının (İKT) geniş tətbiqi informasiya təhlükəsizliyi məsələsini ön plana çıxarır. Ümumiyyətlə, cəmiyyətin bütün sahələrinin və insanların İKT-dən asılılığı gücləndikcə informasiya təhlükəsizliyinin əhəmiyyəti özünü daha çox büruzə verir. İnformasiya cəmiyyətinin qurulmasının əsas vəzifələrindən biri kimi informasiya təhlükəsizliyi dövlətin, cəmiyyətin və şəxsiyyətin təhlükəsizliyinin təmin edilməsinin əsas istiqamətlərindən birinə çevrilir.

İnformasiya təhlükəsizliyinin təmin olunmasına dair beynəlxalq təcrübə

Cəmiyyət informasiyalaşdıqca insanlar informasiyadan daha artıq dərəcədə asılı vəziyyətə düşürlər. İnformasiya təhlükəsizliyinin təmin olunmaması isə cəmiyyət üçün böyük fəsadlar törədə bilər. Hər hansı ölkədə informasiya təhlükəsizliyinin prioritetləri dövlətin, cəmiyyətin və vətəndaşların maraqlarının balanslı nisbəti əsasında müəyyənləşir. Ölkədəki siyasi, hərbi, fəvqəladə və s. vəziyyətlərdən asılı olaraq bu nisbət dəyişə bilər. Cəmiyyətin təhlükəsizliyinin əsas komponentlərindən biri kimi informasiya təhlükəsizliyinin vəzifələri informasiyanın konfidensiallığı, tamlığı, əlyetərliliyi və ziyanlı kontentlərlə mübarizədir.

İlk dəfə 1988-ci ilin noyabr ayının 30-da universitetlər, elmi-tədqiqat institutları və hərbi idarələr də daxil olmaqla, ARPANET-in minlərlə qovşağını sıradan çıxaran ilk kompyuter virusu meydana gəldi və böyük itkilərə səbəb oldu. Yaradıcısının adına uyğun olaraq "Morris soxulcanı" adlandırılan bu virusun vurduğu ziyan təxminən 100 milyon dollar həcmində qiymətləndirilmişdi.

“Morris soxulcanı” göstərdi ki, informasiya təhlükəsizliyi həqiqətən də çox ciddi məsələdir və insanlar tərəfindən böyük səylər və müvafiq tədbirlərin həyata keçirilməsini tələb edir. Buna görə də dünya ictimaiyyəti informasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşmanın zəruriliyi haqqında ciddi düşünməyə başladı. Həmin vaxtdan bəri informasiya texnologiyaları, informasiya cəmiyyəti inkişaf etdikcə bu problem daha da aktuallaşır. Bunları əsas tutaraq, 1988-ci ildə Kompüter Avadanlığı üzrə Amerika Assosiasiyası 30 noyabrı Beynəlxalq informasiya təhlükəsizliyi günü elan etdi. Ona görə ki, informasiya təhlükəsizliyi məsələsi bir ölkə üçün yox, bütün bəşəriyyət üçün mühüm əhəmiyyət daşıyır.

İnformasiya təhlükəsizliyinin təmin edilməsi sistemik, kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlər aparılmalıdır. 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, əhəlinin 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. Beynəlxalq təcrübədə qlobal informasiya təhlükəsizliyinin təmin olunması məqsədilə bir sıra proqramlar, layihələr, mexanizmlər işlənmişdir. Onların sırasında 2002-ci ildə BMT tərəfindən qəbul etmiş Qlobal İnformasiya Təhlükəsizliyi Mədəniyyəti haqqında Qətnaməni, 2008-ci ildə Beynəlxalq Telekomunikasiya İttifaqı tərəfindən qəbul olunmuş Qlobal İnformasiya Təhlükəsizliyi proqramını göstərmək olar [1,2]. Bununla yanaşı, 2010-cu ildə NATO-nun Lissabon sammitində qəbul olunmuş Bəyannamənin 40-cı maddəsinə əsasən, 2012-ci ildə Tam Operativ Hazırlıq (*Full Operational Capability, FOC*) mərkəzləşdirilmiş qurumunun yaradılması nəzərdə tutulur [3]. Bu qurum NATO-nun bütün infrastrukturunun informasiya təhlükəsizliyini həyata keçirəcəkdir.

Azərbaycan Respublikasında da informasiya təhlükəsizliyi məsələləri milli təhlükəsizliyin əsas tərkib hissələrindən biridir və bu sahədə normativ-hüquqi bazanın formalaşması informasiya cəmiyyəti quruculuğunda prioritet məsələlərdən hesab olunur. Ölkəmizdə informasiya təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasının formalaşdırılması və inkişaf etdirilməsi istiqamətində bir sıra mühüm konseptual sənədlər, normativ-hüquqi aktlar qəbul edilmişdir. Bunlara misal olaraq 2007-ci ildə qəbul olunmuş “Azərbaycan Respublikasının Milli Təhlükəsizlik Konsepsiyası”nı, eləcə də, “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında”, “Dövlət sirri haqqında”, “Elektron sənəd və elektron imza haqqında”, “Elektron ticarət haqqında”, “İnformasiya əldə etmək haqqında”, “Telekommunikasiya haqqında” qanunları və s. göstərmək olar [4-10].

İnformasiya texnologiyalarının inkişafı və istifadəçilərinin sayının sürətlə çoxalması kompyuter sistemlərinə olan təhdidlərin daha geniş xarakter almasına və onların reallaşdırılmasının daha böyük fəsadlar törətməsi ehtimallarının artmasına səbəb olur. Buna görə də, informasiya təhlükəsizliyi sistemlərində baş verən anomal hadisələrə və qeyri-qanuni hərəkətlərə çevik reaksiya verilməsi, kompüter cinayətlərinin müxtəlif növlərinə əks-təsir vasitələrindən biri də dünya təcrübəsində geniş istifadə olunan Kompüter İnsidentləri üzrə Yardım Komandalarının (*Computer Emergency Response Team, CERT*) yaradılmasıdır. Dünyada ilk CERT də məhz 1988-ci ilin noyabr ayında baş vermiş virus epidemiyasından bilavasitə sonra yaradılmışdı. Hazırda müxtəlif ölkələrdə çoxlu sayda CERT qurumları fəaliyyət göstərir.

Cəmiyyətin informasiya təhlükəsizliyinin təmin olunmasına dair konseptual yanaşmalar

Məlumdur ki, qlobal informasiya cəmiyyətində informasiya iqtisadiyyatın, elmin, təhsilin, siyasi və ictimai fəaliyyətin digər sahələrinin aparıcı amilinə çevrilir. Bu baxımdan, informasiya cəmiyyəti çox mürəkkəb formada qarşılıqlı münasibətdə olan korporativ və açıq informasiya fəzalarının toplusundan ibarətdir. Ümumiyyətlə, informasiya cəmiyyətinin formalaşması mərhələləri beş səviyyədən ibarətdir: kommunikasiyalaşma, kompyuterləşmə, şəbəkələşmə, informasiyalaşma və virtuallaşma. Cəmiyyətin informasiya təhlükəsizliyinə olan təhlükələrin hədəfləri də məhz bu səviyyələrdədir [11]. İnformasiya təhlükəsizliyinə olan təhlükələrin meydana çıxmasının əsas səbəblərindən biri kimi isə beynəlxalq səviyyədə İnternetin fəaliyyətini tənzimləyən mexanizmlərin olmamasını göstərmək olar. İnternetin sürətli inkişafı və istifadəçilərinin sayının kütləvi şəkildə artması ilə kompyuter və kommunikasiya sistemlərinə olan təhdidlər daha ehtimallı olur və onların realizəsi nəticəsində yaranan fəsadlar daha da geniş miqyas alır. Müxtəlif səviyyələrdə təhlükələrin olmasına baxmayaraq, istənilən halda, təhlükələrin mənbəyi insandır. Hər bir insanın daxili dünyası, yaşadığı mühit, psixoloji durumundan asılı olaraq cəmiyyət qarşısında məsuliyyətini itirməsi başqalarının hüququnun pozulması ilə nəticələnir. Statistik hesabatlarla görə, sistemin öz istifadəçilərinin hərəkətləri nəticəsində vurulan ziyanın həcmi artıq virusların vurduğu ziyanı üstələyir. Təhlükəsizlik sahəsində bir çox problemlər istifadəçilərin, sistem administratorlarının və digər mütəxəssislərin informasiya təhlükəsizliyi sahəsində biliklərinin lazımı səviyyədə olmaması nəticəsində yaranır. Təbii ki, insan amilinə bağlı olan bu problemlərin aradan qaldırılması informasiya təhlükəsizliyi mədəniyyətinin formalaşmasını zəruri edir.

Vətəndaşlarda informasiya mədəniyyətinin vacib hissəsi olan informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması istiqamətində davamlı və məqsədyönlü tədbirlərin görülməsi də müasir dövrdə mühüm məsələyə çevrilir. Belə ki, istifadəçilərə informasiya-kommunikasiya sistemlərində iş zamanı gözlənilən təhlükələr və onlarla mübarizə mexanizmləri haqqında zəruri biliklər verilməlidir. İnternet şəbəkəsindən istifadə mədəniyyətini formalaşdırmaq, neqativ təsirlərə qarşı “immunitet”in möhkəmləndirilməsi üçün bu mədəniyyət normalarını aşılamaq lazımdır.

Cəmiyyətin informasiya təhlükəsizliyinin təmin olunmasına məsuliyyət bölgüsü də qeyd olunan bütün səviyyələr üzrə aparılmalıdır. Hər bir korporativ informasiya fəzasının təhlükəsizlik siyasəti işlənilməli və həyata keçirilməlidir. Xüsusən, cəmiyyətin informasiya təhlükəsizliyinin əsas komponenti sayılan enerji təhlükəsizliyi məsələsi daim diqqət mərkəzində saxlanılmalıdır. Nəzərə alınmalıdır ki, enerji təhlükəsizliyi hər hansı bir dövlətin daxili məsələsi olmadığı üçün istənilən ölkədə olan serverin sıradan çıxması mövcud informasiya resurslarına digər ölkələrdən də çıxış imkanının məhdudlaşdırılmasına gətirib çıxarır.

İnformasiya təhlükəsizliyinin mühüm vəzifələrindən biri də informasiya azadlığının təmin olunmasıdır. İnformasiya azadlığının təmin olunmasının mühüm göstəricisi kimi fasiləsiz, məhdudiyətsiz informasiya resurslarına çıxış imkanının (əlyetərliliyin) olmasıdır. İnsanların İnternetə çıxış sürətinə tələbatının çox yüksək tempə artması bəzi ölkələrdə informasiya azadlığının təmin olunması üçün vətəndaşların İnternetə çıxış sürətinin minimum həddi haqqında qanunlar qəbul olunmasını zəruri etmişdir. Qeyd etmək lazımdır ki, 2005-ci ildə “İnformasiya əldə etmək haqqında” Azərbaycan Respublikasının Qanunu qəbul edilmişdir. Bu qanundan irəli gələn vəzifələrin yerinə yetirilməsi məqsədi ilə Xüsusi Dövlət Mühafizə Xidməti ilə birgə AMEA İnformasiya Texnologiyaları İnstitutu *gov.az* domen zonasında fəaliyyət göstərən veb-saytların yaradılması və istismarına dair qaydaları işləyib hazırlamışdır.

Mühüm məsələlərdən biri də vətəndaşların şəxsi və ailə həyatı ilə bağlı toplanan, emal olunan və ötürülən məlumatların mühafizə olunması ilə bağlıdır. Qeyd etmək lazımdır ki, bir sıra ölkələrdə İnsan Hüquqları haqqında Bəyannamənin 19-cu və 21-ci maddələrinin həyata keçirilmə vəziyyətinin monitorinqi məqsədi ilə “informasiya ombudsmanı”, “informasiya

tribunali”, “informasiya telekommunikasiya ombudsmanı” kimi institutlar fəaliyyət göstərir [12]. Başqa sözlə, informasiya ombudsmanları, bir tərəfdən, informasiya azadlığının (19-cu maddə), digər tərəfdən isə, fərdi məlumatların mühafizə vəziyyətinin (21-ci maddə) monitorinqini həyata keçirir. İnformasiya cəmiyyəti quruculuğu prosesində ölkədə formalaşan fərdi məlumatlar infrastrukturunu ən önəmli məsələlərdən birini təşkil edir. Ölkəmizdə 2010-cu ildə “Fərdi məlumatlar haqqında” qanun qəbul olunmuşdur və hal-hazırda qanundan irəli gələn vəzifələrin yerinə yetirilməsi məqsədilə müvafiq işlər aparılır [13]. Bu sahədə dünyada olan mövcud təcrübəni nəzərə alaraq ölkəmiz Avropa Şurasının 1981-ci il tarixli “Fərdi məlumatların avtomatlaşdırılmış sistemlərdə emalı vaxtı fiziki şəxslərin qorunması haqqında” Konvensiyasına (108 sayılı Konvensiya) qoşulmuşdur [14].

Cəmiyyətin təhlükəsizliyinin təmin olunmasında biometrik informasiya texnologiyaları böyük imkanlara malikdir. Təcrübədən məlumdur ki, informasiya-kommunikasiya sistemlərində, xüsusən də, İnternet mühitində baş verən cinayətlərin, qeyri-etik davranışın əsas səbəblərindən biri istifadəçilərin zəruri hallarda identifikasiyası mexanizmlərinin mükəmməl olmamasıdır. 2001-ci ilin 11 sentyabrında ABŞ-da baş verən terror hadisəsindən sonra BMT-nin Təhlükəsizlik Şurası insanların onlara məxsus biometrik məlumatlara əsasən identifikasiyasının həyata keçirilməsi, yeni nəsil sənədlərin tətbiqi haqqında qətnamə qəbul etmişdir. 2007-ci ildə Azərbaycanda da “Biometrik eyniləşdirmə sisteminin yaradılması haqqında” Dövlət Proqramı qəbul olunmuşdur [15]. Hesab etmək olar ki, yaxın gələcəkdə on-layn biometrik servislərin tətbiqi cəmiyyətin təhlükəsizliyinin yüksək səviyyədə təmin olunması üçün geniş imkanlar yaradacaqdır.

Milli eyniləşdirmə sisteminin iki vacib elementinin - biometrik eyniləşdirmə sisteminin və elektron imza infrastrukturunun yaradılması, onların imkanlarının səmərəli şəkildə birləşdirilməsi və istifadəsi təkcə bu problemin həllində deyil, ümumiyyətlə, informasiya məkanının təhlükəsizliyinin təmin edilməsində mühüm rol oynayacaq.

Cəmiyyətin informasiya təhlükəsizliyinin təmin olunmasında İnternet provayderlərinin də rolu böyükdür və onların üzərinə mühüm vəzifələr qoyulur. Bu gün ölkə üzrə təxminən 40-a yaxın provayder tərəfindən İnternet xidmətləri göstərilir. Cəmiyyətin informasiya təhlükəsizliyi, əsasən, bu provayderlərdən və onların administratorlarından asılıdır. Ona görə də İnternet-provayderlərin və administratorların cəmiyyət qarşısında məsuliyyəti hüquqi mexanizmlərlə təsbit olunmalıdır. İnformasiya cəmiyyəti məsələlərinə həsr olunmuş Ümumdünya Sammitinin yekun Bəyannaməsində, beynəlxalq qurumların, Avropa Birliyinin və inkişaf etmiş ölkələrin qəbul etdiyi hüquqi sənədlərdə spamlarla, viruslarla, ziyanlı kontentlərin yayılmasına qarşı mübarizə məqsədi ilə şəbəkə operatorları və İnternet-provayderlərin qarşısında mühüm vəzifələr qoyulur. Spamlarla, viruslarla, ziyanlı kontentlərlə mübarizə şəbəkə operatoru və provayderlər səviyyəsində aparılarsa, çox az vəsait hesabına kompyuterləri viruslardan mühafizə etmək olar. Bununla yanaşı, beynəlxalq təcrübəyə əsaslanaraq şəbəkə operatorlarının və provayderlərinin maliyyələşdirməsi mexanizmlərinin işlənilməsinə də xüsusi diqqət yetirilməlidir [17].

Mühüm məsələlərdən biri də elektron dövlət proqramlarının reallaşdırılması zamanı təhlükəsizlik məsələlərinin təmin edilməsidir. Həyata keçirilən elektron dövlət proqramlarının məqsədlərinə hakimiyyət orqanlarının fəaliyyətində şəffaflığın təmin olunması, səmərəliliyin yüksəldilməsi, informasiya azadlığının, demokratiyanın inkişafı və insan hüquqlarının təmin olunması, vətəndaşların (fiziki imkanlarından asılı olmadan) dövlətin idarə edilməsində yaxından iştirakı, onlayn mühitdə dövlət xidmətlərinin göstərilməsi, təhlükəsizliyinin təmin olunması və s. aid etmək olar.

E-dövlət proqramlarının həyata keçirilməsi üçün texniki və inzibati-hüquqi xarakter daşıyan bir sıra məsələlər həll olunmalıdır. Bunların arasında idarələrarası qarşılıqlı əlaqə reqlamentlərinin hazırlanması, dövlət xidmətlərinin təsnifatının yaradılması, eləcə də, vahid texniki arxitekturun qurulmasını, proqram-aparat platformasının reallaşdırılmasını və informasiya təhlükəsizliyinin təmin olunmasını göstərmək olar.

Ölkəmizdə formalaşan informasiya cəmiyyətinin bir seqmenti də e-elmdir. E-elmin şəbəkə platforması *AzScienceNet* Elm kompyuter şəbəkəsi *UNESCO*-nun xüsusi komissiyasının tövsiyəsi ilə *AMEA*-nın üzvlüyü çərçivəsində *TERENA*-da (Trans-Avropa Elmi-tədqiqat və Təhsil Şəbəkə Assosiasiyası) qeydiyyatda alınmışdır [18]. Bunun nəticəsində Azərbaycan elmi qurumlarının Avropa və beynəlxalq elmi şəbəkələrə inteqrasiyasının həyata keçirilməsi üçün əlverişli zəmin yaranmışdır. *AzScienceNet* şəbəkəsinin infrastrukturunun genişlənməsi, təhlükəsizlik və monitoring sisteminin etibarlı şəkildə qurulması, *DATA* mərkəzinin yaradılması, açıq *grid*, *cloud computing* və *eduroam* servislərinin tətbiqi, videokonfrans sisteminin təşkili, beynəlxalq səviyyədə və digər ölkələrdə fəaliyyət göstərən müvafiq elmi şəbəkə qurumları ilə inteqrasiya istiqamətində kompleks işlərin həyata keçirilməsinə kömək edir. Bu baxımdan, *AzScienceNet*-in informasiya təhlükəsizliyinin təmin olunması da mühüm əhəmiyyət kəsb edir. Bu məqsədlə *AMEA* İnformasiya Texnologiyaları İnstitutunda *AzScienceNet*-in “İstifadə siyasəti” və “İnformasiya təhlükəsizliyi siyasəti” işlənmiş və şəbəkənin təhlükəsizliyinin təmin olunması üçün kompleks tədbirlər həyata keçirilir. Həmçinin *AzScienceNet*-in monitoring və təhlükəsizlik xidməti təşkil olunmuş, şəbəkə mühiti üçün *Az-CERT* komandası yaradılmışdır və hal-hazırda fəaliyyət göstərir [19]. Eyni zamanda, *AzScienceNet* institutda informasiya təhlükəsizliyi sahəsində aparılan elmi tədqiqatların tətbiqi üçün eksperimental baza rolunu oynayır.

Hal-hazırda informasiya resurslarından və texnologiyalarından cinayət və terror məqsədləri ilə istifadə etməyin qarşısının alınması, insan hüquqlarının qorunması, o cümlədən, fərdi məlumatların toxunulmazlığı və söz azadlığının təmin olunması da aktualıq kəsb edir. İnsan haqlarının qorunması ilə yanaşı, İnternetdə terrorizmin bütün formaları və təzahürlərinə qarşı mübarizə aparılmalı, rəqəmsal bərabərsizliyin aradan qaldırılması üçün ciddi tədbirlər görülməlidir. Eləcə də, gənc nəslin şəxsiyyət kimi formalaşmasında, məhdud imkanlı insanların problemlərinin, gender məsələsinin həllində İKT-nin rolunun artırılması cəmiyyətin inkişafında informasiya təhlükəsizliyinin təmin olunmasını mühüm məsələ kimi ön plana çıxarır. Bütün bunlar nəzərə alınaraq, Azərbaycanın hüquqi sistemi də beynəlxalq səviyyədə virtual məkana dair qəbul olunmuş normativ sənədlərin tələblərinə uyğunlaşdırılmışdır.

Ölkəmizdə informasiya cəmiyyətinin inkişafı yeni keyfiyyət mərhələsinə – elektron tranzaksiyaları, elektron xidmətləri dəstəkləyən, aparıcı dövlətlərin təcrübəsinə əsaslanan elektron dövlətin formalaşması mərhələsinə qədəm qoymuşdur. Ona görə də elektron dövlətin dayanıqlı və təhlükəsiz fəaliyyətini təmin etmək məqsədi ilə vətəndaşlara dövlət orqanları tərəfindən göstərilən elektron xidmətlər və interaktiv münasibətlər yüksək informasiya təhlükəsizliyi tələblərinə cavab verməlidir. Bunun üçün də dövlət, elm, biznes və vətəndaş sektorlarında fəaliyyət göstərən müvafiq qurumlar ölkəmizdə formalaşmaqda olan informasiya cəmiyyətinin təhlükəsizliyinin təmin olunması işlərində səylərini, intellektual potensialını səfərbər etməli və qarşıda duran vəzifələri birgə həll etməlidirlər.

Nəticə

İnformasiya cəmiyyəti inkişaf etdikcə elektron dövlətin yaradılması prosesində vahid və çoxsəviyyəli ümumdövlət informasiya təhlükəsizliyi sisteminin yaradılması zərurəti meydana çıxır. Ümumiyyətlə, informasiya cəmiyyətinin formalaşdırılması ölkələrin informasiya təhlükəsizliyini təmin etmək, immunitetini artırmaq, müxtəlif təbiətli və miqyaslı təhlükələrlə təkbaşına mübarizə aparmağı xeyli çətinləşdirir. Ona görə də qlobal informasiya təhlükəsizliyi mühitini formalaşdırmaq bütün ölkələrin, ictimai birliklərin, biznes sektorunun və vətəndaşların marağında olmalıdır. Ən əsası, ölkələrin informasiya təhlükəsizliyinin təmin olunmasında vəzifə və məsuliyyət bölgüsü müəyyənləşdirilməlidir. Hər bir korporativ informasiya fəzasının öz *CERT* komandası yaradılmalı və dövlət, biznes və vətəndaş cəmiyyəti sektorlarının qarşılıqlı inam mexanizmləri əsasında üfüqi və şaquli münasibətlər qurulmalıdır. Beynəlxalq təcrübəyə əsaslanaraq ölkə üzrə informasiya təhlükəsizliyinin vəziyyətinin monitoringinin (statistikasının)

aparılması üçün indikatorlar işlənilməli, təhlillər aparılmalı və səmərəli qərarların qəbul edilməsi üçün mexanizmlər yaradılmalıdır.

Ədəbiyyat

1. Создание глобальной культуры кибербезопасности, 2002, <http://www.un.org>
2. Global Cybersecurity Agenda, 2008, <http://www.itu.int>
3. Lisbon Summit Declaration, 20 November 2010, , <http://www.nato.int>
4. «İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında» Azərbaycan Respublikasının Qanunu, 3 aprel 1998-ci il, <http://www.e-qanun.az>
5. «Dövlət sirri haqqında» Azərbaycan Respublikasının Qanunu, 7 sentyabr 2004-cü il, <http://www.mia.gov.az>
6. «Elektron sənəd və elektron imza haqqında» Azərbaycan Respublikasının Qanunu, 9 mart 2004-cü il, <http://www.e-qanun.az>
7. «Elektron ticarət haqqında» Azərbaycan Respublikasının Qanunu, 10 may 2005-ci il, <http://www.e-qanun.az>
8. «İnformasiya əldə etmək haqqında» Azərbaycan Respublikasının Qanunu, 30 sentyabr 2005-ci il, <http://www.ikt.az>
9. «Telekommunikasiya haqqında» Azərbaycan Respublikasının Qanunu, 14 iyun 2005-ci il, <http://www.e-qanun.az>
10. «AR-nın Milli təhlükəsizlik konsepsiyası», 23 may 2007-ci il, <http://www.mns.gov.az>
11. Əliyuliyev R.M., Valehov C.F., Mahmudov R.Ş. İnternet-jurnalistikanın formalaşmasının bəzi aspektləri. Ekspres-informasiya. İnformasiya cəmiyyəti seriyası. Bakı: «İnformasiya Texnologiyaları» nəşriyyatı, 2008, 32 səh.
12. The Universal Declaration of Human Rights, <http://www.un.org>
13. «Fərdi məlumatlar haqqında» Azərbaycan Respublikasının Qanunu, 4 iyun 2010-cu il, <http://www.e-qanun.az>
14. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, <http://www.conventions.coe.int>
15. «Biometrik eyniləşdirmə sisteminin yaradılması haqqında 2007-2012-ci illər üçün Dövlət Proqramı», 13 fevral 2007-ci il, <http://www.migration.gov.az>
16. World Summit on the Information Society, <http://www.itu.int/wsis>
17. Əliyuliyev R.M., Mahmudov R.Ş. İnternetin tənzimlənməsi problemləri. Ekspres-informasiya. İnformasiya cəmiyyəti seriyası, Bakı: «İnformasiya Texnologiyaları» nəşriyyatı, 2010, 115 səh.
18. AzScienceNet Elm kompyuter şəbəkəsi, <http://www.terena.org>
19. AZ-CERT, <http://www.cert.az>

УДК 004.9:351

Алгулиев Расим М.¹, Имамвердиев Ядигар Н.², Юсифов Фархад Ф.³

Институт Информационных Технологий НАНА, Баку, Азербайджан

¹secretary@iit.ab.az, ²yadigar@lan.ab.az, ³farhadysuifov@gmail.com

Некоторые концептуальные подходы к информационной безопасности общества

В данной статье были исследованы механизмы по обеспечению информационной безопасности в мировой практике, а также рассмотрены особенности по направлению формирования национальной нормативно-правовой базы и даны рекомендации в этой области. Как один из важных компонентов безопасности общества были определены основные функции информационной безопасности, выявлены существующие угрозы и их цели, а также даны предложения и рекомендации по обеспечению информационной безопасности общества.

Ключевые слова: *информационная безопасность, информационное общество, электронная наука.*

Rasim M. Alguliev¹, Yadigar N. Imamverdiyev², Farhad F. Yusifov³

Institute of Information Technology of ANAS, Baku, Azerbaijan

¹secretary@iit.ab.az, ²yadigar@lan.ab.az, ³farhadysuifov@gmail.com

Some conceptual views on information security of the society

Mechanisms existing in the international practice on ensuring information security were studied, the work done in the direction of formation of a national legal and regulatory base in this area was investigated and proposals were put forward. As one of the-key component of security of the society, the duties of information security were specified, existing threats and their targets were investigated, proposals and recommendations to ensure information security of the society were put forward.

Keywords: *information security, information society, electronic science*