Dayanıqlı, etibarlı və təhlükəsiz elektron dövlətin formalaşmasına bəzi konseptual yanaşmalar

Fərhad Yusifov

AMEA İnformasiya Texnologiyaları İnstitutu
farhadyusifov@gmail.com

***Xülasə*— Elektron dövlət sisteminin informasiya təhlükəsizliyinin təmin olunması məsələləri araşdırılır. Elektron dövlətin təhlükəsizliyinə olan təhdidlər, potensial risklər və onların idarə olunması məsələləri tədqiq olunur. E-dövlətin informasiya təhlükəsizliyinin aktual problemləri müəyyən edilir.**

Açar sözlər*— *elektron dövlət, informasiya təhlükəsizliyi, təhdidlər, təhlükəsizlik riskləri

I. GİRİŞ

İnformasiya-kommunikasiya texnologiyalarının (İKT-nin) sürətli inkişafı cəmiyyətə fayda verdiyi kimi onun təhlükəsizliyinə də yeni təhdidlər, təhlükələr yaradır. Bu təhlükələr İnternetin sürətli inkişafı və yeni texnologiyaların tətbiqi ilə daha da dərinləşməkdədir. Elekrton dövlətin (e-dövlətin) inkişafını əsas hədəf kimi seçmiş dövlətlər üçün iki müxtəlif tendensiya xarakterikdir: bir tərəfdən qanunla hakimiyyət orqanlarının açıqlığı təmin olunur, digər tərəfdən isə açıqlığın artması dövlətə yeni təhdilərin və risklərin yaranmasına gətirib çıxarır. Bu da dövləti yeni normativ hüquqi aktların qəbuluna, eləcə də, informasiya təhlükəsizliyinin təmin olunması istiqamətində təşkilati və texniki məhdudiyyətlərin qoyulmasına məcbur edir.

Mühüm məsələlərdən biri də elektron dövlət proqramlarının realizəsi zamanı təhlükəsizlik məsələləridir. Həyata keçirilən e-dövlət proqramlarının məqsədlərinə hakimiyyət orqanlarının fəaliyyətində şəffaflığın təmin olunması, hakimiyyət orqanlarının səmərəliliyinin yüksəldilməsi, informasiya azadlığının, demokratiyanın inkişafı və insan hüquqlarının təmin olunması, vətəndaşların hakimiyyət (fiziki imkanlarından asılı olmadan) strukturlarında yaxından iştirakı, dövlət xidmətlərinin onlayn mühitdə göstərilməsi, təhlükəsizliyinin təmin olunması və s. aid etmək olar.

E-dövlət proqramının 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 arxitektura, aparat-proqram platformasının reallaşdırılmasını və informasiya təhlükəsizliyi təmin olunmasını göstərmək olar.

E-dövlətin formalaşdırılmasını müşayiət edən əsas problemlərdən biri informasiya təhlükəsizliyinin təmin olunmasıdır [1,2]. Başqa sözlə, informasiya təhlükəsizlyi və kibertəhlükəsizlik sahəsində əsas problemlərdən biri e-dövlət sisteminin təhlükəsizliyinin təmin olunması məsələsidir. E-dövlətin infrastrukturunun təhlükəsizliyinə olan təhdidlər geniş əhatəyə malikdir. Bu təhdilər daxili, xarici və obyektiv xarakterili, məsələn, texnogen mənşəli fövqəladə hallarda informasiyanın məhv olması, itirilməsi və s. ola bilər. Bu səbəbdən e-dövlətin informasiya təhlükəsizlinin təmin olunması sistemlərinin layihələndirilməsində kompleks yanaşma əsas götürülür.

II. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ

Hər hansı ölkədə informasiya təhlükəsizliyinin prioritetləri dövlətin, cəmiyyətin və vətəndaşların maraqlarının balanslı nisbəti əsasında müəyyənləşir. Ölkədəki siyasi, hərbi, fövqəladə və s. vəziyyətlərdən asılı olaraq bu nisbət dəyişə bilər. Cəmiyyətin təhlükəsizliyinin əsas komponentlərindən biri kimi informasiya təhlükəsizliyinin vəzifələri informasiyanın konfidensiallığı, informasiyanın tamlığı, informasiyanın əlyetərliliyi və ziyanlı kontentlərlə mübarizədir.

İnformasiya təhlükəsizliyinin təmin edilməsi sistematik, kompleks yanaşma tələb edir. Bu sahədə əlaqədar qurumlar tərəfindən konseptual, təşkilati, elmi-metodoloji, qanunvericilik, maddi-texniki əsasların yaradılması üzrə işlər aparılmalıdır [3,4]. Dövlətin informasiya təhlükəsizliyinin təmin olunması üçün zəruri olan tədbirlər kimi beynəlxalq hüquqi mexanizmlərin ciddi araşdırılması, milli normativ-hüquqi bazanın formalaşdırılması, təhlükəsizlik siyasətinin işlənilməsi və reallaşdırılması, xüsusi texnologiyaların tətbiqi, ölkə və korporativ səviyyədə informasiya təhlükəsizliyinin monitorinqi və menecmentinin aparılması, kadr hazırlığı, əhalinin maarifləndirilməsi və vətəndaşlarda informasiya mədəniyyətinin tərkib hissəsi kimi informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması göstərilə bilər.

Ümumiyyətlə, informasiya təhlükəsizliyinin təmin olunması və eləcə də, zəruri tədbirlərin həyata keçirilməsi üçün beynəlxalq hüquqi mexanizmlərin, milli normativ-hüquqi bazanın formalaşdırılması mühüm əhəmiyyət kəsb edir 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 işlənilmişdir. Onların sırasında 2002-ci ildə BMT tərəfindən qəbul etmiş Qlobal İnformasiya Təhlükəsizliyi Mədəniyyəti haqqında Qətnaməni, 2008-ci ildə Beynəlxalq Telekommunikasiya İttifaqı tərəfindən qəbul olunmuş Qlobal İnformasiya Təhlükəsizliyi proqramını göstərmək olar [5,6]. Bununla yanaşı, 2010-cu ildə NATO-nun Lissabon sammitində qəbul olunmuş Bəyannamənin 40-cı maddəsinə əsasən 2012-ci ildə Full Operational Capability (FOC) mərkəzləşdirilmiş qurumunun yaradılması nəzərdə tutulurdu [7]. 2012-ci ildə Çikaqo və

2014-cü ildə Uels sammitlərində qəbul edilmiş bəyanamələrə əsasən qurum çoxmillətli əməkdaşlıq çərçivəsində fəaliyyətini daha da gücləndirməsi və NATO-nun bütün infrastrukturunun informasiya təhlükəsizliyinin təmin olunması istiqamətində 2016-cı ildə də təşəbbüslərin, səylərin birləşdirilməsi nəzərədə tutulur [8,9].

İnformasiya təhlükəsizliyi dövlət xidmətlərinin elektron formada göstərilməsinin mühüm komponentlərindən biridir. Dövlət xidmətlərinin vahid portalının yaradılması prosesində ola biləcək potensial təhdidlər analiz olunmaqla portaldan istifadə zamanı informasiyanın təhlükəsizliyinin təmin olunması üçün tələblər formalaşdırılmalıdır. Təcrübədə "bir pəncərə" prinsipi əsasında qurulan dövlət portalarının təhlükəsizlik sistemində çox sayda təhlükəsizlik mexanizmlərindən istifadə olunur. Belə mexanizmlər kimi şəbəkəarası ekranlar, kontentin analizi vasitələri, informasiyanın mühfizəsi üçün antivirus proqramları, veb-analitika, mühafizənin monitorinqi və idarə olunması vasitələri, istifadəçi profillərinin monitorinqi və s. göstərilə bilər [1,4].

İnformasiya təhlükəsizliyinin lazımi səviyyədə təmin olunması üçün ilk növbədə vətəndaşların fərdi məlumatlarının təhlükəsizliyinin təmin olunması e-dövlət proqramlarının həyata keçirilməsinədə öndə gələn məsələlərdən biridir. Beynəlxalq təcrübədə e-dövlət layihələrinin uğur qazanmasında əsas amillərdən biri kimi fərdi məlumatların təhlükəsizliyi məsələsi göstərilir. Bu baxımdan e-dövlət layihələrinin həyata keçirilməsi dövlətlər üçün əsas prioritet hesab olunsada informasiya təhlükəsizliyi məsələsinə çox ciddi yanaşılmalıdır.

E-dövlətin infrastrukturunun formalaşdırılmasına külli miqdarda vəsait qoyulsa da, göstərilən xidmətlərin sayından və əhatə dairəsinin asılı olmayaraq e-dövlət sisteminin funksionallığının və effektivliyinin təmin olunması üçün bir sıra mühüm problemlərin həlli əhəmiyyət kəsb edir [1,3].

E-dövlət xidmətlərindən istifadə edərkən vətəndaşlar əsas istəkləri yüksək keyfiyyətli xidmət almaq, informasiyanın tam əlyetərli olması və mümkün olan ən yüksək səviyyədə təhlükəsizliyin təmin edilməsidir. Təbiidir ki, belə olan halda əsas diqqət e-dövlətin təhlükəsizliyi və zəifliyi məsələlərinə yönəlir [1].

Zəiflik anlayışının müxtəlif mənaları olsa da ümumilikdə, sistemin prosedurlarında, layihəsində, realizəsində, daxili nəzarətində səhvlər və ya zəifliklər nəticəsində meydana çıxır və çox hallarda sistemin təhlükəsizlik siyasətinin pozulması üçün istifadə edilə bilər. Məlumdur ki, istənilən sistemə təhdidlər əsasən 4 istiqamətdə ola bilər: proqramlar, texniki vasitələr, kommunikasiya, giriş və çıxış. Bununla yanaşı, bir sıra amillər vardır ki, sistemdə zəifliklərə təsir edir. Onların sırasında texniki və texnoloji, insan, sosial, siyasi, iqtisadi və şəbəkə amilləri xüsusilə qeyd olunmalıdır [1,3,4].

E-dövlətin informasiya təhlükəsizliyinə əsas təhdidlər aşağıdakılardır [2-4,10]:

- E-dövlət sisteminə müdaxilələr, informasiyanın konfidensiallığının, tamlığının və əlçatanlığının pozulmasına yönəlmiş xarici dövlətlərin xüsusi xidmət orqanlarının, təşkilat və qrupların, ayrı-ayrı şəxslərin qanunsuz fəaliyyəti;
- Başqa ölkələrdə istehsal olunmuş aparat və proqram vasitələrinin məcburi istifadəsi;
- İnformasiyanın toplanması, emalı və ötürülməsinə qoyulan tələblərin qəsdən və ya bilməyərəkdən pozulması, texniki sistemlərin və proqram təminatlarının sıradan çıxması;
- İnformasiya təhlüksəsizliyi tələblərinə cavab verməyən və lisenziyasız sistemlərin istifadəsi;
- İnformasiya sistemlərinin yaradılması və inkişaf etdirilməsi işinə bu cür fəaliyyətlə məşğul olmağa dövlət lisenziyası olmayan təşkilat və ya firmaların cəlb olunması və s.

Potensial təhdidlərin daxili, xarici və obyektiv xarakterli ola biləcəyi nəzərə alınaraq e-dövlətin informasiya təhlükəsizliyi sisteminin dayanıqlığının təmin edilməsi sistemli, kompleks yanaşma tələb edir.

III. İNFORMASİYA SAHƏSİNDƏ DÖVLƏTİN TƏHLÜKƏSİZLİYİNƏ TƏHDİDLƏR

XXI əsrdə dünya informasiya fəzasının əsasını inkişaf etmiş ölkələrin, o cümlədən ABŞ, ÇXR, Qərbi Avropa ölkələri, Cənubi Koreya və Yaponiya kimi ölkələrin milli informasiya infrastrukturları təşkil edir. İnformasiyalaşdırmanın texnoloji imkanlarının artması cəmiyyətin həyati əhəmiyyətli sahələrində - telekommunikasiya, e-dövlət, nəqliyyat, bank sistemi, müdafiə və milli təhlükəsizlik və s. tətbiq imkanlarını genişləndirir. Bununla yanaşı, informasiya sistemlərinin və texnologiyalarının sürətli inkişafı dünya iqtisadi sisteminə inteqrasiya prosesində dövlətə aşkar olunmayan, gizli təhdidlər yaradır. Bu təhdidlər vətəndaşalara e-dövlətin fəaliyyətinin genişləndrilməsi, onlayn dövlət xidmətlərinin göstərilməsi və resursların əlyetərli olması ilə daha da artmaqdadır. Beynəlxalq təcrübədə lider ölkələrin hərbi-siyasi sahədəki fəaliyyətlərinin analizi göstərir ki, hazırda əsas diqqət kiberfəzanın təhlükəsiliyinə yönəldilib [3,4,10].

Ümumilikdə bütün kibertəhdidləri 3 qrupa ayırmaq olar: haker, kriminal və xüsusi xidmət orqanları tərəfindən kibertəhdidlər. Elektron təhdidlərin sayının artması və miqyasının fasiləsiz transformasiyası ölkə üzrə vahid informasiya mühitinin müdafiəsi mərkəzinin yaradılmasını zəruri edir. Hazırda qabacıl ölkələrdə bu sahədə normativ hüquqi bazanın formalaşdırılması, ölkə üzrə informasiya təhlükəsizliyinin təmin olunmasının vahid standartının yaradılması və s. ciddi araşdırmalar aparılır.

Son illərdə xüsusən lider ölkələrdə informasiya müharibəsinin komponenti kimi informasiya-psixoloji silahların yaradılması sahəsində fəaliyyətlərini gücləndirmişlər. Mütəxəssilərin fikrincə bu silah informasiyanın ələ keçirilməsi və ya məhv edilməsi, istifadəçilərin əlyetərliliyinin məhdudlaşdırılması, kompüter sistemlərinin və ya şəbəkənin işinə müdaxiləyə və s. imkan verir və bütövlükdə cəmiyyətin, dövlətin həyati əhəmiyyətli sahələrinə potensial təhdid hesab olunur [4].

E-dövlət sisteminin inkişafı və göstərilən elektron xidmətlərin sayının sürətlə artması terrorçular üçün potensial yeni imkanlar yaranmış oldu. Bu cür təhdidlər kimi dövlət

strukturları ilə göstərişli polemikalar, qərəzli ideyaların təbliği, vətəndaşlarla hakimiyyət orqanları arasında müxtəlif qarşıdurmaların yaranmasını hədəf alan fəaliyyətlər və s. misal göstərilə bilər.

Hazırda müxtəlif xüsusi xidmət orqanları tərəfindən sosial şəbəkələrin analizi, gizli şəbəkələrin aşkarlanması istiqamətində aparılan işlər, dezinformasiyanın yayılması və s. cəmiyyətin idarə olunmasına cəhdlər kimi qiymətləndirilir və dövlətə birbaşa potensial təhdid hesab olunur.

Dövlətin informasiya təhlükəsizlinə əsas təhdidlər həyati əhəmiyyətli müxtəlif sahələrdə, o cümlədən iqtisadi, daxili siyasət, elm və texnika, e-dövlət, informasiya və kommunikasiya sistemləri, müdafiə, hüquq mühafizəsi, məhkəmə və s. göstərilə bilər [3,4,10,11].

Ölkəmizdə də, İnformasiya təhlükəsizliyi məsələləri milli təhlükəsizliyin əsas tərkib hissələrindən biridir və bu sahədə normativ-hüquqi bazanın formalaşması informasiya cəmiyyəti quruculuğunda prioritet məsələlərdən hesab olunur. Azərbaycanda informasiya təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasının formalaşdırılması və inkişaf etdirilməsi istiqamətində bir sıra mühüm qanunlar, normativ aktlar, fərman və sərəncamlar qəbul edilmişdir [12].

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 təcrübə nəzərə alınaraq ölkəmiz Avropa Şurasının 1981-ci il tarixli "Fərdi məlumatların avtomatlaşdırılmış sistemlərdə emalı vaxtı fiziki şəxslərin qorunması haqqında" Konvensiyasına (108 saylı Konvensiya) qoşulmuşdur [14].

2012-ci ildə qəbul edilmiş "Azərbaycan 2020: gələcəyə baxiş" inkişaf konsepsiyasında e-dövlət quruculuğu, effektli idarəetmənin formalaşdırılması və informasiya təhlükəsizliyinin təmin edilməsi prioritet istiqamətlər kimi göstərilmişdir. Konsepsiyaya informasiya təhlükəsizliyi sahəsində kiberhücumların qarşısının alınması, informasiyanın mühafizəsi, dövlət orqanlarının informasiya resurslarının və sistemlərinin mümkün təhdidlərdən qorunması, kibertəhlükəsizlik sahəsində ümummilli hazırlığın qaldırılması və maarifləndirmənin genişləndirilməsi kimi mühüm məsələlər daxil edilmişdir [15].

2014-cü ildə qəbul edilmiş "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya"da milli təhlükəsizlik sahəsində fəaliyyətin səmərəliliyi atırılması istiqamətində müvafiq qurumlar qarşısında mühüm vəzifələr qoyulmuşdur [16].

IV. E-DÖVLƏTİN TƏHLÜKƏSİZLİK RİSKLƏRİNİN İDARƏ OLUNMASI

E-dövlət layihələrinin həyata keçirilməsi prosesində e-dövlət sisteminin təhlükəsizliyi probleminin necə həll edilməsi olduqca aktual məsələdir. E-dövlətin təhlükəsizlik risklərinin idarə olunması proseduralarının analizi üç aspektdə aparılır: risklərin identifikasiyası, riskin analizi və idarə olunması [11,17,18]. Hazırda informasiya texnologiyalarının sürətli inkişafı ilə risklərin idarə olunması sistemlərinin daha etibarlı olması e-dövlət sistemlərinin təhlükəsizliyinin təmin olunması üçün effektiv vasitə hesab olunur.

Ümumiyyətlə, e-dovlətin təhlükəsizlik riskləri aşağıdakı kimi təsnif oluna bilər [17,18]:

- informasiyanın ələ keçirilməsi;
- informasiyanın saxtalaşdırılması;
- xidmətlərdən imtina,
- sistem resurslarının oğurlanması;
- resurslara müdaxilələr.

Risklərin identifikasiyası – risklərin idarə olunmasının birinci mərhələsi olmaqla e-dövlətin təhlükəsizliyi sahəsində risklərin effektiv qiymətləndirilməsi məqsədi daşıyır. E-dovlət sisteminin təhlükəsizlik tələbləri risklərin qiymətləndirmə sistemi tərəfindən təsdiqlənir. Müvafiq təhdilərin, boşluqların və əks-tədbirlərin toplanması əsasında e-dövlət sisteminin mümkün riskləri və ya potensial təhdidlər müəyyən olunaraq risklər identifikasiya edilir.

Risklərin identifikasiya etmək üçün müxtəlif növ metodlar vardır. Risklərin identifikasiyasının məqsədi şəbəkə mühitində, verilənlərdə və ya verilənlərin mübadiləsində mövcud olan risklərin tanınmasıdır. Qeyd etmək lazımıdır ki, risklərin identifikasiya olunması hələ e-dövlət sisteminin risklərini hamısı demək deyil.

Müxtəlif növ kəmiyyət və keyfiyyət metodlarının köməyi ilə risklərin analizi e-dövlət riskinin bütün mühüm faktorlarının müəyyən olunmasına imkan verir [3,11,10,17,18]. Risklərin analizi prosesində təhdidlərin müəyyən olunması və mənbəyinin təyini vacib məsələlərdir. Təhdidlərin mümkün mənbələri kimi məqsədli, qəsdən törədilən (məsələn, haker, terrorçu tərəfindən), məqsədli olmayan (məsələn, istifadəçilər tərəfindən) və təbii təhlükələr (məsələn, zəlzələ, təbii fəlakət) göstərilə bilər.

Risklərin idarə olunması müxtəlif metodlardan istifadə olunmaqla risklərin mükün qədər azaldılması və müəyyən olunmuş həddə saxlanımasına zəmanət verir. E-dövlətin təhlükəsizlik risklərinin idarə olunması e-dövlət sistemlərinin funksionallığının saxlanması və risklərin mümkün qədər minimallaşdırılmasına imkan verir. Bununla yanaşı qeyd etmək lazımdır ki, risklərin idarə olunması üçün qəbul olunmuş mükəmməl, standart qaydalar yoxdur. E-dövlətin təhlükəsizlik risklərinin idarə olunması üçün birinci addım e-dövlət sisteminin daxili və xarici mühiti analiz edilməli və aşkarlanmalı, eləcə də, sistemin zəif tərəfləri və boşluqları yoxlanmalıdır. Risklərin qarışısını almaq və itkilərin mümkün qədər azaltmaq üçün mütəmadi duzəlişlər və ya yeni qurğuların əlavə olunması həyata keçirilməlidir. Hər bir tətbiq mərhələsində planların və göstəricilərin izlənməsi, monitorinqi aparılmalıdır.

E-dövlətin informasiya təhlükəsizliyin təmin olunmasının aktual məsələlərini aşağıdakı kimi təsnif etmək olar:

- E-dövlətin dayanıqlı fəaliyyətinin təmin edilməsinin konseptual əsaslarının işlənməsi;
- E-dövlətin informasiya təhlükəsizliyi təmini və idarə olunması üçün konseptual-arxitektur modellərin işlənməsi;
- E-dövlətin intellektual monitorinqi sisteminin işlənilməsi;

- İnformasiya təhlükəsizliyi risklərinin analizi və idarə olunması üçün modellərin işlənməsi;
- Kibercinayətkarlığa qarşı mübarizə texnologiyalarının işlənməsi;
- E-dövlət mühitinə təhlükə yaradan qeyri-aşkar kriminal sosial şəbəkələrin aşkarlanması və analizi metodlarının işlənməsi;
- Korporativ şəbəkə mühitinin verilənlərin intellektual analizi texnologiyaların köməyi ilə spamlarla və digər ziyanlı kontentlərlə mübarizə metodları və alqoritmlərinin işlənməsi;
- E-dövlət mühitində fərdi məlumatların qorunması və istifadəçilərə yönəlik mühafizə mexanizmlərinin işlənməsi;
- E-dövlət mühitində Kompüter İnsidentləri üzrə Yardım Komandalarının (Computer Emergency Response Team, CERT) şəbəkəsinin yaradılması;
- Onlyn mühitində informasiya müharibəsi, informasiya hücumu və informasiya hücumundan müdafiə texnologiyalarının araşdırılması, yeni metodların və alqoritmlərin işlənməsi.

Təcrübə göstərir ki, e-dövlət layihələrinin uğurlu olması e-dövlətin etibarlı informasiya təhlükəsizliyinin təmin edilməsindən birbaşa asılıdır. İnformasiya təhlükəsizliyi e-dövlətin effektivliyinə və vətəndaşların dövlətə xidmətlərinə inamına böyük ölçüdə təsir edir. Bu baxımdan e-dövlətin formalaşdırılması prosesində cəmiyyətin, dövlətin vahid informasiya təhlükəsizliyinin sisteminin yaradılması aktual məsələ kimi qarşıya çıxır.

Aydındır ki, e-dövlətin təhlükəsizliyinə qoyulan tələblər informasiya texnologiyaları inkişaf etdikcə daha da artmaqdadır və getdikcə daha yüksək tələblər irəli sürülür. Bu səbəbdən e-dövlətin təhlükəsizlik risklərinin analizi və idarə edilməsi böyük əhəmiyyət kəsb edir. Hazırda təhlükəsizlik risklərin analizi və idarə olunması sistemlərinin dayanıqlı, etibarlı olması e-dövlət sistemlərinin təhlükəsizliyinin təmin olunması üçün effektiv vasitə hesab olunur.

NƏTİCƏ

E-dövlət quruculuğunu prioritet kimi qəbul etmiş ölkələrdə informasiya təhlükəsizliyini təmin etmək, etibarlı mühit formalaşdırmaq, müxtəlif təbiətli və miqyaslı təhlükələrlə təkbaşına mübarizə aparmaq xeyli çətinləşir və ona görə də qlobal informasiya təhlükəsizliyi mühitini yaratmaq bütün ölkələrin, vətəndaş cəmiyyətinin, şirkətlərin və insanların marağında olmalıdır. Bununla yanaşı, e-dövlətin formalaşdırılması prosesində vahid və çoxsəviyyəli ümumdövlət informasiya təhlükəsizliyi sisteminin yaradılması aktual məsələ kimi qarşıya çıxır.

Məqalədə e-dövlət sisteminin informasiya təhlükəsizliyinin təmin olunması məsələləri araşdırılmışdır. E-dövlətin informasiya təhlükəsizliyinə təhdidlər və potensial risklər analiz olunmuşdur. E-dövlətin informasiya təhlükəsizliyinin aktual problemləri şərh edilmişdir.

Qeyd etmək lazımıdr ki, informasiya təhlükəsizliyi sisteminin dayanıqlığının təmin edilməsi üçün hər bir korporativ informasiya fəzasının öz kompüter insidentləri üzrə komandası yaradılmalı və dövlət, biznes və vətəndaş cəmiyyəti sektorlarının qarşılıqlı inam mexanizmləri əsasında üfüqi və şaquli münasibətlər qurulmalıdır. E-dövlətin informasiya təhlükəsizliyinin vəziyyətinin monitorinqinin aparılması üçün indikatorlar sistemi işlənilməli və səmərəli qərarların qəbul edilməsi üçün mexanizmlər yaradılmalıdır.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun mailyyə yardımı ilə yerinə yetirilmişdir – **Qrant № EİF/GAM-2-2013-2(8)-25/03/1**

ƏDƏBİYYAT

[1] R. Alshboul, “Security and vulnerability in the e-Government society,” Contemporary Engineering Sciences, vol. 5, No. 5, pp. 215-226, 2012.

[2] Y.N. İmamverdiyev, “E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatlarin müasir vəziyyətinin analizi,” İnformasiya cəmiyyəti problemləri, №2(6), səh.19-26, 2012.

[3] A. AlKalbani, H. Deng, B. Kam, “A conceptual framework for information security in public organizations for s-Government development,” 25th Australasian Conference on Information Systems, 2014, pp. 1-11.

[4] М.И. Фалеев, Г.С. Черных, “Угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности,” Стратегия гражданской защиты: проблемы и исследования, том 4, № 1, стр. 21-34, 2014.

[5] Создание глобальной культуры кибербезопасности, 2002, www.un.org

[6] Global Cybersecurity Agenda, 2008, www.itu.int

[7] Lisbon Summit Declaration, 20 November 2010, www.nato.int

[8] Chicago Summit Declaration, 20 May 2012, www.nato.int

[9] Wales Summit Declaration, 5 September 2014, www.nato.int

[10] Y.N. İmamverdiyev, “E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli,” İnformasiya cəmiyyəti problemləri, №1(7), səh. 20-31, 2013.

[11] I. Alsmadi, “Security challenges for expanding e-Governments’ services,” International Journal of Advanced Science and Technology vol. 37, pp. 47-60, 2011.

[12] R.M. Əliquliyev, Y.N. Imamverdiyev, F.F. Yusifov, “Cəmiyyətin informasiya təhlükəsizliyinə dair bəzi konseptual baxışlar,” İnformasiya cəmiyyəti problemləri, №2, səh. 3-9, 2011.

[13] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, 4 iyun 2010-cu il, http://e-qanun.az

[14] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int

[15] “Azərbaycan 2020: gələcəyə baxış” inkişaf konsepsiyası, 29 dekabr 2012-ci il, www.president.az

[16] “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”, 2 aprel 2014-cü il, www.president.az

[17] Z. Zhou, C. Hu, “Study on the e-Government security risk management,” International Journal of Computer Science and Network Security (IJCSNS), vol.8, No.5, pp. 208-213, 2008.

[18] R.D. Choudhari, D.K. Banwet, M.P. Gupta, “Identifying risk factors in for E-governance Projects,” pp. 270-277,2007. www.csi-sigegov.org