UOT 004.9:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİ ÜZRƏ TƏDQİQATLARIN MÜASİR VƏZİYYƏTİNİN ANALİZİ

E-dövlət mühitində informasiya təhlükəsizliyinin təmin edilməsi və fərdi məlumatların qorunması e-dövlət texnologiyasının əsas problemləridir. E-dövlətin e-xidmətləri inkişaf etdikcə və genişləndikcə bu problemlər daha kəskin xarakter alır. Etibarlı informasiya təhlükəsizliyinin təmin edilməsi sistematik yanaşma, şəraitə adekvat və çevik idarəetmə modelləri tələb edir. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sahəsində elmi tədqiqatların müasir vəziyyəti analiz edilir və aktual tədqiqat problemləri seçilir.

Açar sözlər: *e-dövlət, e-xidmət, informasiya təhlükəsizliyi, informasiya təhlükəsizliyinin idarə edilməsi.*

Giriş

Müasir dövrdə informasiya-kommunikasiya texnologiyaları (İKT) cəmiyyət həyatının müxtəlif sahələrinə geniş tətbiq edilir və 1990-cı illərdən dünya ölkələrinin çoxunda bu sahədə müxtəlif miqyaslı proqramlar həyata keçirilir. Elektron dövlətin (e-dövlətin) qurulması proqramları ilə yanaşı, digər dövlət hakimiyyəti və yerli özünüidarəetmə orqanlarının da elektronlaşdırılması üzrə işlər aparılır, nəticədə, elektron dövlətə keçid baş verir. E-dövlətin formalaşması insanların yaşayış tərzini və təşkilatların fəaliyyət formalarını dəyişir, insanların həyatı və təşkilatların fəaliyyəti e-idarəçilikdən tamamilə asılı olur. Buna görə də e-dövlətin informasiya təhlükəsizliyi xüsusi əhəmiyyət daşıyır.

BMT 2001-ci ildən başlayaraq iki ildən bir üzv ölkələrin e-dövlət quruculuğu fəaliyyətini qiymətləndirir və ölkələrin reytinqini (e-dövlətin hazırlıq indeksini) müəyyənləşdirir [1]. Bir çox inkişaf etmiş və inkişaf etməkdə olan ölkələrdə e-dövlət quruculuğu təcrübəsi müxtəlif tədqiqatlarda analiz edilmişdir [2-4]. E-dövlət quruculuğunda qarşıya çıxan maneələr sırasında informasiya təhlükəsizliyi və fərdi məlumatların qorunması məsələlərinə daha tez-tez istinad edilir [5, 6].

Elmi tədqiqatlar və ölkələrin təcrübəsi göstərir ki, vətəndaşların e-dövlətə inamının vacib komponentlərindən biri e-dövlətin informasiya təhlükəsizliyidir [7, 8]. Vətəndaşlar təhlükəsizliyi şübhəli olan veb-saytdan istifadə etməkdənsə, ənənəvi üsullardan istifadə etməyi üstün tuturlar. Hazırda e-dövlətin informasiya təhlükəsizliyinin etibarlı təmin edilməsi e-dövlətin inkişafının yeni mərhələsində daha aktual problemə çevrilir.

İnformasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatlar 1970-ci illərin sonlarından başlanmışdır, 1990-cı illərin sonuna doğru ilk milli və beynəlxalq standartlar (*ISO/IEC 17799*) qəbul edilmişdir [9]. Lakin bu tədqiqatlar və standartlar informasiya təhlükəsizliyinin, əsasən, təşkilatlar səviyyəsində idarə edilməsini nəzərdə tutur. Son dövrlər informasiya təhlükəsizliyinin milli, regional və beynəlxalq səviyyələrdə idarə edilməsi məsələləri ön plana çıxır [10, 11]. Bu səviyyələrin hər biri informasiya təhlükəsizliyinin idarə edilməsi üçün özünəməxsus metodoloji bazanın işlənilməsini tələb edir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin strateji məqsədi e-dövlətin informasiya sistemlərinin mühafizəsi və onlayn biznes mühitinin təhlükəsizliyinin təmin edilməsidir [12]. Bu strateji məqsədin həyata keçirilməsinin mürəkkəbliyi e-dövlət mühitinin heterogenliyi, informasiya təhlükəsizliyinə daha yüksək tələblərin irəli sürülməsi, informasiya təhlükəsizliyinin təmin edilməsində iştirak edən tərəflərin maraqlarının balanslaşdırılmasında ziddiyyətlər, effektiv idarəetməyə əsaslanan vahid informasiya təhlükəsizliyi sisteminin yaradılmasının çətinliyi ilə şərtlənir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə elmi və praktiki tədqiqatlar nisbətən yaxın dövrlərdə meydana çıxmışdır. Eyni zamanda, e-dövlətin informasiya təhlükəsizliyi mühiti çox dinamik dəyişir, təhlükəsizliyə təhdidlər daim təkamül yolu keçir və mühafizə mexanizmləri yenilənir. Meydana çıxan yeni təhlükəsizlik çağırışlarına operativ cavab verilməsi informasiya təhlükəsizliyinin idarə edilməsinin təkmilləşdirilməsini, yeni idarəetmə modellərinin işlənməsini tələb edir. Bunu nəzərə alaraq, bu işdə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi sahəsində elmi-praktiki tədqiqatların müasir vəziyyəti analiz edilir, mövcud yanaşmaların üstün və çatışmayan cəhətləri müəyyən olunur və aktual tədqiqat problemləri seçilir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi

Tədqiqatlar göstərir ki, informasiya təhlükəsizliyinin təmin edilməsində texnoloji məsələlərlə yanaşı, qeyri-texnoloji məsələlər də olduqca vacibdir və e-dövlət, informasiya təhlükəsizliyi və idarəetmə (menecment) məsələləri arasında sıx əlaqələr mövcuddur [13].

İdarəetmə – məqsədlərin müəyyən edilməsi və resurslardan optimal istifadə etməklə bu məqsədlərə çatılmasıdır. *ISO/IEC 13335-1* standartı informasiya təhlükəsizliyinin idarə edilməsini konfidensiallığın, tamlığın, əlyetərliliyin, hesabatlılığın, autentikliyin və etibarlılığın müvafiq səviyyələrinin təmin edilməsi üçün proses kimi müəyyən edir [14].

Digər tərəfdən informasiya təhlükəsizliyinin idarə edilməsinin yetkinlik modeli *ISM3* (*Information Security Management Maturity Model*) informasiya təhlükəsizliyinin idarə edilməsini, informasiya sistemlərinin və onların dəstəklədiyi təşkilati proseslərin təhlükəsizliyini təhdid edən hücumların, səhvlərin və qəzaların qarşısını alan və onların nəticələrini aradan qaldıran sistem kimi nəzərdə tutur [15].

İnformasiya təhlükəsizliyinin idarə edilməsi risklərin identifikasiyası və risklərin nəticələrinin azaldılması üçün adekvat nəzarət mühitinin yaradılmasını təmin edir. Bəzi müəlliflərə görə, informasiya təhlükəsizliyi təhlükəsizlik siyasətini, risklərin analizini, risklərin idarə edilməsini, fəaliyyətin fasiləsizliyinin planlaşdırılmasını və qəzadan sonra bərpanı nəzərdə tutur və informasiya təhlükəsizliyinin idarə edilməsinə praqmatik baxış fəaliyyətin fasiləsizliyini təmin etmək, ziyanı minimallaşdırmaq və təhlükəsizlik üzrə fəaliyyəti xərclər baxımından effektiv təşkil etməkdən ibarətdir [16].

Hazırda təşkilatda informasiya təhlükəsizliyinin idarə edilməsində proses yanaşması geniş istifadə edilir. Proses yanaşması idarəetməyə proses – qarşılıqlı əlaqəli kəsilməz əməliyyatların toplusu kimi baxır. *ISO 27001* standartı *PDCA* (*Plan-Do-Check-Act*) tsiklik modelini informasiya təhlükəsizliyinin idarə edilməsi prosedurları üçün əsas kimi təsvir edir [17]. *PDCA* modelində informasiya təhlükəsizliyinin idarə edilməsi prosedurlarının hamısı ardıcıl olaraq dörd mərhələdən keçir: planlaşdırma – yerinə yetirmə – yoxlama – yaxşılaşdırma. Hər bir mərhələdə müxtəlif prosedurlar yerinə yetirilir. Qeyd etmək lazımdır ki, *PDCA* modeli informasiya təhlükəsizliyinin idarə edilməsi prosedurlarının həyat tsiklini təsvir edir, bu modeldə konkret idarəetmə prosedurları göstərilmir.

İnformasiya təhlükəsizliyinin idarə edilməsi hətta ən yaxşı praktiki təcrübəyə əsaslansa və beynəlxalq standartlara cavab versə belə, o, yalnız təşkilati proseslərlə dəstəkləndikdə effektli ola bilər. İnformasiya təhlükəsizliyinin idarə edilməsinin effektli olması üçün təşkilati fəaliyyət üzrə effektli idarəetmə qərarlarının qəbul edilməsi tələb edilir.

İnformasiya təhlükəsizliyinin idarə edilməsi planlaşdırma, təşkiletmə, əmrvermə, əlaqələndirmə və nəzarət funksiyalarını əhatə edir. İnformasiya təhlükəsizliyinin effektivliyinin qiymətləndirilməsi, onun baza səviyyəsi ilə müqayisə edilməsi, təhlükəsizliyin ölçülməsi və digər təşkilatlarla müqayisə edilməsi, təhlükəsizlik mədəniyyətinin formalaşdırılması, təhlükəsizliyin dinamik və fasiləsiz ölçülməsi məsələləri də informasiya təhlükəsizliyinin idarə edilməsi sahəsinə daxildir.

Yuxarıda sadalanan idarəetmə funksiyalarından da göründüyü kimi, informasiya

təhlükəsizliyinin idarə edilməsi təşkilat səviyyəsində də kifayət qədər mürəkkəb, kross-funksional fəaliyyətdir. Müəlliflərin bir çoxu razılaşır ki, təşkilatda informasiya təhlükəsizliyinin idarə edilməsi siyasət, standartlar, qaydalar, ən yaxşı təcrübələr toplusu, texnologiya, humanitar, hüquq və etik məsələlər kimi aspektləri əhatə edir [18].

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi təşkilat səviyyəsi ilə müqayisədə daha mürəkkəbdir və burada bir sıra keyfiyyət dəyişiklikləri müşahidə edilir. Bu məsələ texnoloji, siyasi, hüquqi, iqtisadi, sosial, mədəni, beynəlxalq aspektləri əhatə edir.

E-dövlət mühiti bir-biri ilə qarşılıqlı əlaqədə və əməkdaşlıqda olan, özünün müstəqil informasiya təhlükəsizliyi siyasətinə əməl edən dövlət və yerli özünüidarəetmə orqanları, özəl və beynəlxalq təşkilatlardan ibarətdir [19]. Bu mühitdə bir-birindən əhəmiyyətli dərəcədə fərqlənən müxtəlif təhlükəsizlik məqsədləri ola bilər. Əməkdaşlıq edən avtonom tərəflər öz təhlükəsizlik məqsədlərinə çatmaq üçün özəl təhlükəsizlik domenlərini yarada bilərlər.

Belə mühiti dəstəkləyən infrastrukturda heterogen aparat və proqram təminatı komponentləri, servislər, tətbiqi proqramlar ola bilər, o cümlədən verilənlər bazaları federasiyaları, çoxsəviyyəli təhlükəsiz idarəetmə sistemləri, çoxsəviyyəli təhlükəsiz əməliyyat sistemləri daxil ola bilər. Bu domenlərdə müxtəlif autentifikasiya və avtorizasiya platformaları istifadə edilə bilər, e-dövlət onların avtonomluğunu saxlamaqla onları inteqrasiya etməyə çalışır.

E-dövlətin informasiya təhlükəsizliyi sistematik şəkildə müxtəlif səviyyələrdə - e-xidmətlər, maraqlı tərəflər, istifadəçilər, şəbəkə (İnternet), İKT aktivləri səviyyəsində idarə edilməlidir. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsində maraqlı tərəflər kimi dövlət, nazirliklər, təşkilatlar, vətəndaşlar, iri şirkətlər, informasiya texnologiyaları istehsalçıları, beynəlxalq təşkilatlar çıxış edirlər.

E-dövlətin əsas məqsədi istifadəçilərə e-dövlət xidmətlərini istənilən yerdə və istənilən vaxt təqdim etməkdir. E-dövlət xidmətlərinin bir neçə kateqoriyası fərqləndirilir: e-idarəçilik, e-xidmətlər, e-kommersiya, e-qərar qəbuletmə (e-demokratiya). E-xidmətlərin təhlükəsizliyi elmi ədəbiyyatda, əsasən, texnoloji baxımdan analiz edilir [20, 21]. E-xidmətlərin təhlükəsizliyinə müxtəlif səviyyələrdə baxmaq olar:

- tətbiqi proqram səviyyəsinin təhlükəsizliyi;
- şəbəkə səviyyəsinin təhlükəsizliyi;
- verilənlərin təhlükəsizliyi.

E-dövlət xidmətlərinin təhlükəsizliyində əsas problemlər istifadəçilərin identifikasiyası, autentifikasiyası, avtorizasiyası, tranzaksiyaların imzalanması, açıq və konfidensial informasiyanın təhlükəsiz şəkildə saxlanması və emalı, konfliktlərin həlli, audit və s. ibarətdir.

Təşkilatda olduğu kimi, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsinə də üç müxtəlif səviyyədə baxmaq olar: strateji, taktiki və operativ. İnformasiya təhlükəsizliyinin idarə edilməsi üçün motivatorlar kimi siyasət (strateji səviyyə), rəhbər göstərişlər (taktiki səviyyə) və tədbirlər (operativ səviyyə) çıxış edir. Müxtəlif təşkilati səviyyələr arasındakı fərqləndirici faktorlar ondan ibarətdir ki, strateji səviyyə korporativ strategiyaya təsir edir, taktiki səviyyə informasiya təhlükəsizliyinin idarə edilməsi üçün istifadə edilən proseslərə və metodologiyalara aiddir, operativ səviyyədə informasiya təhlükəsizliyi alətlərinin və tədbirlərinin reallaşdırılması və istismarı çıxış edir. Qeyd edək ki, təşkilatda informasiya təhlükəsizliyinin idarə edilməsi, əsasən, operativ səviyyədə qərarlaşır.

E-dövlətin informasiya təhlükəsizliyi arxitekturunda e-dövlətin təhlükəsizlik hədəfləri müəyyən edilir və bütün e-idarəetmə iyerarxiyasında əməl edilməsi zəruri olan prosedurlar təsvir olunur. Müvafiq qanunvericilik bazası və hüquq-mühafizə sistemi e-dövlətin sistematik və dayanıqlı inkişafı üçün mütləq şərtdir, informasiya təhlükəsizliyinin idarə edilməsi, o cümlədən kibercinayətkarlıqla mübarizə üçün olduqca vacibdir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin arxitektur elementlərinə, əsasən, inzibati idarəetmə və texnoloji idarəetmə daxildir. İnzibati idarəetməyə iki səviyyədə baxmaq olar: makro (ölkə) səviyyə və mikro səviyyə (tətbiqi sistemlərdən istifadə edən subyektlər).

İnzibati idarəetmə səviyyəsində əsas problem tətbiqi sistemlərdən istifadə edən subyektlərin ölkənin makroidarəetmə prinsiplərini, strategiyalarını və mövcud şərtləri nəzərə alaraq informasiya təhlükəsizliyi üzrə müvafiq təşkilati sistemi qurmaqdır. Burada insan resurslarının inkişafı və idarə edilməsi məsələləri də xüsusi vurğulanmalıdır.

E-dövlət İKT-nin inkişafının və tətbiqinin nəticəsidir, buna görə də, onun informasiya təhlükəsizliyinin idarə edilməsi istifadə edilən İKT-ə əsaslanmalıdır. Texnoloji idarəetmə inzibati idarəetmə ilə İKT arasında körpü rolunu oynayır. Texnoloji idarəetməyə vacib hostların təhlükəsizliyinin idarə edilməsi, verilənlərin idarə edilməsi, verilənlərin təhlükəsizliyinin idarə edilməsi, insidentlərin idarə edilməsi, təhlükəsizliyin qiymətləndirilməsi və s. daxildir.

Əlaqədar tədqiqatların analizi

E-dövlətin informasiya təhlükəsizliyi məsələlərinin aktual tədqiqat istiqamətlərinə konseptual modeldə e-dövlətin informasiya təhlükəsizliyinin əsas komponentləri kimi informasiya fəzasının, informasiya infrastrukturunun və nəhayət, informasiyanın özünün təhlükəsizliyinin vəziyyəti seçilmişdir [12]. Bu tədqiqat işində informasiya təhlükəsizliyinin qlobal aspektləri, informasiya müharibəsi, informasiya cəmiyyətinə olan təhdidlər və e-dövlətin etibarlı informasiya təminatı məsələləri geniş araşdırılmışdır.

E-dövlət hər birinin müstəqil informasiya təhlükəsizliyi siyasəti olan ayrı-ayrı təhlükəsizlik domenlərindən ibatətdir. E-dövlətin bu multi-domen mühitinin əsas xüsusiyyətləri və komponentləri analiz edilir, bu mühitdə informasiya təhlükəsizliyi sistemlərinin yaradılması zamanı əsas tələblərin rahat girişin təmin edilməsi ilə müfəssəl monitorinq icazələri arasında diqqətli balanslaşdırma olduğu göstərilir [19].

E-dövlətdə qarşılıqlı əlaqənin üç modeli (*C2G, G2G* və *G2C*) əsasında dövlət strukturları çərçivəsində informasiya təhlükəsizliyi, təhlükəsizliyin xarakteristikaları və təhlükəsizlik tələblərinin reallaşdırılması məsələləri, adətən, texnoloji baxımdan analiz edilir [22].

E-dövlətin informasiya təhlükəsizliyinin müxtəlif aspektlərinə hərtərəfli baxış üçün vahid konsepsiya işlənilməsinə də cəhdlər edilir [23]. Bu vahid yanaşma 4 səviyyədən ibarətdir: strateji, proses, qarşılıqlı əlaqə və informasiya. Burada təhlükəsizlik aspektləri strateji səviyyədən verilənlər səviyyəsinə kimi inteqrasiya edilir.

E-dövlət sistemləri də e-kommersiya sistemlərinin məruz qaldığı təhdidlərə məruz qalır, lakin e-dövlət sistemləri başqa məhdudiyyətlər çərçivəsində işləyirlər. E-kommersiya sistemlərinin çoxu yalnız əhalinin bir hissəsi ilə işləyir, onlar özləri bunu necə və nə vaxt edəcəklərini seçirlər. Bundan fərqli olaraq, e-dövlət bütün vətəndaşlarla işləyir [24]. İstifadəçilərin və tranzaksiyaların sayının olduqca çox olması, vətəndaşların fərdi məlumatlarının və dövlətin konfidensial məlumatlarının həssaslığı və bir sıra digər məsələlər nəticəsində e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi daha vacib olur.

E-kommersiya üçün geniş istifadə edilən təhlükəsizlik yanaşmaları e-dövlətə də tətbiq edilə bilər, lakin e-dövlət e-kommersiyadan xeyli fərqlidir. Adətən, e-dövlət şəbəkələri bir-biri ilə kommersiya şəbəkələrinə nisbətən daha yaxşı kommunikasiya yaradırlar, çünki onların çoxunda informasiyanın ötürülməsi prosesləri inteqrasiya edilib, kommersiya şəbəkələri isə rəqibdirlər və öz konfidensial informasiyalarını paylaşmırlar. Bu məsələlər bir sıra tədqiqatlarda müzakirə edilir [5, 23], e-dövlətin informasiya təhlükəsizliyi problemləri texnoloji və qeyri-texnoloji baxımdan analiz edilərək təhlükəsizliyin müxtəlif tələbləri üçün kompleks həllər təklif edilir [23].

E-dövlət və e-kommersiya sistemləri arasındakı fərqlər V.Konklin tərəfindən daha detallı şəkildə müzakirə edilir və müvafiq modellər işlənilir [5]. E-dövlətin reallaşdırılmasının dövlət tələblərinə uyğunluğunu müəyyən etmək üçün kompüter təhlükəsizliyi üzrə məlumatların toplanması sistemi təklif edilir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin əsas faktorlarının analizi mühüm əhəmiyyət daşıyır. Bu faktorların təhlükəsizlik mədəniyyəti, idarəetmə, informasiya

təhlükəsizliyi infrastrukturu və dəyişikliklərin idarə edilməsi kimi qruplaşdırılması təklif edilir [25, 26]. Müəlliflərin təqdim etdiyi ranqlaşdırma nəticələrinə görə, uğurlu təhlükəsizlik prosesləri üçün üç əsas faktor yüksək rəhbərliyin fəal dəstəyi, yetərli maliyyələşdirmə və kadrların səriştəsidir (treninqidir).

E-dövlətin informasiya təhlükəsizliyi üçün *workflow* model də təklif edilir [27]. Həmin modelin komponentləri e-xidmətlərin təhlükəsizliyinin təmin edilməsinə yönəlib Bu komponentlər informasiya təhlükəsizliyinin təmin edilməsi üçün siyasi qərarın qəbulu, bu qərarın reallaşdırılması üçün informasiya təhlükəsizliyinin analizi, müvafiq qanunvericilik bazasının formalaşdırılması, istifadəçilərin inamının qiymətləndirilməsi, təhlükəsizlik strategiyalarının müəyyən edilməsi ilə yanaşı, fərdi məlumatların qorunması, girişin idarə edilməsi, autentifikasiya və şəbəkə təhlükəsizliyinin təmin edilməsi mexanizmləri kimi texnoloji məsələləri də əhatə edir.

E-dövlət xidmətlərinin təhlükəsizlik tələbləri üçün təşkilati model (*Organizational framework for the Security Requirements of E-government Services*) e-dövlət sistemində hər bir xidmətin təhlükəsizlik risklərini identifikasiya etməyə imkan verir [28]. Bu təşkilati modelə əsaslanaraq, e-dövlətin hər bir xidməti üçün təhlükəsizlik tələbləri təsnif edilir və *PKI* əsasında bu tələbləri ödəyən inteqrativ platforma təklif edilir [29]. Müəlliflər bu təhlükəsizlik tələblərinin həyata keçirilməsinin mümkünlüyünü e-dövlət modelinin *Webocrat* sistemində yoxlayırlar [30].

Fərdi məlumatların qorunması tələbləri baxımından identifikasiyanın yerinə yetirilməsi məsələləri həm elmi, həm də siyasi və ictimai dairələrdə geniş müzakirə olunur. Bu baxımdan, müxtəlif tətbiq sahələrində konfidensiallığı təmin etmək üçün üç təhlükəsizlik səviyyəsindən (normal istifadə üçün təhlükəsizlik, etibarlı infrastruktur ilə təhlükəsizlik, texniki *end-to-end* təhlükəsizlik) ibarət model daha çox elmi-praktiki maraq kəsb edir [31]. Bu tədqiqat işində Avstriya vətəndaşlarının identifikasiya kartlarının reallaşdırılması nümunəsinin köməyi ilə e-dövlətin rəqəmsal imza, *PKI* və s. texnologiyalara əsaslanan təhlükəsizlik arxitekturu da təklif edilmişdir.

E-dövlət xidmətlərinin praktiki reallaşdırılmasında veb-servis texnologiyaları geniş istifadə edilir [32]. E-dövlətin informasiya təhlükəsizliyinin təkmilləşdirilməsi üçün veb-servis texnologiyalarında girişin idarə edilməsi modeli təklif edilir [33]. Müxtəlif dövlət orqanlarını əhatə edən böyük sistemlərdə vəzifələrin ayrılması (ing. *separation*) çox vacibdir və bu mexanizmi rollara əsaslanan girişə nəzarət mexanizmi (ing. *Role Based Access Control – RBAC*) reallaşdırır. E-dövlət sisteminin təklif edilən girişin idarə edilməsi arxitekturu autentifikasiya, avtorizasiya (*PKI* istifadə edilir) və rola əsaslanan girişə nəzarət hissələrindən ibarətdir. *RBAC* modeli istifadəçilər, rollar, icazələr və sessiyalardan ibarətdir. İstifadəçilər insan, kompüter, veb-servis, şəbəkə, proses və ya intellektual agent ola bilər. Rollar sistemdə yerinə yetirilən funksiyaları bildirir, çox zaman təşkilatın iş profilinə bağlı olur. Hər bir istifadəçiyə bir və ya bir neçə rol təyin edilə bilər. İcazə e-dövlət sistemindəki obyekt üzrərində yerinə yetirilə bilən giriş rejimidir. İstifadəçi obyektə (fayl, veb-servis, verilənlər bazasından məlumat) müraciət etdikdə sistem istifadəçiyə ayrılmış icazələri yoxlayır və istifadəçiyə giriş hüququ verir və ya imtina edir.

İnformasiya təhlükəsizliyinin idarə edilməsi predmetinin daha ətraflı formal təsviri məqsədi ilə metamodelin yaradılmasına da təşəbbüs göstərilir, metamodelə müxtəlif komponentlər daxildir [34]. Metamodelin elementləri (meta-primitivlər) informasiya təhlükəsizliyinin idarə edilməsinin biznes-strategiyası və missiyası, idarəetmə məqsədləri və idarəetmə strategiyası, təhlükəsizliyin idarə edilməsi sistemi, təhlükəsizliyin idarə edilməsi proqramı, təhlükəsizliyin idarə edilməsi strukturu, modelin təkmilləşdirilməsi və onu dəstəkləyən metodologiya və müəssisənin biznes-sistemləridir.

İnformasiya təhlükəsizliyinin idarə edilməsi proqramı təhlükəsizlik idarəçiliyinin, təhlükəsizliyin idarə edilməsi sisteminin, təhlükəsizlik siyasətinin, texnologiyanın, infrastrukturun və risk menecmentinin aqreqasiyasıdır. İnformasiya təhlükəsizliyinin idarə

edilməsi sistemi təhlükəsizliyin idarə edilməsi proses modelindən, proses metodologiyasından və təhlükəsizlik proseslərinin təkmilləşdirilməsi modelindən ibarətdir.

İnformasiya təhlükəsizliyinin idarə edilməsinin yetkinlik modelləri də təklif edilmişdir. Bu modellərdə əsas diqqət təşkilatlara təklif edilən təhlükəsizlik servislərinə yönəldilir [15, 35]. Yetkinlik modeli müxtəlif səviyyələrdə tələb edilən təhlükəsizlik elementlərinin strukturlaşdırılmış toplusunu təqdim edir. Bu elementlər təşkilatlara mövcud təhlükəsizlik nöqsanlarını identifikasiya etməyə və anlamağa, təhlükəsizliyin təmin edilməsinin gedişini müşahidə (monitorinq) etməyə, təhlükəsizlik siyasətlərini, ən yaxşı təcrübələri, keyfiyyəti, investisiyaları, təşkilati auditi monitorinq etməyə imkan verir.

E-dövlətin informasiya təhlükəsizliyinin cari vəziyyətinin ölçülməsi üçün müvafiq informasiya təhlükəsizliyi indikatorlarının işlənilməsinə ciddi ehtiyac vardır. Bu sahədə tədqiqatlara son illər başlanılsa da, artıq bir neçə indikator sistemi təklif edilmişdir. Məsələn, e-dövlətin formalaşması təcrübəsində rast gəlinən 20-ə yaxın zəruri informasiya təhlükəsizliyi indikatoru müəyyən olunmuşdur [36].

Nəticə

E-dövlət İKT-dən istifadə etməklə dövlət idarəçiliyinin səmərəliliyini və göstərilən xidmətlərin keyfiyyətini yaxşılaşdırmaqda mühüm rol oynayır. Lakin e-dövlət quruculuğu sahəsində öz həllini gözləyən bir sıra problemlər də vardır, onlardan biri də informasiya təhlükəsizliyidir. İnformasiya təhlükəsizliyi e-dövlətin effektivliyinə və vətəndaşların dövlətə inamına birbaşa təsir edir.

E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi mürəkkəb məsələdir. E-dövlət texnologiyası inkişaf etdikcə təhlükəsizliyə daha yüksək tələblər irəli sürülür. E-dövlətin informasiya təhlükəsizliyi olduqca dinamikdir və sürətlə inkişaf edir. O, innovativ yanaşma tələb edir. Təhlükəsizliyin dövri olaraq monitorinqi aparılmalı, müvafiq texnologiyalar səmərəli tətbiq edilməli və informasiya təhlükəsizliyinin idarə edilməsi daim təkmilləşdirilməlidir. Buna görə də e-dövlətin informasiya təhlükəsizliyi problemlərini geniş tədqiq edilməsi və problemlərin həlli üçün müvafiq yanaşmaların işlənilməsi zəruridir.

Ədəbiyyat

1. United Nations E-Government Survey 2012: E-government for the people. UN Department of Economic and Social Affairs, United Nations New York, 2012, 160 p.
2. Pina V., Torres L., Acerete B., Are ICTs promoting government accountability?: A comparative analysis of e-governance developments in 19 OECD countries // Critical Perspectives on Accounting, 2007, vol. 18, no. 5, pp. 583-602.
3. Ndou V.M., E-government for developing countries: opportunities and challenges // The Electronic Journal on Information Systems in Developing Countries, 2004, vol. 18, no. 1, pp. 1-24.
4. Norris D. F., Moon M. J., Advancing e-government at the grassroots: tortoise or hare? // Public Administration Review, 2005, vol. 64, no. 1, pp. 65-75.
5. Conklin W.A., Barriers to adoption of e-government / Proc. of 40th Annual Hawaii International Conference on System Sciences (HICSS), 2007, pp.1-8.
6. Ebrahim Z., Irani Z., E-government adoption: architecture and barriers // Business Process Management Journal, 2005, vol. 11, no. 5, pp. 589-611.
7. Belanger F., Carter L., Trust and risk in e-government adoption // Journal of Strategic Information Systems, 2008, vol. 17, no. 2, pp. 165-176.
8. Tassabehji R., Inclusion in e-government: a security perspective / eGovernment Workshop'05 (eGOV05), 2005, pp.1-9.
9. Saint-Germain R., Information security management best practice based on ISO/IEC 17799 // Information Management Journal, 2005, vol. 39, no. 4, pp. 60-66.

10. Dhillon G., Backhouse J., Information systems security management in the new millennium // Comm. ACM, 2000, vol. 43, no. 7, pp. 125-128.
11. Wiander T., Savola R., Karppinen K., Rapeli M., Holistic information security management in multi organization environment / Proc. of the IEEE International Symposium on Industrial Electronics, 2006, vol. 4, pp. 2942 – 2947.
12. Əliquliyev R.M., İmamverdiyev Y.N., E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri // İnformasiya Cəmiyyəti Problemləri, № 1, s. 3-13, 2010.
13. von Solms B., Information security - the fourth wave // Computers & Security, 2006, vol. 25, no. 3, pp. 165-168.
14. ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management, 2004.
15. ISM3 Consortium: Information security management maturity model, Consortium version 2.10, 2007.
16. Hong K.-S., Chi Y.-P., Chao L., Tang J.-H., An integrated system theory of information security management // Information Management & Computer Security, 2003, vol. 11, no. 5, pp. 243-248.
17. ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements. 2005, 34 p.
18. Eloff J., Eloff M., Information security management – a new paradigm / Proc. of the annual research conference of the South African Institute of Computer Scientists and Information Technologists on enablement through technology, 2003, pp. 130-136.
19. Joshi J., Ghafoor A., Aref W.G., Spafford E.H., Digital government security infrastructure design challenges // IEEE Computer, 2001, vol. 34, no. 2, pp.66-72.
20. Mehta M., Singh S., Lee Y., Security in e-services and applications / Network Security: Current Status and Future Directions, Edited by Douligeris C. & Serpanos D.N., John Wiley & Sons, 2007, pp.157-178.
21. Yee G, Personalized security for e-services / Proc. of the First International Conference on Availability, Reliability and Security (ARES'06), 2006, pp.140-147.
22. Hof S., Reichstädter P., Securing e-Government / EGOV 2004, 2004, pp. 336-341.
23. Wimmer M., von Bredow B., E-government: aspects of security on different layers / Proc. of the 12th International Workshop on Database and Expert Systems Applications, 2001, pp.350-355.
24. Stibbe M., E-government security // Infosecurity Today, 2005, vol. 2, no. 3, pp.8-10.
25. Smith S., Jamieson R., Determining key factors in e-government information system security // Information Systems Management, 2006, vol. 23, no. 2, pp.23-32.
26. Wang J., E-government security management: key factors and countermeasure / Proc. of 5 th International Conference on Information Assurance and Security, 2009, pp. 483-486.
27. Benabdallah S., Guemara-ElFatmi S., Boudriga N., Security issues in e-government models: what governments should do? / IEEE International Conference on Systems, Man and Cybernetics, 2002, pp.398-403.
28. Gritzalis S., Lambrinoudakis C., Security requirements of e-government services: an organizational framework / Proc. of International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'02), 2002, vol. 1, pp.127-131.
29. Lambrinoudakis C., Gritzalis S., Dridi F., Pernul G., Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy // Computer Communications, 2003, vol. 26, no. 16, pp. 1873-1883.
30. http//www.webocrat.com

31. Posch R., Leitold H., Identification and confidentiality for e-government / International Workshop on Certification and Security in E-Services (CSES 2002), IFIP (International Federation for Information Processing), vol. 127, 2003, pp. 267-279.
32. Wang H., Huang J.Z., Qu Y., Xie J., Web services: problems and future directions // Web Semantics: Science, Services and Agents on the World Wide Web, 2004, vol. 1, no. 3, pp. 309-320.
33. Zeng Z., Chen T., Zhang Y., E-government information security in the web environment based on role based access control technology / Proc. of the International Seminar on Business and Information Management (ISBIM), 2008, pp. 210-213.
34. Nnolim A., Steenkamp A., An architectural and process model approach to information security management // Information Systems Education Journal, 2008, vol. 6, no. 31, pp. 1-27.
35. Karokola G., Kowalski S., Yngström L., Towards an information security maturity models for secure e-government services: a stakeholders view / Proc. of the 5th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011), 2011, pp. 58-73.
36. Shayan A., Abdi B., Qeisari M., Identification of the required security practices during e-government maturity / Proc. of the 6th İnternational Conference Global Security, Safety, and Sustainability (ICGS3 2010), 2010, pp. 250-262.

УДК 004.9:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Анализ современного состояния исследований по управлению информационной безопасностью э-государства

Обеспечение информационной безопасности и защита персональных данных в среде э-государства являются основными проблемами технологии э-государства. С развитием и расширением э-услуг э-государства эти проблемы становятся все более актуальными. Надежное обеспечение информационной безопасности требует систематического подхода и гибких и адекватных к условиям моделей управления. В этой статье проанализировано современное состояние исследований в области управления информационной безопасностью э-государства и выбраны актуальные проблемы для дальнейших исследований.

Ключевые слова: *э-государство, э-услуги, информационная безопасность, управление информационной безопасностью*.

Yadigar N. Imamverdiyev,
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

State-of-the-art analysis of the researches on e-government information security management

Ensuring of information security and personal data protection in e-government environment are the main challenges of e-government technology. Along with the development and expansion of e-services of the e-government, these problems are becoming more acute. Reliable information security requires a systematic approach, flexible and appropriate to the conditions management model. This article analyzes the current state of research in the field of e-government information security management and selects actual problems for further research.

Keywords: *e-government, e-service, information security, information security management.*