E-dövlət mühitində dövlət sirrinin mühafizəsinin təmin edilməsi problemləri

Davud Rüstəmov

AMEA İnformasiya Texnologiyaları İnstitutu

drustamov@mns.gov.az

***Xülasə*— Məqalənin məqsədi müxtəlif səviyyələrdə aparılan e-dövlət xidmətlərində İnformasiya Təhlükəsizliyinin İdarə olunması probleminə diqqəti yönəltmək və bu problemə beynəlxalq tələblər prizmasından baxışı təmin etməkdir. Azərbaycan Respublikasında e-dövlət quruculuğu sahəsində xeyli işlər görülmüş və ölkəmiz beynəlxalq statistika indeksini hər il yüksəkliyə doğru dəyişir. Lakin informasiya təhlükəsizliyi məsələsi dövlət qurumlarını daim narahat edən məsələ olaraq qalacaqdır. Bu baxımdan da, e-dövlət mühitində informasiya təhlükəsizliyinin idarə edilməsi probleminin elmi ictimaiyyətin müzakirə obyektinə çevrilməsi bu məqalənin əsas məqsədi hesab olunur.**

Açar sözlər— e-dövlət, informasiya təhlükəsizliyi, dövlət sirri.

I. GİRİŞ

E-dövlət termini ilk dəfə İqtisadi İnkişaf və Əməkdaşlıq Təşkilatı (OECD) tərəfindən işlədilmişdir. E-dövlət dövlətin bütün fəaliyyət sahələrində yeni İKT-nın tətbiqi nəticəsində vətəndaşlara, qeyri-hökumət təşkilatlarına, biznes və s. sahələrə elektron xidmətlərin göstərilməsini nəzərdə tutur, şəbəkə mühitinin, eləcə də internetin yeni imkanlarından istifadə etməklə dövlətin funksional sahələrində inkişafa gətirib çıxarır. Belə bir mühitdə informasiya təhlükəsizliyinin effektiv idarə olunması vacib faktorlardan hesab olunur. Belə ki, müxtəlif istifadəçilərin (vətəndaşlar, digər qrup istifadəçilər) e-dövlətin müxtəlif xidmətlərindən istifadəsi zamanı meydana gələn problemlərin mərkəzində etibarlılıq göstəricisi dayanır.

ABŞ-da 2002-ci ildə "e-dövlət haqqında" qanun qəbul olunmuşdur. Bu qanunda informasiya təhlükəsizliyinin təmin olunması məsələlərinə geniş yer ayrılmışdır. Aşağıda göstərilən iki əsəs normativ akt "e-dövlət haqqında" qanunun tələblərindən irəli gəlir:

- FISMA (the Federal Information Security Management Act of 2002) ;
- CIPSEA (the Confidential Information Protection and Statistical Efficiency Act).

Son zamanlar e-dövlət ifadəsi ilə yanaşı müxtəlif elmi mənbələrdə kağızsız dövlət, mobil dövlət və s. yanaşmalara da rast gəlinir. E-dövlət termini 1990-cı illərdən sonra meydana gəlmişdir. Lakin dövlət orqanlarında kompüterləşmənin tətbiqi sahəsində beynəlxalq elmi ədəbiyyatlarda göstərildiyi kimi 1970-ci illərdə "IT in government" mövzusu dərc olunmuşdur [1].

II. İNFORMASİYA TƏHLÜKƏSİZLİYİ

Məlumdur ki, e-dövlət xidmətlərinə keçid təkcə yeni texnologiyanın tətbiqi nəticəsində ictimai idarəetmədə uğur əldə etməkdən ibarət deyildir [2]. Vətəndaş dövlət arasında qarşılıqlı şəffaflığın yaradılması ilə qanuna müvafiq formada konfidensiallığın mühafizəsinin gücləndirilməsi əsas məqsədlərdən hesab olunur. İnformasiya təhlükəsizliyinin idarə edilməsi sisteminə (İTİS) yanaşma prosesi hər bir koporativ istifadəçi üçün aşağıdakı vacib məqamları xüsusi qeyd edir [3]:

- Təşkilatın informasiya təhlükəsizliyi tələblərinin öyrənilməsi, informasiya təhlükəsizliyi üzrə obyektlərin müəyyən olunması və siyasətin qurulması.
- Təşkilatın fəaliyyət sahəsinə uyğun informasiya təhlükəsizliyinə yönəlmiş risklərin idarə olunmasına nəzarət edilməsi.
- Müntəzəm olaraq təşkilatın İTİS-inin effektivliyini monitorinq etmək, yenidən baxmaq və inkişaf etdirmək.
- Təşkilatın funksional fəaliyyətinə uyğun inkişaf proseslərinin davam etdirilməsi və s.

Verilənlərin təhlükəsizliyinin təmin olunması üçün çox-elementli təhlükəsizlik tələbləri çoxluğuna ehtiyac var: autentifikasiya, avtorizasiya, konfidensiallıq, tamlıq, nəzarət oluna bilmə imkanı (ing. traceability), əlyetənlik və digər törəmə tələblər mövcuddur. İcazəsiz girişlərin qarşısının alınması üçün müxtəlif təşkilati və texniki qaydalar mövcuddur[4]:

- Sistem və tətbiqi proqram təminatının və giriş-çıxış qurğularının mühafizəsi;
- Həssas tipli məlumatlarla işləməyə buraxılmış proqram təminatının mühafizəsi;
- Verilənlərin ötürülməsi zamanı həssas məlumatlara icazəsiz girişlərin qarşısının alınması;
- Həssas tipli məlumatların silinməsi, bloklanması, ləğv olunması zamanı istifadə olunan metodların effektivliyinə əminlik;
- Həssas tipli məlumatlarla işləməyə buraxılmış istifadəçilərin hüquq və səlahiyyətlərinin onların funksional vəzifələri baxımından müəyyən olunması və s.

Beynəlxalq aləmdə e-dövlət üçün informasiya təhlükəsizliyi qaydalarının müəyyən olunmasına baxmayaraq, hələ də BMT-nin (2012) araşdırmaları göstərir ki, dünyada e-

dövlət portallarının yalnız 20% təhlükəsizlik tələblərinə cavab verir. Bu araşdırmada yerli, regional və mərkəzləşdirilməmiş ictimai portallar daxil edilmədən Avropa ölkələri 44% ilə öndə yer almışdır [9].

III. İNFORMASİYA TƏHLÜKƏSİZLİYİNƏ TƏHDİDLƏR

E-dövlətin vətəndaşlara, müəssisələrə, ictimai təşkilatlara, dövlət orqanlarına və agentliklərinə göstərdiyi xidmət İnternet və mobil əlaqələr üzərindən aparıldığı zaman müxtəlif təhlükələrlə rastlaşılır. Daha ciddi hesab olunan kiber əhlükələr detalları ilə [5]-də göstərilmişdir. Belə ki, packet sniffer, probe, malware, İnternet infrastrukturuna hücumlar, DoS (ing. Denial-of-Service) hücumları, kənardan şəbəkəyə qoşulmaqla hücumlar və insayder problemi kimi təhlükələr daim müzakirə obyekti olmalıdır. [6]-da göstərildiyi kimi, təşkilatda İTİS-in uğurla həyata keçirilməsi informasiya mülkiyyətinin qorunmasında çox vacib məsələdir və bu da öz növbəsində hər bir təşkilat üçün aşağıdakı üstünlükləri təqdim edir:

- İnformasiya resursunun qorunmasında uğurlu təminatı yaratmaq üçün davamlılıq əsasında informasiya təhlükəsizliyinə olan risklərə qarşı adekvat tədbirlər görülür;
- İnformasiya risklərinin müəyyən olunması, ölçülməsi, nəzarət olunması və effektivliyinin artırılması imkanı;
- Nəzarət mühitinin davamlı inkişafının aparılması imkanı;
- Əldə olunmuş təcrübə əsasında qanunvericilik və tənzimləyici qaydaların inkişaf etdirilməsi imkanı və s.

IV. KADR HAZIRLIĞI PROBLEMLƏRİ

Dövlət orqanlarında informasiya təhlükəsizliyini qismən təmin edən antivirus, şəbəkələrarası ekran, müdaxilələrin aşkarlanması sistemləri, kriptoqrafik mühafizə və şəbəkə təhlükəsizliyi istifadə edilir, lakin nizamlı və dayanıqlı olması üçün bu proses müvafiq standartların tələbləri, müəssisənin müəyyən olunmuş siyasəti əsasında həyata keçirilməlidir. Korporativ istifadəçilər hər gün informasiya təhlükəsizliyi sahəsində yeni biliklərlə maarifləndirilməli və buna funksional vəzifələrinin bir hissəsi kimi baxmalıdırlar. Kolumbiya Universitetində Kompüter Elmləri Departament [8] tərəfindən aparılan tədris göstərmişdir ki, insan faktoru kibertəhlükəsizlik siyasətinə daha çox təsir edir və dövlət orqanları və agentliklərində informasiya təhlükəsizliyinin təmin edilməsi sahəsində çalışan kadrların bilik səviyyəsi beynəlxalq sertifikatların (ISO 27001; ISACA – CISM, CISA, CRISC, CGAIT; CISSP və s.) tələblərinə cavab verməlidir. ECDL – European Computer Driving Licence sertifikatı 1995-ci ildə Council of European Professional Informatics Society tərəfindən yaradılmışdır. Bu sertifikatın məqsədi e-dövlət mühitində çalışan kadrların kompüter biliklərinin standartlara cavab verən minimal həddə qiymətləndirməsidir.

NƏTİCƏ

Məqalənin məqsədi müxtəlif səviyyələrdə aparılan e-dövlət xidmətlərində İTİS-in təmin olunmasına diqqəti yönəltməkdir. Azərbaycan Respublikasında da e-dövlət quruculuğu sahəsində xeyli işlər görülmüşdür və ölkənin beynəlxalq statistik indeksi hər il irəliyə doğru dəyişir. Lakin informasiya təhlükəsizliyi məsələsi daim dövləti narahat edən məsələ olaraq qalacaqdır. İnformasiya təhlükəsizliyi sahəsində beynəlxalq standartların ölkəmizdə tanınması və ya milli səviyyədə müvafiq işlərin görülməsi, informasiya ehtiyatlarının təsnifatına uyğun təhlükəsizlik siyasətinin müəyyən olunması, bu sahədə beynəlxalq standartların tələbinə uyğun kadr hazırlığı, ali təhsil müəssisələrində informasiya təhlükəsizliyinin elmi-nəzəri və praktiki tədrisi və s. bu kimi həlli vacib məsələlər e-dövlət mühitində informasiya təhlükəsizliyinin idarə olunmasında mühüm əhəmiyyətə malikdir.

ƏDƏBİYYAT

[1] A. Gronlund Örebro University, Sweden. "Electronic Government" International Journal of Electronic Government Research page-9, 2007 year

[2] United Nations, Department of Economic and Social Affairs (2012). "E-Government Survey 2012. E-Government for the People". ISBN: 978-92-1-123190-8.

[3] ISO/IEC 2700:2005 (2009). Information technology — Security techniques — Information security management systems — Requirements.

[4] Chatzidimitriou, Marios and Adamantios Koumpis (2008). "Marketing One-stop E-Government Solutions: the European OneStopGov Project". IAENG International Journal of Computer Science, 35:1, IJCS_35_1_11. (Advance online publication: 19 February).

[5] Shailendra, Sing; Singh Karaulia (2011). "E-Governance: Information Security Issues". International Conference on Computer Science and Information Technology (ICCSIT'2011).

[6] ISO/IEC 2700:2009 (2009). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[7] Vebjorn Moen, André N. Klingsheim, Kent Inge Fagerland Simonsen, and Kjell Jorgen Hole (2007). "Vulnerabilities in e-governments". International Journal of Electronic Security and Digital Forensics, vol. 1, issue 1, pages 89-100.

[8] Brian M. Bowen, Ramaswamy Devarajan, Salvatore Stolf (2012). "Measuring the Human Factor of Cyber Security". Homeland Security Affairs, Supplement 5, article 2.

[9] Hector D. Puyosa P. "e-Government: Security Threats". IEEE e-Government STC. November 11, 2012.