E-dövlət mühitində informasiya təhlükəsizliyinin idarə edilməsi problemləri

Elçin Əliyev

AMEA İnformasiya Texnologiyaları İnstitutu

elchinaa@gmail.com

***Xülasə*— İnformasiya təhlükəsizlyinin idarə edilməsi coxeşalonlu, geniş coğrafiyaya, təsnifatlı məqsəd, prosedur və vəzifələrə, fərqli səlahiyyətli iştirakçılara malik aktual problemdir. Azərbaycan Respublikasında bu sahə üçün 1971-ci ildən başlayaraq müəyyən "dayaqlar" yaradılmağa başlanılmış, həmin işlər müstəqillik illərində genişlənmişdir. Bu proses 2003-cü ildə Milli Strategiyanın qəbul edilməsindən sonra davamlı inkişaf etdirilir. Həm milli məkan, həm də korporativ informasiya mühitləri üçün informasiya təhlükəsizlyinin idarə edilməsinə hüquqa əsaslanma, vahid siyasət, proses yanaşması və standartların tətbiqi tələb olunur. Bu tədqiqat işində ISO/IEC-27001 standartına uyğun olaraq informasiya təhlükəsizlyinin idarə edilməsi üzrə vəzifələr və idarəetmənin iştirakçıları identifikasiya olunur, bu vəzifələrin uyğun iştirakçılar arasında bölünməsi, koordinasiyası və digər problemlər qaldırılır. Bəzi problemlər daha "qaynar" kimi seçilir və onlar üçün həllər təklif edilir.**

Açar sözlər*— *informasiya təhlükəsizliyi; informasiya təhlükəsizliyinin idarə edilməsi; proses yanaşması; PDCA-modeli

I. GİRİŞ

Azərbaycan Respublikasında informasiya təhlükəsizliyinin idarə edilməsi sisteminin mövcud "dayaqları" ümimmilli lider Heydər Əliyevin şəxsi iştirakı və rəhbərliyi ilə 1971-ci ildən həyata keçirilən informatika sahəsində elm-təhsil-istehsalat üçlüyünün yaradılması strategiyasının çərçivəsində yaradılmışdır[1]. O cümlədən, 1971-ci ildə AMEA Kibernetika İnstitutunda Avtomatlaşdırılımış İdarəetmə Sistemləri şöbəsi təşkil edilmiş (2002-ci ildən AMEA İnformasiya Texnologiyaları İnstirtutu), Azərbaycan Dövlət Universitetində tətbiqi riyaziyyat fakültəsi (hazırda Bakı Dövlət Universitetinin tətbiqi riyaziyyat və kibernetika fakültəsi) yaradılmışdı. Elə həmin ildə keçmiş SSRİ "СоюзЭВМкомплекс" Ümumittifaq Birliyində Bakı İxtisaslaşmış Ərazi İdarəsi (sonralar Azərbarbaycan Elm və Texnika Komitəsində "АzərİnformatikaƏ Elmi İstehsalat Birliyi – hazırda ləğv edilib) də yaradılmışdı.

Müstəqillik illərində Azərbaycan Respublikasında informasiya təhlükəsizliyinin idarə edilməsi (İTİ) üçün bir sıra xüsusi qurumlar yaradılmışdır.

17.01.1997-ci il Azərbaycan Respublikasının Prezidenti yanında Dövlət Sirrinin Mühafizəsi üzrə İdarələrarası Komissiya yaradılmışdır. Azərbaycan Respublikası Prezidentinin 26 sentyabr 2012-ci il tarixli sərəncamı ilə Azərbaycan Respublikası Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi və Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyi yanında Elektron Təhlükəsizlik Mərkəzi yaradılmışdır.

Qeyd edək ki, 2012-ci ildə ölkənin bir neçə internet informasiya resursları kiberhücumlara məruz qalmış, onların funksionallığında fasilələr yaranmışdır.

İTİ üzrə əsas fəaliyyət istiqamətləri aşağıdakı sərəncamlarla müəyyən edilmişdir:

- Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003 - 2012-ci illər) - Azərbaycan Respublikası Prezidentinin 17.02.2003-cü il tarixli sərəncamı)[2];
- Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan) - Azərbaycan Respublikası Prezidentinin 21.10.2005-ci il və 11.08.2010-cu il tarixli sərəncamları[3];
- Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan) - Azərbaycan Respublikası Prezidentinin 21.10.2005-ci il və 11.08.2010-cu il tarixli sərəncamları[4];
- Azərbaycan Respublikasında 2010-2011-ci illərdə "Elektron hökumət"in formalaşdırılması üzrə Fəaliyyət Proqramı - Azərbaycan Respublikası Nazirlər Kabinetinin 14.05.2010-cu il tarixli sərəncamı[5].

İTI üçün hüquqi baza aşağıdakı qanunlarla müəyyən edilmişdir:

- İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında (1998-ci il);
- Müəlliflik hüququ və əlaqəli hüquqlar haqqında (1996-cı il);
- Dövlət sirri haqqında (1996, 2004-cü il);
- Məlumat azadlığı haqqında (1998-ci il)/ İnformasiya azadlığı haqqında (2005-ci il);
- Kommersiya sirri haqqında (2001-ci il);
- Banklar haqqında (2004-cü il);
- Elektron imza və elektron sənəd haqqında (2004-cü il);
- Milli təhlükəsizlik haqqında (2004-cü il);
- Məlumat toplularının hüquqi qorunması haqqında (2004-cü il);
- İnformasiya əldə etmək haqqında (2005-ci il);
- Fərdi məlumatlar haqqında (2010-cu il).

Beynəlxalq konvensiyalara qoşulmaqla İTİ üçün bir sıra beynəlxalq hüquqi alətlərdən istifadə imkanı yaradılmışdır.

Azərbaycan Respublikası 2009-cu ildə Avropa Şurasının "Kibercinayətkarlıq haqqında" 23.11.2001-ci il tarixli 185№-li Konvensiyasına[7] və Avropa Şurasının "Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında" 28.01.1981-ci il tarixli 108№-li Konvensiyasına qoşulmuşdur.

İnformasiya təhlükəsizliyi üzrə milli standartlar bazasını genişləndirmə işləri davam etdirilir[8]. İnformasiya təhlükəsizliyi üzrə bir neçə beynəlxalq standart istifadə üçün Azərbaycanda dövlət qeydiyyatına alınmışdır[9]:

- AZS-324:2008 (ISO/IEC-27002:2005). İnformasiya təhlükəsizliyinin idarə edilməsi üzrə əməli qaydalar.
- AZS-494:2010 (ISO/IEC-27001:2005). İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri. Tələblər.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİNİN OBYEKTLƏRİ

İTİ-nin hədəfi aşağıdakı obyektlərdir :

- informasiya resursları;
- proqram təminatı vasitələri;
- texniki təminat vasitələri, o cümlədən şəbəkə avadanlığı, informasiya daşıyıcıları;
- mühəndis qurğuları və digər maddi vasitələr;
- biznes proseslər, o cümlədən informasiya xidmətləri;
- insan resursları, onların səlahiyyət və kvalifikasiyası;
- reputasiya, biznes əlaqələri və digər qeyri-maddi aktivlər.

İTİ-nin coğrafiyası ölkə daxilində və ölkə xaricində olan bir sıra informasiya mühitləri aid edilir:

a) ölkə daxilində:

- e-dövlət mühiti;
- milli və dövlət əhəmiyyəti olan qurumlararası makroinformasiya mühitləri;
- qurumlardaxili korporativ informasiya mühitləri;
- qurumların struktur bölmələrində lokal informasiya mühitləri;
- ölkə ərazisində olan əhalinin fərdi informasiya mühitləri.

b) ölkə xaricində:

- ölkəninin xaricdəki diplomatik və digər nümayəndəliklərində olan lokal informasiya mühitləri;
- ölkəninin xaricdəki hava və dəniz nəqliyyatı vasitələrində olan bortdaxili informasiya mühitləri;
- ölkə xaricində rəsni səfərdə olan vətəndaşların fərdi informasiya mühitləri;
- ölkə qurumlarının əməkdaşlıq etdiyi xarici qurumlara təqdim edilmiş mikro informasiya mühitləri.

İTİ üçün məlumatlara müxtəlif təhlükəsizlik dərəcələri (qrifləri) verilir:

a) dövlət sirri olan məlumatlar üçün: "tam məxfi", "məxfi", "xüsui əhəmiyyətli";

b) konfidensial məlumatlar üçün: "konfidensial", "fərdi məlumat", "xidməti istifadə üçün", "bank sirri", "kommersiya sirri" və s.

c) əqli mülkiyyət olan məlumat;

d) açıq məlumatlar.

Təhlükəsizlik qriflərinin digər istifadə sahələri də mövcuddur. Məsələn, müvafiq qrifli məlumatların daşıyıcılarına da eyni qriflər yazılır. Qrifindən asılı olaraq müvafiq işçilərə (qurumlara) həmin məlumatlara müəyyən buraxılış dərəcəsi verilir. Qrifindən asılı olaraq, həmin məlumatlarlarla aparılan informasiya proseslərini təmin etmək üçün yaradılan, tətbiq edilən proqram və texniki təminat vasitələri, xidmət proseslərinə müəyyən sertifikatlar verilir.

III. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİNİN STANDART PROSEDURLARI

İTİ-nin əsas vəzifələri aşağıdakılardan ibarətdir:

- mühafizə vasitələrini aşmağın mümkünsüzlüyünun təmin edilməsi;
- İTİ obyektinin "açıq" (mühafizəsiz) vəziyyətə keçməyə yol verilməməsi;
- səlahiyyətlərin minimallaşdırılması;
- vəzifə və məsuliyyət bölgüsü;
- mühafizənin çox eşalonlu qurulması;
- mühafizə üçün müxtəlif vasitələrinin tətbiqi (mühafizənin çox xarakterli olması);
- informasiya sisteminin strukturlaşması və sadə idarə olunması ("parçala – idarəet");
- təhlükəsizlik tədbirlərinə hamı tərəfindən dəstək verilməsi.

İTİ-nin əsas prinsiplərini hüquqa əsaslanma; insan hüquqlarını, cəmiyyət və dövlət maraqlarını tarazlaşdırma; vahid siyasət; informasiya təhlükəsizliyi üzrə səlahiyyətləri bölüşdürlmə və proses yanaşması təşkil edir.

"Proses yanaşması" termini ilə (AZS-494:2010, ISO/IEC-27001:2005 standartına görə) – İTİ üçün sistemin yaradılması, tətbiqi, istismarı, daim nəzarət edilməsi, təhlili, işlək vəziyyətdə saxlanılması və təkmilləşdirilməsi nəzərdə tutulur.

Bu standart İTİ proseslərini qurmaq üçün "Planlaşdırma – Reallaşdırma – Kontrol – Aktuallaşdırma" (PRKA, PDCA – "Plan-Do-Check-Act") Şukart-Deminq tsiklik modelini tətbiq edir.

a) Planlaşdırma:

- İTİ obyektini dəqiqləşdirmək, dekompozisiya;
- tələbləri və məqsədləri müəyyənləşdirmək;
- riskləri aşkarlamaq və qiymətləndirmək, reyestrə daxil etmək;
- adekvat prosedur və vasitələri müəyyənləşdirmək, reyestrə daxil etmək;
- fəaliyyət planı (strateji plan), ümumi menecment (planının tərkib hissəsidir).

b) Reallaşdırma (tətbiq və istismar):

- realizasiya planları (taktiki və operativ planlar);
- təhsil, təlim və məlumatlandırma proqramları;
- risklərin emalı və ya qabaqlanması işləri.

c) Kontrol (daimi nəzarət və təhlil):

- planların icrasına nəzarət;
- audit və təhlillər, uyğunsuzluqlar və səbəblər;
- planlara korreksiyaedici və preventiv təkliflər.

d) Aktuallaşdırma (davamlı təkmilləşdirmə):

- planları təkmilləşdirmək və razılaşdırmaq;

– risk, prosedur və vasitələr reyestrlərini təkmilləşdirmək;
– qayda və təlimatları təkmilləşdirmək.

İnformasiya təhlükəsizliyi risklərinin aşağıdakı təsnifat bölmələri mövcuddur:

– risklərin hədəf sahələri üzrə – tamlığa, əlçatanlığa, konfidensiallığa.
– risklərin üsulları üzrə – hücumlar, zəifliklər, təsadüfi hərəkətlər, texnogen proseslər;
– risklərin mənbələri üzrə – daxili və ya xarici.

İTİ prosedurları təyinat üzrə preventiv, pozuntu hallarını aşkarlama, pozucu subyektləri aşkarlama, lokallaşdırma, pozuntuların təsirini daraltma, təhlükəsizlik rejimini bərpaetmə kimi siniflərə bölünür.

İTİ prosedurlarının əsas vəzifələri aşağıdakılardan ibarətdir:

– cəhd edilən və baş verən təhlükəsizlik hadisələrinin tez müəyyən edilməsinə imkan verməli;
– təhlükəsizlik insidentlərinə cavab reaksiyası verməyə nabil olmalı;
– təhlükəsizlik hadisələrinin operativ qeydiyyatını təmin etməli;
– təhlükəsizlik insidentlərinin səbəblərinin təhlilinə imkan yaratmalıdır.

AZS-494:2010, ISO/IEC-27001:2005 standartında korporativ mühit üçün İTİ üzrə məqsəd və prosedurların təsnifat bölmələri:

1) İnformasiya təhlükəsizliyinin idarə edilməsinin rəhbər sənədləri (normativ hüqiqi aktlar, standatlar, İTİ üçün korporativ konsepsiya və təlimatlar)

2) İnformasiya təhlükəsizliyinin təşkil edilməsi, rəhbərliyin öhdəlikləri, koordinasiya, icazələr, konfidensiallıq sazişləri

3) Aktivlərin (İTİ-nin obyektlərinin) təsnifatlaşdırılması və idarə edilməsi

8) İnsan resurslarının təhlükəsizliyi, rollar, öhdəliklər, serifikatlaşdırma və filtrasiya

4) Fiziki təhlükəsizlik və ətraf mühitin təhlükəsizliyi, energi və kabel sisteminin mühafizəsi

5) Rabitə və istismar vasitələrinin idarə edilməsi, test mühitinin avtonomluğu

6) Səlahiyyətlərin və müraciətin idarə edilməsi

7) İnformasiya sistemlərinin əldə edilməsi, işlənib hazırlanması və texniki dəstək, kriptoqrafik mühafizə

8) İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi, sübutların toplanması, CERT xidməti

9) Biznesin fasiləsizliyinin idarə edilməsi

10) Hüquqi və texniki tələblərə uyğunluq, auditi məsələləri

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İDARƏ EDİLMƏSİNİN VƏZİFƏLƏRİ VƏ "QAYNAR" PROBLEMLƏRİN HƏLLİ ÜSULLARI

İnformasiya təhlükəsizliyinin idarə edilməsi ilə bağlı olan vəzifə səlahiyyətlərinin aşağıdakı təsnifat bölmələri təklif edilir[10]:

– hüquqi təminat;
– səlahiyyətləri təyinetmə;
– standartlaşdırma;
– elmi təminat;
– təhsil, təlim, konsaltinq;
– informasiya müvəkkilyi (ombudsman);
– lisenziyalaşdırma;
– layihələndirmə;
– layihələrin ekspertizası;
– tender və müsabiqələr;
– istehsal (işləyib-hazırlama);
– telekommunikasiya təminatı;
– elektrik təminatı;
– inşaat və mühəndis təminatı;
– fiziki mühafizə;
– yanğından mühafizə;
– əməyin mühafizəsi;
– kargüzarlıq;
– sertifikatlaşdırma;
– audit;
– kibercinayətlərin təhqiqatı (əməliyyat-axtarış);
– kriminalist təminatı (sübutları toplamaq);
– administratorluq;
– texniki dəstək;
– təcili yardım (CERT);
– məlumat-sorğu və axtarış;
– məlumat yaratma;
– maliyyələşdirmə;
– təchizat və nəqliyyat daşıma;
– anbar xidmətləri;
– kommunal xidmətlər.

İnformasiya təhlükəsizliyinin idarə edilməsinin iştirakçıları aşağıdakılardır:

– Azərbaycan Respublikasının Prezidenti (icra hakimiyyəti);
– Azərbaycan Respublikasının Nazirlər Kabineti;
– Azərbaycan Respublikasının Milli Məclisi (qanunvericilik hakimiyyəti);
– məhkəmə hakimiyyəti orqanları;
– Azərbaycan Milli Elmlər Akademiyası;
– mərkəzi icra hakimiyyəti orqanları;
– Azərbaycan Respublikasının Prezidenti yanında Dövlət Sirrinin Mühafizəsi üzrə İdarələrarası Komissiya;
– İKT üzrə fəaliyyəti göstərən özəl qurumlar və fiziki şəxslər;
– sertifikatlaşdırma orqanları;
– CERT şəbəkəsi.

İTİ-nin aşağıdakı "qaynar" problemlərini qeyd etmək zəruridir:

1) İTİ üzrə səlahiyyətlərin bu idarəetmə iştirakçıları arasında bölgüsünü dəqiqləşdirmək;

2) İTİ üzrə səlahiyyətlərin icrasını koordinasiya etmək;

3) İnformasiya təhlükəsizliyi üzrə qanunvericilik bazasını müasir tələblərə uyğunlaşdırmaq;

4) İnformasiya təhlükəsizilyi üzrə təhsili, administartorların filtrasiyasını təşkil etmək;

5) İnformasiya təhlükəsizliyi insidentlərinin qeydiyyatını, statistikasını və və auditini yaratmaq;

6) İTİ üzrə fəaliyyəti adekvat maliyyələşdirmək, təhlükəsizlik həlləri üzrə əqli mülkiyyətin iqtisadi qorunmasını təşkil etmək;

7) İKT üzrə layihələrin təhlükəsizlik tələbləri üzrə dövlət ekspertizasını təşkil etmək, bunun üçün həmin layihə sənədlərinin tərtibinə müvafiq standartlar tətbiq etmək;

8) İnformasiya mühafizə vasitələrinin sertifikatlaşdırılmasını təşkil etmək, belə vasitələrin reyestrini yaratmaq;

9) Bütün dövlət orqanlarının, fəaliyyəti İKT ilə əlaqəsi olan bütün qurumların İSO/İEC-27001 üzrə sertifikatlaşdırılması mütləqliyini təşkil etmək (Qeyd: həmin standart ilə ISO-9001, ISO-14001, ISO/IEC-12207 standartları arasında olan uyğunluqlardan istifadə olunarsa, bu iş asanlaşar).

ƏDƏBİYYAT

[1] "Azərbaycanda informatikanın təşəkkülü" kitabı, Bakı, 2011-ci il

[2] "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya (2003-2012-ci illər)" // "Azərbaycan" qəzeti, Bakı, 2003-cü il 18 fevral, № 38, www.e-qanun.az.

[3] "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı"nın (Elektron Azərbaycan)", Azərbaycan Respublikası Prezidentinin 2005-ci il 21 oktyabr tarixli 1055 nömrəli Sərəncamı, www.e-qanun.az.

[4] "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan)", Azərbaycan Respublikası Prezidentinin 2010-cu il 11 avqust tarixli Sərəncamı, www.e-qanun.az.

[5] "Azərbaycan Respublikasında 2010-2011-ci illərdə "Elektron hökumət"in formalaşdırılması üzrə Fəaliyyət Proqramı", Azərbaycan Respublikası Nazirlər Kabinetinin 2010-cu il 14 may tarixli 136s nömrəli sərəncamı

[6] "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı", 26 sentyabr 2012-ci il, www.e-qanun.az

[7] Avropa Şurasının 2001-ci il 23 noyabr tarixli 185 № -li "Kibercinayətkarlıq haqqında" Konvensiyasının təsdiq edilməsi barədə Azərbaycan Respublikasının qanunu, 30 sentyabr 2009-cu il, № 874-IIIQ, www.e-qanun.az.

[8] Avropa Şurasının 1981-ci il 28 yanvar tarixli 108 №-li "Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxslərin qorunması haqqında" Konvensiyasının təsdiq edilməsi barədə Azərbaycan Respublikasının qanunu, 30 sentyabr 2009-cu il, № 879-IIIQ, www.e-qanun.az.

[9] "İnformasiya Təhlükəsizliyi. Təhlükəsizlik metodları.İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri.Tələblər." AZS 494-2010 (Information technology. Security techniques. Information security management systems. Requirements ISO/IEC 27001-2005)

[10] "Milli informasiya məkanının təhlükəsizlik arxitekturası", Elçin A.Əliyev, Rasim Alquliyev, Yadigar İmamverdiyev, "Kibernetika və informatika problemləri" – PCI'2012 IV Beynəlxalq konfransın materialları, Bakı şəhəri, 12-14.09. 2012-ci il