Proqram Təminatı və Fərdi Məlumatların Təhlükəsizliyi Məsələləri

Elçin Əliyev[1], Yadigar İmamverdiyev[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*elchinaa@gmail.com*, [2]*yadigarimam@gmail.com*

***Xülasə*— Bu məqalədə "proqram təminatı" və "fərdi məlumatların təhlükəsizliyi" sahələrinə aid məsələlər qoyulur. Bunun üçün: həmin anlayışlar və onların predmetini formalaşdıran komponentlər identifikasiya edilir;bu predmet komponentləri arasında səbəb-nəticə və digər qarşılıqlı təsir əlaqələri dəqiqləşdirilir;bu sahələrə aid normativ hüquqi və texniki aktlarəsasında informasiya təhlükəsizliyi tələbləri və səlahiyyətlər bölgüsü aləti araşdırılır.**

Açar sözlər*— *proqram təminatı, fərdi məlumatlar, informasiya təhlükəsizliyi, təhlükəsizlik alətləri, səlahiyyətlər bölgüsü.

I. GİRİŞ (ƏSAS ANLAYIŞLAR)

Bu məqalədə istifadə olunan "proqram təminatı", "fərdi məlumatlar" və "informasiya təhlükəsizliyi" anlayışlarını milli və beynəlxalq normativ hüquqi və texniki aktlar aşağıda göstərilən oxşar mənalarda izah edir[1-6]:

A. Proqram təminatı

Proqram təminatı vasitəsi –funksional təyinata, tərkib hissələrinə və parametrlərə malik olur, İKT məhsuludur, sənədləşdirilə və identifikasiya oluna bilir.

Proqram təminatı vasitələrininəsas kateqoriyaları aşağıdakılardır:

- biznes təyinatlı tətbiqi proqram təminatı vasitələri, onların tərkib hissələri və funksional imkanlar;
- əməliyyat sistemləri;
- verilənlər bazalarını idarəetmə sistemləri;
- kompüter şəbəkələrini idarəetmə sistemləri;
- xüsusi proqram əlavələri (utilitlər).

Proqram təminatı vasitəsi müəyyən kompüterləşdirilmiş (avtomatlaşdırılmış) sistemin konfiqurasiya obyektidir.

Bu sistemlər – tətbiq sahəsinə aid informasiya proseslərini təmin edən aşağıdakı üsul və vasitələrinnizamlanmış toplumudur:

- informasiya resursları;
- proqram təminatı vasitələri;
- texniki təminat vasitələri;
- kompüter şəbəkəsi infrastrukturu;
- mühəndis qurğuları və vasitələri;
- funksionallıq prosedurları, sxemləri və rollar;
- üsul və vasitələrə səlahiyyətlər bölgüləri.

B. Fərdi məlumatlar

Fərdi məlumatlar – şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən informasiyadır.Fərdi məlumatlar şəxsin özü və ailə həyatı ilə bağlı olur.

Fərdi məlumatların informasiya resursu qanunvericiliklə müəyyən edilmiş məqsədlə, səlahiyyətli qurumlar və ya şəxsin özü tərəfindən müvafiq qaydalarla formalaşdırılır, istifadə olunur, həmin informasiya resursunun sahibi tərəfindən mühafizə edilir.

C. İnformasiya təhlükəsizliyi

İnformasiya təhlükəsizliyi – onun tamlıq, əlçatarlıq və konfidensiallıq xassələrinin təmin edilməsidir, informasiya prosesləri üçün tətbiq olunan üsul və vasitələrin yetərli və yararlı olmasıdır.

D. Normativ texniki tələblərin mənbələri – standartlar

Proqram təminatı vasitələrinin və kompüterləşmiş sistemlərinin həyat tsikli prosesləri və informasiya təhlükəsizliyi tələbləri, müvafiq olaraq, ISO/IEC-12207 [1], ISO/IEC-15288 [2], ISO/IEC-27001 [3] standartlarına uyğun müəyyən edilir.

II. PROQRAM VASİTƏLƏRİNİN VƏ KOMPÜTERLƏŞMİŞ SİSTEMLƏRİN HƏYAT TSİKLİ PROSESLƏRİ

ISO/IEC-12207:2008 standartı proqram təminatının həyat tsikli prosesləri üçün beynəlxalq standartdır, onun ilk versiyası hələ 1995-ci ildə qəbul olunmuşdu. Proqram təminatının həyat tsikli – fasiləsiz prosesdir, proqramın yaradılmasının zəruriliyi haqqında qərar qəbulu anından başlayır və onun istismardan tam çıxarılması anında başa çatır. ISO/IEC-12207:2008 standartı proqram təminatının işlənməsi və tətbiqi üzrə vahid terminologiya daxil edir, proqram təminatının həyat tsikli və həyat tsikli modeli anlayışlarını bir-birindən ayırır, həyat tsiklinin təşkilinin və strukturunun (proseslərinin) təsvirini verir. Standart həmçinin həyat tsiklinin konkret modellərini qurmaq üçün adaptasiya proseslərini ayırır.

ISO/IEC-12207:2008 standartıproqram sistemlərinin həyat tsikli ərzində yerinə yetirilə bilən müxtəlif işləri yeddi proses qrupu üzrə təsnif edir:

- razılaşdırma prosesləri(2 proses);
- layihənin təşkilati təminatı prosesləri(5 proses);
- layihə prosesləri (7 proses);

DOI: 10.25045/NCSoftEng.2017.74

- texniki proseslər(11 proses);
- proqram vasitələrinin reallaşdırılması prosesləri(7 proses);
- proqram vasitələrinin dəstəklənməsi prosesləri(8 proses);
- proqram vasitələrinin təkrar tətbiqi prosesləri (3 proses).

Bu qruplar çərçivəsində həyat tsiklinin hər bir prosesi məqsəd və arzulanan nəticələr və bu nəticələrə nail olmaq üçün yerinə yetirilməsi zəruri olan hərəkətlər və məsələlər siyahısı ilə təsvir olunur.

ISO/IEC-12207:2008 həyat tsiklinin konkret modelini təklif etmir. Onun müddəaları proqram sistemlərinin yaradılmasının həyat tsiklinin istənilən modeliüçün ümumidir. Standart həyat tsikli proseslərinin strukturunu təsvir edir, lakin bu proseslərə daxil olan hərəkətlərin və məsələlərin necə yerinə yetiriləcəyini və ya reallaşdırılacağını konkretləşdirmir.

Proqram sistemlərinin geniş tətbiqi səbəbindən proqram təminatına və onun yaradılması proseslərinə ayrılıqda (təcrid edilmiş şəkildə) yox, sistemlərin və onların yaradılması proseslərinin tərkib hissəsi kimi baxılması daha məqsədəuyğundur. Buna görə ISO/IEC 12207 standartından sonra 2002-ci ildə sistemlərin həyat tsikli proseslərinə həsr olunmuş ISO/IEC 15288 standartı meydana çıxdı. ISO/IEC 12207 standartı ISO/IEC-15288 standartıilə sıx əlaqəlidir və bir çox məsələdə ona istinad edir.

Qeyd edək ki, ISO/IEC/IEEE 15288:2015 standartı insan tərəfindən yaradılmış və aşağıdakı sistem elementlərindən biri və ya bir neçəsi tərəfindən konfiqurasiya edilə bilən sistemlərə baxır: aparat təminatı, proqram təminatı, verilənlər, insanlar, proseslər (məsələn, istifadəçilərə xidmərlərin göstərilməsi üçün proseslər), prosedurlar (məsələn, operator üçün təlimatlar), qurğular, materiallar və təbii meydana çıxan subyektlər.

III. FƏRDİ MƏLUMATLAR SAHƏSİNDƏ QANUNVERİCİLİKLƏ TƏNZİMLƏMƏ MƏSƏLƏLƏRİ

Fərdi məlumatlar toplandığı andan mühafizə olunur və bu məqsədlə konfidensial və açıq kateqoriyalara bölünür.

Fərdi məlumatlar yalnız qanuni məqsədlər üçün toplanılmalı və göstərilmiş məqsədlərə uyğun üsullarla işlənilməlidir. Bu məlumatların həcmi və xarakteri həmin məqsədlərə və mülkiyyətçilərin səlahiyyətlərinə uyğun olmalıdır.

Fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi proseslərinə bu məlumatın subyektinin nəzarət hüquqları üçün milli və beynəlxalq normativ hüquqi aktlarla təminat verilir. Bu sahədə dövlət tənzimlənməsi üçün aşağıdakı tədbirlər görülür:

- bu informasiya sistemlərinin, habelə müvafiq informasiya texnologiyaları vasitələrinin sertifikatlaşdırılması;
- hüquqi və texniki sənədləşdirmənin standartlaşdırılması, layihə sənədlərinin dövlət ekspertizası;

Fərdi məlumatların subyekti aşağıdakı hüquqlara malikdir:

- ona təminat verilmiş tədbirlər barədə məlumat almaq;
- özü barəsində toplanılmış fərdi məlumatların məzmunu ilə tanış olmaq, onların mühafizəsini tələb etmək;
- özü barəsində fərdi məlumatların toplanılmasına və işlənilməsinə qadağan qoyulmasını tələb etmək.

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİNİ TEXNİKİ STANDARTLARLA İDARƏETMƏ MƏSƏLƏLƏRİ

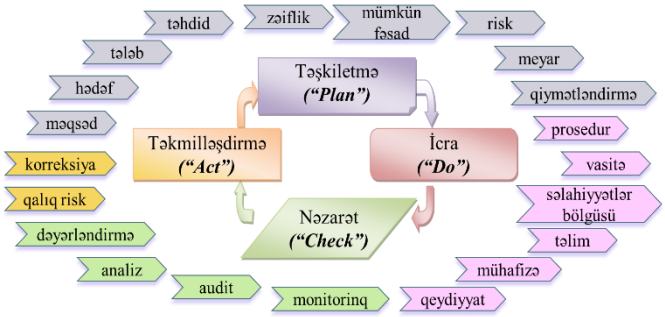
A. İnformasiya təhlükəsizliyini idarəetmə

İnformasiya təhlükəsizliyinin idarəedilməsi prosesləri iki əsas istiqamət üzrə qruplaşır [7]:

- riskləri idarəetmə;
- insidentləri idarəetmə.

İnformasiya təhlükəsizliyini idarə etmək üçün aşağıdakı prinsiplər tətbiq olunur (şəkil 1):

- strukturlaşdırma, dekompozisiya;
- prosesli yanaşma;
- risklərə adekvatlıq;
- üsul və vasitələrə səlahiyyətlər bölgüsü,cavabdehlik;
- mühafizədə çoxeşalonlu və çeşidli olma;
- davamlı təkmilləşmə.



Şəkil 1. İnformasiya təhlükəsizliyinin idarə edilməsi prosesləri

Fərdi məlumatların təhlükəsizliyi bu məlumatların konfidensiallığına əsaslanır. İnformasiyanın bu xassəsinin təmin olunması üçün prioritet tədbirlər, o cümlədən səlahiyyətlər bölgüsü matrisi müəyyən edilir [8].

B. Səlahiyyətlər bölgüsü matrisi

Səlahiyyətlər bölgüsü matrisirolların üsul və vasitələrə icazələrini təyin etmək üçün tətbiq olunur, *“Role Based Access Control”* modelinə əsaslanır.

Fərdi məlumatların informasiya sistemləri üçün işlənib hazırlanan tətbiqi proqram təminatı vasitələri, onların tərkib hissələri,funksional imkanları və mümkün rollar bu sistemin layihəsində əvvəldən müəyyən edilməlidir.

İnformasiya sisteminin proqram təminatı vasitələri elə struktur vahidlərindən (proqram modullarından, proqram interfeysi rejimlərindən və s.) ibarət olmaqla layihələndirilməlidir ki, aşağıdakı şərtlər səlahiyyətlər bölgüsündə nəzərdə tutula və təmin edilə bilinsin:

DOI: 10.25045/NCSoftEng.2017.74

- bu struktur vahidləri yalnız aidiyyəti səlahiyyətlər üçün əlçatan, o cümlədən məlum olsun;

- hər bir struktur vahidinə müraciət və istifadə imkanının yalnız aidiyyəti işçi yerləri və təyin olunmuş seans (iş, növbə) vaxtı üçün əlçatanlı olması təmin edilsin.

Fərdi məlumatların informasiya resursları elə struktur vahidlərindən (məsələn, verilənlər bazalarından, onların məlumat cədvəllərindən) ibarət olmaqla layihələndirilməlidir ki, aşağıdakı şərtlər səlahiyyətlər bölgüsündə nəzərdə tutula və təmin edilə bilinsin:

- bu struktur vahidləri, o cümlədən həmin vahiddə olan informasiya yalnız müvafiq səlahiyyətlər üçün aidiyyəti üzrə açıq, tam və əlçatar olsun;

- hər bir struktur vahidində aparılan informasiya proseslərinin yalnız müvafiq səlahiyyətlər üçün əlçatar olması təmin edilsin;

- hər bir struktur vahidinə müraciət imkanının yalnız müvafiq işçi yerlər və təyin olunmuş seans (iş, növbə) vaxtı üçün əlçatar olması təmin edilsin.

ƏDƏBİYYAT

[1] ISO/IEC-12207: 2008 “Systems and software engineering. Software life cycleprocesses.”123 p. 2008.

[2] ISO/IEC-15288: 2015 “Systems engineering. System life cycle processes.” 108 p. 2015.

[3] ISO/IEC-27001:2013 “Information technology. Security techniques. İnformation security management systems. Requirements.” 23 p. 2013.

[4] Council of Europe Convention No. 108: “Convention for the protection of individuals with regard to automatic processing of personal data.” Strasbourg, 28/01/1981.

[5] “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu, 1998.

[6] “Fərdi məlumatlar haqqında” Azərbaycan Respublikası Qanunu, 2010.

[7] E. A. Əliyev, “Korporativ informasiya sistemlərində informasiya təhlükəsizliyinin menecmenti üçün təhlükəsizlik tələblərinin təsnifatlmodeli,” İnformasiya cəmiyyəti problemləri, №2(8), s. 67-76, , 2013.

[8] E. A. Əliyev, “Korporativ mühitdə biznes, informasiya texnologiyaları və təhlükəsizliyi üzrə fəaliyyət növlərinin koordinasiyası problemləri,”İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransının materialları, səh. 209-212, 2015.

DOI: 10.25045/NCSoftEng.2017.74