Fərdi məlumat subyektlərinin hüquqlarını mühafizə mexanizmlərinə etimad səviyyəsinin ölcülməsi metodu

Elçin Əliyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
elchinaa@gmail.com

***Xülasə*— Bu məqalədə fərdi məlumatların informasiya sistemlərində şəxsin hüquqlarını mühafizə mexanizmlərinin mükəmməllik və etimad səviyyələrini ölcmək üçün bir metodun işlənilməsi problemi qoyulur. Bu problemin həlli üçün: a) fərdi məlumat subyektlərinin hüquqları, bu hüquqları mühafizə mexanizmləri beynəlxalq və milli normativ alətlər əsasında identifikasiya olunur; b) bu mühafizənin obyektlərinin ümumi səviyyədə arxitekturası müəyyən edilir, bu sahədə və bu səviyyədə etalon müqayisə üçün orientir (*“benchmark”*) təyin olunur; c) beynəlxalq standartların təklif etdiyi mükəmməllik və etimad meyarları, müvafiq qiymət (reytinq) şkalaları və fərdi məlumatların mühafizəsində bu meyar və şkalaların tətbiqi imkanları araşdırılır; d) fərdi məlumatların mühafizəsinin obyektlərinə, mükəmməllik səviyyələrini və onlara etimad dərəcələrini ölcmək üçün metod təklif olunur; e) bu ölcmə metodunun tətbiq sahəsi, o cümlədən e-dövlətdə fərdi məlumatların təhlükəsizliyinə “etimad zonaları”nı müəyyən edə bilmək üçün hüquqi və texnoloji əhəmiyəti təsvir olunur.**

Açar sözlər— fərdi məlumatların mühafizəsi; mühafizə obyekti; mühafizə aləti; etimad səviyyəsi; etimad meyarı; ölcmə metodu; qiymət şkalası; etimad zonası; GDPR

I. GİRİŞ

Məlumdur ki, hər bir fəaliyyətin icraçısı (operatoru) tərəfindən ona bu fəaliyyət prosesləri üçün lazım olan informasiya yaradılır (əldə olunur), işlədilir və mühafizə olunur. Bu informasiyanın həmin fəaliyyət üçün təhlükəsizliyinin (tamlıq, əlçatarlıq, konfidensiallıq və dəyərlilik xassələrinin) təmin olunma əmsalı fəaliyyət davamlılığının təmin olunma dərəcəsinə təsir edir, kritik parametr olur.

Əldə olunma növünə görə informasiya ümumi istifadə üçün açıq olan və məhdudlaşdırılan kateqoriyalara bölünür, məxfi (dövlət sirri) və konfidensial (fərdi məlumat, xidməti sirr, o cümlədən həkim, vəkil, notariat və digər peşə sirləri, kommersiya sirri, bank sirri, istintaq və məhkəmə sirri) olur.

Məxfi və konfidensial informasiya onun subyekti olan dövlət, özəl və içtimai təşkilatın öz qanuni maraqlarını həyata keçirmək üçün özü (kontroller) və ya təyin etdiyi icraçı (operator) tərəfindən yaradılır (əldə olunur), işlədilir, mühafizə olunur. Bu informasiyanın təhlükəsizliyinin, o cümlədən konfidensiallığının pozulması həmin subyektin (kontrollerin) qanuni maraqlarının pozulmasına və bu subyektin fəaliyyət davamlılığına, nüfuzuna aid fəsadların yaranmasına səbəb olur.

İnformasiyanı mühafizə üsullarının və vasitlərinin yetərliyi və yararlığı üçün məqbul hədd və təhlükəsizlik tələbləri bu fəsadların və onları yaradan təhdidlərin ölçüsunü nəzərə almaqla təyin edilir. Bu hədd həmin ölçüdən aşağı olmamalıdır. Təhlükəsizlik tələbi mühafizə obyektinə təhdidin qarşısını almaq və ya onun yarada biləcəyi fəsadı minimallşadırmaq, bu obyektdə təhdidin istifadə edə biləcəyi zəifliyi aradan qaldırmaq üçün – nəticədə fəaliyyət davamlılığını təmin edə bilmək və ya məqbul həddə bərpa edə bilmək üçün təyin edilir.

Fərdi məlumatlar dövlət, özəl, içtimai təşkilat və fiziki şəxs (kontroller), o cümlədən həmin məlumat subyektinin özu tərəfindən yaradılır (əldə olunur), işlədilir, mühafizə olunur. Fərdi məlumatların təhlükəsizliyinin, xüsusən də konfidensiallığının pozulması nəticəsində kontrollerə və həmin fərdi məlumatın subyektinə müəyyən fəsad yaranır. Subyekt üçün fəsadın ölçüsü kontroller üçün fəsadın ölçüsündən daha kritik, daha böyük ola bilir.

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə təsir imkanları həmin məlumatların subyektində minimal, hətta yox dərəcədə olur, kontrollerdə (onun opeatorunda) maksimal, hətta absolyut dərəcədə olur.

Bu isə kontrollerin fərdi məlumat subyekti qarşısında məsuliyyətinin dəqiq təyin edilməsini, fərdi məlumat subyektinin bu sahədə hüquqlarının kontroller tərəfindən mühafizə olunma, fərdi məlumatlar ilə əlaqədar olan fəaliyyətin ölçmə subyekti tərəfindən monitorinq-audit-dəyərləndirmə səviyyələrinin, bu səviyyələrə subyektin etimad dərəcəsinin ölçülə bilinməsini zəruri edir.

DOI: 10.25045/NCInfoSec.2019.26

Bu məqalədə onun istinadlar bölməsində siyahısı verilmiş mənbələrdə müəyyən edilmiş normalardan və anlayışlardan istifadə olunur.

Fərdi məlumatların mühafizəsinə bu məlumatlar ilə əlaqədar olan fəaliyyəti təmin edən arxitekturanın obyektləri, proeseslər və subyektləri, o cümlədən onların və struktur vahidlərinin, onlar arasında asılılıq əlaqələrinin mükəmməlik vəziyyəti təsir edir:

Obyektlər – milli və korporativ informasiya məkanlarının fərdi məlumatlar üzrə seqmqentləri, ölkənin bimetrik identifikasiya sistemi, əhali reyestri, fərdi identifikasiya nömrəsi (FİN) servisi, fərdi məlumatların informasiya sistemləri, əhaliyə e-xidmətlər, serverlər kompleksləri, telekommunikasiya və kompüter şəbəkəsi infrastrukturları, avtomatlaşdırılmış məlumat faylları, fərdi məlumatların informasiya sistemlərinin dövlət reyestri, İKT konfiqurasiyanın məlumat bazası (*“CMDB”*), məlumat toplularına, fayllara və proqram təminatı vasitələrinin modullarına icazələr matrisaları, risklər reyestri, monitorinq servisi, mühafizə servisləri, ehtiyat surətlər, İKT məhsulları işləyib hazırlama alətləri, sınaq-test mühiti, “*ServiceDesk*” portalı, “*CERT/CSİRT*” portalı, insidentlərin qeydiyyat bazası, “biliklər bankı”, servislər kataloqu, “*SysEventLog*” faylları və s. vahidlərdən ibarət olur;

Proseslər – məçburedici (*“imperative”*) əsaslar, tətbiqetdirici aktlar (*“implementing act”*), iş axınlarının təsviri (*“work flow”*), onların nəticələrinin və şəhadətlərin *(“evidence”)* qeydiyyatı (sübut toplama) və s. vahidlər əsasında müəyyən olunur:

a) məçburedici əsaslar – beynəlxalq və milli normativ hüquqi aktlar, beynəlxalq, regional, milli texniki normativ hüquqi aktlar (standartlar, qabaqcıl tövsiyələr topluları), subyektlər haqqında əsasnamələr, beynəlxalq və milli səviyyəli məsuliyyət (vəzifə və hüquqlar) bölgüsü matrisaları, kompetensiya tələbləri, reytinq şkalaları, məcburi korporativ qaydalar (*“binding corporate rules”*) və s.;

b) hədəflər – milli və korporativ dəyərlər, prinsiplər, strategiyalar, siyasətlər, strategi proqramlar, taktiki və operativ planlar, kompetensiya tələbləri və s.;

c) tətbiqetdirici aktlar – lokal normativ hüquqi aktlar, davranış kodeksləri, struktur bılmələr haqqnda əsasnamələr, vəzifə təlimatları, korporativ və infrastruktur səviyyəli məsuliyyət (vəzifə və hüquq) bölgüsü matrisaları, reqlamentlər, müqavilə, razılaşma və öhdəliklər, zəmanətlər, sertifikatlar, lisenziyalarqiymətləndirmə şkalaları və s.;

d) iş axınları – müraciət, təhlil, layihələndirmə, ekspertiza, işləyib hazırlama, sınaqlar, tətbiq, istifadə, məlumat-sorgu və axtarış, təhlil, məlumat mübadiləsi, psevdonimləşdirmə (adsızlaşdırma), xidmət, sorğu, monitorinq, statistika, müqayisə, audit, qiymətləndirmə, kompensasiya, araşdırma, verifikasiya və validasiya test ssenari, həll və ya imtina, dəyişiklik və təkmilləşdirmə və s.;

e) şəhadətlər – sınaq testi qiymətləri, konfiqurasıyanın, zəifliklərin və anomaliyaların, iş axınlarının və digər hadisələrin, fəsadların qeydiyyaları və s.;

Subyektlər – fərdi məlumat subyektı, kontroleri, mülkiyətçisi, operatoru (emalçı/içraçı, “processor”), ekspert, inspektor, səlahiyətli müşahidəçi (“supervisory authority”), rəhbər orqan, şura, istifadəçi, digər maraqlı tərəf və s. fiziki və hüquqi şəxslərdən ibarət olur.

II. MƏSƏLƏNİN QOYULUŞU

Fərdi məlumatların mühafizəsinə subyektin etimadı müəyyən oluna və onun dərəcəsi ölçülə bilinməlidir. Bu isə:

Subyekt qarşısında kontrollerin məsuliyyətinin daha dəqiq təyin edilməsini, meyarların konktretləşdirilməsini, kontrollerin fəaliyyətinin və idarəetmə alətlərinin (kontrolların), o cümlədən funksionallıq və konfiqurasiyanın (onların göstəricilərinin) meyarlara uyğunluğunun monitorinqini zəruri edir;

Fərdi məlumatların toplanılmasında, işlənilməsində, mühafizəsində iştirak edən tərəflərin kompetensiya, resurs potensialı və fəaliyyət mükəmməliyindən, onların istifadəsində olan meyar, şəhadət, alət və aşağıda göstərilən digər amillərin formalaşdırılması dərəcəsindən asılı olur:

a) kontrollerlər – fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə (qanuni əsaslarla bu sahədə həvalə edilmiş digər vəzifə və hüquqların həyata keçirilməsinə) lazım olan infrastrukturun, informasiya sistemlərinin mülkiyyətçiləridir, sahibləridir;
b) ölçmə subyekti – ölçmə üçün meyarlara və metodlara, o cümlədən alətlərə aid kompetensiyaya malik olan mütəxəssis resurslarından seçilir, formalaşdırılır, səlahiyətli müşahidəçi (*“supervisory authority”*), inspektor rollarını icra edir;
c) kontrollerin məsuliyyəti – kontrollerin fəaliyyətinə normativ tələblərdir (onun qəbul etdiyi öhdəliklər vasitəsilə qoyulur, ölçmə üçün meyar olur);
d) ölçmənin obyekti – kontrollerin işgüzar (biznes) fərdi məlumatlar ilə əlaqədar olan fəaliyyəti, tətbiq etdiyi üsul və vasitələrdir;
e) ölçmənin predmeti – ölçmə üçün obyektin təyin olunmuş meyarlara uyğunluğunu müəyyənləşdirmə vəzifəsidir;
f) ölçmə üçün şəhadətlər – kontrollerin bu fəaliyyətinində yaradılan sənədləşdirilmiş informasiyadır (sənədlər və yazılar), tətbiq olunan üsul və vasitələrin funksionallıq və konfiqurasiya göstəriçiləridir;
g) ölçmə üçün metod – ölçmə üçün meyar, obyekt, predmet və şəhadətlərdən asılı olaraq müəyyən olunan üsuldur;

h) ölçmə üçün alətlər – ölçmə üçün metodlarlar əsasnda yaradılır, üsullardan (siyasətlərdən, prosedurlardan, alqoritmlərdən), vasitələrdən (proqram və texniki təminat məhsullarından), reqlamentlərdən (səlahiyyətlər bölgüsündən, əlaqələr və məhdudiyyət sxemlərindən) və informasiya resurlarından (verilənlər və biliklər bazalarından) ibarət servisdir.

Fərdi məlumatların mühafizəsinə etimad səviyyəsinə bu məlumatların toplanılmasına və işlənilməsinə milli və beynəlxalq qanunvericilik əsasında təyin edilmiş şərtlər və onlara əməl olunma vəziyyəti, fərdi məlumat subyeklərinə verilmiş hüquqlar və onların həyata keçirilmə imkanları, fərdi məlumat kontrollerlərinə həvalə edilmiş vəzifələr və onların həyata keçirilmə vəziyyəti təsir edir.

Fərdi məlumatların toplanılmasına və işlənilməsinə təyin edilmiş əsas şərtlər aşağıdakılardır:

a) Fərdi məlumatlar yalnız məçburedici əsaslara, tətbiqetdirici aktlara uyğun olaraq və əvvəlcədən dəqiq müəyyən olunmuş hədəflər üçün toplanılmalı və onlara adekvat üsullarla işlənilməlidir. Bu əsaslar aradan qalxdıqda həmin məlumatlar təxirə salınmadan məhv edilməlidir
b) Fərdi məlumatların toplanılması və işlənilməsi subyekt buna öz razılığını verdikdə, yaxud qanunla müəyyən olunmuş hallarda məcburi xarakter daşıdıqda, yaxud bu məlumatlar açıq kateqoriyalı olduqda həyata keçirilə bilər.
c) Toplanılan və işlənilən fərdi məlumatların həcmi və xarakteri bəyan edilmiş hədəflərə və kontrollerin səlahiyyətlərinə uyğun olmalıdır.
d) Elmi və statistik tədqiqat məqsədləri üçün fərdi məlumatlar onların mütləq qaydada adsızlaşdırılması (psevdonimləşdirilməsi) aparılmaqla işlənilməlidir.
e) İnformasiya sistemlərində və ehtiyatlarında fərdi məlumatların toplanılması, işlənilməsi, sorğuların verilməsi və icrası, ərizələrin qeydiyyatının və baxılmasının nəticələri, habelə informasiya sistemlərinin idarə olunması və mühafizəsi ilə bağlı əməliyyatlar barədə qeydlər müvafiq nəzarət-audit jurnallarında toplanılmalıdır, bu qeydiyyatlar kontroller (və ya onun operatoru) tərəfindən təmin olunmalıdır.
f) Fərdi məlumatların transsərhəd ötürülməsi qanunvericiliklə müəyyən olunan tələblərə riayət edilməklə həyata keçirilir. Transsərhəd ötürülmə üçün nəzərdə tutulan ölkənin qanunvericiliyi həmin məlumatların Azərbaycan Respublikasının qanunvericiliyi ilə müəyyən edilmiş səviyyədə hüquqi mühafizəsini təmin edə bilməlidir, əks halda bu ötürülmə qadağan edilir.

Fərdi məlumat subyeklərinə verilmiş əsas hüquqlar aşağıdakılardır:

a) özü barəsində fərdi məlumatlar mövcud olan informasiya sistemləri, məlumatların məzmunu, bu məlumatların toplanılmasının və işlənilməsinin hüquqi əsası, məqsədi, işlənilmə müddəti, üsulları, əldə edilmə mənbələri, bu sistemlərin kontrolleri və operatoru, məlumat mübadiləsi aparılması nəzərdə tutulan informasiya sistemlərinin dairəsi haqqında məlumat almaq;
b) fərdi məlumatların toplanılmasının və işlənilməsinin qanunvericiliklə müəyyən olunmuş qaydada məcburi xarakter daşıdığı hallar istisna olmaqla, subyekt onun barəsində olan məlumatların toplanılmasına və işlənilməsinə razılıq və ya etiraz etmək (etirazın əsaslandırılması tələb olunmur), razılığı geri götürmək;
c) informasiya sistemində özü barəsində toplanılmış və işlənilən fərdi məlumatların mühafizəsini tələb etmək;
d) özü barəsində toplanılan və işlənilən fərdi məlumatların olduğu informasiya sistemlərinin uyğunluq sertifikatının mövcudluğu və dövlət ekspertizasından keçirilməsi haqqında məlumat almaq;
e) informasiya sistemində özü barəsində fərdi məlumatların dəqiqləşdirici dəyişiklik edilməsini və qanunvericiliklə müəyyən olunmuş hallar istisna olmaqla, informasiya sistemindən təxirə salınmadan çıxarılmalmasını, məhv edilməsini tələb etmək;
f) İKT vasitəsilə fərdi məlumatların toplanılması və işlənilməsi nəticəsində qəbul olunan qərar subyektin mənafeyini pozduğu halda, qanunvericiliklə müəyyən olunmuş qaydada məcburi xarakter daşıdığı hallar istisna olmaqla, bu məlumatların göstərilən üsulla toplanılmasına və işlənilməsinə etiraz etmək;
g) fərdi məlumatların toplanılması və işlənilməsi, mühafizəsi sahəsində mövcud normativ tələblərə əməl olunmaması nəticəsində onun hüquqlarının pozulduğu hallarda nəzarət orqanına və ya məhkəməyə şikayət etmək, habelə ona vurulmuş mənəvi və maddi ziyanın ödənilməsini məhkəmə qaydasında tələb etmək.

Fərdi məlumat kontrollerlərinə həvalə edilmiş əsas vəzifələr aşağıdakılardir:

a) fərdi məlumatların toplanılmasının və işlənilməsinin qanuniliyini və təhlükəsizliyini təmin etmək;
b) fərdi məlumatların korporativ informasiya sistemlərində yalnız müvafiq icazəsi olan istifadəçilərə xidmət göstərmək;
c) fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi sahəsində fəaliyyət göstərən fiziki şəxslərdən onların fəaliyyət müddətində və işdən çıxdıqdan sonra həmin məlumatların yayılmaması barədə yazılı iltizam almaq;
d) fərdi məlumatların mühafizəsinin təmin edilməsinə zəmanət verən təşkilati və texniki tədbirlər görmək;
e) fərdi məlumatların təhlükəsizliyinə təhdidləri və mühafizə səviyyəsini qiymətləndirmək;
f) fərdi məlumatlar ilə əlaqədar fəaliyyəti lisenziya əsasında həyata keçirmək;
g) fərdi məlumatların informasiya sistemlərinin dövlət qeydiyyatına alınması üçün öz tərəfinə aid tədbirlər görmək, bu qeydiyyat zəruri olan məlumatları, o cümlədən fərdi məlumatların mühafizəsi ilə bağlı öhdəsinə götürdüyü tədbirlərin, monitorinq və audit mexanizmlərinin ümumi təsvirini, əhaliyə göstərilə bilən e-xidmətlərin əhatə dairəsi barədə məlumati təqdim etmək;

h) fərdi məlumatların informasiya sistemlərini, habelə müvafiq informasiya texnologiyaları vasitələrini sertifikatlaşdırılması üçün öz tərəfinə aid tədbirlər görmək;
i) fərdi məlumatların informasiya sistemlərinin yaradılması və tətbiq edilməsi sahəsində hüquqi və texniki sənədləşdirməni və onun standartlaşdırılmasını təmin etmək;
j) fərdi məlumatların informasiya ehtiyatlarının və sistemlərinin və onların layihə sənədlərinin dövlət ekspertizasının həyata keçirilməsi üçün öz tərəfinə aid tədbirlər görmək.
k) fərdi məlumat subyekinin onun barəsində olan məlumatların toplanılmasına və işlənilməsinə etirazını aldıqda göstərilən fərdi məlumatların toplanılmasını və işlənilməsini dərhal dayandırmaq;
l) subyektdən onun fərdi məlumatlarının toplanılması və işlənilməsi üçün razılığın alınması haqqında, açıq fərdi məlumatların toplanılmasını və işlənilməsini həyata keçirilən hallarda, subyektin tələbi ilə həmin məlumatların açıq fərdi məlumatlar kateqoriyasına aid olduğu haqqında sübutları təqdim etmək**.**

III. PROBLEMİN HƏLL ÜSULLARI

Fərdi məlumatların mühafizəsinə bu məlumatların subyektinin etimad dərəcəsi bu məlumatların toplanılmasını, işlənilməsini, mühafizəsini təmin edən arxitekturanın, onun obyektlərinin, proeseslərinin və subyektlərinin, o cümlədən onların struktur vahidlərinin və onlar arasında asılılıq əlaqələrinin mükəmməlik dərəcəsinə düz mütənasib olur.

Mükəmməlik dərəcəsini ölçmə probleminin həlli üçün müəyyən alətlər müvafiq texniki normativ hüquqi aktlarda (menecment standartlarında) nəzərdə tutulmuşdur. Bu sahədə aşağıda göstərilən alətlərdən istifadə səmərəli hesab edilir:

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlənilməsinə, mühafizəsinə lazım olan obyektlərə etimadi müəyyən etmək üçün:

İKT- məhsullar onlara qoyulmuş funksional tələblərə, bu tələblər isə məçburedici (*“imperative”*) əsaslara, tətbiqetdirici aktlara (*“implementing act”*) uyğun olmalı, iş axınlarını təyinatı üzrə təmin etməli, onların nəticələrinin və şəhadətlərin *(“evidence”)* qeydiyyatlarını təyinatı üzrə və strukturlaşmış yarada bilməlidir.

a) İKT- məhsullar onlar üçün qoyulan funksional tələbləri (onlar müvafiq siniflər, ailələr üzrə təsnifatlaşdırılr) əhatə etməlidir; (Bax: Bu funksional tələblərin sinifləri, ailələri və komponentlərinin iyerarxiyasının daha detallı təsviri üçün [13].)
b) İKT-məhsullara etimad (*“assurance”*) səviyyələri (EQS, *“EAL, Evaluation Assurance Level”*) 7 dərəcəli qiymət (*“rating”*) şkalası üzrə müəyyən olunur [13] (*Qeyd: fərdi məlumat subyektinin etimadı üçün bu qiymət 4-cü dərəcədən aşağı olmamalıdır*):
   - EAL1: Funksional testetmə; *(Qeyd: Bu səviyyə etimada minimal dərəcədə zəmanətlər verir. Qiymətləndirmə obyektlərinin mühafizəsi üçün yalnız ən aşkar zəifliklərinin minimal xərclərlə aşkarlanması üçün nəzərdə tutulub. Bu səviyyədə etimad təhlükəsizliklə əlaqədar ciddi risklər olmadığı hallarda tətbiq edilə bilər.)*
   - EAL2: Strukturlu testetmə;
   - EAL3: Metodiki testetmə və yoxlama;
   - EAL4: Metodiki layihələşdirmə, testləşdirmə və dərinləşdirilmiş yoxlama;
   - EAL5: Yarıformal layihələndirmə və testləşdirmə;
   - EAL6: Layihənin yarıformal verifikasiyası və testetmə;
   - EAL7: Layihənin formal verifikasiyası və testetmə; *(Qeyd: Bu səbviyyədə etimadı qiymətləndirmə obyektlərinin mühafizəsinə praktikada real əldə edilməsi mümkün olan yuxarı dərəcədə zəmanətlər verir. Qiymətləndirmə obyektlərinin mühafizə vasitələri kompleksinin layihələndirilməsi zamanı formal modelin istifadəsi, funksional spesifikasiyaların formal təsvirləri, aşağı səviyyə layihəsinin yarıformal təsvirləri və onlar arasında uyğunluğun formal və ya yarıformal nümayişi ilə xarakterizə edilir.)*

Cədvəl: Etimad tələblərinin siniflər və ailələr üzrə iyerarxiyası və etimadın qiymətləndirmə səviyyələrinin xülasəsi.

Etimad sinfi	**Etimad ailəsi**	**EQS-ə (*“EAL”*) aid olan etimad komponentləri** (müvafiq № ilə)						
		EAL1	***EAL2***	***EAL3***	***EAL4***	***EAL5***	***EAL6***	***EAL7***
Konfiqurasiyanın idarə edilməsi – Kİ (ACM) [6]	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Təchizat və istismar (ADO) [6]	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
İşlənib-hazırlanma (ADV) [9, 10, 13]	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Rəhbər sənədlər (AGD)	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Həyat dövrünün dəstəklənməsi (ALC) [6]	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Testləşdirmə (ATE) [9, 10, 13]	ATE_COV		1	2	2	2	3	3
	ATE_ DPT			1	1	2	2	3
	ATE_ FUN		1	1	1	1	2	2
	ATE_ IND	1	2	2	2	2	2	3
Zəifliklərin qiymətləndirilməsi (AVA) [5]	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1

	AVA_VLA		1	1	2	3	4	4

(*Qeyd*: Bu etimad sinifləri, ailələri (tam və qısa adları) və komponentlərinin iyerarxiyası müvafiq standartda [13] daha detallı təsvir olunmuşdur.)

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə aid proseslərinə etimadi müəyyən etmək üçün:

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə aid proseslərin siyahısının tamlığı təmin olunmalıdır, bu proseslər arasında səbəb-nəticə asılılığı əlaqələri dəqiqləşdirilməlidir. Bu proseslərə risklər qiymətləndirilməli, o cümlədən bu proseslərdə boşluqlar, təkrarlanmalar, zəfliklər, təzadlar və mövcud meyarlara digər uyğunsuzluqlar aradan qaldırılmalıdır.

Bu proseslər üçün təyin olunan məqsədlər, tədbirlər “*SMART” (“Specific, Measurable, Achievable, Relevant, Timely”* – Konkret, Ölçüləbilən, Nəticəli/mümkün, Əhəmiyyətli/uyğun, Zamanında olma) meyarlarına uyğun olmalıdır;

Bu proseslərin mükəmməllik (*“maturity"*) səviyyələri aşağıdakı 5 dərəcəli qiymət (*“rating”*) şkalası üzrə müəyyən olunur (*müəllifin qeydi: fərdi məlumat subyektinin etimadı üçün bu qiymət 3-cü dərəcədən aşağı olmamalıdır, 0-cı səviyyə isə əslində şərtidir, yəni səviyyə yoxdur*) [12, 15]:

Qiymət (“rating”) **şkalası**	**Prosesin imkanları**	**Kontekst**
5. Optimal-laşdırılan proses	*Öncə məlum proses müəssisənin cari və gələcək məqsədlərinə nail olmaq üçün davamlı təkmilləşdirilir.*	Korporativ mühit kontekst: **korporativ biliklər**
4. Öncə məlum proses	*Müəyyənləşmiş proses verilmiş məhdudiyyətlər şəraitində nəticələr alır.*	
3. Müəyyən-ləşmiş proses	*İdarə olunan proses nəzərdə tutulan nəticələrə nail olmaq imkanına malikdir.*	
2. İdarə olunan proses	*İcra olunan proses idarə olunur (yəni planlaşdırılır, izlənilir, təkmilləşdirilir). Prosesin nəticələri yaranır, onlara nəzarət və dəstək olunur.*	Əlaqəsizlik mühiti kontekst: **fərdi biliklər**
1. İcra olunan proses	*Proses tətbiq olunur və təyinatına uyğundur.*	
0. Natamam proses	*Proses icra olunmur yaxud nəzərdə tutulan məqsədə (gözləntiyə) nail ola bilməmişdir. Prosesin nəticələri barədə qeydiyyatlar azdır yaxud yoxdur.*	

Fərdi məlumatların informasiya sistemlərinin əhatə sahəsində korporativ idarəetmə proseslərinə etimad həmin sahədə keyfiyyətin [4] və işgüzar fəaliyyət (biznes) davamlılığının [18] menecmenti sistemlərinin müvafiq standartlara uyğunluq dərəcəsindən (sertifikatlaşdırmadan) asılıdır.

Fərdi məlumatların informasiya sistemlərinin əhatə sahəsində mühafizə proseslərinə [4, 5] etimad həmin sahədə informasiya təhlükəsizliyinin menecmenti sisteminin müvafiq standartlara uyğunluq dərəcəsindən (sertifikatlaşdırmadan) asılıdır.

Fərdi məlumatların informasiya sistemlərinin həyat tsikli proseslərinə [9, 10, 13], layihə menecmenti proseslərinə [8, 16] etimad bu proseslərin müvafiq standartlara uyğunluq dərəcəsindən asılıdır.

Fərdi məlumatların informasiya sistemlərinə İKT-xidmət proseslərinə etimad bu xidmətləri idarəetmə sisteminin müvafiq standartlara [6, 7, 14, 15, 17] uyğunluq dərəcəsindən (sertifikatlaşdırmadan), xüsusən xidmətlər səviyyəsi barədə Razılaşmaların (*“Service Level Agreement, SLA”*) və xidmətlərin səmərəlilik göstəricilərinin – metrikasının (*“Key Performance Indicator, KPI”*) mükəmməlik səviyyələrindən, bu xidmətlər nəticəsində yaranan şəhadətlərin təhlükəsizliyindən (tamlığından, əlçatarlığından, konfodnesiallığından və dəyərliyndən) asılıdır.

Fərdi məlumatların subyektinin hüquqlarının mühafizə sisteminə etimad bu sistemin arxitekturasının səmərəliliyinin qiymətləndirilməsi nəticələrindən, müvafiq İKT-xidmətin (vahid pəncərə formasında e-xidmətin) formalaşdılmasından asılıdır.

Fərdi məlumatların yaradılmasında (əldə olunmasında), işlədilməsində və mühafizəsində subyektlərə etimadi müəyyən etmək üçün:

Fərdi məlumatların yaradılmasına (əldə olunmasına), işlədilməsinə və mühafizəsinə aid proseslərə və risklərə cavabdehlər təyin olunmalı və digər iştirakçı rollar müəyyən olunmalı, bu subyektlər (maraqlı tərəflər) arasında beynəlxalq və milli səviyyəli, korporativ və infrastruktur səviyyəli məsuliyyət (vəzifə və hüquqlar) bölgüsü dəqiqləşdirilməlidir. Bu bölgüdə boşluqlar, təkrarlanmalar, təzadlar və mövcud meyarlara digər uyğunsuzluqlar aradan qaldırılmalıdır.

Bu subyektlərə etimad onlara aid əsasnamələrin, vəzifə təlimatlarının bu subyektlərə həvalə olunan proseslərə uyğun olmasından, bu proseslərin həyata keçirilməsinə lazım olan kompetensiya, resurs potensialı və fəaliyyət göstəriçilərinin səviyyəsindən asılıdır.

NƏTİCƏ

Fərdi məlumat subyektlərinin hüquqlarını mühafizə mexanizmlərinə etimad səviyyəsini ölçmək üçün metodun formalaşdırılması bu etimad səviyyəsi göstəricilərinin – metrikasının (ESM) da tərtib olunmasını, bu hüquqların

mühafizəsi üzrə İKT-xidmətin (əhaliyə e-xidmətin) formalaşdırılmasını zəruri edir.

Bu ölcmə metodunun tətbiqi milli informasiya məkanının fərdi məlumatlar üzrə seqmentində, e-dövlətdə fərdi məlumatların təhlükəsizliyinə “etimad zonaları”nı müəyyən edə bilmək üçün hüquqi və texnoloji zəmin yaradılır.

İSTİNADLAR

[1] GDPR “General Data Protection Regulation”), EC, www.ec.europa.eu
[2] “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, CE, www.coe.int
[3] “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, www.-e-qanun.az
[4] ISO-9K“Quality management systems”, www.iso.org
[5] ISO/IEC-27K “Information technology. Security techniques. Information security management systems”, www.iso.org
[6] ISO/IEC 20K “Information technology. Service management. Service management system”, www.iso.org
[7] ISO/IEC-38500 “Governance of IT for the organization”, www.iso.org;
[8] ISO-21500 “Project management ”, www.iso.org
[9] ISO/IEC-12207 “Systems and software engineering. Software life cycle processes”, www.iso.org
[10] ISO/IEC-15288 “System engineering. System life cycle processes”, www.iso.org
[11] ISO/IEC/IEEE-15289 “Systems and software engineering. Content of life cycle information products (documentation)”, www.iso.org
[12] ISO/IEC-15504 “Information technology. Process assesstment”, www.iso.org
[13] ISO/IEC-15408 “Information technology. Security techniques. Evaluation criteria for IT security”, www.iso.org
[14] ITIL (“Information Ttechnology Infrastructure Library”), www.axelos.com
[15] COBIT (“Control Objectives for Information and Related Technologies”), www.isaca.org
[16] PMBOK (“Project Management Body of Knowledge”), www.pmi.org
[17] TOGAF (“The Open Group Architecture Framework”), www.opengroup.org
[18] ISO-22301 “Societal security. Business continuity management systems. Requirements”, www.iso.org

A METHOD FOR MEASURİNG OF TRUST LEVEL OF PROTECTİON MECHANİSMS FOR RİGHTS OF PERSONAL DATA SUBJECTS

Elchin Aliyev

ANAS Institute of Information Technology, Baku, Azerbaijcan,

elchinaa@gmail.com

Abstract— This article addresses the problem of developing a method for measuring the level of excellence and confidence of mechanisms to protect human rights in personal data information systems. To address this problem: a) the rights of individual data subjects and their protection mechanisms are identified on the basis of international and national regulatory instruments; (b) The overall architecture of the objects of this protection is defined, and the benchmark for benchmarking in this area and at this level is designated; c) examining the criteria for excellence and confidence offered by international standards, the appropriate value (rating) scale, and the applicability of these criteria and schemes for the protection of personal data; d) a method for measuring the level of excellence and confidence levels of data protection objects is proposed; (e) The scope of this measurement method, including the legal and technological significance of defining "zones of confidence" in the security of personal data in the e-government.

Keywords— *personal data protection, security object, security instrument, confidence level, confidence-building measure, measurement method, value scale, confidence zone, GDPR*