Proqram təminatının sınağı zamanı fərdi məlumatların təhlükəsizliyinin təmin olunması problemləri

Tofiq Kazımov[1], Nəzakət Məlikova[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*tofig@mail.ru*, [2]*naranara_68@mail.ru*

***Xülasə*— Məqalədə proqram təminatının sınağı prosesində yarana biləcək problemlər, xüsusilə fərdi məlumatların təhlükəsizliyinin təmin olunmasında yarana biləcək çətinliklər və bununla bağlı həyata keçirilə biləcək tədbirlər öz əksini tapmışdır. Daha sonra problemlərin yaranma səbəbləri araşdırılmış, testləşmə prosesində fərdi məlumatların təhlükəsizliyinin təmin olunması yolları göstərilmiş və onların nəzərə alınmasının vacibliyi vurğulanmışdır.**

Açar sözlər— proqram təminatının sınağı; məlumat təhlükəsizliyi; fərdi məlumatlar; data-masking

I. GİRİŞ

İnformasiya texnologiyaları müasir cəmiyyətin infrastrukturunun ən vacib və əvəzolunmaz elementlərindən biri sayılır. O, bəşəriyyətin sosial, mədəni inkişafı və iqtisadi fəaliyyəti üçün əsas amillərdən olmaqla, insanların müxtəlif tip məlumatlar əldə etməsini və harda olmasından asılı olmayaraq onların bir-biriylə ünsiyyət qurmasını təmin edir.

İstənilən informasiya sistemi aparat və proqram təminatından (PT) təşkil olunmuşdur. Məlumdur ki, PT-nin mürəkkəbliyi onda olan səhvlərin sayının çox olması ehtimalını da artırır. PT-də buraxılan xətalar, baş verən səhvlər, böyük fəlakətlərə, maddi ziyanlara, insanların həyatının itirilməsinə, vaxt itkisinə və müxtəlif şəbəkə infrastrukturlarnın sıradan çıxmasına səbəb ola bilər.

Müasir informasiya sistemlərinin düzgünlüyünə və etibarlılığına müəyyən mənada zəmanət, təminat vermək üçün PT-nin həyat dövrünün müxtəlif mərhələlərində sınaq metodlarından istifadə etməklə onda olan səhvlər ardıcıl şəkildə aradan qaldırılır. PT-nin sınağı (software testing) – keyfiyyətə nəzarət mexanizmlərindən biri olmaqla proqramın gözlənilən və real icrası (işi) arasındakı uyğunluğu müəyyən edir və seçilmiş testlər dəsti əsasında lazımi qaydada həyata keçirilir. Proqram təminatının sınağı zamanı mümkün səhvlər, qüsur və xətalar aşkara çıxarılaraq aradan qaldırılır [1].

Demək olar ki, hazırda proqram təminatının effektiv sınağı ilə bağlı tədqiqatlar, hələ də özünün yetkinlik mərhələsinə çatmamışdır. Çünki dünyanın ən məşhur şirkət və təşkilatları belə hər il proqram təminatlarında baş verən çoxlu sayda səhvlər nəticəsində böyük ziyanlarla üzləşirlər. Məhz buna görə də proqram təminatı sahəsində çalışan tədqiqatçılar yeni sınaq metodları tapmağa, mövcud metodları isə daha da inkişaf etdirib təkmilləşdirməyə çalışırlar [2]. Proqram təminatı sifarişçinin tələblərinə cavab verməlidir. Bunun təmin olunması üçün həm statik, həm də dinamik şəkildə analiz aparılmalıdır. Proqram təminatının sınaq mərhələsi resurslar və səylər baxımından ən çox vəsait tələb edir. Proqramı sınaqdan keçirərkən iki növ problem yarana bilər: texniki və qeyri-texniki. Ən məşhur proqram test problemləri "Üçbucaq problemi", "Sonrakı tarix problemi", "Komissiya problemi", "SATM problemi", "Kvadrat tənlik problemi" dir. Üçbucaq problemi proqram təminatında ən geniş yayılmış problemdir [3].

PT-da olan səhvləri aşkarlamaq üçün proqramın işlənilməsi prosesi başa çatdıqdan sonra “alfa” versiyası hazırlanır və əvvəlcədən müəyyən olunmuş test edən şəxs tərəfindən sınaqdan keçirilir.

II. PROQRAM TƏMİNATININ SINAĞI STRATEGİYASI

Hər hansı şirkət və təşkilatda fəaliyyət göstərən insanların fərdi məlumatları (FM), həmin şirkət və təşkilatlar üçün həssas məlumatlar hesab olunur və onların konfidensiallığının qorunması əhəmiyyətli məsələdir. Bu konfidensiallıq informasiya sistemi daxilində proqram təminatı səviyyəsində də mütləq təmin olunmalıdır. Çünki, bu məlumatların kənara sızması, itirilməsi, qərəzli məqsədlərlə dəyişdirilməsi həm fərdi şəxsə, həm də təşkilatın fəaliyyətinə ziyan vura bilər. Odur ki, hər bir şirkət və təşkilat onlara məxsus fərdi və digər məxfi məlumatların bədniyyətlilərin əlinə keçməməsi üçün müəyyən işlər görməlidir. Bu işlər, xüsusilə, PT yaradılan zaman nəzərə alınmalıdır. FM-in konfidensiallığının qorunması həm texniki, həm də proqram vasitələri ilə həyata keçirilməlidir. Texniki vasitələr dedikdə, kompüterə, şəbəkə kanallarına müdaxilənin cihaz və sistemlərlə təmin olunması, informasiya kanallarının qorunması nəzərdə tutulur. PT ilə qorunmada isə, fərdi məlumatlar yerləşən hissəyə edilən istənilən müdaxilə xüsusi proqram vasitəsilə qeydə alınaraq konfidensiallıq təmin olunur.

PT layihələndirilən zaman fərdi və məxfi məlumatların sifarişçinin tələbinə uyğun olaraq qorunması məsələsi əsas şərtlərdən biri olmalıdır. Layihələndirmənin sonunda sınaq prosesi aparılaraq PT-nin nə dərəcədə sifarişçinin tələblərinə

DOI: 10.25045/NCInfoSec.2019.44

uyğun olması yoxlanılır. Sınaq zamanı FM-in qorunmasına xüsusi fikir verilməli, onun məxfiliyinin qorunma dərəcəsi müəyyən olunmalıdır.

PT-yə olan təhdidlərin qarşısını almaq məqsədilə, proqramda əlavə modulların yazılması lazım gəlir. Təhdidlərə informasiyanın kənara sızmasını və haker hücumlarını misal göstərə bilərik [4]. Bəzən sınaq zamanı fərdi məlumatların qorunma dərəcəsini müəyyən etmək üçün PT-yə bilərəkdən sifarişçi tərəfindən hücumlar olunur. Bu hücumlar etik hakerlər tərəfindən də həyata keçirilə bilər. Fərdi məlumatlar həssas məlumatlar kateqoriyasına aid edilir. Fərdi məlumatlara misal olaraq fərdin bank, kredit, təhsil, əmək fəaliyyəti, tibbi, vergi məlumatlarını göstərmək olar.

FM həssaslığa görə, əsasən 3 kateqoriyaya bölünür:

1. Adi fərdi məlumatlar – onların emalı, istifadəsi, ötürülməsi milli qanunlarda müəyyən edilmiş qaydada, xüsusi icazə olmadan da mümkündür.
2. Həssas fərdi məlumatlar – onların yığımı, emalı, istifadəsi qanunla müəyyən edilmiş xüsusi təhlükəsizlik tədbirləri tələb edir.
3. Xüsusi həssas fərdi məlumatlar - onların emalı, istifadəsi, ötürülməsi qanuna görə qadağandır, ya da xüsusi mühafizə və təhlükəsizlik tədbirlərindən istifadə etməklə mümkündür.

FM – insan haqqında mühüm şəxsi məlumatlardır və onların dövlət təşkilatları tərəfindən, insan hüquqlarının qorunması baxımından etibarlı müdafiəsi tələb olunur. Fiziki şəxslərin təhlükəsizliyinin təmin olunmasında FM-in müdafiə sisteminin qurulması çox mühüm və vacib məsələlərdəndir. Çünki bu məlumatların qorunmaması FM-in subyekti üçün bir çox neqativ, arzuolunmaz və ziyanlı hallara gətirib çıxara bilər. Bu məqsədlə Fərdi Məlumatların adekvat Müdafiə Sistemi (FMMS) yaradılır. Sistemin yaradılması üçün aşağıdakı addımlar tövsiyə olunur [5]:

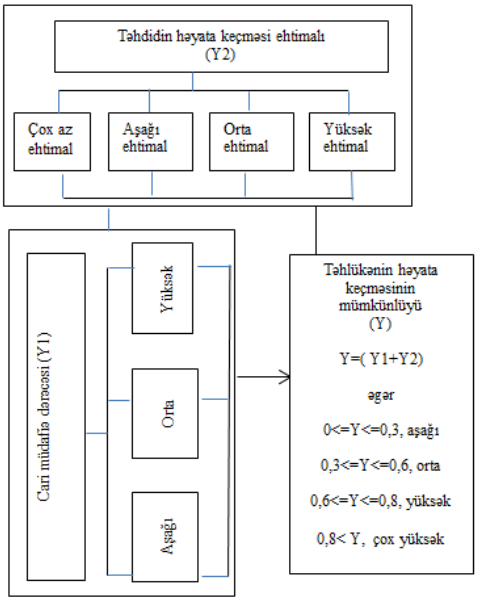
1. Fərdi Məlumatlar İnformasiya Sisteminin (FMİS) layihə qabağı tədqiqi:
   - FMİS–in təsnifatı;
   - Təşkilati-sərəncam sənədlərinin işlənib hazırlanması;
   - FMİS-in ilkin müdafiə dərəcəsinin müəyyən olunması;
   - FM-in təhlükəsizliyinə olan xüsusi təhdidlər modelinin yaradılması;
   - Xüsusi texniki tapşırığın işlənməsi.
2. FMMS-in layihələndirilməsi.
3. FMMS-in istifadəyə verilməsi.

FMİS-i FM–in kateqoriyasından asılı olaraq 4 sinfə bölürlər:

1. İrqi, milli mənsubiyyəti, siyasi baxışları, dini və fəlsəfi əqidəsi, sağlamlıq vəziyyəti, intim həyatı haqqında olan FM.
2. FM subyektini identifikasiya etməyə imkan verən və onun haqqında əlavə informasiya (1-ci kateqoriyada olan informasiya istisna olmaqla) almağa imkan verən FM.
3. FM-in subyektini identifikasiya etməyə imkan verən FM.
4. Şəxsiyyəti məlum olmayan və ya hamı üçün əlçatan FM.

Hər kateqoriya üçün informasiya sistemində informasiyanın müdafiəsi metodu və ya üsulu müəyyən olunur.

Fərdi məlumatların təhlükəsizliyi dərəcəsini müəyyən etmək üçün aşağıdakı sxemdə ekspert qiymətləndirməsi göstərilir [6].



Şəkil 1. Fərdi məlumatların təhlükəsizlik dərəcəsinin müəyyən edilməsi

III. PROQRAM TƏMİNATININ TESTLƏŞDİRİLMƏSİNDƏ YARANA BİLƏCƏK PROBLEMLƏR

Sınaqda istifadə olunan məlumatların (verilənlərin) əl ilə (*ing*. manual) hazırlanması effektiv hesab edilə bilməz. Bunun əsas səbəbi həddən artıq əl əməyinin tələb olunmasıdır. Test məlumatlarının avtomatik yaradılması isə az əmək tələb etdiyindən daha məqsədəuyğundur. Proqram təminatının sınağı zamanı istehsal (real) məlumatlarından istifadə edilməsinin üstünlükləri olsa da, bir sıra problemlər də mövcuddur. Əsasən üç problemi nəzərdən keçirirlər.

1. Həcm problemi. Sınaqda istehsal məlumatlarından istifadə etdikdə qarşılaşdığımız ən böyük problemlərdən biri məlumatların həcminin olduqca böyük olmasıdır. Bankların timsalında bunu aydın görə bilərik. Çoxsaylı müştəri məlumatlarının və onların etdikləri bütün əməliyyatların həcmi olduqca böyük olur. Sadə bir misala baxaq. 100 min müştərinin ay ərzində orta hesabla 5 əməliyyat həyata keçirməsini fərz edək. Bu, ayda təxminən 500 min əməliyyat qeydlərinin yaranması deməkdir. Bank yarandığı gündən bu günə kimi olan əməliyyatların ümumi sayı olduqca böyükdür. Təbii ki, bütün bu məlumatların testləşmə bölgəsinə köçürüləcəyi təqdirdə işin həcminin nə dərəcədə böyük olduğunu təsəvvür etmək o qədər də çətin deyil. Bütün bu məlumatların sınaq zonasına keçirilməsi klonlaşdırma üsulu adlanır. Bu da yüklənmə müddətinin və disk-yaddaş xərclərinin artması kimi bir sıra mənfi hallara gətirib çıxarır.

2. Mənbə problemi. Digər bir əsas problem məlumat mənbələrinin müxtəlifliyidir. Məsələn, məlumatlar bir çox mənbədən, yəni Oracle, DB2, SQL Server, Sybase, Excel, Word Fayllar, Mainframe faylları, Verilənlərin Elektron Mübadiləsi (*ing.* Electronic Data İnterchange, EDI) sənədləri kimi mənbələrdən əldə edilə bilər. Eyni zamanda cari məlumatlar və bu məlumat mənbələri arasında əlaqələrin olması vəziyyəti bir qədər də qəlizləşdirir. Emal olunacaq məlumatları sınaq zonasına yükləyərkən məlumat əlaqələri və məlumat bütövlüyünün qorunmasına da çox diqqət yetirilməlidir.

3. Məlumat təhlükəsizliyi problemi. Emal məlumatlarının sınaq prosesində istifadə olunmasında daha vacib problemlərdən biri də həssas məlumatların mövcudluğudur. Həssas məlumatların təhlükəsizliyinin təmin olunmaması maliyyə, marketinq və bəlkə də hüquqi sferada ciddi problemlərə səbəb olacaq bir məsələdir. Buna misal olaraq məşhur maliyyə təşkilatları və ya tibbi sığorta şirkətlərinin sistemində baş vermiş məlumatların oğurlanması hadisələrini göstərə bilərik. 2017-ci ildə Equifax (Amerika kredit tarixi bürosu) məlumatlarının oğurlanması buna ən bariz nümunələrdən biridir [7].

Həssas məlumatların qorunmamasından yaranan təhlükələrin qarşısını almaq məqsədilə təşkilatlar proqram təminatına və istehsal sistemlərinə aid prosedurlara çoxlu maliyyə vəsaiti ayırırlar. Ümumiyyətlə, onu da qeyd edək ki, istehsalat məlumatlarından sui-istifadə olunması böyük risklərə səbəb ola bilər. Bank misalında bir nümunəyə baxsaq görərik ki, istehsalat məlumatlarında adlar, ünvanlar, hesab nömrələri, qalıqlar, kredit kartı nömrələri kimi real müştəri məlumatları vardır. Bu məlumatlardan sui-istifadə etmək bank üçün ağır nəticələrə səbəb ola bilər. Belə hallarda problemin aradan qaldırılması üçün məlumat maskalanması (*ing*. data-masking) üsulundan istifadə etmək olar.

Məlumat maskalanması – həssas məlumatların dəyişdirilməsi, anonimləşdirilməsi və ya silinməsilə icazəsiz istifadənin qarşısının alınması prosesidir. Məlumatın qorunması tələbləri bir çox mənbədən, o cümlədən hökumət qanunlarından, sənaye agentliklərinin milli və beynəlxalq qaydalarından və daxili korporativ siyasətlərdən (məsələn, ödəniş məlumatları kimi həssas məlumatlardan) irəli gəlir. Bu tənzimləmələrdə format və məzmun bölgəyə görə dəyişir. Məsələn, ABŞ-ın Ədalətli və Dəqiq Kredit Əməliyyatları Qanunu (*ing.* Fair and Accurate Credit Transactions Act - FACTA), ABŞ-dakı 95/46 / EC Avropa Məlumat Qoruma Direktivindən fərqlidir. ABŞ-dakı tibbi sığorta və səhiyyə təminatçıları Tibbi Sığorta Daşınması və Hesabatlılıq Qanununa (ing. Health Insurance Portability and Accountability Act, HIPAA) uyğun olmalıdır.

Bu qaydalar zamanla dəyişdiyindən təşkilatlar dəyişiklikləri izləməli və bu dəyişikliklərə uyğunlaşmalıdırlar.

Şirkətlər və təşkilatlar məlumatların qorunması qaydalarından boyun qaçırdıqları təqdirdə, hansı cəza tədbirlərinin olacağını da bilməlidirlər. Son vaxtlar tənzimləyici orqanların həssas məlumatların itirilməsinə, tamlığının pozulmasına görə təşkilatlara böyük cərimələrin tətbiq etməsi halları olduqca geniş yayılmışdır. Məlumatların Qorumasının Ümumi Qaydası (ing. General Data Protection Regulation, GDPR) cərimələri qlobal gəlirin 4%-i və ya 20 milyon avro həcmində ola bilər. Təbii ki, faktiki məbləğ pozuntu növünə görə dəyişir və ilkin məhkəmə qərarlarında müəyyən edilmiş qaydaya uyğun olaraq müəyyənləşdirilir. Eyni zamanda burada korporativ markaya və nüfuza dəyən zərərdən də söhbət gedir. Şübhəsiz ki, şirkətin reputasiyasına, imicinə dəyən ziyan bununla əlaqəli cəzalarla müqayisədə şirkət üçün daha böyük itkidir.

IV. MƏLUMATLARIN QORUNMASI STRATEGİYALARI

Məlumatların pozulması (itirilməsi, köçürülməsi və s.) – PT-nin sınağının strategiyaları çərçivəsində həqiqi məlumatların istifadə olunmasının ən böyük təhdididir. Məlumatların qorunması üçün aşağıdakı strategiyaları göstərə bilərik [8]:

1. Həqiqi məlumatları qoruma siyasəti strategiyası. Təşkilatlar istehsal məlumatlarının qeyri-istehsal şəraitində istifadə edilməməsi üçün strategiya qurmalıdırlar. Bu strategiyada, sınaq zamanı test məlumatlarının yaradılması və ya saxlanması üçün məsuliyyət daşıyan şəxslər açıq şəkildə bilinməlidir.

2. Müvafiq giriş hüquqlarının təmin edilməsi. Təşkilatlar məlumatların qorunması məqsədilə fiziki girişi intensiv şəkildə qoruyur və istehsal mühitində məlumat pozuntularının baş verməməsini təmin etmək üçün diskləri və məlumatları hakerlərin hücumlarından qorunmaq üçün şifrələyirlər. Məhz buna görə də təşkilat test proqramı strategiyalarının bir hissəsi olaraq daxili istifadəçilər və proqram təminatını işləyənlər üçün ciddi təhlükəsizlik və girişə nəzarət mexanizmlərini təmin etməlidir.

3. Həqiqi məlumatları qorumaq üçün müvafiq üsullardan istifadə olunması. Bu üsullardan biri aşkarlayıcı üsuldur. Bu

üsul başqa cür “məlumatları həssaslaşdıran” üsul kimi də tanınır. Aşkarlayıcı üsul bir istehsal sistemindən məlumatı alaraq testləşdirmə və ya analiz üçün uyğun olmayan həssas məlumatlara çevirir.

4. Məlumat maskalanmasından istifadə edilməsi. Təşkilatların test məlumatlarının əl ilə yaradılması və məlumat maskalanması olmaqla iki variantı vardır. Qeyd edək ki, məlumatların maskalanması daha asandır. Bu texnologiyalar düzgün yerinə yetirildiyi halda səmərəlidir, genişlənə bilir və sadədir. Məsələn, yalnız həssas məlumatlar maskalanmalı və maskalanmış məlumatlar həqiqi məlumatları təmsil etməlidir .

NƏTİCƏ

Şirkət və təşkilatlar üçün keyfiyyətli proqram təminatının olması olduqca vacib və əhəmiyyətli bir məsələdir. Çünki kefiyyətli proqram təminatı şirkətin etibarlı fəaliyyətini təmin edir, onun inkişafına kömək edir. Məhz bu səbəbdən də proqram təminatının keyfiyyətinin yüksəldilməsi üçün PT- nin sınağı məsələlərinə xüsusi diqqət yetirilməlidir. Yuxarıda qeyd elədiyimiz kimi proqram təminatının həyat dövrünün müxtəlif mərhələlərində sınaq aparılaraq onda olan səhvlər ardıcıl şəkildə aradan qaldırılmalıdır. Lakin proqram təminatının sınağı zamanı bir sıra problemlər meydana çıxır ki, bunlardan da ən vacibi məlumatların təhlükəsizliyi problemidir və bu sahədə əsas problem FM-in mövcudluğu ilə bağlıdır. Təəssüf ki, bir çox şirkətlər təhlükəsizlik məsələlərini dəfələrlə, görməzlikdən gələrək və ya məlumatların qorunması öhdəliklərindən xəbərsiz olaraq çoxlu sayda problemlərlə üzləşməli olurlar. Son zamanlar FM–lə bağlı müşahidə olunan pozuntular bu məsələlərə xüsusilə ciddi yanaşmağı tələb edir. Odur ki, bütun şirkət və təşkilatlarda informasiya təhlükəsizliyi qrupları yaradılmalı, infomasiyanın və xüsusilə də FM–in təhlükəsizliyi onların daim diqqət mərkəzində olmalıdır..

İSTİNADLAR

[1] T. Bayramova, N. Abbasova, “Proqram Təminatının Verifikasiya və Sınaq Metodlarının Müqayisəli Təhlili,” Proqram mühəndisliyinin aktual elmi-praktiki problemləri I respublika konfransı, Bakı, 17 may 2017-ci il, səh. 198- 202.

[2] S.Chaudhary, “Latest Software Testing Tools and Techniques: A Review,” International, Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, may 2017, pp.538-540.

[3] K. Solanki, S. Dalal, S. R. Scholar, M.R. Scholar , “Comprehensive Study of Popular Software Testing Problems”, International Conference on “Computing for Sustainable Global Development. 1-3 March, 2017, pp.1157-1160.

[4] E. Bağırov, “Proqram təminatı boşluqlarının analizi üsulları”, Proqram mühəndisliyinin aktual elmi-praktiki problemləril I respublika konfransı, Bakı, 17 may 2017-ci il, səh. 259-262.

[5] А. А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель, «Автоматизированная система предпроектного обследования информационной системы персональных данных», «АИСТ-П» Доклады ТУСУРа, № 1 (21), часть 1, июнь 2010 , стр. 14- 22.

[6] А. А. Шелупанов, В.Г. Миронова, «Анализ этапов предпроектного обследования информационной системы персональных данных», 2011, стр. 45-48.

[7] R. Raghuraman, “Top 3 Challenges in using Production data in Test Environments”, https://tdminsights.blogspot.com/2013/02/top-3-challenges-in-using-production.html?fbclid=IwAR3tdNfVxwQIBYboUG5lcVdOerLfYbMLM2vEVZStYuk1sL8dGGQnNfElV_0

[8] Sh.Gupta,”Software testing strategy for protection of real data”, october 2010, https://www.computerweekly.com/tip/Software-testing-strategy-for-protection-of-real-data?fbclid=IwAR2ogZ3io9j3EfYS_rmLjxjgtarqMJ5EXwb84aicpgGC6ZOv0LnBxIrruS4.

PROBLEMS OF ENSURING THE SECURITY OF PERSONAL DATA IN SOFTWARE TESTING

Tofig Kazimov[1], Nazaket Malikova[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]*tofig@mail.ru*, [2]*naranara_68@mail.ru*

Abstract— The article describes the problems that may arise in the software testing process, in particular the difficulties that may arise in ensuring the security of personal data, and the measures that can be done in this regard. The causes of the problems are then investigated, ways to ensure the safety of personal data during the testing process, and the importance of their consideration are highlighted.

Keywords— *software testing; information security; personal data; data-masking*