Proqram təminatının təhlükəsizliyinin təmin olunmasının bəzi üsulları haqqında

Şəfəqət Mahmudova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shafagat_57@mail.ru

***Xülasə*— Bu işdə proqram təminatının təhlükəsizliyi və s. haqqında məlumat verilmişdir. Proqram təminatının təhlükəsizliyinin təmin olunmasının analiz metodları öyrənilmişdir. Proqram təminatının qorunması üçün vacib olan problemlər müəyyənləşdirilmişdir. Proqram layihələri üçün risklər, onların idarəolunması, təyin olunması, kateqoriyaları və s. araşdırılmışdır.**

Açar sözlər—proqram təminatı, təhlükəsizlik, analiz metodları, risklər

I. GİRİŞ

Müasir dövrdə informasiya cəmiyyəti inkişaf edərək getdikcə daha böyük vüsət alır. Kompüterlər cəmiyyətdəki bütün proseslərə, o cümlədən elmi–tədqiqat işlərinə, iqtisadiyyata təsir göstərərək, ümumilikdə insanın fəaliyyət formasını dəyişdirir və yeni sahələrin yaranmasına səbəb olur. İnsanların yeni texnologiyaları öyrənməsi və onu müxtəlif sahələrə tətbiq etməsi yeni sistemlərin və proqram təminatının (PT) yaranmasına və inkişafına səbəb olur.

Müasir dövrdə terrorizm və cinayətkarlara qarşı mübarizə kəskin surətdə artmışdır. Bütün dünyanı bürümüş terror aktlarının dalğası aşkarlayıcı və önləyici təhlükəsizlik sistemlərinin və proqram təminatının təkmilləşdirilməsi ehtiyacını yaratmışdır.

Əksər dövlətlərdə qarşıda duran əsas məsələlərdən biri qaçaqmalçılıq, terror aktlarının qarşısının alınması və müxtəlif sistemlərin yaradılması üçün yeni yanaşmaların, yeni prinsiplərin təşkilinə imkan vermək və milli təhlükəsizlik, beynəlxalq səviyyədə inteqrasiyalar və s. üzrə PT mərkəzlərinin yaradılmasıdır.

Axtarışın, aşkar etmənin və şəxsiyyətə, cəmiyyətə və dövlətə qarşı cinayətlərin təşəbbüskarlarının identifikasiyasi sisteminin təkmilləşdirilməsi, bütovlükdə, xüsusi əhəmiyyət kəsb edir. Belə məsələlərin həlli qlobal miqyasda yeni yanaşmalar və ən müasir texnologiyaların tətbiqini tələb edir. Araşdırma və ya operativ-axtarış fəaliyyəti çərçivəsində alınmış istənilən dəlil real vaxt müddətində effektiv istifadə edilməlidir [1].

Milli zəmində hüquq-mühafizə sistemi, dövlət təhlükəsizliyi sisteminin və ölkənin müdafiə təminatı orqanlarının qarşısında duran məsələlərin geniş spektrini həll etməyə imkan verir:

- Potensial olaraq qeyri-qanuni işlər və təhlükəli əməllərin (vətəndaşların həyatı, dövlət qurumları və s.) həyata keçirilməsində şübhəli bilinənlərin və ya günahkarların axtarışı;
- Hadisələrin iştirakçılarının tapılması və aşkar edilməsi hüquq-mühafizə, dövlət təhlükəsizliyi və ölkənin müdafiəsinin təminatı sistemlərinin əsas məsələlərindən biridir;
- Dövlət səviyyəsində bu məsələlərin uğurla həlli artıq müasir proqram təminatlarından istifadə etməklə mümkündür;
- Multimedia məlumatlarının (şəkillər, videoyazılar və s.) yığımı və saxlanması üçün paylanmış sistemin yaradılması mühüm əhəmiyyət kəsb edir;
- İstintaq fəaliyyəti və operativ-axtarış tədbirləri prosesində yığılmış məlumatlar əsasında yaradılmış bazalarda şübhəli şəxslərin interaktiv axtarışının həyata keçirilməsi vacibdir və s.

Proqram təminatının hazırlanması prosesi (ing. Software development process)—ilk növbədə proqram təminatının hazırlanması üçün razılaşdırılmış strukturun işlənməsidir [2].

Proqram təminatının yaradılması zamanı alqoritmin effektiv işlənilməsi və verilənlərin strukturunun düzgün müəyyən edilməsi əsas rol oynayır. Məsələnin alqoritmi və verilənlərin strukturu effektivliyə təsir edən əsas aspektlərdir. Beləki, sonradan verilənlərin strukturunu dəyişmək alqoritmi dəyişməkdən daha çətindir.

Böyük paylanmış sistemlərin tərtibində əksər hallarda bir neçə proqramlaşdırma dillərindən istifadə olunur ki, bu da müəyyən çətinliklərin əmələ gəlməsinə səbəb olur. Yəni belə hallarda təhlükəsizlik təmin olunmur [3].

Proqram təminatının təhlükəsizliyi dedikdə onun müdafiəsinə yönəldilmiş tədbirlər kompleksi başa düşülür.

Bu baxımdan proqram təminatının təhlükəsliyinin təmin olunması üsullarının araşdırılması xüsusi əhəmiyyət kəsb edir.

Proqram təminatının istismarında da təhlükəsizliyin təmin olunması vacib məsələlərdən biridir.

II. PROQRAM TƏMINATININ QORUNMASININ PROBLEMLƏRİ

Proqram təminatının təhlükəsizliyi dedikdə müxtəlif problemlər (xətalar, səhvlər və s.) meydana çıxmadan onun işləmək xüsusiyyəti başa düşülür. PT-nin qorunması

DOI: 10.25045/NCInfoSec.2018.15

məsələlərini tədqiq edərkən aşağıdakı problemləri diqqətə almaq lazımdır [4]:

- PT-nin icrası zamanı xətaların aşkarlanması;
- Xətaların meydana çıxmasına zəmin yaradan subyektlərin araşdırılması;
- Mövcud proqram xətalarının sayının müəyyən edilməsi;
- Proqram xətalarının proqram səhvlərindən fərqləndirilməsi;
- PT-nin istismarı zamanı dağıdıcı proqram vasitələrinin aktivləşməsi nəticəsində ehtimal edilən nəticələrin müəyyənləşdirilməsi və s.

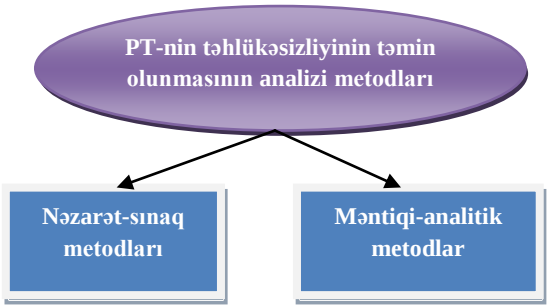
İnformasiyanın təhlükəsizliyinə təhdidlər PT-nin istismarı prosesində yaranır. Hal-hazırda kompüter sistemlərində informasiyaya zərərli təsirlərdən biri ən təhlükəli vasitələr sayılan viruslar olur. PT-lər inkişaf etdikcə virusların da növü artır. Son illər ərzində kompüter virusları həm avadanlıqlara, həm də proqram təminatına çox böyük ziyan vurmuşdur.Belə ziyanların ölçüsü milyon dollarladır. 21 noyabr 1988-ci ildə ən təhlükəli olan Morris virusu 24 saat ərzində ARPANET şəbəkəsini sıradan çıxarmışdır. Şəbəkənin işlək vəziyyətə salınması üçün milyon dollarla pul xərclənmişdir.

PT-nin texnologi təhlükəsizliyi modelinin yaradılması infosferada təhlükəsizliyin ümumiləşdirilmiş konsepsiyasına əsaslana bilər [5]. Bunun üçün aşağıdakı məsələlərə diqqət yetirmək lazımdır:

- PT-nin texnologi təhlükəsizliyi probleminin praktik həlli üçün onun nəzəri əsaslarının işlənilməsi;
- təhlükəsiz informasiya texnologiyalarının yaradılması;
- kompüter infosferisının təhlükəsizliyinin təmin edilməsi üçün nəzarət sisteminin genişləndirilməsi.

III. PROQRAM TƏMINATININ TƏHLÜKƏSLİYİNİN TƏMİN OLUNMASININ ANALİZİ METODLARI

PT-nin təhlükəsizliyinin təmin olunmasında müxtəlif analiz metodlarından istifadə olunur. Bu metodlar müxtəlif funksiyaları yerinə yetirilər. Analiz metodlarının bəziləri şəkil 1-də göstərilmişdir[6].



Şəkil 1. PT-nin təhlükəsizliyinin təmin olunması metodları

Nəzarət-sınaq metodları vasitəsilə proqramın icra prosesinə nəzarət edilir. Bu metodlar geniş yayılmışdır, çünki onlar formal analiz tələb etmirlər, cari texniki və proqram vasitələrindən istifadə etməyə icazə verirlər, qısa müddət ərzində hazır metodikaların yaradılmasına imkan yaradırlar [7].

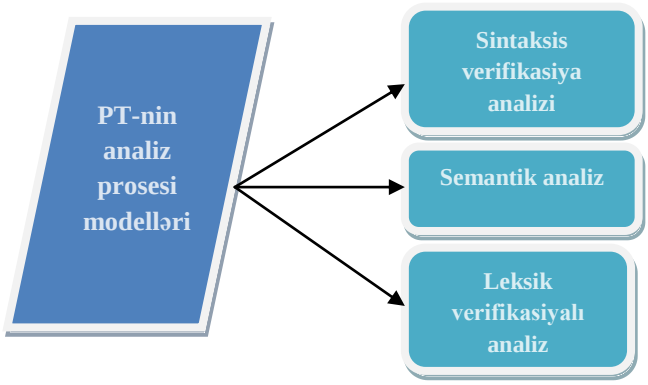
Məntiqi-analitik metodların köməyi ilə təhlükəsizliyin analizi vaxtı proqramın modeli qurulur və tədqiq edilən proqramın modelinin və qrupda olan PT-nin modelinin ekvivalentliyi rəsmi sübut edilir [8]. Proqramın modeli kimi ən sadə halda onun maşın kodu (bitlərlə) ola bilər və proqramda virusların olmasını onların hücum siqnaturlarını tapmaqla sübut etmək olar. Hücum siqnaturu — kompüter virusunun xüsusiyyətləridir [8]. Daha çox formal modellərdən istifadə edir.

PT-nin analiz prosesinə aid modellər [10] şəkil 2-də göstərilmişdir.

Leksik verifikasiyalı analiz modeli axtarış, tanıma və icra edilən kodlarda təqdim edilmiş proqramın obyektlərinin müxtəlif leksemlərinin təsnifatını tədqiq edir. Leksem— translyator üçün məna daşıyan proqramlaşdırma dilinin mümkün simvollarının ardıcıllığıdır [11]. Bu halda leksemlər siqnaturlardır.

Hazırda siqnaturların axtarışı aşağıdakı qruplarda həyata keçirilir:

1. virusların siqnaturları;
2. proqram təminatı sistemlərinin elementlərinin siqnaturları;
3. "şübhəli funksiyaların" siqnaturları.



Şəkil 2. PT-nin analiz prosesi modelləri

Sintaksis verifikasiya analizi modeli axtarış, tanıma və PT-nin sintaksis strukturlarının təsnifatı hesab edir, proqramın özünün strukturuna uyğun alqoritmin qurulmasıdır.

Semantik analiz - kompüterin əməliyyat sistemində PT-nin funksiyalarının (prosedurlarının) mənasını öyrənməklə onun tədqiqini həyata keçirir. Statik tədqiqata əsaslanan analizin əvvəlki növlərindən fərqli olaraq semantik analiz proqramın dinamikasının öyrənilməsinə yönəlmişdir. Semantik analiz modeli analizin ən effektiv növüdür, bu həm də çox zəhmət tələb edir.

PT-nin təhlükəsizliyinin təmin olunması prinsipləri aşağıda qeyd olunmuşdur:

- etalon proqram vasitələrinin girişinə məhdudiyyətlərin qoyulması, onlarda dəyişikliklərin edilməsinə icazənin verilməməsi;
- xətalı proqramın tam skan edilməsi və profilaktik məqsədlə testin yerinə yetirilməsi;
- PT-nin istismara verildiyi andan ona nəzarət edilməsi və təhlükəsizliyi baxımından identifikasiyasının həyata keçirilməsi;
- PT-nin istismarı zamanı strukturu dəyişmədən onun ayrı-ayrı modullarının əvəz edilməsinin təmin edilməsi;
- müşayiət edilən bütün proqram vasitələrinin ciddi uçotunun və kataloqlaşdırılmasının həyata keçirilməsi;
- bütün proseslər, işçi əməliyyatlar, PT-nin funksionallığı haqqında olan informasiyanın statistik analizinin aparılması;
- PT-nin qorunması məqsədilə informasiya təhlükəsizliyinin yeni, gözlənilməz təhlükələrinin üzə çıxardılması halında.əlavə vasitələrin tətbiq edilməsi;
- və s.

Proqram təminatının təhlükəsizliyinin təmin olunması üçün xətaların aşkar edilməsinin və qüsurların aradan qaldırmasının avtomatlaşdırılmış metodu haqqında məlumat [12]-də verilmişdir. İşdə PT-də qüsurların aşkar edilməsi və bərpası ilə bağlı metodlar təhlil edilmişdir.

IV PROQRAM LAYİHƏLƏRİ ÜÇÜN MÜMKÜN RİSKLƏR

Onlayn rejimdə işləyən proqramların təhlükəsizliyinin təmin olunması vacib məsələlərdən biridir. Proqram təminatının təhlükəsizliyinin təmin olunmasında risklər əsas rol oynayır [13]. Layihə üçün risklər layihənin icrası üçün lazım olan işlərin qrafikinə və ya resurslarına təsir edirlər.

Proqram layihələri üçün mümkün risklərin bəziləri və onların idarəolunması və kateqoriyaları aşağıda qeyd edilmişdir [14, 15]:

- İşlənən proqram məhsulları üçün risklər;
- Təşkilatda istehsalçıya aid olan bisnes risklər.

Risklərin idarə olunması.

- Risklərin təyini. Layihə, hazırlanan məhsul və biznes üçün mümkün risklər təyin edilir;
- Risklərin analizi. Təhlükəli vəziyyətlərin yaranması ehtimalı risklərinin ardıcıllığı qiymətləndirilir;
- Risklərin planlaşdırılması. Risklərin qarşısının alınması və ya layihəyə onların təsirinin minimallaşdırması üzrə tədbirlər planlaşdırılır;
- Risklərin monitorinqi. Risklərin ehtimallarının daima qiymətləndirməsi və təhlükəli vəziyyətlərin təzahürünün nəticələrinin azalması üzrə tədbirlərin icra edilməsi.

Risklərin mümkün kateqoriyalarının siyahısı aşağıda göstərilmişdir:

- Texnologi risklər. Sistemin işlədiyi proqram və aparat texnologiyalarında axtarılırlar;
- Personalla bağlı risklər. İstehsalçılar komandasının üzvləriylə bağlıdır;
- Təşkilati risklər. Layihənin yerinə yetirildiyi təşkilatın mühitində baş verir;
- İnstrumental risklər. CASE-vasitələrdən istifadə etməsi və PT-nin təşkili prosesini dəstəkləməsilə əlaqədardır;
- Sistemin tələblərilə bağlı risklər. İşlənən sistemə qoyulan tələblərlə bağlı risklər ola bilər;
- Qiymətləndirmənin riskləri. Layihənin reallaşdırması üçün lazım olan proqram sisteminin və resursların xarakteristikalarının qiymətləndirilməsiylə bağlıdır.

Risklərin analizi.

- Risklərin qarşısının alınmasının strategiyaları. Bu strategiyalara əsasən risklərin təzahürünün ehtimalını aşağı salan tədbirləri həyata keçirtmək lazımdır. Nümunə olaraq, potensial qüsurlu komponentlərin xaric edilməsi strategiyasını göstərmək olar;
- Strategiyanın minimallaşdırılması. Risklərlə bağlı mümkün zərərin azaldılmasına yönəldilmişdir. Misal olaraq, istehsalçıların komanda üzvlərinin xəstəliyi ilə əlaqədar zərərin azaldılması strategiyasını göstərmək olar;
- "Qəzalı" vəziyyətlərin planlaşdırılması. Bu strategiyalara əsasən tədbirlər planına malik olmaq lazımdır. Belə ki, təhlükəli vəziyyətin təzahürü halında onu yerinə yetirmək lazımdır.

NƏTİCƏ

İşdə proqram təminatının qorunmasının problemləri araşdırılmışdır. Proqram təminatınnn təhlükəsliyinin təmin olunmasının analizi metodları öyrənilmişdir. Proqram layihələri üçün mümkün risklərin bəziləri, onların idarəolunması və kateqoriyaları qeyd edilmişdir.

Tövsiyyə olunur ki, PT-nin təhlükəsizliyinin təmin edilməsi üçün kriptoqrafiyanın imkanlarından istifadə olunsun. Bu PT-nin etibarlılığının yüksəlməsinə səbəb ola bilər. İnformasiyanın məxfiliyinin pozulması PT-nin təhlükəsizliyinin pozulmasına imkan yaradır. Buna görə məxfi məlumatların emalı prosesində informasiyanın qəbulu və siqnalların işlənməsi tədqiqatların dərinləşməsinə səbəb olur və bu da bu tipli məsələlrin aktuallığını bir daha sübut edir.

ƏDƏBİYYAT

[1] Для защиты информации предлагается применять технологии распознавания лиц, İnformation Security journal,29.10.2008. http://www.itsec.ru/newstext.php?news_id=51127#sthash.HQGrMBJh.dpuf.

[2] В. В. Бахтизин, Л. А. Глухова, «Технология разработки программного обеспечения», Минск: БГУИР, 2010, 267 с.

[3] Ю.Ю. Громов, О.Г. Иванова М.П., Беляев, Ю.В. Минин, «Технология программирования», ФГБОУ ВПО «ТГТУ». 2013, 172 с.

[4] Кадан А.М. «Методология и технология программирования», http://mf.grsu.by/Kafedry/kaf001/academic_process/048/28

[5] А.И. Ефимов, Б.П. Пальчун, «О технологической безопасности компьютерной инфосферы», Вопросы защиты информации, 1995, №3(30), с. 86-88.

[6] В. Казарин, «Безопасность программного обеспечения компьютерных систем», Москва: МГУЛ, 2003, 212 с.

[7] Методы анализа безопасности программного обеспечения, https://studbooks.net/2043842/informatika/metody_analiza_bezopasnosti_programmnogo_obespecheniya

[8] С. А. Середа, Программно-аппаратные системы защиты программного обеспечения. ЭР, http://www.ase.md/~osa/publ/ru/pubru427.html.
[9] Сигнатура, https://ru.wikipedia.org/wiki/ Сигнатура
[10] В. В. Ященко, «Введение в криптографию», М.:МЦНМО: «ЧеРо», 2003, 272 с.
[11] Лексема, https://ru.wikipedia.org/wiki/ Лексема
[12] J. Jeesoo, K. Taeeun, K. Hwankuk, “An Automated Vulnerability Detection and Remediation Method for Software Security”, International journal of wireless information networks, 2018, vol. 10, issue 5, pp. 117-129.
[13] M. Mihailescu, S. Nita, M. Pirloaga, “Software security techniques: risks and challenges” Mircea cel Batran Naval Academy Scientific Bulletin, 2016, vol. 19, issue 1, 8 p.
[14] V. Georg, “Winning With Open Process Innovation. MIT”, Sloan management review, 2018, vol. 59, pp. 53-56.
[15] Л. Тимоти, Основные риски проекта по разработке программного обеспечения, https://econ.wikireading.ru/78462

ABOUT SOME METHODS FOR ENSURING SOFTWARE SECURITY

Shafagat Mahmudova
Institute of Information Technology of ANAS, Baku, Azerbaijan
shafagat_57@mail.ru

Abstract -- This paper provides information about software security. Methods of analysis of software security have been studied. The problems that are important to protect software have been identified. Risks for software projects, their management, assignment, categories and so on. studied.
Keywords -- software, security, analysis methods, risks