Elektron elm infrastrukturunun təhlükəsizliyi problemlərinin analizi

Təhmasib Fətəliyev, Nərgiz Verdiyeva

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

depart3@iit.ab.az

***Xülasə*— Müvafiq e-elm infrastrukturu müasir elmi-tədqiqat fəaliyyətinin zəruri tərkib hissəsidir. İnfrastrukturun layihələndirilməsi və reallaşdırılmasında informasiya təhlükəsizliyi problemlərinin təhlili mühüm məsələdir. Məqalədə e-elmin təhlükəsizlik problemləri, onun qrid infrastrukturunun təhlükəsizliyinin konseptual məsələləri araşdırılmış və Globus Toolkit təhlükəsizlik vasitələrinin problemlərin həllində rolu müəyyənləşdirmişdir.**

Açar sözlər— e-elm; açıq elm; informasiya təhlükəsizliyi; proqram təminatı; Globus Toolkit

I.GİRİŞ

Azərbaycan Milli Elmlər Akamediyasında e-elm sahəsində aparılan tədqiqatlar və alınmış praktiki nəticələr mühüm əhəmiyyət kəsb edir və perspektiv elmi istiqamət kimi inkişaf etdirilir [1]. E-elmin əsas tərkib hissələrini şəbəkə, hesablama, yaddaş və informasiya resursları təşkil edir. Bu konteksdə qrid e-elm üçün əsas infrastruktur hesab edilir, e-elm məsələlərinin reallaşdırılmasında ilk və əsas yolu bu texnologiyalar açmışdır. E-elmin qrid infrastrukturu üçün mühüm tələblərdən biri informasiya təhlükəsizliyi və fərdi məlumatların mühafizəsidir.

Təqdim edilən işdə e-elmin formalaşması və inkişafında informasiya təhlükəsizliyi problemləri araşdırılmış və bu sahədə təhlükəsizlik üzrə qabaqcıl proqram vasitələrinin tətbiqinin problemlərin həllində rolu müəyyənləşdirmişdir.

II. E-ELMİN İNFORMASİYA TƏHLÜKƏSİZLİYİ PROBLEMLƏRİ

İnformasiya texnologiyalarının müasir səviyyəsi informasiyanın istehsalı, emalı, saxlanılması, paylanması və verilənlərə çıxış imkanlarını son dərəcədə inkişaf etdirmiş və insan fəaliyyətinin bütün sahələrini, xüsusən də elmi-tədqiqatları dəyişmişdir. İnformasiyanın əlyetənliyi, böyük həcmli verilənlərin emalı, əməkdaşlıq və hesablama vasitələri üzrə naliyyətlər nəzəriyyə və praktika ilə yanaşı elm üçün üçüncü bir əsas alətə çevrilmiş və onun həyata keçiriməsinin yeni yollarını yaratmışdır. E-elmin formalaşması və reallaşması burada mühüm rol oynayır. Onun inkişafı nəticəsində elmi fəaliyyətdə açıqlıq və şəffaflıq prinsiplərini ifadə edən “Açıq elm” konsepsiyası da getdikcə reallaşır.

Elm sahələrində açıqlıq prinsiplərinin həyata keçirilməsi tarixən qəbul olunmuş məsələdir və bəzi tədqiqat sahələri, xüsusən həyat elmləri, kimya və astronomiya bu sahədə daha ön plandadırlar. Onu da qeyd edək ki, “Açıq elm”-in inkişafı mühüm bir problem kimi beynəlxalq səviyyədə dəstəklənir. Buna misal olaraq Avropa Komissiyasının “Avropa bulud təşəbbüsü”-nü göstərmək olar. Təşəbbüs çərçivəsində formalaşdırılan “Avropa açıq elm buludu” layihəsi Avropanın 1,7 milyon tədqiqatçısını və 70 milyon elm və texnologiya mütəxəssisini böyük həcmli verilənlərin saxlanılması, birgə və təkrar istifadəsi üçün virtual bir mühitlə təmin edəcəkdir.

Qeyd etmək lazımdır ki, e-elmin və onunla da yanaşı açıq elmin formalaşdırılması proseslərinin sosial-mədəni, texnoloji, siyasi, təşkilati, iqtisadi, hüquqi, məxfilik, mühafizə və təhlükəsizlik kimi müxtəlif aspektlərdə həll edilməli problemləri qarşıda durur. Bunlardan informasiya təhlükəsizliyi problemlərini nəzərdən keçirək. Burada təhlükəsizlik təhdidlərinin obyektlərinə kompüter və kompüter avadanlıqlarını, hesablama və yaddaş resurslarını, şəbəkələri, rəqəmsal sensorları, qabaqcıl elmi avadanlıq və alətləri, elmi verilənləri və verilənlər bazalarını, vizualizasiya və analiz vasitələrini, proqram təminatını, təhlükəsizlik və mühafizə sistemlərini və s. aid etmək olar.

E-elmin mühafizəsi özünün geniş sərhədləri ilə xarakterizə olunur. Belə ki, onun təhlükəsizliyinə həm daxili, həm də xarici təhdidlər ola bilər. Digər tərəfdən e-elmin formalaşması və inkişafı ilə onun təhlükəsizliyinə yeni təhdidlər və təhlükələr yaranır. Bu da ilk növbədə yeni texnologiyaların tətbiqi ilə baglıdır. İnformasiya təhlükəsizliyinə sistemli yanaşma onun obyektlərinin, subyektlərinin, prinsiplərinin, vasitələrinin, təhdidlərin və onların mənbələrinin müəyyən edilməsini tələb edir [3]. Ona görə də qeyd olunanlar e-elmin təhlükəsizliyinin təmin olunmasında kompleks yanaşmalar tələb edir. Onun həlli üçün tədbirlər təhlükəsizlik təhdidlərinin aşağıdakı obyektləri üzrə aparılmalıdır:

A. Sistem və aparat təminatı:

- *Şəbəkələr:* Verilənlərin əlyetənliyi və ya ötürülməsində istifadə olunan infrastruktur;
- *Serverlər:* Digər obyektlərə giriş, onların saxlanması, yaradılması və/və ya manipulyasiyası üçün istifadə olunan sistem;
- *Kompüter və avadanlıqları;*
- *Hesablama və yaddaş resursları;*
- *Mobil cihazlar;*

DOI: 10.25045/NCInfoSec.2017.13

- *İstifadəçi portalı:* Verilənlərin yaradılmasına və emalına imkan verən system.

B. Proqram təminatı:

- *Xarici proqram təminatı:* Sistem və instrumental proqramlar, xarici tətbiqlər, alqoritmlər, modellər;
- *Daxili proqram təminatı:* Daxildə yaradılmış tətbiqlər, alqoritmlər və ya modellər.

C. Verilənlər

Verilənlərə ənənəvi olaraq alqoritm, protokol, konfiqurasiya, mühasibat, fərdi və idarəetmə verilənləri ilə yanaşı emal olunmamış (“çiy”) verilənlər də aid edilir:

- *İctimai verilənlər:* nəşr edilmiş və toplanmış açıq elmi verilənlər;
- *Emal olunmamış verilənlər:* nəşr edilməmiş elmi verilənlər;
- *Daxili verilənlər:* nəşri nəzərdə tutulmayan verilənlər;
- *Sənədlər;*
- *Uçot informasiyası:* jurnallar və verilənlər bazaları;
- *İcazəli giriş üçün:* Açıq elmin fəaliyyəti üçün lazım olan layihə / fərdi məlumatlar.

D. İnformasiya resursları;

E. Avadanlıq və cihazlar:

- *Sensorlar*;
- *Şəbəkəyə qoşulmuş elmi cihazlar və idarəetmə sistemləri* (məs., mikroskoplar, teleskoplar, işıq mənbələri, zərrəcik sürətləndiriciləri).

F. Xidməti obyektlər

Təhdid obyektlərinin fiziki saxlanması, qidalanma və iqlim nəzarəti üçün istifadə olunan yerlər; onlara çıxış üçün heyət tərəfindən istifadə olunan müəssisə sistemləri, məsələn, işçi yerlər, noutbuklar, smartfonlar və onların istifadə etdiyi infrastrukturlar.

III. E-Elmin Qrid İnfrastrukturunun Təhlükəsizliyinin Konseptual Məsələləri

E-elmin qrid infrastrukturu uzaq hesablama və informasiya resurslarının aşkar olunması və onlara giriş üçün miqyaslama, təhlükəsiz və sürətli fəaliyyət göstərən mexanizmləri ilə xarakterizə olunur. Qrid texnologiyası vahid virtual təşkilat (VT) çərçivəsində müxtəlif inzibati domenlərin paylanmış informasiya və hesablama resurslarının birləşdirilməsi üçün nəzərdə tutulan aralıq səviyyəli (*middleware*) proqram təminatından istifadəni təklif edir [4]. Bu sahədə *gLite* proqram təminatı əsas təhlükəsizlik standartı sayılır. Həmin xidmət virtual təşkilatlara dinamik şəkildə yeni üzvlər və altqruplar əlavə etməyə imkan verir. Uyğun *gLite* proqram komponenti X.509 standartlı vasitəçi sertifikatlara əsaslanır və bu sertifikatların və iyerarxik verilənlər bazalarının genişləndirilmiş mexanizmindən istifadə edir. Aydındır ki, bu cür mürəkkəb sistemlərin işlənib hazırlanması zamanı ən vacib məsələlərdən biri də təhlükəsizliyin təmin edilməsidir.

VT təşkilatlar üçün real təşkilatların lokal siyasətlərini tamamlayan müxtəlif təhlükəsizlik siyasətləri işlənib hazırlanmışdır. Qrid-sistemlərlərın fəaliyyəti zamanı qarşılıqlı təhlükəsizliyin təmin edilməsi üçün VT-lərin təhlükəsizlik siyasətlərinin üst-üstə düşməsi və ya biri-birinə yaxın olması vacib məsələdir. Müdaxilələrin aşkarlanması sistemləri və resursların idarə edilməsi vasitələrindən istifadə edərkən təhlükəsizliyin təmin olunmasının bir sıra məsələləri lokal olaraq, ayrı-ayrı qrid resursları səviyyəsində həll edilir. Xüsusilə də, bu məsələlərə autentifikasiya və avtorizasiyanın təmin olunması, sertifikatların mübadiləsi, verilənlərin məxfiliyi və tamlığının təmin olunması, həmçinin resursların və istifadəçilərin auditi və monitorinqi aiddir. Onların əksəriyyəti *Globus Toolkit*-in alətlər dəstinə daxil olan *Globus Security Infrastructure - GSI* əsasında həll olunur [5]. *GSI*-infrastrukturu vahid girişi (single sign on), səlahiyyətlərin həvalə olunmasını və sertifikatların mübadiləsini dəstəkləyir.

Qrid resurslarına giriş *Globus Toolkit-in* alətlər dəstinə daxil olan idarəetmə sistemi *(Grid Resource Allocation Management - GRAM)* ilə nəzarət olunur. Verilənlərin ötürülməsi *GridFTP* protokolu vasitəsilə təmin olunur ki, bununla da standartlaşdırma, qarşılıqlı uyğunluq və informasiya təhlükəsizliyi, həmçinin qridin fəaliyyətinin idarə olunmasında və monitorinqində koordinasiya əldə edilir. Qridin informasiya təhlükəsizliyi vasitələrinin çevikliyinə *gLite*-ın xidmət-yönümlü arxitekturası və ilkin mətnlərinin açıqlığı kömək edir.

Qridlər üçün informasiya təhlükəsizliyi tələblərini baza (əlyetənlik, tamlıq, konfidensiallıq) və inkişaf etdirilmiş (vahid giriş, səlahiyyətlərin həvalə edilməsi, inam münasibətlərinin dinamik qurulması və s.) kimi qruplaşdırmaq olar. Bu tələblər lokal mühafizə, subyektlərin identifikatorlarının translyasiyası, kommunikasiya təhlükəsizliyi, təhlükəsizlik funksiyaları və təhlükəsizlik tətbiqləri kimi beş səviyyəni birləşdirən modeldən istifadə etməklə yerinə yetirmək olar.

Lokal mühafizə səviyyəsində idarəçilik sahəsində mövcud olan təhlükəsizlik mexanizmləri tətbiq olunur və onlar müxtəlif idarəçilik sahələri üşün fərqli ola bilər. Bu mexanizmlər təkcə lokal deyil, həmçinin uzaq məsafəli subyektlər üçün də fəaliyyət göstərir.

Növbəti səviyyə bir idarəçilik sahəsinin (məsələn, uzaq məsafəli) subyektlərinin identifikatorlarının digər sahə (lokal) identifikatorlarına translyasiyası üçün funksiyaları təqdim edir. Bundan sonra isə uzaq məsafəli subyektlərə lokal siyasətlər və təhlükəsizlik mexanizmləri tətbiq oluna bilər.

Kommunikasiya təhlükəsizliyi *TCP/IP* protokolunun nəqliyyat səviyyəsində təmin edilir. Həyata keçirilməsi üçün yeni veb təhlükəsizlik standartı olan *WS-Security* istifadə olunur.

Aşağıda izah olunan inkişaf etdirilmiş təhlükəsizlik tələblərinin yerinə yetirilməsi üçün isə *WS-Policy, WS-Trust, WS-Federation* və s. kimi veb-təhlükəsizlik standartlarından istifadə olunur. Təhlükəsizlik tətbiqləri səviyyəsində bundan

əvvəlki səviyyənin funksiyaları təhlükəsizlik xidmətləri şəklində əlyetən edilir və həm lokal, həm də uzaq məsafəli idarəçilik sahələrindən istifadə oluna bilər.

Beləliklə, mobillik, adaptivlik, həmçinin məhsuldarlığın saxlanılması şərti ilə təhlükəsizliyin və nasazlığa dayanıqlığın qorunub saxlanılması qrid sistemlərin uğurlu layihələndirilməsinin mühüm məsələləridir. Təsvir edilmiş çoxsəviyyəli təhlükəsizlik arxitekturası qridlər üçün informasiya təhlükəsizliyi vasitələrinin qarşılıqlı uyğunluğu və inteqrasiyasını təmin edərək sistemlərin mürəkkəbliyini azaltmağa kömək edir.

IV. E-Elmin İnformasiya Təhlükəsizliyinin Proqram Təminatı

Globus layihəsi çərçivəsində e-elmin əsasını təşkil edən qrid layihələrinin həyata keçirilməsi üçün hazırlanmış təhlükəsizlik proqram vasitələrini nəzərdən keçirək [6].

“Globus Alliance” biznes, elm, mühəndislik və digər fəaliyyət sahələri üçün paylanmış əməkdaşlığa imkan verən hesablama arxitekturası olan qridi formalaşdıran texnologiyaları, standartları və sistemləri inkişaf etdirmək üçün tədqiqatlar aparır və layihələndirmə işləri həyata keçirir.

Arqonna Milli Laboratoriyası, Cənubi Kaliforniyanın İnformasiya Elmləri İnstitutu, Çikaqo Universiteti, Edinburq Universiteti, İsveçin Paralel Kompüterlər Mərkəzi və Superkompüter əlavələri Milli Mərkəzinin bazasında yaradılmış *Globus Alliance* elm və mühəndislik fəaliyyətinin mərkəzində duran və qrid məhsullarının əsasını təşkil edən açıq kodlu proqram təminatı istehsal edir. Onun *Globus Toolkit* alətlər dəstinə resursların monitorinqi, aşkarlanması və idarə olunması, həmçinin təhlükəsizlik və faylların idarə edilməsi üçün proqram xidmətləri və kitabxanalar daxildir. Bunlar *Globus Toolkit* proqram vasitələri toplusunu təşkil edir və tam funksional qrid sistemi yaratmağa imkan verir. *Globus Toolkit* vasitələri qridin zəruri hissələrini həyata keçirən proqram komponentləridir:

- *GRAM* – proseslərin yaradılması və silinməsinə cavab verir.
- *MDS (Monitoring and Discovery Service)* – sistem haqqında informasiyanın təqdim edilməsi yollarını təmin edir. Bu informasiya sistemin konfiqurasiyası və vəziyyəti, həm də onun ayrı-ayrı resursları (resursun tipi, disklərdəki boş yerlər, prosessorların sayı, yaddaşın həcmi, məhsuldarlıq və s.) haqqında ola bilər.
- *GSI* – verilənlərin şifrələnməsini, həmçinin autentifikasiya və avtorizasiya da daxil olmaqla təhlükəsizliyini təmin edir.
- *GASS (Global Access to Secondary Storage)* – paylanmış mühitdə böyük həcmdə verilənlərin saxlanılması və onlara çıxışı təmin edir.
- *Globus kitabxanaları* – tətbiqi proqramlar, həmçinin *GlobusToolkit* komponentləri tərəfindən qovşaqların şəbəkədə heterogen mühitdə qarşılıqlı əlaqəsi üçün istifadə olunur.

Qrid hesablamaları paylanmış “virtual təşkilatlarda” müxtəlif resursların mübadiləsi və razılaşdırılmış istifadəsi ilə əlaqəlidir. Bu mühitlərin dinamik və çoxmüəssisəli xarakteri yeni texnoloji yanaşmalar tələb edən mürəkkəb təhlükəsizlik məsələlərini qarşıya qoyur.

Qrid mühitində təhlükəzliyin təmin olunması üçün tətbiqi proqramlar və xidmətlərin autentifikasiya, avtorizasiya, identifikasiya verilənlərinin emalı, auditi və səlahiyyətlərin həvalə edilməsi *(delegation)* kimi müxtəlif təhlükəsizlik funksiyalarının dəstəklənməsi tələb olunur. Qrid tətbiqi proqramları bir sıra təhlükəsizlik mexanizmləri və tələbləri olan digər tətbiqi proqramlar və xidmətlərlə qarşılıqlı fəaliyyət göstərməlidir. Bu mexanizmlər və tələblər yeni mexanizmlərin işlənməsi və ya siyasət dəyişikliyi nəzərə alınmaqla inkişaf etdirilə bilər.

Yuxarıda qeyd olunduğu kimi qridin təhlükəsizliyi problemləri üçün ilk inteqrasiya edilmiş həllərdən biri *Globus Toolkit*-dir. *Globus Toolkit* istifadəçi və ya xidmətlərin identifikasiyasını təyin edən, əlaqələri qoruyan, kimin hansı əməliyyatları aparmağa icazəsi olduğunu müəyyən edən, eləcə də istifadəçilərin identifikasiya verilənlərini idarə edən çoxsaylı təhlükəsizlik komponentlərini özündə birləşdirir.

GSI C: Globus Toolkit-in Grid Təhlükəsizlik İnfrastrukturu *GSI* qrid hesablamaların bir sıra təhlükəsizlik problemlərini həll edir. Bu komponent autentifikasiya, avtorizasiya və sertifikatların idarə edilməsi üçün *API* və alətlər təqdim edir. Autentifikasiya üçün *API Public Key* (aşıq açarlar) *Infrastructure (PKI)* texnologiyası, məsələn, X.509 sertifikatları və *Transport Layer Security - TLS*-dən istifadə edilməklə qurulmuşdur. Autentifikasiya ilə yanaşı, o, X.509 proksi sertifikatlarına əsaslanan səlahiyyətlərin həvalə edilməsi mexanizmini təqdim edir. Avtorizasiya dəstəyini iki *API* formalaşdırır. Birincisi, kliyentin identifikasiya verilənlərinə (yəni, X509 sertifikat zənciri) əsaslanan giriş nəzarətini həyata keçirən ümumi avtorizasiya *API*-sidir. İkincisi isə, avtorizə edilmiş uzaq hüquqi şəxsləri lokal (sistem) istifadəçi adları ilə təsvir edən sadə giriş nəzarət siyahısını təmin edir. Yuxarıdakılarla yanaşı, sertifikatların idarə edilməsi və sorğuların aşkarlanması üçün daha aşağı səviyyəli müxtəlif *API*-lər və alətlər də vardır.

MyProxy: Standart veb texnologiyalarına əsaslanan qrid portalları qridlərin interfeyslərini təqdim etmək üçün geniş istifadə olunur. Bununla belə, belə qrid portalları *GSI* kimi mövcud qrid təhlükəsizliyi sistemləri ilə inteqrasiya olunmur, bunun da əsas səbəbi veb təhlükəsizlik mexanizmində səlahiyyətlərin həvalə edilməsi imkanlarının olmamasıdır. *MyProxy* imkan verir ki, qrid portalları *GSI*-dən istifadə etməklə qrid resursları ilə standart, təhlükəsiz üsulla qarşılıqlı əlaqə yaratsın. *MyProxy* komponenti *X.509 Public Key Infrastructure*-un təhlükəsizlik identifikasiya verilənlərini (sertifikatlar və məxfi açarlar) idarə etmək üçün nəzərdə tutulmuş açıq kodlu proqram təminatıdır. *MyProxy* onlayn identifikasiya verilənləri bazasını onlayn sertifikat mərkəzi ilə birləşdirərək istifadəçilərə istənilən vaxtda və harada olmasından asılı olmayaraq təhlükəsiz identifikasiya verilənlərini əldə etmək imkanı yaradır.

GSI-OpenSSH: Secure Shell (SSH) tətbiqi səviyyəli şəbəkə protokolunun modifikasiya olunmuş bu versiyası X.509 proksi sertifikatının autentifikasiya və səlahiyyətlərin həvalə edilməsinə dəstəyi əlavə etməklə uzaqdan girişin və faylların ötürülməsinin vahid xidmətini təmin edir. O, həmçinin uzaqda yerləşən sistemlərə daxil olmaq və parol daxil etmədən, əvəzində autentifikasiya üçün proksinin uçot verilənlərindən istifadə etməklə sistemlər arasında faylları ötürmək imkanı yaradır. *GSI-OpenSSH* sistemə giriş zamanı proksi-serverin identifikasiya verilənlərini uzaq sistemə ötürür, beləliklə, proksi-serverin identifikasiya verilənlərini tələb edən əmrlər (*GSI-OpenSSH* əmrləri də daxil olmaqla) uzaq sistemdə istifadə olunur və əllə proksi-serverin yeni identifikasiya verilənlərini yaratmağa ehtiyac yaranmır.

NƏTİCƏ

E-elm infrastrukturunun formalaşması, istismarı və inkişafında informasiya təhlükəsizliyi problemlərinin həlli mühüm rol oynayır. Bu sahədə aparılmış araşdırmalar göstərir ki, təhlükəsizliyin təmin olunması kompleks yanaşmalar tələb edir. Konseptual məsələlərin reallaşdırılmasında acıq kodlu təhlükəsizlik proqram vasitələrindən istifadə etməklə elmin daha səmərəli inkişafına nail olmaq olar.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir – **Qrant № EİF-2014-9(24)-KETPL-14/02/1**

ƏDƏBİYYAT

[1] T.X. Fətəliyev, Elektron elmin təhlükəsizliyinin təmin edilməsi məsələləri haqqında, İnformasiya Cəmiyyəti Problemləri, №1, 2016, s. 56-62

[2] European Cloud Initiative, https://ec.europa.eu/digital-single-market/en/european-cloud-initiative

[3] Y.N.İmamverdiyev, E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli, İnformasiya cəmiyyəti problemləri, №1, 2013, s. 20-31

[4] I.Foster, C.Kesselman, S.Tuecke, The Anatomy of the Grid: Enabling Scalable Virtual Organizations, High Performance Computing Applications, v.15, №3, 2001, pp. 200-222

[5] Globus Toolkit, http://toolkit.globus.org/toolkit

[6] Globus Alliance, http://toolkit.globus.org/alliance/about.php

ANALYSIS OF THE SECURITY PROBLEMS OF ESCIENCE INFRASTRUCTURE

Tahmasib Fataliyev[1], Nargiz Verdiyeva[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
depart3@iit.ab.az

Abstract – The relevant e-science infrastructure is a necessary part of modern scientific-research activities. Analysis of information security issues in the design and implementation of infrastructure is an important problem. In the article the security issues of e-science, and the conceptual issues of its security infrastructure are discussed and the role of Globus Toolkit security tools in solving problems is identified.

Keywords – e-science; open science; information security; software; Globus Toolkit