Elektron elmin informasiya təhlükəsizliyi haqqında

Təhmasib Fətəliyev

AMEA İnformasiya Texnologiyaları İnstitutu

depart3@iit.ab.az

Xülasə– Məqalədə Azərbaycan Respublikasında formalaşdırılan e-elmin informasiya təhlükəsizliyi məsələlərinə baxılmışdır. E-elmin effektiv kiber müdafiəsi üçün prioritet istiqamətlər və bu sahədə görülmüş işlər təqdim olunmuşdur.

Açar sözlər– ***informasiya cəmiyyəti; e-elm; AzScienceNet; e-elmin intormasiya təhlükəsizliyi; CERT; hesablama resursları.***

I. GİRİŞ

Müasir dövrdə informasiya – kommunikasiya texnologiya-larının (İKT) tətbiqi nəticəsində cəmiyyətin bütün sahələrində köklü dəyişikliklər baş verir. Bu sahələrdən biri də elmdir. Azərbaycan Milli Elmər Akademiyasında (AMEA) reallaşdırılan "e-elm" layihəsi belə aktual işlərdəndir. Məlumdur ki, e-elmin məqsədi müasir İKT-nin tətbiqi ilə AMEA institut və təşkilatlarının, eləcə də respublikanın digər elmi qurumlarının fəaliyyətinin yenidən qurulması, vahid milli elmi onlayn infrastrukturun və informasiya fəzasının formalaşdırılmasıdır. Nəticədə elmi təşkilat, kollektiv və alimlərin virtual məkanda birgə səmərəli fəaliyyəti təmin edilir. E-elmin əsas vəzifələri elmin kommunikasiya, şəbəkə və hesablama infrastrukturunun formalaşdırılması, elmi fəaliyyətdə və idarəetmədə İKT-nin geniş tətbiqi, informasiya resurslarının yaradılması, normativ-hüquqi bazanın təkmilləşdirilməsi və kadr hazırlığıdır [1].

E-elm ərazicə paylanmış infrastruktura malik olub respublikanın elmi qurumlarını tam əhatə etmək vəzifəsini daşıyır. Məlumdur ki, respublikanın əksər elmi qurumlarını təşkil edən AMEA-nın, ali təhsil müəssisələrinin və digər elmi qurumların institut və təşkilatları Bakı şəhərində, AMEA-nın Naxçıvan və Gəncə Bölmələri, Şəki və Lənkəran Regional Elmi Mərkəzləri isə respublikanın coğrafi paylanmış ərazilərində yerləşirlər. Respublikada Azərbaycan Respublikası (AR) Rabitə və Yüksək Texnologiyalar Nazirliyinin (RYTN) dəstəyi ilə "Elektron Azərbaycan"-nın tərkib hissəsi kimi həyata keçirilən e-elm belə bir mürəkkəb infrastruktura malikdir və AzScienceNet şəbəkəsi əsasında formalaşır.

Beləliklə, ölkədə formalaşan e-elmin vahid bir mürəkkəb sistem kimi qorunması həm iqtisadi, həm də təhlükəsizlik baxımından çox vacibdir və son zamanların ən mürəkkəb texnoloji və sosial problemlərindən biridir [2].

Qlobal Internet şəbəkəsi ilə inteqrasiya və bu sistemə hücum təhlükəsi ilə bərabər istifadəçilərin artan tələbatı qeyd olunan problemlərin həllində informasiya təhlükəsizliyi sahəsində yeni biliklərin, profesional bacarığın və insan resurslarının əhəmiyyətini artırmış və aktual etmişdir.

II. E-ELMİN KOMPONENTLƏRİ

Qeyd olunduğu kimi e-elm mürəkkəb bir sistem olub infrastruktur, verilənlərin toplanması, saxlanması, emalı, axtarışı, analizi, ötürülməsi, təqdim olunması və s. kimi tərkib hissələrə malikdir. Göründüyü kimi bu blokların hər biri mürəkkəb, informasiya təhlükəsizliyi də daxil olmaqla kompleks məsələlərin həlli ilə formalaşır.

E-elmi vahid bir sistem kimi təsəvvür etsək, onda onun həll etdiyi məsələlərə görə aşağıdakı altsistemlərdən təşkil olunduğunu görmək olar:

- Elmin informasiya təminatı;
- Elmmetrik (elmmetriya, bibliometriya, vebometriya) təhlillər;
- İntellektual analiz;
- Qərarların qəbulu;
- Elektron xidmətlər;
- Fərdi məlumatların qorunması;
- Beynəlxalq qurumlarla əlaqə;
- E-elmin informasiya təhlükəsizliyi;
- Vətəndaş elmi;
- Big Data;
- Şəbəkə infrastrukturunun yaradılması və s.

Yuxarıda qeyd olunduğu kimi e-elmin əsas vəzifələrindən biri kommunikasiya-şəbəkə və hesablama infrastrukturunun formalaşdırılmasıdır. Bu istiqamətdə aparılmış işlərin nəticəsi kimi e-elmin şəbəkə platforması olan *AzScienceNet* şəbəkəsi əsasında böyük hesablama və yaddaş resurslarına malik olan Verilənlərin Emalı Mərkəzi yaradılmışdır:

- E-elmin şəbəkə platforması olan AzScienceNet AMEA-nın bütün elmi müəssisələrini əhatə edir [3]. Qeyd etmək lazımdır ki, e-elmin tam formalaşdırılması üçün onun respublikanın digər elmi qurumlarını əhatə etməsi vacibdir. Bü istiqamətdə aparılacaq işlərin intensivləşməsi üçün qarşıda mühüm vəzifələr durur.
- Böyük yaddaş və hesablama resurslarına malik (yaddaş-200 Terabayt, hesablama məhsuldarlığı - 14 Tflops) Data Mərkəzin texniki xarakteristikaları daim inkişaf etdirilir.
- Fəaliyyətdə olan bu şəbəkə və hesablama e-infrastrukturu elmi qurumlar arasında sürətli əlaqə

yaradır, istifadəçilərə çoxsaylı xidmətlər (hosting, AzCloud, AzStorage, e-poçt, e-kitabxana, distant təhsil, AzScienceCERT, eduroam və s.) təqdim edir və eyni zamanda beynəlxalq sistemlərlə inteqrasiya imkanları yaradır.

- AMEA, RYTN və Təhsil Nazirliyinin birgə təşəbbüsü ilə AzScienceNet şəbəkəsi ölkəni təmsil edən milli operator kimi GEANT Assosiasiyasında qeydiyyatdan keçmişdir. AzScienceNet milli operator kimi Assosiasiyanın təqdim etdiyi layihələri və xidmətləri ölkəmizin elm və təhsil ictimaiyyətinə çatdırılmasında əməkdaşlıq edir.

E-elm çərçivəsində bu istiqamətlərdə görülmüş işlərin cari vəziyyəti onun informasiya təhlükəsizliyinin elmi-nəzəri və praktiki problemlərinin tədqiqi və həllinin nə dərəcədə vacib və aktual olduğunu bir daha təsdiq edir.

III. E-ELMİN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN PRİORİTET İSTİQAMƏTLƏRİ

E-elmin effektiv kiber müdafiəsi üçün aşağıdakı kompleks məsələlərin həlli nəzərə alınmalıdır:

1. E-elmin layihələndirilməsinin təhlükəsizlik məsələləri:
   - Şəbəkə və hesablama infrastrukturunun təhlükəsizlik tələblərinə uyğun layihələndirilməsi;
   - Mobil qurğular, kompüterlər, işçi stansiyalar və serverlərin avadanlıq və proqram vasitələri üçün təhlükəsiz konfiqurasiyaların seçilməsi;
   - Şəbəkə qurğuları (şəbəkələrarası ekranlar, marşrutlaşdırıcılar, kommutatorlar və s.) üçün təhlükəsiz konfiqurasiyaların seçilməsi;
   - Təhlükəsizlik proqram vasitələrinin tətbiqi;
   - Səlahiyyətli və icazəsiz qurğuların və proqram vasitələrinin inventarlaşdırılması;
   - Şəbəkə portları, protokolları və xidmətlərinə məhdudiyyət və nəzarətin təşkili;
   - Müdafiə sərhədinin seçilməsi.

2. E-elmin təhlükəsizliyinə nəzarət və mühafizəsi məsələləri:
   - Səlahiyyətə müvafiq girişə nəzarət;
   - Naqilsiz girişə nəzarət;
   - İnzibati imtiyazlardan istifadəyə nəzarət;
   - Zərərli proqramlardan mühafizə;
   - Verilənlərin mühafizəsi;
   - Verilənlərin bərpa edilməsi imkanlarının nəzərə alınması.

3. E-elmin təhlükəsizliyinin idarə olunması məsələləri:
   - Texniki xidmət, monitorinq, auditin təşkili və onlara müvafiq jurnalların təhlili;
   - Monitorinq və nəzarətin hesabatının hazırlanması;
   - İnsidentlərə cavab verilməsi və insidentlərin idarəolunması;
   - Təhdidlərin fasiləsiz qiymətləndirilməsi və aradan qaldırılması;
   - Testlərin və qaynar təlim komandalarının tətbiqi;
   - İnformasiya təhlükəsizliyinin qiymətləndirilməsi bacarığı və çatızmamazlıqların öyrədilməsi üçün təlimlərin keçirilməsi.

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİ SAHƏSİNDƏ GÖRÜLMÜŞ İŞLƏR

İKT-nin sürətli inkişafı, geniş yayılması və rəqabətin kəskinləşməsi elmi-metodoloji prinsiplərə əsaslanan informasiya təhlükəsizliyinin təmin edilməsini, həmçinin şəbəkə texnologiyalarının müasir inkişaf meyllərinin nəzərdə tutulduğu hüquqi, təşkilati, texniki və fiziki mühafizə tədbirlərini qarşılıqlı surətdə əlaqələndirməklə AzScienceNet şəbəkəsində vahid informasiya təhlükəsizliyi sisteminin yaradılmasını zəruri edir. İnformasiya təhlükəsizliyinin təmin edilməsi dedikdə informasiyanın konfidensiallığının, tamlığının və əlyetərliyinin təmin edilməsi başa düşülür. İnformasiyanın konfidensiallığı informasiyaya çıxış yalnız icazə verilmiş şəxslərə verildiyi, tamlığı verilənlərə razılaşdırılmış dəyişikliklər edildikdə, əlyetərliyi isə icazə verilmiş şəxslərin lazımi vaxtda informasiya resurslarına çıxış əldə etdikləri halda təmin edilir.

İnformasiya təhlükəsizliyi sisteminin yaradılması zamanı həlli vacib olan məsələlər aşağıdakılardır:

- informasiya təhlükəsizliyinə potensial təhdidlərin siyahısının müəyyənləşdirilməsi və analizi;
- informasiya resurslarının təsnifatı;
- tətbiq edilən yeni informasiya texnologiyalarına qoyulan informasiya təhlükəsizliyinin vahid tələblərinin müəyyənləşdirilməsi;
- İnformasiya təhlükəsizliyi sisteminə dair tələblərin formalaşdırılması.

Bu məqsədlə *AzScienceNet* şəbəkəsinin vahid informasiya təhlükəsizliyi siyasəti işlənmişdir. Siyasətin məqsədi təhdidlərin AMEA-nın şəbəkə və informasiya resurslarına vura biləcəyi maddi və mənəvi ziyanın minimuma endirilməsi; AMEA-nın işgüzar nüfuzunun yüksəldilməsi; informasiya təhlükəsizliyi sisteminin qurulması üçün vahid prinsiplərin formalaşdırılması; informasiya təhlükəsizliyi sisteminin yaradılması, fəaliyyəti və inkişafı üçün müvafiq təşkilati-metodiki bazanın formalaşdırılmasıdır.

AzScienceNet-in imkanlarından səmərəli istifadə etmək məqsədi ilə istifadəçi kompüterlərinin reyestri sistemi yaradılmışdır. *AzScienceNet* şəbəkəsi və ona qoşulmuş bütün kompüterlər haqqında məlumatlar reyestrin vahid verilənlər

bazasında toplanılır. Bu sistem aşağıdakı məsələlərin həllinə köməklik göstərir:

- İstifadəçilərin şəbəkəyə icazəsiz qoşulmasının qarşısının alınması;
- Monitorinq sisteminin nəticələrinin analizinin daha dəqiq aparılması;
- Təhdidlərə qarşı mübarizənin aparılması;
- Şəbəkə daxilində yaranan təhlükələrin vura biləcəyi ziyanın minimuma endirilməsi;
- İstifadəçilərin qadağan olunmuş saytlara müraciətlərinin qarşısının alınması;
- Şəbəkə trafikinin lazımsız məlumatlarla yüklənməsinin qarşısının alınması;
- Şəbəkənin profilinə uyğun olmayan veb resurslara müraciətlərin qarşısının alınması.

AzScienceNet-in səmərəli idarə olunması və təhlükəsizliyinin təmin edilməsi məqsədi ilə şəbəkə təhlükəsizliyinin monitorinqi (ŞTM) sistemi yaradılmış və fəaliyyət göstərir. ŞTM - əsas funksiyaları şəbəkə haqqında informasiyanın toplanması, analizi və nəticələri haqqında məlumatları əlaqədar şəxslər və ya sistemlərə yönləndirən, müasir tələbləri ödəyən, proqram və aparat komplekslərindən ibarət olan mürəkkəb bir sistemdir [4]. Monitorinq sistemi bir çox funksiyaların yerinə yerirlməsini təmin edir ki, bu da şəbəkənin səmərəliliyinin artırılmasına kömək edir. ŞTM-in əsas vəzifələrini aşağıdakı kimi izah etmək olar:

- İnternet-trafikin müşahidəsi və qeydiyyatı;
- İnternetlə bağlı real vaxt rejimində işləyən sistemlərin təhlükəsizliynə nəzarət;
- İnternet istifadəçilərinin təhlükəsizliyi, konfidensiallığı və mühafizəsi;
- Sistemlərdə boşluqların aşkarlanması;
- Fəaliyyətin fasiləsizliyi;
- Riskin qiymətləndirilməsi.

İnformasiya təhlükəsizliyi risklərinin idarə edilməsini təmin etmək məqsədi ilə *AzScienceCERT (CERT–Computer Emergency Response/Readiness Team)* xidməti yaradılmışdır [5]. Xidmətin əsas məqsədi informasiya təhlükəsizliyi risklərinin qəbul edilmiş səviyyədə idarə edilməsini təmin etməkdir [6]. Bu məqsədlə *AzScienceCERT* informasiya təhlükəsizliyinin pozulmasına yönəlmiş hərəkətlərin aşkarlanmasında, qarşısının alınmasında və istifadəçilərin məlumatlandırılmasında istifadəçilərə kömək edir. *AzScienceCERT* xidməti e-elmin şəbəkə platforması olan *AzScienceNet*-də zərərli proqramların yayılması və şəbəkə hücumları ilə əlaqədar statistik verilənlərin toplanmasını, saxlanılmasını və analizini həyata keçirir. Qarşıya qoyulmuş vəzifələrin yerinə yetirilməsi üçün *AzScienceCERT* ölkədə fəaliyyət göstərən digər oxşar qruplarla, AR dövlət hakimiyyəti orqanları, informasiya təhlükəsizliyi insidentlərinin emalı ilə məşğul olan xarici ölkə qrupları və informasiya təhlükəsizliyi sahəsində fəaliyyət göstərən digər təşkilatlarla qarşılıqlı əlaqə saxlayır. Məlumdur ki, İKT sahəsində qabaqcıl ölkələrdə *CERT* mərkəzləri, onları birləşdirən milli və beynəlxalq şəbəkələr fəaliyyət göstərir, təcrübə mübadiləsi aparılır və biliklər bazaları formalaşdırılır. Kiberhücumların, təhdidlərin, informasiya müharibəsi təzahürlərinin artmasının real təhlükəyə çevrilməsini nəzərə alaraq ölkənin adekvat əks-tədbirlər sisteminin, həyata keçilirməsi üçün onun beynəlxalq təşkilatlarda təmsil olunması vacib məsələyə çevrilmişdir. Ona görə *AzScienceCERT* komandası 31 may 2011-ci ildə *TERENA (Trans-Evropean Research and Education Networking Assosiation)* təşkilatının himayəsində olan *TI - Trustel Introducer* sistemində qeydiyyatdan və akkreditasiyadan keçmişdir. Onun əsas vəzifəsi Avropa ölkələrinin *CERT* mərkəzləri arasında inam infrastrukturunun yaradılmasıdır. Tİ xidməti *CERT*-lərin qeydiyyatı, akkreditasiyası və sertifikatlaşdırılması məsələləri ilə məşğul olur. *TI* akkreditasiya edilmiş *CERT*-lər üçün bir sıra xidmətlər göstərir: xüsusi informasiya materiallarına və xəbərdarlıq sisteminə giriş, xüsusi verilənlər bazasından istifadə və insident obyektlərinin bu bazada qeydiyyatı, yalnız üzvlər üçün nəzərdə tutulmuş tədbirlərdə iştirak, insidentlərin emalı zamanı məlumat mübadiləsi üçün şifrələmə və elektron imza infrastrukturu və s. Beləliklə də qlobal informasiya infrastrukturu mühitində informasiya təhlükəsizliyi insidentlərinin qarşısının alınması və cavablandırılması üçün beynəlxalq əməkdaşlıq xüsusi əhəmiyyət daşıyır. Bu cəhətdən *TI* və oxşar beynəlxalq infrastrukturlara inteqrasiya *AzScienceCERT* komandasına dünyanın müxtəlif ölkələrindən olan həmkarları ilə səmərəli əməkdaşlıq üçün geniş imkanlar açır.

NƏTİCƏ

Azərbaycan Respublikasında formalaşan e-elmin informasiya təhlükəsizliyinin təmin olunması çoxistiqamətli, mürəkkəb və aktual məsələdir. E-elmin araşdırılmış tərkib hissələri və təqdim olunmuş təhlükəsizlik mexanizmləri bunu bir daha təsdiq edir. AzScienceNet şəbəkəsi timsalında bu sahədə görülmüş işlər mühüm əhəmiyyət kəsb edir və e-elmin həll etdiyi məsələlər çərçivəsində daha geniş miqyasda, daim inkişaf etdirilməlidir.

ƏDƏBİYYAT

[1] R.M.Əliquliyev, T.X.Fətəliyev, “Elektron elm: məqsədləri, vəzifələri və inkişaf perspektivləri,” Elektron elm problemləri üzrə I Respublika elmi-praktiki konfransı, 15-16 noyabr, 2012, s.11-12.

[2] T.X.Fətəliyev, Y.N.İmamverdiyev, “E-elm mühitində informasiya təhlükəsizliyi problemləri,” İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı, 17-18 may, 2013, s.113-115.

[3] AzScienceNet. www.azsciencenet.az

[4] R.M.Əliquliyev, Y.N.Imamverdiyev, B.R.Nəbiyev, “Şəbəkə təhlükəsizliyinin monitorinqi metodlarının analizi,” İnformasiya texnologiyaları problemləri, №1, s.60-68, 2014.

[5] AZScienceCERT. www.sciencecert.az

[6] R.M.Əliquliyev, Y.N.Imamverdiyev, ‘İnformasiya təhlükəsizliyi insidentləri.” Bakı : İnformasiya Texnologiyaları, 2012, 219 s.