Dövlət sirrinin təhlükəsizliyi sahəsində ictimai problemlərin analizi və həlli yolları

Davud Rüstəmov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı şəhəri, Azərbaycan Respublikası
davudrustamov@yahoo.com

***Xülasə*— Məqalədə dövlət sirrinin təhlükəsizliyi ilə bağlı ictimai problemlər analiz olunur. Bəzi texnogen xarakterli həllər və milli təhlükəsizlik sisteminə ictimai dəstəyin verilməsinə dair bəzi təkliflər irəli sürülür.**

Açar sözlər - dövlət sirri, açıq mənbə kəşfiyyatı, milli təhlükəsizlik sistemi, insayder

I. GİRİŞ

Dövləti, cəmiyyəti və şəxsiyyəti potensial təhdidlərdən qorumaq üçün milli təhlükəsizlik sistemi formalaşdırılır. Milli Təhlükəsizlik Sistemi (MTS) aşağıdakı kimi bölünür [1]:

1) milli maraqların müəyyən olunması;
2) milli maraqlara olan real və potensial təhdidlərin müəyyən olunması;
3) təhdidlərə qarşı Milli Təhlükəsizlik Siyasətinin hazırlanması.

Kissincerin fikrincə "Milli Təhlükəsizlik Siyasəti cəmiyyətin bütün fəaliyyətini əhatə etdiyinə görə, cəmiyyət də öz üzərinə düşən vəzifələri həyata keçirməlidir". Deməli, MTS-in səmərəli fəaliyyəti ölkə vətəndaşlarının ictimai fəallığından da asılıdır. İctimai mühitdə dövlət sirri anlayışı kəşfiyyat və ya əks-kəşfiyyat xarakterli məlumatlar kimi başa düşülür. "Dövlət sirri haqqında" Azərbaycan Respublikasının qanunvericilik aktlarının açıq olmasına baxmayaraq, onlara baxış statistikası çox azdır. Aparılan müşahidələr göstərir ki, heç bir TV, radio, qəzet, elektron KİV-lər, tədris vəsaiti, məktəbdən kənar tədris materialları və s. mənbələrdə dövlət sirrinin təhlükəsizliyi barədə heç bir məlumat (qanunların şərhi, maarifləndirici vəsaitlər, dövlə sirrinin yayılmasında ictimai qınaq və s.) yoxdur.

İnternetin inkişafı açıq mənbə kəşfiyyatının (eng. OSINT – **O**pen **S**ource **INT**elligence) fəaliyyətini genişləndirir. Kəşfiyyat məlumatların 80%-ni açıq mənbələrdən – turistlərin söhbətləri, təşkilatların bəyanatları, statistikalar, sosial media, forumlar, internet tv, radio, qəzet, jurnal və s. mənbələrdən toplanır [2]. Dövlət sirri kəşfiyyat üçün əlyetənli olmadığından, açıq mənbələrdən mümkün məlumatlar OSINT yolu ilə toplanır və müxtəlif məqsədlərlə emal olunur. Nəticədə dövlət sirrinə çıxış yolları müəyyən olunur.

Mobil şəbəkənin əhatə dairəsinə görə Azərbaycan 2014-cü ildə dünya reytinqində birinci yerdə göstərilib [3]. Deməli, ölkə əhalisinin hər bir nəfəri potensial internet istifadəçisidir və eyni zamanda onlar dövlət sirrini açıqlayan məlumatların internet üzərindən yayılmasında potensial təhlükə hesab oluna bilər.

Məqalənin əsas məqsədi dövlət sirrinin təhlükəsizliyində ictimai problemlərin aktuallığını göstərmək, mövcud problemləri təhlil etmək və məsələnin həlli istiqamətində müvafiq təkliflər hazırlamaqdır.

II. DÖVLƏT SİRRİNİN TƏHLÜKƏSİZLİYİNDƏ SOSİAL-İCTİMAİ PROBLEMLƏRİN ANALİZİ

İnternet texnologiyalarının inkişafı fonunda dövlət sirrinin təhlükəsizliyi xeyli çətinləşir. Belə ki, ölkədə təhlükəsizlik tədbirlərinin aparılması, milli təhlükəsizlik və müdafiə xarakterli xüsusi əhəmiyyətli obyektlərin dislokasiyası, silahlı birləşmələrin yerləşməsi, hərbi hissələr və şəxsi heyətin sayı və s. məlumatların internet mühitində yayılmasına qarşı nəzarət mexanizmlərinin işlənməsi aktuallıq kəsb edir [4]. Yəni, dövlət sirrinin təhlükəsizliyində ictimai problemlərin olduğu aydın şəkildə görünür. Bu baxımdan, aşağıdakı bəzi problemlər təhlil olunmuşdur:

A) Ünsiyyət zamanı dövlət sirrinin yayılması problemləri

Qeyri-rəsmi olaraq sirr daşıyan insanlarla, ailə üzvləri və ya yaxınları ilə "məqsədli" söhbətlərin aparılması dövlət sirrinin qeyri-qanuni yollarla ələ keçirilməsi məqsədi daşıyır [2]:

- biznesin qurulması haqqında xəyali danışıqlar aparmaq;
- yanlış müsabiqələrin təşkili və ;
- aparıcı mütəxəssislərin işə dəvət olunması;
- təchizat məlumatlarının alınması;
- istehlakçılar, fondlar və xeyriyyə təşkilatları vasitəsilə əhali arasında dövlətçilik əleyhinə söhbətlərin aparılması və s.

Virtual ünsiyyət zamanı iri həcmli məlumatların sürətli, şifrəli və gizlin kanallarla ötürülməsi dövlət sirrinin yayılmasına şərait yaradır. Bir qrup insanlar – hərbçilər (sirr daşıdığına görə), KİV nümayəndələri (informasiya yayımı ilə məşğul olduğuna görə), cəbhəboyu zonalarda məskunlaşmış vətəndaşlar (yaşayış yerinə görə), digər vətəndaşlar (hərbi texnikanın operativ yerdəyişməsini müşahidə etdən) dövlət sirrini açıqlayan məlumatların yayılmasında potensial risk faktorudur. Onlar virtual ünsiyyət zamanı aşağıdakı qaydaları nəzərə almalıdırlar:

- Dövlət sirrini açıqlaya bilən məlumatların (strateji ərazinin fotoşəkili, video mateial, geolokasiya verilənləri və s.) paylaşılması yolverilməzdir;

- Saytlarda qeydiyyat zamanı fərdi məlumatların istifadəsi yolverilməzdir;
- Hərbi xidmət barədə məlumatların müzakirəsi yolverilməzdir;
- Elektron poçt yazışmaları təhlükəsizlik şəraitində aparılmalıdır və s.

B) Smartfon tipli mobil telefonlardan istifadə zamanı yaranan problemlər

2014-cü il üzrə Azərbaycanda hər 100 nəfərə 108 mobil telefon istifadəçisi var [5]. Belə olduğu halda, xüsusi ilə smartfon tipli mobil telefonlar dövlət sirrinin qeyri-qanuni yayılmasında risk faktoru hesab oluna bilər. Smartfonlar kəşfiyyat xidmətləri üçün mobil informasiya paylayıcısı hesab olunur [6]. Əksər proqramlar smartfonlara yükləndiyi zaman fərdi məlumatlara giriş hüququ tələb edir. Bu zaman telefonun yaddaşındakı məlumatlar risk altına düşür. Müxtəlif yollarla (reklamlar, yükləmələr, yenilənmələr və s.) smartfonlara yeridilmiş casus proqramlar telefonun işinə nəzarət edir – mikrofon, kamera, GPS və s. qurğularını aktiv və ya deaktiv edir, SMS-lərin, zənglərin qeydiyyatını aparır və bədniyyətlini məlumatlandırır. Bu səbəbdən də sirr daşıyan insanlar üçün smartfonların istifadəsi riskli hesab olunur.

C) Dövlət sirri saxlanılan yaddaş qurğuları ilə bağlı problemlər

Bütün kompüter istifadəçiləri daşınan yaddaş qurğularından (fləş yaddaş kartları, SD yaddaş kartları, xarici sərt disk yaddaş qurğuları və s.) istifadə edirlər. Bu qurğular vasitəsilə dövlət sirrini açıqlaya bilən informasiya bilərəkdən və ya bilməyərəkdən yayıla bilər. Bilərəkdən yayılma halları insayder təhlükəsinin görünən tərəfidir. Bilməyərəkdən yayılma isə bu qurğuların texniki xüsusiyyətinin nəzərə alınmaması ilə bağlıdır. Belə ki, yaddaş qurğularından informasiyanın adi qaydalarla tam silinməsi mümkünsüzdür. Dövlət sirri saxlanılan yaddaş qurğularının şəxsi ehtiyaclar üçün istifadəsi zamanı və eləcə də başqa əllərə düşdüyü zaman informasiyanın potensial yayılma riski artır. Beynəlxalq təcrübədə dövlət sirri saxlanılan yaddaş qurğuları xüsusi qaydalarla və beynəlxalq standartlarla tənzimlənir. Belə olduqda yaddaş qurğularının təkrar istifadəsi nəzarət altında olur. İnformasiyanın yaddaş qurğusundan bərpa edilməz formada silinməsini təmin edən çoxlu elmi işlər var [7], [8] və s.

Ölkədə müvafiq standartların hazırlanması və ya beynəlxalq standartların ratifikasiyası, eləcə də dövlət sirri saxlanılan informasiya sistemlərində belə qaydaların tətbiqi vacibdir.

D) Sosial şəbəkələrdən istifadə zamanı yaranan problemlər

Dünyada milyonlarla sosial şəbəkə veb saytları mövcuddur. Bunlar virtual icmalar, forumlar, fondlar, tanışlıq və s. xarakterli olurlar. Sosial şəbəkədə qeydiyyata alınan istifadəçilərə aid fərdi məlumatlar, fəaliyyət, əlaqələr, maraqlar və s. toplanır. Belə saytlar biznes fəaliyyəti ilə məşğul olduğundan əldə olunan məlumatları 3-cü tərəfə verməkdə maraqlıdır. Eyni zamanda müxtəlif kəşfiyyat xidmətləri bu mühitdə yayılan məlumatlardan faydalanırlar. Bu səbəbdən, dövlət sirrini açıqlayan hər hansı məlumatların sosial şəbəkə mühitində yerləşdirilməsi və dövlət sirri daşıyan şəxslərin bu mühitdə qeydiyyatı yolverilməzdir.

E) Elektron poçtdan istifadə zamanı yaranan problemlər

E-poçtdan istifadə zamanı məlumatlar xidmət göstərənin serverində saxlanılır. Yəni, bütün məlumatlar e-poçt xidmətinin sahibi üçün əlyetəndir. Əksər e-poçt xidmətindən istifadə zamanı məktubu göndərənin ünvanı asanlıqla müəyyən olunur.

İnformasiya resurslarına istənilən zaman əlçatanlığın təmin olunması üçün istifadəçilərə "bulud" xidmətləri təklif olunur. Lakin belə xidmətlər də məlumatların toplanması və 3-cü tərəfə verilməsində maraqlıdır.

Deməli, dövlət sirri ilə işləyən şəxslər yalnız xüsusi ayrılmış milli e-poçt xidmətindən istifadə etməli və dövlət sirrini açıqlayan hər hansı məlumatın "bulud" xidmətində saxlanılması yolverilməzdir.

III. PROBLEMİN HƏLLİ YOLLARI

İnternet texnologiyalarının inkişaf etdiyi dövrdə insan faktoru dövlət sirrinin qeyri-qanuni yayılmasında ən çətin nəzarət olunan informasiyanın sızma kanalıdır. Tədqiqat zamanı rast gəlinən problemləri nəzərə alaraq aşağıdakı təkliflər irəli sürülür:

1. Dövlət sirrinin təhlükəsizliyi ilə bağlı müxtəlif metodlarla ictimaiyyətin maarifləndirilməsi həyata keçirilməlidir. Bununla bağlı aşağıdakılar tövsiyə olunur:
   - Milli internet resurslarında "dövlət sirrinin təhlükəsizliyinə ictimai dəstək" mövzusuna geniş yer ayrılması;
   - "dövlət sirrinin təhlükəsizliyi təkcə dövlətin deyil, eləcə də hər bir kəsin vətəndaşlıq borcudur" adlı yeni ictimai fikrin formalaşdırılması;
   - KİV-lərdə, radio, tv, qəzet və jurnallarda "dövlət sirri haqqında qanundan şərhlər, izahlar, cəzalar və s." mövzuların müntəzəm müzakirəsi;
   - Ali təhsil müəssisələri üçün "dövlət sirrinin təhlükəsizliyi" mövzusunda tədris vəsaitinin hazırlanması və ölkənin təhsil standartına daxil edilməsi qoyulmuş problemin həllində çox faydalıdır. Buna Rusiya təcrübəsini misal göstərmək olar[9].
   - Dövlət sirrinin qorunmasının faydaları və eyni zamanda yayılması zamanı gözlənilən acı nəticələr barədə animasion vəsaitlərin hazırlanması və KİV-lərdə yayılması;
2. Dövlət sirrinin qeyr-qanuni yayılması hallarına aid məhkəmə işlərindən ibarət məlumat-axtarış sisteminin yaradılması;
   - Məhkəmədə baxılmış işlərin statistik-analizinin aparılması və müəyyən zaman intervalında belə halların başvermə dinamikasının izlənməsi;
   - Baş vermiş insidentlər əsasında dövlət sirrinin təhlükəsizliyi sahəsində qərar qəbuletmə sisteminin hazırlanması;

3. Azərbaycanda cəbhəboyu ərazilərin və eləcə də ölkə ərazisində digər strateji zonaların geolokasiya verilənlərindən ibarət məlumat-axtarış sistemin hazırlanması tövsiyyə olunur:
   - Bu sistem kəşfiyyat-əks kəşfiyyat, əməliyyat-axtarış və istintaq tədbirləri zamanı əldə olunan rəqəmsal fotoşəkil, sxem, koordinatlar və s. məlumatların bu zonalar və ya ona yaxın ərazilərə aid olmasını yoxlamağa imkan verəcək.
   - Ölkə ərazisində baş vermiş hər hansı hadisələrin (terror, ixtişaş, təbii fəlakət və s.) bu sistemdəki koordinatlara yaxınlıq dərəcəsi yoxlanılmaqla strateji zonaların təhlükəsizliyi daha etibarlı təmin oluna bilər;
4. Dövlətin müvafiq icra hakimiyyəti orqanına aid rəsmi internet saytında ictimayyətlə əlaqələrin interaktiv formada qurulması təklif olunur. Bu zaman dövlət sirrinin qorunmasında ictimai fəallıq aşkar hiss olunacaq. Daxil olan müraciətlər əsasında mövcud problemlərin həlli də operativlik sürətlənəcək.

Göstərilən həllərin hər biri qoyulmuş problemlə bağlı mövcud risk faktorlarının sayını azaldır. Eyni zamanda müvafiq dövlət qurumlarının diqqətini və eləcə də ictimai fikri dövlət sirrinin təhlükəsizliyinə yönəldir. Qoyulmuş problemin daim aktuallıq kəsb etməsini nəzərə alaraq, bu sahədə elmi-nəzəri tədqiqatların da aparılması vacib hesab olunur.

IV. NƏTİCƏ

Tədqiqat zamanı internet informasiya ehtiyatlarında dövlət sirrini açıqlayan məlumatların yerləşdirilməsi fakları diqqət çəkmişdir. Açıq informasiya mühitində belə məlumatların yayılmasının qanunla qadağan olunmasına baxmayaraq, bəzi elektron KİV-lər və ayrı-ayrı vətəndaşlar tərəfindən belə hərəkətlərə yol verilməsi yeni nəzarət mexanizmi tələb edir. Texnoloji imkanların artdığı bir dövrdə dövlətin bu sahəyə nəzarət mexanizmi zəif görünür. Qoyulmuş problemin həlli istiqamətində ölkədə ictimai maarifləndirmə və nəzarət mexanizminin aktuallığı önə çəkilir. Aşkarlanmış bəzi ictimai və texnogen xarakterli problemlərin həlli istiqamətində müvafiq həllər təklif olunur. Ermənistanın Azərbaycanla müharibə apardığı və torpaqlarının 20%-dən çoxunu işğal etdiyi bir vəziyyətdə cəbhəboyu və digər strateji ərazilərdə dövlət sirrinin təhlükəsizliyi ilə bağlı texnoloji boşluqların aradan qaldırılması və ictimai dəstəyin formalaşdırılması çox aktualdır.

ƏDƏBIYYAT

[1] N.Nağıyev; “Milli Təhlükəsizlik və onun təmin olunması sistemi”, “Dirçəliş – XXI əsr” – 2008. № 124-125. Səh. 191

[2] В.А. Хорошко, А.А. Чекатков «Методы и средства защиты информации», стр. : 504, изд.: Юниор – 2003 г.

[3] Bilbao-Osorio, B., Dutta, S. & Lanvin, B. (Eds.), Global Information Technology Report 2014. Rewards and Risks of Big Data. Geneva: World Economic Forum and INSEAD. Retrieved April 25, 2014

[4] “Azərbaycan Respublikası Silahlı Qüvvələrinin Ermənistan Respublikası Silahlı Qüvvələri ilə təmas xəttində bəzi təhlükəsizlik tədbirləri haqqında” Azərbaycan Respublikasi Prezidentinin № 742, 24 sentyabr 2014-cü il tarixli Sərəncamı. Azərbaycan Qəzeti 25.09.2014-cü il.

[5] Global Risks 2013; 8-th Edition Insight Report. An Initiative of the Risk Response Network.

[6] Kuehnhausen, M.; Frost, V. S., “Trusting smartphone Apps? To install or not to install, that is the question,” Cognitive Methods in Situation Awareness and Decision Support (Cog SIMA), 2013 IEEE International Multi-Disciplinary Conference, pp. 30-37, 25-28 Feb. 2013

[7] Medsger, J.; Srinivasan, A., «ERASE- entropy-based sanitization of sensitive data for privacy preservation», Internet Technology and Secured Transactions, International Conference, pp.427, 432, 10-12 Dec. 2012;

[8] Hughes, G. F., Coughlin, T.; Commins, D. M., “Disposal of Disk and Tape Data by Secure Sanitization,” Security & Privacy, IEEE, vol.7, no.4, pp.29, 34, July-Aug. 2009.

[9] М. А. Вус, А. В. Федерова; “Государственная тайна и ее защита в Российской Федерации: учебное пособие” 620 с., ноябрь 2007, Издательство: Юридический центр Пресс.