UOT 004.351

Əliquliyev R.M., İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
director@iit.ab.az, yadigar@lan.ab.az

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ: AKTUAL TƏDQİQAT İSTİQAMƏTLƏRİ

E-dövlət quruculuğunda qarşıya çıxan ən vacib və ən çətin məsələlərdən biri e-dövlətin etibarlı informasiya təhlükəsizliyinin təmin edilməsidir. Tədqiqat işində e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə aktual elmi-tədqiqat problemləri müəyyən olunmuş və onların müasir vəziyyəti analiz edilmişdir. E-dövlətin informasiya infrastrukturuna yeni təhdidlər, təhdid aktorlarında baş vermiş keyfiyyət dəyişiklikləri ətraflı analiz edilmiş, ənənəvi təhlükəsizlik modellərinin e-dövlət kimi mürəkkəb obyektə tətbiqində meydana çıxan əsas çətinliklər göstərilmişdir.

***Açar sözlər**: e-dövlət, informasiya təhlükəsizliyi, informasiya müharibəsi, asimmetrik təhdidlər, informasiya təhlükəsizliyi siyasəti, informasiya təhlükəsizliyinin idarə edilməsi, informasiya təhlükəsizliyi mədəniyyəti.*

Giriş

Hazırda informasiya-kommunikasiya texnologiyaları (İKT) cəmiyyətin bütün sahələrinə geniş nüfuz etməkdədir. Bunun nəticəsində bəşəriyyət yeni inkişaf mərhələsinə – informasiya cəmiyyətinin formalaşması dövrünə qədəm qoyur [1].

Cəmiyyətin idarə olunması proseslərini optimallaşdırmaq məqsədi ilə dövlət idarəetmə orqanlarında və təşkilatlarında, yerli özünüidarəetmə orqanlarında İKT-nin geniş tətbiqi və inkişaf etdirilməsi informasiya cəmiyyətinin formalaşmasında mühüm mərhələ olan e-dövlətin qurulmasına şərait yaradır. Təhsil prosesində və elmi fəaliyyətdə elektron kitabxanalar və distant təhsil formaları istifadə edilir. Səhiyyədə İKT-nin inkişafı telesəhiyyəni formalaşdırır. İnternetin inkişafı xüsusi "virtual mədəniyyətin" meydana çıxmasına şərait yaradır. İKT-nin iqtisadi münasibətlərdə geniş istifadəsi nəticəsində "şəbəkə" iqtisadiyyatı formalaşır, "elektron pullar", "elektron ticarət" meydana çıxır. Yeni şəraitdə hüquqi münasibətlərin tənzimlənməsi üçün "informasiya hüququ" formalaşır. İnformasiya cəmiyyətinə keçid üçün əlverişli şəraitin yaradılmasında dövlət aparıcı rol oynayır və bu keçid prosesində dövlətin özü də e-dövlətə çevrilir. Son onillikdə dünyanın bir çox ölkəsində e-dövlətə keçid üzrə bir sıra milli və beynəlxalq proqramlar həyata keçirilməkdədir [2].

Aydındır ki, ölkənin informasiya cəmiyyəti mərhələsinə keçməsi onun informasiya-kommunikasiya sistemlərindən və informasiya texnologiyalarından asılılığını daha da gücləndirir. İnformasiyalaşdırma bəşəriyyətin inkişafını sürətləndirməklə yanaşı, milli, regional və qlobal təhlükəsizliyə yeni təhdidlər də yaradır. Qlobal informasiya cəmiyyətinin mənfi tərəfləri sırasında aşağıdakıları qeyd etmək olar [3]:

1. Dövlətlərarası ziddiyyətlərin və münaqişələrin informasiya fəzasına keçirilməsi təhlükəsi, informasiya qarşıdurmasının yaranması, informasiya silahının tətbiqi, informasiya müharibəsinin aparılması imkanları.

2. Qlobal informasiya-kommunikasiya şəbəkələrində səhvlər və ya qəzalar nəticəsində fəlakətlərin yeni növünün – infogen fəlakətlərin meydana çıxması.

3. Cinayətkar və terrorçu təşkilatların çətin nəzarət edilən qlobal informasiya infrastrukturları yaratması.

4. Kibercinayətkarlığın yeni növlərinin, o cümlədən mütəşəkkil kibercinayətkarlığın inkişafı.

5. Fərdi məlumatların cinayət məqsədləri üçün toplanması.

6. Kütləvi informasiya vasitələrinin inhisara alınması və ictimai şüurla manipulyasiya edilməsi.

Bu təhdidlərlə əlaqədar olaraq e-dövlətin informasiya təhlükəsizliyi ön plana çıxır, milli və beynəlxalq təhlükəsizliyin getdikcə daha vacib komponentinə çevrilir. E-dövlət ideyasının həyata keçirilməsində müəyyən mərhələləri arxada qoymuş ölkələrin təcrübəsi sübut edir ki, e-dövlət quruculuğunda qarşıya çıxan əsas və ən çətin məsələlərdən biri yeni şəraitdə fəaliyyət göstərən dövlətin etibarlı informasiya təhlükəsizliyinin təmin edilməsidir [4-8].

E-dövlətin informasiya təhlükəsizliyini sosiumun elə vəziyyəti kimi müəyyən etmək olar ki, bu zaman şəxsiyyət, cəmiyyət və dövlət təbii və süni meydana çıxan, informasiya və kommunikasiya axınları şəklində çıxış edən, ictimai və fərdi şüurun qəsdən deformasiya olunmasına, şəxsiyyətin, cəmiyyətin və dövlətin varlığı üçün vacib əhəmiyyəti olan infrastrukturun məhv edilməsinə yönəlmiş təhdidlərdən fasiləsiz olaraq etibarlı və hərtərəfli qorunsun [9]. Araşdırmalar göstərir ki, e-dövlətin informasiya təhlükəsizliyinin komponentləri aşağıdakılardır:

- informasiya fəzasının təhlükəsizlik vəziyyəti – bu zaman vətəndaşların, təşkilatların və dövlətin maraqları naminə informasiya fəzasının formalaşması və inkişafı təmin edilir;
- informasiya infrastrukturunun təhlükəsizlik vəziyyəti – bu zaman informasiya yalnız öz təyinatı üzrə istifadə edilir və istifadə edildiyi zaman sistemə (obyektə) mənfi təsir göstərmir;
- informasiyanın özünün təhlükəsizlik vəziyyəti – bu zaman informasiyanın tamlıq, konfidensiallıq və əlyetərlilik kimi xassələrinin pozulması istisna edilir və ya olduqca çətinləşir.

İnformasiya sahəsində dövlətin maraqlarına ən ciddi təhdid mənbəyi "informasiya silahı"nın nəzarətsiz yaradılması, yayılması və bu sahədə "informasiya müharibəsi"nin aparılması cəhdləridir. İnformasiya sistemləri və şəbəkələri ilə əlaqəli hücum və müdafiə əməliyyatları sürətlə inkişaf edir, informasiya əməliyyatları müasir silahlı qüvvələrin hərbi doktrinalarında artıq özünə yer tapmaqdadır [10].

Qlobal informasiya cəmiyyəti şəraitində e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi problemi beynəlxalq, kompleks və sahələrarası xarakter kəsb edir və onun ideal həlli (verilən zəmanətlər baxımından) müvafiq elmi-metodoloji bazanın mükəmməllik səviyyəsindən birbaşa asılı olur.

Təqdim olunan işdə e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə aktual elmi tədqiqat problemləri analiz edilir. E-dövlətin informasiya təhlükəsizliyinin təmin edilməsinin elmi problemlərini humanitar, elmi-texnoloji və kadr təminatı məsələləri kimi üç əsas istiqamətdə qruplaşdırmaq olar [11]. Qeyd etmək lazımdır ki, informasiya təhlükəsizliyinin elmi-texnoloji komponenti nisbətən ətraflı və əsaslı, humanitar komponenti isə olduqca zəif tədqiq edilib. Lakin aparılmış elmi tədqiqatlar

əsasən korporativ şəbəkə miqyasını nəzərdə tutur, qlobal informasiya cəmiyyəti mühitində e-dövlətə heterogen korporativ şəbəkələrin məcmusu kimi baxıldıqda belə mövcud texnoloji həllərin yetərsiz olmasını etiraf etmək lazımdır. Çünki belə mürəkkəb sistemdə yalnız miqyasın böyüməsi və komponentlərin bircins olmaması nəticəsində bir sıra keyfiyyət dəyişiklikləri meydana çıxır:

- komponentlərin sayı artır, nəticədə sistemin mümkün vəziyyətlərinin sayı dəfələrlə artır;
- təhlükəsizlik perimetrinin müəyyən edilməsində çətinliklər meydana çıxır, bəzi hallarda bu perimetri müəyyən etmək mümkün olmur;
- sistemin komponentləri arasında kanalların vəziyyətinə nəzarət etmək mümkün olmur;
- şəbəkənin müxtəlif seqmentlərində resursların istifadəsinə və deməli, mühafizəsinə müxtəlif tələbləri nəzərə almaq lazımdır (məsələn, nüvə seqmenti və periferiya seqmenti).

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsinin çətinliyi, həmçinin mühafizə obyekti kimi informasiya infrastrukturunun yüksək səviyyədə qarşılıqlı əlaqəli olması, təhdidlərin bütün çoxluğunu, hücumların mümkün formalarını, növlərini və hücum nöqtələrini əvvəlcədən bilməyin və müəyyən etməyin mümkün olmaması, obyektlərin hamısının eyni zamanda mühafizəsinə fiziki və maliyyə məhdudiyyətləri, təhdidlərin və hücumların mənbələrinin müəyyən edilməsinin çətinliyi, e-dövlətin informasiya infrastrukturunun dünya informasiya infrastrukturu ilə sıx qarşılıqlı əlaqəsi və transsərhəd informasiya mübadiləsinin mövcudluğu və s. kimi faktorlarla da müəyyən edilir.

Əlbəttə, yuxarıda sadalanan faktorların çoxu informasiya təhlükəsizliyi modellərinin qurulmasına ənənəvi yanaşmaların böyük miqyaslı paylanmış sistemlər üçün tətbiqi zamanı meydana çıxır. Qlobal informasiya cəmiyyətinin formalaşması nəticəsində informasiya təhlükəsizliyi üçün tamamilə yeni modellər işləməyi tələb edən mühüm konsepsiyalar və faktorlar da meydana çıxmışdır. İnformasiya təhlükəsizliyi üzrə elmi-tədqiqat problemlərini analiz etmək üçün bu faktorları nəzərə almaq vacibdir.

Yeni müharibə konsepsiyaları

İlk olaraq informasiya təhlükəsizliyinə təhdidlərin xarakterində baş verən dəyişiklikləri qeyd etmək lazımdır. İnformasiya riskləri və təhdidləri yumşaq xarakter daşıyır, yəni informasiya hücumu zamanı silahlı qüvvələrin bilavasitə toqquşması, düşmən ərazisinə soxulması, insanların həlak olması, infrastrukturun məhv edilməsi baş vermir, informasiya təsirinin obyekti hərbi infrastruktur deyil, daha çox iqtisadi və sənaye infrastrukturları olur. İKT-nin ikili xarakteri mümkün informasiya hücumlarının hədəfləri kimi hərbi və mülki informasiya sistemlərinin bir-birindən fərqləndirilməsini çətinləşdirir.

İnformasiya fəzası transmilli xarakter daşıyır, bu, qlobal informasiya infrastrukturunda milli komponenti ayırmağa imkan vermir, eyni zamanda, informasiya-kommunikasiya sistemləri qloballaşır və milli səviyyədə nəzarətdən çıxır. Eləcə də, informasiya texnologiyalarının, sistemlərinin və proqram təminatının yaradılması tədricən transmilli səviyyəyə qalxır. İKT məhsulları bazarında bir neçə ölkə şirkətlərinin inhisarçı vəziyyətində olması bu və ya digər siyasi məqsədlərin əldə

edilməsi üçün istifadə edilə bilər. Baxılan təhdidlər dövlət sirri və konfidensial sirr təşkil edən digər məlumatlara icazəsiz giriş əldə etmək şəklində də meydana çıxa bilər.

Asimmetrik təhdidlərin aktorları qeyri-konvension yanaşmalardan istifadə edirlər, informasiya təhlükəsizliyinin təmin edilməsinə ənənəvi yanaşmalar belə aktorlara qarşı tamamilə səmərəsiz ola bilər, onlara qarşı tamamilə yeni əks-tədbirlər strategiyası tələb edilir. Ən pisi odur ki, yanaşmaların bir çoxu problemin mahiyyətini tam başa düşmür və buna görə kiberfəzada "Majino xətti"nin elektron ekvivalentini yarada bilərlər. Qeyd edək ki, qeyri-konvension təhlükəsizlik təhdidləri yalnız terrorçu və kriminal qrupların təhdidləri və ya dövlətlərarası rəqabətlə bağlı deyil.

"Elektron Perl Harbor" ssenarisinin – kritik vacib informasiya sistemlərinin, enerji sistemlərinin və ya uçuşu idarəetmə sistemlərinin əvvəlcədən planlaşdırılmış kütləvi ələ keçirilməsi ssenarilərının həyata keçirilməsi təhdidləri meydana çıxır.

Qeyd edək ki, beynəlxalq-siyasi münaqişələr üçün yeni konsepsiyanın "asimmetrik müharibə" konsepsiyasının meydana çıxması da İKT-nin və informasiya-kommunikasiya infrastrukturunun xüsusiyyətləri ilə əlaqədardır. Bu müharibədə düşmənlər keyfiyyətcə müxtəlif silahlara müraciət edirlər: güclü aktor tərəfindən silahın və kəşfiyyat vasitələrinin ənənəvi növlərindən istifadə edilməsinə cavab olaraq zəif aktorlar müasir kommunikasiya və informasiya vasitələrindən, psixoloji terrordan istifadə etməklə qeyri-ənənəvi, lakin təsirdə geri qalmayan üsullara əl atırlar [12].

Həyatı təmin edən əsas sahələrin aşağı səviyyədə informasiyalaşdırılması "zəif" aktoru informasiya silahı qarşısında heç də zəif etmir. Bununla yanaşı, zəif aktor düşmənin informasiya-kommunikasiya sistemlərinə böyük itkilərə səbəb olan ciddi zərbələr vurmaq iqtidarındadır. Nəticədə informasiya üstünlüyü anlayışı mahiyyətcə dəyişir. Müasir asimmetrik münaqişələrdə qələbənin təminatı düşməni düzgün qiymətləndirməyə, özünün isə zəif yerlərini müəyyən etməyə və diqqətlə öyrənməyə imkan verən informasiya mübarizəsidir.

"Şəbəkə" (*network-centric warfare*) və "dövlətsiz" (*stateless*) müharibə konsepsiyalarının meydana çıxması beynəlxalq təhlükəsizlik təhdidlərinin transformasiyası ilə əlaqədardır. Aydındır ki, gələcəkdə əsas təhlükə müxtəlif ölkələrin nizami orduları tərəfindən deyil, hər cür terrorçu, kriminal və digər analoji təşkilatlardan qaynaqlanacaq, onların iştirakçıları müəyyən şəbəkə strukturlarında birləşəcək. Bu transmilli sosial qrupları identifikasiya etmək çətindir, onların daimi ünvanı yoxdur, "onların fəaliyyət meydanı bütün dünyadır". Belə qruplar və təşkilatlar dəqiq iyerarxik tabeçiliyə malik deyillər, çox zaman onların ümumi rəhbərliyi də olmur. Onlar öz fəaliyyətlərini qlobal kommunikasiya vasitələrindən istifadə etməklə əlaqələndirirlər. Belə strukturların fərqləndirici xüsusiyyəti – vahid strateji məqsədin mövcudluğu və taktiki səviyyədə planlaşdırmanın yoxluğudur. Belə strukturları işarə etmək üçün xüsusi termin – "seqmentlərə bölünmüş, polisentrist, ideologiya çulğalamış şəbəkə" (*segmented, polycentric, ideologically integrated network – SPIN*) təklif edilmişdir [9].

İnformasiya təhlükəsizliyinin idarə edilməsi problemləri

İnformasiya təhlükəsizliyi bir praktiki fəaliyyət sahəsi və bir elmi tədqiqat istiqaməti kimi son bir neçə onillikdə formalaşmış, "verilənlərin mühafizəsi", "kompyuter təhlükəsizliyi", "şəbəkə təhlükəsizliyi" və nəhayət, "informasiya təhlükəsizliyi" adlarını daşımışdır. Solms son 40-50 il ərzində informasiya

təhlükəsizliyinin idarə edilməsi sistemlərinə yanaşmaların inkişafını analiz edir və onları "dörd dalğa"ya bölür. Hər dalğa verilmiş zaman kəsiyində informasiya texnologiyalarına və onların idarə edilməsinə ümumi yanaşmanı təsvir edir [13]. İlkin yanaşmalarda hansısa bir texnoloji həll vasitəsi ilə problemləri həll etməyə çalışırdılar, belə həllər çoxaldıqca bu yanaşmanın problemi həll edə bilmədiyi meydana çıxdı. Hazırda əsas yanaşma informasiya təhlükəsizliyinin idarə edilməsi yanaşmasıdır. Bu yanaşmada informasiya təhlükəsizliyi sisteminin əsas komponentləri kimi texniki aspektlər deyil, idarəetmə (menecment) komponentləri götürülür.

İnformasiya təhlükəsizliyinin idarə edilməsi sahəsində ilk nəzəri tədqiqatlara 1970-ci illərin sonlarında başlanmışdır. 1990-cı illərin sonlarında isə ilk milli və beynəlxalq standartlar meydana çıxdı (ISO/IEC 17799). Lakin standartların meydana çıxması o demək deyil ki, informasiya təhlükəsizliyinin idarə edilməsi sahəsində bütün elmi və praktiki problemlər həll edilib. Əksinə, informasiya texnologiyalarının istifadəsinin genişlənməsi ilə əlaqədar informasiya təhlükəsizliyinin idarə edilməsi problemləri getdikcə çətinləşir.

Qeyd etmək lazımdır ki, yaxın vaxtlara qədər informasiya təhlükəsizliyinin idarə edilməsi dedikdə, yalnız (iri) təşkilat səviyyəsi nəzərdə tutulurdu. Son dövrlər isə daha çox milli informasiya infrastrukturunun təhlükəsizliyinin idarə edilməsindən söhbət gedir. Aydındır ki, bu səviyyələrin hər birində informasiya təhlükəsizliyinin idarə edilməsi məsələləri özünün məxsusi metodoloji bazasının inkişafını tələb edir.

Aşağıda e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi istiqamətində əsas elmi-tədqiqat problemləri identifikasiya edilir. Problemlərin identifikasiyası zamanı başlıca meyarlar kimi əsas idarəetmə elementlərinin nəzərə alınması, elmi ədəbiyyatda formalaşmış istiqamətlərə, informasiya təhlükəsizliyinin idarə edilməsi üzrə beynəlxalq standartlar seriyasına [14] mümkün qədər uyğunluq götürülmüşdür.

Heterogen şəbəkələrdə informasiya təhlükəsizliyi siyasətinin modelləşdirilməsi

Paylanmış böyük sistemlərin müxtəlif struktur elementləri, servisləri və tətbiqi proqramları üçün təhlükəsizlik siyasəti modellərinin (qraf, avtomat, statistik, determinik) işlənməsi, TS-ni modelləşdirmə dillərinin yaradılması bu sahədə müəyyən tədqiqatların mövcud olmasına baxmayaraq, aktualdır [15]. TS üçün vacib tələblərdən biri siyasətdə ziddiyyətlərin (konflikt və anomaliyaların) olmamasına zəmanət verilməsi və şəbəkənin mövcud (planlaşdırılan) konfiqurasiyasında realizə edilməsinin mümkünlüyüdür. Buna görə də mürəkkəb sistemlərin TS-nin verifikasiyası üçün müxtəlif təyinatlı metodların və proqram vasitələrinin işlənməsi də aktualdır [16,17].

Autentifikasiyanın və avtorizasiyanın idarə edilməsi

E-dövlət yalnız servislərin göstərilməsini deyil, həmin servislərin təhlükəsiz təqdim edilməsini və biznes və vətəndaşlar üçün təhlükəsiz e-mühitin yaradılmasını da təmin etməlidir. Vətəndaşların e-dövlət servislərindən təhlükəsiz və rahat istifadəsi üçün şəxsiyyəti müəyyən edən elektron identifikatorlar (e-İD) əsas autentifikasiya vasitəsi kimi mühüm rol oynayırlar. İdentifikatorların idarə edilməsi informasiya cəmiyyətində mobillik, əlyetərlilik və interoperabellik üçün əsas problemlərdəndir. Bir sıra ölkələr müxtəlif e-İD sxemləri tətbiq etmişlər. Bu işlərin sərhədlər boyunca yeni rəqəmsal baryerlər əmələ gətirməsinin qarşısını almaq, e-İD həllərin uyuşan olmasını təmin etmək üçün minimum tələblərin və ümumi standartların qəbul edilməsi vacibdir. e-İD texnologiyalarının, o cümlədən e-imza və biometrik texnologiyaların, böyük

miqyaslı e-İD sistemlərinin qurulması problemlərinin, e-İD sistemlərinin kiber-cinayətkarlığa qarşı mübarizədə istifadə edilməsinin tədqiqi aktual tədqiqat istiqamətləridir [18, 19]. Qeyd edək ki, hazırda şəbəkə vasitəsi ilə müxtəlif xidmətlər göstərən informasiya sistemlərinə ən geniş yayılmış təhdid "şəxsiyyətin oğurlanması" (*ID-theft*) hücumlarıdır. ABŞ Federal Ticarət Nazirliyi hər il *ID-theft* üzrə statistik məlumatları dərc etdirir [20]. Məsələn, 2006-cı ildə 364 mindən çox şikayət daxil olmuş, ümumilikdə 1,187 milyard dollar ziyan vurulmuşdur. Bir *ID-theft* zamanı orta hesabla 3 257 dollar ziyan vurulmuşdur.

İnformasiya sistemlərində verilənlərə müraciətlərə zəif nəzarət, funksiyaların və vəzifələrin müəyyən edilməsi və paylanması ilə bağlı problemlər ən geniş yayılmış zəifliklər arasındadır. Autentifikasiyanın və avtorizasiyanın idarə edilməsi sisteminin qarşısında e-servislərə asan inteqrasiya, bütün e-servislər üçün vahid təhlükəsizlik siyasəti, səlahiyyətlərin bölgüsü, insan faktorunun aşağı salınması, avtorizasiyanın idarə edilməsi sisteminin təşkilatda mövcud biznes proseslərinə uyğun olaraq çevik qurulması, avtorizasiya və çoxsəviyyəli autentifikasiyanın mərkəzləşdirilmiş idarə edilməsi, müxtəlif istifadəçi qrupları ilə (çevik, avtomatlaşdırılmış, statik, dinamik, daxili) işləmək üçün istifadəçilərin uçot yazılarının mərkəzləşdirilmiş qaydada idarə edilməsi, vahid giriş nöqtəsinin təşkili vəzifələri qoyulur.

İnformasiya təhlükəsizliyi hadisələrinin idarə edilməsi

Bu istiqamətdə həyata keçirilən əsas idarəetmə funksiyası e-dövlət infrastrukturuna hücumların aşkarlanması və təhlükəsizliyin pozulması haqqında real vaxtda xəbər verilməsidir. Bu istiqamət üzrə ənənəvi olaraq aşağıdakı problemlər üzrə modellərin, metod və alqoritmlərin işlənməsi aktualdır [21]:

- müxtəlif informasiya təhlükəsizliyi sistemlərindən, informasiya-kommunikasiya sistemlərindən hadisələr haqqında məlumatların toplanması, emalı (normallaşdırma, süzülmə, klassifikasiya, aqreqasiya, korrelyasiya və prioritetləşdirmə) və analizi;
- informasiya təhlükəsizliyi hadisələrinin retrospektiv analizi və təhqiqatı.

İnformasiya təhlükəsizliyi üzrə adekvat metrikaların işlənməsi

Son onillikdə aparıcı sənaye dövlətləri kritik vacib infrastrukturun və milli informasiya sistemlərinin təhlükəsizliyinin təmin olunması sahəsinə əhəmiyyətli kapital qoymuşlar. Lakin informasiya təhlükəsizliyi sferasına əhəmiyyətli investisiyalar qoyulmasına baxmayaraq, qəbul edilən qərarların keyfiyyəti, informasiya təhlükəsizliyi strategiyalarının effektivliyi, əks-tədbirlərin asimmetrik təhdidlərə adekvatlığı, müxtəlif resurslar üçün təhdidlərin səviyyəsinin qiymətləndirilməsi, sistemlərin destruktiv təsirlərə dayanıqlığının qiymətləndirilməsi, təhdidlərin proqnozlaşdırılması və s. kimi suallar hələlik açıq qalır [22, 23].

İnformasiya təhlükəsizliyinin idarə edilməsində əsas nəzarət parametri informasiya təhlükəsizliyi riskidir. Lakin hətta böyük olmayan korporativ şəbəkələr üçün də riskin qısa müddətdə hesablanması problematikdir. Riskin dinamik hesablanması, yayılması, azaldılması üzə uzlaşdırılmış qərar qəbul edilməsi modelləri olduqca vacibdir [24, 25].

İnformasiya təhlükəsizliyinin monitorinqi

E-dövlətin informasiya təhlükəsizliyinin monitorinq sistemi üçün informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsi vəziyyəti barəsində məlumatların ölkə miqyasında müvafiq nəzarət nöqtələrindən toplanması və ümumiləşdirilməsi, informasiya təhlükəsizliyi üzrə situasiyaların analizi, informasiya təhlükəsizliyinin təmin edilməsində ən "zəif" yerlərin müəyyən edilməsi, şəbəkədə aktiv qarşıdurma modellərinin, informasiya təhlükəsizliyi təhdidlərinin və onların həyata keçirilməsi modellərinin, informasiya müharibəsinin taktikası və strategiyasının işlənməsi problemləri vacibdir [23].

İnformasiya təhlükəsizliyi üzrə qərarların qəbul edilməsi

Mütəxəssislər qeyd edirlər ki, müasir informasiya yönümlü münaqişələrdə struktural və doktrinal üstünlük texnoloji üstünlükdən daha vacibdir [9, 12]. İyerarxik (dövlət) və şəbəkə (qeyri-dövlət) strukturlarının toqquşması zamanı birincilər daha əlverişsiz vəziyyətdə olurlar, çünki qərar qəbul etmək və baş verən hadisələrə adekvat cavab vermək üçün onlara daha çox vaxt lazım gəlir. "Şəbəkə çağırışları" bu gün dövlətlərdən idarələrarası əlaqələndirmənin yeni mexanizmlərinin işlənməsini və tətbiqini, qeyri-hökumət təşkilatları ilə sıx qarşılıqlı əlaqəni, dövlətlərarası əməkdaşlığı və milli hüquq məcəllələrinin unifikasiyasını nəzərdə tutan "şəbəkə cavabları" tələb edir.

Müasir kiberhücumlar desentralizə olunmuş, avtomatlaşdırılmış, gizli, intellektual və kooperativdir, buna görə qəbul edilmiş qərarlar və əks tədbirlər də çoxölçülü, əlaqələndirilmiş, kooperativ olmalı, informasiya təhlükəsizliyi vasitələrinin ortaq istifadəsini və məlumat mübadiləsini nəzərdə tutmalıdır.

E-dövlətin informasiya təhlükəsizliyinin humanitar problemləri

E-dövlətin informasiya təhlükəsizliyinin humanitar komponenti üzrə həyata keçirilən əsas funksiyalar informasiya sahəsində şəxsiyyətin, cəmiyyətin və dövlətin maraqları balansının təmin edilməsinə, informasiya texnologiyalarının geniş istifadə edilməsinin sosial-psixoloji nəticələrinin proqnozlaşdırılmasına, fərdi, qrup və kütləvi şüura qeyri-qanuni informasiya təsirlərindən informasiya-psixoloji mühafizənin təmin edilməsi sisteminin yaradılması və inkişafına yönəlmişdir. Bu tematik blokda informasiya təhlükəsizliyinin təmin edilməsinin aşağıdakı problemləri aktualdır [26, 27]:

- informasiya təhlükəsizliyinin ümummetodoloji problemləri (fəlsəfi, siyasi, iqtisadi, kulturoloji);
- informasiya təhlükəsizliyinin hüquqi təminatının inkişafı problemləri;
- fərdi, qrup və kütləvi şüurun sosial, psixoloji təhlükəsizliyinin təmin edilməsi problemləri.

İnformasiya təhlükəsizliyinin kadr təminatı

Son dövrlərə kimi informasiya təhlükəsizliyi problemlərinin həlli zamanı əsas diqqət müxtəlif texnoloji həllərə verilirdi. Aydın məsələdir ki, informasiya təhlükəsizliyi problemlərini təkcə texnologiyaların köməyi ilə həll etmək mümkün deyil, texnoloji həllər yalnız bəzi təhlükələrdən mühafizə olunmağa imkan verir.

Burada çox şey insan faktorundan, təşkilatın konkret əməkdaşlarının informasiya mübadiləsi proseslərində iştirakından, informasiya sistemi resurslarından istifadədən asılıdır. İnformasiya təhlükəsizliyi üzrə qəbul edilmiş beynəlxalq standartların hətta

səthi analizindən də görünür ki, informasiya təhlükəsizliyi üsullarının və vasitələrinin təxminən dörddə üçü təşkilat əməkdaşlarının iştirakını nəzərdə tutur.

Hazırda informasiya təhlükəsizliyi üzrə təhsil, əsasən, informasiya təhlükəsizliyinin texnoloji aspektləri üzrə kadrların hazırlanması və yenidən hazırlanmasına yönəlib. İnformasiya hüququ və kompyuter cinayətlərinin təhqiqatı üzrə mütəxəssislərin hazırlanmasında çox böyük gerilik mövcuddur. İnformasiya təhlükəsizliyinin kadr təminatı üzrə tədqiqat problemlərinə aşağıdakılar aiddir:

- informasiya təhlükəsizliyinin kadr təminatının ümummetodoloji əsaslarının işlənməsi, elmi biliklərin fənlərarası sahəsi kimi informasiya təhlükəsizliyi sahəsində kadr hazırlığının predmet sahəsinin analizi və əsaslandırılması;
- informasiya təhlükəsizliyi sahəsində biliklərin yayılmasının səmərəsinin yüksəldilməsi məqsədi ilə müasir təhsil texnologiyalarından istifadə yollarının tədqiqi;
- informasiya təhlükəsizliyi sahəsində kadr hazırlığının elmi, tədris-metodik və texnoloji təminat sisteminin yaradılması, o cümlədən dərsliklərin, xüsusi və tədris vəsaitlərinin, metodikaların işlənməsi, təhsil prosesində müasir informasiya texnologiyalarından effektli istifadə mexanizmlərinin formalaşdırılması.

İnformasiya təhlükəsizliyi mədəniyyəti

Səmərəli informasiya təhlükəsizliyi sisteminin fəaliyyətinin bütün cəhətləri insanlardan və proseslərdən asılıdır. İnformasiya təhlükəsizliyi məsələləri mədəniyyətin tərkib hissəsi, biznes fəaliyyətinin və xidməti vəzifənin yerinə yetirilməsinin təbii şərti olmayana kimi e-dövlətin informasiya infrastrukturu son dərəcə zəif olaraq qalacaq. Qeyd edək ki, BMT Baş Məclisinin 20 dekabr 2002-ci il tarixli 57/239 saylı qətnaməsi ilə qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün 9 element təsdiq edilmişdir (məlumatlı olmaq; cavabdehlik; reaksiya; etika; demokratiya; riskin qiymətləndirilməsi; təhlükəsizliyin layihələndirilməsi və realizə edilməsi; təhlükəsizliyin idarə edilməsi; yenidən qiymətləndirmə) [28].

Məqalələrin çoxunda informasiya təhlükəsizliyi mədəniyyətinə təşkilati mədəniyyət çərçivəsində baxılır [29, 30]. Milli və təşkilati mədəniyyətin, mühitin və məlumatlılıq faktorlarının informasiya təhlükəsizliyi və onun idarə edilməsi ilə necə əlaqəli olması müvafiq elmi ədəbiyyatda geniş müzakirə edilmir. İnformasiya təhlükəsizliyi mədəniyyətinin mürəkkəb təbiəti, elementləri, çoxmədəniyyətli mühitdə formalaşması, sosial sistem kimi modelləşdirilməsi aktual məsələlərdir.

Nəticə

E-dövlət təşəbbüslərinin uğurla həyata keçirilməsində ən vacib və ən çətin məsələlərdən biri e-dövlətin etibarlı informasiya təhlükəsizliyinin təmin edilməsidir. Bunun üçün e-dövlətin qurulması prosesində ölkə miqyasında vahid informasiya təhlükəsizliyinin idarəetmə sisteminin yaradılması zəruridir. Bu işdə e-dövlətin informasiya infrastrukturuna yeni təhdidlər, təhdid aktorlarında baş vermiş keyfiyyət dəyişiklikləri ətraflı analiz edilmiş, ənənəvi təhlükəsizlik modellərinin e-dövlət kimi mürəkkəb obyektə tətbiqində meydana çıxan əsas çətinliklər göstərilmiş, e-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə aktual elmi-tədqiqat problemləri və onların müasir vəziyyəti analiz edilmişdir.

Ədəbiyyat

1. Тоффлер Э. Третья волна. М. ООО «Издательство АСТ», 1999, с. 277.
2. The UN E-Government Survey 2008: from e-Government to connected governance, United Nations, 2007, 225 pages. http://www2.unpan.org/egovkb/global_reports/08report.htm
3. Остапенко Г.А., Мешкова Е.А. Информационные операции и атаки в социотехнических системах. Организационно-правовые аспекты противодействия. Изд.: Горячая Линия – Телеком, 2008, 208 стр.
4. Ye-Sho Chen, P.Pete Chong, Bin Zhang. Cyber security management and e-government // Electronic Government, 2004, V.1, № 3, pp.316-327
5. Wimmer M., von Bredow B. E-government: aspects of security on different layers / Proceedings of the 12th International Workshop on Database and Expert Systems Applications, 2001, pp.350-355.
6. Norris D.F. and Moon M.J. Advancing E-Government at the Grassroots: Tortoise or Hare? // Public Administration Review, 2005, V.64, № 1, pp.65-75.
7. Gilbert D., Balestrini P., and Littleboy D. Barriers and benefits in the adoption of e-government // The International Journal of Public Sector Management, 2004. V. 17, № 4/5, pp.286.
8. Conklin W.A. Barriers to Adoption of e-Government / 40th Annual Hawaii International Conference on system sciences (HICSS 2007), 2007.
9. Мешкова Т.А. Социально-политические аспекты глобальной информатизации // Полис. М., 2002. № 6, с. 24-33
10. Remarks by the President at the National Academy of Sciences Annual Meeting, National Academy of Sciences, Washington D.C., April 27, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-the-National-Academy-of-Sciences-Annual-Meeting/
11. Dhillon G. and Backhouse J. Current directions in IS security research: towards socioorganizational perspectives // Information Systems Journal, 2001, V.11, № 2, pp.127-153.
12. Arreguin-Toft I. How the Weak Wins Wars: A Theory of Asymmetric Conflict // International Security, 2001. V.26, № 1.
13. von Solms B. , Information Security - The Fourth Wave // Computers & Security, 2006, V.25, № 3, pp.165-168.
14. Edward Humphreys, Implementing the ISO/IEC 27001 Information Security Management System Standard, Artech House Publishers. 2007, 290 pages
15. Zhang N., Ryan M.D., Guelev D. Evaluating Access Control Policies Through Model Checking // Lecture Notes in Computer Science V.3650, Springer-Verlag, 2005, pp. 446-460.
16. Al-Shaer E. and. Hamed H. Discovery of Policy Anomalies in Distributed Firewalls / Proceedings of IEEE INFOCOM'2004, 2004.
17. Dunlop N., Indulska J., Raymond K., Methods for Conflict Resolution in Policy-Based Management Systems // EDOC. 2003. pp. 98-111.
18. Rachna Dhamija, Lisa Dusseault, The Seven Flaws of Identity Management Usability and Security Challenges // IEEE Security&Privacy, March/April 2008.
19. Future of Identity in the Information Society http://www.fidis.net/

20. Koong K.S., Liu L.C., Bai S. and Lin. Identity Theft in the USA: Evidence from 2002 to 2006 // International Journal of Mobile Communications, 2008, V.6, № 2, pp. 199-216.
21. Ryan Trost Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century, 1st edition, 2009, 480 pages.
22. Jaquith A., Security metrics: Replacing fear, uncertainty, and doubt. NJ: Addison-Wesley Pearson Education, 2007.
23. Krag Brotby W. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, Auerbach Publication, 2009, 200 pages.
24. Alberts C., Dorofee A. Managing information security risks: The OCTAVE (sm) approach. Boston, MA: Addison-Wesley, 2002.
25. Peltier T.R., Information security risk analysis (2nd ed.), Boca Raton, FL: Auerbach Publications, 2005.
26. Manish Gupta, Raj Sharman, Social and Human Elements of Information Security, 2008, 383 pages.
27. Ryan West, The Psychology of Security. Communications of the ACM, V.51, 4 (April 2008), pp. 34-40.
28. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002. www.oecd.org/dataoecd/16/22/15582260.pdf
29. Schlienger T., Teufel S. Information Security Culture: The Socio-Cultural Dimension in Information Security Management / Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), 2002, IFIP Conference Proceedings 214, pp. 191-202
30. Chang S.E., and Ho C.B. Organizational factors to the effectiveness of implementing information security management // Industrial Management & Data Systems, 2006, V.106, № 3, pp.345-361.

УДК 004.351

Алгулиев Р.М., Имамвердиев Я.Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
director@iit.ab.az, yadigar@lan.ab.az

Информационная безопасность э-государства: актуальные направления исследования

Одной из самых важных и трудных задач, возникающих при построении э-государства, является обеспечение надежной информационной безопасности. В этой работе идентифицированы актуальные научные проблемы по управлению информационной безопасностью э-государства и анализируется их современное состояние. Детально проанализированы новые угрозы информационной инфраструктуре э-государства и качественные изменения акторов угроз, указаны основные трудности, возникающие при попытке применения традиционных моделей информационной безопасности к сложным объектам, таким, как э-государство.

***Ключевые слова**: э-государство, информационная безопасность, информационная война, асимметричные угрозы, политика информационной безопасности, управление информационной безопасностью, культура информационной безопасности.*

Alguliev R.M., Imamverdiyev Y.N.
Institute of Information Technology ANAS, Baku, Azerbaijan
director@iit.ab.az, yadigar@lan.ab.az

E-Government Information Security Management Research Challenges

One of the most important and the most difficult tasks encountered in the e-government building is providing reliable and trustful information security for e-government. In this paper actual research problems in the field of e-government information security management are identified and state-of-the-art of problems is analyzed. The new threats to the information infrastructure of e-government, and qualitative changes of the threats are analyzed in details. The basic difficulties emerged in adapting of traditional security models of information security to complex objects as e-government are shown.

Key words: *e-government, information security, information war, asymmetric threats, information security policy, information security management, information security culture.*