# E-dövlətin informasiya təhlükəsizliyi və texnoloji çağırışlar

Şakir Mehdiyev[1], Yadigar İmamverdiyev[2]
*AMEA İnformasiya Texnologiyaları İnstitutu*
[1]shakir@iit.ab.az, [2]yadigar@lan.ab.az

***Xülasə*— E-dövlətin informasiya təhlükəsizliyinə yönəlmiş təhdidlər informasiya sahəsində milli maraqlara qarşı yönəlib. E-dövlətin informasiya təhlükəsizliyinin etibarlı təmin edilməsi üçün siyasi, hüquqi, təhsil, idarəetmə ilə yanaşı, adekvat texnoloji bazanın formalaşdırılması və təkmilləşdirilməsi xüsusi əhəmiyyət daşıyır. Bu işdə milli informasiya təhlükəsizliyi sisteminin formalaşdırılması və təkmilləşdirilməsində qarşıya çıxan əsas texnoloji çağırışlar analiz edilir, inkişaf etmiş ölkələrin bu sahədə təcrübəsi araşdırılır və bir sıra elmi-praktiki tövsiyələr verilir.**

***Açar sözlər*— *e-dövlət; informasiya təhlükəsizliyi; informasiya suverenliyi; aparat troyanları; sertifikatlaşdırma.***

## I. GİRİŞ

İnformasiya təhlükəsizliyinin təmin edilməsi hüquqi, təşkilati və texnoloji aspektləri nəzərdə tutan kompleks yanaşma tələb edir. Son dövrlər ölkəmizdə informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin, hüquqi bazanın təkmilləşdirilməsi, dövlət agentlikləri səviyyəsində təşkilati strukturların yaradılması və onların fəaliyyətə başlaması ilə yanaşı, informasiya təhlükəsizliyinin texnoloji komponentlərinin yaradılması sahəsində də məqsədyönlü işlər aparılır. Buna misal olaraq, e-imza infrastrukturunun yaradılması ilə əlaqədar kompleks işləri göstərmək olar.

İnformasiya təhlükəsizliyi mühiti dinamik inkişaf edir, yeni hücum texnologiyaları meydana çıxır və müvafiq müdafiə texnologiyalarının təkmilləşdirilməsini və yenilərinin yaradılmasını tələb edir.

Ölkənin informasiya fəzasının müasir təhdidlərdən qorunması hazırda milli təhlükəsizliyin təmin edilməsinin prioritet istiqamətlərindən biridir. "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununda "informasiya texnologiyaları sahəsində geriləmə və dünya informasiya məkanına daxil olmağa maneələrin mövcudluğu" informasiya sahəsində milli təhlükəsizliyə əsas təhdidlərdən biri olaraq göstərilir (Maddə 7.9) [1]. İnformasiya və kommunikasiya texnologiyalarının inkişafı sahəsində məqsədyönlü dövlət siyasəti sayəsində bu maneələrin aradan qaldırılması üzrə bir sıra işlər görülmüşdür (o cümlədən, Azərbaycanın süni peykinin orbitə buraxılması). Dövlətlərarası rəqabət mühitinə çevrilən qlobal informasiya fəzasında ölkənin informasiya müstəqilliyini və suverenliyini təmin etmək, milli maraqlarını etibarlı şəkildə qorumaq üçün dövlətin bu sahədə fəaliyyəti ardıcıl şəkildə genişləndirilir, informasiya təhlükəsizliyi sahəsində əlavə tədbirlər kompleksi həyata keçirilir [2].

Bu işin məqsədi milli informasiya təhlükəsizliyi sahəsində meydana çıxan texnoloji çağırışları analiz etmək və onların həlli istiqamətində müəyyən yollar axtarmaqdır.

## II. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNƏ ƏSAS TƏHDİDLƏR

E-dövlətin informasiya təhlükəsizliyi informasiya sahəsində milli maraqların təmin edildiyi vəziyyət kimi müəyyən edilir. İnformasiya sahəsi – ölkənin informasiya infrastrukturunun və informasiyanın yaradılmasını, informasiyanın toplanmasını, formalaşdırılmasını, yayılmasını və istifadəsini həyata keçirən subyektlərin və bu zaman meydana çıxan ictimai münasibətlərin tənzimlənməsi sisteminin məcmusudur.

İnformasiya sahəsində ölkənin milli maraqlarının aşağıdakı komponentlərini müəyyən etmək olar:

- vətəndaşların informasiya azadlığının təmin edilməsi;
- ölkənin milli-mənəvi dəyərlərinin və ənənələrinin, mədəni və elmi potensialının qorunması və inkişafı;
- fərdi, qrup və ictimai şüurun bədniyyətli təsirlərdən qorunması;
- e-xidmətlərin (e-hökumət, e-səhiyyə, e-biznes, e-maliyyə, e-bank, e-seçki və s.) təhlükəsizliyinin təmin edilməsi;
- fərdi məlumatların konfidensiallığının qorunması;
- dövlət siyasətinin informasiya təminatı;
- informasiya resurslarının konfidensiallığının, tamlığının və əlyetərliliyinin təmin edilməsi;
- informasiya və telekommunikasiya sistemlərinin təhlükəsizliyinin təmin edilməsi;
- kritik infrastrukturun informasiya təhlükəsizliyinin təmin edilməsi;
- informasiya sənayesi və informasiya texnologiyaları sahəsində milli istehsalın rəqabətədavamlı inkişafının təmin edilməsi.

E-dövlət digər dövlətlərdən, transmilli terror şəbəkələrindən, mütəşəkkil kibercinayətkarlıqdan, haktivist qruplardan, yeni texnologiyalardan qaynaqlanan təhdidlərlə xarakterizə olunan mürəkkəb informasiya təhlükəsizliyi mühiti ilə qarşı-qarşıyadır.

Siyasi, iqtisadi və hərbi hədəflərə qarşı kibercasusluq həyata keçirilir.

Müəyyən ölkələr qlobal informasiya fəzasında özlərinin üstün vəziyyətlərindən hərbi-siyasi məqsədlərinə çatmaq üçün, öz maraqlarına nail olmaq üçün "yumşaq güc" aləti, siyasi

təzyiq aləti kimi də istifadə edirlər. Bununla da, kiberfəza informasiya müharibəsi, informasiya qarşıdurması məkanına çevrilir.

Digər dövlətlər, eləcə də qeyri-dövlət aktorları tərəfindən kiberfəzaya hücumlar həyata keçirilir. Kiberhücum metodları və vasitələri, bu hücumların həyata keçirilməsi taktikaları daim təkmilləşir, onların intensivliyi isə beynəlxalq vəziyyətdən birbaşa asılı olur.

Kibercinayətkarlıq getdikcə böyük miqyas alır.

Ölkəni, onun müttəfiqlərini və digər dövlətləri, eləcə də qeyri-dövlət aktorları cəlb edən dövlətlərarası beynəlxalq hərbi münaqişələr mövcuddur.

Beynəlxalq terrorizm şəbəkəsi kiberfəzadan öz ideologiyasını yaymaq, təbliğat aparmaq, insanları öz sıralarına cəlb etmək üçün geniş istifadə edir.

Milli miqyasda yayılan böyük qəzalar və təbii fəlakətlər də istisna edilmir.

E-dövlətin informasiya təhlükəsizliyinin informasiya-texniki (məsələn, kiber-müharibə) və informasiya-psixoloji (informasiya müharibəsi) komponentlərinin təmin edilməsi tələb edilir. Bu tələbin yerinə yetirilməsi üçün ideal şərait bütün istiqamətlərdə texnoloji müstəqilliyin təmin edilməsidir:

- aparat platforması (prosessorlar və mikrosxemlər, şəbəkə avadanlığı, GPS);
- proqram təminatı platforması (əməliyyat sistemləri, ofis proqramları, VBİS, brauzerlər, antivirus proqramları);
- mobil platforma (avadanlıq və əməliyyat sistemləri, tətbiqi proqramlar);
- müstəqil İnternet infrastrukturu;
- informasiya infrastrukturu (axtarış sistemləri, ənənəvi və e-KİV, sosial media, ani məlumat xidməti);
- kontent resursları və analitika;
- uşaqlar üçün təhlükəsiz İnternet;
- informasiya təsirinin idarə edilməsi sistemi (social medianın və trafikin monitorinq və analizi, trafikin filtrasiyası, informasiyanın yayılması və rəyin idarə olunması üçün insan və texniki resurslar);
- informasiya fəzasının fasiləsiz monitorinqi sistemi (monitorinq, hücumların aşkarlanması, qarşısının alınması, bloklama, proaktiv əks-hücumlar).

Aydındır ki, hətta inkişaf etmiş ölkələrin də bütün bu məsələlərin öhdəsindən gəlməsi problematikdir. İnkişaf etməkdə olan ölkələrin strategiyası müvafiq riskləri adekvat qiymətləndirmək, ilk növbədə həll edilməsi ölkənin texnoloji, iqtisadi, insan resursları imkanında olan təxirəsalınmaz imkanları müəyyən etmək, digər problemlərin həlli üçün bu sahədə strateji müttəfiqlərlə səylərini birləşdirməkdir.

## III. APARAT TƏMİNATINDA TROYANLAR

Kompüterləşdirilmiş aparat təminatı həm mülki, həm də hərbi təyinatlı sistemlərdə geniş istifadə edilir. Ölkələrin əksəriyyətinin bu texnologiyaları müstəqil inkişaf etdirmək imkanları yoxdur. Bu bölmədə mikrosxemlərin təhlükəsizliyi sahəsində vəziyyəti qiymətləndirmək üçün aparat təminatında zərərli proqramların bir növü − troyanlar haqqında qısa icmal aparılır.

Aparat troyanları üzrə tədqiqatlar 2005-ci ildə ABŞ Müdafiə Nazirliyi hərbi avadanlıqda xaricdə istehsal edilmiş mikrosxemlərdən geniş istifadəsi ilə bağlı öz narahatlığını bəyan edəndən sonra başlanmışdı [3].

Kaliforniya Universitetinin (Los-Anceles) professoru Con Villasenor qeyd edir ki, mikroçiplərin layihələndirilməsində və istehsalında bütün dünyaya səpələnmiş yüzlərlə müəssisə iştirak edir və ehtimal var ki, bütün texnoloji zəncirdə nəzarət edilməyən yerlər olsun. Mikroçip bloklarının mürəkkəbliyi hazırda elə səviyyədədir ki, heç bir təşkilat onlarda nəzəri mümkün, sənədləşdirilməmiş funksiyaların mövcud olmasını tam yoxlamaq imkanında deyil. Boşluqlar mikrosxemlərə həm layihələndirmə, həm də istehsal prosesində daxil edilə bilər. Hazır çipləri də modifikasiya etmək mümkündür, lakin bunun üçün qiyməti bir neçə milyon dollar olan avadanlıq (ion tavlama qurğusu) tələb edilir. Bu qurğuda fokuslanmış ionlar dəstəsinin köməyi ilə çipin müxtəlif məntiqi elementləri arasında əlaqələri dəyişmək olur [4].

Müasir mikrosxemin funksional bloku müxtəlif istehsalçılar və şirkətlər tərəfindən layihələndirilir, offşor zavodlarda istehsal edilir, başqa bir şirkət tərəfindən qablaşdırılır və digər bir şirkət tərəfindən isə satılır. Çip istehsalının belə autsorsinqi və qloballaşması etimad və təhlükəsizlik problemləri yaradır.

Məsələn, Kembric Universitetinin informasiya təhlükəsizliyi üzrə qrupu Çin istehsalı olan PROAsic 3 çipində təhlükəli boşluq aşkarlamışdı [5]. Bu boşluq kriptoqrafik müdafiə sistemini söndürməyə, AES şifrləmə açarlarını dəyişməyə, şifrlənməmiş verilənlərə giriş əldə etməyə və ya hətta çipi sıradan çıxarmağa imkan verir. Tədqiqatçılar bu boşluğu aktivləşdirən məxfi açarı əldə edə bilmişdilər. Bu mikrosxemlər infrastruktur obyektlərində, atom stansiyalarında və hətta silah sistemlərində geniş istifadə edilir.

Aparat təminatına, xüsusilə də hərbi və digər kritik tətbiqlər üçün nəzərdə tutulanlara istehsal prosesində daxil edilmiş troyanların aşkarlanması və onlarla mübarizə üçün bir sıra yanaşmalar təklif edilmişdir. Aparat troyanlarının aşkarlanması üsullarına destruktiv testləri, mikrosxemin Rentgen şüaları ilə müayinəsini, test edilən mikrosxemin işinin nəticələrini troyan olmayan ideal çipin (“qızıl çip“) nəticələri ilə müqayisə edilməsi və s. aiddir [6-9]. Başqa bir üsul qeyri-səlis test metodudur (ing. fuzzy testing). Çipə qeyri-standart sorğular göndərməklə test edilən mikrosxemdə bədniyyətlə yaradılmış və ya dəyişiklik edilmiş blokları aşkarlamaq mümkündür.

Zərərli proqramların istənilən proqram təminatı məhsulunu yoluxdura bilməsi bir qanunauyğunluq kimi qəbul edilir. Ümid edilirdi ki, aparat vasitələrində zərərli proqramlar ola bilməz. Lakin son dövrlər mikroçiplərdə troyanların yerləşdirilməsi texnologiyalarında xeyli inkişaf haqqında məlumatlar verilir [10]. Məsələn, ABŞ, Almaniya, İsveçrə və Niderlanddan olan

tədqiqatçılar qrupu yarımkeçirici mikrosxemlərə troyanların gizli yerləşdirilməsi metodunu işləyib hazırlamışlar. Bu metodla hazırlanmış boşluğu nə destruktiv testlərlə, nə də etalon çiplərlə və digər analoji metodlarla aşkarlamaq mümkün deyil. Yoluxdurma üçün mikrosxemə hər hansı əlavə tranzistorlar və ya yollar salmaq lazım deyil. Bu metodun mahiyyəti çipin istehsalı gedişində tranzistorun müəyyən sahələrində dopantların polyarlaşmasını dəyişməkdən ibarətdir (dopant − materialın xüsusi elektrik keçiriciliyini artıran əlavə qatqıdır). Tədqiqatçılar öz metodlarını üçüncü nəsil Intel Core prosessorunda sınaqdan keçirərək, psevdotəsadüfi ədədlər generatorunu modifikasiya etməklə kriptoqrafik təhlükəsizliyi əhəmiyyətli şəkildə aşağı salmışdılar (128 bitdən 32 bitə).

Kibersilah arsenalında daha bir inqilabi texnoloji yenilik kritik texnoloji proseslərin idarə edilməsində istifadə edilən mikrosxemlər (ing. programmable logic controllers, PLC) üçün nəzərdə tutulmuş virusların yaradılmasıdır. 2009-2012-ci illərdə aşkarlanmış Stuxnet virusunun və onun ardıcıllarının (Flame, Gauss, Duqu) analizi göstərir ki, bu zərərli proqramları hansısa haker qrupu deyil, dövlət dəstəkli təşkilat(lar) yaradıb. Belə virusların hazırlanmasına on milyonlarla dollar vəsait sərf edildiyi güman edilir. Bundan başqa, viruslar o qədər mürəkkəbdirlər ki, onları mütəxəssislərin böyük qrupu bir neçə il (məsələn, Gauss – 5 il) ərzində hazırlaya bilərdi (Kaspersky Lab) [11].

Son zamanlar çiplərin geniş istifadə edildiyi daha bir sahə - “Əşyaların İnterneti” meydana çıxır və tədricən “İnsanların interneti”nə çevrilir. Tibbi məqsədlər üçün implant-çiplərin – kardiosimulyatorların, insulin dozatorlarının, eşitmə aparatlarının və s. istifadəsi genişlənməkdədir. Eyni zamanda, implantant-çiplərin insan-kompüter qarşılıqlı əlaqəsinin rahat aləti kimi insanların gündəlik işlərində − əlin bir hərəkəti ilə qapını açmaq, alış-veriş etmək, kompüterə, binaya daxil olmaq və s. üçün istifadəsi də artır. İnsanın “çipləşdirilməsi” ideyasının populyarlaşdırılması ilə məşğul olan İsveç biohakerlərinin cəmiyyəti Kaspersky Lab ilə birgə “insanın İnternətə qoşulması”nın təhlükəsizliyini qiymətləndirmək üçün birgə tədqiqat layihəsi həyata keçirir.

## IV. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ SİSTEMİ: TEXNOLOJI ÇAĞIRIŞLAR

İlk növbədə İnternetin milli seqmentinin dayanıqlılığını və təhlükəsizliyini təmin etmək vacibdir. İnternetin milli seqmentinin işini pozmağa yönəlmiş cəhdlərin qarşısı operativ alınmalıdır. Belə cəhdlərin qarşısının alınması üzrə idarələrarası təlimlərin keçirilməsi və bu təlimlərin nəticələri əsasında ölkənin bu sahədə suverenliyini etibarlı təmin etmək üçün müvafiq tədbirlər işlənib hazırlanmalıdır.

Kommunikasiya şəbəkələrinin, dövlət və özəl informasiya resurslarının kiberhücumlara qarşı müdafiəsi də lazımi səviyyədə gücləndirilməlidir.

Vətəndaşların onlayn mühitdə onları gözləyən risklərdən qorunması da e-dövlətin vəzifələrindən biridir. Burada dünyanın qabaqcıl ölkələrində tətbiq edilən praktikadan istifadə edilməsi məqsədəuyğundur.

İşlərin digər istiqaməti – milli texnologiyaların, texnikanın və informasiya məhsullarının inkişaf etdirilməsidir. Eyni zamanda, onların dövlət strukturlarında və yerli şirkətlərdə istifadəsini stimullaşdırmaq lazımdır. Bu sahədə prioritet tədbirlər işlənib hazırlanmalıdır.

Qlobal informasiya təhlükəsizliyinin təmin edilməsi sahəsində qlobal və regional təşkilatlar çərçivəsində əməkdaşlığın genişlənməsi də vacib istiqamətlərdən biridir.

İnformasiya təhlükəsizliyi üzrə milli sertifikatlaşdırma sisteminin formalaşdırılması, o cümlədən xüsusi sınaq laboratoriyalarının yaradılması da vacib məsələdir.

Açıq kodlu proqram təminatı əsasında milli əməliyyat sisteminin yaradılması və informasiya təhlükəsizliyi baxımından kritik sistemlərdə istifadəsi də strateji vacib məsələdir.

Ekspertizadan keçmiş açıq kodlu proqram təminatı bazasının yaradılması da nəzərə alınmalıdır.

## V. İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜZRƏ MİLLİ SERTİFİKATLAŞDIRMA SİSTEMİ

İnformasiya təhlükəsizliyi vasitələrinin (aparat və proqram) informasiya təhlükəsizliyi tələbləri üzrə sertifikatlaşdırılması informasiya təhlükəsizliyinin təmin edilən səviyyəsinə zəmanət sistemində vacib yer tutur. Həm proqram vasitələrinin, həm də aparat vasitələrinin informasiya təhlükəsizliyi tələbləri üzrə sertifikatlaşdırılması sistemi nəzərdə tutulmalıdır.

Qanunvericilikdə informasiya sistemlərinin informasiya təhlükəsizliyi tələbləri üzrə attestasiyası da nəzərdə tutulub.

Təşkilatın informasiya təhlükəsizliyinin idarə edilməsi sisteminin ISO 27001 standartının tələblərinə uyğunluğunun sertifikatlaşdırılması da zamanın tələbidir.

Qiymətləndirmə standartlarının içərisində ən tamı və müasiri İSO/İEC 15408 "İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları" standartıdır (“Ümumi meyarlar”).

Bir sıra səbəblərdən kriptoqrafik alqoritmlərin spesifik xassələrinin qiymətləndirilməsi üçün meyarlar “Ümumi meyarlara” daxil edilməyib, belə qiymətləndirmə standartı kimi “Ümumi meyarlar” FIPS 140-2 standartına müraciət edir.

İnformasiya təhlükəsizliyi vasitələrinin Ümumi Meyarlar standartının tələbləri üzrə sertifikatlarının digər ölkələr tərəfindən tanınması məsələsi meydana çıxır (ing. Common Criteria Recognition Arrangement – CCRA) [12].

## NƏTİCƏ

Uğurlu informasiya təhlükəsizliyi strategiyası siyasi, hüquqi, təhsil, idarəetmə və texnoloji səviyyələrdə həllər təklif edən multi-disiplinar yanaşmaya əsaslanır. İnformasiya sahəsində kəskinləşən beynəlxalq rəqabət şəraitində informasiya təhlükəsizliyinin etibarlı təmin edilməsi dövlətin texnoloji müstəqilliyi ilə müəyyən edilir.

## ƏDƏBİYYAT

[1] Milli təhlükəsizlik haqqında Azərbaycan Respublikasının Qanunu.

[2] İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı, 26 sentyabr 2012-ci il.

[3] Defense Science Board Task Force on High Performance Microchip Supply, 2005. www.cra.org/govaffairs/images/2005-02-HPMS_Report_Final.pdf

[4] J. Villasenor, "The Hacker in Your Hardware," Scientific American, pp. 82-87, August 2010.

[5] S. P. Scorobogatov, "Semi-invasive attacks – a new approach to hardware security analysis." PhD diss., University of Cambridge, 2005.

[6] R. Karri, J. Rajendran, K. Rosenfeld, M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," Computer, vol. 43, no. 10, pp. 39-46, 2010.

[7] С. В. Балыбин, Е. Н. Белов, В. Н. Федорец, "Информационная безопасность военной техники, использующий интегральные схемы иностранного производства," Военная мысль, №12, с.11-21, 2011.

[8] J. A. Roy, F. Koushanfar, I.Markov, "Ending privacy of integrated circuits," Computer, vol. 43, no. 10, pp. 30-38, 2010.

[9] Y. Jin and Y. Makris "Hardware trojan detection using path delay fingerprint", Proc. IEEE Int-l Workshop Hardware-Oriented Security and Trust (HOST 08), pp.51 -57 2008.

[10] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans," Cryptographic Hardware and Embedded Systems-(CHES), pp. 197-214, 2013.

[11] D. Kushner, "The Real Story of Stuxnet," IEEE Spectrum, February 2013

[12] Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security. https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf