Elektron dövlətdə kriptoqrafiya sahəsində siyasətin formalaşdırılması problemləri

Rasim Əliquliyev[1], Yadigar İmamverdiyev[2]
AMEA İnformasiya Texnologiyaları İnstitutu
[1]*director@iit.ab.az;* [2]*yadigar@lan.ab.az*

***Xülasə*— E-dövlətin informasiya təhlükəsizliyinin təmin edilməsinin texnoloji komponentlərində kriptoqrafik metodlar mühüm rol oynayır. Bu işdə e-dövlətdə kriptoqrafiya üzrə siyasətin formalaşdırılması problemləri analiz edilir, inkişaf etmiş ölkələrin bu sahədə təcrübəsi araşdırılır, kriptologiya sahəsində elmi tədqiqatların müasir vəziyyəti açıq beynəlxalq kriptoqrafik müsabiqələrin təcrübəsi əsasında analiz edilir. Nəticə olaraq, inkişaf etməkdə olan ölkələr üçün model kriptoqrafiya siyasətinin əsas istiqamətləri müəyyən edilir və bu siyasətin praktiki həyata keçirilməsində qarşıya çıxması gözlənilən bir sıra problemlər üzrə tövsiyələr verilir.**

Açar sözlər*— *e-dövlət; informasiya təhlükəsizliyi; kriptoqrafiya; kriptoanaliz; kriptoqrafiya siyasəti.

I. GİRİŞ

E-dövlətin informasiya təhlükəsizliyinin təmin edilməsində kriptoqrafiya metodlarına əsaslanan texnologiyalar mühüm rol oynayır. Dövlət sirlərinin qorunması üçün kriptoqrafik mühafizə vasitələri uzun müddətdir ki, istifadə edilir. Bununla yanaşı, e-dövlətdə açıq açarlı kriptoqrafiya əsasında etimad infrastrukturu formalaşdırılır, e-dövlətin aktorları arasındakı kommunikasiyaların konfidensiallığı məxfi açarlı kriptoqrafiya ilə qorunur, elektron xidmətlərdə tranzaksiyaların etibarlılığı elektron imza texnologiyaları ilə təmin edilir [1]. Kriptoqrafik metodlar informasiya təhlükəsizliyinin təmin edilməsinin bir sıra digər tədbirlərinin həyata keçirilməsində də baza texnologiyaları kimi çıxış edir.

E-dövlətdə kriptoqrafiyaya əsaslanan texnologiyaların tətbiqi bir çox problemlərlə müşayiət olunur. Dünya ölkələrində kriptoqrafiyanın tətbiqi təcrübəsinin analizi iki tendensiya arasında mübarizənin gücləndiyini ortaya qoyur. Bir tərəfdən, kriptoqrafiyanın geniş istifadəsi müxtəlif sahələrdə qanunsuz hərəkətlərin qarşısının alınması üzrə hüquq-mühafizə orqanlarının axtarış-kəşfiyyat işlərini əhəmiyyətli dərəcədə çətinləşdirə bilər. Digər tərəfdən, İnsan hüquqları üzrə Ümumdünya Bəyannaməsinin 12-ci bəndi ilə qorunan əsas insan hüquqlarının – şəxsi həyatın toxunulmazlığı, ailə sirlərinin və fərdi məlumatların konfidensiallığının qorunması hüquqlarının təmin edilməsi üçün kriptoqrafik metodların istifadəsi qaçılmazdır.

Kriptoqrafiya həmişə dövlət sirlərinin qorunması ilə əlaqəli olmuş və dövlətlərarası rəqabətdə və münaqişələrdə müəyyən mənada iştirak etmişdir. Hətta bəzi müəlliflər kriptoqrafiyanı nüvə silahı və raket texnologiyaları ilə birgə güclü dövlətin simvolu hesab edirlər [2]. Qloballaşan dünyada güclü kriptoqrafiya da bir neçə dövlətin inhisarındadır. Müstəqilliyini yeni qazanmış və inkişaf etməkdə olan ölkələrdə kriptoqrafiya sahəsində yetərli təcrübə, kadr potensialı və müvafiq elmi-tədqiqatlar yoxdur və kriptoqrafiya sahəsində aparat və proqram vasitələrinin istehsalı müasir tələblər səviyyəsində deyil. Adətən, kriptoqrafik mühafizə vasitələrindən istifadə məsələləri bir neçə dövlət təşkilatının səlahiyyəti çərçivəsində olur və bu müvafiq koordinasiyanı tələb edir. Eyni zamanda, e-dövlət mühitində kriptoqrafik metodların biznes sektoru və vətəndaş cəmiyyəti institutları tərəfindən geniş istifadə edilməsi də dövlətin maraqları çərçivəsindədir.

Göstərilən bu və ya digər problemlərin dövlətin, biznes sektorunun və vətəndaş cəmiyyətinin uzlaşdırılmış maraqları və əlaqələndirilmiş fəaliyyətləri çərçivəsində effektiv həll edilməsi üçün kriptoqrafiya sahəsində müvafiq dövlət siyasətinin formalaşdırılması vacibdir. Təqdim olunan işdə e-dövlətin kriptoqrafiya sahəsində siyasətinin formalaşdırılması problemləri analiz edilir, bu sahədə beynəlxalq təcrübə araşdırılır, dövlət siyasətinin əsas istiqamətləri üzrə bir sıra tövsiyələr təklif edilir.

II. KRİPTOQRAFİYA HAQQINDA QISA ARAYIŞ

«Kriptoqrafiya» sözü yunan dilində κρυπτός (kryptos) – «gizli» və γραφω (grapho) – «yazı» sözlərindən yaranmışdır. Son dövrlər «kriptoqrafiya» sözü ilə yanaşı, «kriptologiya» sözü də tez-tez işlədilir, lakin onların arasındakı münasibət heç də həmişə düzgün başa düşülmür. Kriptologiya iki hissədən – *kriptoqrafiya* və *kriptoanalizdən* ibarət elmdir [3].

Kriptoqrafiya – bədniyyətlinin müəyyən hərəkətlərindən qorunmaq məqsədi ilə informasiyanın çevrilməsi üsullarını öyrənir.

Kriptoanaliz – qorunan informasiyanı əldə etmək məqsədi ilə kriptoqrafik çevirmələrin (şifrlərin) analizi metodları haqqında elmdir (və onların tətbiqi praktikasıdır).

Kriptologiya tətbiqi elmdir, o, fundamental elmlərin, ilk növbədə, riyaziyyatın ən son yeniliklərindən istifadə edir. Digər tərəfdən, kriptoqrafiyanın bütün konkret məsələləri texnikanın və texnologiyanın inkişaf səviyyəsindən, tətbiq edilən rabitə vasitələrindən və informasiyanın ötürülməsi üsullarından əhəmiyyətli dərəcədə asılıdır.

Əsrlər boyu qapalı elm olan kriptoqrafiya yalnız dövlət, diplomatik və hərbi sirlərin qorunması üçün istifadə edilirdi. Kriptoqrafik metodların açıq kommersiya sistemlərində, hər şeydən əvvəl, bank sistemlərində istifadəsinə fəal cəhdlər 1960-ci illərin sonlarından başladı. Bu da kriptoqrafiya

sahəsində açıq tədqiqatların meydana çıxmasına gətirib çıxartdı. Bəzi tədqiqatçılar bunu "*açıq kriptoqrafiya*" adlandırırlar. 1970-ci illərdə kriptoqrafiyanın sonrakı inkişafına böyük təkan verən iki inqilabi hadisə baş verdi [2].

Birinci inqilabi hadisə 1977-ci ildə ABŞ-da DES (Data Encryption Standard) verilənləri şifrləmə standartının qəbul edilməsi idi. Bu proses digər ölkələrdə də davam etdi və inkişaf etmiş ölkələr öz şifrləmə standartlarını işləməyə başladılar. Nəticədə, 1990-cı illərin əvvəlində dövlət sirri təşkil etməyən məlumatların qorunması sahəsində ənənəvi şifrləmə vasitələrindən imtina yolunda ilk prinsipial addım atıldı – ölkələrin əksəriyyətində məxfi alqoritmlərin yerinə açıq alqoritmlərin istifadəsinə üstünlük verilməyə başlandı.

İkinci inqilab 1976-cı ildə açıq açarlı kriptoqrafiyanın meydana çıxması ilə baş verdi. Açıq açarlı kriptoqrafiya bir neçə yeni tətbiq sahəsinin, o cümlədən rəqəmsal imza və elektron pul sistemlərinin yaranmasına səbəb oldu. Açıq açarlı kriptoqrafiyanın meydana çıxması kriptoqrafik texnologiyaların tətbiqi imkanlarını köklü surətdə genişləndirdi. Hazırda kriptoqrafiya konfidensiallığın təmin edilməsi, tamlığa nəzarət, autentifikasiya və rəqəmsal imza kimi informasiya təhlükəsizliyi funksiyalarının təmin edilməsi üçün ən effektiv vasitədir.

III. ABŞ-IN KRİPTOQRAFİYA SİYASƏTİ

Mövcud işlərdə "kriptoqrafiya siyasəti" anlayışı "kriptoqrafiyanın tətbiqi siyasəti" anlayışı ilə eyniləşdirilir. Bu anlayışın məzmununu isə kriptoqrafik məhsulların idxalı, ixracı və tətbiqi məsələləri təşkil edir. İnformasiyanın kriptoqrafik mühafizəsi vasitələrinin tətbiqinin tənzimlənməsinin əsas mexanizmləri bu vasitələrin yaradılması, istifadəsi və yayılması sahəsində fəaliyyətin lisenziyalaşdırılması və məhsulun sertifikatlaşdırılmasıdır. Daha bir mexanizm kriptoqrafik məhsulların idxalı, ixracı, tətbiqi və onlara xidmət məsələlərinə nəzarətin həyata keçirilməsidir.

İnformasiya və kommunikasiya texnologiyaları ilə yanaşı, kriptoqrafiya sahəsində də dünyada lider mövqeyində olan ABŞ-ın kriptoqrafiya siyasətinin formalaşdırılmasına və həyata keçirilməsinə bir neçə dövlət orqanı cəlb edilib. Kriptoqrafiyanın istifadəsi və yayılması sahəsində ABŞ-ın siyasətinə ölkə prezidenti nəzarət edir. ABŞ-da kriptoqrafiya sahəsində dövlət siyasətinin formalaşdırılmasında və həyata keçirilməsində Milli Təhlükəsizlik Agentliyi (ing. National Security Agency, NSA) aparıcı rol oynayır. Bu agentlik radio-elektron vasitələrdən istifadə etməklə və potensial düşmənlərinin və hətta öz müttəfiqlərinin də şifrlərini açmaqla kəşfiyyat məlumatları əldə etməklə məşğuldur. Kriptoqrafiya sahəsində standartların işlənməsini və qəbul edilməsini Milli Standartlar və Texnologiyalar İnstitutu koordinasiya edir. Kriptoqrafiya sahəsində açıq elmi-tədqiqat prioritetlərinin müəyyən edilməsi və maliyyələşdirilməsi isə Milli Elm və Texnologiya Şurası ilə Milli Elm Fondunun səlahiyyətlərinə aiddir.

Vaasenaar sazişinə görə, kriptoqrafik mühafizə vasitələri silah sistemlərinə aid edilir və ABŞ-da kriptoqrafiyanın istifadəsini və ixracını Silahların beynəlxalq ticarətinə nəzarət Qanunu (International Traffic in Arms Regulations, ITAR) məhdudlaşdırırdı.

Açıq açarlı kriptoqrafiyanın meydana çıxması ilə kriptoqrafiyanın yalnız dövlətin maraqları üçün istifadəsinə tərəfdar olanlarla onun daha geniş tətbiqini zəruri və məqsədəuyğun hesab edənlər arasında mübarizə də kəskinləşdi.

İlk əvvəl, RSA alqoritminin nəşrinə mane olmaq istəyirdilər (1977-ci il), lakin bu baş tutmadı və güclü kriptoqrafiyanın istifadəsinə hüquqi maneələr yaratmağa cəhdlər edildi.

1982-ci ildə Milli Təhlükəsizlik Agentliyi ilə sənaye və akademik dairələrin birgə komissiyası tərəfindən ABŞ-da kriptoqrafiya sahəsində açıq elmi tədqiqatların aparılmasına məhdudiyyətlər qoyulması haqqında qərar qəbul edildi. Sonradan etiraf edildiyi kimi, bu tədbir ideyaların dünyada yayılmasını və inkişafını məhdudlaşdırmadı, əksinə, amerikan açıq kriptoqrafiyasında geriliyə gətirib çıxardı. Nəticədə, bir neçə il sonra bu məhdudiyyətlər faktiki olaraq yaddan çıxdı və 1990-cı illərdə formal olaraq ləğv edildi.

Kriptoqrafiyanın praktiki istifadəsində əsas məsələ açarlara kimin nəzarət etməsidir. ABŞ hökuməti açar depoziti ilə şifrləmə (ing. "key escrow encryption") adlanan yanaşmanı dəstəkləyirdi. Bu yanaşmaya görə, istifadəçilər güclü kriptoqrafiyadan istifadə edə bilərlər, lakin üçüncü tərəf, məsələn, dövlət strukturu və ya dövlətin səlahiyyət verdiyi şirkət açarları depozitdə saxlayır və qanuni əsaslar olduqda (məsələn, məhkəmənin qərarı və ya milli təhlükəsizlik maraqları) sorğu əsasında dövlət orqanlarına verir. Açar depoziti ilə şifrləmə sistemini həyat keçirmək üçün 1992-ci ildə Clipper Initiative irəli sürüldü. Clipper kriptoçipinin telefonlarda, fakslarda və elektron poçtda şifrləmə zamanı istifadə edilməsi nəzərdə tutulurdu. Hökumət Clipperin istifadəsinin könüllü olacağını bəyan etmişdi, lakin ictimaiyyətin reaksiyası hökumətin gözlədiyinin əksinə oldu. Nəticədə dəstək qazana bilməyən hökumət bu təşəbbüsü geri çəkməyə məcbur oldu.

ABŞ Konqresi 30 noyabr 1993-cü il tarixində qəbul etdiyi qərarla ABŞ Milli Elmlər Akademiyasının Tədqiqatlar üzrə Milli Şurasına (National Research Council) kriptoqrafik texnologiyaları və kriptoqrafiya sahəsində dövlət siyasətini ətraflı analiz etməyi həvalə etdi və əlaqədar dövlət orqanlarına bu işdə Milli Şuraya hərtərəfli dəstək göstərməyi tapşırdı.

Bu tədqiqatda (1) kriptoqrafik texnologiyaların ABŞ hökumətinin milli təhlükəsizliyin təmin edilməsi üzrə maraqlarına, ABŞ hökumətinin hüquq-mühafizə fəaliyyəti maraqlarına, ABŞ sənayesinin kommersiya maraqlarına və ABŞ vətəndaşlarının şəxsi həyatın toxunulmazlığının qorunması maraqlarına təsirini və (2) kriptoqrafik texnologiyaların ixracına nəzarətin ABŞ sənayesinin kommersiya maraqlarına təsirini qiymətləndirmək nəzərdə tutulurdu.

Milli Şuranın hesabatı [4] elm dairələrini, dövlət təşkilatlarını, özəl şirkətləri və bankları təmsil edən mütəxəssislər komitəsi tərəfindən hazırlanmış və mütəxəssislərin başqa bir qrupu tərəfindən isə resenziyadan keçirilmişdi. Komitə kriptoqrafiyanın geniş istifadəsinin faydalarının onun nöqsanlarını üstələdiyi nəticəsinə gələrək, bu sahədə dövlət siyasətinin dəyişməsinə çağırış etdi. Komitənin dövlət kriptoqrafiya siyasəti üzrə tövsiyələrinə aşağıdakılar daxildir:

- Heç bir qanun kriptoqrafiyanın ABŞ hüdudlarında istehsalına, satışına və istifadəsinə maneə yaratmamalıdır.
- Kriptoqrafiya üzrə dövlət siyasəti hakimiyyətin icra və qanunvericilik qolları tərəfindən açıq ictimai müzakirələr əsasında işlənilməli və qanuna riayət edilməsinə əsaslanmalıdır. Kriptoqrafiya üzrə dövlət siyasəti kommersiya kriptoqrafiyasının işlənilməsi və istifadəsində bazarın aparıcı gücləri ilə daha yaxşı razılaşdırılmalıdır.
- Kriptoqrafiyaya dair ixrac məhdudiyyətləri tədricən yumşaldılmalı, lakin tam ləğv edilməməlidir.
- Hökumət hüquq-mühafizə və milli təhlükəsizlik orqanlarının informasiya əsrinin yeni texnoloji reallıqlarına uyğunlaşması üçün tədbirlər görməlidir.
- Hökumət özəl sektorda informasiya təhlükəsizliyinin təmin edilməsi üçün mexanizmlər işləməlidir.

1998-ci ilə kimi ABŞ-da şifrləmə vasitələrinin ölkə daxilində istifadəsinə nəzarət edilmirdi. 1999-cu ildə ixrac məhdudiyyətləri yumşaldıldı, bəzi istisnalarla açarın uzunluğuna məhdudiyyət qoyulmadan şifrləmə vasitələrinin ixracına icazə verilirdi. 2001-ci ilin 11 sentyabr hadisələrindən dərhal sonra bəzi senatorlar hökumətlərə müəyyən nəzarət imkanları verməyən bütün şifrləmə məhsullarının qlobal miqyasda qadağan edilməsini təklif edirdilər.

IV. KRİPTOQRAFİYANIN TƏTBİQİ SAHƏSİNDƏ DÜNYA ÖLKƏLƏRİNİN TƏCRÜBƏSİ

Elektron Gizlilik İnformasiya Mərkəzi (Electronic Privacy Information Center, EPIC) 1998-ci ildə əksər dünya ölkələrində kriptoqrafiya sahəsində milli siyasət və qanunvericiliyin vəziyyəti barəsində hesabat hazırlamışdı [5]. Bu hesabatda ölkələr qəbul etdikləri və həyata keçirdikləri kriptoqrafiyaya nəzarət siyasətinin xarakterindən asılı olaraq yaşıl, sarı və qırmızı rənglə şərti işarələnmiş üç qrupa bölünüb:

- **yaşıl qrup** – kriptoqrafiyanın tətbiqini praktiki olaraq məhdudlaşdırmayan ölkələr;
- **sarı qrup** – ölkə daxilində kriptoqrafiyanın tətbiqi və ikili təyinatlı proqram vasitələrinin ixracına müəyyən nəzarəti həyata keçirmək niyyətində olan ölkələr;
- **qırmızı qrup** – kriptoqrafiyaya və ölkə daxilində onun tətbiqinə nəzarət edən ölkələr.

Hesabatın analizi göstərir ki, hazırda dünya ölkələrinin əksəriyyətində kriptoqrafiyanın tətbiqinə nəzarət yoxdur, informasiyanın kriptoqrafik mühafizəsi vasitələri hər hansı məhdudiyyət olmadan istehsal oluna, istifadə oluna və satıla bilər (yaşıl qrup). Kriptoqrafiya vasitələrinin tətbiqinə ciddi nəzarət edilən qırmızı qrupa Belarus, Çin, İsrail, Pakistan, Rusiya və Sinqapur daxildir. Yeni nəzarət tədbirlərinin tətbiqini nəzərdən keçirən ölkələr ABŞ, Hindistan və Cənubi Koreyadır. Bununla yanaşı, hazırda ABŞ müxtəlif ölkələrdə tətbiq edilən kriptoqrafik açarlara beynəlxalq nəzarətin həyata keçirilməsinə və bu açarların Braziliya, Sinqapur və Cənubi Afrika Respublikası kimi ölkələrə verilməsini təklif edir.

V. KRİPTOQRAFİYA SİYASƏTİNİN ƏSAS PRİNSİPLƏRİ

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (İƏİT) kriptoqrafik mühafizəsi vasitələrindən istifadəyə nəzarətin zəifləməsi ilə bağlı beynəlxalq səviyyədə müşahidə olunan tendensiyaya əsaslanaraq, 1997-ci ildə "Kriptoqrafiya sahəsində siyasətin əsas prinsipləri"ni qəbul etdi [6]. Prinsiplər baxılan məsələdə dövlətin və fərdlərin maraqları arasında kompromis tapmağa yönəlmişdi. Hökumətlərə tövsiyə olunur ki, şəxsi həyatın toxunulmazlığı hüququna hörmətlə yanaşaraq, milli təhlükəsizlik və hüquq-mühafizə orqanlarının maraqlarını nəzərə alaraq, biznes əməliyyatlarını qorumaq üçün də kriptoqrafiyadan istifadəyə kömək etsinlər.

Əsas prinsiplər aşağıdakıları əhatə edir:

1. Kriptoqrafik metodlara etimad. Kriptoqrafik metodlar informasiya və kommunikasiya sistemlərinin istifadəsində etimad yaratmaq üçün etibarlı olmalıdır.

2. Kriptoqrafik metodların seçilməsi. İstifadəçilərin qüvvədə olan qanuna uyğun hər hansı kriptoqrafik metodu seçmək hüququ olmalıdır.

3. Kriptoqrafik metodların istifadəçilərin tələbatı əsasında işlənilməsi. Kriptoqrafik metodlar fərdlərin, biznes sektorunun və dövlətin ehtiyacları, tələbatı və məsuliyyəti əsasında inkişaf etdirilməlidir.

4. Kriptoqrafik metodlar üçün standartlar. Milli və beynəlxalq səviyyədə kriptoqrafik metodlar üçün texniki standartlar, meyarlar və protokollar işlənilməli və qəbul edilməlidir.

5. Şəxsi həyatın toxunulmazlığı və fərdi məlumatların qorunması. Milli kriptoqrafiya siyasətində və kriptoqrafik metodların realizəsi və istifadəsində yazışmaların gizliliyi və fərdi məlumatların qorunması da daxil olmaqla, əsas insan hüquqlarına hörmət edilməlidir.

6. Qanun əsasında giriş. Milli kriptoqrafiya siyasəti qanun əsasında açıq mətnə, kriptoqrafik açarlara və ya şifrlənmiş məlumatlara girişə icazə verə bilər. Belə siyasət bu Prinsiplərdə öz əksini tapan digər prinsiplərə mümkün dərəcədə uyğun olmalıdır.

7. Məsuliyyət. Müqavilə və ya qanunvericiliklə müəyyən edilməsindən asılı olmayaraq, kriptoqrafik xidmətlər təklif edən, kriptoqrafik açarları saxlayan və ya istifadə edən şəxslərin və ya təşkilatların məsuliyyəti aydın ifadə edilməlidir.

8. Beynəlxalq əməkdaşlıq. Hökumətlər kriptoqrafiya siyasətlərini koordinasiya etmək üçün əməkdaşlıq etməlidirlər. Bu əməkdaşlığın bir hissəsi kimi, hökumətlər kriptoqrafiya siyasəti adından ticarətə əsassız maneələr yaradılmasının qarşısını almalı və ya maneələri aradan qaldırmalıdırlar.

VI. KRİPTOQRAFİYA SİYASƏTİNİN ƏSAS İSTİQAMƏTLƏRİ

Kriptoqrafiya sahəsində dövlət siyasətinin əsas strateji məqsədi bu sahədə xarici ölkələrdən texniki və texnoloji asılılığın azaldılması və mümkün olan ən aşağı səviyyədə aradan qaldırılmasıdır.

Aparılan analizin nəticələrinə görə, kriptoqrafiya sahəsində dövlət siyasətinin əsas istiqamətlərini aşağıdakılar təşkil edir:

- kriptoqrafiya sahəsində vahid dövlət siyasətinin və qanunvericilik bazasının təkmilləşdirilməsi;
- e-dövlətdə etimad infrastrukturunun yaradılması;
- kriptoqrafik texnologiyaların işlənməsi sahəsində strateji prioritetlərin müəyyən edilməsi və kriptologiya sahəsində müvafiq prioritet elmi-tədqiqat istiqamətlərinin seçilməsi;
- kriptoqrafiya sahəsində insan resurslarının inkişafı;
- kriptoqrafiya və kriptoanaliz sahəsində qabaqcıl elmi-tədqiqat və layihə-konstruktor işlərinin təşkili;
- kriptoqrafiya sahəsində standartların işlənilməsi;
- kriptoqrafik mühafizə vasitələrinin sertifikatlaş-dırılması sisteminin yaradılması;
- kriptoqrafik texnologiyalar sahəsində beynəlxalq əməkdaşlığın inkişaf etdirilməsi;
- idxal olunan kriptoqrafik avadanlığa və proqram modullarına etimadın qiymətləndirilməsi;
- kriptoqrafik texnologiyalar sahəsində milli istehsalın təşkili.

VII. KRİPTOQRAFİYA SİYASƏTİNİN HƏYATA KEÇİRİLMƏSİ PROBLEMLƏRİ

Kriptoqrafiya sahəsində qanunvericilik bazasının təkmilləşdirilməsi istiqamətində aşağıdakı elmi-praktiki problemlərin araşdırılması və həlli zəruridir:

- informasiyanın kriptoqrafik mühafizəsi vasitələrinin yaradılması və istismarı sahəsində münasibətlərin hüquqi tənzimlənməsi problemləri;
- informasiyanın kriptoqrafik mühafizəsi sahəsində normativ-metodiki bazanın təkmilləşdirilməsi problemləri;
- kriptoqrafiya sahəsində vahid terminoloji bazanın işlənilməsi problemləri;
- elektron sənəd dövriyyəsi və rəqəmsal imza texnologiyası sahəsində münasibətlərin hüquqi tənzimlənməsi problemləri.

E-dövlətdə etimad infrastrukturunun yaradılması üçün aşağıdakı elmi-praktiki problemlərin araşdırılması zəruridir [7]:

- rəqəmsal sertifikatların milli idarəetmə sisteminin inkişafı və qlobal infrastruktura inteqrasiyası;
- rəqəmsal imza sxemlərinin və açıq açarlı kriptoqrafiya alqoritmlərinin yaradılması və milli kriptoqrafik məhsullarda istifadə edilməsi.

İdxal olunan kriptoqrafik avadanlığa və proqram modullarına etimadın qiymətləndirilməsi olduqca vacibdir [8]. Xarici kriptoqrafik mühafizə vasitələrinin yerinə yetirilən funksiyalara və təmin edilən təhlükəsizlik səviyyəsinə uyğunluğu lazımi qaydada analiz edilmədən kritik infrastruktur sistemlərində istifadəsi yolverilməzdir. Xarici təşkilatların sertifikatları milli sertifikatları heç cür əvəz edə bilməz. Bəzi müəlliflər istismar olunan kriptoqrafik avadanlıqda təhlükəsizliyi aşağı salan və kriptoanalizi asanlaşdıran aşağıdakı üsullardan istifadə edildiyini iddia edirlər [3,9]:

- açarın bitləri vaxtaşırı olaraq, şifrmətnə qarışdırılır;
- açar rəsmən elan olunmuş uzunluqdan əhəmiyyətli dərəcədə qısa olur (məsələn, 100 bit əvəzinə 30 bit);
- şifrlənən hər bir məlumatın əvvəlinə sabit başlıq qoyulur ki, açıq mətni bilməklə kriptoanalitik hücum asanlaşsın;
- istənilən şifrlənmiş məlumat müəyyən açıq mətn və ona uyğun şifrmətn fraqmentinə malik olur.

Buna görə kriptoqrafik mühafizə vasitələrinin sertifikatlaşdırılmasının milli sisteminin yaradılması olduqca vacibdir. Bu istiqamətdə əsas problem xüsusi laboratoriyaların yaradılmasıdır.

VIII. NƏTICƏ

Kriptoqrafiya uzun müddət yalnız dövlət maraqları üçün istifadə olunurdu, buna görə də qapalı elm sahəsi idi. Son dövrlər vəziyyət köklü surətdə dəyişməkdədir. İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı, onların praktik olaraq insan fəaliyyətinin bütün sahələrinə nüfuz etməsi dövlətin, təşkilatların və vətəndaşların informasiya təhlükəsizliyinin təmin olunmasında kriptoqrafiyanın istifadəsinə yol açır. Kriptoqrafiyanın tətbiq sahələrinin genişlənməsi ilə əlaqədar olaraq (rəqəmsal imza, autentikasiya, elektron sənədlərin həqiqiliyinin və tamlığının təsdiqi, elektron kommersiyanın təhlükəsizliyi, İnternet vasitəsilə ötürülən informasiyanın mühafizəsi və s.) müasir cəmiyyətin həyatında kriptoqrafiyanın rolu artır.

Vətəndaşların və biznes sektorunun, beynəlxalq tərəfdaşların e-dövlətin informasiya təhlükəsizliyinə etimadını təmin etmək üçün müasir telekommunikasiya şəbəkələrinə xas olan xüsusiyyətləri, qlobal informasiya fəzasında sərhədlərin müəyyən edilməsi və qorunmasındakı çətinlikləri nəzərə alaraq, müvafiq insan hüquq və azadlıqları qorumaqla, elm, biznes, hüquq-mühafizə və müdafiə orqanları cəlb edilərək kriptoqrafiya sahəsində düzgün, balanslaşdırılmış siyasətin işlənilməsi olduqca vacibdir.

ƏDƏBIYYAT

[1] R.M. Əliquliyev, Y. N. İmamverdiyev “Rəqəmsal imza texnologiyası.” Bakı: Elm, 2003, 132 s.

[2] R.M. Əliquliyev, Y. N. İmamverdiyev “Kriptoqrafiya tarixi.” Bakı: İnformasiya Texnologiyaları, 2006, 192 s.

[3] R.M. Əliquliyev, Y. N. İmamverdiyev “Kriptoqrafiyanın əsasları.” Bakı: İnformasiya Texnologiyaları, 2006, 698 s.

[4] K. W. Dam, H. S. Lin, Cryptography's role in securing the information society. Washington, DC: National Academy of Sciences, 1996, 688 p.

[5] Global Internet Liberty Campaign. An International Survey of Encryption Policy.1998. http://gilc.org/crypto/crypto-survey.html

[6] OECD Guidelines for Cryptography Policy, 1997.

[7] Я. Н. Имамвердиев, М. Ш. Гаджирагимова “Архитектура инфраструктуры доверия электронным документам в среде электронного государства,” Телекоммуникации, 2011, № 11, С. 18-26.

[8] З. М. Ахадова “Актуальные вопросы совершенствования стандарта FIPS 140-2,” Вопросы защиты информации, 2006, N 4, С. 6-11.

[9] Y. N. Imamverdiyev “QOST-28147-89 standartında əvəzetmə bloklarının generasiyası,” 3-cü Beynəlxalq elmi-praktiki konfrans “İnformasiya texnologiyaları və telekommunikasiya (IT&TC), 2007.