UOT 004.9:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

İNFORMASİYA CƏMİYYƏTİNDƏ MİLLİ KRİPTOQRAFİYA SİYASƏTİNİN FORMALAŞDIRILMASI PROBLEMLƏRİ

İnformasiya cəmiyyətində informasiya təhlükəsizliyinin təmin edilməsinin texnoloji komponentlərinin reallaşdırılmasında kriptoqrafiya metodları mühüm rol oynayır. Bu tədqiqat işində informasiya cəmiyyətində milli kriptoqrafiya siyasətinin formalaşdırılması və həyata keçirilməsi problemləri analiz edilir, inkişaf etmiş ölkələrin bu sahədə təcrübəsi araşdırılır, kriptoqrafiya üzrə açıq beynəlxalq müsabiqələrin təcrübəsi əsasında kriptoqrafiya sahəsində elmi tədqiqatların müasir vəziyyəti 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**: informasiya cəmiyyəti; informasiya təhlükəsizliyi; kriptoqrafiya; kriptoanaliz; kriptoqrafiya siyasəti.*

Giriş

İnformasiya cəmiyyətində 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, informasiya cəmiyyətində açıq açarlı kriptoqrafiya əsasında etimad infrastrukturu formalaşdırılır, informasiya cəmiyyətinin 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.

İnformasiya cəmiyyətində 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 və kadr potensialı yoxdur, müvafiq elmi-tədqiqatlar aparılmır 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, informasiya cəmiyyəti 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 fəaliyyəti çərçivəsində effektiv həll edilməsi üçün kriptoqrafiya sahəsində müvafiq dövlət siyasətinin formalaşdırılması vacibdir.

Təqdim olunan tədqiqat işində informasiya cəmiyyətində kriptoqrafiya üzrə siyasətin formalaşdırılması problemləri analiz edilir, bu sahədə beynəlxalq təcrübə araşdırılır, dövlət siyasətinin əsas istiqamətləri üzrə bir sıra tövsiyələr təklif edilir.

Məqalənin sonrakı strukturu belədir: əvvəlcə kriptoqrafiya, onun funksiyaları və inkişaf mərhələləri haqqında çox qısa məlumat verilir, digər ölkələrin kriptoqrafiya siyasətinin formalaşmasına da böyük təsir göstərən ABŞ-ın kriptoqrafiya siyasətinin formalaşması və həyata keçirilməsi təcrübəsi analiz edilir, dünya ölkələrində kriptoqrafiyanın istifadəsi siyasətinə nəzər salınır və beynəlxalq təşkilatlarda formalaşmış kriptoqrafiya siyasətinin əsas prinsipləri təhlil olunur. Kriptoqrafiyanın yayılmasında müstəsna rol oynamış açıq kodlu proqram təminatının iki qabaqcıl nümayəndəsi haqqında məlumat verilir. Daha sonra, aparılmış təhlil nəticəsində inkişaf etməkdə olan ölkələr üçün model kriptoqrafiya siyasətinin əsas istiqamətləri identifikasiya edilir və onların həyata keçirilməsi üçün həlli vacib elmi-praktiki problemlər müəyyən edilir, uyğun mexanizmlər və tövsiyələr təklif edilir.

Kriptoqrafiya haqqında qısa arayış

"Kriptoqrafiya" sözü yunan dilindəki κρυπτός (kryptos) – "gizli" və γραφω (grapho) – "yazı" sözlərinin birləşməsindən 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, ilk növbədə, 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. 1989-cu ildə SSRİ-də verilənlərin kompüter şəbəkələrində şifrlənməsi üçün *QOST 28147-89* dövlət standartı qəbul olundu. Təxminən həmin ildə *DES* alqoritminin alternativi olaraq Yaponiyada verilənlərin şifrlənməsi standartının layihəsi təklif olundu (*FEAL* şifri). 1990-cı ildə K.Ley və C.Messi (İsveçrə) verilənlərin şifrlənməsi üzrə beynəlxalq standartın layihəsini irəli sürdülər (*International Data Encryption Algorithm, IDEA*). Həmin il Avstraliyada da *LOKI* adlanan şifrləmə standartının layihəsi dərc olundu. 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 əvəzinə 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.

ABŞ-ın kriptoqrafiya siyasəti

ABŞ informasiya-kommunikasiya texnologiyaları (İKT) ilə yanaşı, kriptoqrafiya və kriptoanaliz sahəsində də dünyada lider mövqeyindədir. Bu ölkənin kriptoqrafiya siyasəti bir sıra dövlətlərin, xüsusilə də, Vaasenaar sazişini (1996-cı ildə Hollandiyanın eyni adlı şəhərində 33 ölkə tərəfindən imzalanan bu razılaşma adi silahların, məhsulların və ikili təyinatlı texnologiyaların ötürülməsi zamanı məsuliyyətin gücləndirlməsini nəzərdə tuturdu) imzalayan dövlətlərin kriptoqrafiya siyasətinin formalaşmasına kritik təsir etmişdir. Buna görə də ABŞ-ın kriptoqrafiya siyasətinin formalaşması proseslərini analiz etmək bu məqalədə qarşıya qoyulan məsələnin həlli üçün vacibdir. Qeyd edək ki, ABŞ-ın kriptoqrafiya siyasətinin formalaşması prosesləri 1990-cı illərdə xüsusilə dramatik şəkil almışdı [4].

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 (*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, açarın uzunluğu 40-bitdən kiçik olan şifrləmə vasitələrinin ixracına icazə verilirdi.

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. Mübarizədə birinci tərəfin əsas arqumentləri milli təhlükəsizlik, kriptoqrafik vasitələrin terrorçular və cinayətkarlar tərəfindən istifadəsi təhlükəsi və hüquq-mühafizə orqanlarının işinin çətinləşəcəyi idi. Mübarizədə ikinci tərəfi hüquq müdafiəçiləri, ABŞ kompüter texnikası və rabitə texnikası istehsalçıları və e-kommersiya şirkətləri təşkil edirdi. Onların arqumentləri milli təhlükəsizliyin təkcə dövlət sirrini qorumaqdan ibarət olmadığı, ABŞ şirkətlərinin sənaye casusluğundan qorunmasının və bank sirlərinin konfidensiallığının təmin edilməsinin də milli təhlükəsizlik məsələsi olduğu, ABŞ şirkətlərinin bu məhdudiyyətlər ucbatından yüz milyonlarla dollar itirdiyi, kriminal elementlərin yüksək keyfiyyətli kriptoqrafik vasitələri dünyanın digər ölkələrindən əldə edə biləcəkləri, ABŞ-ın iqtisadi liderliyi itirməsi və s. idi.

Vətəndaş hüquq və azadlıqlarının müdafiəçiləri və İnternet şəbəkəsinin istifadəçiləri isə bu və ya digər kriptoqrafik sistemdən öz seçimi ilə istifadə hüququnun və azadlığının pozulmasına etiraz edirdilər. 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 *NSA* 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 çıxartdı. 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 (*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 həyata keçirmək üçün 1992-ci ildə *Clipper* təşəbbüsü irəli sürüldü. *Clipper* kriptoçipinin telefonlarda, fakslarda və elektron poçtda şifrləmə zamanı istifadə edilməsi nəzərdə tutulurdu. Tezliklə mütəxəssislər təklif edilən sistemdə zəif yerlər tapdılar, bu həmin sistemə inamı azaldır və onun tətbiqini praktiki olaraq qeyri-mümkün edirdi. Hökumət *Clipper*-in istifadəsinin könüllü olacağını bəyan etmişdi, lakin ictimaiyyətin reaksiyası hökumətin gözlədiyinin əksinə oldu. Nəticədə, dəstək qazana bilməyən hökumət bu təşəbbüsdən imtina etməyə 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 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 kriptoqrafik texnologiyaların ixracına nəzarətin ABŞ sənayesinin kommersiya maraqlarına təsirini qiymətləndirmək nəzərdə tutulurdu.

Milli Şuranın hesabatı elm dairələrini, dövlət təşkilatlarını, özəl şirkətləri və bankları təmsil edən mütəxəssislər komitəsi tərəfindən hazırlanmış və mütəxəssislərin başqa bir qrupu tərəfindən isə ekspertizadan keçirilmişdi [5]. Komitə kriptoqrafiyanın geniş istifadəsinin faydalarının onun nöqsanlarını üstələdiyi nəticəsinə gələrək, bu sahədə dövlət siyasətinin dəyişməsinə çağırmışdır. 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. "Hamının etibar etdiyi üçüncü tərəf" rolunu Etibarlı kompüter platforması Alyansının (*Trusted Computing Platform Alliance, TCPA*) qurucuları olan *Intel, Microsoft, IBM, HP-Compaq* və *AMD* öz üzərlərinə götürməyi qərara aldı (2004-cü ildən *Trusted Computing Group (TCG)* adlanır).

Kriptoqrafik-çip ideyası başqa məzmunda və başqa oyunçularla yenidən gündəmə gəldi. *TCPA* alyansı "etibarlı platforma modulu" adlanan (*Trusted Platform Module, TPM*) texnologiyanın spesifikasiyasını hazırladı [6]. *TPM* kriptoqrafik açarlardan istifadə etməklə əsas informasiya təhlükəsizliyi funksiyalarını reallaşdırmağa xidmət edən mikrokontrollerdir (onu rəqəmsal müəlliflik hüquqlarını dəstəkləməsi ilə məşhur olan keçmiş senator Ernest "Frits" Hollinqsin şərəfinə "Frits-çip" də adlandırırlar). *TPM* çipi kompüterin ana platasına quraşdırılır və sistemin digər komponentləri ilə sistem şini vasitəsilə qarşılıqlı əlaqədə olur. Bəzi müəlliflər iddia edirlər ki, *TPM* əsasında hazırlanmış "təhlükəsizlik qurğusu" istifadəçinin öz kompüteri üzərində nəzarətini məhdudlaşdırır və kompüterdə yerinə yetirilən işlərin məsafədən izlənməsini asanlaşdırır [7].

Kiptoqrafiyanın tətbiqi sahəsində dünya ölkələrinin təcrübəsi

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 [8]. 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 edilə 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 keçirilməsini və bu açarların Braziliya, Sinqapur və Cənubi Afrika Respublikası kimi ölkələrə verilməsini təklif edir.

Kriptoqrafiya siyasətinin əsas prinsipləri

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (İƏİT) kriptoqrafik mühafizə vasitələrindən istifadəyə nəzarətin zəifləməsi ilə bağlı beynəlxalq səviyyədə müşahidə edilən tendensiyaya əsaslanaraq, 1997-ci ildə "Kriptoqrafiya sahəsində siyasətin əsas prinsipləri"ni qəbul etdi [9]. Prinsiplər baxılan məsələdə dövlətin və fərdlərin maraqları arasında kompromis tapmağa yönəlmişdi. Hökumətlərə tövsiyə olunurdu 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 reallaşdırılması 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 şəkildə 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.

Qeyd edək ki, ABŞ bir sıra ölkələrə və İƏİT də daxil olmaqla, beynəlxalq təşkilatlara açarların depoziti ideyasını qəbul etdirmək üçün təzyiqlər göstərirdi. Lakin İƏİT ölkələri kriptoqrafiyanın məhdudlaşdırılması əleyhinə çıxırdılar və 6-cı prinsip (qanun əsasında açarların əldə edilməsi) ölkələr arasında müəyyən kompromisin nəticəsidir.

Kriptoqrafiya sahəsində nəzarətin yumşaldılmasını nəzərdə tutan "Kriptoqrafiya sahəsində siyasətin əsas prinsipləri" tövsiyə xarakteri daşıyır. Bir sıra dövlətlər 1997-ci ildən bu prinsiplərə əməl edirlər. Məsələn, Belçika, Almaniya, İrlandiya, Kanada və Finlandiya bəyan etmişdilər ki, onların kriptoqrafiya sahəsində milli siyasətləri məhz bu prinsiplərə əsaslanacaq [10]. Aparıcı Qərb dövlətlərindən yalnız Böyük Britaniya kriptoqrafiya üzərində müəyyən nəzarət tədbirlərini həyata keçirməkdə davam edir [11].

Kiptoqrafiya üzrə açıq kodlu proqram təminatı

Kriptoqrafik metodları proqram və aparat təminatında reallaşdırmaq olar. Kriptoqrafik metodların aparat təminatında reallaşdırılması bir sıra üstünlüklərə malikdir (kriptoqrafik alqoritmlərin dəyişməzliyinə zəmanət, açarların generasiyası və saxlanması, sürət və s.) və onların istifadəsi miqyası genişlənir (mobil rabitə, kommersiya televiziyası, Əşyaların İnterneti, müşahidə videokameraları və müxtəlif siqnalizasiya qurğuları bunu tələb edir) [12]. Praktiki kriptoqrafiyanın aktual problemlərindən biri ucuz mikroelektron sxemlər – kriptoçiplər şəklində realizə edildikdə 1500 Mbit/san.-dən böyük şifrləmə sürəti təmin edən alqoritmlərin qurulmasıdır.

İstənilən kriptoqrafik alqoritmi proqram təminatı şəklində reallaşdırmaq olar. Belə reallaşdırmanın da bir çox üstünlükləri vardır: kriptoqrafik proqram təminatının əlavə nüsxəsini (surətini) yaratmaq asandır, istifadəsi çətin deyil, konkret tələblərə uyğun olaraq onları asanlıqla modifikasiya etmək olar və s. Qeyd edək ki, geniş yayılmış bütün əməliyyat sistemlərində faylları şifrləmə vasitələri vardır; bundan əlavə, informasiyanın icazəsiz girişlərdən və dəyişikliklərdən müdafiəsi funksiyaları da mövcuddur ki, onları da kriptoqrafik alqoritmlər vasitəsilə reallaşdırırlar.

Açıq kodlu kriptoqrafik proqram təminatı kriptoqrafiyanın geniş yayılmasında mühüm rol oynamışdır. Kriptoqrafiyanın yayılmasının qarşısını almağa çalışan dövlətlərə qarşı ən kəsərli mübarizənin açıq kodlu proqram təminatı yaratmaq və onu İnternet vasitəsilə yaymaq olduğunu düşünən amerikalı proqramçı Filip Zimmerman 1991-ci ildə *PGP* (*Pretty Good Privacy, Mükəmməl Gizlilik*) adı verdiyi kriptoqrafik kitabxanasını yaratdı və kitabxana əvvəlcə *Usenet*-də, sonra isə İnternetdə sürətlə yayılmağa başladı.

PGP kriptoqrafik proqram kitabxanası gizli və açıq açarların generasiyası funksiyasını, məlumatları, faylları və elektron şəkildə olan informasiyanı şifrləmə və rəqəmsal imzalama funksiyalarını həyata keçirməyə imkan verirdi. 1993-cü ildə ABŞ hökuməti *PGP* müəllifi F.Zimmermana qarşı məhkəmədə ixrac məhdudiyyətini pozmaq iddiası qaldırmışdı, çünki qanun

açarın uzunluğu 40 bitdən böyük olan istənilən kriptoqrafik həllin ixracını qadağan edirdi. *PGP*-də isə 128 bit və daha uzun açarlar istifadə edilirdi. Zimmerman proqramın bütün ilkin kodunu *MIT Press* tərəfindən nəşr edilmiş kitabda göstərməklə ixrac məhdudiyyətindən yan keçə bilmişdi [13]. Kitabın ixracı ABŞ Konstitusiyasında söz azadlığına təminat verən birinci düzəlişə görə qadağan oluna bilməz. Arzu edən istənilən şəxs kodu skanerdən keçirə və tanıma proqramları ilə mətni bərpa edə bilərdi. 1996-cı ildə məşhur kriptoqraf Bryus Şnayer *PGP*-ni "hərbi kriptosistemlərə yaxın" sistem kimi xarakterizə etmişdi. Hazırda *PGP*-nin *OpenPGP* (*RFC* 4880) standartı əsasında bir sıra əməliyyat sistemləri üçün realizə olunmuş həm pulsuz yayılan, həm də kommersiya variantları mövcuddur.

OpenSSL açıq kodlu, pulsuz kriptoqrafik prosedurlar kitabxanası barəsində də qeyd etmək lazımdır. 1999-cu ildən istifadəçilərə təqdim olunan *OpenSSL* kriptoqrafik metodların populyarlaşdırılması üçün böyük işlər görmüşdür (müəllifləri Erik Yanq və Tim Hadsondur). *OpenSSL*-də praktiki olaraq bütün müasir kriptoqrafik alqoritmlərin yaxşı sazlanmış ilkin kodları var. İlkin kodların açıq olması əlfəcinlər və gizli əl yerləri haqqında sonsuz mübahisələrə son qoyulur – ilkin kodları istənilən şəxs analiz edə bilər. Proqram kodlarının açıq nəşr olunmasına kifayət qədər mürəkkəb olan kriptoqrafik alqoritmlərin proqram realizələrində hər hansı kritik səhvin olmamasına zəmanət kimi baxılır, ümid edilir ki, bu proqram təminatı milyonlarla istifadəçi tərəfindən test edilir və buraxılmış səhvlərin aşkarlanması və aradan qaldırılması ehtimalı böyükdür.

Kriptoqrafiya sahəsində siyasətin əsas istiqamətləri

Mövcud tədqiqat işlərində "kriptoqrafiya siyasəti" anlayışı "kriptoqrafiyanın tətbiqi siyasəti" anlayışı ilə eyniləşdirilir. Bu anlayışın məzmununu isə kriptoqrafik məhsulların idxalı, ixracı və tətbiqi məsələləri təşkil edir. Kriptoqrafik məhsulların istehsalı və sertifikatlaşdırılması məsələləri, uyğun elmi tədqiqatların və elmi-praktiki işlərin təşkili və maliyyələşdirilməsi, müvafiq elmi kadrların hazırlanması məsələləri nəzərə alınmır. Zənnimizcə, sadalanan bu məsələləri də nəzərə almaqla kriptoqrafiya siyasəti anlayışına daha geniş miqyasda baxmaq zəruridir. Eyni zamanda, nəzərə almaq lazımdır ki, kriptoqrafiya siyasəti milli informasiya təhlükəsizliyi siyasətinin tərkib hissəsidir.

İnformasiya cəmiyyətində tərəfdaşlar arasında təhlükəsiz kommunikasiyanı, e-xidmətlərin təhlükəsizliyini və e-kommersiya tranzaksiyalarının təhlükəsizliyini təmin edən, beynəlxalq sazişlər çərçivəsində kriptoqrafik məhsulların ixracına və idxalına imkan yaradan, hüquq-mühafizə orqanlarının milli və ictimai təhlükəsizliyi təmin edəcək potensialını dəstəkləyən kriptoqrafiya siyasəti həyata keçirilməlidir. Digər texnologiyalar kimi kriptoqrafiyanın da həm müsbət, həm də mənfi cəhətləri var və bu heç zaman dəyişməyəcək – kriptoqrafiya siyasəti e-kommersiya tranzaksiyalarını qorumaq üçün güclü kriptoqrafiya tələbatı ilə cinayət və terror şübhəlilərini izləmək ehtiyacı, şəxsi həyatın toxunulmazlığı və fərdi məlumatların konfidensiallığı hüquqları arasında düzgün balansı da təmin etməlidir.

Kriptoqrafiya sahəsində dövlət siyasətinin əsas strateji hədəfi 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;
- kriptoqrafik texnologiyaların işlənməsi sahəsində strateji prioritetlərin müəyyən edilməsi və kriptologiya sahəsində müvafiq prioritet elmi-tədqiqat istiqamətlərinin seçilməsi;
- informasiya cəmiyyətində e-imza texnologiyaları əsasında etimad infrastrukturunun yaradılması;
- kriptoqrafiya sahəsində insan resurslarının inkişafı;

- kriptoqrafiya və kriptoanaliz sahəsində qabaqcıl elmi-tədqiqat və layihə-konstruktor işlərinin təşkili və həyata keçirilməsi;
- kriptoqrafiya sahəsində standartların işlənilməsi;
- kriptoqrafik mühafizə vasitələrinin sertifikatlaşdırılması sisteminin yaradılması;
- kriptoqrafik texnologiyalar sahəsində beynəlxalq əməkdaşlığın inkişaf etdirilməsi;
- idxal olunan kriptoqrafik avadanlığa və proqram modullarına etimadın qiymətləndirilməsi;
- kriptoqrafik texnologiyalar sahəsində milli istehsalın təşkili.

Əksər dövlətlərdə kriptoqrafik mühafizə 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.

Kriptoqrafiya siyasətinin həyata keçirilməsi problemləri

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, rəqəmsal imza texnologiyası və əl imzasının digər analoqlarının istifadəsi sahəsində münasibətlərin hüquqi tənzimlənməsi problemləri [14].

İnformasiya cəmiyyətində etimad infrastrukturunun yaradılması üçün aşağıdakı elmi-praktiki problemlərin araşdırılması zəruridir [15]:

- 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 [16]. 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, 17]:

- 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 ixtisaslaşdırılmış xüsusi laboratoriyaların yaradılması və kriptoanaliz sahəsində yüksək keyfiyyətli qabaqcıl elmi-tədqiqatların aparılması ilə bağlıdır.

Kriptoqrafik sistemlərin tam təhlükəsiz olmasını sübut etmək üçün bir sıra geniş yayılmış hücumlar, o cümlədən baxılan sinif alqoritmlər üçün olan hücumlara qarşı dözümü sübut

olunmalıdır. Qeyd etmək lazımdır ki, son bir neçə onillikdə (daha doğrusu, 1975-ci ildə *DES* standartının nəşrindən sonra) kripto-analiz üsulları geniş inkişaf edib, mühəndis analizi üsulları meydana çıxıb, yüksək məhsuldarlıqlı hesablamalar inkişaf edib. Buna görə, tam davamlı kriptoqrafik sistem icad edildiyini iddia etmək asan, onun, doğrudan da, təhlükəsiz olduğunu sübut etmək isə olduqca çətindir. Hollandiyalı alim Oqust Kerxoffun hələ 1863-cü ildə nəşr etditdiyi "Hərbi kriptoqrafiya" kitabında verilmiş bir fikrə istinad yerinə düşərdi: "Bəzi şifrlərə belə hədsiz inamı yalnız şifrləmə işi sahəsində elmi tədqiqatların yetərsizliyi ilə izah etmək olar..." [2].

Kriptoqrafik sistemlərin təhlükəsizliyi haqqında bu sistemlərin müəllifləri deyil, yalnız mütəxəssis kriptoanalitiklər qərar verməlidirlər. Kriptoqrafik sistemlərin ekspertizası uzunmüddətli prosesdir, çox vaxt hər biri kriptoanalizin bir sahəsində ixtisaslaşan yüzlərlə mütəxəssis cəlb edilməklə həyata keçirilir.

Kriptoqrafiya və kriptoanaliz sahəsində qabaqcıl elmi-tədqiqatlar sahəsində aşağıdakı aktual elmi-praktiki problemləri xüsusilə fərqləndirmək lazımdır:

- nəzəri kriptoqrafiyanın və riyaziyyatın əlaqədar sahələrinin fundamental problemləri;
- simmetrik şifrləmə alqoritmlərinin, açıq açarlı şifrləmə alqoritmlərinin və heş funksiyaların işlənməsi problemləri;
- kriptoqrafik mühafizə vasitələrində istifadə edilən kriptoqrafik alqoritmlərin və protokolların analizi problemləri;
- kritik vacib informasiya sistemlərində elektron sənəd dövriyyəsinin təhlükəsizliyinin təmin edilməsi üçün kriptoqrafik protokolların işlənməsi problemləri;
- kriptoqrafiya və kriptoanaliz məsələlərinin həlli üçün yüksək məhsuldarlıqlı hesablama sistemlərinin, alqoritmik və proqram təminatının qurulması problemləri.

Kriptoqrafiya sahəsində elmi-tədqiqatların aktual istiqamətləri

Müasir kriptoqrafiyada dörd böyük tədqiqat istiqaməti formalaşıb: 1) simmetrik kriptosistemlər; 2) açıq açarlı (asimmetrik) kriptosistemlər; 3) elektron imza sistemləri; 4) açarların idarə edilməsi.

Simmetrik kriptosistemlər sahəsində tədqiqatların əsas istiqamətləri blok şifri primitivləri, axın şifri primitivləri, məlumatı autentifikasiya kodu primitivləri, heş funksiya primitivləri, əməliyyat rejimləri və simmetrik kriptoqrafik primitivlərin istifadəsi, simmetrik üsullar və psevdo-təsadüfi funksiyalar daxil olmaqla, onların nəzəri əsaslarının işlənməsidir.

Kriptoqrafiya sahəsində elmi-tədqiqatların hazırki vəziyyətini qiymətləndirmək üçün Kriptologiya Tədqiqatları üzrə Beynəlxalq Assosiasiyanın (*The International Association for Cryptologic Research, IACR*) təşkil etdiyi *Eurocrypt, CRYPTO, Asiacrypt* kimi konfransların və bir çox seminarların təcrübəsini izləmək faydalıdır. Assosiasiyanın www.iacr.org veb-saytından konfransların və seminarların əsərlərinə çıxış imkanı vardır.

Kriptoqrafiya sahəsində keçirilən açıq müsabiqələr tədqiqatların inkişafına xüsusi stimul vermişdir. Məxfi açarlı kriptoqrafiyada müsabiqələrin müəyyən ənənəsi artıq formalaşıb. 1997-ci ildə ABŞ Milli Standartlar və Texnologiyalar İnstitutu (*National Institute of Standards and Technology, NIST*) yeni şifrləmə standartını (*Advanced Encryption Standard, AES*) müəyyən etmək üçün açıq müsabiqə elan etmişdi. Müsabiqəyə dünyanın müxtəlif ölkələrindən olan 50 kriptoqraf tərəfindən 15 blok şifri təqdim olunmuşdu. Müsabiqə bir neçə mərhələdə keçirilmiş, burada təqdim olunmuş blok şifrlərin təhlükəsizliyi və məhsuldarlığı çox sayda kriptoqraf tərəfindən qiymətləndirilmişdi.

AES-in uğurları nəzərə alınaraq, Avropa İttifaqı 2000-2003-cü illərdə *NESSIE* (*New European Schemes for Signatures, Integrity and Encryption*) müsabiqəsini keçirdi, Yaponiya isə 2003-cü ildə *CRYPTREC* (*Cryptography Research and Evaluation Committees*) komitəsini yaratdı.

ECRYPT şəbəkəsi 2004-cü ilin fevralında başladılmış 4 illik Avropa tədqiqat təşəbbüsü idi, məqsədi informasiya təhlükəsizliyi, xüsusən də kriptologiya və rəqəmsal su nişanları sahəsində Avropa tədqiqatçıları arasında əməkdaşlığı inkişaf etdirmək idi. 2008-ci ildə növbəti 4 illik mərhələ *ECRYPT* II adı ilə davam etdirildi. *ECRYPT* virtual laboratoriya adlandırılan beş əsas tədqiqat sahəsi müəyyən edir – simmetrik açarlı alqoritmlər (*STVL*), açıq açarlı alqoritmlər, protokollar (*PROVILAB*), təhlükəsiz və effektiv realizələr (*VAMPIRE*) və su nişanları (*WAVILA*).

ECRYPT çərçivəsində həyata keçirilmiş ən uğurlu layihələrdən biri axın şifr standartlarının müəyyən edilməsini hədəfləyən *eSTREAM* layihəsi idi (2004-2008-ci illər).

Kriptoqrafik müsabiqələrdən ABŞ-ın *SHA-3* kriptoqrafik heş funksiya standartının seçilməsi üzrə layihəni (*NIST*, 2007-2012-ci illər) və *CAESAR* (*Competition for Authenticated Encryption: Security, Applicability, and Robustness*, Avtomatlaşdırılmış Şifrələmə Müsabiqəsi: təhlükəsizlik, tətbiq və etibarlılıq) layihəsini qeyd etmək olar (2012-ci ildən, *NIST* qrantı ilə maliyyələşir).

Avropa İttifaqının "Horizon 2020" Layihəsi çərçivəsində *ICT 2014 – Information and Communications Technologies* (*H2020-ICT-2014-1*) aşağıdakı aktual tədqiqat problemləri müəyyən edir [18]:

- aparat əsasında real zamanda işləyən kriptoqrafiya üçün resurs baxımından səmərəli, yüksək səviyyədə təhlükəsiz texnologiyalar;
- resurs baxımından səmərəli, real zamanda işləyən, yüksək səviyyədə təhlükəsiz tam homomorf kriptoqrafiya;
- paylanmış kriptoqrafiya, o cümlədən funksional kriptoqrafiya;
- istifadə olunan kriptoqrafik primitivlərin uyğunlaşmaq imkanı olmaqla və ya olmadan proqram və aparat mühitlərinə təhlükəsiz qoşulması üçün kriptoqrafik alətlər;
- uzunmüddətli təhlükəsizlik üçün post-kvant kriptoqrafiyası;
- uzunmüddətli təhlükəsizlik üçün kvant açar paylaşımı sistemləri və şəbəkələri, o cümlədən:
    - qısa məsafəli, aşağı bit sürətli kvant açar paylaşımı üçün ucuz komponentlər;
    - küy və itkilərə dayanıqlı yüksək bit sürətli kvant açar paylaşımı sistemləri.

Homomorf şifrləmə sistemi şifrlənmiş məlumatlar üzərində məlumatları deşifrləmədən riyazi əməliyyatlar (məsələn, toplama, çıxma, birləşmə, kəsişmə) aparmağa imkan verir. Bu fərdi məlumatların qorunması, elektron səsvermə, maliyyə məlumatlarının emalı, tövsiyə sistemlərində tətbiq edilə bilər.

Nəticə

Kriptoqrafiya uzun müddət yalnız dövlət maraqları üçün istifadə olunurdu, buna görə də qapalı elm sahəsi idi. Son dövrlər vəziyyət köklü surətdə dəyişməkdədir. İKT-nin sürətli inkişafı, praktiki 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, autentifikasiya, 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 informasiya cəmiyyətinin 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. Əliquliyev R. M., İmamverdiyev Y. N. Rəqəmsal imza texnologiyası. Bakı: Elm, 2003, 132s.
2. Əliquliyev R. M., İmamverdiyev Y. N. Kriptoqrafiya tarixi. Bakı: İnformasiya Texnologiyaları, 2006, 192 s.
3. Əliquliyev R. M., İmamverdiyev Y. N. Kriptoqrafiyanın əsasları. Bakı: İnformasiya Texnologiyaları, 2006, 698 s.
4. Diffie W., LandauS. The Export of Cryptography in the 20th and the 21st Centuries. Karl de Leeuw, Jan Bergstra, ed. The history of information security. A comprehensive handbook. Elsevier, 2007, pp. 725-737.
5. Dam K.W., Lin H.S. Cryptography's role in securing the information society. Washington, DC: National Academy of Sciences, 1996, pp. 1-688.
6. Gallery E., Mitchell C.J. Trusted Computing: Security and Applications // Cryptologia, 2008, Vol. 33, No. 3, pp. 217-245.
7. Green L. Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers. 2002, https://www.cypherpunks.to/TCPA_DEFCON_10.pdf
8. Global Internet Liberty Campaign. An International Survey of Encryption Policy.1998, http://gilc.org/crypto/crypto-survey.html
9. OECD Guidelines for Cryptography Policy, 1997, http://www.oecd.org
10. Government of Canada: A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society, 1998, 42 p., http://www.strategis.ic.gc.ca/crypto
11. Herson D. The changing face of international cryptography policy Part 2 — The United Kingdom // Computer Fraud & Security, 1999, Vol. 1999, No. 7, pp. 10–11.
12. İmamverdiyev Y.N., Kang T.W. Əşyaların İnterneti üçün yüngülçəkili kriptoqrafiya / Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı"nın materialları, 2013, s. 137-140.
13. Zimmermann Ph. PGP Source Code and Internals. MIT Press. 1995, 933 p.
14. Imamverdiyev Y.N., Teoh A.B.J., Kim J. Biometric cryptosystem based on discretized fingerprint texture descriptors // Expert Systems with Applications, 2013, .vol. 40, no. 5, pp. 1888–1901.
15. Имамвердиев Я. Н., Гаджирагимова М. Ш. Архитектура инфраструктуры доверия электронным документам в среде электронного государства // Телекоммуникации, 2011, № 11, с. 18-26.
16. Ахадова З. М. Актуальные вопросы совершенствования стандарта FIPS 140-2 // Вопросы защиты информации, 2006, N 4, с. 6-11.
17. İmamverdiyev Y. N. QOST-28147-89 standartında əvəzetmə bloklarının generasiyası / "İnformasiya texnologiyaları və telekommunikasiya" (IT&TC'2007), 3-cü Beynəlxalq elmi-praktiki konfrans, 2007.
18. Information and Communications Technologies (H2020-ICT-2014-1), Topic: Cybersecurity, Trustworthy ICT (ICT-32-2014), http://www.ec.europa.eu

УДК 004.9:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Проблемы формирования национальной политики информационного общества в области криптографии

Криптографические методы защиты информации играют важную роль в технологических компонентах обеспечения информационной безопасности информационного общества. В этой работе исследуются проблемы формирования национальной политики по криптографии в информационном обществе, анализируется опыт развитых стран в этой области, а также современное состояние исследований в области криптографии на основе опыта международных конкурсов по криптографии. Как результат, определяются основные направления модельной политики по криптографии для развивающихся стран, и разрабатываются рекомендации по решению ряда проблем, ожидаемых при практической реализации этой политики.

Ключевые слова: *э-государство; информационная безопасность; криптография; криптоанализ; политика в области криптографии.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

Problems of formation of the national cryptography policy in the information society

Cryptographic methods of information protection play an important role in the technological components of ensuring of information security in information society. In this paper, we study the problem of formation of national cryptography policy in information society, analyze the experience of developed countries in this field, as well as the current state of research in the field of cryptography based on the experience of international cryptography competitions. As a result, the main directions of the model cryptography policy for developing countries are defined, and recommendations are developed to address some of the problems anticipated in the practical implementation of this policy.

Keywords: *information society; information security; cryptography; cryptanalysis; cryptography policy.*