Milli Kibersuverenlik üçün Kriptoqrafiya Yol Xəritəsi

Yadigar İmamverdiyev[1], Ağa Ağayev[2]
[1,2]Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[1]*yadigar.imamverdiyev@aztu.edu.az*, [2]*agha.aghayev@aztu.edu.az*

Xülasə*— Kriptoqrafiya kibersuverenliyin təmin olunmasında baza texnologiyalarından biri kimi çıxış edir: dövlətin strateji sənədlərini, vətəndaşların fərdi məlumatlarını qoruyur, e-dövlətin etimad infrastrukturunun texnoloji əsasını təşkil edir (e-imza, eID, rəqəmsal müqavilələr), kritik informasiya infrastrukturunda idarəetməni stabil və təhlükəsiz edir. Kibersuverenlik üçün ən vacib məsələlərdən biri bu sahədə xarici asılılığın azaldılması və kriptoqrafik müstəqilliyin təmin olunmasıdır. Bu məqalədə milli kibersuverenliyin təmin olunmasında kriptoqrafiyanın strateji rolu əsaslandırılır və dövlət səviyyəsində kriptoqrafik imkanların sistemli inkişafı üçün "Milli kriptoqrafiya yol xəritəsi" konseptual modeli təklif olunur. Yol xəritəsi modeli kriptoqrafiyanı yalnız texniki alət kimi deyil, hüquqi-normativ baza, institusional idarəetmə, standartlaşdırma, texnoloji infrastruktur (açar idarəetməsi), elmi-tədqiqat və kriptoanaliz, insan kapitalı, eləcə də sənaye və yerli məhsul ekosistemi ilə birlikdə milli səviyyədə idarə olunan kompleks sistem kimi təqdim edir. Məqalədə simmetrik kriptoqrafiyanın yol xəritəsində xüsusi yer tutduğu göstərilir və bu sahədə qısa, orta və uzunmüddətli inkişaf mərhələləri təklif edilir. Nəticədə təqdim edilən çərçivə modeli kriptoqrafik asılılıqların azaldılması, kriptoçevikliyin təmin olunması və post-kvant dövrünə keçidin planlaşdırılması üçün konseptual və tətbiqi model kimi çıxış edir.

Açar sözlər— kibersuverenlik; milli kriptoqrafiya; simmetrik şifrləmə; post-kvant kriptoqrafiyası.

I. GİRİŞ

Rəqəmsallaşmanın sürətlənməsi, dövlət xidmətlərinin elektron mühitə keçidi, kritik infrastrukturun (enerji, nəqliyyat, su, telekommunikasiya və s.) şəbəkə əsaslı idarəetməyə inteqrasiyası kibertəhlükəsizlik məsələlərini milli təhlükəsizlik gündəliyinin əsas komponentinə çevirmişdir. Bu şəraitdə "kibersuverenlik" anlayışı dövlətin rəqəmsal məkan üzərində idarəetmə, nəzarət, müdafiə və etibar mexanizmlərini formalaşdırmaq qabiliyyətini ifadə edən strateji konsepsiya kimi ön plana çıxır. Lakin kibersuverenliyin təmin edilməsi təkcə təşkilati və hüquqi tədbirlərlə məhdudlaşmır; bu prosesin texniki təməli etibarın, konfidensiallığın, tamlığın və autentikliyin təmin olunmasıdır.

Müasir informasiya sistemlərində etibarın qurulması və qorunması birbaşa kriptoqrafik mexanizmlərin mövcudluğu və düzgün tətbiqi ilə bağlıdır. Dövlət səviyyəsində elektron identifikasiya (eID), elektron imza, açıq açar infrastrukturu (Public Key Infrastructure, PKI), təhlükəsiz rabitə protokolları, açarların idarə olunması, məlumatların şifrlənməsi və imzalanması kimi mexanizmlər olmadan rəqəmsal dövlət xidmətlərinin etibarlı işləməsi mümkün deyil. Eyni zamanda, xarici texnologiyalardan və "qapalı" kriptoqrafik həllərdən asılılıq, açarların idarəetməsinin ölkə xaricində yerləşməsi və post-kvant dövrünə hazırlığın zəif olması kibersuverenlik üçün əlavə risklər yaradır. Buna görə də milli kibersuverenlik kontekstində kriptoqrafiya yalnız "təhlükəsizlik aləti" deyil, həm də rəqəmsal idarəetmənin və milli etibar infrastrukturunun əsas dayağı kimi qiymətləndirilməlidir.

Bu məqalənin məqsədi milli kibersuverenliyin təmin olunmasında kriptoqrafik mexanizmlərin rolunu sistemli şəkildə təhlil etmək, dövlət səviyyəsində tətbiq sahələrini strukturlaşdırmaq və prioritet istiqamətləri müəyyənləşdirməkdir. Məqalədə kriptoqrafiyanın kibersuverenlik üçün yaratdığı texniki imkanlar və bu imkanların reallaşdırılması zamanı ortaya çıxan idarəetmə və asılılıq riskləri də nəzərdən keçirilir.

Məqalənin əsas elmi və praktiki töhfəsi aşağıdakılardan ibarətdir:

- Konseptual: Kibersuverenlik anlayışı kriptoqrafiya prizmasından təhlil olunur və kriptoqrafiyanın "etibar infrastrukturu" kimi strateji rolu əsaslandırılır.
- Strukturlaşdırma: Dövlət səviyyəsində kriptoqrafik mexanizmlər tətbiq sahələrinə görə (eGov, kritik infrastruktur, sektorlararası məlumat mübadiləsi, identifikasiya və autentifikasiya, açar idarəetməsi) sistemləşdirilir.
- Risk və asılılıq analizi: Xarici vendor asılılığı, açarların suveren idarə olunmaması, qapalı kriptoqrafik modul riskləri və post-kvant təhlükəsi kibersuverenlik çərçivəsində ayrıca risk sinfi kimi təqdim edilir.
- Praktiki istiqamətləndirmə: Milli səviyyədə kriptoqrafiya siyasətinin formalaşdırılması, PKI idarəetməsi, açar idarəetmə sisteminin arxitekturası və post-kvant keçid planlaması üçün prioritet istiqamətlər göstərilir.

II. MİLLİ KİBERSUVERENLİYİN TƏMİNİNDƏ KRİPTOQRAFİK MEXANİZMLƏR

Milli kibersuverenliyin təminində kriptoqrafik mexanizmlər, əsasən, dövlət etibar infrastrukturunun formalaşdırılmasına yönəlir. Bu infrastrukturun nüvəsini aşağıdakı texnoloji komponentlər təşkil edir:

- Açıq açar infrastrukturu (PKI): sertifikatların buraxılması, idarə olunması, ləğvi və etibar zəncirinin qurulması;
- Elektron imza: dövlət xidmətlərində hüquqi qüvvəyə malik rəqəmsal təsdiqləmə;

DOI: 10.25045/cyber.gov.2026.06

- Elektron identifikasiya (eID): vətəndaş və təşkilatların rəqəmsal mühitdə etibarlı identifikasiyası;
- Təhlükəsiz rabitə protokolları: dövlət sistemləri arasında şifrlənmiş və autentifikasiya edilən rabitə;
- Açar idarəetməsi: açarların generasiyası, saxlanması, yenilənməsi və idarə olunması.

Bu komponentlərin birgə fəaliyyəti nəticəsində dövlətin rəqəmsal xidmətləri "etibar edilə bilən ekosistem" şəklini alır. Burada əsas prinsip ondan ibarətdir ki, dövlətin suverenliyi yalnız fiziki sərhədlərlə deyil, eyni zamanda rəqəmsal etibar zəncirləri və kriptoqrafik idarəetmə mexanizmləri ilə möhkəmləndirilir.

III. KİBERSUVERENLİK KONTEKSTİNDƏ KRİPTOQRAFİK RİSKLƏR VƏ ÇAĞIRIŞLAR

Kriptoqrafiyanın kibersuverenlikdə rolu artdıqca, bu sahədə risklərin xarakteri də daha strateji səviyyəyə yüksəlir. Xüsusilə aşağıdakı risklər milli kibersuverenlik üçün kritik hesab olunur:

- Xarici texnoloji asılılıq: kriptoqrafik modulların, HSM cihazlarının və ya sertifikat infrastrukturunun xarici vendorlardan asılı olması;
- Açarların suveren idarə olunmaması: açarların ölkə xaricində yerləşməsi və ya üçüncü tərəf tərəfindən idarə olunması;
- Xüsusi (ing. proprietary) kriptoqrafiya riskləri: audit olunmayan alqoritmlər, qeyri-şəffaf reallaşdırmalar və potensial "arxa qapı" ehtimalları;
- Post-kvant təhlükəsi: uzunmüddətli dövlət məlumatlarının gələcəkdə kvant kompüterləri vasitəsilə deşifrə olunması riski;
- Əməliyyat riskləri və insan faktoru: açarların sızması, sertifikatların yanlış idarə edilməsi, zəif kriptoqrafik siyasətlər.

Bu risklər göstərir ki, kriptoqrafiyanın varlığı kibersuverenliyin təmin edilməsi üçün zəruri şərt olsa da, təkbaşına kifayət deyil. Kriptoqrafik mexanizmlər milli səviyyədə düzgün idarə olunmadıqda və standartlaşdırılmadıqda, təhlükəsizlik əvəzinə sistemli zəiflik mənbəyinə çevrilə bilər.

IV. MİLLİ KRİPTOQRAFİYA YOL XƏRİTƏSİ

Qeyd edildiyi kimi, milli kibersuverenliyin texniki dayaqlarından biri kriptoqrafiyadır. Lakin bir çox ölkədə kriptoqrafiya sistemli və koordinasiya olunan milli proqram kimi deyil, ayrı-ayrı layihələr və texniki tətbiqlər səviyyəsində reallaşdırılır. Bu məqalədə dövlət səviyyəsində kriptoqrafik suverenliyin təmin edilməsi üçün "Milli kriptoqrafiya yol xəritəsi" adlı konseptual çərçivə təklif olunur. Çərçivə yeddi əsas sütun üzərində qurulur: (1) hüquqi və normativ baza, (2) institusional idarəetmə, (3) standartlaşdırma və milli kriptoqrafiya profili, (4) texnoloji infrastruktur (PKI, HSM, açar idarəetməsi), (5) elmi-tədqiqat və kriptoanaliz, (6) insan kapitalı və kriptoqrafiya məktəbi, (7) sənaye və yerli məhsul ekosistemi. Yol xəritəsinin mərhələli tətbiqi dövlət sistemlərində kriptoqrafiya asılılıqlarını azaltmağa, post-kvant dövrünə keçidi planlaşdırmağa və kriptoçevikliyi təmin etməyə imkan verir.

A. Hüquqi və normativ baza

Bu sütun kriptoqrafiyanın dövlət səviyyəsində tətbiqini normativ əsaslarla təmin edir. Buraya aşağıdakılar daxildir:

- dövlət informasiya sistemlərində şifrləmə tələbləri,
- məlumatların təsnifatı (açıq, məhdud, məxfi və s.),
- kriptoqrafik modulların sertifikatlaşdırması,
- dövlət satınalmalarında kriptoqrafik uyğunluq meyarları,
- kriptoqrafiya siyasətinin hüquqi çərçivəsi.

Normativ baza olmadan kriptoqrafiya yalnız texniki seçimlər toplusu kimi qalır və milli idarəetmə aləti rolunu oynaya bilmir.

B. İnstitusional idarəetmə

Yol xəritəsinin mühüm hissəsidir, kriptoqrafiya üzrə koordinasiyanı təmin edən institutların formalaşdırılmasına xidmət edir və aşağıdakılar daxildir:

- milli kriptoqrafiya siyasətini koordinasiya edən şura və ya mərkəz,
- dövlət PKI infrastrukturu (Root CA, Issuing CA),
- kriptoqrafik test və sertifikatlaşdırma laboratoriyası,
- dövlət CERT/SOC strukturları ilə kriptoqrafiya siyasətinin inteqrasiyası.

Bu sütun kriptoqrafiyanın "sahibsiz texnologiya" olmasının qarşısını alır və məsuliyyət bölgüsünü müəyyənləşdirir.

C. Standartlaşdırma və "Milli kriptoqrafiya profili"

Bu sütun dövlət sistemlərində istifadə ediləcək kriptoqrafik mexanizmlərin vahid profilini müəyyən edir. Milli kriptoqrafiya profili aşağıdakıları əhatə etməlidir:

- simmetrik şifrləmə (məs., AES-GCM, ChaCha20-Poly1305),
- heş funksiyalar (SHA-2, SHA-3),
- açar generasiya mexanizmləri (HKDF, PBKDF2, Argon2),
- RNG/DRBG tələbləri,
- protokol profilləri (TLS, IPsec, SSH və s.),
- kriptoqrafik açar uzunluqları və istifadə müddətləri.

Bu profil dövlət sistemlərində "minimum təhlükəsizlik səviyyəsini" normativ şəkildə təmin edir.

D. Texnoloji infrastruktur: PKI, HSM və açar idarəetməsi

Kriptoqrafiya yalnız alqoritm seçimi deyil, eyni zamanda açarların idarə olunması deməkdir. Bu sütunda aşağıdakı

elementlər əsas yer tutur:

- dövlət PKI arxitekturasının təkmilləşdirilməsi,
- HSM profilləri və yerləşdirilmə siyasəti,
- açarların rotasiyası, audit və loq mexanizmləri,
- sertifikat siyasəti (CP/CPS),
- "etibarın apparat kökü" (TPM, Secure Element) inteqrasiyası.

E. Elmi-tədqiqat və kriptoanaliz

Milli kibersuverenliyin kriptoqrafik təminatı üçün ölkə daxilində elmi-tədqiqat potensialı vacibdir. Bu sütun aşağıdakıları əhatə edir:

- kriptoanaliz qrupları,
- protokol təhlükəsizliyi və formal verifikasiya,
- yan-kanal hücumları üzrə tədqiqatlar,
- post-kvant kriptoqrafiyası üzrə araşdırmalar,
- milli kriptoqrafiya müsabiqələri və peer-review mexanizmi.

Elmi-tədqiqat olmadan kriptoqrafiya sahəsində yalnız "istehlakçı" mövqeyi formalaşır.

F. İnsan kapitalı və kriptoqrafiya məktəbi

Yol xəritəsinin davamlılığı üçün kriptoqrafiya üzrə kadr hazırlığı strateji komponentdir. Bu sütun özündə aşağıdakı tədbirləri birləşdirir:

- universitetlərdə kriptoqrafiya və kriptoqrafiya mühəndisliyi kursları,
- magistr və doktorantura ixtisaslaşmaları,
- kriptoqrafiya laboratoriyalar, CTF və praktiki təlimlər,
- dövlət qurumları üçün kriptoqrafik sertifikatlaşdırma proqramları.

G. Sənaye və yerli məhsul ekosistemi

Son sütun kriptoqrafiyanın real tətbiq bazasını formalaşdırır. Buraya daxildir:

- yerli kriptoqrafik proqram kitabxanalarının inkişafı,
- PKI və HSM inteqrasiya xidmətləri,
- kriptoqrafik modul sertifikatlaşdırması ilə bazara giriş,
- dövlət satınalmaları vasitəsilə yerli məhsulların stimullaşdırılması.

Bu sütun milli kriptoqrafiyanı yalnız akademik sahə kimi deyil, iqtisadi və sənaye komponenti kimi də formalaşdırır.

V. KRİPTOQRAFİYA MƏKTƏBİNİN FORMALAŞDIRILMASI

Bu məqalədə "kriptoqrafiya məktəbi" dedikdə insan, elmi ənənə, laboratoriya, standart, məhsul + kadr bazarı ekosistemi nəzərdə tutulur.

Kriptoqrafiya məktəbi 3 sütun üzərində qurulur:

1. Elmi tədqiqat sütunu – kriptoqrafik alqoritmlər, kriptoqrafik protokollar, post-kvant kriptoqrafiyası;
2. Tətbiqi kriptoqrafiya mühəndisliyi sütunu –kriptoqrafik implementasiyalar, məhsullar və həllər;
3. Kriptoqrafiya siyasəti və standartlaşdırma sütunu – milli kriptoqrafiya siyasəti, dövlət standartları, sertifikatlaşdırma və audit.

Kriptoqrafiya məktəbi üçün ən sağlam yol – universitetdə kadr hazırlığı üçün "konveyer" modelidir:

- Bakalavr (fundamental baza): diskret riyaziyyat, ehtimal nəzəriyyəsi və riyazi statistika, alqoritmlərin dizaynı, kriptoqrafiyaya giriş, təhlükəsiz proqramlaşdırma.
- Magistr (dərinləşmə): tətbiqi kriptoqrafiya, protokol dizaynı və analizi, post-kvant kriptoqrafiyası, kriptoanaliz, sıfır biliklə isbat və gizlilik texnologiyaları.
- Doktorantura – məktəbi yaradan mərhələdir: seçilmiş 2–3 istiqamətdə "özək tədqiqat"lar aparılır.

VI. SİMMETRİK KRİPTOQRAFİYANIN YOL XƏRİTƏSİNDƏ YERİ

Milli kriptoqrafiya yol xəritəsində simmetrik kriptoqrafiya üç mərhələdə nəzərə alınmalıdır:

1) Qısa müddət: dövlət sistemlərində simmetrik şifrləmə üçün vahid minimum profil (AES-GCM, ChaCha20-Poly1305 və s.).

2) Orta müddət: sertifikatlaşdırılmış implementasiyalar, yan-kanal hücumlarına dayanıqlılıq, performans optimallaşdırması.

3) Uzun müddət: kriptoqrafiya məktəbi formalaşdıqdan sonra milli simmetrik alqoritm dizaynı və açıq kriptoqrafiya yarış modeli.

Bu yanaşma "sıfırdan alqoritm yazmaq" ideyasını emosional qərar kimi deyil, elmi məktəb və kriptoanaliz potensialı üzərində qurulan strateji qərar kimi təqdim edir.

NƏTİCƏ

Son illərdə kibertəhlükəsizlik dövlətlərin milli təhlükəsizlik gündəliyinin ayrılmaz hissəsinə çevrilmişdir. Rəqəmsal xidmətlərin artması, dövlət sistemlərinin buludlaşması, kritik infrastrukturun rəqəmsal transformasiyası və transsərhəd məlumat axınlarının intensivləşməsi kibersuverenlik anlayışını aktuallaşdırmışdır. Kibersuverenlik dövlətin öz informasiya məkanında təhlükəsizlik, idarəetmə, etibar və nəzarət mexanizmlərini təmin etmək qabiliyyəti kimi qəbul edilə bilər. Bu kontekstdə kriptoqrafiya yalnız texniki alət deyil, həm də strateji güc komponentidir. Bu məqalədə milli kibersuverenliyin təmin olunmasında kriptoqrafiyanın strateji rolu əsaslandırılmış və dövlət səviyyəsində kriptoqrafik imkanların sistemli şəkildə inkişafı üçün "Milli Kripto

Roadmap” çərçivəsi təklif edilmişdir. Təhlil göstərir ki, kriptoqrafiya yalnız informasiya təhlükəsizliyinin texniki elementi deyil, eyni zamanda milli rəqəmsal etibar infrastrukturu, dövlətin kritik informasiya resurslarının qorunması və rəqəmsal idarəetmənin dayanıqlılığı üçün fundamental komponentdir. Bu səbəbdən kriptoqrafiyanın inkişafı ayrı-ayrı texniki layihələr şəklində deyil, milli səviyyədə koordinasiya olunan, mərhələli və ölçülə bilən proqram kimi idarə edilməlidir. Təklif olunan yol xəritəsi modeli hüquqi-normativ baza, institusional idarəetmə, standartlaşdırma, texnoloji infrastruktur, elmi-tədqiqat, insan kapitalı və sənaye ekosistemi olmaqla yeddi əsas sütun üzərində qurulmuşdur. Yol xəritəsinin mərhələli tətbiqi dövlət sistemlərində kriptoqrafik asılılıqların azaldılmasına, standartlaşdırmanın gücləndirilməsinə, açar idarəetməsinin mərkəzləşdirilməsinə və post-kvant dövrünə keçidin planlaşdırılmasına imkan verəcəkdir. Nəticə etibarilə, Milli kriptoqrafiya yol xəritəsi konsepsiyası Azərbaycan kimi ölkələr üçün kriptoqrafiyanın milli təhlükəsizlik və rəqəmsal dövlət quruculuğu kontekstində strateji alətə çevrilməsi istiqamətində tətbiq oluna biləcək praktik model təqdim edir.

MİNNƏTDARLIQ

Bu tədqiqat Azərbaycan Texniki Universitetinin daxili qrantı ilə dəstəklənir.

ƏDƏBİYYAT

[1] R. M. Alguliyev, Y. N. Imamverdiyev, R. S. Mahmudov, & R. M. Aliguliyev, “Information security as a national security component” Information Security Journal: A Global Perspective, vol. 30(1), pp. 1-18, 2021.

[2] Y. N. İmamverdiyev Y., “İnformasiya cəmiyyətində milli kriptoqrafiya siyasətinin formalaşdırılması problemləri.” Problems of information society, 6(1), s. 12-23, 2015.

[3] Y.N. Imamverdiyev, H. H. Abbasov, “National e-signature infrastructure: Current problems of scientific research.” Problems of Information Technology, pp. 33-45, 2021.

[4] R. Əliquliyev, Y. İmamverdiyev, “Elektron dövlətdə kriptoqrafiya sahəsində siyasətin formalaşdırılması problemləri.” “Elektron dövlət quruculuğu problemləri” I Respublika elmi-praktiki konfransı, s. 152-154, 2014.

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

Cryptography Roadmap for National Cybersovereignty

Yadigar Imamverdiyev[1], Agha Aghayev[2]

[1,2]Azerbaijan Technical University, Baku, Azerbaijan

Abstract— Cryptography acts as one of the basic technologies in ensuring cybersovereignty: it protects strategic state documents, personal data of citizens, forms the technological basis of the trust infrastructure of e-government (e-signature, eID, digital contracts), and secures management in critical information infrastructure. One of the most important issues for cybersovereignty is reducing external dependence in this area and ensuring cryptographic independence. This article justifies the strategic role of cryptography in ensuring national cybersovereignty and proposes a conceptual model of the “National Cryptography Roadmap” for the systematic development of cryptographic capabilities at the state level. The roadmap model presents cryptography not only as a technical tool, but also as a complex system managed at the national level, together with the legal and regulatory framework, institutional governance, standardization, technological infrastructure (key management), scientific research and cryptanalysis, human capital, as well as the industrial and local product ecosystem. The article shows that symmetric cryptography occupies a special place in the roadmap and proposes short, medium and long-term development stages in this area. As a result, the presented framework model acts as a conceptual and applied model for reducing cryptographic dependencies, ensuring crypto agility and planning the transition to the post-quantum era.

Keywords— cybersovereignty; national cryptography; symmetric encryption; post-quantum cryptography.