Kvant Texnologiyalarının Dövlətin Kibersuverenliyinin Təmin Edilməsində Rolu: Mövcud Vəziyyət, Problemlər və Perspektivlər

Məmməd Həşimov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
mamedhashimov@gmail.com

***Xülasə*— Müasir dövrdə rəqəmsal texnologiyaların sürətli inkişafı dövlətlərin informasiya mühitindəki mövqeyini və təhlükəsizlik yanaşmalarını yenidən formalaşdırır. Bu kontekstdə kvant texnologiyaları kibersuverenlik baxımından yeni imkanlar və çağırışlar təqdim edir. Bu məqsədlə məqalədə kibersuverenlik anlayışı və onun əhəmiyyəti izah edilir, kvant texnologiyalarının xüsusiyyətləri, işləmə prinsipləri və mövcud inkişaf mərhələsi təhlil olunur. Bu texnologiyaların kibersuverenliyin təmin edilməsində rolu, dövlət informasiya sistemlərinin təhlükəsizliyi və məlumatların qorunması baxımından əhəmiyyəti qiymətləndirilir. Bununla yanaşı, kvant texnologiyalarının tətbiqi ilə bağlı mövcud çətinliklər və məhdudiyyətlər araşdırılır. Yekun olaraq Azərbaycan kontekstində rəqəmsal transformasiya fonunda kvant texnologiyalarına uyğunlaşmanın və post-kvant kriptoqrafiyaya keçidin zəruriliyi əsaslandırılır.**

Açar sözlər*— *kvant texnologiyaları; kibertəhlükəsizlik; kibersuverenlik; post-kvant kriptoqrafiyaya; kvant açar paylanması.

I. GİRİŞ

Müasir dövrdə rəqəmsal texnologiyaların sürətli inkişafı və geniş tətbiqi cəmiyyətin bütün sahələrində dərin transformasiyalara səbəb olmuşdur. Dövlət idarəetməsi və sosial xidmətlər getdikcə daha çox rəqəmsal mühitə inteqrasiya olunur. Bu proses informasiya resurslarının və rəqəmsal infrastrukturun əhəmiyyətini daha da artırır. Eyni zamanda rəqəmsal sistemlərin genişlənməsi yeni təhlükəsizlik çağırışlarını da gündəmə gətirir. Bu şəraitdə dövlətlərin idarəetmə imkanları və rəqəmsal müstəqilliyi xüsusi aktuallıq kəsb edir.

Bu kontekstdə dövlətlərin rəqəmsal mühitdə yalnız təhlükəsizlik deyil, həm də idarəetmə, nəzarət və müstəqil qərarvermə imkanları ön plana çıxır. Rəqəmsal infrastruktur, informasiya resursları və texnoloji platformalar üzərində suverenlik məsələsi getdikcə daha da aktuallıq qazanır. Dövlətlərin öz rəqəmsal resurslarını və informasiya-kommunikasiya infrastrukturunu müstəqil şəkildə idarə edə bilməsi strateji əhəmiyyət kəsb edir. Bu yanaşma çərçivəsində kibersuverenlik anlayışı formalaşır və dövlətlərin rəqəmsal müstəqilliyinin əsas göstəricilərindən biri kimi çıxış edir [1]. Beləliklə, rəqəmsal mühitdə suverenliyin təmin olunması məsələsi müasir dövlətlərin əsas prioritetlərindən birinə çevrilmişdir. Bu yanaşma kibersuverenliyin müasir dövlət idarəçiliyində strateji konsepsiya kimi formalaşdığını göstərir.

II. KİBERSUVERENLİK ANLAYIŞI VƏ ONUN ƏHƏMİYYƏTİ

Kibersuverenlik, bir dövlətin öz rəqəmsal hüdudları daxilində informasiya-kommunikasiya texnologiyaları üzərində tam və müstəqil nəzarət hüququnu ifadə edən müasir təhlükəsizlik konsepsiyasıdır. Bu anlayış, dövlətin kritik informasiya infrastrukturlarını xarici müdaxilələrdən qorumaqla yanaşı, həm də milli məlumatların saxlanılması və emalı prosesində texnoloji asılılığı minimuma endirməyi hədəfləyir [2].

Kibersuverenlik dövlətin milli informasiya infrastrukturu üzərində nəzarət imkanlarını, dövlət məlumatlarının təhlükəsiz saxlanılmasını və kritik informasiya sistemlərinin qorunmasını əhatə edir. Eyni zamanda bu anlayış rəqəmsal texnologiyalar sahəsində xarici asılılığın azaldılmasını və milli texnoloji müstəqilliyin təmin edilməsini də nəzərdə tutur.

Müasir dövrdə dövlətlərin kibersuverenliyi bir neçə əsas təhlükə ilə üzləşir. Bu təhlükələrə kiberhücumlar, məlumat sızmaları, kiberkəşfiyyat fəaliyyətləri və xarici texnologiya platformalarından asılılıq daxildir. Xüsusilə kritik infrastruktur sistemləri (enerji, nəqliyyat, maliyyə) və dövlət idarəetmə sistemləri kiberhücumlar üçün əsas hədəflərdən hesab olunur. Bu sistemlərin təhlükəsizliyinin təmin edilməsi dövlətlərin milli təhlükəsizliyi üçün mühüm əhəmiyyət kəsb edir [3, 4]. Bu baxımdan mövcud təhdidlərə qarşı daha güclü və davamlı texnologiyalara ehtiyac yaranır. Bu kontekstdə kvant texnologiyaları kibersuverenliyin yeni texnoloji əsaslarının formalaşmasında mühüm rol oynaya bilər.

III. KVANT TEXNOLOGİYALARI

Rəqəmsal infrastruktur üzərində nəzarət və müstəqil idarəetmə imkanlarının genişləndirilməsi yeni nəsil texnologiyaların tətbiqini zəruri edir. Bu baxımdan kvant texnologiyaları informasiya emalı və ötürülməsi sahəsində köklü dəyişikliklər vəd edən əsas istiqamətlərdən biri kimi çıxış edir. Kvant mexanikasının prinsiplərinə əsaslanan bu texnologiyalar ənənəvi hesablama yanaşmalarından fərqli olaraq daha yüksək hesablama gücü və paralel emal imkanları təqdim edir [5]. Xüsusilə kvant texnologiyalarii mürəkkəb hesablamaların qısa müddətdə yerinə yetirilməsi baxımından böyük potensiala malikdir.

Kvant texnologiyalarının əsası XX əsrin əvvəllərində kvant mexanikasının formalaşması ilə qoyulmuşdur. Max Planck və

DOI: 10.25045/cyber.gov.2026.16

Albert Einstein kimi alimlərin tədqiqatları bu sahənin inkişafında mühüm rol oynamışdır. 1980-ci illərdə kvant texnologiyalarıinin nəzəri modeli Richard Feynman tərəfindən irəli sürülmüşdür. Daha sonra 1990-cı illərdə kvant alqoritmlərinin hazırlanması bu sahəyə marağı daha da artırmışdır [6]. Son onilliklərdə isə kvant texnologiyaları nəzəri mərhələdən çıxaraq praktiki tətbiq mərhələsinə keçməyə başlamışdır.

A. Kvant texnologiyalarının işləmə prinsipi

Kvant texnologiyalarının işləmə prinsipi kvant mexanikasının əsas qanunlarına əsaslanır və klassik fizikanın yanaşmalarından əhəmiyyətli dərəcədə fərqlənir. Bu texnologiyaların əsasını kubit (quantum bit) anlayışı təşkil edir. Klassik kompüterlərdə məlumat 0 və ya 1 şəklində saxlanıldığı halda, kubit eyni anda həm 0, həm də 1 vəziyyətində ola bilər ki, bu xüsusiyyət superpozisiya adlanır. Digər mühüm prinsip kvant dolaşıqlığıdır (eng. entanglement). Bu zaman iki və ya daha çox kubit bir-biri ilə əlaqəli olur və onlardan birinin vəziyyəti dəyişdikdə digəri də dərhal təsirlənir, məsafədən asılı olmayaraq. Bu xüsusiyyət kvant sistemlərində məlumatın daha sürətli və effektiv emalına imkan yaradır. Bundan əlavə, kvant sistemlərində interferensiya prinsipi də mühüm rol oynayır. Bu prinsip vasitəsilə düzgün nəticələr gücləndirilir, səhv ehtimallar isə zəiflədilir. Nəticə etibarilə kvant texnologiyaları paralel hesablama imkanları sayəsində mürəkkəb problemlərin daha qısa müddətdə həllinə şərait yaradır [7].

B. Kvant texnologiyalarının mövcud vəziyyəti

Hazırda kvant texnologiyaları sürətlə inkişaf etsə də, hələ tam formalaşmamış və yetkin səviyyəyə çatmamışdır. Dünyanın aparıcı texnologiya şirkətləri və dövlətləri kvant texnologiyalarıinin yaradılması və tətbiqi istiqamətində intensiv tədqiqatlar aparır. Bu sahədə hazırkı mərhələ "səs-küylü orta miqyaslı kvant sistemləri" (eng, Noisy Intermediate-Scale Quantum, NISQ) dövrü kimi xarakterizə olunur. Yəni mövcud kvant cihazları müəyyən sayda kubitə malik olsa da, onların işləməsində səhvlər və səs-küy hələ yüksəkdir. Buna görə də bu texnologiyalar geniş və tam praktik istifadə üçün hələ kifayət qədər stabil hesab olunmur.

ABŞ, Çin və Avropa İttifaqı kimi ölkələr kvant texnologiyalarına böyük vəsait yatıraraq bu sahədə üstünlük qazanmağa çalışırlar. Kvant texnologiyalarıi, kvant rabitə sistemləri və kvant kriptoqrafiyası üzrə artıq müəyyən nəticələr əldə olunub. Hətta bəzi kvant texnologiyalarıi müəyyən xüsusi məsələlərdə klassik kompüterlərdən daha yaxşı nəticə göstərə bilir [8].

C. Kvant texnologiyalarının mövcud tətbiqləri

Kvant texnologiyaları artıq təkcə nəzəri deyil, bəzi sahələrdə praktik olaraq istifadə olunur. Amma bu istifadə hələ geniş yayılmayıb və yalnız müəyyən sahələrlə məhdudlaşır. Onlardan bəziləri aşağıda göstərilmişdir [9, 10]:

- Kvant kommunikasiya və KAP. Kvant texnologiyalarının ən real tətbiq sahəsi kvant açar paylanması (Eng, Quantum Key Distribution, QKD) sistemləridir. Bu texnologiya artıq bəzi ölkələrdə təhlükəsiz rabitə şəbəkələrində istifadə olunur. Xüsusilə Çin kvant peykləri vasitəsilə uzun məsafəli təhlükəsiz kommunikasiya sistemlərini test etmişdir. Bu yanaşma dövlət səviyyəsində diplomatik və hərbi rabitənin qorunması üçün tətbiq edilir.
- "Bulud əsaslı kvant hesablama xidmətləri" (eng, Quantum computing-as-a-service, QCaaS). Bu xidmət kvant texnologiyalarıə uzaqdan çıxış imkanı yaradır. Kvant texnologiyaları artıq bəzi şirkətlər tərəfindən bulud servisi kimi təqdim olunur, məsələn IBM Quantum Experience, Google Quantum AI və D-Wave Systems. Bu platformalar vasitəsilə tədqiqatçılar və şirkətlər kvant alqoritmlərini test edə bilir. Bu yanaşma bahalı kvant avadanlıqlarına ehtiyac olmadan geniş istifadə imkanları yaradır. Eyni zamanda kvant texnologiyalarının daha sürətli yayılmasına və praktik tətbiqinin genişlənməsinə şərait yaradır.
- Kimya və material elmləri. Kvant texnologiyaları molekulyar səviyyədə mürəkkəb sistemlərin modelləşdirilməsi üçün istifadə olunur. Bu, kimyəvi reaksiyaların daha dəqiq öyrənilməsinə və onların nəticələrinin əvvəlcədən proqnozlaşdırılmasına imkan verir. Eyni zamanda yeni dərmanların hazırlanması və daha effektiv materialların yaradılması prosesini sürətləndirir. Bu cür tətbiqlər xüsusilə tibb, kimya və sənaye sahələrində böyük əhəmiyyət kəsb edir.
- Optimallaşdırma məsələləri. Kvant texnologilyalar mürəkkəb optimallaşdırma problemlərinin daha effektiv həlli üçün istifadə olunur. Klassik üsullarla çox vaxt aparan və çətin həll olunan məsələlər kvant alqoritmləri vasitəsilə daha qısa müddətdə analiz edilə bilir. Bu yanaşma çoxsaylı variantların eyni anda qiymətləndirilməsini mümkün edir. Məsələn, logistika sahəsində marşrutların optimallaşdırılması, maliyyədə investisiya portfellərinin balanslaşdırılması və sənayedə istehsal planlaşdırılması kimi məsələlər daha səmərəli həll olunur. Nəticədə xərclər azalır və qərarvermə prosesi sürətlənir.
- Post-kvant kriptoqrafiya: Hal-hazırda kvant texnologiyaları mövcud kriptoqrafik sistemləri tam şəkildə sındırmaq imkanına malik olmasa da, bu risk nəzəri olaraq sübut edilmişdir. Bu səbəbdən dövlətlər və təşkilatlar gələcək kvant təhlükələrini nəzərə alaraq post-kvant kriptoqrafiyaya keçid üzərində artıq indidən işləməyə başlamışdır. Bu yanaşma uzunmüddətli məlumat təhlükəsizliyinin təmin olunması məqsədi daşıyır və "indi topla, sonra deşifrə et" riskinin qarşısını almağa yönəlib. Bu çərçivədə lattice əsaslı və hash əsaslı post-kvant alqoritmlər geniş şəkildə araşdırılır. Xüsusilə CRYSTALS-Kyber və CRYSTALS-Dilithium kimi alqoritmlər artıq standartlaşdırma prosesində ön plana çıxmış və real sistemlərdə tətbiq üçün perspektivli həllər kimi qiymətləndirilir.
- Kvant texnologiyalarının tətbiqləri artıq mövcuddur, lakin onlar hələ geniş yayılmayıb və əsasən tədqiqat, pilot layihələr və dövlət səviyyəli xüsusi sistemlər çərçivəsində istifadə olunur. Bununla belə, bu

texnologiyaların geniş yayılması üçün hələ də texniki çətinliklər, yüksək xərclər və ixtisaslı mütəxəssis çatışmazlığı mövcuddur. Ümumilikdə, kvant texnologiyaları hazırda keçid mərhələsindədir və yaxın gələcəkdə daha geniş istifadə olunacağı gözlənilir.

IV. KVANT TEXNOLOGİYALARININ KİBERSUVERENLİYİN TƏMİN EDİLMƏSİNDƏ ROLU

Kvant texnologiyaları sahəsində baş verən inkişaflar onların yalnız elmi deyil, həm də strateji əhəmiyyət kəsb etdiyini göstərir. Bu baxımdan kvant texnologiyalarının dövlətin kibersuverenliyinin təmin edilməsində rolu xüsusi diqqət tələb edir. Kvant texnologiyalarının inkişafı dövlətlərin kibersuverenliyinə həm müsbət, həm də mənfi təsirlər göstərir. İlk növbədə bu texnologiyalar dövlətlər üçün yeni imkanlar və üstünlüklər yaradır.

Kvant texnologiyalarının əsas üstünlüklərindən biri onların yüksək hesablama gücüdür. Klassik kompüterlərlə müqayisədə kvant kompüterləri paralel hesablama prinsipi əsasında işlədiyi üçün böyük həcmli məlumatların emalı və analizi daha qısa müddətdə həyata keçirilə bilir. Bu xüsusiyyət xüsusilə böyük verilənlər (Big Data) analitikası və real vaxt qərar qəbuletmə sistemləri üçün mühüm üstünlük təşkil edir.

Dövlət səviyyəsində kvant texnologiyaları planlaşdırma və modelləşdirmə işlərində istifadə oluna bilər. Məsələn, iqtisadi proqnozlar vermək, enerji sistemlərini idarə etmək, nəqliyyatı optimallaşdırmaq və iqlim dəyişikliklərini analiz etmək kimi sahələrdə daha sürətli və dəqiq nəticələr əldə etməyə kömək edir.

Kvant texnologiyaları süni intellekt sistemlərinin daha effektiv işləməsinə kömək edir. Bu, dövlət informasiya sistemlərinin daha ağıllı və çevik olmasına şərait yaradır. Kvant yanaşmaları böyük həcmli məlumatların daha sürətli və dəqiq analizinə imkan verir. Bu proses zamanı gizli qanunauyğunluqlar və istifadəçi fəaliyyətləri daha asan müəyyən edilir. Məsələn, maliyyə əməliyyatlarında saxtakarlığın aşkarlanması və sistemlərdə anomaliyaların tapılması kimi tətbiqlərdə bu texnologiyalar mühüm rol oynayır.

Eyni zamanda kvant texnologiyaları kriptoanaliz və təhlükəsizlik analizində də yüksək hesablama gücü təmin edir ki, bu da dövlətlərin öz informasiya sistemlərini daha dərindən analiz etməsinə və potensial zəiflikləri vaxtında müəyyən etməsinə imkan verir.

Kvant texnologiyaları kibertəhlükəsizlik sahəsində daha güclü və etibarlı qorunma mexanizmləri təqdim edir. Ən vacib texnologiyalardan biri olan kvant açar paylanması (KAP) məlumatların ötürülməsi zamanı yüksək təhlükəsizlik təmin edir və rabitə kanalında hər hansı müdaxiləni dərhal aşkar etməyə imkan verir. Bu xüsusiyyət xüsusilə dövlətlər üçün kritik əhəmiyyət daşıyan məlumatların qorunmasında mühüm rol oynayır [11].

Kvant texnologiyaları kibertəhlükəsizlik sahəsində mövcud sistemləri tamamlayaraq daha güclü qorunma imkanları yarada bilər. Hazırda geniş istifadə olunan RSA, AES və elliptik əyri kriptoqrafiyası kimi alqoritmlər klassik kompüterlər üçün kifayət qədər etibarlı hesab olunur və dövlət informasiya sistemlərində geniş tətbiq edilir [12]. Lakin kvant texnologiyalarının inkişafı bu sahədə daha güclü və davamlı təhlükəsizlik mexanizmlərinin formalaşdırılmasına şərait yaradır. Xüsusilə kvant əsaslı yanaşmalar və post-kvant kriptoqrafiya gələcəkdə məlumatların daha etibarlı qorunmasını təmin edə bilər. Bu isə dövlətlərin kibersuverenliyinin gücləndirilməsi və rəqəmsal müstəqilliyinin təmin edilməsi baxımından mühüm üstünlük yaradır.

Kvant texnologiyalarına sahib olmaq dövlətlər arasında üstünlük yaradır. Bu üstünlük yalnız texniki deyil, həm də iqtisadi və siyasi baxımdan əhəmiyyətlidir. Bu texnologiyalara sahib olan ölkələr məlumat emalı və təhlükəsiz rabitədə daha güclü olur. Bu isə onların qlobal səviyyədə təsir imkanlarını artırır. Nəticədə kvant texnologiyaları dövlətlərin kibersuverenliyini gücləndirir.

Kvant texnologiyalarının inkişafı ilə yanaşı bir sıra ciddi risklər və mənfi təsirlər də ortaya çıxır. Ən əsas risk mövcud kriptoqrafik sistemlərin zəifləməsi ilə bağlıdır. Kvant texnologiyalarii gələcəkdə RSA və elliptik əyri kriptoqrafiyası kimi geniş istifadə olunan şifrələmə üsullarını sındıra biləcək potensiala malikdir. Bu isə dövlətlərin məxfi məlumatlarının təhlükəsizliyini risk altına qoya bilər.

Digər mühüm risk uzunmüddətli məlumatların qorunması ilə bağlıdır. Bu gün şifrələnmiş məlumatlar gələcəkdə kvant texnologiyaları vasitəsilə açıla bilər. Bu vəziyyət “indi topla, sonra deşifrə et” yanaşması ilə izah olunur və xüsusilə dövlət arxivləri və strateji məlumatlar üçün ciddi təhlükə yaradır [13].

Bundan əlavə kvant texnologiyalarının inkişafı dövlətlər arasında texnoloji bərabərsizliyi artırır. Bu sahədə yalnız inkişaf etmiş ölkələr ciddi irəliləyiş əldə edə bildiyi üçün digər dövlətlər texnoloji asılılıq vəziyyətinə düşə bilər. Bu isə qlobal rəqəmsal mühitdə balansın pozulmasına səbəb olur.

Eyni zamanda kvant texnologiyalarının yüksək maliyyə dəyəri və texniki mürəkkəbliyi onların geniş tətbiqini çətinləşdirir. Bu sahədə ixtisaslı mütəxəssislərin çatışmazlığı da mühüm problemlərdən biridir. Nəticədə kvant texnologiyalarının tətbiqi bütün dövlətlər üçün eyni səviyyədə əlçatan olmur.

Nəticə etibarilə kvant texnologiyaları yalnız üstünlüklər deyil, həm də ciddi risklər yaradır. Bu risklərin vaxtında qiymətləndirilməsi və uyğun tədbirlərin görülməsi dövlətlərin kibersuverenliyinin qorunması baxımından mühüm əhəmiyyət kəsb edir.

Mövcud problemlər və çağırışlar

Kvant texnologiyalarının tətbiqi bir sıra texniki və təşkilati problemlərlə müşayiət olunur. Bu problemlər texnologiyanın geniş yayılmasını və praktik tətbiqini müəyyən qədər məhdudlaşdırır. Bunlardan bəziləri aşağıda göstərilmişdir [14]:

Əsas problemlərdən biri kvant texnologiyalarının yüksək maliyyə dəyəridir. Bu sahədə tədqiqatların aparılması və infrastrukturun qurulması böyük investisiya tələb edir. Digər mühüm məsələ texnologiyanın hələ erkən inkişaf mərhələsində olmasıdır ki, bu da onun sabit və geniş tətbiqinə mane olur.

Kvant rabitə kanalları, xüsusilə optik liflər, foton itkiləri və müxtəlif səs-küy təsirlərinə həssasdır. Bu amillər siqnalın keyfiyyətini zəiflədir və effektiv ötürmə məsafəsini məhdudlaşdırır. Hazırda mövcud KAP sistemləri əsasən bir neçə yüz kilometr məsafədə etibarlı işləyə bilir və bu məsafənin artırılması üçün intensiv tədqiqatlar aparılmaqdadır.

KAP-nın mövcud klassik rabitə infrastrukturu ilə uyğunlaşdırılması həm texniki baxımdan mürəkkəb avadanlıqların, həm də xüsusi protokolların tətbiqini tələb edir. Praktik və geniş miqyasda tətbiq oluna bilən həllər yaratmaq məqsədilə klassik və kvant kriptoqrafiya yanaşmalarını birləşdirən hibrid sistemlər üzərində tədqiqatlar davam etdirilir.

Bundan əlavə, kvant texnologiyaları sahəsində ixtisaslı mütəxəssislərin çatışmazlığı müşahidə olunur. Eyni zamanda bu sahədə standartların və normativ bazanın tam formalaşmaması tətbiq prosesini çətinləşdirən amillərdən biridir.

V. Azərbaycan Kontekstində Kvant Texnologiyaları və Kibersuverenlik

Müasir dünyada dövlətlərin suverenliyi artıq yalnız fiziki sərhədlərlə deyil, həm də rəqəmsal mühitin təhlükəsizliyi ilə müəyyən olunur. Kvant texnologiyalarının inkişafı isə mövcud klassik kriptoqrafiya sistemlərini zəiflətmək potensialına malikdir. Bu isə dövlət sirrləri, kritik infrastruktur və milli məlumat bazaları üçün yeni risklər yaradır və mövcud kiber-müdafiə yanaşmalarının yenidən nəzərdən keçirilməsini tələb edir.

Eyni zamanda, kvant texnologiyaları sahəsində qlobal rəqabət fonunda kibersuverenliyin qorunması daha strateji əhəmiyyət kəsb edir. Bu artıq təkcə proqram təminatı məsələsi deyil, həm də kvant-davamlı alqoritmlərin tətbiqi və milli kvant infrastrukturunun qurulması ilə bağlıdır. Beləliklə, kvant texnologiyaları həm təhlükə, həm də dövlətlərin rəqəmsal müstəqilliyini gücləndirən mühüm vasitə kimi çıxış edir.

Bu qlobal texnoloji dəyişikliklər fonunda Azərbaycan üçün də kvant texnologiyalarının rolu xüsusi aktuallıq kəsb edir. Rəqəmsal transformasiyanın sürətləndiyi və dövlət xidmətlərinin geniş şəkildə elektron mühitə keçdiyi şəraitdə milli informasiya resurslarının qorunması prioritet məsələlərdən birinə çevrilmişdir. Xüsusilə e-hökumət sistemləri və kritik informasiya sistemlərinin təhlükəsizliyi kvant texnologiyalarının yaratdığı yeni çağırışlar kontekstində yenidən qiymətləndirilməlidir.

Azərbaycanda rəqəmsal transformasiya prosesi “Elektron hökumət”, dövlət bulud infrastrukturu və milli data mərkəzlərinin inkişafı ilə sürətlənmişdir [15]. Kritik informasiya infrastrukturları (enerji, bank sektoru, telekommunikasiya və dövlət informasiya sistemləri) əsasən klassik kriptoqrafik mexanizmlərə əsaslanır. Bu isə uzunmüddətli perspektivdə kvant təhlükələri baxımından risk yaradır.

Azərbaycan enerji istehsal edən və ixrac edən ölkə olduğu üçün SCADA və sənaye idarəetmə sistemlərinin təhlükəsizliyi xüsusi əhəmiyyət daşıyır. Kvant texnologiyalarının inkişafı gələcəkdə enerji şəbəkələri və neft-qaz infrastrukturu üçün risk yarada bilər. Bu baxımdan post-kvant kriptoqrafiyaya keçid enerji sahəsində təhlükəsizliyin təmin edilməsi üçün vacib hesab olunur.

Yuxarıda qeyd olunan məsələləri nəzərə alaraq, Azərbaycanın kvant texnologiyaları sahəsində qlobal trendlərə uyğunlaşması və kibersuverenliyini gücləndirməsi üçün kompleks yanaşma tələb olunur. Bu istiqamətdə bir neçə əsas strateji addımın həyata keçirilməsi məqsədəuyğun hesab olunur.

İlk növbədə dövlət səviyyəsində post-kvant kriptoqrafiyaya mərhələli keçid planı hazırlanmalıdır. Mövcud informasiya sistemlərində istifadə olunan şifrələmə üsulları müəyyən olunmalı və tədricən kvantadavamlı alternativlərlə əvəz edilməlidir. Bu proses xüsusilə dövlət məlumat bazaları, bank sistemi və kritik infrastruktur üçün prioritet olmalıdır.

İkinci mühüm istiqamət kvant texnologiyaları üzrə tədqiqat və innovasiya mühitinin yaradılmasıdır. Hazırda bu sahədə ixtisaslaşmış tədqiqat mərkəzləri məhdud saydadır, bu isə inkişafı müəyyən qədər ləngidir. Buna görə universitetlərdə kvant hesablama, kvant kriptoqrafiya və kvant kommunikasiya üzrə xüsusi proqramların açılması vacibdir. Eyni zamanda kvant informasiya nəzəriyyəsi və post-kvant kriptoqrafiya istiqamətində magistr və doktorantura səviyyəsində ixtisaslaşmış təhsil proqramlarının yaradılması zəruridir. Bu yanaşma gələcəkdə yerli mütəxəssislərin hazırlanmasına və texnoloji müstəqilliyin güclənməsinə kömək edəcəkdir.

Bundan əlavə, beynəlxalq əməkdaşlığın genişləndirilməsi vacibdir. Azərbaycan kvant texnologiyaları sahəsində qabaqcıl ölkələrlə və təşkilatlarla birgə layihələrdə iştirak etməlidir. Bu əməkdaşlıq vasitəsilə yeni texnologiyaların öyrənilməsi və təcrübə mübadiləsi mümkün olacaq. Nəticədə texnoloji inkişaf sürətlənəcək və qlobal standartlara uyğunlaşma asanlaşacaq.

Nəticə olaraq, kvant texnologiyalarına uyğunlaşma Azərbaycanın rəqəmsal inkişafının vacib hissəsi olmalıdır. Bu, kibersuverenliyin qorunmasına və texnoloji müstəqilliyin güclənməsinə töhfə verəcəkdir.

Nəticə

Kvant texnologiyalarının sürətli inkişafı müasir rəqəmsal mühitdə dövlətlərin fəaliyyətinə və kibersuverenliyinə əhəmiyyətli təsir göstərir. Bu texnologiyalar bir tərəfdən yüksək hesablama imkanları və yeni təhlükəsizlik mexanizmləri vasitəsilə dövlətlər üçün mühüm üstünlüklər yaradır, digər tərəfdən isə mövcud kriptoqrafik sistemlər üçün ciddi risklər formalaşdırır. Məqalədə göstərildiyi kimi, kvant texnologiyaları kibertəhlükəsizlik, məlumatların qorunması və rəqəmsal infrastruktur üzərində nəzarət baxımından yeni yanaşmalar tələb edir.

Eyni zamanda kvant texnologiyalarına sahib olmaq dövlətlər üçün texnoloji, iqtisadi və geosiyasi üstünlüklər qazandırır və onların rəqəmsal müstəqilliyini gücləndirir. Lakin bu sahədə mövcud problemlər, o cümlədən yüksək maliyyə xərcləri, kadr çatışmazlığı və texnologiyanın erkən inkişaf mərhələsində olması geniş tətbiqi məhdudlaşdırır. Azərbaycan kontekstində isə kvant texnologiyalarına uyğunlaşma, post-

kvant kriptoqrafiyaya keçid və milli elmi potensialın inkişafı xüsusi əhəmiyyət kəsb edir.

Nəticə etibarilə, kvant texnologiyalarının imkanlarından effektiv istifadə və onların yaratdığı risklərin vaxtında idarə olunması dövlətlərin kibersuverenliyinin təmin edilməsində həlledici rol oynayacaqdır.

ƏDƏBİYYAT

[1] G. Gordon, “Digital sovereignty, digital infrastructures, and quantum horizons,” AI & Society, vol. 39, pp. 125-137, 2024.

[2] Y. Shen, “Cyber sovereignty and the governance of global cyberspace,” Chinese Political Science Review, vol. 1, pp. 81–93, 2016, doi: 10.1007/s41111-016-0002-6.

[3] ENISA, ENISA Threat Landscape 2025, Eur. Union Agency for Cybersecurity, 2025.

[4] NIST, Cybersecurity Framework (CSF) 2.0, Nat. Inst. Standards Technol., 2024.

[5] J.D. Whitfield, “Quantum Computing”, pp. 1-14, 2022. https://doi.org/10.48550/arXiv.2201.09877

[6] M.A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, p. 710, 2010.

[7] P.B. Upama et al., “Evolution of quantum computing: A systematic survey,” IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), 2022. 10.48550/arXiv.2204.01856

[8] OECD, An overview of national strategies and policies for quantum technologies, OECD Digit. Economy Papers, no. 379, 2025.

[9] M.A. Shafique, A. Munir, and I. Latif, “Quantum computing: Circuits, algorithms, and applications,” IEEE Access, vol. 12, pp. 22296–22314, 2024, doi: 10.1109/ACCESS.2024.3362955.

[10] V.Raseena, “Quantum computing: Foundations, algorithms, and emerging applications,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 13, no. 1, pp. 45–52, 2023.

[11] S.Pirandola et al., “Advances in quantum cryptography,” Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012–1236, 2020.

[12] NIST, Post-quantum cryptography: Selected algorithms and standardization process, 2024.

[13] Y.Ghayad, Harvest now, decrypt later: A time-dependent threat model and migration framework for post-quantum cryptography. Södertörn University. 2026. https://doi.org/10.13140/RG.2.2.21526.00325

[14] S. K. Sahu and K. Mazumdar, “State-of-the-art analysis of quantum cryptography: Applications and future prospects,” Front. Phys., vol. 12, 2024, doi: 10.3389/fphy.2024.1456491.

[15] F. Yusifov, “Cloud in digital government: Problems and perspectives in the case of Azerbaijan”. In Digital transformation and public administration. IGI Global. 2023. https://doi.org/10.4018/979-8-3693-0200-2.ch003

The Role of Quantum Technologies in Ensuring State Cyber Sovereignty: Current Status, Challenges, and Perspectives

Mammad Hashimov

Institute of Information Technology, Baku, Azerbaijan

Abstract— In the modern era, the rapid development of digital technologies is reshaping the position of states in the information environment and their approaches to security. In this context, quantum technologies present new opportunities and challenges in terms of cyber sovereignty. For this purpose, the paper explains the concept of cyber sovereignty and its significance, and analyzes the characteristics, operating principles, and current stage of development of quantum technologies. The role of these technologies in ensuring cyber sovereignty, particularly their importance for the security of state information systems and data protection, is also evaluated. In addition, existing challenges and limitations related to the implementation of quantum technologies are examined. Finally, in the context of Azerbaijan, the necessity of adapting to quantum technologies and transitioning to post-quantum cryptography within the framework of digital transformation is justified.

Keywords— Quantum technologies; cybersecurity; cyber sovereignty; post-quantum cryptography; quantum key distribution.