Rəqəmsal Dövlət Xidmətlərində Data və Bulud Suverenliyinin Təmin Olunması üçün Metodik Yanaşmalar

Aidə Mustafayeva
Mingəçevir Dövlət Universiteti, Mingəçevir,
İdarəetmə Sistemləri İnstitutu, Bakı, Azərbaycan
aida.mustafayeva@mdu.edu.az

***Xülasə*— Qlobal rəqəmsal transformasiya dövlət idarəçiliyində struktur dəyişikliklərini və informasiya resurslarının sürətli artımını şərtləndirmişdir. Elektron hökumət, bulud texnologiyaları və süni intellektin tətbiqi xidmətlərin səmərəliliyini artırsa da, məlumat təhlükəsizliyi və suverenliyi sahəsində yeni çağırışlar yaradır. Tədqiqat göstərir ki, hüquqi boşluqlar, texnoloji asılılıq, institusional çatışmazlıqlar və kadr potensialının yetərsizliyi data və bulud suverenliyini risk altına qoyur. Milli "sovereign cloud" infrastrukturunun yaradılması, məlumatların lokallaşdırılması, kriptoqrafik protokollar, normativ gücləndirmə və kadr hazırlığı kompleks yanaşma olaraq bu risklərin minimuma endirilməsini təmin edir və dövlətin kibersuverenliyini gücləndirir.**

Açar sözlər*— *data suverenliyi; sovereign cloud; rəqəmsal dövlət; məlumat təhlükəsizliyi; hüquqi və texnoloji təminat; kibersuverenlik.

I. GİRİŞ

Qlobal miqyasda rəqəmsal transformasiya proseslərinin sürətlənməsi dövlət idarəçiliyində fundamental struktur dəyişikliklərinə səbəb olmuşdur. Elektron hökumət, rəqəmsal dövlət xidmətləri, bulud əsaslı informasiya sistemləri və süni intellekt texnologiyalarının geniş tətbiqi dövlət–vətəndaş münasibətlərinin operativliyini və səmərəliliyini artırmaqla yanaşı, məlumatların təhlükəsizliyi, məxfiliyi və suverenliyi ilə bağlı yeni risk və çağırışlar formalaşdırmışdır. Xüsusilə dövlət məlumatlarının transsərhəd axını, xarici bulud provayderlərindən asılılıq və kritik informasiya infrastrukturunun kibertəhdidlərə məruz qalması müasir dövrdə data və bulud suverenliyini strateji prioritetə çevirmişdir [1,2]. Beynəlxalq hesabatlara əsasən, 2024-cü ildə dünya üzrə dövlət qurumlarının 70%-dən çoxu əsas xidmətlərini qismən və ya tam şəkildə bulud infrastrukturları üzərindən təqdim edir və bu göstəricinin 2027-ci ilə qədər 85%-i keçəcəyi proqnozlaşdırılır [3]. ITU-nun Qlobal Kibertəhlükəsizlik İndeksinə görə isə, kibertəhlükəsizlik insidentlərinin təxminən 40%-i məhz dövlət sektorunda məlumatların mərkəzləşdirilmiş saxlanması və zəif data idarəetmə mexanizmləri ilə əlaqələndirilir [1]. OECD və World Bank hesabatları göstərir ki, inkişaf etmiş ölkələrdə data suverenliyinin təmin olunması məqsədilə milli bulud platformalarının yaradılması, məlumatların lokallaşdırılması və dövlət üçün xüsusi "sovereign cloud" modellərinə keçid əsas tendensiyaya çevrilmişdir [4,5].

Avropa İttifaqında ENISA tərəfindən aparılan tədqiqatlara əsasən, kritik dövlət xidmətlərində istifadə olunan bulud platformalarının təxminən 60%-i üçün data yerləşmə yeri və hüquqi yurisdiksiya risk amili kimi qiymətləndirilir [2]. Bu kontekstdə Fransa, Almaniya və Hollandiya kimi ölkələr dövlət sektorunda yalnız milli və ya sertifikatlaşdırılmış regional bulud infrastrukturundan istifadəyə üstünlük verir. BMT-nın Elektron Hökumət İnkişaf İndeksinə (EGDI) əsasən isə, rəqəmsal dövlət xidmətlərinin keyfiyyəti ilə informasiya təhlükəsizliyi və data idarəetmə mexanizmləri arasında birbaşa korrelyasiya mövcuddur [6].

Azərbaycan Respublikasında da rəqəmsal dövlətin formalaşdırılması dövlət siyasətinin əsas istiqamətlərindən biri kimi müəyyən edilmişdir. "Azərbaycan Respublikasının Rəqəmsal İnkişaf Konsepsiyası" və "2026–2029-cu illər üçün Rəqəmsal İqtisadiyyatın İnkişaf Strategiyası"nda dövlət informasiya resurslarının təhlükəsiz, dayanıqlı və suveren əsaslarla idarə olunması prioritet vəzifə kimi təsbit edilmişdir [7,8]. Eyni zamanda, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiya"da dövlət məlumatlarının qorunması, kritik informasiya infrastrukturunun təhlükəsizliyi və bulud texnologiyalarının risklərinin minimallaşdırılması əsas hədəflər sırasında yer alır [9].

Azərbaycan Respublikasında kritik informasiya infrastrukturlarının təhlükəsizliyinin təmin edilməsi üzrə normativ-hüquqi baza formalaşdırılmış, dövlət əhəmiyyətli sistemlərin identifikasiyası və qorunması mexanizmləri müəyyən edilmişdir [10]. Bununla belə, artan rəqəmsal xidmətlər fonunda data suverenliyi, bulud mühitlərində hüquqi nəzarət, texnoloji asılılığın azaldılması və kadr potensialının gücləndirilməsi kimi məsələlər aktuallığını qoruyur. Aparılan tədqiqatlar göstərir ki, kibertəhlükəsizlik sahəsində ixtisaslı kadr hazırlığı və metodiki yanaşmaların yetərli səviyyədə olmaması data və bulud suverenliyinin təminində əsas məhdudlaşdırıcı amillərdən biridir [11-13].

Bundan əlavə, süni intellekt texnologiyalarının dövlət idarəçiliyində tətbiqi məlumatların toplanması, emalı və saxlanması həcmini kəskin artırmaqla fərdi məlumatların qorunması və insan hüquqları kontekstində yeni risklər yaradır [14,15]. Bu baxımdan data və bulud suverenliyinin yalnız

DOI: 10.25045/cyber.gov.2026.24

texnoloji deyil, eyni zamanda hüquqi, təşkilati və etik aspektləri də nəzərə alınmalıdır [16].

Yuxarıda qeyd olunan qlobal və milli çağırışlar onu göstərir ki, rəqəmsal dövlət xidmətlərində data və bulud suverenliyinin təmin olunması kompleks, sistemli və metodik yanaşma tələb edir. Məhz bu səbəbdən təqdim olunan məqalədə rəqəmsal dövlət mühitində məlumatların təhlükəsizliyinin və suverenliyinin təmin edilməsi üçün mövcud beynəlxalq təcrübə, statistik göstəricilər və Azərbaycan reallıqları əsasında metodik yanaşmaların təhlili aparılmışdır. Mövzunun seçilməsi dövlətin kibersuverenliyinin gücləndirilməsi, rəqəmsal xidmətlərin etibarlılığının artırılması və milli maraqların qorunması baxımından xüsusi elmi və praktiki əhəmiyyət daşıyır.

II. Rəqəmsal Dövlət Xidmətlərində Data Suverenliyi Anlayışı

Rəqəmsal dövlət xidmətlərinin sürətlə genişlənməsi informasiya resurslarının həcminin, müxtəlifliyinin və strateji əhəmiyyətinin kəskin şəkildə artmasına səbəb olmuşdur. Dövlət informasiya sistemlərində toplanan məlumatlar yalnız inzibati idarəetmənin effektivliyini təmin etmir, həm də milli təhlükəsizlik, iqtisadi sabitlik və vətəndaş hüquqlarının qorunması baxımından kritik resurs kimi çıxış edir. Bu kontekstdə “data suverenliyi” anlayışı rəqəmsal dövlət idarəçiliyinin əsas konseptual sütunlarından birinə çevrilmişdir [1-9,14,17,18].

Data suverenliyi dövlətin öz yurisdiksiyası daxilində formalaşan, emal olunan və saxlanılan məlumatlar üzərində tam hüquqi, texnoloji və institusional nəzarətinin təmin edilməsi kimi izah olunur. Beynəlxalq təşkilatlar, o cümlədən OECD və World Bank, data suverenliyini yalnız məlumatların fiziki yerləşmə yeri ilə məhdudlaşmayan, həmçinin məlumatların emalı prosesində tətbiq olunan hüquqi rejimi, texnoloji platformaların mənşəyini və məlumat axınlarına nəzarət mexanizmlərini əhatə edən anlayış kimi qiymətləndirir [4,5].

Beynəlxalq təcrübələr göstərir ki, rəqəmsal dövlət xidmətlərində data suverenliyinin zəifləməsi bir sıra sistemli risklər yaradır. Bunlara məlumatların icazəsiz transsərhəd ötürülməsi, xarici hüquqi mexanizmlərin tətbiqi, kommersiya yönümlü bulud provayderlərinin dövlət məlumatlarına dolayı nəzarəti və kiberkəşfiyyat riskləri daxildir [2,3]. Məsələn, ITU-nun hesabatına görə, dövlət sektorunda baş verən kibertəhlükəsizlik insidentlərinin əhəmiyyətli hissəsi məlumatların saxlanması və idarə olunmasında suverenlik prinsiplərinin tam təmin olunmaması ilə əlaqələndirilir [1].

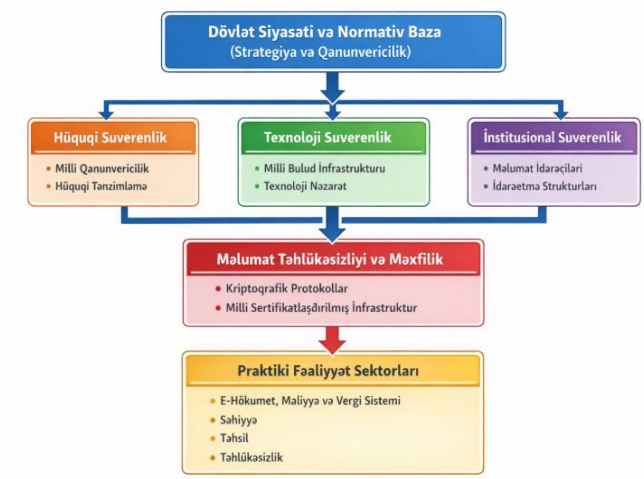
Rəqəmsal dövlət mühitində data suverenliyi aşağıdakı əsas komponentlər üzərində formalaşır (Şəkil 1):

1) Hüquqi suverenlik – dövlət məlumatlarının milli qanunvericiliyə tabe olması və xarici hüquqi müdaxilələrdən qorunması [1, 2, 4].

2) Texnoloji suverenlik – istifadə olunan proqram təminatlarının, platformaların və alqoritmlərin milli səviyyədə idarə oluna bilməsi və xarici asılılığın minimuma endirilməsi [2, 13, 18].

3) İnstitusional suverenlik – məlumatların idarə olunmasına cavabdeh qurumların səlahiyyət və məsuliyyətlərinin aydın müəyyənləşdirilməsi [11, 12].

4) Məlumat təhlükəsizliyi və məxfilik – fərdi və dövlət məlumatlarının qorunması mexanizmlərinin effektivliyi, kriptoqrafik protokolların və milli sertifikatlaşdırılmış infrastrukturun tətbiqi [1,15,16].



Şəkil 1. Rəqəmsal dövlət xidmətlərində data və bulud suverenliyinin komponentləri və qarşılıqlı əlaqəsi

Praktiki fəaliyyət sektoru nümunələri göstərir ki, ictimai idarəetmə və e-hökumət sahələrində vətəndaşların şəxsiyyət məlumatları, ünvan reyestrləri və sosial statusları Elektron Hökumət Portalı (e-gov.az) vasitəsilə toplanır və milli məlumat mərkəzlərində saxlanılır. Bu yanaşma data lokallaşdırılması və milli məlumat infrastrukturunun qorunması prinsipini təmin edir ki, xarici bulud xidmətlərinə ötürülmənin qarşısını alaraq, məlumatların tamlığını və məxfiliyini qoruyur. Vergi və maliyyə idarəetməsi sahəsində elektron vergi bəyannamələri, onlayn kassa sistemləri və ödəniş platformalarının Milli Ödəniş Sistemi və eVBS vasitəsilə milli serverlərdə işlənməsi iqtisadi suverenlik və fiskal təhlükəsizlik konseptlərini praktik olaraq həyata keçirir. Bu yanaşma məlumatın iqtisadi müstəqilliyi və rəqəmsal maliyyə ekosisteminin etibarlılığı üçün strateji əhəmiyyət daşıyır. Sosial müdafiə və səhiyyə sahəsində e-sosial.az platforması üzrə elektron sağlamlıq kartları və sosial yardım reyestrlərinin milli sertifikatlaşdırılmış sistemlərdə saxlanılması isə fərdi məlumatların məxfiliyinin qorunması və vətəndaş hüquqlarının müdafiəsi baxımından data suverenliyinin tətbiqi kimi qiymətləndirilir. Bu yanaşma fərdi məlumatların kriptoqrafik qorunması, identifikasiya autentifikasiyası və sistem təhlükəsizliyi prinsiplərinə uyğun təşkil edilmişdir.

Təhsil və elm sektorunda tələbə məlumatları, akademik göstəricilər və elmi tədqiqat nəticələrinin emalı Təhsil və Elektron Kitabxana Platforması üzərində aparılır. Lakin məlumatların xarici buludlarda saxlanması intellektual mülkiyyətin qorunması və milli innovasiya təhlükəsizliyi aspektindən risklər yaradır. Təhlükəsizlik və hüquq-mühafizə sahəsində cinayət reyestrləri, biometrik məlumatlar və videomüşahidə sistemləri yalnız milli infrastruktur üzərində

idarə olunur, Daxili İşlər Nazirliyinin Milli Məlumat Sistemi vasitəsilə bütün məlumatlar qorunur ki, bu da kritik informasiya infrastrukturlarının qorunması və biometrik məlumatların etibarlı identifikasiyası prinsiplərinə xidmət edir.

Azərbaycan Respublikasında data suverenliyi normativ və strateji sənədlər vasitəsilə institusional şəkildə təmin olunur. “Azərbaycan Respublikasının Rəqəmsal İnkişaf Konsepsiyası” dövlət informasiya ehtiyatlarının təhlükəsiz idarə olunmasını prioritet kimi müəyyən edir, “2026–2029-cu illər üçün Rəqəmsal İqtisadiyyatın İnkişaf Strategiyası” milli məlumat ekosisteminin formalaşdırılması və data əsaslı qərar qəbuletməni vurğulayır, “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiya” isə kritik informasiya infrastrukturlarına nəzarəti təmin edir. Beləliklə, data suverenliyi yalnız texniki və hüquqi məsələ deyil, həm də dövlətin kibersuverenliyinin ayrılmaz tərkib hissəsi kimi qiymətləndirilir. Onun konseptual və praktik təminatı bulud texnologiyaları, transsərhəd məlumat axınları və milli informasiya infrastrukturu kontekstində dövlətin strateji qərar qəbuletməsini dəstəkləyən həlledici amil kimi çıxış edir.

III. BULUD TEXNOLOGİYALARI VƏ BULUD SUVERENLİYİ PROBLEMLƏRİ

Bulud texnologiyaları müasir rəqəmsal dövlət xidmətlərinin və informasiya infrastrukturunun əsas komponentinə çevrilmişdir. Gartner və Cloud Security Alliance (CSA) hesabatlarına görə, 2024-cü ildə dünya üzrə dövlət və kommersiya sektorlarının 75%-i məlumatlarını qismən və ya tam şəkildə bulud infrastrukturları üzərindən idarə edir və bu göstəricinin 2027-ci ilə qədər 85%-ə çatacağı proqnozlaşdırılır [3, 18]. Lakin bulud texnologiyalarının istifadəsi bir sıra strateji və praktiki problemləri ortaya çıxarır ki, bunlar həm hüquqi, həm texnoloji, həm də institusional səviyyədə suverenliyi təhlükə altına qoyur.

Hüquqi və yurisdiksiya problemləri

Bulud provayderlərinin serverləri xarici ölkələrdə yerləşdikdə, həmin məlumatlar həmin ölkənin qanunvericiliyinə tabe olur. Bu xüsusilə dövlət sektorunda, səhiyyə, maliyyə, təhsil və milli təhlükəsizlik sahələrində ciddi risklər yaradır. Məsələn, Almaniyanın Federal Data Protection Office (BfDI) məlumat verir ki, açıq bulud provayderlərindən istifadə zamanı şəxsi və dövlət məlumatlarının xarici hüquqi tələblərə tabe olması nəticəsində 2022–2023-cü illərdə 15-dən çox dövlət sektoru məlumat sızması hadisəsi qeydə alınmışdır [2].

Avropa İttifaqında ENISA araşdırmaları göstərir ki, kritik xidmətlərin bulud infrastrukturunda saxlanması zamanı hüquqi yurisdiksiya və məlumatların yerləşdiyi yer əsas risk faktorlarıdır. Buna görə də Fransa, Almaniya və Niderland dövlət sektorunda yalnız milli və ya sertifikatlaşdırılmış regional bulud platformalarından istifadə edir [2].

Azərbaycan üçün hüquqi risklərin praktik nümunəsi olaraq, əvvəlki illərdə bəzi pilot e-hökumət layihələrində məlumatların xarici buludda saxlanması nəticəsində milli hüquqi nəzarətin məhdudlaşması müşahidə olunmuşdur. Bu isə milli suverenliyin təmin edilməsində vacib çağırış yaradır [7, 8].

Texnoloji və kibertəhlükəsizlik problemləri

Bulud mühitində məlumatların təhlükəsizliyi texnoloji baxımdan ciddi risklərlə müşayiət olunur. Xarici provayderlərin idarə etdiyi bulud serverləri üzərində kiberhücumlar və məlumat sızması halları daha yüksəkdir. Məsələn, 2023-cü ildə Kanada və ABŞ dövlət sektorunda istifadə olunan kommersiya buludlarında baş verən insidentlər nəticəsində on minlərlə vətəndaş məlumatı müvəqqəti olaraq icazəsiz əldə olunmuşdur [1,3].

Texnoloji suverenliyin təmin olunmaması, yəni milli proqram təminatı və alqoritmlərin xarici asılılıqla idarə olunması, məlumatların milli nəzarətini zəiflədir. Cloud Security Alliance (CSA) və Gartner araşdırmaları göstərir ki, milli “sovereign cloud” infrastrukturunun yaradılması və kriptovə protokolların tətbiqi texnoloji risklərin azalmasına ən effektiv həll yoludur [3, 18].

Azərbaycanın nümunəsi olaraq, Mingəçevir Dövlət Universitetinin Təhsil Platforması və Bakı Dövlət Universitetinin Elektron Kitabxana Sistemi məlumatlarını milli serverlərdə saxlayır, bu da bulud asılılığını azaldır və texnoloji suverenliyi təmin edir [11-15].

Transsərhəd məlumat axınları və kəşfiyyat riskləri

Bulud xidmətləri ilə məlumat axınları xarici provayderlərin serverləri vasitəsilə həyata keçirilirsə, dövlətin məlumat üzərində nəzarəti zəifləyir. Bu vəziyyət kiberkəşfiyyat və kommersiya casusluğu üçün əlverişli şərait yaradır. Məsələn, 2021-ci ildə ABŞ və Avropa ölkələrində açıq buludlarda saxlanmış dövlət məlumatlarının icazəsiz monitorinqi nəticəsində kiberhücum riskləri artırmışdır [2,6].

Azərbaycan üçün risk nümunəsi: pilot dövlət xidmətlərinin xarici buludlarda saxlanması zamanı məlumatların milli hüquqi və texnoloji nəzarət imkanları məhdudlaşmışdır. Bu problem, milli kibersuverenlik və iqtisadi təhlükəsizlik baxımından ciddi çağırış yaradır [8-10].

Kadr potensialı və institusional məhdudiyyətlər

Data və bulud suverenliyinin qorunmasında ixtisaslı kadr çatışmazlığı əsas problem kimi qalır. Araşdırmalar göstərir ki, kibertəhlükəsizlik sahəsində yetərli təhsil və metodik vəsaitlərin olmaması, milli bulud infrastrukturlarının idarə edilməsində ciddi çətinliklər yaradır [11-13].

Məsələn, Azərbaycanda bulud texnologiyaları üzrə dövlət və təhsil sektorlarında ixtisaslı mütəxəssis çatışmazlığı nəticəsində bəzi pilot sistemlərin təhlükəsizlik auditləri və əməliyyat idarəsi gecikmişdir. Bu isə suverenlik və milli məlumatların qorunmasını əngəlləyir.

Azərbaycan reallıqları və praktik həllər

Azərbaycan Respublikasında bulud texnologiyalarının milli məlumat infrastrukturunda tətbiqi və data suverenliyinin qorunması istiqamətində strateji tədbirlər həyata keçirilir. “Azərbaycan Respublikasının Rəqəmsal İnkişaf Konsepsiyası” və “2026–2029-cu illər üçün Rəqəmsal İqtisadiyyatın İnkişaf Strategiyası” milli bulud infrastrukturu və məlumatların lokallaşdırılmasını prioritet vəzifə kimi müəyyən edir [7,8]. Eyni zamanda “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər

üçün Strategiya” kritik informasiya infrastrukturunun qorunmasını və bulud texnologiyalarının risklərinin minimallaşdırılmasını hədəfləyir [9,10].

Milli təhsil və elmi sistemlərdə, məsələn, Mingəçevir Dövlət Universiteti və Bakı Dövlət Universitetinin elektron təhsil sistemləri, məlumatların milli serverlərdə saxlanması ilə bulud suverenliyini praktik şəkildə təmin edir [11-15]. Bu yanaşma həm hüquqi, həm texnoloji, həm də institusional riskləri minimuma endirir.

Bulud texnologiyaları dövlət və kommersiya sektorları üçün infrastruktur və funksionallıq imkanlarını genişləndirir, lakin data və bulud suverenliyinin təminatı üçün kompleks və metodik yanaşmalar tələb olunur. Hüquqi çərçivələrin gücləndirilməsi, milli “sovereign cloud” infrastrukturunun yaradılması, məlumatların lokallaşdırılması, kriptoqrafik protokolların tətbiqi və ixtisaslı kadr potensialının artırılması bu sahədə əsas prioritetlərdir. Azərbaycan üçün bu yanaşmalar milli kibersuverenlik, rəqəmsal xidmətlərin etibarlılığı və informasiya təhlükəsizliyi baxımından strateji əhəmiyyət daşıyır [1-6, 17-19].

IV. DATA VƏ BULUD SUVERENLİYİNİN TƏMİN OLUNMASI ÜÇÜN METODİK YANAŞMALAR

Data və bulud suverenliyinin təmin olunması üçün metodik yanaşmaların formalaşdırılması, yuxarıda müəyyən edilmiş problemlərin həlli baxımından həm elmi, həm də praktik əhəmiyyət kəsb edir. Hüquqi təminat bu yanaşmanın ilkin komponenti kimi çıxış edir; milli qanunvericilik çərçivəsinin gücləndirilməsi, məlumat axınının monitorinqi və kritik informasiya infrastrukturlarının hüquqi qorunması data suverenliyinin əsasını təşkil edir. Texnoloji təminat isə milli "Sovereign Cloud" infrastrukturunun yaradılması, kriptoqrafik protokolların tətbiqi və sertifikatlaşdırılmış sistemlərin istifadəsi ilə özünü göstərir, bu da həm milli məlumatların təhlükəsizliyini, həm də xarici asılılığın minimuma endirilməsini təmin edir (Şəkil 2).

Transsərhəd məlumat axını və risklərin idarə olunması prosesində məlumatların lokallaşdırılması, data mapping və risk analizinin aparılması, həmçinin əlaqəli protokolların tətbiqi vacibdir. Bu yanaşmalar xüsusilə dövlət sektorunda, məsələn, Elektron Hökumət Portalı (e-gov.az), Milli Ödəniş Sistemi və eVBS kimi platformalarda effektivdir. Hüquqi və texnoloji tədbirlər institusional və kadr potensialının gücləndirilməsi ilə birləşdirildikdə, məlumatların idarə edilməsinə cavabdeh qurumların səlahiyyət və məsuliyyətləri dəqiq müəyyən edilir, kadrların ixtisas hazırlığı və metodik vasitələrin inkişafı təmin olunur.

Praktiki texnoloji həllərin inteqrasiyası milli məlumat mərkəzlərinin qurulması, hibrid bulud modellərinin tətbiqi və analitik monitorinq alətlərinin istifadəsi vasitəsilə həyata keçirilir. Bu yanaşmalar, məsələn, Daxili İşlər Nazirliyinin Milli Məlumat Sistemi, e-sosial.az, Bakı Dövlət Universitetinin Təhsil və Elektron Kitabxana Platforması kimi real sistemlərdə tətbiq edilərək məlumatların təhlükəsiz və məxfi saxlanmasını təmin edir.

Nəticə etibarilə, data və bulud suverenliyinin təmin olunması yalnız hüquqi və texnoloji tədbirlərdən ibarət deyil,

Şəkil 2. Suveren bulud infrastrukturu

həm də institusional strukturun və kadr potensialının gücləndirilməsi, risklərin idarə olunması və real texnoloji həllərin inteqrasiyası ilə sistemli yanaşmanı tələb edir. Bu metodik yanaşma dövlətin kibersuverenliyini gücləndirir, rəqəmsal xidmətlərin etibarlılığını artırır və milli maraqların qorunmasında həlledici rol oynayır.

V. TƏHLİL VƏ PRAKTİK TÖVSİYƏLƏR

Rəqəmsal dövlət xidmətlərinin sürətlə genişlənməsi fonunda data və bulud suverenliyinin təmin olunması, həm hüquqi, həm texnoloji, həm də institusional baxımdan kompleks problemlər yaradır. Aparılan araşdırmalar göstərir ki, milli informasiya sistemlərinin xarici bulud provayderlərinə asılılığı dövlət məlumatlarının təhlükəsizliyini zəiflədir, transsərhəd məlumat axınları isə milli suverenliyə potensial təhlükə yaradır [1,3,10]. Məsələn, Avropa İttifaqında ENISA tərəfindən aparılan tədqiqatlar göstərir ki, kritik dövlət xidmətlərində istifadə olunan bulud platformalarının təxminən 60%-ində data yerləşmə yeri və hüquqi yurisdiksiya riskləri mövcuddur [2]. ABŞ və Almaniya kimi ölkələrdə milli “sovereign cloud” infrastrukturunun yaradılması məlumatların lokallaşdırılması və hüquqi nəzarətin təmin olunması məqsədilə prioritet olaraq həyata keçirilir [4,5].

Azərbaycan reallığında, Elektron Hökumət Portalı (e-gov.az), Milli Ödəniş Sistemi (eVBS) və e-sosial.az kimi platformalar milli serverlərdə yerləşdirilməklə data suverenliyinin praktik təminatını nümayiş etdirir [7-10]. Bununla belə, süni intellekt texnologiyalarının tətbiqi ilə məlumatların həcmi, müxtəlifliyi və emal sürəti kəskin artmış, nəticədə fərdi məlumatların qorunması və kibertəhlükəsizlik riskləri daha da aktuallaşmışdır [14,15]. Aparılan təhlillər göstərir ki, milli bulud infrastrukturunun mövcud vəziyyəti aşağıdakı əsas problemlərlə üzləşir: Hüquqi məhdudiyyətlər və normativ boşluqlar: Məlumatların xarici bulud provayderləri vasitəsilə saxlanılması və işlənməsi zamanı milli qanunvericiliyə riayət edilməməsi, həmçinin məlumatların transsərhəd axını ilə bağlı risklərin düzgün qiymətləndirilməməsi.

Texnoloji asılılıq: Xarici proqram təminatı və bulud platformalarına yüksək asılılıq milli informasiya infrastrukturu üzərində tam nəzarəti çətinləşdirir. Bu, kritik informasiya

sistemlərinin müdaxiləyə açıq olmasına səbəb ola bilər [2,13,18].

İnstitusional çatışmazlıqlar: Məlumatların idarə olunmasına cavabdeh qurumların səlahiyyət və məsuliyyətlərinin tam müəyyən edilməməsi nəticəsində məlumatların qorunması mexanizmlərində boşluqlar yaranır [11,12].

Kadr potensialının yetərsizliyi: Kibertəhlükəsizlik sahəsində ixtisaslı mütəxəssislərin və metodik yanaşmaların məhdudluğu milli bulud və data suverenliyinin effektiv təmin olunmasına əngəl törədir [11-13].

Bu problemlərin həlli üçün praktik tövsiyələr aşağıdakı istiqamətlər üzrə təklif olunur:

Birincisi, milli bulud infrastrukturunun tam formalaşdırılması və “sovereign cloud” modellərinin tətbiqi vacibdir. Buraya mərkəzi və regional data mərkəzlərinin yaradılması, milli və sertifikatlaşdırılmış bulud platformalarının istifadəsi, məlumatların lokallaşdırılması və kriptoqrafik protokollarla qorunması daxildir. Bu yanaşma məlumatların transsərhəd axınına nəzarəti gücləndirir və milli suverenliyi təmin edir [2,4,5].

İkincisi, hüquqi və normativ bazanın gücləndirilməsi tövsiyə olunur. Bu, data suverenliyinin qorunması üçün milli qanunvericilikdə aydın tələblərin müəyyən edilməsi, xarici provayderlərlə müqavilə şərtlərinin hüquqi baxımdan tənzimlənməsi və milli kibertəhlükəsizlik standartlarının tətbiqini əhatə edir [7-9].

Üçüncüsü, texnoloji suverenliyin artırılması məqsədilə milli proqram təminatı, bulud platformaları və idarəetmə alqoritmlərinin inkişafı vacibdir. Bu yanaşma milli informasiya infrastrukturu üzərində tam nəzarəti təmin etməklə yanaşı, xarici asılılığın azaldılmasına və kibertəhlükəsizlik risklərinin minimuma endirilməsinə imkan verir [2,13,18].

Dördüncüsü, institusional və idarəetmə mexanizmlərinin təkmilləşdirilməsi tələb olunur. Məlumatların qorunmasına cavabdeh qurumların səlahiyyət və məsuliyyətləri dəqiq müəyyən edilməli, koordinasiya mexanizmləri və operativ monitorinq sistemi tətbiq edilməlidir [1,11,12].

Beşincisi, kadr potensialının artırılması və metodik yanaşmaların inkişafı zəruridir. Bu, yüksək ixtisaslı mütəxəssislərin hazırlanması, təlim və seminarların təşkil edilməsi, milli standartların tətbiqi və təcrübəyə əsaslanan davamlı təhlillərin aparılması ilə təmin olunur [11-13,16].

Beləliklə, data və bulud suverenliyinin təmin olunması yalnız texnoloji və hüquqi məsələ deyil, həm də milli təhlükəsizlik, iqtisadi və sosial sabitliyin qorunması baxımından strateji əhəmiyyət daşıyan kompleks sahədir. Azərbaycan kontekstində, milli bulud infrastrukturunun yaradılması, hüquqi normativlərin təkmilləşdirilməsi, texnoloji asılılığın azaldılması və kadr potensialının gücləndirilməsi metodik yanaşmaların əsas komponentlərini təşkil edir. Bu yanaşmaların ardıcıl tətbiqi dövlətin kibersuverenliyini gücləndirir, rəqəmsal xidmətlərin etibarlılığını artırır və milli maraqların qorunmasını təmin edir [1-6,17-19].

NƏTİCƏ

Aparılan tədqiqat göstərir ki, rəqəmsal dövlət xidmətlərinin genişlənməsi və bulud texnologiyalarının tətbiqi milli informasiya sistemlərinin fəaliyyətində strateji əhəmiyyət daşıyan məlumat həcmini artırmış, data və bulud suverenliyi məsələlərini aktual problemlər sırasına çıxarmışdır. Analiz nəticəsində müəyyən edilmişdir ki, data və bulud suverenliyinin zəif təmin olunması hüquqi boşluqlar, texnoloji asılılıq, institusional koordinasiya çatışmazlıqları və kadr potensialının yetərsizliyi kimi sistemli risklər yaradır. Bu risklər, öz növbəsində, milli təhlükəsizlik, iqtisadi sabitlik və vətəndaşların fərdi məlumatlarının qorunması baxımından ciddi təhdidlər meydana gətirir [1–19].

Tədqiqatın metodik hissəsində təqdim olunan yanaşmalar – milli “sovereign cloud” infrastrukturunun qurulması, məlumatların lokallaşdırılması və kriptoqrafik protokolların tətbiqi, hüquqi və normativ bazanın gücləndirilməsi, texnoloji və proqram təminatlarının milli səviyyədə idarə olunması, institusional koordinasiya mexanizmlərinin təkmilləşdirilməsi və kadr potensialının artırılması – data və bulud suverenliyinin təmin olunması üçün sistemli və praktik həll yollarını formalaşdırır. Bu yanaşmalar yalnız texnoloji və hüquqi sferanı deyil, həm də idarəetmə, sosial və strateji aspektləri əhatə edir [1-6,11-19].

Praktiki baxımdan, Azərbaycan Respublikasında tətbiq olunan milli informasiya infrastrukturunun təkmilləşdirilməsi, milli bulud platformalarının istifadəsi, dövlət vətəndaş məlumatlarının təhlükəsiz və sertifikatlaşdırılmış mühitdə idarə olunması, eyni zamanda normativ-hüquqi sənədlərin gücləndirilməsi data və bulud suverenliyinin real təminatını nümayiş etdirir [7-10,14]. Bu yanaşmalar həm milli maraqların qorunması, həm də rəqəmsal xidmətlərin etibarlılığının artırılması baxımından strateji əhəmiyyətə malikdir.

Nəticə olaraq, data və bulud suverenliyinin təmin olunması müasir rəqəmsal dövlət xidmətlərinin etibarlı, dayanıqlı və milli maraqlara uyğun fəaliyyətinin əsas göstəricisi kimi çıxış edir. Tədqiqat göstərir ki, bu sahədə kompleks və metodik yanaşmaların tətbiqi dövlətin kibersuverenliyini gücləndirir, rəqəmsal transformasiya proseslərinin təhlükəsizliyini təmin edir və milli informasiya ekosisteminin davamlı inkişafına töhfə verir.

ƏDƏBİYYAT

[1] International Telecommunication Union (ITU), “Global cybersecurity index & digital government statistics.” [Online]. Available: https://www.itu.int

[2] European Union Agency for Cybersecurity (ENISA), “Cloud security and data sovereignty reports.” [Online]. Available: https://www.enisa.europa.eu

[3] Gartner Research, “Cloud strategy, data governance and digital sovereignty reports.” [Online]. Available: https://www.gartner.com

[4] World Bank, “Digital government, data governance and cloud computing reports.” [Online]. Available: https://www.worldbank.org

[5] Organisation for Economic Co-operation and Development (OECD), “Digital government index & data governance statistics.” [Online]. Available: https://www.oecd.org

[6] United Nations Department of Economic and Social Affairs (UN DESA), “E-government development index (EGDI).” [Online]. Available: https://publicadministration.un.org

[7] Azərbaycan Respublikasının Prezidenti, “Azərbaycan Respublikasında rəqəmsal inkişaf konsepsiyası.” [Online]. Available: https://e-qanun.az/framework/58765

[8] Azərbaycan Respublikasının Prezidenti, “Azərbaycan Respublikasında 2026–2029-cu illər üçün rəqəmsal iqtisadiyyatın inkişaf strategiyası.” [Online]. Available: https://e-qanun.az/framework/60981

[9] Azərbaycan Respublikasının Prezidenti, “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün strategiya.” [Online]. Available: https://e-qanun.az/framework/55045

[10] “Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydalarının təsdiq edilməsi haqqında.” [Online]. Available: https://e-qanun.az/framework/54651

[11] “Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında.” [Online]. Available: https://e-qanun.az/framework/47253

[12] A. M. Mustafayeva, G. S. Baxşiyeva, Ş. S. Nəsirova, “İnformasiya infrastrukturlarında kibertəhlükəsizliyin perspektivləri,” *Tezis*, “V International Bahtiyar Vahabzade Turkish World History, Culture and Literature Congress” mövzusunda Beynəlxalq elmi-praktiki konfransın materialları, Şəki, Azərbaycan, 16–17 Avqust 2023, s. 7–8.

[13] A. M. Mustafayeva, *Şəbəkə təhlükəsizliyi*, Dərslik, Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin maliyyə dəstəyi ilə həyata keçirilən Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyasının təşkilatçılığı ilə “İnformasiya təhlükəsizliyi ixtisası üzrə elmi-metodiki tədris (çap və onlayn) vəsaitlərin hazırlanması” layihəsi çərçivəsində hazırlanmışdır, 2024, 310 s.

[14] Azərbaycan Respublikasının Prezidenti, “Azərbaycan Respublikasında 2025–2028-ci illər üçün süni intellekt strategiyası.” [Online]. Available: https://e-qanun.az/framework/59218

[15] A. M. Mustafayeva, *Şəbəkə təhlükəsizliyi*. Bakı, Azərbaycan: Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası, 2024, 310 p. [Online]. Available: https://lectures.ozunoyren.com/assets/posts/lecture-notes/şəbəkə-təhlükəsizliyi/book.pdf

[16] G. Rzayeva and A. İbrahimova, *Süni intellekt, insan hüquqları və fərdi məlumatların təhlükəsizliyi*. Bakı, Azərbaycan: “Nurlar” nəşriyyatı, 2021, 200 p.

[17] Statista Research Department, “Cloud computing, data sovereignty and cybersecurity statistics.” [Online]. Available: https://www.statista.com

[18] Cloud Security Alliance (CSA), “Global cloud security and data governance studies.” [Online]. Available: https://cloudsecurityalliance.org

[19] R. Ş. Mahmudova, “Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində beynəlxalq təcrübənin analizi,” *İnformasiya cəmiyyəti problemləri*, no. 1, pp. 85–94, 2022.

Methodological Approaches to Ensuring Data and Cloud Sovereignty in Digital Government Services

Aida Mustafayeva

Mingachevir State University, Mingachevir,
Institute of Control Systems, Baku, Azerbaijan

Abstract— Global digital transformation has triggered structural changes in public administration and rapid growth of information resources. While the implementation of e-government, cloud technologies, and artificial intelligence enhances service efficiency, it simultaneously creates new challenges in data security and sovereignty. The study demonstrates that legal gaps, technological dependency, institutional deficiencies, and insufficient human capital pose risks to data and cloud sovereignty. The establishment of a national “sovereign cloud” infrastructure, data localization, cryptographic protocols, regulatory strengthening, and personnel training provide a comprehensive approach that minimizes these risks and reinforces the state’s cyber-sovereignty.

Keywords— data sovereignty, sovereign cloud, digital government, information security, legal and technological assurance, cyber-sovereignty.