Rəqəmsal Dövlətin Bulud Suverenliyi: Mövcud Vəziyyət, Problemlər, Təhlükəsizlik, Risklər və Həll Yolları

Oqtay Ələkbərov
İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
oqtayalakbarov@yahoo.com

***Xülasə*— Rəqəmsallaşmanın sürətlənməsi dövlət idarəçiliyində bulud texnologiyalarının geniş tətbiqinə səbəb olmuşdur. Lakin məlumatların xarici provayderlərdə saxlanması milli təhlükəsizlik, hüquqi müstəqillik və kiber təhlükəsizlik baxımından ciddi risklər yaradır. Bu səbəbdən "bulud suverenliyi" anlayışı rəqəmsal dövlət konsepsiyasının əsas sütunlarından birinə çevrilmişdir. Məqalədə bulud suverenliyinin konseptual əsasları, komponentləri, mövcud problemlər, təhlükələr və risklər təhlil olunur, həmçinin effektiv həll yolları təqdim edilir.**

Açar sözlər— rəqəmsal dövlət; bulud suverenliyi; məlumat təhlükəsizliyi; milli bulud infrastrukturu; kiber risklər; hüquqi müstəqillik; hibrid bulud model.

I. GİRİŞ

Rəqəmsal transformasiya proseslərinin sürətlənməsi dövlət idarəçiliyində bulud texnologiyalarının geniş tətbiqini aktuallaşdırmışdır. Elektron dövlət sistemləri, rəqəmsal xidmət platformaları və böyük həcmli dövlət məlumatlarının emalı bulud infrastrukturunu strateji resursa çevirmişdir. Lakin bu məlumatların xarici provayderlərin nəzarətində saxlanılması hüquqi müstəqillik, informasiya təhlükəsizliyi və milli suverenlik baxımından ciddi risklər yaradır.

Məlumatların digər ölkələrin yurisdiksiyasına tabe olması, kiberhücumların artması və texnoloji asılılığın dərinləşməsi fonunda bulud suverenliyi məsələsinin aktuallığı əhəmiyyətli dərəcədə yüksəlmişdir. Bu konsepsiya dövlətin rəqəmsal resursları üzərində hüquqi, texnoloji və təhlükəsizlik nəzarətinin təmin edilməsini nəzərdə tutur və rəqəmsal dövlət modelinin əsas dayaqlarından biri kimi çıxış edir. Beynəlxalq təcrübə göstərir ki, bir çox dövlətlər milli bulud infrastrukturlarının yaradılmasına yönəlmiş strategiyalar formalaşdırır və məlumatların milli sərhədlər daxilində qorunmasını prioritet elan edirlər. Bu baxımdan bulud suverenliyinin öyrənilməsi və tətbiqi müasir dövlət idarəçiliyi üçün həm elmi, həm də praktiki baxımdan yüksək aktuallığa malikdir.

II. TƏDQİQAT İŞLƏRİ

Tədqiqat işində [1] ictimai bulud mühitində məlumat suverenliyi modellərinin müqayisəsi və məlumatların milli yurisdiksiyada saxlanması, hüquqi uyğunluq və təhlükəsizlik mexanizmləri təhlil edilir. Tədqiqat işində [2] Avropa ölkələrinin suveren bulud siyasətlərindəki fərqləri araşdırılır və rəqəmsal müstəqilliyin təminində müxtəlif strategiyaların tətbiqi göstərilir. Tədqiqat işində [3] Gaia-X və digər Avropa bulud təşəbbüslərinin siyasi və texnoloji aspektləri, dövlət suverenliyi ilə əlaqəsi araşdırılır. Tədqiqat işində [4] dövlət sektorunda bulud xidmətlərinin istifadəsinin hüquqi və tənzimləyici riskləri, xüsusən xarici provayderlərdə məlumat saxlanmasının beynəlxalq hüquq və suverenlik problemləri araşdırılır. Tədqiqat işində [5] məxfi hesablama və təhlükəsiz bulud arxitekturaları vasitəsilə rəqəmsal suverenliyi təmin edən yeni təhlükəsizlik modelləri araşdırılır. Tədqiqat işində [6] qlobal bulud platformalarının məlumat suverenliyi və beynəlxalq idarəetməyə təsirini, Çin nümunəsi üzərindən bulud infrastrukturu, dövlət nəzarəti və rəqəmsal iqtisadiyyat arasındakı geopolitik əlaqələri araşdırılır. Tədqiqat işində [7] Avropa İttifaqı rəqəmsal suverenliyini gücləndirmək və bulud texnologiyalarına xarici asılılığı azaltmaq üçün Gaia X və European Alliance for Industrial Data, Edge, and Cloud kimi təşəbbüsləri istifadə edir, strateji asılılıqlar və bulud bazarının dinamikalarını təhlil edilir. Tədqiqat işində [8] Hindistan, Hollandiya, Pakistan, Tayvan, Ukrayna və Birləşmiş Krallığın rəqəmsal suverenliyi müqayisə olunur; hər bir ölkənin xarici bulud infrastrukturuna asılılığı, suverenlik strategiyaları və geo-siyasi konteksti analiz edilir, dövlət xidmətləri və vətəndaş trafikinin xarici infrastrukturlarda səviyyəsi ölçülür.

III. BULUD SUVERENLİYİNİN MÖVCUD VƏZİYYƏTİ: QLOBAL VƏ REGİONAL YANAŞMALAR

Son illərdə rəqəmsal transformasiyanın sürətlənməsi və dövlət məlumatlarının həcminin artması fonunda bulud suverenliyi qlobal informasiya siyasətinin prioritetinə çevrilmişdir. Bir çox inkişaf etmiş ölkələr milli bulud infrastrukturlarının yaradılmasına yönəlmiş strategiyalar həyata keçirir, beləliklə, xarici provayderlərin nəzarətindən yaranan hüquqi, təhlükəsizlik və strateji asılılıq risklərini azaltmağa çalışırlar. Xüsusilə Avropa İttifaqında GDPR çərçivəsi suveren bulud yanaşmalarının formalaşmasına təkan vermiş və "European Cloud Sovereignty" təşəbbüsü altında Gaia-X layihəsi inkişaf etdirilmişdir. Gaia-X Avropada açıq standartlara əsaslanan, etibarlı və interoperabilləşmiş bulud ekosistemi yaratmağı hədəfləyir. Layihəyə Avropa dövlətləri, iri və orta biznes şirkətləri, eləcə də tədqiqat institutları qoşularaq məlumatların təhlükəsiz saxlanması, emalı və idarəsini təmin edir. 2021-ci ildə Brüsseldə qeyri-kommersiya

DOI: 10.25045/cyber.gov.2026.18

təşkilatı kimi təsis edilən Gaia-X hazırda 300-dən çox iştirakçını birləşdirir və milli strategiyalarla uyğun bulud mühiti yaratmağa imkan və ABŞ-da hökumət qurumları üçün xüsusi “government cloud” modelləri geniş tətbiq olunur və dövlət məlumatlarının təhlükəsizliyinə yönəlmiş sertifikatlaşdırılmış bulud mühitləri formalaşdırılır. Asiya regionunda isə Çin və Hindistan kimi ölkələr rəqəmsal suverenlik strategiyaları çərçivəsində dövlət məlumatlarının milli sərhədlər daxilində saxlanılmasını məcburi edən hüquqi mexanizmlər tətbiq edir və dövlətə məxsus bulud platformalarının inkişafına böyük investisiyalar ayırır. Yaxın Şərq ölkələrində də milli təhlükəsizlik maraqları fonunda suveren bulud tələbləri gücləndirilir və dövlət sektorunda yerli data mərkəzlərinə keçid prosesi sürətlənir.

Regional səviyyədə müşahidə olunan bu tendensiyalar göstərir ki, bulud suverenliyi artıq yalnız texnoloji məsələ deyil, eyni zamanda dövlətlərin informasiya təhlükəsizliyi, hüquqi müstəqilliyi və strateji idarəetmə qabiliyyəti ilə birbaşa bağlıdır. Azərbaycan və region ölkələrində də dövlət informasiya ehtiyatlarının milli infrastrukturda saxlanmasına yönəlmiş təşəbbüslər genişlənir, milli data mərkəzlərinə investisiyalar artırılır və kiber təhlükəsizlik üzrə normativ baza gücləndirilir. Bu proseslər bulud suverenliyinin rəqəmsal dövlət quruculuğunda fundamental rol oynadığını və yaxın illərdə daha da aktuallaşacağını göstərir.

IV. RƏQƏMSAL DÖVLƏTDƏ BULUD SUVERENLİYİNİN KONSEPTUAL MODELİ VƏ KOMPONENTLƏRİ

Son dövrlərdə bir çox dövlətlər milli məlumatların qorunması, hüquqi uyğunluq və kibertəhlükəsizlik baxımından suveren bulud infrastrukturuna maraq göstərir; bu çərçivədə dövlətlər həm milli data mərkəzləri və hibrid bulud modelləri qurur, həm də provayder asılılığını minimuma endirmək, məlumatların ölkə daxilində saxlanmasını təmin etmək və kritik dövlət resurslarının təhlükəsizliyini gücləndirmək məqsədilə hüquqi və texnoloji mexanizmləri fəal şəkildə tətbiq edirlər, bunlarla bağlı rəqəmsal dövlətin bulud suverenliyi diqqət yetirilir.

Bulud suverenliyi dövlətin rəqəmsal resursları üzərində texnoloji, hüquqi, təhlükəsizlik və idarəetmə nəzarətinin təmin edilməsinə əsaslanır. Bu mexanizmlər birgə şəkildə informasiya müstəqilliyini formalaşdırır. Rəqəmsal dövlətin bulud suverenliyi konseptual modeli dövlət resursları üzərində tam nəzarəti, məlumatların milli qanunvericiliyə uyğun qorunmasını və kibertəhlükəsizlik prinsipləri əsasında dövlət fəaliyyətlərinin davamlılığını təmin etməyə yönəlir (Şəkil 1).

Şəkil 1. Rəqəmsal dövlətdə bulud suverenliyinin konseptual modeli

Bu model özündə beş əsas nəzarət sahəsini birləşdirir:

- Milli məlumatların saxlanması – Dövlət məlumatlarının ölkə daxilində yerləşdirilməsi və milli hüquqi çərçivəyə tabe olması məlumatların xarici yurisdiksiyalardan qorunmasını təmin edir və milli təhlükəsizlik baxımından strateji əhəmiyyət daşıyır.
- Hüquqi uyğunluq mexanizmləri – Məlumatların işlənməsi və saxlanmasının milli qanunvericiliyə uyğunluğunu, şəxsi məlumatların və dövlət sirrlərinin mühafizəsini, eləcə də hüquqi nəzarətin təmin edilməsini əhatə edir.
- Kibertəhlükəsizlik infrastrukturu – SOC mərkəzləri, şifrələmə və açar idarəetmə sistemləri, təhlükəsizlik auditləri vasitəsilə dövlət məlumatlarının kiberhücumlara və icazəsiz girişlərə qarşı qorunmasını təmin edir.
- Milli bulud platformaları – Dövlətə məxsus və ya dövlət nəzarətində olan data mərkəzləri vasitəsilə kritik məlumatların təhlükəsiz saxlanmasını, emalını və texnoloji müstəqilliyi təmin edir.
- İnteroperabillik və davamlılıq – Bulud sistemlərinin inteqrasiya oluna bilməsini, xidmətlərin fasiləsizliyini, fövqəladə hallara davamlılığını və genişlənmə imkanlarını təmin edir.

V. BULUD SUVERENLİYİ: PROBLEMLƏR, TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ VƏ RİSKLƏR

Bu bölmədə bulud suverenliyinin tətbiqi zamanı qarşıya çıxan əsas problemlər, o cümlədən maliyyə xərclərinin yüksəkliyi, texnoloji resursların məhdudluğu, ixtisaslı kadr çatışmazlığı və normativ yükün artması kimi məsələlər təhlil edilir. Eyni zamanda, hüquqi və normativ uyğunluq, kibertəhlükəsizlik, provayderdən asılılıq, məlumatların itirilməsi, infrastrukturun dayanıqlılığı və təhlükəsizliklə bağlı digər məsələlər də ətraflı şəkildə qiymətləndirilir.

Əsas problemlər:

- Yüksək maliyyə xərcləri – Milli bulud infrastrukturu üçün böyük investisiyalar tələb olunur: data mərkəzlərinin tikintisi, texniki avadanlıqlar, təhlükəsizlik sistemləri və ehtiyat mərkəzlərin təmin edilməsi.
- Texnoloji resursların məhdudluğu – Qabaqcıl bulud texnologiyalarına çıxışın məhdud olması və yerli provayderlərin kifayət qədər inkişaf etməməsi suveren bulud həllərinin tətbiqini çətinləşdirir.
- İxtisaslı kadr çatışmazlığı – Bulud mühəndisliyi, kibertəhlükəsizlik və məlumat idarəetməsi sahələrində peşəkar mütəxəssislərin azlığı milli bulud

infrastrukturunun qurulmasını və idarə olunmasını gecikdirir.

- Skalabilik çətinlikləri – Böyük həcmli məlumatların və yüksək performans tələb edən xidmətlərin milli infrastrukturda yerləşdirilməsi genişlənmə imkanlarını məhdudlaşdırır.
- Normativ yükün artması – Dövlət buluduna tam nəzarət nəticəsində bütün hüquqi tələblərin, təhlükəsizlik standartlarının və məlumat qorunması qaydalarının icrasına cavabdeh olmaq əlavə inzibati yük yaradır.

Təhlükəsizlik məsələləri:

- Məlumatların sızması və icazəsiz giriş – Xarici ölkələr, bulud provayderləri və üçüncü tərəf təşkilatlar tərəfindən dövlət məlumatlarına icazəsiz çıxış riski mövcuddur.
- Dövlət səviyyəli kiberhücumlar – DDoS, zərərli proqramlar və dövlət-sponsored hücumlar bulud infrastrukturunu hədəf ala bilər.
- Provayderə həddindən artıq etibar – Xarici provayderlərin təhlükəsizlik siyasətinin tam şəffaf olmaması və xidmət dayanmaları dövlətin təhlükəsizlik səviyyəsini zəiflədir.
- Açarların idarə olunması – Şifrələmə açarlarının provayder nəzarətində olması real suverenliyi məhdudlaşdırır, açarların dövlət tərəfindən idarə olunması vacibdir.
- Daxili risklər – İşçi səhvləri, düzgün konfiqurasiya edilməmiş sistemlər və zəif patch idarəetməsi təhlükəsizlik boşluqları yaradır.
- İnteroperabillik zəifliyi – Fərqli buludlar arasında məlumat mübadiləsi zamanı itkilər və uyğunluq səhvləri yarana bilər.
- Fiziki təhlükəsizlik problemləri – Data mərkəzlərinin qeyri-kafi mühafizəsi, təbii fəlakətlərə dayanıqsızlıq və enerji kəsintiləri təhlükəsizlik risklərini artırır.

Əsas risklər:

- Xarici hüquqi təsirlər və məcburi məlumat açıqlamaları – Məlumatlar xarici serverlərdə yerləşirsə, digər ölkələrin qanunları dövlət məlumatlarına çıxışı tələb edə bilər.
- Kiberhücumlar və məlumat sızması – DDoS, ransomware, phishing və digər hücumlar dövlət buludunu hədəf ala bilər.
- Provayderdən asılılıq (vendor lock-in) – Yalnız bir provayderə bağlı qalmaq xidmətlərin dayanmasına, məlumatların miqrasiyasının çətinləşməsinə və maliyyə itkilərinə səbəb ola bilər.
- Məlumatların itirilməsi və korlanması – Konfiqurasiya səhvləri, server nasazlığı və insan faktorundan yaranan itkilər ciddi riskdir.
- Açarların (encryption keys) düzgün idarə olunmaması – Şifrələmə açarları provayderin nəzarətindədirsə, məlumatların real suverenliyi təmin olunmur.
- İnfrastrukturun fiziki təhlükələri – Təbii fəlakətlər, enerji kəsintiləri və fiziki müdaxilələr bulud xidmətlərinin dayanıqlılığını risk altına alır.
- Normativ və uyğunluq riskləri – Bulud infrastrukturunun milli qanunvericilik və məlumat mühafizəsi standartlarına tam uyğun olmaması hüquqi və maliyyə risklərinə səbəb olur.
- Daxili işçi və idarəetmə riskləri – Düzgün konfiqurasiya edilməmiş sistemlər və işçi səhvləri təhlükəsizlik boşluqları yaradır.
- İnteroperabillik və inteqrasiya riskləri – Fərqli bulud sistemləri arasında əlaqənin zəif olması məlumat itkiləri və sistem uyğunsuzluqlarına gətirib çıxara bilər.

VI. PROBLEMLƏR, TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ VƏ RİSKLƏRİN HƏLLİ YOLLARI

Bulud suverenliyində qarşıya çıxan maliyyə, texnoloji, kadr və təhlükəsizlik problemləri ilə hüquqi və normativ risklərin effektiv şəkildə idarə olunması üçün milli bulud infrastrukturunun qurulması, hibrid suveren bulud modeli, dövlət tərəfindən açar idarəetməsi, güclü kiber müdafiə, normativ baza və audit sistemi, multi-cloud strategiyası və yerli İT ekosisteminin inkişafı kimi inteqrasiya olunmuş həll yolları tətbiq edilməlidir.

- Milli bulud infrastrukturunun qurulması – Dövlət məlumatlarının ölkə daxilində saxlanması və emalı təmin olunur, kritik məlumatlar xarici təsirdən qorunur, məlumat sızması və geopolitik risklər azalır, milli təhlükəsizlik güclənir.
- Hibrid suveren bulud modeli – Məlumatlar risk səviyyəsinə görə təsnifləndirilir; yüksək məxfilikli məlumatlar milli buludda, az riskli məlumatlar kommersiya buludlarında saxlanır, bu isə təhlükəsizliklə çevikliyi balanslaşdırır.
- Dövlət tərəfindən açar idarəetməsi (Key Management System – KMS) – Şifrələmə açarları tam milli nəzarətdə saxlanılır, provayderlərə giriş məhdudlaşdırılır, məlumatların icazəsiz deşifrə olunması riski minimuma endirilir.
- Kiber müdafiənin gücləndirilməsi – 24/7 təhlükəsizlik əməliyyat mərkəzləri (SOC), milli CERT/CSIRT strukturları, real vaxt hücum aşkarlama sistemləri (SIEM, IDS/IPS) və mütəmmadi penetrasiya testləri ilə hücumlara qarşı dayanıqlılıq artırılır.
- Normativ baza və audit sistemi – ISO 27001, NIST, GDPR-ə uyğun təhlükəsizlik siyasətləri, müstəqil auditlər, risk qiymətləndirmələri və uyğunluq nəzarət mexanizmləri ilə sistemlərin təhlükəsizliyi davamlı şəkildə yoxlanılır.

- Multi-cloud strategiyası – Məlumat və xidmətlərin bir neçə platformaya bölüşdürülməsi bir provayderin sıradan çıxması və ya təhlükəsizlik insidenti zamanı xidmət fasilələrinin qarşısını alır, məlumat itkisi riskini azaldır.
- Yerli IT ekosisteminin inkişafı – Kiber təhlükəsizlik üzrə mütəxəssislərin hazırlanması, etik haker proqramları (bug bounty), milli təhlükəsizlik startaplarının dəstəklənməsi ilə daxili müdafiə potensialı gücləndirilir.

Əlavə təhlükəsizlik yönümlü həllər:

- Məlumatların tam həyat dövrü üzrə qorunması – Toplanma, saxlanma, ötürülmə və silinmə mərhələlərində şifrələmə və giriş nəzarəti tətbiq olunur.
- Zero Trust təhlükəsizlik modeli – Şəbəkə daxilində belə heç bir istifadəçiyə avtomatik etibar olunmur, hər giriş davamlı şəkildə yoxlanılır.
- Fəlakətdən bərpa və ehtiyat nüsxə strategiyası (DR & Backup) – Kiberhücum və texniki nasazlıq hallarında məlumatların sürətli bərpası təmin edilir.
- Daxili təhdidlərin idarə olunması – İşçi girişlərinin monitorinqi, rol əsaslı icazələr və davranış analitikası ilə məlumat sızmalarının qarşısı alınır.

NƏTİCƏ

Rəqəmsal dövlətin bulud suverenliyi, milli məlumatların qorunması, hüquqi uyğunluq, kibertəhlükəsizlik və infrastruktur dayanıqlılığı baxımından strateji əhəmiyyət daşıyır. Analiz nəticələri göstərir ki, suveren bulud texnologiyalarının tətbiqi həm maliyyə, texnoloji və insan resursları baxımından ciddi çətinliklərə səbəb olur, həm də hüquqi və kibertəhlükəsizlik aspektlərində müxtəlif risk və problemlər yaradır. Məqalədə bu problemlərin həlli üçün bir sıra təkliflər irəli sürülür, o cümlədən milli bulud infrastrukturu, hibrid suveren bulud modeli, dövlət tərəfindən açar idarəetməsi, kiber müdafiənin gücləndirilməsi, normativ baza və audit sistemi, multi-cloud strategiyası və yerli IT ekosisteminin inkişafı. Bu tədbirlər dövlətin rəqəmsal müstəqilliyini gücləndirməyə və bulud suverenliyini dayanıqlı şəkildə təmin etməyə xidmət edir.

ƏDƏBİYYAT

[1] S. Galij, G. Pawlak, S. Grzyb, Modeling Data Sovereignty in Public Cloud—A Comparison of Existing Solutions. Applied Sciences, 14(23), Article 10803, 2024.
DOI: https://doi.org/10.3390/app142310803

[2] J. Rone, The Sovereign Cloud' in Europe: Diverging Nation State Preferences and Disputed Institutional Competences. Journal of European Public Policy, 2024, pp. 2343–2369.
DOI: https://doi.org/10.1080/13501763.2024.2348618

[3] A. Baur, European Dreams of the Cloud: Imagining Innovation and Political Control. Geopolitics, 2023, pp. 796–820
DOI: https://doi.org/10.1080/14650045.2022.2151902

[4] A. D. Mitchell, T. Samlidis, Cloud Services and Government Digital Sovereignty in Australia and Beyond. International Journal of Law and Information Technology, Volume 29, Issue 4, 2022, pp. 364–394.
DOI: https://doi.org/10.1093/ijlit/eaac003

[5] C. Joel, Digital Sovereignty Enforcement via Confidential Cloud Computation Models. International Journal of Cloud Security (IJCDS), Volume 4, Issue 1, 2023, pp. 1-8.

[6] M. Tang, The Challenge of the Cloud: Between Transnational Capitalism and Data Sovereignty. Information, Communication & Society, 2022, pp. 2397–2411.
DOI: https://doi.org/10.1080/1369118X.2022.2128598

[7] F.G. Blancato, The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet, 2023, 16 (1), pp. 12-32. DOI: 10.1002/poi3.358

[8] B. Jansen, N. Kadenko, D. Broeders and etc., Pushing boundaries: An empirical view on the digital sovereignty of six governments. Government Information Quarterly, Volume 40, Issue 4, October 2023, 101862. DOI: 10.1016/j.giq.2023.101862

Digital State Cloud Sovereignty: Current State, Problems, Security, Risks, and Solutions

Ogtay Alakbarov

Institute of Information Technology, Baku, Azerbaijan

Abstract— The acceleration of digitalization has led to the widespread adoption of cloud technologies in public administration. However, storing data with foreign providers creates serious risks in terms of national security, legal independence, and cybersecurity. For this reason, the concept of cloud sovereignty has become one of the key pillars of the digital state framework. This article analyzes the conceptual foundations and components of cloud sovereignty, as well as the existing problems, threats, and risks associated with it. In addition, effective solution approaches are proposed.

Keywords— digital state; cloud sovereignty; information security; national cloud infrastructure; cyber risks; legal independence; hybrid cloud model.