Elektron Dövlət Mühitində Kibersuverenliyin Təmin Edilməsi və Milli Kibertəhlükəsizliyin Konseptual Modelinin İşlənməsi

Babək Nəbiyev[1], Könül Daşdəmirova[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
babek.nabiyev@gmail.com[1], konulahmed@gmail.com[2]

***Xülasə*— Müasir dövrdə rəqəmsal transformasiya dövlətlərin suverenlik anlayışına yeni məzmun qazandıraraq kiberməkanı milli təhlükəsizliyin əsas komponentlərindən birinə çevirmişdir. Məqalədə kibersuverenlik anlayışı elektron dövlət mühitində təhlil olunur, qloballaşma şəraitində yaranan rəqəmsal asılılıqların riskləri araşdırılır və milli səviyyədə kibertəhlükəsizliyin təmin edilməsi üçün konseptual model təklif edilir. Tədqiqat çərçivəsində Whole-of-Government və Whole-of-Society yanaşmaları əsasında çoxsəviyyəli idarəetmə mexanizmləri, hüquqi-normativ baza və texnoloji arxitektura inteqrativ şəkildə təhlil edilmişdir. Eyni zamanda Milli Kibertəhlükəsizlik Sistemi və onun ölçülə bilən komponenti kimi Milli Kibertəhlükəsizlik İndeksinin strukturu və funksional modeli təqdim olunur. Təklif edilən yanaşma kibersuverenliyin təmin olunmasını ölçülə bilən, analitik və proqnozlaşdırıla bilən idarəetmə müstəvisinə keçirməyə imkan verir.**

Açar sözlər— kibersuverenlik; kibertəhlükəsizlik; elektron dövlət; rəqəmsal transformasiya.

I. GİRİŞ

Rəqəmsal texnologiyaların sürətli inkişafı nəticəsində dövlətlərin idarəetmə modelləri fundamental dəyişikliklərə məruz qalmışdır. İnformasiya və kommunikasiya texnologiyalarının dövlət idarəçiliyinə inteqrasiyası elektron dövlət mühitinin formalaşmasına səbəb olmuş və bu mühitdə məlumat axınlarının idarə olunması strateji əhəmiyyət kəsb etməyə başlamışdır. Bu kontekstdə kibersuverenlik anlayışı yalnız texnoloji deyil, həm də siyasi, hüquqi və sosial aspektləri özündə birləşdirən kompleks yanaşma kimi çıxış edir.

Kibersuverenlik dövlətin rəqəmsal məkan üzərində müstəqil qərarvermə imkanlarını, informasiya axınlarına nəzarəti və milli məlumat resurslarının qorunmasını təmin edən əsas konsepsiyadır. Bu anlayış artıq ənənəvi suverenlik komponentləri ilə yanaşı, kiberməkanın da milli təhlükəsizliyin beşinci elementi kimi qəbul edilməsini zəruri edir. Elektron dövlət mühitində kibersuverenliyin təmin edilməsi yalnız texniki tədbirlərlə deyil, kompleks idarəetmə, hüquqi tənzimləmə və institusional inteqrasiya ilə mümkündür.

II. KİBERSUVERENLİK VƏ RƏQƏMSAL ASILILIQLARIN TƏHLİLİ

Qloballaşma şəraitində rəqəmsal ekosistemlərdə formalaşan asılılıqlar kibersuverenlik üçün əsas çağırışlardan biri hesab olunur. Müasir dövlətlər bulud texnologiyaları, beynəlxalq proqram platformaları və xarici məlumat mərkəzləri üzərində artan asılılıq səbəbindən informasiya təhlükəsizliyi riskləri ilə üzləşirlər [1]. Bu vəziyyət milli məlumatların digər ölkələrin yurisdiksiyasına düşməsi, xidmətlərin dayandırılması və ya manipulyasiya olunması kimi təhlükələri aktuallaşdırır.

Bununla yanaşı, qlobal rəqəmsal platformalar ictimai rəyin formalaşdırılmasında mühüm rol oynayaraq informasiya müharibəsi və "soft power" mexanizmlərinin tətbiqinə imkan yaradır. Beləliklə, kibersuverenlik yalnız texnoloji müstəqillik deyil, həm də informasiya mühitinin qorunması və ideoloji təhlükəsizliyin təmin olunması kimi aspektləri də əhatə edir [2].

Bu problemlərin həlli üçün dövlət, özəl sektor və cəmiyyət arasında koordinasiyalı fəaliyyət tələb olunur. Whole-of-Government yanaşması dövlət qurumları arasında vahid koordinasiya və məlumat mübadiləsini təmin edərək qərarvermə prosesinin effektivliyini artırır. Whole-of-Society yanaşması isə kibertəhlükəsizliyi cəmiyyətin bütün təbəqələrinin ortaq məsuliyyəti kimi müəyyən edir və maarifləndirmə, təhsil və etik davranış kimi faktorların əhəmiyyətini ön plana çıxarır [3].

III. HÜQUQİ VƏ İNSTİTUSİONAL ÇƏRÇİVƏ

Kibersuverenliyin təmin olunması üçün hüquqi baza əsas rol oynayır. Azərbaycan Respublikasında informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində qəbul edilmiş normativ sənədlər bu istiqamətdə mühüm hüquqi çərçivə formalaşdırır. Bu sənədlərə informasiya təhlükəsizliyi haqqında qanunlar, kritik informasiya infrastrukturunun qorunması ilə bağlı fərmanlar və milli strategiyalar daxildir.

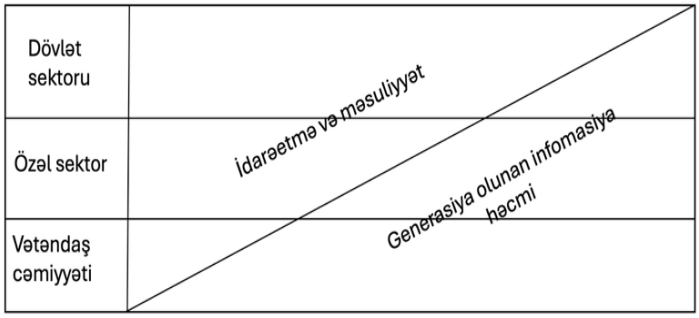
Beynəlxalq səviyyədə isə Budapeşt Konvensiyası, NIS2 direktivi, ENISA çərçivələri və OECD tövsiyələri kimi sənədlər kibertəhlükəsizliyin qlobal standartlarını müəyyən edir. Bu standartlara uyğunlaşma milli sistemlərin beynəlxalq inteqrasiyasını təmin etməklə yanaşı, kibersuverenliyin qorunmasına da töhfə verir [4, 5]. Hüquqi çərçivənin effektivliyi yalnız sənədlərin mövcudluğu ilə deyil, onların tətbiq səviyyəsi və monitorinq mexanizmləri ilə müəyyən olunur. Bu baxımdan, hüquqi və institusional komponentlərin vahid sistemdə inteqrasiyası zəruridir.

DOI: 10.25045/cyber.gov.2026.11

IV. MİLLİ KİBERTƏHLÜKƏSİZLİK SİSTEMİNİN KONSEPTUAL MODELİ

Elektron dövlət mühitində kibersuverenliyin təmin edilməsi üçün Milli Kibertəhlükəsizlik Sistemi (MKTS) konseptual model kimi təklif olunur. Bu sistem dövlət, özəl sektor, elm və cəmiyyət arasında əlaqələndirilmiş fəaliyyət mexanizmi yaradaraq kibertəhlükəsizliyin proaktiv idarə olunmasını təmin edir [6].

Təqdim olunan şəkil 1-də dövlət sektoru, özəl sektor və vətəndaş cəmiyyəti arasında funksional bölgünü və qarşılıqlı asılılığı konseptual şəkildə əks etdirir. Diaqonal xətt boyunca idarəetmə və məsuliyyətin dövlət sektoruna doğru artdığı, əks istiqamətdə isə generasiya olunan informasiya həcminin vətəndaş cəmiyyəti səviyyəsində maksimuma çatdığı müşahidə olunur. Özəl sektor bu iki müstəvi arasında aralıq mövqe tutaraq həm idarəetmə proseslərində iştirak edir, həm də əhəmiyyətli informasiya axınının formalaşmasına töhfə verir. Beləliklə, model rəqəmsal mühitdə müxtəlif aktorlar arasında rol bölgüsünü və onların sistem daxilində funksional tarazlığını baxımdan ümumiləşdirir.



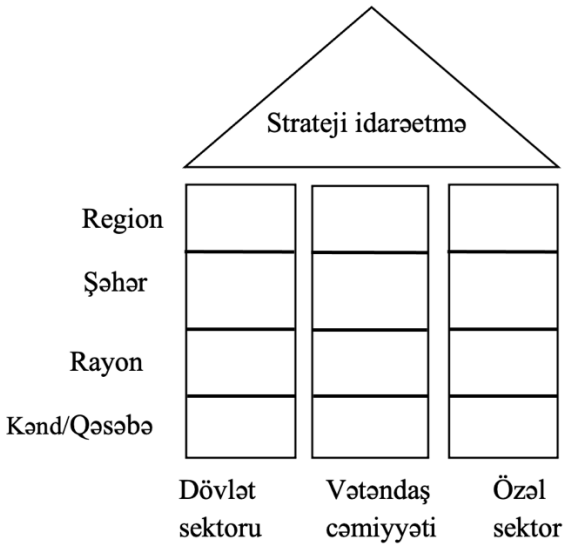
Şəkil 1. Funksional bölgünü

MKTS-in əsas məqsədi milli rəqəmsal məkan üzərində nəzarətin təmin edilməsi, risklərin erkən aşkarlanması və təhlükəsizlik tədbirlərinin koordinasiyalı şəkildə həyata keçirilməsidir. Sistem kiberdayanıqlılıq prinsipinə əsaslanaraq yalnız müdafiə deyil, həm də adaptasiya və davamlı inkişaf yanaşmasını tətbiq edir.

Texnoloji baxımdan MKTS çoxqatlı arxitekturaya malikdir. Məlumatların toplanması, monitorinq, analitik emal, qərarvermə və proqnozlaşdırma qatları bir-biri ilə inteqrasiya olunaraq vahid idarəetmə mühiti yaradır. Süni intellekt və böyük verilənlər texnologiyalarının tətbiqi isə sistemin proaktiv təhlükəsizlik imkanlarını genişləndirir [7].

Secure-by-Design yanaşması bu modelin əsas prinsiplərindən biri kimi çıxış edir və təhlükəsizliyin sistemin ilkin dizayn mərhələsində inteqrasiya olunmasını təmin edir. Bu isə sonradan yaranan zəifliklərin minimuma endirilməsinə imkan verir.

Təqdim olunan model çoxsəviyyəli və çoxtərəfli idarəetmə yanaşmasını əks etdirərək strateji idarəetmənin (yüksək səviyyə), müxtəlif inzibati-coğrafi səviyyələr (region, şəhər, rayon, kənd/qəsəbə) üzrə tətbiqini və eyni zamanda üç əsas aktor qrupunun dövlət sektoru, vətəndaş cəmiyyəti və özəl sektorun paralel və qarşılıqlı əlaqəli iştirakını sistemli şəkildə



Şəkil 2. Strateji idarəetmə modeli

göstərir (Şəkil 2). Modelin strukturunda şaquli ox idarəetmənin ərazi üzrə iyerarxiyasını, üfüqi istiqamət isə idarəetmədə iştirak edən institusional tərəflərin bölünməsini ifadə edir; bu isə hər bir səviyyədə qərarların yalnız mərkəzləşdirilmiş deyil, həm də inklüziv və çoxtərəfli mexanizmlər əsasında formalaşmasını təmin edir. Belə yanaşma xüsusilə müasir idarəetmə konsepsiyalarına Whole-of-Government (WGA) və Whole-of-Society (WoS) prinsiplərinə uyğun olaraq, müxtəlif maraqlı tərəflərin koordinasiyasını, resursların effektiv bölgüsünü və strateji qərarların yerli səviyyələrə adaptasiyasını təmin etməyə xidmət edir. Nəticə etibarilə, bu model kompleks sosial-texniki sistemlərin, o cümlədən rəqəmsal transformasiya və kibertəhlükəsizlik kimi sahələrin idarə olunmasında inteqrativ və dayanıqlı idarəetmə çərçivəsi kimi çıxış edir.

V. MİLLİ KİBERTƏHLÜKƏSİZLİK İNDEKSİ VƏ ÖLÇMƏ MODELİ

Kibertəhlükəsizliyin effektiv idarə olunması üçün onun ölçülə bilən olması vacibdir. Bu məqsədlə Milli Kibertəhlükəsizlik İndeksi (MKİ) təklif olunur. MKİ kibertəhlükəsizlik sahəsində mövcud vəziyyətin qiymətləndirilməsi, müqayisə edilməsi və qərarvermə prosesinin dəstəklənməsi üçün analitik alət kimi çıxış edir [5].

MKİ hüquqi, texnoloji, institusional və sosial indikatorların inteqrasiyasına əsaslanır. Bu indikatorlar vasitəsilə müxtəlif sektorlar üzrə kibertəhlükəsizlik səviyyəsi ölçülür və inkişaf dinamikası təhlil olunur.

İndeksin işləmə mexanizmi verilənlərin toplanması, normallaşdırılması, qiymətləndirilməsi, skorlama və vizuallaşdırma mərhələlərindən ibarətdir. Bu proses nəticəsində əldə olunan göstəricilər dövlət siyasətinin formalaşdırılmasında və resursların effektiv bölüşdürülməsində istifadə olunur [2,7].

MKİ-nin tətbiqi kibertəhlükəsizlik sahəsində şəffaflıq və hesabatlılıq səviyyəsini artırmaqla yanaşı, beynəlxalq indekslərlə uyğunluğun təmin edilməsinə də imkan yaradır. Bu

isə ölkənin qlobal kibertəhlükəsizlik mühitində mövqeyini gücləndirir.

NƏTİCƏ

Tədqiqat nəticələri göstərir ki, kibersuverenlik müasir dövlətlərin milli təhlükəsizlik sistemində əsas komponentlərdən biri kimi çıxış edir və onun təmin edilməsi kompleks yanaşma tələb edir. Elektron dövlət mühitində kibertəhlükəsizliyin təmin olunması yalnız texnoloji tədbirlərlə məhdudlaşmır, hüquqi, institusional və sosial mexanizmlərin inteqrasiyasını tələb edir.

Təklif olunan Milli Kibertəhlükəsizlik Sistemi və Milli Kibertəhlükəsizlik İndeksi modeli kibersuverenliyin təmin olunmasını sistemli və ölçülə bilən müstəviyə keçirir. Bu yanaşma dövlətin kiberməkanda dayanıqlılığını artırmaqla yanaşı, risklərin proaktiv idarə olunmasına və strateji qərarların elmi əsaslarla qəbuluna şərait yaradır.

Gələcək tədqiqatlarda süni intellekt əsaslı analitik modellərin təkmilləşdirilməsi, sektorlararası məlumat inteqrasiyasının genişləndirilməsi və beynəlxalq əməkdaşlığın gücləndirilməsi istiqamətləri prioritet olaraq müəyyən edilə bilər.

ƏDƏBİYYAT

[1] M. Carr, "Public–private partnerships in national cyber-security strategies," International Affairs, vol. 92, no. 1, pp. 43–62, 2016.

[2] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?" Journal of Computer Security, vol. 19, no. 1, pp. 33–56, 2011.

[3] S. Shackelford, "Toward cyberpeace: Managing cybersecurity through polycentric governance," American University Law Review, vol. 62, no. 5, pp. 1273–1344, 2013.

[4] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," European Union Agency for Cybersecurity, Athens, Greece, 2018.

[5] ITU, "Global Cybersecurity Index (GCI) 2020," International Telecommunication Union, Geneva, Switzerland, 2021.

[6] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.

[7] E. Bertino, "Data security and privacy: Concepts, approaches, and research directions," IEEE Transactions on Big Data, vol. 2, no. 1, pp. 1–13, 2016.

Ensuring cyber sovereignty in the e-government environment and developing a conceptual model of national cybersecurity

Babak Nabiyev[1], Konul Dashdemirova[2]

[1,2]Institute of Information Technology, Baku, Azerbaijan

Abstract— In the modern era, digital transformation has given new content to the concept of sovereignty of states and turned cyberspace into one of the main components of national security. The article analyzes the concept of cyber sovereignty in the e-government environment, examines the risks of digital dependencies arising in the context of globalization, and proposes a conceptual model for ensuring cybersecurity at the national level. Within the framework of the study, multi-level governance mechanisms, legal and regulatory framework, and technological architecture are analyzed in an integrative manner based on the Whole-of-Government and Whole-of-Society approaches. At the same time, the structure and functional model of the National Cybersecurity System and the National Cybersecurity Index as its measurable component are presented. The proposed approach allows to transfer the provision of cyber sovereignty to a measurable, analytical and predictable management level.

Keywords— cyber sovereignty; cybersecurity; e-government; digital transformation.