Kibersuverenliyin Təmin Olunması üçün Milli Kibertəhlükəsizlik Sisteminin Formalaşdırılması Mexanizmləri

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

***Xülasə*— Elektron dövlət mühitində informasiya-kommunikasiya texnologiyalarından geniş istifadə edilməsi, eləcə də milli təhlükəsizliyi təşkil edən bütün sahələrin kiberməkana inteqrasiyası informasiya təhlükəsizliyi problemlərinin aktuallaşmasına səbəb olmuşdur. Tədqiqatda kibermühitdə informasiya təhlükəsizliyinin milli təhlükəsizliyin və kibersuverenliyin təmin olunması üçün əsas komponentlərdən birinə çevrilməsi ön plana çəkilmişdir. Qlobal mühitdə kibersuverenliyi təmin etmək və milli kiberməkan üzərində effektiv nəzarəti həyata keçirmək üçün Milli Kibertəhlükəsizlik Sistemlərinin yaradılması təklif edilmişdir.**

Açar sözlər*— *milli təhlkükəsizlik; kibersuverenlik; informasiya təhlekəsizliyi; milli kiberməkan.

I. GİRİŞ

Müasir dövrdə qloballaşma prosesinin sürətlənməsi, rəqəmsal texnologiyaların geniş yayılması və beynəlxalq münasibətlər sistemində baş verən dəyişikliklər təhlükəsizlik anlayışını köklü surətdə dəyişir. Rəqəmsal texnologiyaların tətbiqi nəticəsində dövlət idarəçiliyi, ictimai xidmətlər və kommunikasiya sistemləri kiberməkana inteqrasiya edir. Bu yeni imkanlar yaratmaqla yanaşı, çoxsaylı kibertəhlükələr də formalaşdırır [1]. Milli kiberməkan üzərində nəzarətin gücləndirilməsi, informasiya təhlükəsizliyinin təmin edilməsi və rəqəmsal müstəqilliyin qorunması problemləri aktuallaşır.

Ənənəvi təhlükəsizlik yanaşmalarda hərbi və siyasi sahələrə üstünlük verilsə də, hazırda milli təhlükəsizlik fiziki sərhədlərin qorunması ilə məhdudlaşmır, eyni zamanda dövlətin milli informasiya məkanını, rəqəmsal infrastrukturunu və texnoloji müstəqilliyini də əhatə edir. Rəqəmsal texnologiyaların geniş tətbiqi və məlumat mübadiləsinin bu texnologiyalar üzərindən aparılması kibersuverenlik anlayışını milli təhlükəsizliyin ayrılmaz tərkib hissəsinə çevirir [2].

Kibersuverenlik dövlətin öz rəqəmsal məkanı üzərində nəzarət imkanlarını, milli informasiya resurslarının qorunmasını və kiberməkanda müstəqil qərarvermə qabiliyyətini ifadə edir. Müasir şəraitdə dövlətlərin siyasi, iqtisadi və sosial sabitliyi getdikcə daha çox rəqəmsal sistemlərdən asılı olduğundan, kiberməkanda təhlükəsizliyin təmin olunması birbaşa milli təhlükəsizliyin təmin olunması ilə bağlıdır. Belə şəraitdə kibertəhlükəsizlik və kibersuverenlik strateji və milli maraqların qorunması üçün əsas vasitə kimi çıxış edir.

Təqdim olunan tezisdə milli təhlükəsizlik anlayışına beynəlxalq və milli yanaşmalar, kiberməkanda yaranan müasir çağırışlar, kibersuverenlik məsələləri, milli kibertəhlükəsizliyin əsas problemləri və bu sahədə effektiv idarəetmə mexanizmi kimi Milli Kibertəhlükəsizlik Sisteminin formalaşdırılması təklif olunur.

II. "MİLLİ TƏHLÜKƏSİZLİK" ANLAYIŞINA BİRLƏŞMİŞ MİLLƏTLƏR TƏŞKİLATININ VƏ AZƏRBAYCAN RESPUBLİKASININ YANAŞMASI

Birləşmiş Millətlər Təşkilatının (BMT) təhlükəsizlik anlayışını yalnız dövlət sərhədlərinin və suverenliyinin qorunması ilə məhdudlaşdırmır. BMT-nin yanaşmasına görə təhlükəsizlik həm dövlətlərin, həm də xalqların və ayrı-ayrı fərdlərin təhlükəsizliyini əhatə edən kompleks bir anlayışdır. Davamlı inkişaf, sosial rifahın təmin olunması, iqtisadi sabitlik və ətraf mühitin qorunması kimi amillər də təhlükəsizlik sisteminin mühüm komponentləri hesab olunur [3].

BMT-nin təhlükəsizlik konsepsiyasında dövlətlərarası münasibətlərin tənzimlənməsi ilə yanaşı, cəmiyyətlər və xalqlar arasında mövcud olan sosial gərginliklərin, qarşıdurmaların və münaqişələrin aradan qaldırılması, beynəlxalq sülhün və əməkdaşlığın qorunması əsas prioritet istiqamətlərdən biri kimi müəyyən edilmişdir. Bu yanaşma təhlükəsizliyin sosial, humanitar və iqtisadi aspektlərdə də təmin edilməsinin vacibliyini ön plana çıxarır.

Milli təhlükəsizliyin müasir çağırışlara uyğun şəkildə təmin olunması istiqamətində Azərbaycan Respublikasında da mühüm normativ-hüquqi baza formalaşdırılmışdır. Bu sahədə əsas strateji sənədlərdən biri "Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyasının təsdiq edilməsi haqqında" Azərbaycan Respublikası Prezidentinin sərəncamıdır [4]. Konsepsiyaya əsasən Azərbaycan Respublikasının təhlükəsizlik mühiti dövlətin suverenliyinə, ərazi bütövlüyünə, sərhədlərinin toxunulmazlığına, milli maraqlarına, davamlı inkişafına, həmçinin əhalinin rifahının və milli dəyərlərinin qorunmasına təsir göstərən amillərin məcmusu kimi müəyyən edilir.

DOI: 10.25045/cyber.gov.2026.22

Sonrakı dövrlərdə milli təhlükəsizliyin müxtəlif istiqamətlərini əhatə edən bir sıra mühüm normativ-hüquqi sənədlər qəbul edilmişdir. Bu sənədlər sırasında “Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi ilə bağlı tədbirlər haqqında” fərman, “İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə 2023–2027-ci illər Strategiyası”, “Rəqəmsal İnkişaf Konsepsiyası”, “Azərbaycan Respublikasının 2025–2028-ci illər üçün süni intellekt Strategiyası”, həmçinin “Azərbaycan Respublikasında məhkəmə ekspertizası sahəsinin inkişafına dair 2026–2030-cu illər üçün Konsepsiya” xüsusi əhəmiyyət daşıyır [5].

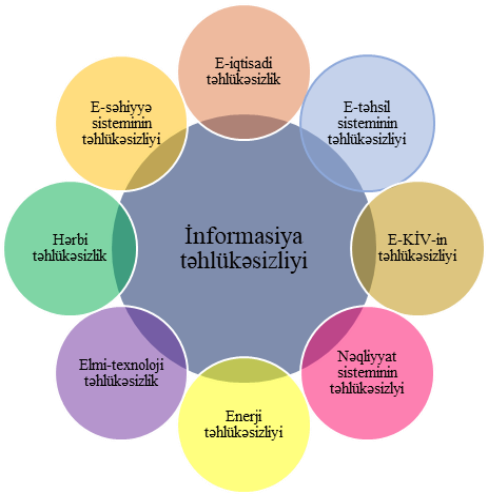
III. MİLLİ TƏHLÜKƏSİZLİK VƏ KİBERSUVERENLİK KONTEKSTİNDƏ MÜASİR YANAŞMALAR

Müasir təhlükəsizlik konsepsiyalarında fərdin, cəmiyyətin və dövlətin təhlükəsizliyinin təmin olunması bütövlükdə milli təhlükəsizlik anlayışı formalaşdırır. Bu yanaşmaya görə təhlükəsizlik həm dövlət institutlarının qorunması, həm də cəmiyyətin sabitliyi, vətəndaşların təhlükəsizliyi və milli maraqların qorunmasını əhatə edir [6].

Milli təhlükəsizlik mürəkkəb, çoxsəviyyəli və dinamik xarakterə malik olan bir sistemdir və dövlət fəaliyyətinin bütün sahələrini (siyasi, iqtisadi, hərbi, sosial və s.) əhatə edir (Şəkil 1). Bu sistem daxilində təhlükəsizliyin müxtəlif komponentləri bir-biri ilə sıx əlaqədə fəaliyyət göstərir və onların hər biri ümumi təhlükəsizlik mexanizminin ayrılmaz tərkib hissəsi hesab olunur. Milli təhlükəsizliyin ayrı-ayrı sahələrinin təhlükəsizliyi digər sahələrin təhlükəsizliyinin təmin edilməsindən asılıdır və hər hansı bir istiqamətdə yaranan problemlər digər sahələrə də mənfi təsir göstərə bilər [7].

Rəqəmsal texnologiyaların sürətli inkişafı fonunda milli təhlükəsizliyi əhatə edən bütün sahələr rəqəmsəl mühitə inkikas edir. Bu sahələrin kiberməkana inteqrasiyası həm yeni imkanlar, həm də yeni təhlükələr yaradır. Müasir dövlətlər idarəetmə prosesində, ictimai xidmətlərin göstərilməsində və əhali ilə kommunikasiya qurulmasında rəqəmsal texnologiyalardan geniş şəkildə istifadə edirlər. İnformasiya-

Şəkil 1. Milli təhlükəsizliyi əhatə edən sahələr



Şəkil 2. İnformasiya təhlükəsizliyi milli təhlükəsizliyin nüvəsi kimi

kommunikasiya texnologiyalarının tətbiqi dövlət idarəçiliyinin effektivliyini artırsa da, eyni zamanda dövlət qurumlarını və kritik infrastrukturları kibertəhlükələr qarşısında daha həssas vəziyyətə gətirə bilər.

Belə şəraitdə informasiya təhlükəsizliyi artıq milli təhlükəsizliyin sadəcə bir komponenti kimi deyil, dövlətin funksionallığını, idarəetmə sisteminin davamlılığını və cəmiyyətin sabit fəaliyyətini təmin edən strateji sistemin nüvəsi kimi çıxış edir (Şəkil 2).

İnformasiya təhlükəsizliyi çətiri altında çoxsaylı təhlükəsizlik anlayışları meydana gəlir (Şəkil 3)

Hazırda internet və rəqəmsal kommunikasiya sistemləri qlobal siyasi, iqtisadi rəqabətin mühüm alətlərindən birinə çevrilmişdir. Dövlətlər, eləcə də müxtəlif qeyri-dövlət aktorları və terror təşkilatları kiberməkan üzərində nəzarəti ələ keçirmək, siyasi, iqtisadi və ideoloji təsir imkanlarını genişləndirmək məqsədilə kiberhücumlardan istifadə edirlər. Bu isə kiberməkanı faktiki olaraq qlobal rəqabət və qarşıdurma müstəvisinə çevirmişdir.

Kiberməkanın xüsusiyyətlərindən biri onun quru, dəniz və hava kimi təbii sərhədlərə malik olmamasıdır. Rəqəmsal şəbəkələr üzərində qurulan bu mühitdə dövlətlərin suverenliyi yalnız fiziki ərazi ilə məhdudlaşmır, eyni zamanda onların rəqəmsal infrastrukturlarını və informasiya məkanını da əhatə edir. Bununla belə, beynəlxalq səviyyədə kiberməkanın fəaliyyətini tənzimləyən məcburi hüquqi normaların və ümumi qəbul edilmiş qaydaların kifayət qədər formalaşmaması bu sahədə müəyyən boşluqlar yaratmış və kiberməkanın müəyyən dərəcədə nəzarətsiz qalmasına səbəb olmuşdur.

Kibertəhlükəsizlik sahəsində əsas problemlərdən biri hücumların mənbəyinin və məqsədinin dəqiq müəyyən edilməsinin çətinliyidir. Kiberhücumların anonim xarakter daşıması və müxtəlif vasitələrlə gizlədilməsi hücumun hansı dövlət və ya qrup tərəfindən həyata keçirildiyini müəyyənləşdirməyi çətinləşdirir.

Şəkil 3. İnformasiya təhlükəsizliyi çətiri altında yaranmış təhlükəsizlik anlayışları

təhlükəsizlik siyasətində yeni risklər yaradır. Xüsusilə informasiya müharibəsində məğlubiyyət hər hansı bir ölkənin siyasi, iqtisadi və sosial sabitliyinə ciddi mənfi təsir göstərə bilər.

Məhz bu səbəbdən son illərdə bir sıra dövlətlər suveren kiberməkan konsepsiyasını inkişaf etdirməyə başlamışdır [8]. Bu yanaşma milli səviyyədə daha sərt tənzimlənən və dövlət nəzarəti altında olan kibermühitin formalaşdırılmasını nəzərdə tutur. Suveren kiberməkanın yaradılması dövlətlərin öz rəqəmsal infrastrukturlarını qorumaq, informasiya təhlükəsizliyini təmin etmək və kiberməkan üzərində milli nəzarəti gücləndirmək məqsədi daşıyır. Milli informasiya məkanında kibersuverenliyin təmin olunması milli təhlükəsizlik sisteminin əsas komponentlərindən birinə çevrilir.

IV. MİLLİ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİ

Milli kibertəhlükəsizliyin təmin olunması kontekstdə aşağıdakı bir sıra əsas problemlər aktuallaşır.

- Texnoloji asılılıq: Xarici bulud xidmətlərinə, proqram təminatına və kritik infrastrukturda istifadə olunan texnologiyalara yüksək bağlılıq dövlətin öz verilənləri və prosesləri üzərində nəzarət imkanlarını zəiflədir. Bu asılılıq istənilən vaxt siyasi və kommersiya təzyiqinə çevrilə bilər.
- Kiberhücumlara qarşı zəiflik: DDoS, ransomware və s. kimi hücumlar dövlət xidmətlərini iflic edə, strateji məlumatları ələ keçirə və kritik infrastrukturu sıradan çıxara bilər. Bu vəziyyət milli təhlükəsizlik orqanlarının informasiya idarəetmə qabiliyyətini məhdudlaşdırır.
- İnformasiya manipulyasiyası və psixoloji təsir: Xarici qüvvələr rəqəmsal platformalar vasitəsilə ictimai rəyi formalaşdıraraq, dezinformasiya yaymaqla siyasi proseslərə təsir göstərə bilər. Bu isə informasiya suverenliyinin itməsi və ictimai sabitliyin pozulması deməkdir.
- Milli verilənlərin nəzarətdən çıxması: Vətəndaşların fərdi məlumatlarının və dövlətin strateji informasiya bazalarının xarici serverlərdə saxlanılması, milli resursların başqa ölkələrin və ya şirkətlərin nəzarətinə keçməsi ciddi təhlükə yaradır.
- Hüquqi və normativ boşluqlar: Kiberməkanın tənzimlənməsi üzrə milli qanunvericiliyin zəifliyi, beynəlxalq hüquqda isə bu sahədəki boşluqlar dövlətlərin kibersuverenliyini qorumaqda çətinlik yaradır.
- İqtisadi və kadr potensialı amili: Yerli texnoloji istehsalın, kibertəhlükəsizlik mütəxəssislərinin və rəqəmsal savadlılığın çatışmazlığı dövlətin rəqəmsal müstəqilliyini məhdudlaşdırır.
- Geosiyasi və diplomatik təsirlər: Qlobal rəqəmsal güclər arasındakı mübarizə, sanksiyalar və texnoloji blokadalar milli kibersuverenliyə təhdid yaradır.
- Milli-mənəvi irsin qorunması: qloballaşma şəraitində xarici adət-ənənələrin cəmiyyətə nəzarətsiz şəkildə aşılanması milli dəyərlərin tədricən zəifləməsi, adət-ənənələrin və milli kimliyin unudulması təhlükəsi yaradır.

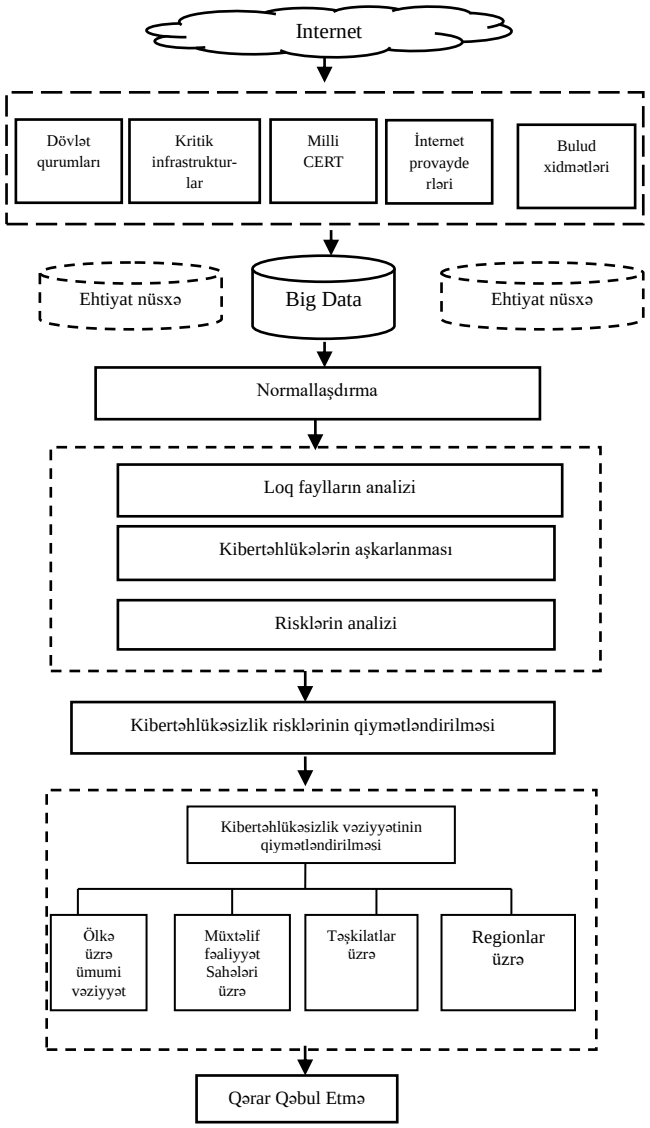
V. MİLLİ KİBERTƏHLÜKƏSİZLİK SİSTEMİNİN ARXİTEKTUR-TEXNOLOJİ MODELİ

Müasir kibermühitdə milli təhlükəsizliyin təmin olunmasının əsas istiqamətlərindən biri ölkə səviyyəsində loq

Bu isə dövlətlərin məlumatlarının sistemli şəkildə toplanması, analizi və monitorinqinin təşkilidir. Loq məlumatları yalnız ayrı-ayrı təşkilatların fəaliyyətini izləmək üçün deyil, bütövlükdə milli kiberməkanın təhlükəsizlik vəziyyətinin monitorinqi və təhlili üçün əsas informasiya mənbəyidir.

Tədqiqat işində Milli Kibertəhlükəsizlik Sisteminin formalaşdırılması təklif olunur. Milli Kibertəhlükəsizlik Sisteminin əsas məqsədi ölkə səviyyəsində müxtəlif mənbələrdən toplanan loq fayllarının təhlili əsasında milli informasiya məkanında mövcud olan sosial miqyaslı kibertəhlükələrin aşkarlanması, onların sistemli şəkildə təhlil edilməsi, risk səviyyəsinin qiymətləndirilməsi və bu təhdidlərin qarşısının alınması üçün effektiv mexanizmlərin formalaşdırılmasından ibarətdir (Şəkil 4).

İlkin mərhələdə müxtəlif mənbələrdən loq fayllar toplanır. Müxtəlif mənbələrdən toplanmış loq fayllarının vahid verilənlər bazasında birləşdirilməsi Big Data mühiti yaradır. Bu mühitdə Maşın Təlimi metodlarını tətbiq edərək kibertəhlükələr aşkarlanır.



Şəkil 4. Milli Kibertəhlükəsizlik Sisteminin arxitektur-texnoloji modeli

Aşkarlanmış kibertəhlükələr müxtəlif əlamətlərə görə siniflərə bölünür, kibertəhlükəsizlik riskləri analiz olunur. Kibertəhlükəsizlik risklərinin və kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi həyata keçirilir.

NƏTİCƏ

Milli Kibertəhlükəsizlik Sistemi milli informasiya məkanına yönəlmiş daxili və xarici kibertəhdidlərin müəyyənləşdirilməsi, müxtəlif sektorlar üzrə kibertəhlükəsizlik vəziyyətinə dair analitik hesabatların hazırlanması və ölkə üzrə ümumi kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi baxımından mühüm rol oynayacaqdır. Bu sistem vasitəsilə toplanan və emal olunan məlumatlar dövlət qurumlarının qərar qəbuletmə prosesində mühüm informasiya mənbəyi kimi çıxış edə bilər.

ƏDƏBİYYAT

[1] R.Alguliyev, B. Nabiyev, K. Dashdamirova, "Cyber threats and their intellectual analysis issues in the context of technological challenges of the IV Industrial Revolution," 2023 IEEE 17th International Conference on Application of Information and Communication Technologies (AICT), IEEE, 2023, pp. 1-6.

[2] Y.Hong, G. T. Goodnight, "How to think about cyber sovereignty: The case of China ," China's globalizing internet, Routledge, 2022, pp. 7-25.

[3] A. Roberts, "The United Nations and international security," Survival, 1993, T. 35, №. 2, pp. 3-30.

[4] Azərbaycan Respublikasının milli təhlükəsizlik konsepsiyasının təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin Sərəncamı, https://e-qanun.az/framework/13373

[5] AR Ədliyyə Nazirliyi Hüquqi aktların vahid elektron bazası, https://e-qanun.az/

[6] R.S. Mahmudova et al., "Analysis of information security problems in the information society environment //Problems of Information Society," 2021? pp. 83-94.

[7] R.M. Əliquliye., Y.N.İmamverdiyev, R.Ş. Mahmudov, " İnformasiya təhlükəsizliyi milli təhlükəsizliyin mühüm komponenti kimi," Problems of Information Society Institute of Information Technology of Azerbaijan National Academy of Sciences, 2020, T. 11, №. 1, pp. 3-25.

[8] A.Barrinha, "Christou Speaking sovereignty: the EU in the cyber domain," European security, 2022, T. 31, №. 3, pp. 356-376.

Mechanisms for Forming a National Cybersecurity System to Ensure Cybersovereignty

Babak Nabiyev[1], Konul Dashdemirova[2]

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

Abstract— The widespread use of information and communication technologies in the e-government environment, as well as the integration of all areas that constitute national security into cyberspace, has led to the relevance of information security problems. The study highlights the fact that information security in the cyber environment has become one of the main components for ensuring national security and cyber sovereignty. It is proposed to create National Cybersecurity Systems in order to ensure cyber sovereignty in the global environment and exercise effective control over the national cyberspace.

Keywords— national security; cybersovereignty; information security; national cyberspace.