Milli Kibertəhlükəsizlik Vəziyyətinin Ölçülməsi və Qiymətləndirilməsi üçün Konseptual Model

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

***Xülasə*— Müasir kibermühitdə risklərin dinamik xarakteri ənənəvi statik qiymətləndirmə metodlarının məhdudluğunu ortaya qoyur. Təklif edilən model real-vaxtda məlumatların toplanması və analizi əsasında kibertəhlükəsizlik vəziyyətinin fasiləsiz diaqnostikasını təmin edir. Kompleks kiber müayinə mexanizmi vasitəsilə göstəricilərin operativ monitorinqi, normallaşdırılması və qiymətləndirilməsi həyata keçirilir. Təqdim olunan yanaşma kiberrisklərin erkən aşkarlanmasına, vəziyyətin çevik qiymətləndirilməsinə və qərar qəbuletmə prosesinin effektiv dəstəklənməsinə imkan yaradır. Bu işdə milli kibertəhlükəsizlik vəziyyətinin operativ səviyyədə ölçülməsi və qiymətləndirilməsi üçün kompleks kiber müayinə yanaşmasına əsaslanan konseptual model təklif olunur.**

Açar sözlər*— *kibertəhlükəsizlik; kompleks kiber müayinə; operativ qiymətləndirmə; konseptual model; monitorinq; risklərin idarə olunması.

I.GİRİŞ

Son illərdə Azərbaycanda dövlət siyasətinin əsas prioritetlərindən biri yeni rəqəmsal dövlət arxitekturasının formalaşdırılmasıdır. Xüsusilə ölkə rəhbərliyi tərəfindən rəqəmsal dövlətin həm texnoloji, həm də idarəetmə üsullarının yenidən qurulması, təkmilləşdirilməsi məsələlərinin aktuallaşdırılması bu sahənin strateji istiqamət olduğunu göstərir.

Rəqəmsal dövlət vahid strateji baxış əsasında formalaşan, dövlət xidmətlərinin effektiv, təhlükəsiz və vətəndaşyönümlü şəkildə təqdim edilməsini təmin edən kompleks ekosistemdir. Bu sistemin əsasını dayanıqlı və koordinasiyalı rəqəmsal arxitektura təşkil edir [1].

Hazırda müxtəlif dövlət qurumlarında rəqəmsallaşmaya münasibətdə pərakəndə yanaşmalar müşahidə olunur. Bu isə vahid sistem əvəzinə parçalanmış rəqəmsal mühitin formalaşmasına səbəb olur.

Mövcud problemlərin əsas səbəbləri sırasında ölkədə fəaliyyət göstərən bəzi qurumların müxtəlif xarici proqram təminatlarını seçməsi, fərqli texnoloji həllər tətbiq etməsi və texnoloji asılılığın mövcudluğu göstərilə bilər.

Bu yanaşma nəticəsində ümumi sistemdə uyğunsuzluqlar yarana və rəqəmsal dövlətin vahid arxitekturası pozula bilər. Belə vəziyyətdə rəqəmsal dövlətin ayrı-ayrı elementləri mövcud olsa da, sistemli inteqrasiyadan uzaq., plansız şəkildə arxitektura formalaşır.

Azərbaycanda qəbul olunmuş bir sıra strateji sənədlər, qanunlar, fəaliyyət planları rəqəmsal dövlətin hüquqi bazasını formalaşdırır və vahid prinsiplər əsasında qurulmasını hədəfləyir. Son illərdə Azərbaycanda qəbul olunmuş əsas sənədlər sırasında "Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi ilə bağlı tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, "İnformasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə 2023–2027-ci illər Strategiyası" Azərbaycan Respublikası Prezidentinin Sərəncamı, "Rəqəmsal İnkişaf Konsepsiyası" Azərbaycan Respublikası Prezidentinin Fərmanı, "Azərbaycan Respublikasının 2025–2028-ci illər üçün süni intellekt Strategiyası"nın təsdiq edilməsi haqqında Respublikası Prezidentinin Sərəncamı və "Azərbaycanın yeni rəqəmsal arxitekturası" adlı vahid fəaliyyət planını göstərmək olar [2].

Bu sənədlər dövlət maraqlarına uyğun vahid milli rəqəmsal arxitekturanın formalaşdırılması, kibertəhlükəsizlik məsələlərinin prioritetləşdirilməsi, xidmətlərin əlçatan olması, beynəlxalq əməkdaşlıq imkanlarının genişləndirilməsi kimi əsas istiqamətləri əhatə edir:

II.MİLLİ KİBERTƏHLÜKƏSİZLİYİN RƏQƏMSAL DÖVLƏTDƏ YERİ VƏ ROLU

Milli kibertəhlükəsizlik dövlətin informasiya resurslarının, rəqəmsal infrastrukturunun və kiberməkanının xarici və daxili təhdidlərdən qorunmasını təmin edən kompleks sistemidir [3].

Dövlətin milli təhlükəsizliyi çoxşaxəli xarakter daşıyır və siyasi, iqtisadi, ideoloji, ictimai, ekoloji, enerji, ərzaq və s. kimi müxtəlif sahələri əhatə edir [4]. Rəqəmsallaşmanın geniş vüsət aldığı bir şəraitdə milli təhlükəsizlik komponentləri rəqəmsal mühitdə öz əksini tapırr. Dövlətin informasiya sistemlərinin, kommunikasiya infrastrukturlarının, bank sektorunun, enerji şəbəkələrinin, səhiyyə sistemlərinin və digər obyektlərin vahid rəqəmsal mühitdə fəaliyyət göstərməsi, onların kibertəhlükəsizlik vəziyyətinin davamlı monitorinqinin aparılması və qiymətləndirilməsi zəruriyyətini yaradır.

Qloballaşmanın yaratdığı rəqəmsal çağırışlar, bu çağırışların doğurduğu risklər və kibertəhlükələr, eləcə də süni intellekt texnologiyalarının təqdim etdiyi yeni imkanlar kontekstində dövlətin rəqəmsal arxitekturası çərçivəsində milli kibertəhlükəsizlik ekosisteminin formalaşdırılması və onun vəziyyətini xarakterizə edən proseslərin ölçülməsi üçün məlumat əsaslı mexanizmlərin yaradılması xüsusi aktuallıq kəsb edir. Milli kibertəhlükəsizliyin təmin olunması üçün ölkənin sosial-iqtisadi sistemini (dövlət qurumları, özəl sektor, sənaye, vətəndaş cəmiyyəti və s.) əhatə edən bütün sahələrin

DOI: 10.25045/forensic.gov.2026.07

informasiya təhlükəsizliyi vəziyyətinin qiymətləndirilməsi zəruriyyəti yaranır. Bütün sahələr üzrə kibertəhlükəsizlik vəziyyətinin kompleks qiymətləndirilməsi ölkənin vahid kibertəhlükəsizlik mənzərəsinin formalaşdırılmasına imkan verə bilər.

III.İLKİN MƏLUMATLARIN TOPLANMASI PROBLEMLƏRİ

Milli kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi prosesi zamanı qarşıya qoyulan əsas məsələlər ilkin məlumatların hansı mənbələrdən və necə toplanması, onların xüsusiyyətlərinin və etibarlılığının müəyyən edilməsi, eləcə də hansı metodlarla ölçülməsidir.

Kibertəhlükəsizlik sahəsində istifadə olunan məlumatlar müxtəlif xarakter daşıyır. Bu məlumatlar sırasında fərdi məlumatlar, kommersiya sirləri, dövlət sirləri, hərbi məlumatlar və kritik infrastruktur göstəriciləri mövcuddur. Bu səbəbdən məlumatların toplanması prosesində texniki məsələlərlə yanaşı, hüquqi və etik tələblər də nəzərə alınmalıdır, vətəndaşların konstitusional hüquqları təmin olunmalıdır. Toplanan məlumatların üçüncü tərəflərə ötürülməyəcəyi və yalnız milli təhlükəsizlik məqsədləri üçün istifadə olunacağına təminat verilməlidir.

Kibertəhlükəsizlik sistemləri vasitəsilə toplanan məlumatların düşmən və ya kənar qüvvələrin əlinə keçməsi dövlətin rəqəmsal suverenliyi üçün ciddi təhlükə yarada bilər. Çünki həmin məlumatların analizi nəticəsində ölkənin zəif infrastrukturu, təhlükəsizlik boşluqları, kritik sistemləri və hücum üçün əlverişli nöqtələri müəyyən edilə bilər [5].

Xüsusilə səhiyyə, enerji, maliyyə və dövlət idarəetməsi sahələrinə aid məlumatların sızdırılması milli təhlükəsizlik baxımından strateji risk hesab olunur. Buna görə də kibertəhlükəsizlik məlumatlarının qorunması ayrıca təhlükəsizlik səviyyəsi tələb edir. Kibertəhlükəsizlik sisteminin özünün də ayrıca qorunma mexanizmləri işlənməlidir [6].

Məlumatların toplanması zamanı əsas problemlərdən biri də onların təhrif olunma ehtimalıdır. Təşkilatlar müəyyən hallarda öz kibertəhlükəsizlik vəziyyətlərini daha yaxşı göstərmək üçün məlumatları dəyişdirə və ya bəzi hadisələri gizlədə bilərlər. Bu baxımdan alternativ mənbələrdən istifadə edilməsi mühüm əhəmiyyət daşıyır. Loq faylları və təhlükəsizlik sensorlarından əldə olunan məlumatlar, audit nəticələri, monitorinq sistemləri və ekspert müşahidələri ilkin məlumatların obyektivliyinin artırılması üçün əsas vasitələr hesab olunur.

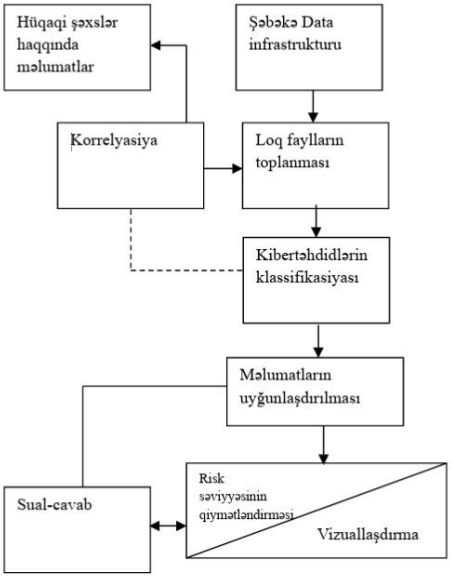
Milli səviyyədə kibertəhlükəsizlik data ekosisteminin formalaşdırılması zamanı məlumatların operativliyi, tamlığı, dəqiqliyi, etibarlılığı və məxfiliyi əsas prinsiplər kimi qəbul edilməli, rəqəmsal dövlətin Data suverenliyi təmin olunmalıdır [7].

IV.KİBERTƏHLÜKƏSİZLİK VƏZİYYƏTİNİN OPERATİV SƏVİYYƏDƏ QİYMƏTLƏNDİRİLMƏSİ

Tədqiqat işində milli kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi üçün Azərbaycan Respublikasının ərazisində dövlət reyestrində qeydiyyatdan keçmiş hüquqi şəxslərdən toplanmış məlumat resurslarının kompleks kiber müayinəsi əsasında arxitektur-texnoloji model təklif olunur (Şəkil 1).

Hüquqi şəxs qanunvericiliklə müəyyən edilmiş qaydada yaradılan, hüquq və vəzifələrə malik olan, müstəqil əmlaka sahib, öz adından fəaliyyət göstərən və məhkəmədə müstəqil hüquqi subyekt kimi çıxış edə bilən təşkilatdır. Azərbaycan Respublikasında hüquqi şəxslərin dövlət qeydiyyatı Azərbaycan Respublikasının Ədliyyə Nazirliyi tərəfindən həyata keçirilir. Bu çərçivədə dövlət, ali və orta təhsil müəssisələri, siyasi partiyalar, fondlar, banklar, sığorta təşkilatları, ictimai birliklər, habelə xarici hüquqi şəxslərin filial və s. dövlət qeydiyyatına alınır [8].

Hüquqi şəxslərin kompleks kiber müayinəsi təşkilatın informasiya sistemlərinin, rəqəmsal infrastrukturunun, məlumat resurslarının və s. təhlükəsizlik vəziyyətinin mütəmadi şəkildə yoxlanılması və qiymətləndirilməsi prosesidir. Bu proses təşkilatın kiber risklərə qarşı davamlılığını təmin etmək və mümkün təhlükələri əvvəlcədən aşkar etmək məqsədi daşıyır.



Şəkil 1. Hüquqi şəxslərdən toplanmış data resursların kompleks kiber müayinəsinə əsası arxitektur-texnoloji modeli

Kompleks kiber müayinə çərçivəsində təşkilatın texniki sistemləri, şəbəkə infrastrukturu, proqram təminatı, istifadəçi girişləri və təhlükəsizlik siyasətləri və s. kompleks şəkildə təhlil olunur. Təhlillərin sorğular və loq fayllar əsasında aparılması nəzərdə tutulur. İlkin mərhələdə hüquqi şəxsə aid loq fayllar və sorğu əsaslı məlumatlar toplanılır. Loq fayllarının və sorğuların analizi nəticəsində mövcud kibertəhlükələr, zəifliklər, potensial risklər, təhlükəsizlik boşluqları və s. müəyyən edilir. Analizin nəticələri qiymətləndirilərək təşkilatın kibertəhlükəsizlik vəziyyəti müəyyən edilir.

Bu proses nəticəsində milli səviyyədə təşkilatları müxtəlif fəaliyyət sahələri (dövlət qurumları, özəl sektor, sənaye, vətəndaş cəmiyyəti və s), ərazi bölgüsü, kibertəhlükələrin növləri, illər üzrə dinamikası və digər parametrlər üzrə

qruplaşdırmaq və analitik məlumatlar əldə etmək mümkün olacaq. Bu təşkilatların kibertəhlükəsizlik reytinqini formalaşdırmağa, zəiflikləri mövcud olan təşkilatları müəyyən etməyə imkan yaradar. Nöqsanlar aşkar olunmuş təşkilatların informasiya infrastrukturu yenidən təhlil oluna və təkmilləşdirmə tədbirləri həyata keçirilə bilər.

Hüquqi şəxslərin kompleks kiber müayinəsi təşkilatın informasiya təhlükəsizliyinin təmin olunması, risklərin azaldılması və dayanıqlı fəaliyyətin qorunması üçün zəruri və strateji əhəmiyyətə malik bir prosesdir. Onun mütəmadi həyata keçirilməsi təşkilatın həm daxili, həm də xarici təhlükələrə qarşı daha hazırlıqlı olmasını təmin edir.

Hüquqi şəxslərin kompleks kiber müayinəsi nəticəsində analiz olunmuş məlumatların qiymətləndirilməsi üçün informasiya təhlükəsizliyinin əsas prinsipləri olan əlçatanlıq, tamlıq, məxfilik və məzmun əsasında Milli Kibertəhlükəsizlik İndeksinin formalaşdırılması təklif olunur [9] .

V.MİLLİ KİBERTƏHLÜKƏSİZLİK İNDEKSİ

Milli kibertəhlükəsizlik səviyyəsinin ölçülməsi dövlətin, təşkilatların rəqəmsal təhdidlərə qarşı hazırlıq səviyyəsini qiymətləndirməyə imkan verə bilər. Ölkənin kibermüdafiə potensialını, hüquqi çərçivəsini, texniki imkanlarını, insan resurslarını və s. sahələri qiymətləndirmək üçün Milli Kibertəhlükəsizlik İndeksinin real loq məlumatlarının analizi ilə yanaşı aşağıdakı indikatorlar üzrə formalaşdırılması təklif olunur.

1) Mövcud kibertəhlükələr. Buraya DDoS hücumları, ransomware, sosial mühəndislik, məlumat sızmaları, kiberhücumların tezliyi və təsir dərəcəsi daxildir. Təhlükələrin növünün və təsir dairəsinin düzgün müəyyənləşdirilməsi müdafiə strategiyalarının qurulmasında əsas rol oynayır.

2) Mövcud müdafiə mexanizmləri. Qanunvericilik bazasının, texnoloji təhlükəsizlik sistemlərinin, insidentlərə cavab planlarının və texniki audit mexanizmlərinin mövcudluğu və effektivliyi qiymətləndirilir.

3) Kibertəhlükəsizliyə cavabdeh qurumlar. Dövlət qurumları, özəl sektor və təhsil müəssisələri arasında məsuliyyət bölgüsü, daxili cavabdehliyin və koordinasiya mexanizmlərinin qiymətləndirilməsi.

4) Müxtəlif sahələrin kibertəhlükəsizlik vəziyyəti. Enerji, nəqliyyat, bank, rabitə, səhiyyə, elm və təhsil kimi sahələrin, eləcə də daxili struktur vahidlərinin kibertəhlükəsizlik səviyyəsinin qiymətləndirilməsi.

5) Elm və təhsilin kibertəhlükəsizliyə verdiyi töhfə. Kadr hazırlığının, rəqəmsal savadlılığın artırılması, yeni texnologiyaların tətbiqinin qiymətləndirilməsi.

6) Kibertəhlükəsizlik sahəsində inkişaf. İllik inkişaf göstəriciləri, investisiya artımı və onların beynəlxalq reytinqlərdə ölkənin mövqeyinə təsirin qiymətləndirilir.

7) Kibertəhlükəsizlik strategiyasının mövcudluğu və icra səviyyəsi. Strategiyaların və qanunların tətbiq səviyyəsi, hesabatlılıq mexanizmləri və monitorinq sisteminin effektivliyinin qiymətləndirilməsi.

8) İnsidentlərə cavab qabiliyyəti. CTI, SOC, SIEM, CERT/CSIRT kimi strukturların insidentlərə cavab vermə sürəti və analitik imkanlarının qiymətləndirilməsi.

9) Kiber kriminalistika. Rəqəmsal sübutların toplanması və ekspertizası, kiber cinayətkarların hüquqi məsuliyyətə cəlb olunması prosesinin səviyyəsinin qiymətləndirilməsi.

10) Rəqəmsal savadlılıq səviyyəsi. Cəmiyyətdə kibertəhlükəsizlik mədəniyyəti, istifadəçi davranışı və fərdi məlumatların qorunmasının qiymətləndirilməsi.

11) Elm və təhsilə dəstəyin verilməsi. Kibersuverenlik çərçivəsində təşkilatlarda elm, təhsil və qrant layihələrinə, kadr hazırlığı proqramlarına göstərilən dəstək səviyyəsinin qiymətləndirilməsi.

12) Beynəlxalq əməkdaşlıq. Beynəlxalq əməkdaşlıq kibertəhlükəsizlik sahəsində xüsusi əhəmiyyət daşıyır. Dövlətin ITU, ENISA və INTERPOL kimi beynəlxalq təşkilatlarla əməkdaşlığının və qlobal təşəbbüslərə inteqrasiyasının qiymətləndirilməsi.

13) Kibersuverenliyin təmin olunması. Texnologiyaların mənimsənilməsi, informasiya axınına nəzarət imkanlarının qiymətləndirilməsi.

14) Resursların həcmi. Bu sahəyə ayrılan maliyyə, texniki infrastrukturun yenilənməsi və insan resurslarının vəziyyətinin qiymətləndirilməsi.

NƏTİCƏ

Müasir dövrdə rəqəmsal dövlət konsepsiyasının effektiv şəkildə qurulması vahid və dayanıqlı rəqəmsal arxitektura əsasında mümkündür. Milli kibertəhlükəsizlik rəqəmsal dövlət arxitekturasında informasiya resurslarının, kritik infrastrukturunun və rəqəmsal xidmətlərinin qorunması istiqamətində mühüm rol oynayır.

Tədqiqatda milli kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsi üçün məlumat əsaslı yanaşmaların tətbiqinin əhəmiyyəti vurğulanır. Hüquqi şəxslərdən toplanmış loq fayllar və sorğu əsaslı məlumatların analizi nəticəsində ölkənin kibertəhlükəsizlik mənzərəsinin formalaşdırılması göstərilir. Bu yanaşma kibertəhlükələrin vaxtında aşkarlanmasına, risklərin müəyyən edilməsinə və zəifliklərin aradan qaldırılmasına şərait yaradır.

Məqalədə təklif olunan arxitektur-texnoloji model hüquqi şəxslərin kompleks kiber müayinəsinin həyata keçirilməsini və nəticələrin sistemli şəkildə qiymətləndirilməsini nəzərdə tutur. Bu model vasitəsilə dövlət qurumları, özəl sektor, sənaye və digər sahələr üzrə kibertəhlükəsizlik vəziyyətinin müqayisəli təhlili mümkün olur. Eyni zamanda təşkilatların kibertəhlükəsizlik reytinqinin formalaşdırılması, zəifliklərı

olan infrastrukturların müəyyən olunması və təkmilləşdirmə tədbirlərinin həyata keçirilməsi üçün real imkan yaranır.

Milli Kibertəhlükəsizlik İndeksinin formalaşdırılması ölkənin kibermüdafiə potensialının, hüquqi və texniki imkanlarının, insan resurslarının, rəqəmsal savadlılıq səviyyəsinin və beynəlxalq əməkdaşlıq imkanlarının kompleks qiymətləndirilməsinə xidmət edir. Təklif olunan indikatorlar kibertəhlükəsizlik sahəsində mövcud vəziyyətin operativ və obyektiv şəkildə monitorinqinə imkan verə bilər.

ƏDƏBİYYAT

[1] J. Schou and M. Hjelholt, "Digital state spaces: State rescaling and advanced digitalization," Territory, Politics, Governance, vol. 7, no. 4, pp. 438–454, 2019.

[2] Qanunvericilik bazasına əsaslanan süni intellekt dəstəkli innovativ hüquqi axtarış platforması, e-qanun.az

[3] S. AlDaajeh et al., "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, vol. 119, p. 102754, 2022.

[4] R. M. Əliquliyev, Y. N. İmamverdiyev, and R. Ş. Mahmudov, "İnformasiya təhlükəsizliyi milli təhlükəsizliyin mühüm komponenti kimi," *Problems of Information Society*, vol. 11, no. 1, pp. 3–25, 2020.

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

[6] B. Nəbiyev, K. Daşdəmirova, "Rəqəmsal tibb infrastrukturunda kiber insidentlər, təhdidlər, risklər və onların intellektual analizi," in "Rəqəmsal tibb 4.0: problemlər, imkanlar və perspektivlər" II Respublika Elmi-Praktiki Konfransı, Bakı, Azerbaijan, May 23, 2025, pp. 87–91.

[7] F. von Scherenberg, M. Hellmeier, and B. Otto, "Data sovereignty in information systems," Electronic Markets, vol. 34, no. 1, p. 15, 2024.

[8] Hüquqi şəxslərin dövlət qeydiyyatı və dövlət reyestri haqqında, e-qanun.az/framework/5403

[9] N. Chitadze, "Basic principles of information and cyber security," in Analyzing New Forms of Social Disorders in Modern Virtual Environments. IGI Global Scientific Publishing, 2023, pp. 193–223.

A Conceptual Model for Measuring and Assessing the National Cybersecurity Situation

Babek Nabiyev[1], Konul Dashdemirova[2]
[1,2] Institute of Information Technology, Baku, Azerbaijan
[1]babek.nabiyev@gmail.com, [2]konulahmed@gmail.com

Abstract- The dynamic nature of risks in the modern cyber environment reveals the limitations of traditional static assessment methods. The proposed model provides continuous diagnostics of the cybersecurity situation based on real-time data collection and analysis. Operational monitoring, normalization and assessment of indicators are carried out through a complex cyber examination mechanism. The presented approach allows for early detection of cyber risks, rapid assessment of the situation and effective support of the decision-making process. In this work, a conceptual model based on the complex cyber examination approach is proposed for measuring and assessing the national cybersecurity situation at an operational level.

Keywords- cybersecurity; complex cyber examination; operational assessment; conceptual model; monitoring; risk management.