Dövlətin Kibersuverenliyi və Enerji Təhlükəsizliyinə Yeni Tələblər

Şakir Mehdiyev[1], Nəzrin Rzayeva[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*shakir.mehtieff@gmai.com*, [2] *nezrinrzayeva@gmail.com*

***Xülasə*— Rəqəmsal transformasiya dövlət idarəçiliyi, sənaye və kritik infrastrukturun fəaliyyət mexanizmlərini köklü şəkildə dəyişmişdir. Enerji sistemlərinin rəqəmsal platformalar, SCADA sistemləri, intellektual şəbəkələr və məlumat emalı texnologiyaları ilə inteqrasiyası enerji təhlükəsizliyinin mahiyyətini yenidən müəyyənləşdirir. Müasir şəraitdə enerji təhlükəsizliyi yalnız fasiləsiz enerji təminatı ilə məhdudlaşmır, həm də idarəetmə sistemlərinin kibermüdafiəsi, məlumatların qorunması və texnoloji asılılığın azaldılması ilə bağlıdır. Məqalədə enerji təhlükəsizliyi dövlətin kibersuverenliyi kontekstində təhlil olunur, bu iki anlayış arasındakı struktur əlaqə əsaslandırılır və onların inteqrasiyasına dair konseptual yanaşma təqdim edilir.**

Açar sözlər*— *kibersuverenlik*; *enerji təhlükəsizliyi*; *kritik infrastruktur*; *kiber-fiziki sistemlər*; *dayanıqlılıq*; *texnoloji müstəqillik.

I. GİRİŞ

Rəqəmsal transformasiya enerji sektorunun struktur və funksional əsaslarını köklü şəkildə dəyişdirmişdir. Ənənəvi yanaşmalarda enerji təhlükəsizliyi (ET) əsasən enerji təchizatının fasiləsizliyi, mənbələrin şaxələndirilməsi və geosiyasi risklərin azaldılması ilə əlaqələndirilirdisə, müasir şəraitdə bu anlayış kritik infrastrukturun sistem dayanıqlılığı və texnoloji avtonomluq ölçülərini də əhatə edən daha mürəkkəb məzmun kəsb edir [1]. İntellektual şəbəkələrin, rəqəmsal dispetçer sistemlərinin və avtomatlaşdırılmış generasiya və ötürmə idarəetmə mexanizmlərinin inkişafı nəticəsində enerji sistemləri klassik fiziki infrastruktur modelindən kiber-fiziki sistem arxitekturasına transformasiya olunmuşdur [2]. Bu transformasiya enerji proseslərinin proqram təminatı, telekommunikasiya şəbəkələri və alqoritmik qərar mexanizmlərindən struktur asılılığını gücləndirmişdir. Beləliklə, ET fiziki aktivlərin qorunması ilə məhdudlaşmır; o, rəqəmsal idarəetmə mühitinin bütövlüyü və strateji nəzarət imkanları ilə birbaşa əlaqələnir.

Son illərdə enerji sektorunda qeydə alınmış kiberinsidentlər göstərmişdir ki, rəqəmsal müdaxilələr real fiziki pozuntulara və genişmiqyaslı sosial-iqtisadi nəticələrə səbəb ola bilər [3]. Bu risklərə cavab olaraq Avropa İttifaqında 2022-ci ildə qəbul edilmiş NIS2 Direktivi enerji sektorunun kiberdayanıqlılığına dair tələbləri sərtləşdirmiş, paralel olaraq kritik infrastrukturun dayanıqlılığı üzrə yeni hüquqi mexanizmlər formalaşdırılmışdır [4].

Paralel şəkildə texnoloji və rəqəmsal suverenlik anlayışları strateji diskursun mərkəzinə keçmişdir.

Müasir siyasət sənədlərində dövlətlərin enerji də daxil olmaqla kritik rəqəmsal infrastruktur üzərində strateji nəzarət imkanlarının qorunması milli təhlükəsizliyin əsas komponenti kimi qiymətləndirilir [5]. Transmilli enerji bazarlarının inteqrasiyası və qarşılıqlı asılılığın artması şəraitində ET artıq təkcə təchizat məsələsi deyil, rəqəmsal nəzarət, texnoloji asılılıq və institusional muxtariyyət problemləri ilə üzvi şəkildə bağlı olan çoxsəviyyəli konseptə çevrilmişdir [6].

Buna baxmayaraq, mövcud elmi ədəbiyyatda ET və kiberdayanıqlılıq əsasən paralel istiqamətlər kimi araşdırılır; onların dövlətin kibersuverenliyinin struktur elementi kimi inteqrativ təhlili isə fragmentar xarakter daşıyır. Xüsusilə, fiziki infrastrukturun qorunması ilə rəqəmsal nəzarət imkanlarının strateji idarəetmə çərçivəsində birləşdirilməsi üzrə sistemli konseptual model formalaşdırılmamışdır.

Bu məqalənin məqsədi rəqəmsallaşma şəraitində ET-nə qoyulan yeni tələbləri dövlətin kibersuverenliyi kontekstində nəzəri əsaslandırmaq və fiziki, rəqəmsal və strateji səviyyələrin funksional qarşılıqlı əlaqəsinə əsaslanan inteqrativ model təklif etməkdir. Metodoloji baxımdan tədqiqat beynəlxalq və milli səviyyədə qəbul edilmiş strateji sənədlərin, eləcə də beynəlxalq təşkilatların hesabatlarının müqayisəli təhlilinə əsaslanır.

Təklif olunan yanaşma Azərbaycan nümunəsində tətbiq olunur və yaşıl transformasiya ilə rəqəmsal inteqrasiyanın enerji siyasətinə struktur təsirini nümayiş etdirir.

II. ENERJİ TƏHLÜKƏSİZLİYİ ANLAYIŞININ TƏKAMÜLÜ VƏ RESURS YANAŞMASININ SƏRHƏDLƏRİ

ET anlayışı tarixi olaraq enerji resurslarının fasiləsiz və iqtisadi cəhətdən əlçatan təminatı kimi formalaşmışdır. XX əsrin ikinci yarısında baş vermiş enerji böhranları bu anlayışın mərkəzinə neft və qaz təchizatının sabitliyi məsələsini çıxarmış, nəticədə ET əsasən fiziki ehtiyatların mövcudluğu və tranzit marşrutlarının qorunması prizmasında şərh edilmişdir. Beynəlxalq Enerji Agentliyinin müasir yanaşmalarında belə ET ilk növbədə sistemin xarici şoklara dayanıqlılığı və təchizatın fasiləsizliyi ilə əlaqələndirilir [1].

Zamanla anlayışın məzmunu genişlənmişdir. Müasir ədəbiyyatda ET-nin çoxölçülü və institusional xarakteri vurğulanır [7]. Bu yanaşmaya görə, enerji təhlükəsizliyi yalnız resurs əlçatanlığı ilə deyil, həm də sistemin idarəetmə strukturları və risklərin bölüşdürülməsi mexanizmləri ilə müəyyən olunur. Müasir konsepsiyalar enerji sistemlərinin

DOI: 10.25045/cyber.gov.2026.30

struktur dayanıqlılığı, bazar mexanizmlərinin sabitliyi, infrastrukturun etibarlılığı və institusional koordinasiya qabiliyyəti kimi əlavə ölçüləri də nəzərə alır [8]. Avropa İttifaqının Enerji İttifaqı strategiyasında ET həm təchizatın şaxələndirilməsi, həm də sistemli risklərin qabaqlayıcı idarə olunması kontekstində qiymətləndirilir [9].

Bununla belə, bu genişlənməyə baxmayaraq, ET-nin analitik əsasını hələ də resurs yönümlü paradigma təşkil edir. Bu paradigma üç əsas fərziyyəyə söykənir:

- ET fiziki resursların mövcudluğu ilə müəyyən olunur;
- əsas risklər hasilat və tranzit zəncirində yaranır;
- təhlükəsizlik problemləri əsasən geosiyasi və iqtisadi xarakter daşıyır.

Müasir rəqəmsallaşma mərhələsində isə bu fərziyyələr sistem reallığını tam əhatə etmir. Enerji infrastrukturu artıq yalnız fiziki aktivlərdən ibarət deyil; o, proqram təminatı, telekommunikasiya şəbəkələri və alqoritmik idarəetmə mexanizmləri ilə inteqrasiya olunmuş kiber-fiziki sistem kimi fəaliyyət göstərir. ENTSO-E-nin onillik inkişaf planında transmilli şəbəkələrin sinxronizasiyası və rəqəmsal inteqrasiyası prioritet istiqamətlər kimi göstərilir ki, bu da təhlükəsizlik anlayışının texnoloji ölçüsünü ön plana çıxarır [2].

OECD və Avropa Komissiyasının sənədlərində də vurğulanır ki, kritik infrastrukturun qorunması artıq yalnız fiziki müdafiə tədbirləri ilə məhdudlaşmır, rəqəmsal idarəetmə sistemlərinin bütövlüyü və dayanıqlılığı da eyni səviyyədə əhəmiyyət kəsb edir. Bu transformasiya ET anlayışına keyfiyyətcə yeni ölçü – kiberdayanıqlılıq komponentini daxil edir.

Resurs yanaşmasının əsas sərhədi məhz burada üzə çıxır. ET yalnız ehtiyatların həcmi və tranzit marşrutlarının sabitliyi ilə ölçüldükdə, enerji sisteminin rəqəmsal nəzarət konturları və proqram təminatından asılılığı nəzərə alınmır. Halbuki SCADA sistemləri, avtomatlaşdırılmış dispetçer mərkəzləri və məlumat platformaları enerji axınlarının real vaxt rejimində idarə olunmasını təmin edir və bu sahədə yaranan zəifliklər fiziki nəticələr doğura bilər [3].

Nəticə etibarilə, ET-nin təkamülü göstərir ki, klassik resurs modeli rəqəmsal inteqrasiya mərhələsində sistemin bütün risk profilini izah etmək üçün yetərli deyil. Müasir şəraitdə enerji sistemlərinin dayanıqlılığı yalnız hasilat və ixrac qabiliyyəti ilə deyil, həm də rəqəmsal idarəetmə konturlarının təhlükəsizliyi və texnoloji asılılıq səviyyəsi ilə müəyyən olunur. Bu isə ET-nin dövlətin kibersuverenliyi çərçivəsində yenidən konseptuallaşdırılmasını zəruri edir.

III. Enerji Sektorunun Rəqəmsallaşması və Yeni Sistem Riskləri

Enerji sektorunun rəqəmsallaşması son onillikdə funksional yenilənmə mərhələsindən çıxaraq struktur xarakter almışdır. Elektrik şəbəkələrinin idarə olunmasında SCADA sistemlərinin, real vaxt məlumat analitikasının, avtomatlaşdırılmış balanslaşdırma mexanizmlərinin və süni intellekt əsaslı proqnoz modellərinin tətbiqi enerji sistemlərinin yalnız əməliyyat mexanizmlərini deyil, onların arxitektura məntiqini dəyişmişdir. ENTSO-E tərəfindən hazırlanan inkişaf planlarında transmilli şəbəkələrin sinxronizasiyası və rəqəmsal monitorinq sistemlərinin genişləndirilməsi prioritet istiqamətlər kimi müəyyən edilir [2].

Bu transformasiya enerji sistemini fiziki aktivlər toplusundan proqram təminatı ilə idarə olunan kiber-fiziki kompleksə çevirmişdir. Eyni zamanda enerji sistemlərinin desentralizasiyası və bərpa olunan enerji mənbələrinin (BEM) payının artması risk profilini daha da mürəkkəbləşdirir. Paylanmış generasiya, mikroşəbəkələr və çevik balanslaşdırma mexanizmləri sistemin strukturunu mərkəzləşdirilmiş modeldən şəbəkə əsaslı arxitekturaya transformasiya etmişdir.

Bu şəraitdə IoT əsaslı sensor sistemləri, ağıllı sayğac infrastrukturu və uzaqdan idarəetmə qurğuları enerji şəbəkəsinin ayrılmaz elementi halına gəlmişdir. Tədqiqatlar göstərir ki, artan əlaqəlilik və proqram təminatından asılılıq kiber-fiziki hücum səthini genişləndirir və yeni zəifliklər formalaşdırır [8].

Rəqəmsallaşma səmərəliliyi artırsa da, risk profilini keyfiyyətcə dəyişdirir. ENISA-nın 2023-cü il üzrə enerji sektoru üçün təhdid mənzərəsi hesabatında enerji infrastrukturu kiberhücumlara ən həssas kritik sektorlar sırasında göstərilir [4]. Hücum vektorları artıq yalnız məlumat sızması ilə məhdudlaşmır; onlar əməliyyat texnologiyalarına (ƏT) müdaxilə və fiziki proseslərin pozulması riskini ehtiva edir.

Müasir enerji sistemi üç qarşılıqlı əlaqəli risk səviyyəsində fəaliyyət göstərir.

Birinci risk səviyyəsi idarəetmə sistemlərinə müdaxilə ilə bağlıdır. Rəqəmsal dispetçer sistemlərinin manipulyasiyası və ya sıradan çıxması elektrik təchizatının fasiləsinə səbəb ola bilər. Bu səbəbdən NIS2 Direktivi enerji sektorunu "yüksək kritik" kateqoriyaya daxil etmiş və kiberdayanıqlılıq tələblərini sərtləşdirmişdir [4].

İkinci risk səviyyəsi təchizat zənciri ilə bağlıdır. Enerji avadanlıqları və proqram təminatı qlobal istehsal və texnoloji şəbəkələrə inteqrasiya olunduqca, xarici komponentlərdən asılılıq artır. OECD hesabatlarında vurğulanır ki, kritik infrastrukturun dayanıqlılığı yalnız daxili müdafiə mexanizmlərindən deyil, həm də texnoloji təchizat zəncirinin təhlükəsizliyindən asılıdır.

Üçüncü risk səviyyəsi transmilli inteqrasiya ilə bağlıdır. Yüksək gərginlikli ötürmə xətləri və sualtı kabellər vasitəsilə enerji sistemlərinin inteqrasiyası qarşılıqlı asılılığı artırır. Bu inteqrasiya sistem dayanıqlılığını gücləndirə bilsə də, eyni zamanda lokal pozuntuların regional miqyasda yayılma sürətini artırır [2].

Bu baxımdan, rəqəmsallaşma ET-nin risk strukturunu dəyişir və onu təkcə "təchizatın dayanıqlılığı" prizmasında qiymətləndirməyi qeyri-kafi edir. Enerji sistemi artıq kiber-fiziki kompleks kimi fəaliyyət göstərir və onun sabitliyi proqram təminatının bütövlüyü, məlumat axınlarının təhlükəsizliyi və rəqəmsal idarəetmə mexanizmlərinin dayanıqlılığı ilə müəyyən olunur.

Bu dəyişiklik ET-nə yeni struktur ölçü əlavə edir – kiberdayanıqlılıq. Lakin kiberdayanılılıq yalnız texniki müdafiə

mexanizmləri ilə məhdudlaşmır; o, rəqəmsal nəzarət imkanları, texnoloji asılılıq səviyyəsi və strateji qərarvermə muxtariyyəti ilə sıx bağlıdır. Bu isə ET-nin növbəti konseptual mərhələsinə – kibersuverenlik çərçivəsinə keçidi zəruri edir.

IV. Enerji Təhlükəsizliyi və Kibersuverenlik: Konseptual Əlaqə

Enerji sektorunun dərin rəqəmsallaşması ET-ni yalnız texniki və iqtisadi kateqoriya kimi deyil, dövlətin strateji idarəetmə qabiliyyətinin struktur elementi kimi yenidən nəzərdən keçirməyi zəruri edir. Rəqəmsal idarəetmə sistemlərinin enerji infrastrukturu ilə inteqrasiyası təhlükəsizlik anlayışını fiziki aktivlərin qorunmasından kənara çıxararaq idarəetmə və nəzarət müstəvisinə keçirir. Bu kontekstdə kibersuverenlik ET-nin genişləndirilmiş konseptual ölçüsü kimi çıxış edir.

Kibersuverenlik dövlətin rəqəmsal məkan və kritik informasiya infrastrukturuna dair hüquqi, institusional və texniki nəzarət imkanlarını ifadə edir [10]. Kritik infrastrukturun rəqəmsal komponentləri üzərində nəzarətin zəifləməsi strateji asılılıq riskini artırır və qərarvermə muxtariyyətini məhdudlaşdıra bilər.

Müasir enerji sistemi artıq yalnız generasiya və ötürmə xətlərindən ibarət fiziki şəbəkə deyil, məlumat mərkəzləri, proqram təminatı platformaları, real vaxt analitikası və uzaqdan idarəetmə mexanizmləri ilə inteqrasiya olunmuş kiber-fiziki kompleksdir. Enerji axınlarının idarə olunması getdikcə daha çox alqoritmik qərar mexanizmləri və şəbəkə protokolları vasitəsilə həyata keçirilir.

Əgər klassik enerji suverenliyi resurslar və fiziki infrastruktur üzərində nəzarəti ifadə edirdisə, kibersuverenlik enerji sisteminin rəqəmsal arxitekturası, idarəetmə alqoritmləri və əsas texnoloji komponentləri üzərində təsir imkanlarını əhatə edir. Qlobal təchizat zəncirlərinə bağlılıq və transmilli enerji inteqrasiyası şəraitində bu fərq daha da aktuallaşır.

Normativ müstəvidə bu transformasiya artıq institusional təsbitini tapmışdır. NIS2 Direktivi və kritik infrastrukturun dayanıqlılığına dair Avropa çərçivəsi enerji sektorunu yüksək strateji əhəmiyyətli sahə kimi müəyyən edərək kiberdayanıqlılıq öhdəliklərini sərtləşdirir [4]. OECD sənədlərində isə rəqəmsal təhlükəsizlik risklərinin idarə olunması dövlət siyasətinin ayrılmaz elementi kimi təqdim olunur [11].

Bu əsasda ET üç qarşılıqlı səviyyədə təhlil oluna bilər:

- Fiziki dayanıqlılıq – generasiya və ötürmə sistemlərinin texniki etibarlılığı və fasiləsiz fəaliyyəti;
- Rəqəmsal dayanıqlılıq – idarəetmə sistemlərinin və şəbəkə arxitekturasının kibermüdafiəsi və funksional bütövlüyü;
- Strateji nəzarət – enerji sisteminin əsas rəqəmsal və texnoloji komponentləri üzərində qərarvermə muxtariyyətinin qorunması.

Məhz üçüncü səviyyə ET-ni kibersuverenlik çərçivəsinə inteqrasiya edir. Dövlət kritik proqram təminatı və texnoloji platformalar üzrə strateji qərarları müstəqil şəkildə formalaşdıra bilmədikdə, ET struktur zəiflik riski ilə üzləşir.

Bu kontekstdə, kibersuverenlik ET-nin yalnız fiziki təminat deyil, həm də rəqəmsal idarəetmə və texnoloji muxtariyyət ölçülərini əhatə edən genişləndirilmiş strateji forması kimi çıxış edir.

V. Azərbaycan Üzrə Enerji Təhlükəsizliyi və Rəqəmsallaşma

Azərbaycan enerji siyasəti post-sovet dövründə əsasən resurs əsaslı təhlükəsizlik modeli üzərində formalaşmışdır. Neft və qaz hasilatı, ixrac marşrutlarının şaxələndirilməsi və tranzit infrastrukturunun inkişafı ET-nin əsas dayaqları kimi çıxış etmişdir. Rəsmi sənədlərdə ölkənin enerji müstəqilliyi və daxili tələbatın təmin olunması prioritet istiqamətlər kimi müəyyən edilmişdir [12].

Enerji sisteminin fiziki ölçüsü baxımından generasiya gücünün artırılması, ötürmə xətlərinin modernləşdirilməsi və regional interkonnektorların inkişafı müşahidə olunur. Dövlət proqramlarında 2030-cu ilə qədər əlavə generasiya güclərinin istismara verilməsi və enerji balansının optimallaşdırılması nəzərdə tutulur. Bu yanaşma klassik ET modelinin tələblərinə uyğun gəlir.

Lakin son illərdə enerji sektorunda rəqəmsallaşma prosesləri də sürətlənmişdir. Elektrik şəbəkələrinin avtomatlaşdırılması, SCADA sistemlərinin tətbiqi, ağıllı sayğac infrastrukturunun genişləndirilməsi və enerji axınlarının real vaxt rejimində monitorinqi enerji idarəetməsinin strukturunu dəyişmişdir. Eyni zamanda, transmilli enerji layihələri və yüksək gərginlikli ötürmə xətləri vasitəsilə regional inteqrasiya səviyyəsi artmışdır. Bu proseslər iki paralel tendensiya yaradır.

Bir tərəfdən, enerji sisteminin səmərəliliyi və əməliyyat çevikliyi yüksəlir. Digər tərəfdən, idarəetmə konturlarının rəqəmsal asılılığı artır. Enerji sisteminin dispetçer mərkəzləri, məlumat serverləri və ƏT kimi kritik elementləri artıq qlobal proqram təminatı və avadanlıq təchizat zəncirləri ilə inteqrasiya olunmuşdur.

Aparılmış struktur və analitik təhlil göstərir ki, ET fiziki müstəqillik səviyyəsində təmin olunsa da, rəqəmsal və texnoloji komponentlər üzrə asılılıq riski tam aradan qalxmır. Xüsusilə proqram təminatının xarici mənşəli olması, kritik avadanlıqların idxaldan asılılığı və məlumat infrastrukturunun qlobal platformalarla inteqrasiyası ET-nə yeni ölçü əlavə edir.

Bu kontekstdə Azərbaycan nümunəsi klassik enerji müstəqilliyindən rəqəmsal inteqrasiya mərhələsinə keçidi göstərir. Enerji sisteminin fiziki dayanıqlılığı ilə rəqəmsal nəzarət mexanizmləri arasında balans məsələsi aktuallaşır. Bu isə ET-nin yalnız resurs və infrastruktur səviyyəsində deyil, həm də rəqəmsal və texnoloji ölçülərdə qiymətləndirilməsini zəruri edir.

Beləliklə, mövcud yanaşmalar göstərir ki, ET-nin modeli rəqəmsallaşma mərhələsində genişləndirilməli və kibersuverenlik ölçüsü ilə tamamlanmalıdır.

VI. Təklif Olunan İnteqrativ Qiymətləndirmə Modeli

Bu nəticələr əsasında ET kibersuverenlik kontekstində

inteqrativ qiymətləndirilməsi üçün üçölçülü model təklif olunur.

A. Fiziki-enerji ölçüsü

Bu ölçü generasiya gücünün yetərliliyi, ötürmə və paylayıcı şəbəkələrin etibarlılığı, infrastrukturun modernləşmə səviyyəsi və ehtiyat güc göstəriciləri ilə bağlıdır. O, klassik ET yanaşmasının əsasını təşkil edir.

B. Rəqəmsal dayanıqlılıq ölçüsü

Bu ölçü enerji sisteminin idarəetmə arxitekturasının kibermüdafiə səviyyəsini, SCADA və ƏT-nın təhlükəsizliyini, məlumat axınlarının qorunmasını və kiberinsidentlərin idarə olunması mexanizmlərini əhatə edir.

C. Strateji-texnoloji *ölçü*

Bu ölçü enerji sisteminin əsas texnoloji və proqram təminatı komponentləri üzərində nəzarət imkanlarını, avadanlıq və proqram təminatı üzrə asılılıq səviyyəsini, eləcə də milli texnoloji kompetensiyanı əhatə edir.

Təklif olunan model ET-ni fiziki, rəqəmsal və strateji komponentlərin qarşılıqlı əlaqəsi əsasında qiymətləndirməyə imkan verir. Ölçülərdən hər biri ayrıca təhlil oluna bilsə də, sistemin ümumi dayanıqlılığı onların balanslı inteqrasiyasından asılıdır.

Beləliklə, bu struktur çərçivə enerji siyasətinin prioritet istiqamətlərinin müəyyənləşdirilməsi və risklərin sistemli qiymətləndirilməsi üçün metodoloji çərçivə rolunu oynaya bilər.

NƏTİCƏ

Rəqəmsal transformasiya ET-nin ənənəvi məzmununu keyfiyyətcə dəyişdirmişdir. Aparılmış nəzəri təhlil göstərir ki, resurs yönümlü klassik model müasir kiber-fiziki enerji sistemlərinin struktur risklərini tam əhatə etmir. Enerji sistemlərinin dayanıqlılığı artıq yalnız generasiya gücü və təchizat sabitliyi ilə deyil, rəqəmsal idarəetmə mexanizmlərinin təhlükəsizliyi və texnoloji avtonomluq səviyyəsi ilə müəyyən olunur. Bu şəraitdə ET ilə kibersuverenlik arasında struktur qarşılıqlı asılılıq formalaşır. Enerji infrastrukturu rəqəmsal platformalar və alqoritmik idarəetmə sistemləri ilə inteqrasiya olunduqca, fiziki və rəqəmsal səviyyələr vahid sistem bütövlüyü təşkil edir. Nəticədə ET yalnız təchizatın davamlılığı deyil, həm də dövlətin kritik rəqəmsal infrastruktur üzərində strateji nəzarət imkanlarını əhatə edən kompleks təhlükəsizlik kateqoriyasına çevrilir. Təqdim edilən konseptual çərçivə ET-ni fiziki, rəqəmsal və strateji-texnoloji ölçülərin qarşılıqlı əlaqəsi kontekstində təhlil etməyə imkan verir və göstərir ki, texnoloji asılılıq və rəqəmsal idarəetmə üzərində məhdud nəzarət uzunmüddətli perspektivdə sistem sabitliyinə təsir göstərə bilər. Rəqəmsallaşma mərhələsində ET dövlətin kibersuverenliyinin ayrılmaz komponenti kimi qiymətləndirilməlidir. Bu konseptual dəyişiklik təhlükəsizlik anlayışını klassik resurs modelindən idarəetmə və nəzarət əsaslı sistem yanaşmasına doğru genişləndirir və enerji siyasətində texnoloji suverenlik indikatorlarının nəzərə alınmasını zəruri edir.

ƏDƏBİYYAT

[1] International Energy Agency, World Energy Outlook 2023. Paris: IEA, 2023. [Online]. Available: https://www.iea.org/reports/world-energy-outlook-2023.

[2] European Network of Transmission System Operators for Electricity (ENTSO-E), Ten-Year Network Development Plan 2024–2034, 2025. [Online]. Available: https://tyndp.entsoe.eu/?utm_source=chatgpt.com.

[3] D. Abraham, S. H. Houmb, L. Erdodi, "Cyber-Attacks on Energy Infrastructure–A Literature Overview and Perspectives on the Current Situation," Applied Sciences, 15(17), 9233, 2025. https://doi.org/10.3390/app15179233

[4] European Parliament and Council of the European Union, Directive (EU) 2022/2555 (NIS2), 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[5] European Union Agency for Cybersecurity (ENISA), Threat Landscape 2025, 2025. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

[6] J. Wang et al., "Achieving energy security amidst the world uncertainty in newly industrialized economies: The role of technological advancement," Energy, Volume 261, Part B, 1252565, 2022. https://doi.org/10.1016/j.energy.2022.125265.

[7] A. Cherp, J. Jewell, "The concept of energy security: Beyond the four As," Energy Policy, vol. 75, pp. 415-421, 2014. https://doi.org/10.1016/j.enpol.2014.09.005.

[8] R. Schmitz, et al., "Energy security and resilience: Revisiting concepts and advancing planning perspectives for transforming integrated energy systems," Energy Policy, 207, 114796, 2025.

[9] L. Rodríguez-Fernández, A. B. F. Carvajal, V. F. de Tejada, "Improving the concept of energy security in an energy transition environment: Application to the gas sector in the European Union," The Extractive Industries and Society, Volume 9, 101045, 2022. https://doi.org/10.1016/j.exis.2022.101045.

[10] D. J. S. Cardenas, A. Hahn, C.-C. Liu, "Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations," IEEE Access, vol. 8, pp. 61161-61173, 2020. Doi: 10.1109/ACCESS.2020.2983313.

[11] OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, OECD Publishing, Paris, 2015. [Online]. Available: https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm.

[12] Azərbaycan 2030: sosial-iqtisadi inkişafa dair Milli Prioritetlər. Azərbaycan Respublikası, 2021, Bakı.

New Requirements for State Cyber Sovereignty and Energy Security

Shakir Mehdiyev[1], Nazrin Rzayeva[2]

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

Abstract— Digital transformation has fundamentally reshaped the functioning mechanisms of public administration, industry, and critical infrastructure. The integration of energy systems with digital platforms, SCADA systems, intelligent networks, and data processing technologies redefines the very nature of energy security. Under contemporary conditions, energy security is no longer limited to the uninterrupted supply of energy resources; it increasingly encompasses the cybersecurity of control systems, data protection, and the reduction of technological dependencies. This article analyzes energy security within the framework of state cyber sovereignty, substantiates the structural relationship between these two concepts, and proposes a conceptual approach to their integration.

Keywords— cyber sovereignty; energy security; critical infrastructure; cyber-physical systems; resilience; technological independence.