Enerji sektorunda kibertəhlükəsizliyin təmin olunması məsələləri haqqında

Təhmasib Fətəliyev[1], Şahanə Mansurova[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1,2]*depart3@iit.science.az*

***Xülasə*— Məqalə milli təhlükəsizliyin kritik tərkib hissəsi kimi enerji sektorunda kibertəhlükəsizlik problemlərinin tədqiqinə həsr olunub. Enerji təhlükəsizliyi problemləri araşdırılmış, parametrik göstəricilərin təsnifatı, enerji sektorunda kibertəhlükəsizliyin xüsusiyyətləri və təmin olunması məsələri təqdim edilmişdir. Azərbaycanda bü sahədə siyasət və alternativ enerji perspektivləri verilmişdir.**

Açar sözlər— enerji sektoru; enerji təhlükəsizliyi; kibertəhlükəsizlik; təhlükəsizlik riskləri; enerji birliyi.

I. GİRİŞ

Enerji təhlükəsizliyi həm fərdi dövlətlərin, həm də bütövlükdə dünya təhlükəsizliyinin vacib bir komponentidir. Müasir kəskin geosiyasi qarşıdurma şəraitində ölkə iqtisadiyyatı, suverenliyi və müdafiə qabiliyyəti birbaşa enerji təhlükəsizliyinin təmin edilməsindən asılıdır. Buna görə strateji sahə sayılan enerji sektorunun tam dövlət nəzarətində olması milli təhlükəsizliyə nəzarətin vacib şərtidir.

Enerji təhlükəsizliyi məsələlərinin həllində təbii ehtiyatların əvəzedilməz olması nəzərə alınmalıdır. Bu resurslar, ümumiyyətlə, inkişaf etməkdə olan ölkələrdə istehsal və inkişaf etmiş ölkələr tərəfindən isə istehlak olunur və nəticədə onların arasında sosial-iqtisadi münasibətlərin bərabərsizliyinə gətirib çıxarır. Mürəkkəbliyi səbəbindən enerji təhlükəsizliyi konsepsiyası tamamilə iqtisadi, həm də texniki və təşkilati xarakter daşıyır. Ümumiyyətlə, enerji təhlükəsizliyinin formalaşması ilə bağlı təhdidlər daxili və xarici iqtisadi, siyasi, sosial-siyasi, texnogen və təbii sahələrdə mövcuddur. Terrorizm hallarının artması ilə xarakterizə olunan müasir şəraitdə yüksək riskli obyektlərə olan təhdidlərin sayı da sürətlə artır, ona görə də bu kritik bir problem kimi nəzərə alınmalıdır. Enerji təhlükəsizliyi obyektlərinə nüvə və su elektrik stansiyaları, neft platformaları, qaz və neft boru kəmərləri, karbohidrogen ehtiyatları, elektrik xətləri və s. aid edilir. Bu obyektlərə vurulan ziyanlar milli iqtisadiyyat üçün kritik və zərərli sosial hallar yarada bilər. Bütün bunlar, milli təhlükəsizliyin kritik tərkib hissəsi kimi enerji təhlükəsizliyinin təmin olunmasının aktual məsələ olmasına əsas verir.

Məqalədə milli təhlükəsizliyin mühüm tərkib hissəsi kimi enerji sektorunda kibertəhlükəsizlik məsələləri araşdırılmışdır.

II. ENERJİ TƏHLÜKƏSİZLİYİ, PROBLEMLƏR VƏ PARAMETRİK GÖSTƏRİCİLƏR

Enerjinin səmərəliliyi enerji təhlükəsizliyinə nail olunmasında əhəmiyyətli rol oynayır. Enerji təhlükəsizliyinin artırılması cəmiyyətin əsas məqsədi və davamlı enerji strategiyalarından ibarətdir, çünki enerji təhlükəsizliyi əsas insan ehtiyaclarını yerinə yetirmək üçün tələb olunur.

Enerji təhlükəsizliyi siyasəti probleminin vacibliyi onun sosial-iqtisadi sistemdə istifadəsinin aşağıda göstərilmiş dörd əsas aspektindən ibarət olan ümumi ictimai əhəmiyyətinə əsaslanır:

- əsas insan ehtiyaclarının və iqtisadi fəaliyyətin enerji tələbatının təmin edilməsi;
- müasir cəmiyyətin mövcud infrastrukturunun səviyyəsinin saxlanılması;
- əhali, kapital və istehlak artımını təmin etmək üçün enerjidən istifadə;
- iqtisadi infrastrukturda, texniki inkişafda və məhsuldarlığın artımında dəyişikliklərin dinamikasını təmin etmək.

Enerji təhlükəsizliyinə sistemin bütün ölçülərində istənilən təhdidlərdən asılı olmayaraq optimal və davamlı fəaliyyət göstərən xüsusiyyəti (ölçü, vəziyyət və ya statusu) kimi baxmaq olar. Bu tərifə əsasən bütün perspektivlər və risklər nəzərə alınır [1]. Enerji təhlükəsizliyinin ölçüləri və onlara uyğun parametrlərin təsnifatı aşağıdakı kimidir:

Əlçatanlıq – resursların, istehlakçıların və nəqliyyat vasitələrinin mövcudluğu;

Müxtəliflik – mənbələrin, yanacağın (enerji daşıyıcıları), vasitələrin (texnologiyalar, nəqliyyat) və istehlakçıların müxtəlifliyi;

Dəyər – enerjinin qiyməti (istehlakçılar, istehsalçılar, qiymətləri müəyyən edən sistem / subsidiyalar, enerji azlığı, neftin pik həddi və sabitlik), nasazlığın dəyəri və təhlükəsizlik sisteminin xərcləri;

Texnologiya və səmərəlilik – yeni texnologiyaların inkişafı, enerji sisteminin effektivliyi, enerji tutumluluğu və enerji qənaəti;

Yerləşmə – enerji sistemlərinin sərhədləri, enerji mənbəyinin yeri, sıxlıq əmsalı (mərkəzləşdirilmiş/paylanmış),

DOI: 10.25045/NCInfoSec.2018.26

torpaqdan istifadə, qloballaşma, əhalinin yerləşməsi və sıxlığı, coğrafiya və sənaye intensivliyi;

Müddət – vaxt şkalası, hadisənin müddəti və effektin müddəti (mübarizə və ya zərbə);

Adaptivlik – adaptiv tutum;

Ətraf mühit – resursların kəşfiyyatı və paylanması, ekstraksiya və nəql olunma metodları, enerji istifadəsindən çıxan nəticələr, ətraf mühitin dəyişməsindən yaranan təsir və su hövzəsi ilə əlaqə;

Sağlamlıq – insan sağlamlığının enerji sisteminə təsiri və enerji sisteminin sağlamlığa təsiri (enerji sektoru işçiləri, istehlakçılar və beynəlxalq ictimaiyyət);

Mədəniyyət – enerji sisteminə mədəni təsir (istehsal, əlaqə, istehlak, mədəni aspektlər) və mədəni aspektləri formalaşdıran enerji şərtləri;

Savadlılıq – informasiyanın əlçatanlığı (keyfiyyət, bazar məlumatı, ictimaiyyətin məlumatlandırılması və strukturlaşdırılmış təhsil proqramı), informasiyanın təqdimatı və təminatı; enerji məlumatlarından istifadə;

Məşğulluq – enerji təhlükəsizliyinin işsizliyin səviyyəsinə təsiri və məşğulluğun səviyyəsinin enerji təhlükəsizliyinə təsiri;

Siyasət – siyasi sistem, demokratiya/diktatura (təbiət, sabitlik, vətəndaşın iradəsi, daxili və xarici əlaqələr), tənzimləmə (liberallaşdırılmış və nəzarət edilən bazar, qaydalar və subsidiyalar) və idarəetmə (şəffaflıq qaydalarına tabe olmaq, selektiv qaydalara riayət etmək və qaydalara əməl etməmək/korrupsiya);

Hərbi – enerjinin hərbi məqsədlər üçün istifadəsi, hərbiləşmə, hərbi münaqişədə enerji vasitə kimi (enerji silahı) və destabilizasiya amili (resurslara həmlələr, ətraf mühitin korlanması və zorakılıq iqtisadiyyatı);

Kiber təhlükəsizlik – əlaqələr (kiberhücumlar), proqram vasitələrindən istifadə (müşahidə nəzarəti və məlumatların əldə edilməsi, SCADA, proqramların nasazlıqları) və İT bacarıqları.

Enerjidən istifadə etmək üçün texnologiya tələb olunduğundan, enerji təhlükəsizliyi texnologiyanın inkişafı ilə birbaşa və dolayı şəkildə əlaqəlidir. Bu mənada istehsal, ötürmə, emal, saxlama və paylaşdırma üçün yeni texnoloji həllər enerji təhlükəsizliyinə təsir göstərir. Beləliklə, yeni texnologiyalar yeni enerji mənbələrini təmin etməklə bərabər nəticədə enerji təhlükəsizliyini artırır. Məsələn, yeni elektroliz texnologiyalarının tətbiqi, enerji sisteminə fosil yanacağından başqa yeni bir alternativ enerji daşıyıcısı (hidrogen) qazandırdı. Bərpa olunan enerjilərin inkişaf etdirilməsi bəzi tədqiqatçılar tərəfindən şübhə altına alınsa da, digərləri isə “daha təhlükəsiz enerji gələcəyinin” açarı olduğunu vurğulayırlar [2].

İT sahəsindəki inkişaf meyllərini nəzərə almaqla enerji sektorunun təhlükəsizliyini yalnız fiziki baxımdan deyil, eyni zamanda kiber mənada da qiymətləndirmək vacib məsələlərdən biridir. Kompüter və rəqəmsal proqramlardan istifadə enerji sisteminin (istehsal, nəql olunma və istehlak sahələrində) idarə olunmasının əsasını təşkil edir. Ona görə də kibertəhlükəsizliyin nəzərə alınmaması böyük iqtisadi itkilərə səbəb ola bilər. Çünki enerji sistemləri avtomatlaşdırılmış rəqəmsal proqramlarla idarə olunur və İnternetə qoşulur. Onların müdafiəsinə əlavə olaraq, enerji sistemlərinə qarşı kiber hücumlar artır və nəticədə kibertəhlükəsizlik əsas problemə çevrilir. Belə kiber hücumlar daha asandır və enerji infrastrukturunun rəqəmsal proqramları terroristlər üçün cəlbedici bir hədəfdir. Beləliklə, kiber hücumlardan qorunmanın düzgün təşkili enerji təhlükəsizliyinin təmin olunmasında mühüm rol oynayır.

III. ENERJİ SEKTORUNDA KİBER TƏHLÜKƏSİZLİK

Avropa Komissiyası (AK) üzv dövlətlərlə birlikdə 2016-cı ildə qəbul etdiyi “Şəbəkə və İnformasiya Sistemlərinin Təhlükəsizliyi üzrə Direktiv”i (*Directive on security of network and information systems – NIS Directive*) [3] və “Verilənlərin Mühafizəsinin Ümumi Qaydaları” *(General Data Protection Regulation – GDPR)* [4] ilə kibertəhlükəsizliyin təməlini qoymuşdur. Bu sənədlər Avropa cəmiyyətinin maraqları və vətəndaşları üçün lazımlı xidmətlərin fəaliyyətini müdafiə edərək, AK-nın “Rəqəmsal vahid bazar” (*Digital Single Market*) strategiyasına dəstək verir.

NIS Direktivi və *GDPR* sektorlar arasında fərqləndirmə aparmadan, öhdəlik səviyyəsi yalnız göstərilən xidmətlərin kritikliyindən asılı olan sahələrarası bir yanaşmanı təmsil edir. AK özünün “Enerji Ekspert Kiber Təhlükəsizlik Platforması”na (*Energy Expert Cyber Security Platform – EECSP)* enerji sektorunu mövcud qanunvericiliyin kifayət qədər əhatə etdiyini araşdırmaq və lazımsa, effektiv kibertəhlükəsizliyə nail olmaq üçün əlavə tədbirlərin görülməsi üçün tapşırıq vermiş və müvafiq nəticələr əldə etmişdir. Qeyd etmək lazımdır ki, *EECSP* ekspert qrupunun missiyası AK-na avropa səviyyəsində infrastruktur məsələləri, təchizatın təhlükəsizliyi, smart şəbəkə texnologiyaları və nüvə enerjisi daxil olmaqla enerji sektorunun açar nöqtələrinə aid siyasət və normativ sənədlər barəsində təkliflər verməkdir [5].

Kritik infrastrukturlar müasir cəmiyyətin fəaliyyəti üçün əsas xidmətləri dəstəkləyir və iqtisadi fəaliyyətin əsasının təşkilinə xidmət göstərir. Bunlara enerji, telekommunikasiya, maliyyə, səhiyyə və nəqliyyat sektorları aid edilir. Enerji infrastrukturu ən mürəkkəb və kritik infrastrukturun əsas hissəsi sayıla bilər, çünki digər sektorların xidmətlərinin təmin edilməsi ondan asılıdır. Buna görə də enerji tələbatının təmin olunmaması iqtisadiyyata və vətəndaş cəmiyyətinin düzgün fəaliyyətinə mənfi təsir göstərir. AK tərəfindən enerji sektoru elektrik, neft və qaz kimi üç alt sektorla müəyyənləşdirilmişdir.

Rəqəmsal texnologiyalar enerji sektorunda getdikcə daha əhəmiyyətli rol oynayır. Smart enerji sistemləri enerjinin istehsalını, ötürülməsini, şəbəkə idarəçiliyini və bazar ilə əlaqəli vəzifələrini insanlarla bağlı bir sistemdən daha həssas və daha sürətlə həyata keçirir, beləliklə enerji idarəçiliyinin optimallaşdırılmasına, ondan istifadəyə üstünlük verilməsinə və nasazlıqların tez aradan qaldırılmasına nail olunur.

Enerji idarəetmə sistemləri əsasən real vaxt rejimində fəaliyyət göstərən və tipik olaraq mərkəzi nəzarət stansiyası və ya mərkəzinə qoşulan, bir-biri ilə iyerarxik əlaqəli fiziki və elektron sensorlar, idarə və nəzarət qurğularından təşkil olunur.

“Verilənlərin dispetçer idarə olunması və toplanması” *(Supervisory Control And Data Acquisition – SCADA)* sistemlərindən təşkil olunmuş enerji idarəetmə sistemləri ərazi cəhətdən paylanmış mühitdə elektrik enerjisinin ötürülməsi və paylanması şəbəkələrində əməliyyatların monitorinqini və nəzarətini həyata keçirir. *SCADA* sistemləri uzaqda yerləşmiş məlumat toplama yerlərindən, sensorlardan, nəzarət, idarə qurğularından, və avtomatlaşdırılmış funksiyalardan məlumat toplayır, nümayiş etdirir və saxlayır. Onlar real vaxt rejimində istifadə olunan proseslərin idarəetmə sisteminin (məsələn, ötürülmə və paylanmada) bir hissəsini təşkil edir. “Paylanmış nəzarət sistemi” *(Distributed control systems – DCS)* isə ayrı-ayrı obyektlər və ya kiçik coğrafi sahələr üçün istifadə olunur. İdarəetmə sistemləri uzaq məsafədə yerləşən terminal qurğuları və proqramlaşdırılmış məntiqi kontrollerlərə qoşulmuşdur. Bu qurğular giriş verilənləri və siqnallarına cavab olaraq sistem verilənlərinə nəzarət edir və müvafiq idarəetmə funksiyaları həyata keçirir.

Generasiya sistemlərində enerji istehsalı prosesləri nəzarət altına alınmalıdır. Neft, kömür və ya qazın yanması və nüvə parçalanma prosesləri turbinləri hərəkətə gətirmək üçün istifadə olunan istilik istehsal edir. Bu turbinlər enerji istehsal edir və bütün istehsal prosesi operatorların izlədiyi əsas dispetçer məntəqəsinə bağlanan analog və ya rəqəmsal sistemlər tərəfindən idarə olunur. Bərpa olunan resurslar (külək, günəş, hidro enerjilər) bir-biri ilə olduqca əlaqəli olan sistemlərdir və enerji istehsalını, külək və günəş kimi resursların təbii kəsilmə davranışlarını nəzərə alan mərkəzi stansiyalar tərəfindən idarə olunur.

Hal-hazırda enerji sektoru köhnə, həm də yeni nəsil texnologiyalardan ibarətdir. Müasir texnologiyalar enerji infrastrukturuna keçmişə nəzərən daha qabaqcıl yollarla (ikitərəfli naqil, simsiz rabitə və s.) əlaqə quran yeni ağıllı komponentlər (smart elektrik və qaz sayğacları, rəqəmsal klapanlar və nasoslar və s.) gətirir. Bu yeni komponentlər İT-na əsaslanır. Tipik olaraq, ehtiyyat hissələrinin artıq mövcud olmadığı və ya istifadə olunmadığı üçün analog komponentlər yeni rəqəmli sistemlərlə əvəz olunur.

Beləliklə, İT-nin belə geniş tətbiqi ilə enerji təminatı sistemlərində kiber risklərə və təhdidlərə qarşı davamlılığın təmin edilməsi daha vacib xarakter alır [6]. Kibertəhlükəsizliyin enerji sektorunda mühüm problemi kiber hücüm halında belə etibarlılığı və dayanıqlılığı dəstəkləməkdir. İT sistemlərindən fərqli olaraq, enerji sektorunda kiber hücumların təhlükəsizlik problemləri, nasazlıqlar və hətta elektrik kəsintiləri ilə nəticələnə biləcəyindən idarəetmə sistemi dayanmadan fəaliyyətini davam etdirməyə hesablanmalıdır.

Kibertəhlükəsizlikdə məxfilik, tamlıq və əlçatanlıq kimi ümumi üç müdafiə məqsədi qəbul edilmişdir. Enerji sektorunda ən yüksək prioritetli məsələ sektorda sahə tətbiqləri ilə bağlıdır. Məsələn, generasiya və ötürülmədə əlçatanlıq və tamlıq ən vacib olanlardır. Dəyişdirilmiş və ya gecikmiş məlumatlar qurğuların yanlış konfiqurasiya olunmasına və nəticədə sistemin etibarlılığına təsir göstərə bilər. Qabaqcıl ölçmə infrastrukturu üçün müştərinin şəxsi məlumatlarının məxfiliyi ən vacib olanıdır. Kompüter təhlükəsizliyi olaraq adlandırılan kibertəhlükəsizlik nüvə təhlükəsizliyinin bir hissəsidir. Burada kompüter təhlükəsizliyinin müdafiəsinin məqsədləri nüvə və ya digər radioaktiv maddələrin icazəsiz dəyişdilməsi, nüvə materialları və obyektlərinə qarşı təxribat və ya nüvə məlumatlarının oğurlanmasına gətirib çıxara biləcək kiber hərəkətlərin qarşısını almaqdır.

EECSP ekspertləri enerji sektoruna aid olan kibertəhlükəsizlik sahəsindəki problemləri aşağıdakı kimi təqdim edirlər:

- Transsərhəd əlaqəli enerji şəbəkəsində dayanıqlıq.
- Cari təhdid və riskləri əks etdirən müdafiə konsepsiyaları.
- AB-də kiber hücumların emalı.
- Mövcud enerji şəbəkəsi və ya nüvə obyektinin layihələndirilməsində tam şəkildə nəzərə alınmayan kiber hücumların effekti.
- Yüksək əlaqələndirilmiş yeni texnologiyaların və xidmətlərin tətbiqi.
- İnfrastruktur və xidmətlərdə autsorsinqi.
- Enerji sistemlərində istifadə olunan komponentlərin bütövlüyü.
- Bazar iştirakçıları arasında yüksək qarşılıqlı əlaqə.
- İnsan resurslarının mövcudluğu və onların bacarığı.
- Real zaman/əlçatanlıq rejimində olan tələblərdən fərqli kibertəhlükəsizlik tədbirlərinə qoyulan məhdudiyyətlər.

IV. AZƏRBAYCANDA ENERJİ TƏHLÜKƏSIZLİYİ VƏ ENERJİ BİRLİYİ PERSPEKTİVLƏRİ

Azərbaycan neft və qaz kimi ənənəvi enerji resursları ilə məşhur olan, enerji baxımından zəngin bir ölkədir. Enerji təhlükəsizliyi diğər ölkələrdə olduğu kimi Azərbaycanın milli təhlükəsizliyinin əsasını təşkil edir. Enerji təhlükəsizliyi strategiyası 1994-cü ildə “Əsrin müqaviləsi” imzalandıqdan başlamışdır. “Əsrin müqaviləsi” ölkənin iqtisadi inkişafında, həm də dünya enerji tədarükü üçün yanacaq və enerji ehtiyacının təmin edilməsi prosesində fövqəladə yer tutur. Strateji və əhəmiyyətli obyektlərin etibarlı enerji təchizatı, boru kəmərlərinin təhlükəsizliyi, enerji mənbələrinin diversifikasiyası, ekoloji tələblərin nəzərə alınması və enerji resurslarının səmərəli istifadəsi Azərbaycanın enerji təhlükəsizliyi prinsiplərini təşkil edir [7]. Bu prinsiplərə görə enerji təhlükəsizliyi risklərini aşağıdakı kimi təyin etmək olar:

- Alternativ enerji mənbələrindən istifadə etməklə tükənən enerji resursları olan neft və qaz hasilatının azaldılması.
- Neft və qaz boru kəmərlərinin təhlükəsizliyi.
- Enerji resurslarının sabitliyi və səmərəliliyi.

- Alternativ enerji ehtiyatlarının istehsalının çatışmazlığı.

Milli Enerji Strategiyasına əsasən aşağıdakı həll və imkanları qeyd edək:

- Azərbaycanın tranzit və ixrac boru kəmərlərinin təhlükəsizliyinin artırılması;
- Müasir Avropa standartlarına əsaslanan enerji infrastrukturunun yaradılması;
- Tranzit ölkə olaraq Xəzər hövzəsi və Orta Asiyadan fosil yanacaq enerjisinin həcmini artırmaq;
- Azərbaycanda hərtərəfli enerji tələbatının idarəetmə siyasətini inkişaf etdirmək, başqa sözlə, tələbatın azaldılması;
- Bərpa olunan enerji ehtiyatlarından istifadənin artırılması;
- Enerji resurslarının tədricən təmin edilməsi baxımından enerji resurslarının diversifikasiyası və təhlükəsizliyi.

Avropa birliyi (AB) və Şərq tərəfdaşlığı *(Eastern Partnership – EaP)* ölkələri ilə əməkdaşlıq münasibətləri enerji təhlükəsizliyi problemlərinin səmərəli şəkildə həll edilməsi üçün şərait yaradır. Azərbaycan iqtisadiyyatının enerji sektoru sayəsində inkişaf etdiyini nəzərə alaraq ölkə bu sektoru inkişaf etdirməyə maraqlıdır. Qərb ölkələri Azərbaycanı AB də enerji təhlükəsizliyinin əsas təminatçısı hesab edərək onunla strateji münasibətlərinin səviyyəsini qaldırdılar. Nəticədə, 7 noyabr 2006-cı ildə Azərbaycan Respublikası ilə AB arasında strateji tərəfdaşlığın enerji məsələləri üzrə Anlaşma Memorandumu imzalanmışdır. “Şahdəniz-2” layihəsi çərçivəsində 2013-cü ilin dekabr ayında, dünyanın aparıcı neft-qaz şirkətləri və bir çox Avropa ölkələri tərəfindən təbii qazın istehsalı, pay bölgüsü və ixracatı haqqında son investisiya qərarının imzalanması yalnız Azərbaycan üçün deyil, habelə Avropa və dünyanın enerji təhlükəsizliyinin təmin edilməsində mühüm rol oynayacaqdır. “Şahdəniz-2” layihəsi, Azərbaycan və Gürcüstan arasında Cənubi Qafqaz boru kəmərinin Trans - Asiya və Transadriatik qaz boru xəttini genişləndirərək Avropanın inşaat planlarının həyata keçirilməsinə kömək edəcək və yeni qaz dəhlizi açacaqdır. Bu məsələlər təhlükəsizlik problemlərinin idarə olunması baxımından Azərbaycan təcrübəsini göstərir. Ənənəvi enerji ehtiyatları bərpa edilmədiyindən Azərbaycan bərpa olunan enerji ehtiyatlarına investisiya yatırmağa başlamışdır. Artıq həyata keçirilmiş strateji istiqamətləri aşağıdakı kimi sistemləşdirmək olar. Onlardan biri 2004-cü il 21 apreldə qəbul olunmuş “Alternativ və bərpa olunan enerji ehtiyatlarının istifadəsi üzrə Dövlət Proqramı”dır. Digər bir dövlət proqramı 2005-ci ildə qəbul olunmuş “2005-2013-cü illərdə Alternativ və Bərpa Olunan Enerji Mənbələrinin istifadəsi üzrə Dövlət Proqramı”dır. Bu, 2009-cu ildə Alternativ və Bərpa Olunan Enerji üzrə Dövlət Agentliyinin yaradılmasına gətirib çıxarmışdır.

Beləliklə, Azərbaycanın AB və *EaP* ölkələri ilə əməkdaşlığı enerji təhlükəsizliyinin əsas prinsiplərini təşkil edir. Böyük neft və qaz layihələri baxımından bu münasibətlər çox vacibdir. Azərbaycanın Avropa enerji birliyi ilə əməkdaşlığı neft boru kəmərlərinin təhlükəsizliyi, alternativ enerji stansiyalarının tikintisi və inkişafı, enerji sektorunun diversifikasiyası kimi enerji təhlükəsizliyi problemlərinin həllinə öz töhfəsini verir. AB Azərbaycanda neft boru kəmərlərinin təhlükəsizliyi, bərpa olunan və alternativ enerji obyektlərinin tikintisi və inkişafında da əməkdaşlıqda maraqlıdır. Bütün bunlar göstərir ki, Azərbaycan Respublikası əsas enerji strategiyası kimi bu sektoru yeni investisiyalar qoymaqla inkişaf etdirir. Nəticədə yeni iş yerlərinin açılmasını, enerji təhlükəsizliyini, enerji sabitliyini, iqtisadiyyatın və energetikanın diversifikasiyasını və ətraf mühitin qorunmasını təmin etməkdir.

NƏTİCƏ

Milli təhlükəsizliyin kritik tərkib hissəsi olan enerji təhlükəsizliyinin təmin olunması çoxistiqamətli, mürəkkəb və aktual məsələdir. Neft və qaz resursları ilə zəngin olan Azərbaycan üçün bu problem mühüm əhəmiyyətə malikdir. Məqalədə enerji təhlükəsizliyi sahəsində aparılmış araşdırılmalar nəticəsində problemlər, parametrik göstəricilərin təsnifatı təqdim olunmuş, enerji sektorunda kiber təhlükəsizliyin xüsusiyyətləri və təmin olunması məsələləri verilmişdir. Azərbaycanda bu sahədə aparılan siyasət və perspektivlər şərh olunmuşdur.

ƏDƏBİYYAT

[1] A. Azzuni, C. Breyer, “Definitions and dimensions of energy security: a literature review”, WIREs Energy Environ 2018, 7:e268, doi: 10.1002/wene.268

[2] J. Ren, B. Sovacool, “Enhancing China’s energy security: determining influential factors and effective strategic measures" Energy Conver Manage 2014, 88:589–597.

[3] Directive on security of network and information systems, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[4] General Data Protection Regulation, https://eugdpr.org/

[5] Energy Expert Cyber Security Platform, https://ec.europa.eu/energy /sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf

[6] Cyber Security in the Energy Sector, https://ec.europa.eu/energy/sites/ ener/files/documents/eecsp_report_final.pdf

[7] Energy security and energy union perspectives in Azerbaijan, http://cesd.az/new/wp-content/uploads/2015/11/

CYBERSECURITY ENSURING ISSUES IN THE ENERGY SECTOR

Tahmasib Fataliyev and Shahana Mansurova
Institute of Information Technology of ANAS, Baku, Azerbaijan
depart3@iit.science.az

Abstract- The article focuses on cyber security issues in the energy sector as a critical component of national security. Energy security problems have been studied, types of parametric indicators, and features and provision issues of cyber security in the energy sector have been presented. The policy and alternative energy perspectives have been given in this area in Azerbaijan.

Keywords- energy sector, energy security; cyber security; security risks; energy union.