Sənaye 4.0 Platformasında Əşyaların İnternetinin Təhlükəsizliyi Kibersuverenliyin Dayağı kimi

Xumar Şirəliyeva[1], İnci Abdullayeva[2]
[1,2]Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[1]*khumar.shiraliyeva@aztu.edu.az*, [2]*inci.abdullayeva@aztu.edu.az*

***Xülasə*— Sənaye 4.0 platformasında Əşyaların İnternetinin (Industrial IoT) təhlükəsizliyi kibersuverenliyin kritik komponentlərindən biridir: fiziki proseslərin etibarlılığını, strateji əhəmiyyət daşıyan verilənlərin təhlükəsizliyinə nəzarəti və sənaye əməliyyatlarının davamlılığını təmin edir. Sənaye idarəetmə sistemlərinin (ICS) və əməliyyat texnologiyalarının (OT) rəqəmsal şəbəkələrə inteqrasiyası hücum səthini genişləndirərək dövlətlər və təşkilatlar üçün yeni risklər yaradır. Bu məqalədə IIoT sistemində yaranan texnoloji asılılıqlar, kiber risklər, məlumat suverenliyiproblemləri analiz olunur, həmçinin təhlükəsizliyin gücləndirilməsi üçün yanaşmalar təklif olunur. Nəticədə IıoT təhlükəsizliyi sadəcə texniki məsələ deyil, eyni zamanda milli təhlükəsizlik və iqtisadi dayanıqlılıq konteksində strateji prioritet kimi əsaslandırılır.**

Açar sözlər— kritik informasiya infrastrukturu; enerji sektoru; kibertəhlükəsizlik; Əşyaların İnterneti; kibersuverenlik.

I. GİRİŞ

Dövlətin kibersuverenliyi onun öz rəqəmsal məkanı və məlumat infrastrukturu üzərində tam nəzarəti və kiberhücumlara, xarici təsirlərə qarşı qorunmasını əhatə edən anlayışıdır. Əsas məqsəd məlumat və avadanlıqların daxili siyasət və qaydalara görə qorunmasıdır. Sənaye mühitində (IIoT) kibersuverenlik həm ICT (information & communication technology), həm də OT (operational technology) sistemlərini əhatə edir. IIoT və OT, Sənaye 4.0 konsepsiyasının texnoloji bazasını formalaşdıraraq fiziki və rəqəmsal mühitlərin inteqrasiyanını təmin edir. Xüsusilə enerji sektoru kimi kritik informasiya infrastrukturları üçün bu transformasiya əməliyyat səmərəliliyini artırmaqla yanaşı, sistemlərin təhlükəsizlik və dayanıqlılıq tələblərini də köklü şəkildə dəyişir.

Bununla belə, enerji infrastrukturlarının IIoT əsaslı rəqəmsallaşdırılması yalnız texnoloji üstünlüklər yaratmır, eyni zamanda kibertəhlükəsizlik, texnoloji asılılıq və məlumat suverenliyi ilə bağlı yeni risklər formalaşdırır. Xarici platformalara, bulud xidmətlərinə və qlobal təchizat zəncirlərinə artan asılılıq kritik enerji sistemlərini geosiyasi və kiber təhlükələr qarşısında daha həssas vəziyyətə gətirir. Bu kontekstdə Sənaye 4.0 mühitində fəaliyyət göstərən enerji infrastrukturlarında kibersuverenlik və əməliyyat davamlılığı məsələləri strateji əhəmiyyət kəsb edir.

Bu məqalənin məqsədi Sənaye 4.0 mühitində IIoT əsaslı enerji infrastrukturlarında texnoloji asılılıq və kibertəhlükəsizlik risklərini sistemli şəkildə təhlil etmək, məlumat suverenliyi kontekstində mövcud boşluqları müəyyənləşdirmək və kritik enerji infrastrukturları üçün konseptual təhlükəsizlik çərçivəsi təklif etməkdir.

II. SƏNAYE 4.0 MÜHİTİNDƏ IIOT ƏSASLI ENERJİ İNFRASTRUKTURLARININ ARXİTEKTURASI

A. Enerji sektorunda Sənaye 4.0 arxitektura modeli

Sənaye 4.0 çərçivəsində enerji infrastrukturları ənənəvi texniki sistemlərdən fərqli olaraq kiber-fiziki sistemlər (Cyber-Physical Systems – CPS) kimi formalaşır. Bu sistemlərdə fiziki enerji prosesləri real-zaman monitorinq və avtomatlaşdırılmış idarəetmə mexanizmləri ilə sıx inteqrasiya olunur. CPS arxitekturasının əsas xüsusiyyəti fiziki və kiber komponentlərin qarşılıqlı asılılığıdır: sensorlar vasitəsilə toplanan əməliyyat məlumatları rəqəmsal platformalarda emal edilir, qərar mexanizmləri isə yenidən fiziki infrastruktura təsir göstərir. Bu cür ikitərəfli əlaqə enerji sistemlərinin səmərəliliyini və çevikliyini artırsa da, eyni zamanda hücum səthini genişləndirir və kiber insidentlərin real fiziki nəticələrə çevrilməsi riskini yüksəldir. CPS təhlükəsizliyi üzrə aparılan tədqiqatlar göstərir ki, bu hibrid sistemlərin qorunması yalnız klassik informasiya təhlükəsizliyi tədbirləri ilə məhdudlaşmır, burada əməliyyat davamlılığı, sistem səviyyəli risklər və cəmiyyət üçün kritik nəticələr də nəzərə alınmalıdır [1]. Xüsusilə enerji infrastrukturları kimi kritik informasiya sistemlərində CPS təhlükəsizliyi texniki məsələ olmaqdan çıxaraq strateji sabitlik və kibersuverənlik kontekstində qiymətləndirilməlidir.

B. Smart grid

Sənaye 4.0 mühitində smart grid konsepsiyası enerji şəbəkələrinin təkmilləşdirilmiş versiyası kimi çıxış edir və IIoT-un CPS arxitekturasının praktiki tətbiq nümunələrindən biridir. Smart grid enerji istehsalı, paylanması və istehlakı proseslərinin iki tərəfli məlumat və enerji axını əsasında idarə edildiyi, heterogen cihazlar və sensorlar tərəfindən dəstəklənən şəbəkə yönümlü enerji sistemidir. Belə sistemlərdə informasiya texnologiyaları və kommunikasiya ənənəvi enerji arxitekturalarına inteqrasiya olunaraq rəqəmsal monitorinq, dinamik yük balanslaşdırma, real-zaman proqnozlaşdırma və aşkar etmə kimi funksiyaları mümkün edir. Smart grid arxitekturası yalnız fiziki enerji axınına fokuslanmır, həm də IIoT əsaslı kommunikasiya və nəzarət mexanizmləri ilə çıxış nöqtələri arasında etibarlı əlaqə təmin edir.

DOI: 10.25045/cyber.gov.2026.47

Müasir smart grid modellərində enerji infrastrukturu təkcə fiziki elektrik şəbəkəsi kimi deyil, həm də proqram arxitekturası, kommunikasiya xidmətləri və məlumat emalı qatlarından ibarət kompleks kiber-fiziki ekosistem kimi nəzərdən keçirilir. Bu çoxlaylı struktur paylanmış enerji resurslarının (DER), ağıllı ölçmə sistemlərinin və real-zaman nəzarət mexanizmlərinin koordinasiyalı fəaliyyətini təmin edir. Smart grid arxitekturası proqram təminatı yönümlü dizayn prinsiplərinə əsaslanaraq enerji sistemlərini yüksək miqyaslana bilən, adaptiv və data-yönümlü platformalara çevirir ki, bu da Industry 4.0 çərçivəsində enerji infrastrukturlarının rəqəmsal transformasiyasını sürətləndirən əsas faktorlardan biridir [2].

C. Edge/Cloud inteqrasiyası

Müasir smart grid arxitekturalarında edge və cloud əsaslı hesablama paradigmaları birgə işləyərək real-zaman emal, gecikmə azaldılması və şəbəkə resurslarının optimizasiyası kimi kritik tələbləri qarşılayır. Edge computing smart grid mühitində sensorlardan və nəzarət cihazlarından toplanan məlumatların mənbəyə yaxın hesablama infrastrukturunda emalını təmin edir ki, bu da gecikməni və bant genişliyi istifadəsini azaldır. Cloud computing isə geniş miqyaslı analiz, böyük verilənlərin saxlanması və maşın öyrənməsi modellərinin öyrədilməsi kimi funksiyaları üzərinə götürərək sistemin strateji qərar qəbuletmə qabiliyyətini artırır.

Bu ikisəviyyəli EC-CC modeli smart grid mühitində paylanmış sensor şəbəkələri, enerji istehsalı, ötürmə və istehlak zəncirində real-zaman idarəetməni mümkün edir. Xüsusilə edge qatında məlumatların əvvəlcədən emalı, şifrələnməsi və filtrasiya olunmuş formada buluda ötürülməsi həm gecikməni azaldır, həm də təhlükəsizlik və məxfilik səviyyəsini yüksəldir. Arxitektura baxımından model perceptron qatından başlayaraq şəbəkə, edge və tətbiq qatlarını birləşdirən iyerarxik struktur kimi fəaliyyət göstərir və CPS əsaslı enerji sistemlərində çevik, miqyaslana bilən və gecikməyə həssas əməliyyatlar üçün optimallaşdırılmış platforma yaradır.

Beləliklə, edge/cloud inteqrasiyası bir-birini tamamlayan iki səviyyəli hesablama modeli formalaşdırır: edge səviyyəsi gecikməyə həssas əməliyyatları idarə edir, cloud səviyyəsi isə uzunmüddətli optimizasiyaya və strateji analitikaya fokuslanır. Bu yanaşma smart grid sistemlərinin işləmə səmərəliliyini və etibarlılığını artırmaqla yanaşı, IIoT əsaslı real-zaman nəzarət və enerji idarəetməsi üçün çevik və miqyaslana bilən arxitektura təmin edir. Tədqiqatlar göstərir ki, EC-CC inteqrasiyası yalnız hesablama səmərəliliyini artırmır, həm də smart grid infrastrukturunun dayanıqlılığını, özünübərpa qabiliyyətini və real-zaman təhlükəsizlik reaksiyasını gücləndirir [3]. Nəticədə edge/cloud strukturu IIoT inteqrasiyasını daha səmərəli hala gətirərək smart grid çevikliyini və operativ davamlılığını yüksəldir.

III. IIoT Ekosistemində Məlumat Suverenliyi və Kibersuverenlik Problemi

A. Data ownership və milli təhlükəsizlik

IIoT ekosistemində məlumat suverenliyi problemi texniki idarəetmə məsələsi olmaqla yanaşı həmçinin milli təhlükəsizlik məsələsinə çevrilmişdir. Enerji infrastrukturlarında generasiya olunan əməliyyat məlumatları yalnız sənaye metrikası deyil, eyni zamanda strateji kritik informasiya resursu hesab olunur. Məlumat üzərində mülkiyyət hüququ konsepsiyası bu kontekstdə məlumat üzərində hüquqi nəzarət, saxlanma yurisdiksiyası və dövlətin müdaxilə imkanları ilə birbaşa əlaqəlidir. Son tədqiqatlar göstərir ki, xarici bulud platformalarına yüksək asılılıq dövlətlərin öz kritik məlumatları üzərində faktiki suveren nəzarətini zəiflədə və transsərhəd hüquqi mexanizmlər vasitəsilə üçüncü tərəf müdaxiləsi riskini artıra bilər [4]. Bu risk xüsusilə enerji kimi strateji sektorlarda daha kəskin xarakter daşıyır, çünki əməliyyat məlumatlarının xarici yurisdiksiyalarda saxlanılması fövqəladə vəziyyətlərdə informasiya əlçatanlığına və infrastrukturun davamlı idarə olunmasına təsir göstərə bilər. Bu baxımdan data ownership yalnız texnoloji arxitektura qərarı deyil, dövlətin kibersuverenlik strategiyasının əsas komponentlərindən biri kimi çıxış edir.

B. Xarici platformaların enerji sektorunda rolu

IIoT ekosistemində xarici texnoloji platformalardan asılılıq problemi data suverenliyindən daha geniş olan texnoloji suverenlik çərçivəsində qiymətləndirilir. Xarici texnoloji platformaların enerji sektorunda dominant mövqeyi IIoT ekosistemində struktur asılılıq yaradır. Müasir enerji infrastrukturları proqram təminatı platformaları, bulud xidmətləri və sənaye IoT ekosistemləri vasitəsilə qlobal texnologiya təchizatçılarına inteqrasiya olunur. Bu inteqrasiya innovasiya sürətini artırsa da, uzunmüddətli perspektivdə texnoloji suverenlik problemləri doğurur. Araşdırmalar göstərir ki, kritik infrastrukturların xarici platformalardan asılılığı dövlətlərin strateji qərarvermə müstəqilliyini zəiflədə və kiber riskləri sistem səviyyəsində artıra bilər [5]. Enerji sektoru kimi yüksək kritik sahələrdə platforma asılılığı yalnız texniki risk deyil, eyni zamanda geosiyasi leverage mexanizminə çevrilə bilər. Bu səbəbdən IIoT arxitekturasının dizaynında platforma müxtəlifliyi və lokal alternativlərin inkişafı kibersuverenliyin əsas komponentlərindən biri kimi qiymətləndirilir.

C. Bulud infrastrukturu və jurisdiksiya riski

Bulud infrastrukturu IIoT əsaslı enerji sistemlərinin miqyaslana bilməsi üçün fundamental texnoloji baza yaratsa da, məlumatların saxlanma yurisdiksiyası ciddi hüquqi və təhlükəsizlik problemləri yaradır. Cloud mühitində məlumatların fiziki yerləşmə məkanı ilə hüquqi nəzarət mexanizmləri arasında uyğunsuzluq yarana bilər. Bu vəziyyət xüsusilə enerji infrastrukturlarında əməliyyat məlumatlarının xarici yurisdiksiyalarda saxlanılması halında dövlət suverenliyi ilə bağlı riskləri artırır. Bulud xidmətlərinin transsərhəd xarakteri hüquqi məsuliyyətin bölüşdürülməsini çətinləşdirir və fövqəladə hallarda məlumat üzərində operativ nəzarəti zəiflədə bilər [6]. Nəticədə jurisdiksiya riski yalnız hüquqi problem deyil, həm də kiber müdafiə strategiyasının ayrılmaz hissəsinə çevrilir və bu risklərin idarə olunması enerji sektorunda IIoT arxitekturasının dizayn mərhələsində nəzərə alınmalıdır.

IV. TEXNOLOJİ ASILILIQ VƏ INDUSTRY 4.0 SİSTEMLƏRİNDƏ KİBER RİSKLƏRİN DƏRİNLƏŞMƏSİ

A. Təchizatçı bağlılığı və platforma asılılığı

Sənaye 4.0 mühitində enerji sektorunun IIoT və bulud platformalarına dərin inteqrasiyası təchizatçı (platforma) bağlılığı kritik təhlükəsizlik və əməliyyat riskinə çevirir. Təchizatçı bağlılığı, sistemlərin spesifik platforma arxitekturalarına və özəl interfeyslərə bağlanması nəticəsində alternativ infrastruktura keçidin texniki və iqtisadi baxımdan çətinləşməsi ilə xarakterizə olunur. Enerji kimi yüksək kritik infrastrukturlarda bu asılılıq yalnız maliyyə və qarşılıqlı işləmə qabiliyyəti problemi deyil, həm də kiber davamlılıq riskidir; çünki müdafiə strategiyalarının çevikliyi platforma məhdudiyyətləri səbəbindən azalır və bərpa mexanizmləri təchizatçı ekosistemi daxilində məhdudlaşır. Tədqiqatlar göstərir ki, bulud əsaslı sənaye sistemlərində portativliyin və açıq standartların zəifliyi uzunmüddətli texnoloji asılılıq yaradır və bu asılılıq fövqəladə hallarda əməliyyat nəzarətinin itirilməsi riskini artırır. Bu səbəbdən kritik enerji infrastrukturlarında arxitektura dizaynı mərhələsində təchizatçı müstəqilliyi, açıq interfeyslər və multi-platform strategiyaları kiber təhlükəsizlik siyasətinin ayrılmaz elementi kimi qiymətləndirilməlidir [7].

B. Təchizat zənciri riskləri

Industry 4.0 mühitində enerji infrastrukturlarının rəqəmsallaşması təchizat zəncirini genişləndirərək kiber risklərin sistem səviyyəsində yayılmasına səbəb olur. IIoT ekosistemlərində istifadə olunan sensorlar, firmware, proqram təminatı modulları və bulud xidmətləri çoxsaylı vendor və subvendorlardan asılı olduğuna görə təhlükəsizlik zəifliyi yalnız lokal komponent problemi kimi qalmır, bütün arxitektura boyunca domino effekti yarada bilər. Təchizat zəncirinə daxil edilən zərərli kod, komprometasiya olunmuş yeniləmələr və ya etibarsız üçüncü tərəf komponentləri kritik enerji sistemlərinə dolayı giriş nöqtəsi yaradır. Araşdırmalar göstərir ki, müasir kiber hücumların əhəmiyyətli hissəsi birbaşa hədəfə deyil, onun təchizat ekosisteminə yönəlir və bu yanaşma hücumun aşkarlanmasını çətinləşdirir. Kritik infrastrukturlar üçün supply chain riskləri yalnız texniki zəiflik deyil, həm də strateji təhlükəsizlik problemidir; çünki hücumçu sistemə rəsmi və etibarlı kanallar vasitəsilə daxil olur. Bu səbəbdən enerji sektorunda IIoT arxitekturasının dizaynı zamanı komponentlərin mənşə izlənməsi, etibarlı yeniləmə mexanizmləri və vendor auditləri əməliyyat davamlılığının əsas şərtlərindən biri hesab olunur [8].

C. OT/IT inteqrasiyası nəticəsində hücum səthinin genişlənməsi

Industry 4.0 mühitində əməliyyat texnologiyalarının (OT) informasiya texnologiyaları (IT) ilə inteqrasiyası enerji infrastrukturlarında funksional səmərəliliyi artırsa da, hücum səthinin əhəmiyyətli dərəcədə genişlənməsinə səbəb olur. Ənənəvi olaraq izolyasiya olunmuş sənaye idarəetmə sistemləri real-zaman monitorinq, uzaqdan idarəetmə və analitika məqsədilə korporativ IT şəbəkələri və bulud platformaları ilə birləşdirildikdə, təhlükə modelləri köklü şəkildə dəyişir. OT sistemləri tarixən təhlükəsizlikdən çox davamlılıq və fasiləsiz işləmə prinsipləri əsasında dizayn olunduğuna görə müasir IT yönümlü kiber hücumlara qarşı struktur zəifliklər nümayiş etdirə bilir. Tədqiqatlar göstərir ki, OT/IT konvergensiyası lateral hərəkət imkanlarını artıraraq hücumçulara aşağı kritik səviyyəli IT komponentindən başlayıb birbaşa fiziki enerji proseslərinə təsir göstərmək imkanı yaradır. Xüsusilə sənaye protokollarının autentifikasiya və şifrələmə mexanizmlərinin zəifliyi bu keçidi daha da asanlaşdırır. Buna görə müasir enerji sistemlərində OT və IT qatları arasında segmentasiya, zero-trust arxitekturaları və sənaye təhlükəsizlik standartlarına uyğun dizayn əməliyyat davamlılığının əsas şərti hesab olunur [9].

D. Enerji sektorunda əməliyyat davamlılığı riskləri

Industry 4.0 əsaslı enerji infrastrukturlarında əməliyyat davamlılığı (operational resilience) yalnız texniki etibarlılıq məsələsi deyil, kritik informasiya infrastrukturlarının sistem səviyyəli sabitliyini müəyyən edən strateji göstəriciyə çevrilmişdir. IIoT inteqrasiyası, paylanmış idarəetmə arxitekturaları və real-zaman data axınları enerji sistemlərinin optimallaşdırılmasını sürətləndirsə də, bu komplekslik kaskad nasazlıqlar və kiber-fiziki domino effektləri riskini artırır. Müasir enerji şəbəkələrində bir komponentdə yaranan kiber insidentin fiziki istehsal, ötürmə və paylama zəncirinə yayılma ehtimalı yüksəkdir və bu, klassik təhlükəsizlik modellərindən daha geniş - davamlılıq yönümlü yanaşma tələb edir. Tədqiqatlar göstərir ki, kritik enerji infrastrukturlarında davamlılıq yalnız hücumların qarşısını almaqla deyil, həm də sistemin zərbəni udmaq, adaptasiya olmaq və sürətlə bərpa olunmaq qabiliyyəti ilə ölçülməlidir. Bu kontekstdə çoxqatlı müdafiə arxitekturaları, redundant idarəetmə kanalları və paylanmış qərar mexanizmləri enerji sistemlərinin kiber-fiziki şoklara qarşı dayanıqlılığını artıran əsas dizayn prinsipləri kimi çıxış edir. Xüsusilə kritik infrastruktur çərçivələri vurğulayır ki, əməliyyat davamlılığı təhlükəsizlikdən ayrı bir konsepsiya deyil; əksinə, təhlükəsizlik, risk idarəetməsi və fasiləsiz xidmət təminatının inteqrasiyasından ibarət vahid strateji modeldir [10].

V. KRİTİK ENERJİ İNFRASTRUKTURLARI ÜÇÜN KİBERTƏHLÜKƏSİZLİK VƏ KİBER SUVERENLİK ÇƏRÇİVƏSİ

A. Security-by-design prinsipləri

Industry 4.0 əsaslı enerji infrastrukturlarında təhlükəsizlik sonradan əlavə edilən qoruma mexanizmi deyil, sistem arxitekturasının başlanğıc mərhələsindən inteqrasiya olunan fundamental dizayn prinsipi kimi qəbul edilməlidir. Security-by-design yanaşması IIoT ekosistemində hər qatın - cihaz, kommunikasiya, platforma və tətbiq səviyyəsinin - təhlükəsizlik baxımından sistematik şəkildə modelləşdirilməsini tələb edir. Bu prinsipə görə autentifikasiya, şifrələmə, giriş nəzarəti və audit mexanizmləri arxitekturanın ayrılmaz komponentləri kimi qurulur, nəticədə hücum səthi struktur səviyyədə daraldılır. Enerji infrastrukturlarında bu yanaşmanın xüsusi əhəmiyyəti ondan ibarətdir ki, burada

təhlükəsizlik boşluğu yalnız məlumat itkisinə deyil, fiziki istehsal fasilələrinə və ictimai təhlükəsizlik risklərinə səbəb ola bilər. Təhlükəsizlik tələblərinin erkən mərhələdə arxitektura modellərinə daxil edilməsi sonradan tətbiq olunan qoruma tədbirləri ilə müqayisədə daha yüksək davamlılıq və daha aşağı əməliyyat riski yaradır [11].

B. Milli səviyyədə texnoloji müstəqillik strategiyaları

Kritik enerji infrastrukturlarında kibersuverenlik yalnız texniki təhlükəsizlik tədbirləri ilə təmin olunmur: bu, eyni zamanda milli səviyyədə texnoloji müstəqillik strategiyalarını tələb edən struktur məsələdir. Xarici platformalardan, proqram təminatından və bulud infrastrukturundan yüksək asılılıq dövlətlərin enerji sektorunda strateji qərarvermə imkanlarını məhdudlaşdıra bilər. Buna görə bir çox ölkələr kritik infrastrukturlar üçün lokal platformaların inkişafı, açıq standartların təşviqi və təchizat zənciri müxtəlifliyinin artırılması istiqamətində siyasətlər formalaşdırır. Bu yanaşma yalnız iqtisadi müstəqilliyi deyil, həm də fövqəladə hallarda operativ nəzarətin saxlanmasını təmin edir. Analitik tədqiqatlar göstərir ki, texnoloji müstəqillik strategiyaları enerji sektorunda risklərin paylanmasını optimallaşdırır və sistem səviyyəli kiber asılılığı azaldır [12].

C. Zero-trust və lokal data idarəetmə modelləri

IIoT əsaslı enerji sistemlərində ənənəvi perimetr təhlükəsizlik modelləri artan paylanmış arxitektura səbəbindən effektivliyini itirir. Zero-trust yanaşması hər bir cihazı, istifadəçini və xidmət komponentini potensial risk kimi qəbul edərək davamlı autentifikasiya və kontekst əsaslı giriş nəzarətini tələb edir. Bu model lokal data idarəetmə strategiyaları ilə birləşdirildikdə enerji infrastrukturlarında həm məxfilik, həm də əməliyyat nəzarəti güclənir. Xüsusilə kritik əməliyyat məlumatlarının milli sərhədlər daxilində saxlanması və emalı kibersuverenlik baxımından strateji üstünlük yaradır. Zero-trust arxitekturası paylanmış enerji sistemlərində lateral hərəkət riskini azaldır və hücumların sistem daxilində yayılmasının qarşısını alır. Müasir təhlükəsizlik araşdırmaları göstərir ki, bu model IIoT mühitində adaptiv və davamlı müdafiə mexanizmlərinin qurulması üçün ən uyğun yanaşmalardan biridir [13].

D. Enerji sektorunda davamlılıq üçün hibrid təhlükəsizlik modeli

Enerji infrastrukturlarının mürəkkəbliyi tək bir təhlükəsizlik paradigması ilə qorunmasını mümkünsüz edir; buna görə hibrid təhlükəsizlik modeli zərurətə çevrilir. Bu model kiber müdafiə, əməliyyat davamlılığı və suverenlik strategiyalarını vahid arxitektura çərçivəsində birləşdirir. Hibrid yanaşma lokal təhlükəsizlik nəzarətləri ilə bulud əsaslı analitika sistemlərini inteqrasiya edərək həm real-zaman müdafiəni, həm də strateji risk monitorinqini təmin edir. Enerji sektorunda bu struktur redundant idarəetmə kanalları, paylanmış ehtiyat sistemləri və avtomatlaşdırılmış bərpa mexanizmləri ilə gücləndirilir. Yalnız texniki təhlükəsizlik tədbirlərinə əsaslanan sistemlər uzunmüddətli sabitlik yarada bilmir; davamlılıq üçün təşkilati, texnoloji və hüquqi qatların inteqrasiyası vacibdir [14].

NƏTİCƏ

Bu tədqiqatın əsas məqsədi IIoT əsaslı enerji infrastrukturlarında data suverenliyi, texnoloji asılılıq və kiber risklər kontekstində təhlükəsizlik çərçivəsi təklif etmək idi. Sistematik ədəbiyyat araşdırması və sektor spesifik analiz nəticəsində aşağıdakı əsas tapıntılar müəyyən edilmişdir:

1) Data və kibersuverenliyin ayrılması: Data suverenliyi əsasən məlumatın idarəsi və məxfiliyi ilə bağlıdır, texnoloji suverenlik isə geniş strategiya və beynəlxalq tənzimləmə aspektlərini əhatə edir. Bu fərqləndirmə enerji sektoru üçün kritikdir, çünki transsərhəd data axınları və bulud infrastrukturu dövlət suverenliyinə təsir edir.

2) Texnoloji asılılıq və kiber risklər: Xarici platformalara və təchizat zəncirinə yüksək asılılıq əməliyyat davamlılığı, hücum səthi genişlənməsi və vendor lock-in kimi riskləri artırır. OT/IT inteqrasiyası əlavə hücum vektorları yaradır.

3) Təklif olunan təhlükəsizlik çərçivəsi: Security-by-design, milli səviyyədə texnoloji müstəqillik, zero-trust yanaşmaları və hibrid təhlükəsizlik modeli kritik enerji infrastrukturunda davamlılığı və suverenliyi təmin edə bilər.

Enerji infrastrukturlarında risklər çoxsahəli və qarşılıqlı əlaqəlidir. Platforma asılılığı, transsərhəd məlumat axınları, OT/IT inteqrasiyası və bulud xidmətlərindən istifadə həm hüquqi, həm texniki, həm də strateji risklər yaradır. Hibrid təhlükəsizlik çərçivəsi bu riskləri sistematik şəkildə idarə etməyə imkan verir və fövqəladə hallarda əməliyyat davamlılığını təmin edir.

Gələcək tədqiqat istiqamətləri:

- IIoT əsaslı enerji sistemləri üçün adaptiv və AI əsaslı təhlükəsizlik monitorinqi metodlarının inkişafı;
- Regional və qlobal səviyyədə kibersuverenlik siyasətlərinin harmonizasiyası;
- Real-time risk qiymətləndirmə metodları və təchizat zənciri şəbəkələrinin dinamik modelləşdirilməsi;
- Lokal bulud və edge computing həllərinin enerjinin paylanmış sistemlərinə inteqrasiyası və sınaqları.

Siyasət və sənaye üçün tövsiyələr:

- Dövlətlər milli enerji infrastrukturunda texnoloji müstəqilliyi gücləndirən siyasətlər tətbiq etməlidir;
- Sənaye qurumları Security-by-design və zero-trust prinsiplərini arxitektura səviyyəsindən tətbiq etməlidir;
- Lokal data idarəetmə və hibrid təhlükəsizlik modelləri kritik əməliyyat məlumatlarının suverenliyini qorumağa yönəldilməlidir;
- Tədqiqat və sənaye arasında davamlı əməkdaşlıq məlumat paylaşımı və risklərin bölüşdürülməsində balans yaratmağa kömək edə bilər.

ƏDƏBİYYAT

[1] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," Computers in Industry, vol. 100, pp. 212–223, Sep. 2018.

[2] R. Ananthavijayan et al., "Software architectures for smart grid system—A bibliographical survey," Energies, vol. 12, no. 6, 2019.

[3] J. Li, C. Gu, Y. Xiang, and F. Li, "Edge-cloud computing systems for smart grid: state-of-the-art, architecture, and applications," Journal of Modern Power Systems and Clean Energy, vol. 10, no. 4, pp. 805–817, 2022.

[4] C. Kuner, "Data sovereignty and the cloud—A comparative analysis of legal frameworks," International Data Privacy Law, vol. 5, no. 3, 2015.

[5] M. Hellmeier and F. von Scherenberg, "A delimitation of data sovereignty from digital and technological sovereignty," in Proc. 31st European Conf. Information Systems (ECIS), Kristiansand, Norway, 2023.

[6] S. Pearson, "Cloud computing and the challenge of data sovereignty," Computer Law & Security Review, vol. 29, no. 3, 2013.

[7] U. Malhotra and R. Nagpal, "Navigating jurisdiction and sovereignty in cloud computing: A comparative legal analysis of India, the US, and beyond," in Proc. World Skills Conf. Universal Data Analytics and Sciences, Indore, India, 2025, doi: 10.1109/WorldSUAS66815.2025.11199204.

[8] D. Petcu, C. Crăciun, M. Neagul, S. Panica, and B. Di Martino, "Portable cloud applications—From theory to practice," Future Generation Computer Systems, vol. 29, no. 6, pp. 1417–1430, 2013.

[9] National Institute of Standards and Technology, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NIST Special Publication 800-161, 2015.

[10] International Electrotechnical Commission, IEC 62443 – Industrial communication networks – Network and system security, IEC Standard Series, 2010–2023.

[11] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, NIST Cybersecurity Framework, Version 1.1, 2018.

[12] ENISA, Security-by-design in Industrial Control Systems, European Union Agency for Cybersecurity, 2021.

[13] OECD, Digital Sovereignty and Strategic Autonomy in Critical Infrastructure, OECD Policy Paper, 2022.

[14] S. Rose et al., Zero Trust Architecture, NIST Special Publication 800-207, 2020.

Industrial Internet of Things Security As a Pillar of Cyber Sovereignty

Khumar Shiraliyeva, Inci Abdullayeva
Azerbaijan Technical University, Baku, Azerbaijan

Abstract - IIoT (Industrial IoT) security is one of the critical components of cyber sovereignty, ensuring the reliability of physical processes, secure control over strategically important data, and the continuity of industrial operations. The integration of Industrial Control Systems (ICS) and Operational Technology (OT) into digital networks expands the attack surface, creating new risks for states and organizations. This article analyzes technological dependencies emerging within IIoT systems, cyber risks, and data sovereignty challenges, while also proposing approaches to strengthen security. As a result, IIoT security is substantiated not merely as a technical issue, but as a strategic priority within the context of national security and economic resilience.

Keywords - Industrial IoT; critical information infrastructure; energy sector; cybersecurity; cyber sovereignty.