Enerji Sektorunda Adaptiv Kibertəhlükəsizlik: Dinamik Risk Modelləri

Fərid Qasımlı[1],Yadigar İmamverdiyev[2]
[1,2]Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[1]*farid.gasimli@aztu.edu.az*, [2]*yadigar.imamverdiyev@aztu.edu.az*

Xülasə— Enerji sektoru digər kritik infrastrukturların fəaliyyətininin təmin edilməsində olduqca vacib rol oynayır və bu səbəbdən dövlət dəstəkli təhdid aktorlarının və yaxşı təşkilatlanmış haktivist qrupların hədəfinə çevrilir. Bu məqalədə enerji sektorunda kibertəhlükəsizlik problemləri sistemli şəkildə təhlil edilmiş, hücumların mərhələli inkişafını modelləşdirmək üçün Markov zənciri əsasında dinamik vəziyyət modeli qurulmuş və qeyri-müəyyənlik şəraitində riskin qiymətləndirilməsi üçün Bayes risk çərçivəsi təklif edilmişdir. Təklif olunan inteqrə olunmuş Markov–Bayes yanaşma riskin zaman üzrə dəyişməsini və posterior ehtimalların yenilənməsini nəzərə alaraq daha dəqiq təhlükə qiymətləndirməsinə imkan verir. Tədqiqat nəticələri göstərir ki, adaptiv və riyazi əsaslandırılmış təhlükəsizlik modelləri enerji infrastrukturunda dayanıqlılığın artırılmasına və strateji qərarların optimallaşdırılmasına əhəmiyyətli töhfə verir.

Açar sözlər— kritik informasiya infrastrukturu; enerji sektoru; kibertəhlükəsizlik; IT-OT konvergensiyası; kiber-fiziki sistemlər; Markov modeli; Bayes risk modeli.

I. GİRİŞ

Enerji sektoru kritik informasiya infrastrukturu kimi milli təhlükəsizliyin əsas komponentlərindən biridir [1]. Enerji istehsalı, ötürülməsi və paylanması sistemlərinin fasiləsiz fəaliyyəti iqtisadi sabitlik və ictimai təhlükəsizlik üçün fundamental əhəmiyyət daşıyır.

Dördüncü sənaye inqilabı (Industry 4.0) çərçivəsində enerji sektorunda istehsal tsiklinin bütün mərhələlərində rəqəmsal platformaların, IoT qurğularının, bulud sistemlərinin və uzaqdan idarəetmə mexanizmlərinin tətbiqi genişlənmişdir. IT və OT sistemlərinin inteqrasiyası əməliyyat effektivliyini artırsa da, hücum səthini əhəmiyyətli dərəcədə genişləndirmişdir [2].

Enerji infrastrukturları uzunömürlü sənaye avadanlıqları, köhnə kommunikasiya protokolları və real vaxt rejimində fasiləsiz işləmə tələbi səbəbindən klassik IT təhlükəsizlik yanaşmalarının birbaşa tətbiqinə uyğun deyil. Mövcud təhlükəsizlik mexanizmləri əsasən məlumatların məxfiliyinə fokuslandığı halda, enerji sektorunda prioritetlər fərqlidir — burada əlçatanlıq (availability) və prosesin bütövlüyü (integrity) əsasdır.

Son illərdə sənaye idarəetmə sistemlərinə qarşı həyata keçirilmiş məqsədli hücumlar, o cümlədən BlackEnergy, Industroyer və TRITON kimi hadisələr göstərmişdir ki, enerji sistemləri artıq yalnız informasiya sızması riski ilə deyil, fiziki dağıntı və genişmiqyaslı enerji kəsintiləri ilə də üz-üzədir.

Bu xüsusiyyət enerji sektorunu klassik IT təhlükəsizlik yanaşmalarından fərqli, kiber-fiziki risklərin kompleks qiymətləndirilməsini tələb edən xüsusi sahəyə çevirir.

Ənənəvi təhlükəsizlik modelləri əsasən perimetr müdafiəsi, siqnatura əsaslı aşkarlama və normativ uyğunluq çərçivəsində qurulmuşdur. Lakin dinamik və çoxmərhələli hücum senariləri fonunda bu yanaşmalar yetərsiz qalırlar. Enerji sistemlərində risk zamanla dəyişir, sistem vəziyyətindən və hücum mərhələsindən asılı olaraq yenilənir. Buna görə də kibertəhlükəsizlik statik qoruma mexanizmi deyil, adaptiv və ölçülə bilən idarəetmə prosesi kimi qiymətləndirilməlidir.

Bu məqalədə enerji sektorunda adaptiv kibertəhlükəsizlik konsepsiyası dinamik risk modelləri prizmasından təhlil edilir. Hücumların mərhələli inkişafını təsvir etmək üçün Markov tipli vəziyyət keçidi modeli, qeyri-müəyyənlik şəraitində riskin adaptiv yenilənməsi üçün isə Bayes ehtimal yanaşması nəzərdən keçirilir. Təklif olunan yanaşma riskin zaman üzrə dəyişməsini, IT-OT qarşılıqlı təsirini və fiziki proses parametrlərinin təhlükə indikatoru kimi rolunu inteqrasiya etməyə imkan verir.

Beləliklə, məqalənin məqsədi enerji sektorunda kibertəhlükəsizliyi müvafiq standartların tələblərinə uyğunluq əsaslı yanaşmadan risk əsaslı, adaptiv və riyazi modelləşdirilmiş təhlükəsizlik yanaşmasına transformasiya etmək üçün konseptual və metodoloji əsas təqdim etməkdir. Adaptiv kibertəhlükəsizlik konsepsiyası sistemin vəziyyətini və müşahidə olunan indikatorları nəzərə alaraq risk parametrlərini davamlı şəkildə yeniləyir, riyazi əsaslandırılmış idarəetmə mexanizmləriini nəzərdə tutur.

II. ENERJİ SEKTORUNUN KOMPONENTLƏRİ

Enerji sektoru yalnız elektrik enerjisinin istehsalı və paylanması ilə məhdudlaşmayan, hasilatdan son istehlaka qədər uzanan kompleks və çoxsəviyyəli ekosistemdir. Bu sektor neft və qaz sənayesini (kəşfiyyat, hasilat, nəql və emal mərhələləri), elektrik enerjisi istehsalı və ötürülməsi sistemlərini, bərpa olunan enerji mənbələrini (günəş, külək, hidro və s.), nüvə energetikasını, istilik və kombinə olunmuş enerji qurğularını, enerji saxlama sistemlərini, həmçinin enerji daşıyıcılarının logistikasını və ticarət platformalarını əhatə edir. Beləliklə, enerji sektoru hasilat–emal–istehsal–ötürmə–paylama–saxlama–ticarət zəncirini birləşdirən vahid, lakin

DOI: 10.25045/cyber.gov.2026.35

funksional baxımdan heterogen struktur kimi xarakterizə olunur.

Bu müxtəliflik enerji infrastrukturunun həm texnoloji, həm də idarəetmə baxımından çoxşaxəli olmasına səbəb olur. Neftayırma zavodları, qaz kompressor stansiyaları, elektrik yarımstansiyaları, külək parkları və enerji bazarlarının informasiya sistemləri fərqli əməliyyat mühitinə malik olsalar da, onların hamısı kiber-fiziki sistemlər üzərində qurulmuşdur və qarşılıqlı asılıdır [6]. Nəticə etibarilə, enerji sektorunda kibertəhlükəsizlik yanaşmaları yalnız elektrik şəbəkələrinin mühafizəsi ilə məhdudlaşmamalı, bütün enerji dəyər zəncirini və bu zəncir üzrə inteqrasiya olunmuş IT–OT infrastrukturu əhatə etməlidir.

III. ENERJİ SEKTORUNDA OT-IT KONVERGENSİYASI

Enerji sektorunda IT texnologiyalar ilə yanaşı, sənaye avtomatlaşdırma texnologiyaları geniş istifadə edilir. Ənənəvi IT sistemlər ilə sənaye idarəetmə sistemləri arasındakı texnoloji və funksional fərqləri nümayiş etdirmək üçün "əməliyyat texnologiyaları" (ing. OT – operational technology) termini istifadə edilir. Əməliyyat texnologiyaları sistemin fiziki vəziyyətini monitorinq etmək və dəyişmək üçün istifadə edilən aparat və proqram təminatıdır.

Enerji sektorunda həm texnoloji zərurət, həm də iqtisadi və əməliyyat effektivliyi tələbi nəticəsində OT–IT konvergensiyası baş verir. Bu proses ənənəvi olaraq bir-birindən təcrid olunmuş OT ilə IT-nin inteqrasiyasını ifadə edir.

OT-IT konvergensiyası enerji sektorunda rəqəmsal transformasiyanın əsas elementlərindən biridir. Ənənəvi olaraq təcrid olunmuş sənaye idarəetmə sistemləri (məsələn, SCADA, PLC və DCS platformaları) korporativ şəbəkələr, bulud infrastrukturu və analitika sistemləri ilə əlaqələndirilir. Bu inteqrasiya real vaxt monitorinqi, proqnozlaşdırıcı texniki xidmət, böyük verilənlər analitikası və mərkəzləşdirilmiş idarəetmə kimi üstünlüklər yaratsa da, eyni zamanda hücum səthini genişləndirir və kiber riskləri artırır. IT mühitində yaranan boşluqların OT sistemlərinə keçməsi fiziki proseslərə birbaşa təsir göstərə bilər ki, bu da enerji istehsalı və ötürülməsində fasilələrə səbəb olur. Buna görə OT-IT konvergensiyası şəraitində adaptiv kibertəhlükəsizlik yanaşmaları, şəbəkə seqmentasiyası, Zero Trust arxitekturası və real vaxt anomaliya aşkarlanması mexanizmləri xüsusi əhəmiyyət kəsb edir.

IV. ENERJİ SEKTORUNDA YENİ NƏSİL KİBERTƏHDİDLƏR

Enerji sektoru rəqəmsallaşma, IT-OT konvergensiyası və kiber-fiziki sistemlərin geniş tətbiqi nəticəsində ənənəvi kibertəhlükələrdən fərqli olaraq daha mürəkkəb, koordinasiyalı və məqsədyönlü hücumlarla üzləşir. Yeni nəsil kibertəhdidlər yalnız informasiya sistemlərini deyil, eyni zamanda fiziki prosesləri, istehsal davamlılığını və milli təhlükəsizliyi hədəf alır.

A. Kiber-fiziki hücumlar

Belə hücumların məqsədi informasiya oğurluğu deyil, fiziki zərər və əməliyyatın dayanmasıdır. Bu tip hücumlar OT sistemləri vasitəsilə fiziki proseslərə təsir göstərir. Hücumçular SCADA, PLC və DCS sistemlərini manipulyasiya edərək, fiziki prosesin parametrlərini dəyişə, iş rejimini poza, qoruyucu sistemləri deaktiv edə bilərlər.

B. Təchizat zənciri hücumları

Enerji infrastrukturu çoxsaylı avadanlıq və proqram təminatı istehsalçılarından asılıdır. Zərərli kodun proqram yeniləmələrinə yerləşdirilməsi və ya sənaye avadanlıqlarının firmware səviyyəsində ələ keçirilməsi genişmiqyaslı risk yaradır. Bu hücumlar ənənəvi perimetr müdafiəsini asanlıqla keçə bilir.

C. APT (Advanced Persistent Threat) qrupları

Dövlət dəstəkli və ya yüksək maliyyələşdirilmiş qruplar uzunmüddətli və gizli fəaliyyət strategiyası tətbiq edir. Onlar uzun müddət aşkarlanmayaraq məlumat toplayır, strateji anda fiziki proseslərə müdaxilə edirlər. Enerji sektoru geosiyasi baxımdan həssas olduğuna görə APT hücumlarının əsas hədəflərindən biridir.

D. Ransomware-in OT mühitinə keçidi

Əvvəllər yalnız IT sistemlərini hədəf alan ransomware hücumları artıq sənaye mühitinə yayılıb. OT şəbəkəsinin şifrlənməsi istehsalın dayanmasına, təhlükəsizlik sistemlərinin söndürülməsinə, böyük maliyyə itkilərinə səbəb olur.

*E. IoT və ağıllı şəbəkə zəifliklər*i

Smart Grid və paylanmış enerji resurslarının artması ilə minlərlə IoT cihazı enerji şəbəkəsinə qoşulur. Bu cihazların zəif autentifikasiya mexanizmləri və gec yenilənən proqram təminatı hücum səthini genişləndirir.

F. Süni intellekt əsaslı hücumlar

Yeni nəsil hücumçular anomaliya aşkarlama sistemlərini aldatmaq üçün düşmən maşın öyrənməsi üsullarından istifadə edir, avtomatlaşdırılmış boşluq axtarışı və hücum senariləri qurur. Bu hücumlar klassik müdafiə mexanizmlərini qeyri-effektiv edə bilər.

E. Hibrid və koordinasiyalı hücumlar

Kiberhücumlar artıq fiziki sabotaj, informasiya müharibəsi və sosial mühəndislik ilə paralel həyata keçirilir. Enerji sektoruna qarşı belə hücumlar genişmiqyaslı sosial və iqtisadi təsir yarada bilər.

V. TƏDQİQATIN METODOLOGİYASI

Enerji sektorunda kibertəhlükəsizlik insidentləri dinamik və mərhələli xarakter daşıyır. Hücumlar, adətən, başlanğıc giriş nöqtəsindən başlayaraq, yayılma hərəkəti, imtiyaz yüksəltmə və fiziki təsir mərhələsinə qədər inkişaf edir. Bu dinamik proseslərin modelləşdirilməsi üçün Markov zənciri və Bayes ehtimal çərçivəsi uyğun riyazi alət hesab olunur [7].

A. Hücumun Markov prosesi kimi modelləşdirilməsi

Tutaq ki, enerji sisteminin təhlükəsizlik vəziyyəti diskret zaman anlarında $X(t) = [x_1(t), x_2(t), \ldots, x_n(t)]$ vəziyyət

dəyişəni ilə ifadə olunur. Enerji sektorunun IT-OT arxitekturasında hücum mərhələləri $S = \{S_0, S_1, S_2, S_3, S_4\}$ sonlu vəziyyətlər çoxluğu kimi təsvir edilir, burada:

S_0 – Normal vəziyyət;

S_1 – İlkin giriş;

S_2 – Yayılmal hərəkəti (IT → OT keçidi);

S_3 – Proses manipulyasiyası;

S_4 – Fiziki təsir.

Keçid ehtimalları aşağıdakı keçid matrisi ilə ifadə olunur:

$$P = \begin{bmatrix} 1-p_{01} & p_{01} & 0 & 0 & 0 \\ 0 & 1-p_{12} & p_{12} & 0 & 0 \\ 0 & 0 & 1-p_{23} & p_{23} & 0 \\ 0 & 0 & 0 & 1-p_{34} & p_{34} \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (1)$$

Burada $p_{ij} = (S_{t+1} = j | S_t = i)$ vəziyyət keçid ehtimalını göstərir, sistemin bir təhlükəsizlik vəziyyətindən digərinə keçmə dinamikasını xarakterizə edir.

S_4 absorbsiya vəziyyəti kimi qəbul edilir, fiziki təsirin və ya əməliyyatın dayanmasının baş verməsini göstərir. Bu yanaşma riski yalnız hadisə kimi deyil, proses kimi qiymətləndirməyə imkan verir.

Uzunmüddətli fiziki təsir ehtimalı:

$$\pi = \lim_{n \to \infty} P^n. \quad (2)$$

Bu model vasitəsilə:

- Müxtəlif təhlükəsizlik arxitekturalarının (məsələn, Zero Trust seqmentasiyası) p_{12} və p_{23} ehtimallarına təsiri ölçülə bilər.
- Müdafiə mexanizmlərinin tətbiqi ilə absorbsiya ehtimalının azalması qiymətləndirilə bilər.

B. *Bayes* risk modeli

Enerji sektorunda risk qeyri-müəyyənlik şəraitində formalaşır. Təhdidlərin prior ehtimalları, zəiflik göstəriciləri və təsir səviyyələri qeyri-dəqiq ola bilər. Bu halda Bayes yanaşması daha uyğun çərçivə təqdim edir.

1. Ehtimalın yenilənməsi Bayes teoremi ilə həyata keçirilir:

$$P(A \mid B) = \frac{P(B|A)P(A)}{P(B)} \quad (3)$$

burada:

A – hücumun uğurlu olması hadisəsi;

B – müşahidə edilən anomaliya və ya indikatordur.

Posterior ehtimal real vaxt rejimində yenilənə bilər və və bu, real vaxt monitorinq məlumatları əsasında risk göstəricisinin dinamik adaptasiyasını təmin edir.

2. Bayes şəbəkəsinin strukturu

Bayes şəbəkəsinə aşağıdakı qovşaqlar daxildir:

- T –təhdid aktoru;
- V – boşluq;
- E – istismar hadisəsi;
- C – nəzarət mexanizmi;
- I – fiziki təsir.

Birgə ehtimal:

$$P(T, V, E, C, I) = P(T)P(V)P(E \mid T, V)P(C \mid E)P(I \mid E, C)$$

Risk aşağıdakı kimi ifadə olunur:

$$Risk = E[I] = \sum P(I_i) Impact(I_i), \quad (4)$$

burada $Impact(I_i)$ fiziki və iqtisadi təsirin ölçüsüdür.

C. Kiber-fiziki inteqrasiya modeli

Kiber hadisə fiziki prosesin parametrlərinə təsir göstərir. Fiziki vəziyyət vektoru:

$$X(t) = [x_1(t), x_2(t), \ldots, x_n(t)] \quad (5)$$

Kibermüdaxilə funksiyasını belə ifadə etmək olar:

$$X(t+1) = f(X(t), u(t), a(t)), \quad (6)$$

burada $u(t)$ – legitim idarəetmə siqnalı, $a(t)$ – hücum təsiridir.

Əgər $X(t)$ vəziyyət vektoru $| X(t) - X_{nominal} | > \delta$ bərabərsizliyini ödəyitsə, sistem təhlükəli zonaya daxil olur.

D. Modelin tətbiqi və elmi yenilik

Bu inteqrasiya olunmuş Markov-Bayes modeli aşağıdakı üstünlükləri təmin edir:

- kiberhücumun mərhələli inkişafını riyazi təsvir edir;
- qeyri-müəyyənlik şəraitində riskin dinamik yenilənməsinə imkan verir;
- fiziki təsiri ehtimal əsaslı qiymətləndirir;
- müdafiə mexanizmlərinin effektivliyini ölçmək olar.

Beləliklə, enerji sektorunda kibertəhlükəsizlik dinamik, ölçülə bilən və optimallaşdırıla bilən ehtimal modeli kimi təqdim olunur.

NƏTİCƏ

Bu məqalədə aparılmış tədqiqat göstərir ki, enerji sektorunda kibertəhlükəsizlik yalnız standartların tələblərinə uyğunluğun yoxlamasından ibarət olmamalıdır. Təklif edilən Markov-Bayes dinamik risk yanaşması hücum mərhələlərini riyazi təsvir etməklə riskin dinamik qiymətləndirilməsini təmin edir və fiziki təsiri ölçülə bilən parametr kimi nəzərə alır. Gələcək tədqiqat istiqamətlərinə dinamik və adaptiv risk modellərinin real zamanda yenilənməsi, maşın öyrənməsi modellərinin inteqrasiyası, oyunlar nəzəriyyəsi əsaslı hücum-müdafiə modelləri, rəqəmsal əkiz platformaları üzərində simulyasiya və risk qiymətləndirməsi daxildir.

ƏDƏBİYYAT

[1] R. M. Alguliyev, Y. N. Imamverdiyev, R. S. Mahmudov, & R. M. Aliguliyev, "Information security as a national security component."

Information Security Journal: A Global Perspective, vol. 30(1), pp. 1-18, 2021.

[2] Y. N. Imamverdiyev, "Analysis of cybersecurity problems in process control systems." Problems of Information Techn”ology, pp. 16-29, 2021.

[3] Y. N. Imamverdiyev, G.M.Muradova, “Neft-qaz sənayesində kibertəhlükəsizlik problemləri.” “İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri” IV respublika konfransı, s.110-112, 2018.

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

[5] D. C. Smith, “Cybersecurity in the energy sector: are we really prepared?.” Journal of Energy & Natural Resources Law, vol. 39(3), pp. 265-270, 2021.

[6] P. Cheimonidis, K. Rantos, “Dynamic risk assessment in cybersecurity: A systematic literature review.” Future Internet;15(10):324, 2023.

[7] O. Theodosiadou, D. Chatzakou, T. Tsikrika, S. Vrochidis, I. Kompatsiaris, “Real-time threat assessment based on hidden Markov models.” Risk Analysis, vol. 43(10):2069-81, 2023.

Adaptive Cybersecurity in the Energy Sector: Markov-Bayesian Dynamic Risk Models

Farid Gasimli[1],Yadigar Imamverdiyev[2]

[1,2]Azerbaijan Technical University, Baku, Azerbaijan

Abstract— The energy sector plays a crucial role in ensuring the operation of other critical infrastructures and, therefore, becomes a target of state-sponsored threat actors and well-organized hacktivist groups. In this article, cybersecurity problems in the energy sector are systematically analyzed, a dynamic state model based on Markov chains is built to model the staged development of attacks, and a Bayesian risk framework is proposed for risk assessment under uncertainty. The proposed integrated Markov–Bayesian approach allows for more accurate threat assessment by taking into account the time evolution of risk and the updating of posterior probabilities. The research results show that adaptive and mathematically based security models make a significant contribution to increasing resilience and optimizing strategic decisions in energy infrastructure.

Keywords– Critical information infrastructure; energy sector; cybersecurity; IT-OT convergence; cyber-physical systems; Markov model; Bayesian risk model.