Virtual Məkanda Fövqəladə Halların Dövlətin Kibersuverenliyinə Təsirinin Analizi və Perspektiv Vəzifələr

Kəmalə Həşimova
İnformasiya Texnologiyaları İnstitutu Bakı, Azərbaycan
hashimovakama@gmail.com

***Xülasə*— Müasir dövrdə rəqəmsallaşma dövlət idarəçiliyinin mərkəzi sütununa çevrildiyi üçün dövlətin suverenlik hüquqları artıq həm fiziki, həm də virtual məkanda qorunmalıdır. Bu tədqiqat işində müasir geosiyasi şəraitdə fövqəladə halların dövlətin rəqəmsal sərhədlərinə və idarəetmə mexanizmlərinə təsiri kompleks şəkildə təhlil olunur. Məqalədə rəqəmsallaşmanın dövlət suverenliyinin ayrılmaz tərkib hissəsinə çevrildiyi vurğulanır və böhran vəziyyətlərində yaranan virtual risklərin milli təhlükəsizliyə yaratdığı təhdidlər araşdırılır. Fövqəladə hallarla əlaqədar virtual məkandə yaranan risklər kompleks şəkildə təsnif edilmiş, onların dövlət idarəçiliyinə təsiri analiz olunmuşdur. Tədqiqatın elmi yeniliyi kimi, virtual məkanda yaranan hibrid təhdidlərə qarşı dövlətin rəqəmsal dayanıqlılığını təmin edən "Kiber-Səfərbərlik" konseptual modeli təklif edilir.**

Açar sözlər— milli təhlükəsizlik;, kibersuverenlik; fövqəladə hallar; əşyaların interneti; kiber-fiziki sistemlər; süni intellekt.

I. GİRİŞ

Müasir dövlətin fəaliyyətinin əsas meyarlarından biri onun milli təhlükəsizliyinin təmin edilməsidir. Təhlükəsizliyin təmini dövlət quruculuğunun əsas tərkib hissəsidir. Əhalinin təhlükəsizliyinin təmin edilməsi üçün dövlətin davamlı inkişafı, iqtisadi, sosial, ekoloji və digər resursların qorunması vacibdir. Milli təhlükəsizlik anlayışı bu gün təkcə fiziki hüdudların qorunması deyil, həm də ölkə iqtisadiyyatının və enerji sektorunun virtual təhdidlərdən mühafizəsini təmin etməkdir. Son zamanlar dövlət suverenliyi anlayışı coğrafi sərhədlərdən rəqəmsal məkana keçid etmişdir. Kibersuverenlik artıq sadəcə texnoloji termin deyil, dövlətin varlığını təstiq edən milli təhlükəsizlik elementidir. Fövqəladə hallar (FH) zamanı virtual məkan artıq sadəcə bir informasiya ötürücüsü deyil, həm də böhranın dərinləşdiyi və ya həll edildiyi strateji bir cəbhədir. Bu məkanda yaranan risklər zəncirvari reaksiya yaradaraq fiziki dünyadakı fəsadları qat-qat artıra bilər.

Son zamanlar dünyada baş verən hadisələr Milli kibertəhlükəsizlik sistemi texnologiyaların tamamilə yenidən nəzərdən keçirilməsini zəruri etmişdir. Təhdidlər zamanı təchizat sistemi olan qurğuların, infrastrukturun təhlükəsizliyini və davamlılığını təmin etmək konsepsiyası getdikcə daha vacib hala çevrilmişdir. Sistem bu cür qurğuların təkcə fiziki müdaxilələrə deyil, həm də kibertəhdidlərə qarşı davamlılığını təmin etmək üçün hazırlanmışdır. Milli kibertəhlükəsizlik sisteminin infrastrukturu intellektual, rəqəmsal və avtomatlaşdırmış olmalıdır. Təhlükəsizliyə təminat yaradan sistemin mövcudluğu, müxtəlif sektorlarda kiberfiziki sistemlərin inkişafı təxirəsalınmadan yeni təhdidlərə qarşı hazır olmalıdır. Bu informasiya, kommunikasiya və fiziki (texnoloji) komponentlərin vahid, idarə olunan sistemə sintezini asanlaşdırır. Xüsusilə, ağıllı şəbəkələr yaradılması, ağıllı ölçmə, ağıllı şəhər sistemi - uzaqdan şəbəkə idarəetməsi, real vaxt rejimində informasiyaya giriş və monitorinq, avtomatlaşdırılmış ağıllı cihazların idarə edilməsi, ağıllı əşyaların interneti (IoT), enerji paylanması və özünü bərpa edən şəbəkə imkanları ilə, Smart kiber fiziki sistemin (KFS) yaradılmasını qaçılmaz etdi.

Ənənəvi suverenlik anlayışı coğrafi sərhədlərin və fiziki resursların qorunmasına əsaslanırdı. Lakin rəqəmsallaşma dövründə dövlətin öz rəqəmsal infrastrukturu üzərində nəzarəti itirməsi, onun faktiki müstəqilliyini sarsıdır. Virtual məkandakı hər hansı irimiqyaslı qəza və ya kiber-müdaxilə dövlətin qərar qəbul etmə mexanizmini iflic edirsə, bu, suverenliyin virtual işğalı deməkdir.

II. FÖVQƏLADƏ HALLAR ZAMANI VİRTUAL MƏKANDA YARANAN RİSKLƏR

Virtual məkanda baş verən fövqəladə halların dövlətin suverenliyinə təsirinin analizi, müasir dövrün ən kritik elmi və strateji problemlərindən biridir. Bu problemin aktuallığını şərtləndirən amillər artıq sadəcə texniki xarakter daşımır, həm də dövlətin varlıq və müstəqillik məsələsinə çevrilir.

Müxtəlif səbəbdən yaranan FH bir neçə qrupa bölünür:

- Təbii FH-lara zəlzələ, daşqın, tufan, enerji, qaz və s. kimi hallar səbəb ola bilər. Bunlar magistral fiber-optik kabellərin qırılmasına, data-mərkəzlərin fiziki dağılmasına və enerji kəsintisinə səbəb olur;
- Texnogen FH-lara istehsalat qəzaları, yanğınlar, partlayışlar, kimyəvi sızmalar aid edilir. Xüsusilə enerji stansiyalarında baş verən qəzalar bütün KFS dayanmasına yol açır;
- Sosial-siyasi FH-lara terror aktları, sabotajlar, hərbi münaqişələr səbəb ola bilər. Bu hallar zamanı kritik infrastruktur obyektlərinə (məs. server otaqları) fiziki müdaxilə birbaşa kibersuverenlik riskidir.

Real məkanda baş verən bir hadisələr virtual məkanda "rəqəmsal böhran" yaradır. Fiziki dağıntı - virtual iflicə səbəb olur. Bir rabitə qovşağının yanması dövlət reyestrlərinə girişin məhdudlaşdırılması ilə nəticələnir. Real məkanda xaos yarandıqda, texniki işçilərin diqqəti fiziki xilasetməyə yönəlir.

DOI: 10.25045/cyber.gov.2026.43

Bu an hakerlər üçün "açıq qapı" rolunu oynayır və sistemin kiber-müdafiəsi zəifləyir. Real məkanda baş verən fövqəladə halların dövlətə vurduğu zərəri aşağıdakı faktorlarla ölçmək olar:

- İnfrastrukturun itkisi serverlərin, sensorların və şəbəkə avadanlıqlarının fiziki məhvinə səbəb olur;
- Enerji asılılığı bütün virtual sistemlər elektrik enerjisindən asılıdır. Beləki, real məkanda enerji FH-ı kibersuverenliyin tamamilə sıfırlanması deməkdir;
- Logistik maneələr FH zonasında texniki xidmətin və bərpa işlərinin gecikməsinə səbəb olur. Nümunə kimi sıradan çıxmış avadanlığın dəyişdirilməsini göstərə bilərik [1].

Virtual məkanda yaranan risklərin qarşısını almaq məqsədi ilə bir çox tədqiqatlar aparılmış, alimlər tərəfindən çoxsaylı nəşrlər edilmişdir: Kibersuverenlik anlayışı ilk dəfə Milton Mueller (2017) [2]. rəqəmsal şəbəkələr üzərində dövlət nəzarəti kimi təhlil edilmişdir. O, qlobal internetin milli sərhədlər daxilində parçalanmasını ("Splinternet") suverenlik prizmasından araşdırıb. C.Nye (2011) isə "kiber-güc" (cyber power) nəzəriyyəsində qeyd edir ki, dövlətin suverenliyi onun virtual məkandakı asimmetrik hücumlara qarşı dayanıqlılığı ilə ölçülür [3]. Kiber-fiziki sistemlərin (Smart KFS) fövqəladə hallara qarşı həssaslığı müasir tədqiqatların mərkəzindədir. Liu və başqaları (2011) "Smart Grid" şəbəkələrində yanlış verilənlərin daxil edilməsi (FDI) hücumlarının fiziki fəsadlarını sübut edən ilk fundamental işlərdən birini təqdim etmişlər [4]. Onlar göstərirlər ki, hakerlər sensor məlumatlarını dəyişməklə dövlətin enerji sistemində süni fövqəladə hal yarada bilərlər. Pasqualetti (2013) isə bu cür sistemlərin monitorinqi və idarə olunması üçün kiber-fiziki hücumların aşkarlanması metodologiyasını işləyib hazırlamışdır [5]. Azərbaycanda kibertəhlükəsizlik və virtual məkanın hüquqi-strateji aspektləri R.Əliquliyev və Y.İmamverdiyev tərəfindən geniş tədqiq edilib [6]. Onların işlərində e-dövlətin informasiya təhlükəsizliyi və kritik infrastrukturların kiberdayanıqlılığı məsələləri üstünlük təşkil edir. Xüsusilə, Azərbaycan Respublikasının "İnformasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası" bu sahədəki tədqiqatların praktiki tətbiqi üçün yeni hüquqi perspektivlər açmışdır. Aparılan tədqiqatlar yeniliklərə yol açır, rəqəmsallaşmanın dövlət suverenliyinin ayrılmaz hissəsinə çevrilməsində əsaslı rol oynayır. Böhran vəziyyətlərdə yaranan virtual risklərin milli təhlükəsizliyə yaratdığı təhdidlərin qarşısının alınmasına böyük töhvə verir.

Şəkil 1. Fövqəladə hallarda real və virtual məkanların kəsişməsi

Şəkil 1-dən göründüyü kimi real və virtual məkanlarda baş verən təhlükələr real zamanda daha böyük risklər yaranır.

III. RİSKİN RİYAZİ QİYMƏTLƏNDİRİLMƏSİ

Risklərin qiymətləndirilməsi əsas şərtlərdən biridir. Asılılıq riskini (Rdep) aşağıdakı konseptual düsturla ifadə edə bilərik:

$$R_{dep} = \frac{\sum(C_i \times S_i)}{A_{loc}}$$

C_i-kritik infrastrukturun i-ci komponentinin əhəmiyyəti.

S_i- həmin komponentin xarici mənbədən asılılıq dərəcəsi [0÷1].

A_{loc}- yerli (lokal) alternativlərin və ya açıq kodlu həllərin mövcudluğudur.

Buradan göründüyü kimi, yerli alternativlər (A_{loc})azaldıqca, texnoloji asılılıq riski eksponensial olaraq artır.

Enerji Sektoru üzrə R_{dep} Simulyasiyasını nəzərdən keçirək:

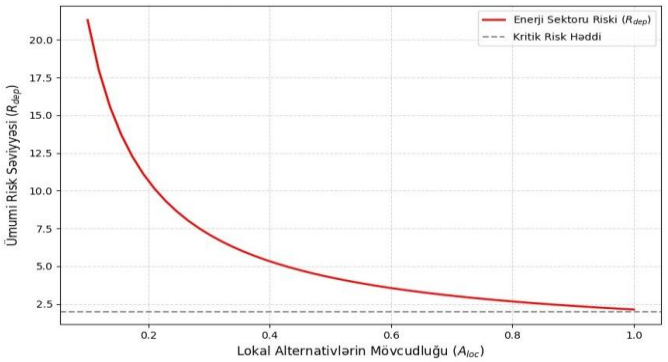
Enerji sisteminin rəqəmsal asılılıq riskini belə hesablaya bilərik:

C_{enerji} - 0.95. Enerji kəsildikdə maliyyə, səhiyyə və nəqliyyat iflic olduğu üçün bu göstərici maksimuma yaxındır.

S_{enerji} - 0.80. Əgər şəbəkəni idarə edən SCADA sistemləri və turbinlərin proqram təminatı tamamilə xarici lisenziyaya bağlıdırsa.

A_{loc} - 0.20. Əgər yerli mütəxəssislərin bu sistemlərin koduna müdaxilə imkanı yoxdursa və alternativ enerji idarəetmə sistemləri inkişaf etməyibsə.

$$Rdep = 0.20 0.95 \times 0.80 = 3.8$$



Şəkil 2. Texnoloji asılılıq riskinin lokal alternativlərdən asılılığı

Şəkil 2-dən göründüyü kimi, enerji sektorunda asılılıq riski kritik həddədir. A_{loc} (yerli potensial) 2 dəfə artırılarsa, risk yarıbayarı azalar.

İnternetdə fövqəladə hallar zamanı yaranan risklərdən biri texnoloji asılılıq riskləridir:

- Aparat asılılığı – mikroçiplər, serverlər və marşrut tənzimləyən (router) fövqəladə hal zamanı bu avadanlıqların təchizatı və ehtiyat hissələrinin tapılması qeyri-mümkün ola bilər.
- Proqram təminatı asılılığı – əməliyyat sistemləri (Windows, Linux-un xarici distributivləri) və ya

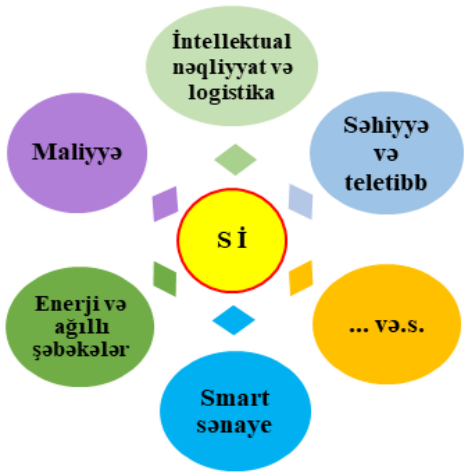
spesifik SCADA sistemləri xarici lisenziyaya bağlıdırsa, bir siqnal ilə sistemin qapadılması mümkündür.

- Alqoritmik asılılıq – Sİ həlləri xarici modellər üzərində qurulubsa, bu modellərin "qara qutu" effekti dövlətin böhran anında hansı qərarın niyə verildiyini anlamamasına səbəb olur.

SCADA – (Supervisory Control and Data Acquisition-Dispetçer Nəzarəti və Verilənlərin Toplanması), sənaye proseslərini, istehsalat avadanlıqlarını və infrastruktur obyektləri olan su, enerji, neft-qazın real vaxt rejimində mərkəzi kompyuter sistemi vasitəsilə izləyən, idarə edən və məlumatları toplayan proqram-aparat kompleksidir [7].

Fövqəladə hallar zamanı virtual məkanda bir çox risklər mövcuddur və sadəcə məlumat axınının baş verdiyi yer deyil, həm də dövlətin kibersuverenliyinin sınağa çəkildiyi strateji bir sahədir. Fiziki fəlakət anında virtual məkanda yaranan risklər "zəncirvari reaksiya" yaradaraq vəziyyəti daha da ağırlaşdıra bilər. Texnoloji asılılıq riski isə FH anında xarici proqram təminatı istehsalçılarının dəstəyi kəsməsi və ya sistemləri uzaqdan qapatmasıdır ("Kill Switch"). Bu təhlükələrin qarşısının alınmasında görülən işlər əsasən Süni İntellektə (Sİ) əsaslanır.

Sİ qabaqlayıcı tədbirlərin və “Rəqəmsal ekiz” texnologiyasının bərpa prosesində əsaslı rol oynayır. Sİ sistemin ən zəif nöqtələrini müəyyən edərək, smart xüsusiyyətini nümayiş etdirir. O, risklərin əvvəlcədən proqnozlaşdırılması, Smart KFS-lərin hadisə baş verdikdən sonra reaksiya verməsi və hadisə baş verməmişdən əvvəl xəbər verməsini təmin edir.



Şəkil 3. Süni intellektin tətbiq edildiyi sahələr

Şəkil 3-dən göründüyü kimi dövlətin kiber-fiziki təhlükəsizlik sistemi iki müstəvidə vizuallaşır: Birinci tərəf fiziki mühitdəki təhdid vektorlarını, ikinci tərəf isə bu təhdidləri idarə edən və ya onlardan təsirlənən Sİ mərkəzli idarəetmə modelini əks etdirir. Bu iki qat arasındakı asılılıq, virtual fövqəladə hallar zamanı kibersuverenliyin qorunmasını zəruri edir. Real məkan ilə rəqəmsal idarəetmənin (Sİ) bir-birini tamamladığı qapalı əks-əlaqə dövr şəklində fəaliyyət göstərir. Buradakı dəyişikliklər (məsələn, zəlzələ dalğaları və ya su səviyyəsinin artması) sensorlar tərəfindən qəbul edilir və rəqəmsal formata çevrilir. Toplanmış məlumatlar mərkəzi dayanan Sİ tərəfindən emal edilir [8]. Sİ eyni vaxtda maliyyə, səhiyyə, nəqliyyat və enerji sektorlarından gələn məlumatları da sintez edir. Həmçinin, alqoritmlər vasitəsi ilə keçmiş zəlzələ və ya hava proqnozlarını təhlil edərək gələcək fövqəladə halları öncədən təxmin edir.

Sİ-nin qəbul etdiyi qərarlar "Real Məkan"dakı prosesləri aktiv şəkildə dəyişir:

- Daşqın və ya zəlzələ anında Sİ avtomatik olaraq təxliyə marşrutlarını optimallaşdırır və intellektual nəqliyyat sistemləri vasitəsilə trafikin istiqamətini dəyişir.
- Enerji qəzası və ya qaz sızma aşkar edildikdə, Sİ "ağıllı şəbəkələr" vasitəsilə zədələnmiş hissəni təcrid edir və enerjini alternativ yollarla yönləndirir.
- Fövqəladə halın miqyasına uyğun olaraq səhiyyə resurslarını və teletibb xidmətlərini kritik nöqtələrə bölüşdürür.

Cədvəl 1-də kiber və fiziki mühitlərin qarşılıqlı əlaqəsi təqdim edilir. Sİ-in bu sahələrdəki rolu dövlətin fiziki infrastrukturunu rəqəmsal olaraq qorumağa və kibersuverenliyin fiziki təhlükəsizliklə tam inteqrasiyasına imkan verir. FH zamanı fəlakətin qarşısının alınması üçün Sİ-in tətbiqi risklərin azalmasında önəmli rol oynayır.

CƏDVƏL 1. SÜNİ İNTELLEKT İNTEQRASİYASI

REAL MƏKAN	VİRTUAL MƏKAN	QARŞILIQLI ƏLAQƏNİN NƏTİCƏSİ
Zəlzələ	Sistemlərin (Serverlərin) çökməsi	Fiziki infrastrukturun itməsi ilə rəqəmsal idarəetmənin dayanması.
Enerji	Kiber-blackout (Şəbəkə hücumu)	Enerji kəsintisi nəticəsində kiber-fiziki sistemlərin sıradan çıxması.
Daşqın	Verilənlərin (Data) itməsi	Fiziki suların altında qalan kabellər və mərkəzlərin yaratdığı informasiya boşluğu.
Nəqliyyat	İntellektual idarəetmənin itirilməsi	Ağıllı işıqforların və qatarların virtual manipulyasiyası ilə yaranan qəzalar.
Qaz və s.	SCADA sistemlərinin sızması	Virtual müdaxilə ilə fiziki sızıntı və ya partlayışın baş verməsi.

Bildiyimiz kimi FH zamanı fəlakətin qarşısının alınması üçün Sİ-nin tətbiqi, əslində Smart KFS-in intellektual fəaliyyət rejimidir. Hər bir sahədə olduğu kimi Smart KFS Fövqəladə Halların fəaliyyəti üçün xüsusi beynəlxalq və sahə standartları mövcuddur. Bu standartlar, əsasən, sistemin etibarlılığı, kiber təhlükəsizliyi (məsələn, ISO/IEC 27001və IEC 62443) fiziki zədələrə davamlılıq və fövqəladə hallarda avtomatik təhlükəsiz rejimə keçid məsələlərini tənzimləyir [9, 10].

Əsas standartlaşdırma istiqamətləri olaraq aşağıdakıları göstərmək olar:

1) *Təhlükəsiz və davamlı*-sistemlərin böhran anında fasiləsiz işləməsi və ya təhlükəsiz şəkildə dayanma standartları.
2) *Kiber təhlükəsizlik*-FH zamanı kiber hücumlara qarşı müdafiə (IEC 62443)
3) *Qarşılıqlı fəaliyyət*-müxtəlif sistemlərin birgə işləməsi üçün texniki norma və qaydalar.

KFS-lərdə, məsələn, sensorlar və idarəetmə komponentləri vasitəsilə fövqəladə halların erkən aşkarlanması və qərarvermə proseslərinin avtomatlaşdırılması bu standartlarla tənzimlənir.

Qəbul edilən standartla yanaşı Azərbaycan Respublikasının Qanunvericiliyində bir neçə qanun qəbul edilmişdir**:**

- “Kibertəhlükəsizlik haqqında” Azərbaycan Respublikasının Qanunu: “Azərbaycan Respublikasının İnformasiya Təhlükəsizliyi və Kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası”nın təsdiq edilməsi haqqında Azərbaycan Respublikası Prezidentinin sərəncamı (Bakı şəhəri, 28 avqust 2023-cü il. № 4060) [11].
- “Fövqəladə vəziyyət haqqında” Qanun: Fövqəladə hallarda (o cümlədən genişmiqyaslı kiberhücumlar zamanı) həyatın təhlükəsizliyini təmin etmək üçün məhdudiyyətlərin tətbiqi, dövlət nəzarətinin gücləndirilməsi və fövqəladə idarəetmə qaydalarını tənzimləyir. (Bakı şəhəri, 4 fevral 1992-ci il.№ 70.) [12].
- “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu qəbul edilmişdir. Burada Azərbaycan Prezidentinin müvafiq fərmanları ilə dövlət informasiya sistemlərinin qorunması məqsədilə kiberhücumların qarşısının alınması mexanizmləri müəyyən edilir [13].

Kiberhücum və ya fövqəladə vəziyyət yaranarsa, qanunvericiliyə əsasən xüsusi rejim və digər təxirəsalınmaz tədbirlər tətbiq edilir.

IV. RİSKLƏRİN QARŞISININ ALINMASI ÜÇÜN KONSEPTUAL MODELİN İŞLƏNİLMƏSİ

Fövqəladə hallar (FH) zamanı dövlətin kibersuverenliyini qorumaq üçün standart təhlükəsizlik tədbirləri yetərli deyil. Belə vəziyyətlərdə kiber-mühitdə rəqəmsal dözümlülük rejiminə keçid edilməlidir. Bu yanaşma sistemin hücum almayacağına deyil, hücum altında belə minimum funksionallığını qoruyub saxlaya biləcəyinə fokuslanır.

Aşağıda bu strategiyanın əsas sütunu olan "Kiber-Səfərbərlik" konseptual modeli təqdim olunur. Təqdim olunan konseptual model fövqəladə hallar şəraitində dövlətin rəqəmsal ekosisteminin davamlı fəaliyyətini təmin etmək məqsədilə kiber-səfərbərlik prinsiplərinə əsaslanan çoxsəviyyəli idarəetmə və müdaxilə mexanizmini təsvir edir. Model funksional ardıcıllıq, struktur koordinasiya və strateji prioritetləşdirmə prinsipləri üzərində qurulmuşdur.

"Kiber-Səfərbərlik" rejiminin tətbiqi:

Fövqəladə hal elan olunduğu andan etibarən dövlətin kiber-resursları hərbi intizam rejiminə keçirilir və modelin mərkəzi idarəetmə komponenti – kiber-səfərbərlik sistemi aktivləşdirilir. İdarəetmə nüvəsi sistemin bütün struktur elementlərinin sinxron fəaliyyətini təmin edir və əməliyyat proseslərinin vahid strateji məqsədlərə uyğun yönləndirilməsini həyata keçirir. Beləliklə, fövqəladə vəziyyət modelin bütün sonrakı mərhələlərinin aktivləşməsini təmin edən başlanğıc şərt rolunu oynayır.

Bu planın tərkib hissələri aşağıdakılardır:

A. Kiber-Rezervist korpusunun yaradılması

Birinci mərhələdə kiber-rezervist potensialının aktivləşdirilməsini nəzərdə tutur. Bu struktur dövlət, akademik və özəl sektor üzrə ixtisaslaşmış mütəxəssislərin operativ şəkildə səfərbər olunmasını təmin edir.

Özəl sektorda və akademik mühitdə çalışan yüksək ixtisaslı İT mütəxəssislərindən ibarət "kiber-rezerv" bazası yaradılır. FH zamanı bu şəxslər strateji infrastrukturun (məsələn, enerji şəbəkəsi) müdafiəsinə cəlb olunur.

B. Kritik infrastrukturun "İzolyasiya protokolu"

İkinci sütun milli rəqəmsal infrastrukturun təhlükəsiz fəaliyyət rejiminə keçirilməsini təmin edən izolyasiya mexanizmini əhatə edir. Bu mərhələdə şəbəkə mühitinin seqmentləşdirilməsi, xarici təsirlərin məhdudlaşdırılması və kritik sistemlərin qapalı rejimdə fəaliyyət göstərməsi təmin edilir. Bu mexanizm sistemin xarici müdaxilələrə qarşı dayanıqlılığını artırır və idarəetmə qərarlarının təhlükəsiz texnoloji mühitdə icrasına şərait yaradır. Böhran anında dövlətin idarəetmə sistemləri xarici internet seqmentindən asılılığını minimuma endirməlidir.

Milli İntranet: Kritik dövlət xidmətlərinin (e-hökumət, bank sistemi) yalnız ölkədaxili trafiklə işləyə biləcəyi "Qapalı dövrə" rejimi aktivləşdirilir.

C. Kiber-Komandanlıq və vahid koordinasiya mərkəzi

Müdafiə Nazirliyi, Daxili İşlər Nazirliyi, Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinin və digər xüsusi xidmət orqanlarının təmsil olunduğu vahid "Kiber-Qərargah" yaradılır. Bu qərargah bütün kiber-insidentləri mərkəzləşdirilmiş şəkildə idarə edir.

Bu struktur prioritetlərin müəyyənləşdirilməsi, resursların bölüşdürülməsi və sektorlararası koordinasiyanın təmin olunması funksiyalarını yerinə yetirir. Kiber-komandanlıq sistemi digər iki sütunun fəaliyyətini strateji məqsədlərə uyğun istiqamətləndirir və sistemin vahid idarəetmə məntiqi əsasında fəaliyyətini təmin edir.

Sistem fəaliyyətinin əsas əməli məqsədi kritik infrastruktur sahələrinin fasiləsiz fəaliyyətini təmin etməkdir. Bu mərhələdə müdaxilə prioritetləri dövlətin funksional sabitliyini müəyyən edən sektorlar üzrə formalaşdırılır. Enerji, maliyyə, elektron idarəetmə və rabitə sistemlərinin qorunması dövlət idarəetmə qabiliyyətinin saxlanmasının zəruri şərti kimi qəbul edilir. Uzunmüddətli perspektivdə isə sistem milli kiber-immunitetin formalaşmasına xidmət edir. Bu, yalnız mövcud təhlükələrə

Səkil 3. Fövqəladə hallar şəraitində "Kiber-Səfərbərlik" konseptual modeli

cavab vermək deyil, həm də gələcək risklərin qarşısını almağa hədəflənmişdir. Kiber-səfərbərlik modeli dövlətin virtual məkandakı "immun sistemidir" (Şəkil 3). Bu sistem nə qədər mərkəzləşdirilmiş və çevik olarsa, kənar müdaxilələrin dövlət suverenliyinə təsiri o qədər az olar.

NƏTİCƏ

Aparılan tədqiqat işi göstərir ki, rəqəmsal transformasiya dövründə dövlətin suverenliyi artıq yalnız coğrafi sərhədlərlə məhdudlaşmır, həm də rəqəmsal ekosistemin bütövlüyündən və idarəetmə dözümlülüyündən birbaşa asılıdır. Fövqəladə halların (FH) virtual məkana təsirinin analizi nəticəsində bir çox nəticələr əldə edilmişdir. Kiber-fiziki konvergensiyanın kritik rolu olaraq, real məkanda baş verən təbii, texnogen və sosial-siyasi fövqəladə hallar virtual məkanda zəncirvari reaksiya yaradaraq dövlət idarəçiliyini iflic edə bilər. Fiziki infrastrukturun itirilməsi ilə rəqəmsal suverenliyin sarsılması arasındakı asılılıq KFS təhlükəsizlik arxitekturasının yenidən qurulmasını zəruri edir. Smart KFS-lərdə Sİ tətbiqi fəlakətlərin qarşısının alınmasında qabaqlayıcı yanaşma tətbiq edilir. Sİ-in idarəetmə effektivliyi dövlətin ümumi dayanıqlılıq indeksinin əsas sütunu kimi çıxış edir. Məqalədə riyazi qiymətləndirmə modeli vasitəsilə təsdiq edilmişdir ki, xarici texnoloji həllərdən asılılıq dərəcəsi artdıqca, virtual fövqəladə hallar zamanı dövlətin imkanları getdikcə azalır. Bu riskin minimuma endirilməsi üçün lokal alternativlərin və açıq kodlu sistemlərin tətbiqi strateji vəzifədir. "Kiber-Səfərbərlik" modelinin elmi yeniliyi kimi, təklif olunan konseptual model - kiber-rezervistlərin cəlb edilməsidir. Milli kibersuverenliyin möhkəmləndirilməsi üçün Azərbaycan Respublikasının 2023–2027-ci illər üzrə Strategiyasına uyğun olaraq, kiber-səfərbərlik qanunvericiliyinin təkmilləşdirilməsi, kritik sektorlarda "Rəqəmsal Ekiz" texnologiyalarının tətbiqi və Sİ əsaslı milli kiber-müdafiə sistemlərinin inkişaf etdirilməsi tövsiyə olunur. Bu addımlar virtual fövqəladə hallar zamanı dövlətin həm rəqəmsal, həm də fiziki varlığının sarsılmazlığının qarantı olacaqdır.

ƏDƏBİYYAT

[1] T. Parhizkar, I. B. Utne, J. E. Vinnem, and A. Mosleh, "Dynamic probabilistic risk assessment of decision-making in emergencies for complex systems: Case study of a dynamic positioning drilling unit," *Ocean Engineering*, vol. 237, p. 1096531, Oct. 2021.
[2] M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge, U.K.: Polity Press, 2017.
[3] J. S. Nye Jr., *The Future of Power*. New York, NY, USA: PublicAffairs, 2011.
[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.
[5] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 1, pp. 59–71, Mar. 2013.
[6] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint* arXiv:1412.6572, 2014.
[7] M. Bruneau *et al*., "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, no. 4, pp. 733–752, Nov. 2003.
[8] C. W. Zobel, "Representing stakeholder priorities in a resilience-based assessment of disaster recovery," *Decision Support Systems*, vol. 50, no. 2, pp. 397–408, Jan. 2011.
[9] R. Alguliyev and Y. Imamverdiyev, "Information security as a component of national security," *Information Technologies Problems*, no. 1.
[10] Republic of Azerbaijan, *Strategy on Information Security and Cybersecurity of the Republic of Azerbaijan for 2023–2027*, approved by Presidential Decree, 2023.
[11] Republic of Azerbaijan, *Law "On the State of Emergency"*, Baku, Feb. 4, 1992, No. 70.
[12] Republic of Azerbaijan, *Law "On Information, Informatization, and Information Protection"*, Baku, Apr. 3, 1998, No. 460-IQ.

An Analysis of the Impact of Cybersecurity Emergencies on State Cyber Sovereignty and Future Challenges

Kamala Hashimova
Institute of Information Technology, Baku, Azerbaijan

***Abstract*—** In the context of modern digitalization, which has become the central pillar of public administration, the sovereign rights of the state must be protected in both physical and virtual space. This study comprehensively analyzes the impact of emergency situations on the state's digital borders and governance mechanisms in the current geopolitical context. The article emphasizes that digitalization has become an integral part of state sovereignty and examines the threats to national security posed by virtual risks arising in crisis situations. Risks arising in virtual space due to emergency situations are comprehensively classified, and their impact on public administration is analyzed. As a scientific innovation, the study proposes a conceptual model of "cybermobilization" that ensures the state's digital resilience to hybrid threats arising in virtual space.

***Keywords*—** national security; cyber sovereignty; emergency situations; Internet of Things; cyber-physical systems; artificial intelligence.