Kibersuverenlik Kontekstində Kritik İnformasiya İnfrastrukturunun Təhlükəsizliyi: Azərbaycan Respublikasının Normativ və Strateji Yanaşması

Elvin Balacanov
Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti, Milli kibermərkəz, Bakı, Azərbaycan
e.balajanov.edu@gmail.com

Xülasə— Məqalədə kritik informasiya infrastrukturunun (Kİİ) təhlükəsizliyinin təmin olunmasının Azərbaycan Respublikası üçün strateji prioritetlərdən biri olduğu və ölkənin kibersuverenliyinin möhkəmləndirilməsi baxımından zəruri sahələr sırasında yer aldığı bildirilir. Vurğulanır ki, Kİİ təhlükəsizliyi dövlətin milli kiberməkan üzərində effektiv nəzarət imkanlarının formalaşmasında əsas faktorlardan biri kimi çıxış edir. Qeyd olunur ki, son illər ərzində Kİİ təhlükəsizliyinin təmin edilməsi məqsədilə hüquqi, təşkilati və texniki-texnoloji sferalarda mühüm addımlar atılmış, müvafiq normativ baza və institusional mexanizmlər formalaşdırılmışdır. Bununla yanaşı, Kİİ subyektləri tərəfindən infrastrukturun təhlükəsizliyinə daha çox önəm verilməsinə və risk əsaslı yanaşmanın dərinləşdirilməsinə zərurət yaranmışdır. Məqalədə mövcud yanaşmalar təhlil edilir, qarşıda duran çağırışlar müəyyənləşdirilir və kibersuverenliyin praktik təminat mexanizmi kimi Kİİ təhlükəsizliyinin gücləndirilməsi üzrə inkişaf istiqamətləri irəli sürülür.

Açar sözlər— kibertəhlükəsizlik; kritik informasiya infrastrukturu; kibersuverenlik; normativ-hüquqi baza.

I. GİRİŞ

Rəqəmsal texnologiyaların sürətli inkişafı və informasiya sistemlərinin beynəlxalq miqyasda inteqrasiyası hazırkı mərhələdə dövlətin və cəmiyyətin sosial-iqtisadi tərəqqisinin aparıcı determinantlarından birinə çevrilmişdir. Azərbaycan Respublikasında da informasiya-kommunikasiya texnologiyalarının geniş tətbiqinə əsaslanan yanaşmalar vasitəsilə dövlət əhəmiyyətli məsələlərin icrası üçün intensiv şəkildə müvafiq informasiya infrastrukturu formalaşdırılmaqdadır. Bununla yanaşı, bu infrastrukturun qlobal informasiya şəbəkələrinə, o cümlədən internet mühitinə inteqrasiyası onun kibertəhdidlər qarşısında daha həssas hala gəlməsinə və potensial kiberhücum hədəfinə çevrilməsinə şərait yaradır.

Dövlətin, cəmiyyətin və vətəndaşların maraqları baxımından mühüm hesab edilən məsələlərin həlli məqsədilə yaradılmış kritik informasiya infrastrukturu dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika, nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı və ekologiya sahələrində fəaliyyəti təmin edən informasiya sistemlərini, avtomatlaşdırılmış idarəetmə sistemlərini və informasiya-kommunikasiya şəbəkələrini əhatə edir. Bu obyektlərin sıradan çıxarılması və ya funksionallığının pozulması dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vurmaq potensialına malikdir [1].

Məhz bu səbəbdən Kİİ-nin təhlükəsizliyi ölkənin müvafiq sahədə milli strateji prioritetlərindən biri kimi çıxış edir və kibersuverenliyin təminat mexanizmlərindən biri hesab olunur. Kİİ-nin təhlükəsizliyi dövlətin milli kiberməkan üzərində effektiv nəzarət imkanlarını formalaşdırmaqla yanaşı, əsas ictimai xidmətlərin fasiləsizliyini və strateji resursların qorunmasını təmin edir. Bu kontekstdə, Azərbaycanda Kİİ təhlükəsizliyinin hüquqi, texnoloji və institusional əsaslarının inkişafı kibersuverenliyin möhkəmləndirilməsinə yönəlmiş sistemli dövlət siyasətinin tərkib hissəsi kimi qiymətləndirilməlidir.

II. KİBERSUVERENLİK VƏ KRİTİK İNFORMASİYA İNFRASTRUKTURU: NƏZƏRİ ASPEKTLƏR

A. Suverenlik

Dövlətin öz ərazisi və əhalisi üzərində beynəlxalq hüquqla tanınmış ali və müstəsna hakimiyyətinin mövcudluğunu, həm daxili və həm də xarici siyasətində müstəqil qərarlar vermək, müstəqil və hüquqi baxımdan bərabər subyekt kimi fəaliyyət göstərmək qabiliyyətini ifadə edən fundamental prinsipdir. Bu anlayış beynəlxalq hüquqda və siyasi nəzəriyyədə dövlətin əsas atributlarından biri kimi qəbul edilir [2]. Bu çərçivədə, kibersuverenlik anlayışı dövlətlərin öz sərhədləri daxilində kiberməkanda hüquqi, texniki və institusional nəzarəti həyata keçirmək iradəsini və qabiliyyətini, o cümlədən informasiya infrastrukturu, məlumatlar və rəqəmsal məzmun üzərində ali hakimiyyətini, daxili suverenliyini və xarici müstəqilliyini ifadə edir. Beləliklə, anlayış yalnız informasiya infrastrukturunun təhlükəsizliyini deyil, həm də davamlı fəaliyyətinin təmin olunmasını ehtiva edir və özündə üç əsas elementi birləşdirir:

1) *Hüquqi suverenlik* – milli qanunvericiliyin rəqəmsal mühitə tətbiqi;
2) *Texnoloji suverenlik* – əsas rəqəmsal resurslar üzərində müstəqil idarəetmə;
3) *İnstitusional suverenlik* – koordinasiyaedici dövlət qurumlarının mövcudluğu.

Bu baxımdan, kibersuverenlik konsepsiyası müasir dövlətlərin rəqəmsal mühitdə normayaratma və icra

DOI: 10.25045/cyber.gov.2026.27

səlahiyyətlərinin legitim əsasını formalaşdırmaqla yanaşı, kibertəhlükəsizlik siyasətinin, məlumatların mühafizəsinin və rəqəmsal iqtisadiyyatın hüquqi çərçivəsinin müəyyən edilməsində mühüm rol oynayır. Eyni zamanda, bu anlayış kiberməkanda fəaliyyət göstərən transsərhəd platformalar və qeyri-dövlət aktorları qarşısında dövlətlərin tənzimləyici imkanlarını qorumağa yönəlmiş institusional və normativ mexanizmlərin inkişafını şərtləndirir. Lakin kiberməkanın sərhədsiz təbiəti səbəbindən kibersuverenliyin beynəlxalq hüquq müstəvisində tətbiqi, xüsusilə yurisdiksiya, məsuliyyət və dövlətlərin qarşılıqlı öhdəlikləri məsələləri doktrinal və praktiki mübahisə predmeti olaraq qalmaqdadır [3-5]. Bu isə dövlətlərin kiberməkanda real nəzarət imkanlarının əsasən kritik informasiya infrastrukturu üzərində effektiv hakimiyyətin təmin edilməsindən asılı olduğunu göstərir (Şəkil 1).

Şəkil 1. Kritik informasiya infrastrukturu

Qeyd olunmalıdır ki, kritik informasiya infrastrukturu dedikdə, dövlət idarəçiliyi, müdafiə, səhiyyə, maliyyə bazarları, energetika, nəqliyyat, informasiya texnologiyaları, telekommunikasiya, su təchizatı və ya ekologiya sahəsində fəaliyyəti təmin edən və funksionallığının pozulması dövlətin, cəmiyyətin və vətəndaşların maraqlarına mühüm zərər vura bilən informasiya sistemlərinin, avtomatlaşdırılmış idarəetmə sistemlərinin və informasiya-kommunikasiya şəbəkələrinin məcmusu başa düşülür [1].

Bu obyektlərin funksionallığının pozulması dövlət təhlükəsizliyinə və ictimai təhlükəsizliyə mühüm təhdidlərin yaranması, əhalinin mühüm təminatlardan məhrum olması, iqtisadi və maliyyə sabitliyinin pozulması, habelə ekoloji tarazlığın pozulması və ekoloji vəziyyətin kəskin pisləşməsi ilə nəticələnə bilər [1].

Məhz buna görə də, Kİİ təhlükəsizliyi kibersuverenliyin mühüm funksional komponenti kimi milli kiberməkan üzərində operativ nəzarətin təmin olunmasını, mühüm xidmətlərin fasiləsizliyini, strateji məlumatların qorunmasını və kiberinsidentlərə çevik reaksiya qabiliyyətinin formalaşdırılmasını ehtiva edir. Nəticə etibarilə, Kİİ-nin təhlükəsizliyinin təmin olunması dövlətin rəqəmsal suverenliyinin institusional və praktiki dayağı kimi çıxış edərək kiberməkanda daxili ali hakimiyyətin və xarici müstəqilliyin real təminat mexanizmini təşkil edir.

III. Azərbaycan Respublikasında Kritik İnformasiya İnfrastrukturunun Təhlükəsizliyinin Normativ-Hüquqi Əsasları

Son illərdə qəbul edilmiş bir sıra normativ-hüquqi aktlar Azərbaycan Respublikasında Kİİ-nin təhlükəsizliyinin təmin olunması sahəsində institusional və hüquqi çərçivənin formalaşdırılmasına xidmət etmişdir.

Belə ki, “Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında” Azərbaycan Respublikası Prezidentinin Fərmanı ilə Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi, o cümlədən kibertəhdidlərə qarşı mübarizə sahəsində səlahiyyətli orqan qismində müəyyən edilmişdir. Dövlət orqanlarına, dövlət adından yaradılan publik hüquqi şəxslərə, dövlətə məxsus olan hüquqi şəxslərə münasibətdə həmin funksiyaları Azərbaycan Respublikasının Dövlət Təhlükəsizliyi Xidməti Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti ilə birgə həyata keçirir [6]. “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Qanuna “Kritik informasiya infrastrukturunun təhlükəsizliyi” başlıqlı yeni fəsil və sahə üzrə bir sıra anlayışlar əlavə edilmiş, kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində rəhbər normalar müəyyən edilmişdir [1].

Azərbaycan Respublikasında Kİİ təhlükəsizliyinin təmin edilməsi qaydaları, o cümlədən Kİİ təhlükəsizliyinə dair ümumi tələblər və kibertəhlükəsizlik xidməti provayderinə, onun işçi heyətinə, texnoloji resurslarına və fəaliyyət proseslərinə dair tələblər “Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi Qaydaları” əsasında həyata keçirilir [7]. “Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması Qaydası” isə Kİİ obyektlərinin reyestrinin strukturunu, yaradılması və aparılmasının hüquqi, təşkilati və texnoloji əsaslarını müəyyən edir. Adıçəkilən qaydaya əsasən, reyestr “kritik informasiya infrastrukturu obyektləri ilə bağlı informasiya proseslərinin (məlumatların yaradılması, toplanılması, işlənilməsi, saxlanılması, axtarışı, mühafizəsi və mübadiləsi) həyata keçirilməsi, eləcə də kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi, o cümlədən kibertəhdidlərə qarşı mübarizənin həyata keçirilməsi ilə bağlı tədbirlərin planlaşdırılması və icra olunması məqsədilə təhlillərin aparılması üçün nəzərdə tutulan informasiya sistemidir” [8]. Qeyd olunmalıdır ki, reyestrin operatoru Dövlət Təhlükəsizliyi Xidmətinin Kibertəhlükəsizlik əməliyyatları mərkəzidir (Milli kibermərkəz) [8].

Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı ilə “Kritik informasiya infrastrukturu obyektlərinin siyahısı” təsdiq edilmişdir [9]. Eyni zamanda, təhlükəsizliklə bağlı

həssaslıq nəzərə alınaraq, həmin siyahı ictimaiyyətə açıqlanmamışdır.

Əlavə olaraq, qeyd olunmalıdır ki, Kİİ-nin təhlükəsizliyinin təmin edilməsi “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası”nda [10] müəyyənləşdirilmiş əsas prioritet istiqamətlərdən biri kimi müəyyən edilmişdir. Strategiyada vurğulanır ki, “cəmiyyətin mühüm həyati funksiyalarını təmin etmək üçün böyük rola malik olan, fəaliyyətindəki nasazlıqların və ya sıradan çıxmasının əhalinin sağlamlığına, təhlükəsizliyinə, iqtisadi və sosial rifahına, həmçinin dövlət qurumlarının fəaliyyətinin davamlılığına ciddi təsir göstərən infrastrukturların və ya onların əhəmiyyətli hissələrinin informasiya təhlükəsizliyinin təmin olunması xüsusilə vacibdir” [10].

Beləliklə, Strategiyada da nəzərə çatdırıldığı kimi, kritik informasiya infrastrukturunun təhlükəsizliyi mülkiyyət formasından asılı olmayaraq daimi diqqət mərkəzində saxlanmalı, müvafiq dövlət orqanları tərəfindən məqsədyönlü və koordinasiyalı tədbirlərlə təmin olunmalıdır. Bu, yalnız texniki və təşkilati tədbirlərin həyata keçirilməsi ilə məhdudlaşmır, eyni zamanda dövlətin milli kiberməkan üzərində effektiv suveren nəzarət imkanlarının möhkəmləndirilməsinə xidmət edir və kibersuverenliyin praktik həyata keçirilməsi üçün hüquqi, institusional və texnoloji əsasları təmin edən strateji əhəmiyyətli funksiyanı yerinə yetirir.

IV. Strategi və İnstitusional Mexanizmlər

Azərbaycan Respublikasında Kİİ-nin təhlükəsizliyinin təmin edilməsi üzrə fəaliyyət bu, infrastrukturun təhlükəsizliyinə dair tələblərin müəyyən edilməsini, həmin tələblərə uyğunluğun qiymətləndirilməsini və aşkar olunan uyğunsuzluqların aradan qaldırılmasını, eləcə də tələblərə uyğun informasiya təhlükəsizliyini idarəetmə sistemlərinin tətbiqini və Kİİ-nin təhlükəsizliyinin təmin olunması vəziyyətinə nəzarəti əhatə edir [1].

Kİİ təhlükəsizliyi üzrə fəaliyyətin ümumi təşkili və əlaqələndirilməsi səlahiyyətli orqan tərəfindən həyata keçirilir. Yuxarıda qeyd olunduğu kimi, Kİİ-nin təhlükəsizliyinin təmin edilməsi, o cümlədən kibertəhdidlərə qarşı mübarizə sahəsində səlahiyyətli orqanın funksiyaları Dövlət Təhlükəsizliyi Xidməti tərəfindən həyata keçirilir. Dövlət orqanları, dövlət adından yaradılmış publik hüquqi şəxslər və dövlətə məxsus hüquqi şəxslər üzrə isə bu funksiyalar Dövlət Təhlükəsizliyi Xidməti və Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti tərəfindən birgə icra olunur. Öz növbəsində, hər bir Kİİ subyekti ona məxsus infrastrukturun təhlükəsizliyini müəyyən edilmiş ümumi və xüsusi tələblərə uyğun təmin etməlidir.

Nəzarət mexanizmi isə tələblərə uyğunluğun qiymətləndirilməsi, aşkar edilmiş uyğunsuzluqların aradan qaldırılması, fasiləsiz monitorinq (24/7), müdaxilə sınaqları və kənar audit yoxlamaları vasitəsilə həyata keçirilir [9].

Ümumilikdə, Azərbaycanın Kİİ təhlükəsizliyi üzrə strateji yanaşması bir neçə əsas istiqaməti əhatə edir və hər bir istiqamət Kİİ-nin dayanıqlılığını və milli kiberməkan üzərində suveren nəzarəti gücləndirmək məqsədini daşıyır. Birincisi, mərkəzləşdirilmiş koordinasiya mexanizmlərinin yaradılmasıdır. Bu mexanizmlər Kİİ subyektləri arasında informasiya mübadiləsinin sistemləşdirilməsini təmin edir, kiberinsidentlərə qarşı operativ və əlaqələndirilmiş reaksiya imkanlarını gücləndirir, həmçinin risklərin qiymətləndirilməsi və təhlilini vahid çərçivədə həyata keçirməyə şərait yaradır. Belə mərkəzləşdirilmiş yanaşma həm dövlət qurumlarının fəaliyyətinin effektivliyini artırır, həm də kritik obyektlərin qorunması sahəsində institusional sinxronizasiyanı təmin edir.

İkincisi, texniki potensialın gücləndirilməsidir. Bu istiqamət Kİİ obyektlərinin fasiləsiz fəaliyyətini təmin etmək üçün monitorinq sistemlərinin, erkən xəbərdarlıq mexanizmlərinin, ehtiyat infrastruktur həllərinin və kibertəhlükəsizlik texnologiyalarının tətbiqini əhatə edir. Yaradılmış texnoloji mühit infrastrukturun dayanıqlılığını artırmaqla yanaşı, potensial kiberhücumlara qarşı çevik müdafiə imkanlarını təmin edir və risk əsaslı yanaşmanın praktik tətbiqini dəstəkləyir.

Üçüncüsü, insan kapitalının inkişafıdır. Belə ki, Kİİ təhlükəsizliyinin effektiv təmin olunması üçün kibertəhlükəsizlik sahəsində ixtisaslaşmış kadrların hazırlanması, onların davamlı təlim və sertifikasiya proqramları vasitəsilə bacarıqlarının artırılması institusional dayanıqlılığın və əməliyyat effektivliyinin mühüm komponenti kimi çıxış edir. Bu yanaşma həm də dövlət və özəl sektor əməkdaşlığının gücləndirilməsinə, kadr resurslarının effektiv idarə edilməsinə və milli təhlükəsizlik maraqlarına müvafiq şəkildə yönəldilməsinə imkan yaradır.

Dördüncüsü, beynəlxalq əməkdaşlıqdır. Xüsusilə qeyd olunmalıdır ki, Azərbaycan Respublikası qlobal təşəbbüslərdə iştirak edərək qabaqcıl təcrübələrin ölkəyə transferini təmin etməklə yanaşı, həm də normativ-hüquqi və institusional yanaşmalarını beynəlxalq standartlara uyğunlaşdırır. Eyni zamanda, ölkəmiz regional və qlobal kibertəhlükəsizlik mexanizmlərində fəal rol oynayır. Nəzərə alınmalıdır ki, beynəlxalq əməkdaşlıq həm də qarşılıqlı informasiya mübadiləsi, ən yaxşı təcrübələrin tətbiqi və kibertəhdidlərin qlobal səviyyədə izlənilməsi baxımından strateji əhəmiyyət kəsb edir.

Beləliklə, Azərbaycan Respublikasının Kİİ təhlükəsizliyi üzrə strateji yanaşması institusional koordinasiya, texnoloji infrastruktur, insan kapitalı və beynəlxalq əməkdaşlıq kimi qarşılıqlı tamamlayıcı istiqamətləri birləşdirərək, milli kiberməkan üzərində suveren nəzarətin möhkəmləndirilməsinə və kibersuverenliyin praktik təminatına xidmət edir.

V. Mövcud Çağırışlar və Potensial İnkişaf İstiqamətləri

Azərbaycan Respublikasında Kİİ təhlükəsizliyinin təmin olunması sahəsində mühüm hüquqi, institusional və texnoloji addımlar atılmasına baxmayaraq, mövcud vəziyyət bir sıra çağırışların və potensial inkişaf sahələrinin mövcud olduğunu göstərir. İlk növbədə, beynəlxalq təcrübəyə uyğun olaraq, xüsusilə ISO/IEC, NIST Cybersecurity Framework (CSF) 2.0, ENISA/NIS2 və ISA/IEC 62443 standartları çərçivəsində Kİİ təhlükəsizliyinə dair tələblərin təkmilləşdirilməsi vacib hesab olunur [11,12]. Belə ki, normativ-hüquqi və texniki sənədlərin

beynəlxalq standartlarla uzlaşdırılması, həmçinin yerli Kİİ subyektlərinin təhlükəsizlik səviyyəsinin yüksəldilməsi yalnız infrastrukturun dayanıqlılığını artırmaqla kifayətlənmir, eyni zamanda dövlətin milli kiberməkan üzərində suveren nəzarət imkanlarının gücləndirilməsinə və kibersuverenliyin praktik həyata keçirilməsinə xidmət edir.

Bundan əlavə, risk əsaslı yanaşma çərçivəsində, eləcə də müasir kibertəhdid modelləri nəzərə alınmaqla, Kİİ obyektlərinin siyahısının mütəmadi yenilənməsi vacib hesab olunur [11]. Mövcud siyahının təkmilləşdirilməsi kibertəhdidlərin real vəziyyətinə uyğun tədbirlərin planlaşdırılmasını və resursların effektiv istifadəsini təmin etməklə, dövlətin kiberməkan üzərində nəzarət imkanlarını strateji səviyyədə daha da möhkəmləndirə bilər.

Kİİ subyektləri üçün xüsusi təhlükəsizlik tələblərinin hazırlanmasının təşviqi də mühüm addımlardan biri hesab olunur [11,12]. Bu tələblər, infrastrukturun spesifik texnoloji və əməliyyat xüsusiyyətlərinə uyğun təhlükəsizlik tədbirlərinin tətbiqinə şərait yaradaraq, dayanıqlılığı artıra və kritik infrastrukturun milli kiberməkan daxilində tam nəzarətə alınmasını təmin edə bilər. Eyni zamanda, SCADA və digər sənaye idarəetmə sistemlərinin təhlükəsizliyi üzrə metodiki tövsiyə sənədlərinin hazırlanması və tətbiqi də kritik proseslərin fasiləsizliyinin qorunması və dövlətin kibersuverenlik mandatının icrası baxımından strateji addım hesab oluna bilər.

Mövcud çağırışlardan biri də Kİİ obyektlərinin kibertəhlükəsizlik vəziyyətinə fasiləsiz nəzarətin təmin edilməsidir [12]. Bu, 24/7 rejimində monitorinq, insidentlərin operativ aşkarlanması və reaksiya mexanizmlərinin tətbiqini, eləcə də kənar audit və müdaxilə sınaqlarının sistemli aparılmasını nəzərdə tutur və dövlətin kiberməkan üzərində suveren nəzarət funksiyasının real tətbiqinə imkan verir.

Həmçinin, risklərin qiymətləndirilməsi və onların idarə olunması məqsədilə Kİİ təhlükəsizliyi üzrə risk xəritəsinin formalaşdırılması da strateji əhəmiyyət daşıyır və milli kiberməkanın dayanıqlılığını əhəmiyyətli dərəcədə artıra bilər. Kİİ ilə bağlı təhlükəsizlik risklərinin müntəzəm olaraq müəyyən edilməsi və kompleks şəkildə qiymətləndirilməsi, həmçinin bu risklərin mümkün iqtisadi və maliyyə nəticələrinin hesablanaraq idarəetmə qərarlarında nəzərə alınması xüsusilə aktualdır [11]. Bu yanaşmanın tətbiqi Kİİ subyektlərinə prioritet təhlükəsizlik investisiyalarını müəyyən etməyə, dövlət orqanlarına isə resursların strateji bölgüsünü daha əsaslandırılmış şəkildə həyata keçirməyə imkan verə bilər.

Eyni zamanda, Kİİ obyektlərinin təhlükəsizliyi ilə bağlı kibertəhlükəsizlik xidməti provayderlərinə dair müəyyən edilmiş tələblərə cavab verməyən hüquqi şəxslər tərəfindən göstərilən xidmətlərdən institusional asılılığın aradan qaldırılması zəruridir [11]. Bu istiqamətdə akkreditasiya və sertifikatlaşdırma mexanizmlərinin gücləndirilməsi, milli və etibarlı provayder ekosisteminin formalaşdırılması və strateji əhəmiyyətli xidmətlərin milli yurisdiksiya daxilində həyata keçirilməsi kibersuverenliyin möhkəmləndirilməsi baxımından mühüm əhəmiyyət kəsb edir.

Nəhayət, Kİİ subyektlərində fəaliyyət göstərən aidiyyəti şəxslərin mütəmadi təlim və sertifikasiya proqramlarına cəlb olunması institutlararası və sektoral dayanıqlılığın gücləndirilməsinə töhfə verə bilər. Bu tədbirlər kadrların peşəkarlığını artırmaqla yanaşı, Kİİ-lərdə daha yüksək kibertəhlükəsizlik mədəniyyətinin formalaşmasına və potensial insidentlərin daha effektiv, koordinasiyalı və milli kiberməkanın suverenliyini qoruyacaq şəkildə qarşısının alınmasına xidmət edə bilər.

Beləliklə, mövcud çağırışların öhdəsindən gəlmək və Kİİ təhlükəsizliyini davamlı təmin etmək üçün beynəlxalq standartlara uyğun normativ bazanın təkmilləşdirilməsi, risk əsaslı yanaşmanın genişləndirilməsi, texnoloji və insan kapitalı resurslarının gücləndirilməsi, eləcə də fasiləsiz monitorinqin tətbiqi yalnız təhlükəsizliyin gücləndirilməsinə deyil, həm də dövlətin kiberməkan üzərində suveren nəzarətinin möhkəmləndirilməsinə və kibersuverenliyin praktik təminatına xidmət edən prioritet istiqamətlər kimi müəyyən edilməlidir.

NƏTİCƏ

Məqalədə kritik informasiya infrastrukturunun təhlükəsizliyinin Azərbaycan Respublikasının milli təhlükəsizlik və kibersuverenlik siyasəti çərçivəsində strateji prioritet kimi mühüm rolu təhlil edilmişdir. Qeyd olunur ki, Kİİ-nin təhlükəsizliyi dövlətin milli kiberməkan üzərində suveren nəzarət imkanlarını institusional və texnoloji baxımdan təmin etməklə yanaşı, əsas ictimai xidmətlərin fasiləsizliyini qorumaq, strateji resursların mühafizəsini həyata keçirmək və kibertəhdidlərə çevik hüquqi-texniki reaksiyanı təmin etmək üçün funksional əsas komponent kimi çıxış edir. Son illər qəbul edilmiş normativ-hüquqi aktlar, Kİİ-nin təhlükəsizliyinin təmin edilməsi üzrə institusional mexanizmlərin və hüquqi çərçivənin formalaşdırılmasına xidmət etmiş, Kİİ subyektlərinin aidiyyəti funksional fəaliyyətini normativ əsaslarla tənzimləyərək monitorinq və qiymətləndirmə imkanlarını reallaşdırmışdır.

Eyni zamanda, müvafiq beynəlxalq standartların tətbiqi, Kİİ obyektlərinin və sahələrinin risk əsaslı prioritetləşdirilməsi, SCADA və digər sənaye idarəetmə sistemlərinin təhlükəsizliyinə dair metodiki tövsiyələrin hazırlanması, habelə xüsusi təhlükəsizlik tələblərinin hazırlanmasının təşviqi və Kİİ subyektlərində ixtisaslı kadrların davamlı təlim və sertifikasiya proqramlarına cəlb edilməsi dövlətin kiberməkan üzərində suveren nəzarətini daha da gücləndirə və kibersuverenliyin daha effektiv həyata keçirilməsini təmin edə bilər. Nəzərə alınmalıdır ki, Kİİ-nin təhlükəsizliyi yalnız infrastrukturun dayanıqlılığının artırılması və risklərin minimallaşdırılması məqsədini daşımır, həm də dövlətin milli kiberməkan daxilində institusional, hüquqi və texnoloji səlahiyyətlərinin effektiv icrasını təmin edən əsas mexanizm kimi çıxış edir və dövlətin rəqəmsal suverenliyinin qorunması və strateji maraqlarının mühafizəsində həlledici əhəmiyyət kəsb edir.

ƏDƏBİYYAT

[1] *“İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu*, Apr. 3, 1998, No. 460-IQ.

[2] *Montevideo Convention on the Rights and Duties of States*, 1933, 165 LNTS 19.

[3] United Nations General Assembly, “Report of the Group of Governmental Experts on developments in the field of information and

telecommunications in the context of international security,” A/70/174, 2015.

[4] United Nations General Assembly, “Report of the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security,” A/76/135, 2021.

[5] M. N. Schmitt, Ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, U.K.: Cambridge University Press, 2017.

[6] Azərbaycan Respublikası Prezidenti, *“Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında” Fərman*, Apr. 17, 2021, No. 1315.

[7] Azərbaycan Respublikası Nazirlər Kabineti, *“Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi qaydaları”*, Jul. 17, 2023, No. 229.

[8] Azərbaycan Respublikası Nazirlər Kabineti, *“Kritik informasiya infrastrukturu obyektlərinin reyestrinin strukturu, yaradılması və aparılması qaydası”*, Jul. 17, 2023, No. 230.

[9] Azərbaycan Respublikası Nazirlər Kabineti, *“Kritik informasiya infrastrukturu obyektlərinin siyahısının təsdiq edilməsi haqqında”*, Nov. 29, 2024, No. 501.

[10] [10] Azərbaycan Respublikası Prezidenti, *“Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası”*, Aug. 28, 2023, No. 4060.

[11] Azərbaycan Dövlət İnformasiya Agentliyi, “Kritik informasiya infrastrukturunun təhlükəsizlik vəziyyətinin qiymətləndirilməsinin ilkin mərhələsi başa çatıb,” 2025. [Online]. Available: https://azertag.az/xeber/kritik_informasiya_infrastrukturunun_tehlukesizlik_veziyyetinin_qiymetlendirilmesinin_ilkin_merhelesi_basa_chatib__komissiyanin_iclasi_kechirildi-3768011

[12] Azərbaycan Dövlət İnformasiya Agentliyi, “Kritik informasiya infrastrukturunun təhlükəsizliyi üzrə Komissiyanın ötən ilin yekunlarına dair iclası keçirilib,” 2026. [Online]. Available: https://azertag.az/xeber/kritik_informasiya_infrastrukturunun_tehlukesizliyi_uzre_komissiyanin_oten_ilin_yekunlarina_dair_iclasi_kechirilib-3968931

Security of Critical Information Infrastructure in the Context of Cyber Sovereignty: the Normative and Strategic Approach of the Republic of Azerbaijan

Elvin Balajanov

The State Security Service of the Republic of Azerbaijan,
National Cybersecurity Center, Baku, Azerbaijan

Abstract— The article highlights that ensuring the security of critical information infrastructure (CII) constitutes a strategic priority for the Republic of Azerbaijan and occupies a key position among the essential areas for strengthening the country’s cyber sovereignty. It emphasizes that CII security serves as a fundamental factor in establishing effective state control over the national cyberspace. The study notes that in recent years, significant measures have been undertaken in the legal, organizational, and technical-technological spheres to ensure CII security, leading to the formation of a relevant normative framework and institutional mechanisms. At the same time, there is an emerging need for CII operators to place greater emphasis on infrastructure security and to further deepen risk-based approaches. The article analyses existing approaches, identifies current challenges, and proposes development directions for strengthening CII security as a practical mechanism for the implementation of cyber sovereignty.

Keywords– cybersecurity; critical information infrastructure; cyber sovereignty; normative-legal framework.