İNFORMASİYA TƏHLÜKƏSİZLİYİ MİLLİ TƏHLÜKƏSİZLİK AMİLİ KİMİ

UOT 327: 140.8
UOT 327: 930.22 UOT 327
DOI:10.30546/3006-0346.2024.2.80.185

NURƏDDİN MEHDİYEV
Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyasının dissertantı

E-mail: nuraddin_mehdiyev@yahoo.com

Giriş

İnformasiya təhlükəsizliyinin milli təhlükəsizlik amili kimi əhəmiyyətini bir-birinə bağlı olan müasir dünyada qiymətləndirməmək olmaz. Bu kritik əlaqə müxtəlif ölçüləri, o cümlədən kibertəhlükəsizlik, iqtisadi təsirlər, diplomatik nəticələr və hərbi əməliyyatları əhatə edir. İnformasiya təhlükəsizliyi təkcə texniki məsələ deyil, həm də texnoloji yenilikləri, diplomatik təşəbbüsləri və beynəlxalq əməkdaşlığı əhatə edən hərtərəfli yanaşmalar tələb edən milli təhlükəsizlik strategiyasının əsas aspektidir. İnformasiya əsrinin mürəkkəbliklərini idarə edərkən dövlətlər qlobal səhnədə suverenliklərini, sabitliklərini və strateji maraqlarını qorumaq üçün rəqəmsal aktivlərinin qorunmasına üstünlük verməlidirlər.

Qlobal təhdidlərin inkişaf edən mənzərəsini və rəqəmsal texnologiyalara artan etibarı nəzərə alaraq, informasiya təhlükəsizliyinin milli təhlükəsizlik amili kimi həlli heç vaxt bu qədər aktual olmayıb. Kibertəhlükələrin tezliyi, mürəkkəbliyi və şiddəti artmışdır. Milli dövlətlər, kriminal təşkilatlar və hakerlər rəqəmsal infrastrukturun zəifliklərindən istifadə etmək üçün qabaqcıl üsullardan istifadə edirlər ki, bu da milli təhlükəsizlik üçün daimi risk yaradır.

Süni intellekt, Əşyaların İnterneti (IoT) və 5G şəbəkələri kimi inkişaf etməkdə olan texnologiyaların sürətlə mənimsənilməsi yeni hücum vektorlarını təqdim edir və kiber təhdidlərin potensial təsirini gücləndirir. Bu texnologiyaların təhlükəsizliyi zərərli aktorların öz zəifliklərindən istifadə etməsinin qarşısını almaq üçün çox vacibdir [9, 28].

Qloballaşan ticarət və bir-biri ilə əlaqəli maliyyə sistemləri dövründə iqtisadi sabitlik təhlükəsiz məlumat axınından asılıdır. Maliyyə institutlarına, sənaye sektorlarına və ya kritik infrastruktura kiberhücumlar nəinki ayrı-ayrı ölkələri, həm də bütün beynəlxalq iqtisadi nizamı sabitsizləşdirərək ardıcıl təsirlərə malik ola bilər.

Diplomatik münasibətlər və beynəlxalq etimad kiber insidentlər nəticəsində ciddi şəkildə pozula bilər. Diplomatik kommunikasiyaların pozulması və ya kiber-casusluq diplomatik böhranlara səbəb ola, xalqlar arasında etimadı sarsıda və geosiyasi dinamikaya təsir edə bilər.

Müasir hərbi əməliyyatlar böyük ölçüdə informasiya texnologiyalarına və bir-biri ilə əlaqəli şəbəkələrə əsaslanır. Komanda və idarəetmə sistemlərinin, kəşfiyyat vasitələrinin və ya kritik infrastrukturun güzəşti ölkənin müdafiə qabiliyyətini və hazırlığını əhəmiyyətli dərəcədə sarsıda bilər.

Dezinformasiya kampaniyaları və sosial media manipulyasiyası da daxil olmaqla informasiya müharibəsindən istifadə xalqların demokratik prosesləri üçün birbaşa təhlükə yaradır. İctimai rəyin manipulyasiya edilməsi həm ölkə daxilində, həm də beynəlxalq səviyyədə dərin siyasi nəticələrə səbəb ola bilər.

Enerji şəbəkələri, nəqliyyat sistemləri və səhiyyə müəssisələri kimi əsas xidmətlər getdikcə bir-biri ilə əlaqəli rəqəmsal sistemlərdən asılıdır. Kritik infrastruktura kiberhücum vətəndaşların rifahına təsir edən və milli təhlükəsizliyi təhdid edən geniş miqyasda pozulmalara səbəb ola bilər.

Kibertəhlükəsizliklə bağlı aydın beynəlxalq normaların və sazişlərin olmaması problemi daha da gücləndirir. Koordinasiyalı və əməkdaşlıq yanaşması transsərhəd kibertəhlükələrlə effektiv mübarizə aparmaq və kiberməkanda məsuliyyətli dövlət davranışı üçün çərçivə yaratmaq üçün vacibdir [4, 77-78].

Bu amillərin fonunda informasiya təhlükəsizliyinin prioritetləşdirilməsinin aktuallığı göz qabağındadır. Millətlər güclü kibertəhlükəsizlik tədbirlərinə sərmayə qoymalı, beynəlxalq əməkdaşlığı inkişaf etdirməli və rəqəmsal dövrlə bağlı çoxşaxəli riskləri azaltmaq üçün hərtərəfli strategiyalar hazırlamalıdır. Bu çağırışların dərhal həll edilməməsi getdikcə bir-birinə bağlı olan dünyada xalqların sabitliyi, rifahı və təhlükəsizliyi üçün geniş nəticələrə səbəb ola bilər.

1. İnformasiya təhlükəsizliyinin milli təhlükəsizliyə təsirləri

Sürətlə inkişaf edən beynəlxalq münasibətlər mənzərəsində informasiya təhlükəsizliyinin rolu milli təhlükəsizliyin hərtərəfli çərçivəsində dayaq

nöqtəsi kimi meydana çıxmışdır. Rəqəmsal texnologiyalar tərəfindən dəstəklənən qarşılıqlı əlaqə informasiyanın mühafizəsinin sadəcə texnoloji problem deyil, həm də bir millətin dayanıqlığının və sabitliyinin kritik müəyyənedicisi olduğu bir dövrün başlanğıcını qoydu.

İnformasiya təhlükəsizliyi məlumatların, rabitə kanallarının və rəqəmsal infrastrukturun icazəsiz girişdən, manipulyasiyadan və ya pozulmalardan qorunmasını əhatə edir. Bu domenin əhəmiyyəti diplomatik, iqtisadi və hərbi işlərin mərkəzinə nüfuz edən kibertəhlükəsizlik sahəsindən çox-çox kənara çıxır. Ölkələr kiber təhdidlər, iqtisadi casusluq və informasiya müharibəsi ilə mübarizə apardıqca, informasiya təhlükəsizliyi ilə milli təhlükəsizlik arasındakı əlaqə getdikcə daha aydın görünür [5, 44].

Müasir geosiyasi mənzərə milli dövlətlərin, qeyri-dövlət aktorlarının və texnoloji irəliləyişlərin mürəkkəb qarşılıqlı təsiri ilə xarakterizə olunur. Milli dövlətlər kəşfiyyat məlumatları toplamaq, ictimai rəyə təsir etmək və düşmənlərin həyati funksiyalarını potensial olaraq pozmaq üçün mürəkkəb üsullardan istifadə edərək kiber əməliyyatlarla məşğul olurlar. Kibercinayətkarlardan tutmuş hakerlərə qədər qeyri-dövlət aktyorları informasiya təhlükəsizliyi mənzərəsinin incəliklərini daha da gücləndirirlər.

İqtisadi təsirlər informasiya təhlükəsizliyi və milli təhlükəsizlik arasında simbiotik əlaqənin digər mühüm tərəfini təşkil edir. Sənaye casusluğu, əqli mülkiyyətin oğurlanması və maliyyə sistemlərinin manipulyasiyası ölkənin iqtisadi rifahına ciddi təsir göstərə bilər. Qlobal iqtisadiyyat daha rəqəmsallaşdıqca, maliyyə institutlarının və kritik infrastrukturun kibertəhlükələrə qarşı həssaslığı möhkəm informasiya təhlükəsizliyi tədbirlərinin vacibliyini vurğulayır [4, 82-83].

Ənənəvi olaraq qapalı qapılar arxasında aparılan diplomatiya indi diplomatik kabellərin və kiber pozuntulara həssas olan həssas kommunikasiyaların mübadiləsi ilə rəqəmsal aləmdən keçir. Həm ənənəvi, həm də kiber-aktiv casusluq dövlət sirrinin, hərbi strategiyaların və kəşfiyyat əməliyyatlarının məxfiliyinə daim təhlükə yaradır və bununla da informasiya təhlükəsizliyinə kompleks yanaşmanı zəruri edir.

Hərbi əməliyyatlar və kritik infrastrukturun qorunmasından tutmuş siyasi təsir və dezinformasiyanın incəliklərinə qədər, bu elementlərin bir-birinə qarışmış təbiəti informasiya əsrinin çağırışlarını həll etmək üçün, dövlətlərin istifadə etdiyi strategiyaları formalaşdırır. Bundan əlavə, beynəlxalq əməkdaşlığın imperativi və kibertəhlükəsizlik problemlərinin həlli üçün diplomatik çərçivələrin inkişafı araşdırılacaq və təhlükəsiz qlobal mühitin yaradılması üçün tələb olunan birgə səylər vurğulanacaq.

İnformasiya təhlükəsizliyi milli təhlükəsizliyin mühüm amili kimi müasir dünyada ölkənin ən qiymətli sərvətlərindən birinə çevrilib. Bu gün informasiya texnologiyaları ölkələrin iqtisadi və siyasi inkişafında, eləcə də milli təhlükəsizliyin təmin edilməsində əsas rol oynayır. Lakin rəqəmsal texnologiyalardan istifadənin artması ilə kiberhücumlar, haker hücumları, məxfi məlumatların oğurlanması, kompüter sistemlərinə haker hücumu və s. riskləri artır [3].

İnformasiya təhlükəsizliyi beynəlxalq siyasi münasibətlər sferasında mühüm amildir və milli təhlükəsizlik anlayışı ilə sıx bağlıdır. Millətlərin texnologiya və informasiya şəbəkələri vasitəsilə bir-birinə bağlandığı müasir dövrdə həssas məlumatların və kommunikasiyaların mühafizəsi əsas məsələyə çevrilib. Beynəlxalq münasibətlər kontekstində informasiya təhlükəsizliyinin milli təhlükəsizlik amili kimi nəzərə alınmalı olan bir neçə əsas aspektini qeyd edirik:

1. Kiber təhdidlər və hücumlar: Hökumətlər kəşfiyyat məlumatları toplamaq, düşmənləri dağıtmaq və ya zərər vurmaq üçün, kiber əməliyyatlarda iştirak edirlər. Nümunələrə dövlət tərəfindən dəstəklənən hakerlik və kibercasusluq daxildir. Kibercinayətkarlar və hakerlər ölkənin informasiya infrastrukturu üçün əhəmiyyətli təhlükələr yarada bilər. Hücumlar hökumət sistemlərini, kritik infrastrukturu və ya özəl müəssisələri hədəfə ala bilər.

2. İqtisadi təsirlər: Millətlər rəqabət üstünlüyü əldə etmək üçün bir-birlərinin sənayelərini hədəfə ala bilərlər. Əqli mülkiyyətin, kommersiya sirlərinin və həssas iqtisadi məlumatların oğurlanması ağır iqtisadi nəticələrə səbəb ola bilər. Maliyyə institutlarına hücumlar və ya maliyyə məlumatlarının manipulyasiyası, iqtisadiyyatları sabitsizləşdirə və qlobal maliyyə sisteminin bütövlüyünü poza bilər.

3. Diplomatiya və dövlət sirləri: Diplomatik əlaqənin pozulması beynəlxalq münasibətləri gərginləşdirə bilər. Məxfi məlumatların icazəsiz açıqlanması, diplomatik böhranlara səbəb ola və bir ölkənin danışıqlar mövqeyinə təsir edə bilər. İnformasiya təhlükəsizliyi dövlət sirlərini, hərbi strategiyaları və kəşfiyyat əməliyyatlarını xarici casusluqdan qorumaq üçün çox vacibdir.

4. Hərbi əməliyyatlar və infrastruktur: Müasir hərbi əməliyyatlar böyük ölçüdə informasiya texnologiyalarına əsaslanır. Komanda və idarəetmə sistemlərinin təhlükəsizliyinin təmin edilməsi ölkənin müdafiə qabiliyyətinin effektivliyini qorumaq üçün vacibdir. Enerji, rabitə şəbəkələri və nəqliyyat sistemləri kimi kritik infrastrukturun qorunması, milli təhlükəsizlik üçün həyati əhəmiyyət kəsb edir. Bu sistemlərə edilən kiberhücumlar ölkənin sabitliyinə ardıcıl təsir göstərə bilər.

5. Siyasi təsir və dezinformasiya: Dövlətlər ictimai rəyi manipulyasiya etmək, dezinformasiya yaymaq və digər dövlətlərdə siyasi proseslərə təsir etmək üçün informasiya müharibəsi aparırlar.

Təbliğat yaymaq, nifaq salmaq və ictimai əhvali-ruhiyyəni manipulyasiya etmək, sosial media platformalarından istifadə bir millətin sabitliyi və beynəlxalq əlaqələri üçün geniş nəticələrə səbəb ola bilər.

6. Beynəlxalq əməkdaşlıq və sazişlər: Millətlər kibertəhlükəsizlik problemlərini həll etmək üçün beynəlxalq müqavilələr və çərçivələr üzərində əməkdaşlıq edirlər. Transsərhəd kibertəhlükələrin yumşaldılması və kiberməkanda məsuliyyətli davranış normalarının yaradılması üçün əməkdaşlıq vacibdir [6, 33].

2. İnformasiya təhlükəsizliyinin təminatı

İnformasiya təhlükəsizliyinin pozulması dövlət sirrinin sızması, mühüm infrastrukturun pozulması, iqtisadi itkilər, habelə vətəndaşların fiziki təhlükəsizliyinə təhdid kimi ciddi nəticələrə səbəb ola bilər. İnformasiya təhlükəsizliyi milli təhlükəsizlik üçün mühüm əhəmiyyət kəsb edən məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını qorumağa yönəlmiş tədbirləri əhatə edir. Bura dövlət sirlərinin, kritik infrastrukturun, vətəndaşların şəxsi məlumatlarının və digər həssas məlumatların qorunması daxil ola bilər. Ona görə də informasiya təhlükəsizliyinin təmin edilməsi milli maraqların qorunmasına yönəlmiş dövlət siyasətinin prioritet istiqamətlərindən biridir. Bura informasiya texnologiyalarından istifadəni tənzimləyən qanunvericiliyin yaradılması, informasiya təhlükəsizliyi sisteminin inkişafı, informasiya təhlükəsizliyi üzrə mütəxəssislərin hazırlanması və ixtisasının artırılması, habelə informasiya təhlükəsizliyi sahəsində risk və təhdidlər barədə ictimaiyyətin məlumatlılığının artırılması daxildir.

İnformasiya sistemləri və informasiya infrastrukturu lazımi səviyyədə qorunmadan milli təhlükəsizlik təmin edilə bilməz. Bu, təkcə müvafiq siyasət və prosedurların işlənib hazırlanmasını və həyata keçirilməsini deyil, həm də məlumatların təhlükəsizliyini təmin etmək üçün kadrların lazımi bacarıq və alətlərlə hazırlanmasını və təchiz edilməsini nəzərdə tutur. Bundan əlavə, bütün milli informasiya infrastrukturunun bütövlüyünü və etibarlılığını təmin etmək üçün müxtəlif dövlət və özəl qurumlar arasında əməkdaşlıq lazımdır [9, 29].

İnformasiya təhlükəsizliyi (İS) informasiyanın icazəsiz əldə edilməsi, istifadəsi, dəyişdirilməsi, yayılması, məhv edilməsi və digər təhlükələrdən qorunması ilə məşğul olan sahədir. Onun bir çox növləri var, onlardan bəziləri aşağıda verilmişdir:

1. Məxfilik: Bu, məlumatın icazəsiz girişdən qorunmasıdır. Məqsəd yalnız səlahiyyətli istifadəçilərin həssas məlumatlara çıxış əldə etməsini təmin etməkdir.

1. Dürüstlük: Bu, məlumatlara icazəsiz dəyişikliklərə qarşı qorunmadır. Məqsəd ötürülmə və ya saxlama zamanı məlumatların dəyişdirilməməsini və ya pozulmamasını təmin etməkdir.

2. Mövcudluq: Bu, informasiyaya girişin kəsilməsinə qarşı qorunmadır. Məqsəd məlumatın hər zaman səlahiyyətli istifadəçilər üçün əlçatan olmasını təmin etməkdir.

3. Doğrulama: Bu, istifadəçilərin və cihazların autentifikasiyasıdır. Məqsəd yalnız səlahiyyətli istifadəçilərin qorunan məlumatlara çıxışını təmin etməkdir.

4. Avtorizasiya: Bu, səlahiyyətli istifadəçilərə girişin verilməsi prosesidir. Məqsəd icazələrə və giriş hüquqlarına əsaslanan məlumatlara çıxışa nəzarət etməkdir.

5. Audit: Bu, məlumatların istifadəsinə nəzarətdir. Məqsəd məlumatın icazəsiz daxil olmasını və ya istifadəsini aşkar etmək və qarşısını almaqdır.

6. Şifrələmə: Bu, verilənlərin şifrələnməsi yolu ilə məlumatın icazəsiz girişdən qorunmasıdır. Məqsəd məlumatın məxfiliyini və bütövlüyünü təmin etməkdir.

7. Zərərli proqram təminatı: Bu viruslar, qurdlar, troyanlar və digər təhlükələr kimi zərərli proqramlardan qorunmadır. Məqsəd məlumatların pozulmasının və ya məhv edilməsinin qarşısını almaq və sistemin təhlükəsizliyini təmin etməkdir.

8. Şəbəkə hücumlarından müdafiə: Bu, şəbəkə infrastrukturunu hədəf alan hücumlara qarşı qorunmadır. Məqsəd informasiyaya icazəsiz girişin, siste-

min zədələnməsinin və ya onun nasazlığının qarşısını almaqdır [8, 36-38].

9. Fiziki müdafiə: Bu, serverlər, kompüterlər və digər cihazlar kimi fiziki resursların qorunmasıdır.

Milli təhlükəsizliyin əsas şərtləri ölkədən və onun vəziyyətindən asılı olaraq fərqlənə bilər. Bununla belə, ümumilikdə, milli təhlükəsizliyin təmin edilməsi üçün vacib sayılan aşağıdakı şərtləri ayırmaq olar:

1. Siyasi sabitlik və sosial ahəngdarlıq. Siyasi sistemin sabitliyi və ictimai harmoniya dövlətin təhlükəsizliyinin əsasını təşkil edir. Siyasi və ya sosial qeyri-sabitlik zamanı bu, ictimai asayişin və vətəndaşların təhlükəsizliyinin pozulmasına səbəb ola bilər.

2. İqtisadi sabitlik və davamlılıq. İqtisadi sabitlik və davamlılıq milli təhlükəsizliyin mühüm şərtidir. İnkişaf etmiş iqtisadiyyat və yüksək məşğulluq səviyyəsi dövlətə öz təhlükəsizliyini təmin etməyə, müdafiə və təhlükəsizlik sahəsində imkanlarını artırmağa imkan verir.

3. Milli sərhədlərin qorunması. Sərhəd təhlükəsizliyinin təmin edilməsi milli təhlükəsizliyin vacib şərtidir. Sərhədin qeyri-kafi mühafizəsi dövlətin ərazisinə qeyri-qanuni girişə səbəb ola və onun vətəndaşlarının təhlükəsizliyini təhdid edə bilər.

4. Terrorizm və ekstremizmlə mübarizə. Terrorçuluq və ekstremizmlə mübarizə milli təhlükəsizliyin təmin edilməsi üçün mühüm şərtdir. Terrorçu və ekstremist təşkilatlar dövlətə və onun vətəndaşlarına ciddi ziyan vura bilər.

5. İnformasiya texnologiyalarının təhlükəsizliyi və informasiya təhlükəsizliyi. İnformasiya texnologiyalarının təhlükəsizliyinin və informasiya təhlükəsizliyinin təmin edilməsi milli təhlükəsizliyin mühüm şərtidir. Kiberhücumlardan və kibercinayətlərdən qorunma, o cümlədən məxfi məlumatların mühafizəsi informasiya təhlükəsizliyi sahəsində ən mühüm vəzifələrdəndir.

6. Vətəndaşların daxili təhlükəsizlik istiqamətində təhdidlərdən qorunması. Vətəndaşları zorakılıq kimi daxili təhlükəsizlik təhdidlərindən qorumaq mühümdür [8, 138-139].

Rəqəmsal dünyada təhlükəsizliyin təmin edilməsində kiber institutların və idarəetmənin tənzimlənməsi (cyber institutions and governance) mühüm aspektlərdəndir. Kiber institutlar rəqəmsal texnologiyalarla məşğul olan və kiberhücumlara məruz qala bilən təşkilatlardır. Bu qurumlara dövlət qurumları, banklar, şirkətlər, təhsil müəssisələri və bir çox başqa qurumlar daxil ola bilər.

Kiber institutların tənzimlənməsi və idarəçiliyinin əsas aspektlərindən biri kiberməkanı təhlükəsiz saxlayan qanunvericilik və siyasətlərin işlənib hazırlanması və həyata keçirilməsidir. Bura məlumatların saxlanması və istifadəsini tənzimləyən qanunlar, şəxsi məlumatların qorunması, kibercinayətkarlığın tənzimlənməsi və s. aid edilə bilər.

Kiber institutların tənzimlənməsinin digər mühüm aspekti müvafiq təhlükəsizlik və mühafizə tədbirlərinin təmin edilməsidir. Bura antiviruslar və firewallar kimi təhlükəsizlik tədbirlərinin istifadəsi, proqram təminatının müntəzəm yenilənməsi, işçilər üçün kibertəhlükəsizlik təlimi və s. daxil ola bilər [7, 376-377].

Kiber institutların idarə edilməsində mühüm element həm də təhlükəsizlik norma və qaydalarının icrasına nəzarətdir. Buraya təhlükəsizlik monitorinqi, log təhlili və s. daxil ola bilər. İstənilən təhlükəsizlik pozuntusuna tez və effektiv reaksiya vermək üçün effektiv təhlükəsizlik insidentinə cavab mexanizminin olması da vacibdir.

Kiber institutların və idarəetmənin tənzimlənməsi rəqəmsal dünyada təhlükəsizliyin təmin edilməsində mühüm aspektlərdəndir. Onlar müvafiq qanunvericilik və siyasətlərin işlənib hazırlanmasını, müvafiq təhlükəsizlik tədbirlərinin tətbiqini və onların icrasını tələb edir.

ABŞ-da kiber institutlar və idarəetmə bir sıra qanunlara və dövlət qurumlarına tabedir. Kiber institutları tənzimləyən əsas qanunlardan biri dövlət təşkilatlarının məxfi məlumatlarının mühafizəsi tələblərini müəyyən edən 2002-ci ildə qəbul edilmiş İnformasiya Təhlükəsizliyi Aktıdır. Digər mühüm qanun ölkənin informasiya infrastrukturunun qorunması üçün tələbləri müəyyən edən 2014-cü il Kibertəhlükəsizlik İnformasiya İnfrastrukturunun Mühafizəsi Aktıdır. Bundan əlavə, ABŞ-da kibertəhlükəsizliyə və kiber institutlara cavabdeh olan bir neçə dövlət qurumu var. Onlardan biri kibertəhlükəsizlik sahəsində dövlət qurumlarının səylərini əlaqələndirən Milli Kibertəhlükəsizlik və Kommunikasiya İnteqrasiya Mərkəzidir [2]. Həmçinin ABŞ-da kibertəhlükəsizliyin yaxşılaşdırılması üçün tövsiyələr hazırlayan Milli Standartlar və Texnologiya İnstitutu var. Federal Təhqiqatlar Bürosu və Milli Təhlükəsizlik Agentliyinin də kibertəhlükəsizliyi qorumaq və kibercinayətkarlıqla mübarizə apar-

maq üçün öz proqramları var. Ümumiyyətlə, ABŞ-da kiberməkanı təhlükəsiz saxlamaq üçün birlikdə işləyən kiber institutları və hökumətləri idarə edən geniş qanun və hökumətlər vardır [1, 47-249].

Kiber institutlar sahəsində təcrübə Azərbaycanda iqtisadiyyatın müxtəlif sektorlarında və dövlət qurumlarında kibertəhlükəsizliyin yaxşılaşdırılması üçün tətbiq oluna bilər. Kiber institutlar kiberhücumlardan müdafiənin müasir üsullarını və kibertəhlükəsizlik üzrə mütəxəssislərin hazırlanmasını təklif edə bilər. Bundan əlavə, onlar kibertəhlükəsizlik sahəsində tədqiqat və yeni texnologiyaların işlənib hazırlanmasında iştirak edə bilərlər.

İdarəetmə təcrübəsi dövlət idarəçiliyinin inkişafı, biznes şəraitinin yaxşılaşdırılması və xarici investisiyaların cəlb edilməsi üçün tətbiq oluna bilər. İdarəetmə bacarıqları qərar qəbuletmə proseslərini təkmilləşdirmək, biznes proseslərini sadələşdirmək və təşkilatların fəaliyyətini yaxşılaşdırmaq üçün tətbiq oluna bilər. Hər iki sahədə təcrübə tətbiq etməyin mümkün yollarından biri kibertəhlükəsizlik sahəsində təlim və tədqiqatlar üzrə ixtisaslaşmış kiber institutun yaradılması ola bilər. Belə bir qurum kibertəhlükəsizlik üzrə mütəxəssislərin təşkilatların ehtiyaclarını daha yaxşı başa düşmələri və kibertəhlükəsizliklə bağlı qərarların qəbul edilməsində iştirak etmələri üçün idarəetmə təhsili proqramları da təklif edə bilər. Bundan əlavə, idarəetmə təcrübəsindən dövlət orqanlarının idarə edilməsinin təkmilləşdirilməsi, o cümlədən qərarların qəbulu proseslərinin təkmilləşdirilməsi, ictimai işlərdə ictimaiyyətin iştirakının təkmilləşdirilməsi və dövlət orqanlarının səmərəliliyinin artırılması üçün istifadə oluna bilər. Bu, Azərbaycan vətəndaşlarının həyat keyfiyyətinin yaxşılaşmasına və ölkəyə xarici investisiyaların cəlb edilməsinə səbəb ola bilər.

Nəticə

İnformasiya təhlükəsizliyi müasir geosiyasi mənzərədə milli təhlükəsizliyin ayrılmaz hissəsidir. Millətlər öz maraqlarını qorumaq və beynəlxalq arenada sabitliyi qorumaq üçün kibertəhlükələrin, iqtisadi casusluğun və informasiya müharibəsinin mürəkkəb şəbəkəsində fəaliyyət göstərməlidirlər. Əməkdaşlıq, diplomatik səylər və güclü kibertəhlükəsizlik tədbirlərinin inkişafı, informasiya təhlükəsizliyi problemlərinin həllində ölkənin strategiyasının vacib komponentləridir.

Açar sözlər: *İnformasiya təhlükəsizliyi, milli təhlükəsizlik, kibertəhlükəsizlik, beynəlxalq əməkdaşlıq, informasiya əsri.*

ƏDƏBİYYAT SİYAHISI:

1. Anagnostakis D. The European Union-United States cybersecurity relationship: a transatlantic functional cooperation/ Journal of Cyber Policy 2021/ vol 6, p. 243-261URL: https://www.tandfonline.com/doi/full/10.1080/-23738871.2021.1916975

2. Cybersecurity Policy (NSPD 54), Cybersecurity Policy via EPIC (HSPD 23) // Federation Of American Scientists [Electronic resource]. URL: http://fas.org/irp/offdocs/nspd/nspd-54.pdf (accessed 25 June 2016).

3. EU Cybersecurity Strategy/ European Commission/ (2022) URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

4. Information warfare. Separating hype from reality. / Ed. by L. Armistead. – Washington: – 2007. – p. 73-93.

5. Information operations. Warfare and the hard reality of soft power. / Ed. By L. Armistead. – Washington: – 2004. – 277 p.

6. Kissinger, G. World Order: [Electronic resource] / New York: Penguin Press. – 2014. – 432 p. URL: https://www.academia.edu/10945701/World_Order_by_Henry_Kissinger

7. Maranga, M.J., Nelson M. Emerging Issues in Cyber Security for Institutions of Higher Education. IJCSN - International Journal of Computer Science and Network, Volume 8, Issue 4, August 2019/ p. 371-379/ URL: https://www.researchgate.net/profile/Jared-Maranga/publication/335664780_Emerging_Issues_in_Cyber_Security_for_Institutions_of_Higher_Education/links/5d729c32299bf1cb808b4629/Emerging-Issues-in-Cyber-Security-for-Institutions-of-Higher-Education.pdf

8. Жидко Е.А. Научно-обоснованный подход к классификации угроз информационной безопасности. Научно-технический журнал №1 (87) 2015, с. 132-140. URL: http://library.oreluniver.ru/polnotekst/-IzvestiyaOrelGTU/ISiT_2015_1.pdf#page=132

9. Ромашкина, Н. Проблема международной информационной безопасности в ООН (История, спорные вопросы, перспективы) [Электронный ресурс] / Мировая экономика и международные отношения, 2020, том 64, № 12, с. 25-32.

– URL: https://www.researchgate.net/profile/Nataliya-omashkina / publication/347874036_Problem_of_International_Information_Security_in_the_UN/links/602a9636299bf1cc26cb4f03/Problem-of-International-Information-Security-in-the-UN.pdf

Nuraddin Mehdiyev
PhD candidate, The Academy of Public Administration under the President of the Republic of Azerbaijan
nuraddin_mehdiyev@yahoo.com

INFORMATION SECURITY AS A FACTOR OF NATIONAL SECURITY

SUMMARY

The significance of information security as a factor of national security cannot be overstated in today's interconnected world. This critical nexus encompasses various dimensions, including cybersecurity, economic implications, diplomatic ramifications, and military operations. Information security is not just a technical issue but a fundamental aspect of national security strategy, requiring comprehensive approaches that encompass technological innovations, diplomatic initiatives, and international cooperation. In navigating the complexities of the information age, nations must prioritize the protection of their digital assets to safeguard their sovereignty, stability, and strategic interests on the global stage.

Keywords: *Information security, national security, cyber security, international cooperation, information age.*

Нураддин Мехтиев
Диссертант Академии Государственного Управления при Президенте Азербайджанской Республики
nuraddin_mehdiyev@yahoo.com

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

РЕЗЮМЕ

Значение информационной безопасности как фактора национальной безопасности невозможно не переоценить в современном взаимосвязанном мире. Эта важнейшая взаимосвязь охватывает различные аспекты, включая кибербезопасность, экономические последствия, дипломатические последствия и военные операции. Информационная безопасность — это не просто технический вопрос, а фундаментальный аспект стратегии национальной безопасности, требующий комплексных подходов, охватывающих технологические инновации, дипломатические инициативы и международное сотрудничество. Преодолевая сложности информационного века, страны должны уделять приоритетное внимание защите своих цифровых активов, чтобы защитить свой суверенитет, стабильность и стратегические интересы на глобальной арене.

Ключевые слова: *Информационная безопасность, национальная безопасность, кибербезопасность, международное сотрудничество, информационный век.*