ISSN 2521-1331

Azərbaycan Respublikası Müdafiə Nazirliyi Milli Müdafiə Universiteti

REPUBLIC OF AZERBAIJAN
MINISTRY OF DEFENCE
NATIONAL DEFENCE UNIVERSITY

MİLLİ TƏHLÜKƏSİZLİK VƏ HƏRBİ ELMLƏR

Elmi-praktik jurnal

NATIONAL SECURITY AND MILITARY SCIENCES

Scientific-practical journal

№ 2(10)/2024

ISSN 2521-1331

Azərbaycan Respublikası Müdafiə Nazirliyi
Milli Müdafiə Universiteti

MİLLİ TƏHLÜKƏSİZLİK VƏ HƏRBİ ELMLƏR

Elmi-praktik jurnal

Cild 10, №2, 2024

Ministry of Defence of the Republic of Azerbaijan
National Defence University

NATIONAL SECURITY AND MILITARY SCIENCES

Scientific-practical journal

Volume 10, №2, 2024

"Milli təhlükəsizlik və hərbi elmlər" jurnalında verilmiş materiallardan istifadə zamanı mütləq jurnala istinad edilməlidir.

Jurnal 09.07.2015-ci il tarixində Azərbaycan Respublikası Ədliyyə Nazirliyində qeydə alınıb. Qeydiyyat nömrəsi: 3991.

"Milli təhlükəsizlik və hərbi elmlər" jurnalı elmi tədqiqatların əsas müddəalarının nəşr edilməsi üçün Azərbaycan Respublikası Prezidenti yanında Ali Attestasiya Komissiyası tərəfindən tövsiyə olunan nəşrlər siyahısına daxil edilmişdir.

Təsisçi: Milli Müdafiə Universiteti
www.mmu.edu.az
AZ1065, Azərbaycan Respublikası, Bakı şəhəri, Yasamal rayonu, "Qırmızı Şərq" hərbi şəhərciyi, Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu.
mmu-heti@mod.gov.az

While using any kind of material given in "National security and military science" you should refer to the journal.

The journal was registered on 09.07.2015 in the Ministry of Justice of the Republic of Azerbaijan. Registration Number: 3991.

"National security and military sciences" journal has been included in the list of recommended publications by Higher Attestation Commission under the President of the Republic of Azerbaijan for the publication of main theses of scientific researches.

Founder: National Defence University
www.mmu.edu.az
AZ1065, Republic of Azerbaijan, Baku, Yasamal district, "Girmizi Sherg" military settlement, National Defence University, Military Scientific Research Institute.
mmu-heti@mod.gov.az

Editorial board members

International editorial board members

MÜNDƏRİCAT

CONTENTS

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 9-21
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 355/359 DOI: 10.30546/9878.2024.2.10.009.

GƏLƏCƏK MÜHARİBƏLƏRİN XARAKTERİ

m.t.h.e.ü.f.d., professor Heydər Piriyev
Milli Müdafiə Universiteti

m.t.h.e.ü.f.d., dosent, general-mayor Arif Həsənov
https://orcid.org/0000-0002-8814-1590
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
arif.h.hasanov@gmail.com

m.t.h.e.ü.f.d., polkovnik Rəşad Tahirov
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
rashad_tahirov1975@yahoo.com

Xülasə. Bugünün hərbi-siyasi reallıqları ölkənin milli təhlükəsizliyini təmin etmək məqsədilə Silahlı Qüvvələrin hər an gələcəkdə baş verə biləcək müharibələrə hazır olmasını tələb edir. Çünki keçmişdə olduğu kimi, hərbi qarşıdurmalara səbəb olan təbii sərvətlər uğrunda mübarizə, dövlətlərarası rəqabət, hegemonluq istəyi, həmçinin ideoloji fərqlər və təhlükəsizlik qayğıları gələcəkdə də davam edəcək. Bununla yanaşı, texnologiya sahəsində əldə edilən və gözlənilən sürətli inkişaf ənənəvi döyüş forma və üsullarını əhəmiyyətli dərəcədə dəyişmişdir. Belə ki, gələcək müharibələrdə hadisələr, o cümlədən döyüş fəaliyyətləri daha sürətlə cərəyan edəcək, məlumat mübadiləsi vəziyyəti tez-tez dəyişəcək, zərbələr qısamüddətli, lakin dəqiq və dağıdıcı olacaqdır. Əvvəlki müharibələrdə hərbi əməliyyatların məqsədlərinə nail olmaqda əsas rol oynayan, düşmənlə bilavasitə təmas tələb edən hücum və müdafiə kimi ənənəvi döyüş növləri əhəmiyyətini itirəcək, döyüşün yeni üsul və formaları yaranacaqdır. Bu forma və üsulların Silahlı Qüvvələrdə öyrənilməsi və məharətlə tətbiqi gələcək müharibələrdə uğur qazanmağın əsas şərtlərindən biri olacaqdır. Gələcək müharibələrin xarakterinin öyrənilməsi, hərbi əməliyyatların üsul və formalarının proqnozlaşdırılması üçün məqalədə elmi-texniki sahədə baş verən və gözlənilən dəyişikliklər təhlil edilərək, onların hərb işinə təsiri araşdırılır. Bundan başqa, məqalənin əvvəlində müharibənin xarakterini daha yaxşı anlamaq məqsədilə onun səbəbləri nəzərdən keçirilir.

Açar sözlər*:* müharibə, siyasi, sülh, münaqişə, ziddiyyət, strategiya, hibrid

Giriş

Müharibə haqqında ilk məlumat təxminən 5000 il bundan əvvəl qeydə alınmışdır və bu günə qədər bəşər tarixinin bir hissəsi olaraq qalmaqdadır. Tarixi hadisələr göstərir ki, heç bir nəsil və ölkə müharibə təhlükəsindən sığortalanmayıb və bu təhlükə dünyanın ən aktual problemlərindən biridir. Ümumilikdə müharibə insanların dincliyini pozan, həyat səviyyəsini aşağı salan və cəmiyyətdə köklü dəyişikliklərə səbəb olan neqativ fenomendir. Çünki müharibələr döyüş, silahlanma, ölüm, əzab-əziyyət və dağıntılar deməkdir. Bununla belə bəzi tədqiqatçılar tərəfindən müharibələrin ölkənin inkişafında müsbət rol oynadığı da qeyd edilir. Belə ki, müharibələr yeni texnologiyaların inkişafını sürətləndirərək, iqtisadi artımı və yeni iş yerlərinin açılmasını stimullaşdırır. Məsələn, İkinci Dünya müharibəsindən sonra ağır sənayedə çalışan həm qadın, həm də əcnəbi vətəndaşların sayı əhəmiyyətli dərəcədə artmışdır. Müharibə ölkənin vətəndaşlarını ümumi düşmənə qarşı birləşdirərək, milli özünüdərkə və oyanışa səbəb olur. Bundan başqa, hərbi əməliyyatlarda silahlı qüvvələr müəyyən döyüş təcrübəsi əldə edir. Lakin müharibənin mənfi cəhətləri və ölkələrə vurduğu ziyan daha çoxdur və bu səbəbdən arzuolunmazdır.

Müharibələr müasir dünyada arzuolunmaz olsa da, beynəlxalq münasibətlər sistemində meydana gələn qarşıdurmaların həll edilməsində hərbi gücün istifadəsi vacib rol oynayır. Beynəlxalq hüquq normalarına baxmayaraq, bəzi dövlətlər müxtəlif bəhanələr gətirərək, başqa dövlətin ərazi bütövlüyü və siyasi müstəqilliyi əleyhinə güc tətbiq etməkdən çəkinmirlər. Fikrimizcə, bu tendensiya gələcəkdə də

davam edəcək. Beləliklə, ölkənin indiki və gələcək dünyada müstəqil bir subyekt kimi mövcudluğu, ərazi bütövlüyünün və maraqlarının mümkün təhlükələrdən qoruya bilməsi böyük ölçüdə silahlı münaqişələrə hazır olmasından asılıdır. Bu isə həm keçmişdə, həm də hazırda cərəyan edən müharibələrin təhlil edilərək, gələcək hərbi əməliyyatların forma və üsullarının proqnozlaşdırılmasını şərtləndirir.

Müharibələrin təhlili və proqnozlaşdırılmasında inkişaf etmiş dövlətlərin təcrübəsinin, hərbi əməliyyatlarda əldə etdikləri uğurların, habelə uğursuzluqların səbəblərinin öyrənilməsi vacibdir. Bununla belə keçmiş təcrübələrin dərindən təhlil edilmədən birəbir təqlidi eyni səhvlərin təkrarlanması, yaxud məğlubiyyət ilə nəticələnir. İkinci Dünya müharibəsində silah və texnika baxımdan güclü olan Fransanın qısa müddətdə Almaniya qarşısında məğlubiyyətə uğramasının səbəbi, məhz hərbi doktrinalarında texniki yeniliklərin nəzərə alınmaması və Birinci Dünya müharibəsinin döyüş forma, üsul və qaydalarına bağlı qalmasıdır [1]. 44 günlük Vətən müharibəsi ərəfəsində Ermənistanın siyasi və hərbi rəhbərləri də oxşar səhvə yol verdilər. Bunları nəzərə alaraq hesab edirik ki, dövrün elmi-texniki tərəqqisi ilə sıx bağlı olan döyüşün yeni forma və üsullarının effektiv tətbiqi müharibədə uğur əldə etmənin ən əsas şərtlərindəndir. Məhz bu səbəbdən döyüşün yeni forma və üsullarının öyrənilməsi və gələcək müharibələrin xüsusiyyətlərinin proqnozlaşdırılması hərb elmində ən aktual problemdir.

Qeyd edildiyi kimi, elm və texnologiyanın inkişafı müharibələrin xarakterinə böyük ölçüdə təsir edir. Məsələn, barıtın ixtirası nəticəsində meydana gələn top, tüfəng, tapança, avtomat və pulemyot kimi odlu silahlar hərb işində inqilaba səbəb olmuş, müharibənin, eləcə də döyüşün forma və üsullarını əhəmiyyətli dərəcədə dəyişmişdir [2]. Oxşar qaydada buxar maşınlarının və daxili yanma mühərriklərinin kəşfi sayəsində meydana gələn qatar, tank, təyyarə və yeni növ gəmilər müharibənin sürət və dərinliyini artırmaqla yanaşı, əhatə dairəsini də genişlədirdi. Nüvə fizikasının inkişafı, nüvə energetikasının yaranmasına təkan verməklə, böyük dağıdıcı qüvvəyə malik olan və bununla da müharibənin yeni qanun və prinsiplərini ortaya qoyan nüvə silahının kəşfinə apardı. Qeyri-səlis məntiq nəzəriyyəsi mürəkkəb və qarışıq mühitdə qərar qəbuletmə imkanına malik, həmçinin müxtəlif əməliyyatları insan müdaxiləsi olmadan yerinə yetirən süni zəkanın inkişafına təkan verdi. Nəticədə yarıavtonom idarəedilən silah sistemləri meydana gəldi. Bu istiqamətdə davam edən araşdırma və aparılan sınaqlar avtonom idarəedilən silah və texnikaların yaxın gələcəkdə döyüşlərdə tətbiq olunacağını göstərir.

Beləliklə, elmi-texniki tərəqqi istisnasız olaraq, insan fəaliyyətinin bütün sahələri kimi, müharibənin də üsul və formalarının inkişafına nəzərəçarpan təsir göstərir. Gələcəkdə də hərbi əməliyyatların məzmun və tipologiyası, strategiya və taktikası, silahlı birləşmələrin tətbiqinin forma və üsulları elmi-texniki tərəqqinin, əsasən, süni zəka, biotexnologiya, nanotexnologiya kimi sahələrdə baş verən sürətli inkişafın təsiri altında formalaşacaqdır.

Müharibənin səbəbləri

Təhlillər bəşər tarixinin sadəcə 8 faizində sülh dövrü olduğunu göstərmişdir [3]. Bununla belə, müharibənin, yaxud silahlı münaqişənin başlanma səbəbləri müxtəlif vaxtlarda fərqli olmuşdur. Bəzi tədqiqatçılar iddia edir ki, müharibə iqtisadi, dini və siyasi səbəblərə görə yaranır. Digərləri isə günümüzdə əksər müharibələrin ideoloji səbəblərə görə aparıldığını düşünürlər. Ümumi olaraq, müharibələrin başlanma səbəbləri iki yanaşma altında qruplaşdırılır: ənənəvi və müasir nəzəriyyələr [4]. Ənənəvi nəzəriyyəyə görə müharibənin başlanma səbəbi müxtəlif millətlər, dövlətlər, cəmiyyətlər, həmçinin etnik və dini qruplar arasında mövcud olan sosial və iqtisadi tarazlığın pozulmasıdır. Tarazlığın pozulması nəticəsində meydana gələn qarşıdurma isə dövlətləri şiddət tətbiq etməyə aparır. Bu nəzəriyyənin tərəfdarları hesab edirlər ki, müharibə insanın təbiətinə xas olan şiddətin təzahürüdür. Bunlardan XVII əsrdə yaşamış böyük filosof Tomas Hobzun "Leviathan" əsərinə görə, ehtiyacları və maraqları naminə, həmçinin həmin maraqlara təhlükə yarandıqda insan şiddət tətbiq etməyə meyillidir [5]. Dövlət və sosial qruplar müəyyən ərazidə oxşar ehtiyac və maraqlara sahib olan insanlardan formalaşdığı üçün onların istəklərini həyata keçirən bir vasitədirlər. Bu səbəbdən bir dövlət və ya ayrı sosial qrup ehtiyaclarının qarşılanmasına, yaxud maraqlarının həyata keçirilməsinə mane və təhlükə

hesab etdiyi digər dövlət, siyasi, dini, etnik ünsürlərə qarşı şiddət tətbiq etməyə meyillidir. Bu şiddət, artan ehtiyacların qarşılanması, yaxud maraqlarının müdafiəsi üçün qabaqlayıcı və zorakı tədbirlərin görülməsini nəzərdə tutur. Gələcəkdə də müxtəlif səbəblərə görə maraqların toqquşması davam edəcəyi və yeni müharibələrin olacağı proqnozlaşdırılır. Ənənəvi nəzəriyyənin nümayəndələrindən biri olan Yakov Novikovaya görə, bir çox hallarda fərqli etnik, ideoloji və dini qruplar arasında silahlı qarşıdurmalar və müharibələr cəmiyyətdə ətalət qüvvəsi yaradan tarixi səbəblərə görə davam edir və təkrarlanır [4].

Müasir yanaşmaya görə müharibənin meydana gəlməsinin səbəbi subyektlər (dövlət, etnik, dini qruplar və s.) arasında mövcud olan ziddiyyətlərin irrasional (məntiqə sığmayan) yolla həll edilməsidir. Bu yanaşmaya görə ziddiyyətlər hər zaman mövcud olub, lakin bunların çözülməsi və sülhün əldə edilməsi üçün rasional yollar mövcud olduğu halda, bəzən qərarlar emosiya, yaxud instinktə əsaslanaraq qəbul edilir. Məsələn, 44 günlük Vətən müharibəsində məğlub olan və ordusu darmadağın edilən Ermənistanda müharibədən sonra revanşizm hərəkətlərinin baş qaldırması və Azərbaycanla sülh müqaviləsinin bağlamasından boyun qaçırması irrasional və təhlükəli davranışdır. Çünki növbəti dəfə Azərbaycan və Ermənistan arasında müharibə olacağı təqdirdə, sonuncunun çox ağır məğlubiyyətə uğradılaraq, varlığına son qoyulacağına dair fikirlər dünyanın aparıcı hərbi ekspertləri tərəfindən dəfələrlə səsləndirilmişdir. Müharibədən sonra Azərbaycanın Qarabağda apardığı uğurlu antiterror əməliyyatları bunun sübutudur. Ermənistanın rasional davranaraq Azərbaycanla sülh müqaviləsini imzalaması ona regional və beynəlxalq layihələrə qoşulmağa və əlavə gəlir əldə etməyə imkan verəcək. Bu səbəbdən Ermənistanda baş qaldıran revanşizm hərəkətləri başa düşülən (məntiqə sığan) deyil. Müasir yanaşmanın nümayəndələri hesab edirlər ki, geosiyasi ambisiyalar, ölkə daxilində şovinist qüvvələrin təsiri, danışıqlarda və daxili siyasətdə uğursuzluq, böyük dövlətlərin təsir dairəsini genişləndirmək arzusu irrasional düşünmənin və müasir müharibələrin əsas səbəblərindəndir [6].

Yuxarıda göstərilən hər iki səbəb birbaşa insan amili, onun təbiəti, həmçinin fəaliyyətinin nəticəsi ilə bağlıdır. Fikrimizcə, gələcəkdə gözlənilən elmi-texniki inqilab, əsasən, süni zəkanın bir çox sahələrdə insanı əvəz etməsi nəticəsində ölkələrarası müharibə, yaxud silahlı münaqişə üçün səbəb insan iradəsi olmadan da yaranacaqdır. Məsələn, hər hansı bir ölkədə strateji müdafiə sistemlərinə inteqrasiya edilmiş süni zəka tərəfindən digər ölkənin fəaliyyətlərinin səhvən real təhdid kimi qiymətləndirilməsi və qabaqlayıcı zərbə endirmək üçün qərar qəbul etməsi mümkün olan ssenaridir.

Beləliklə, həm ənənəvi, həm də müasir yanaşmaların təhlili göstərir ki, beynəlxalq aləmdə mövcud olan ziddiyyətlərin həll edilməsində şiddətin, o cümlədən hərbi gücün tətbiqi əsas vasitələrdən biri olaraq qalmaqdadır. Fikrimizcə, gələcəkdə iqtisadi, ideoloji ilə müqayisədə etnik zəmində müharibələrin sayında artım olacaqdır. Günümüzdə amerikalı sosioloq və politoloq Samuel Filips Hantinqton "Sivilizasiyaların toqquşması" kitabında qeyd etmişdir ki, fərqli sivilizasiya məxsus millət və qruplar var olduqca, dünyada qarşıdurmalar qaçılmazdır və bu da, öz növbəsində yeni müharibələrin yaranmasına gətirib çıxaracaq [7].

Qeyd edildiyi kimi, bəşər tarixində ictimai quruluşun təkamülü ilə birlikdə müharibənin xüsusiyyətləri də daimi dəyişir. Müharibənin xüsusiyyətləri dedikdə, əsasən, onun başlama səbəbi, gedişi və sonu başa düşülür. Bütün bunlar ölkədaxili və ölkəxarici siyasət, sosial və beynəlxalq münasibətlər sistemi, silah və texnikanın yeni növlərindən asılı olaraq inkişaf edir. İnkişaf nəticəsində dövlətlərarası mübarizənin, o cümlədən döyüşün yeni üsul və formaları meydana gəlir.

Hazırda bio, nano, material, süni zəka və informasiya sahəsində baş verən texnoloji inqilablar bir tərəfdən insanın həyat və sağlamlığına, iş şəraitinin keyfiyyətinə təsir göstərməklə müsbət dəyişikliklərə səbəb olmuş, digər tərəfdən isə dövlətlərarası və ölkə daxilində imkanların qeyri-bərabər paylanması və gərginliyin artması ilə nəticələnmişdir. Gərginliyin artması isə bir çox hallarda yeni silahlı münaqişə və müharibələrin yaranmasına səbəb olur. Günümüzdə baş verən bu silahlı münaqişələrin aparılmasında yeni tendensiyalar müşahidə olunur. Bu tendensiyalar baş verən sürətli inkişafın təsiri olaraq, döyüşlərdə süni zəka, informasiya texnologiyalarına əsaslanmış yeni silah və texnikaların geniş tətbiqi ilə əlaqədardır. Fikrimizcə, məhz bu silah və texnikaların geniş tətbiq edilməsi gələcək müharibələrin xarakterini müəyyən edərək, döyüşün forma və üsullarını əvvəlkilərdən fərqləndirəcəkdir.

Gələcək müharibələrin xüsusiyyətləri

Karl Fon Klauzevitsə görə, müharibənin xüsusiyyətləri buqələmun kimi şərait və zamandan asılı olaraq dəyişir [8]. Xüsusiyyətlər altında, o müharibənin paradoksal üçlüyünü nəzərdə tuturdu: ehtiras, yaradıcılıq və siyasət [9]. Ehtiras müharibənin ilkin elementi olaraq insan təbiətinə xas olan nifrət, kin, ədavət və zorakılıq kimi reaksiyaları və düşmənçilik fəaliyyətlərini ehtiva edir. Yaradıcılıq hərb sənəti, ordunun fəaliyyəti, əsasən, müharibənin qeyri-müəyyən və qarışıq mühitində komandirlərin məharət və bacarığı, döyüşün üsul və formaları ilə bağlıdır. Üçüncü isə müharibəni siyasətin vasitəsinə çevirən hökumətin qəbul etdiyi rasional qərarlardır [10]. İctimai-siyasi həyatda, mədəniyyətlərdə baş verən dəyişikliklər, həmçinin elmi-texnoloji tərəqqi yuxarıda qeyd olunan üçlüyün hər birinə yeni formalar verir. Bunun nəticəsində müharibənin başladılması, aparılması və bitirilməsinin yeni şəkil və üsulları ortaya çıxır. Cəmiyyətin sosial strukturunda, həmçinin siyasi və beynəlxalq münasibətlər sistemində baş verən dəyişikliklər, əsasən, üçlüyün birinci və üçüncü elementlərinə təsir edirsə, elmi-texnoloji tərəqqi ikinci elementə aid döyüşün üsul və formalarını əhəmiyyətli dərəcədə dəyişir.

Döyüşün üsul və formaları hər zaman müharibənin məqsədlərinə nail olunmasında əsas rol oynamışdır. Bu üsul və formaların asılı olduqları ən böyük amil silah və texnika olmuşdur. İndiki dövrdə də bu asılılıq dəyişməz olaraq qalır. Sadəcə əgər əvvəlki müharibələrdə ənənəvi silahların təsiri sadəcə kinetik, kimyəvi və istilik enerjinin [11] gücü ilə ölçülürdüsə, gələcəkdə uzaqdan yüksək dəqiqliklə hədəfləri vurma və avtonom çalışma imkanları ilə ölçüləcəkdir. Bu silahlar yüksək informasiya-kommunikasiya texnologiyaları, süni zəka, nanohissəciklər və zərrəciklər fizikası kimi fundamental və tətbiqi elmlərin son nailiyyətlərinə əsaslanaraq, müharibənin şəkli, döyüşlərin üsul və formalarında köklü dəyişikliklərə səbəb olacaqdır.

Son onilliklərdə yeni materialların istehsalı, informasiya, rabitə və biotexnologiya sahələrinin inkişafında böyük irəliləyiş müşahidə olunur. Bu irəliləyiş yeni silah növlərinin, hərbi və xüsusi texnikanın istehsalına gətirib çıxarmışdır. Hazırda informasiya, süni zəka və digər qabaqcıl texnologiyalara əsaslanan yüksək dəqiqliyə malik silah sistemlərinin tətbiqi, onların pilotsuz uçuş aparatlarına və məsafədən idarəedilən digər vasitələrə quraşdırılması döyüşlərin xarakterini xeyli dəyişdirmişdir. Bu dəyişikliklər "hərbi sənətində inqilab" adlanan yeniliklər gətirdi. "Hərb sənətində inqilab" müharibənin strateji, əməliyyat və taktiki səviyyələri, hərbi gücdən istifadənin mahiyyəti, məqsədləri, imkanları və hədləri, həmçinin döyüşün üsul və formaları haqqında yeni mütərəqqi fikirlərin formalaşması ilə bağlıdır. Əslində "hərb sənətində inqilab" yeni anlayış deyil. Yuxarıda qeyd edildiyi kimi, tarixboyu hərbi texnika və silah inkişaf etdikcə döyüşün üsul və formaları da tədricən dəyişmişdir. Dəyişikliklər əvvəlkilərdən fərqlənirsə, onu tətbiq edən tərəfə böyük üstünlük və qəti qələbə qazandırırsa, həmçinin mühüm siyasi və tarixi nəticələrə nail olunarsa, sözükeçən inqilab baş verir. XXI əsrdə bəşəriyyət XV–XVII əsrlərdə odlu silahların kütləvi tətbiqi ilə hərb sənətində baş verən dəyişikliklərlə müqayisə edilə bilən yeni bir inqilabının astanasına yaxınlaşdı [12]. Uzun illərdir hərbi əməliyyatların məqsədlərinə nail olunmasında əsas rol oynayan və düşmənlə bilavasitə təmas tələb edən hücum, müdafiə kimi ənənəvi döyüş növləri arxa plana keçir. Yeni şəraitdə üstünlük qüvvə və vasitələrin həlledici istiqamətdə cəmləşdirilməsi ilə deyil uzaqdan, düşmənlə yaxın təmasa girmədən dəqiq və sarsıdıcı zərbələrlə əldə edilir. Müasir müharibələr uzaq məsafədən, birbaşa təmasa girmədən düşmən qüvvələrini böyük itkiyə məruz qoymaq və texnikasını sıradan çıxarmaqla onların məhv edilməsinin mümkünlüyünü göstərdi. Bundan başqa, süni zəkanın, yüksək texnologiyaların sürətlə inkişafı və onların əhatə dairəsinin daha da genişlənməsi, gələcəkdə daha üstün imkanlara malik, avtonom idarəedilən silah sistemlərinin və xüsusi texnikaların yaradılmasına yol açır. Texnika və texnologiyaların inkişafını proqnozlaşdıran və onların müharibələrin gedişinə təsirini öyrənən aparıcı alimlər hesab edirlər ki, XXI əsrin ortasınadək döyüşlərin görünüşü aşağıda göstərilən sahələrdə meydana gələcək yeni kəşf və ixtiraların təsiri altında şəkillənəcəkdir:

– ***yüksək enerji fizikası:*** zərrəciklər fizikası kimi tanınan, maddəni və şüalanmanı təşkil edən hissəciklərin təbiətini öyrənən fizika bölməsidir [13]. Yüksək enerji fizikası dünyada ən sürətlə inkişaf edən tədqiqat sahələrindəndir və aparıcı dövlətlərin elmi araşdırmalarında mühüm yer tutur. Hesab edirik ki, bu sahədə baş verən texnoloji inkişaf nəticəsində fiziki prinsiplərin istifadəsinə əsaslanan silahlar

təkmilləşəcək, yaxud yeni növləri yaranacaqdır. Bunlar istiqamətləndirilmiş enerji (lazer) silahı, həmçinin yüksəktezlikli və radiodalğalı, elektromaqnit, geofiziki və infrasəs silahlarıdır. Bu silahların ümumi xüsusiyyətləri gizli və qəfil tətbiq edilməsi, elektron sistemləri ani sıradan çıxartmaq imkanının olması və adi silahlardan istifadə etmədən canlı qüvvəni tələfata uğratmasıdır. Hal-hazırda inkişaf etmiş ölkələrdə sözügedən silahların imkanlarının artırılması üzrə işlər davam etdirilir. İstiqamətləndirilmiş enerji (lazer) silahının yeni növlərinin yaradılması və onların effektivliyinin artırılması bu sahədə aparılan ən uğurlu işlərdəndir. Əldə edilən uğurlar bu istiqamətdə aparılan çoxsaylı tədqiqat və yeni texnikaların meydana çıxması ilə əlaqədardır. Bu günə qədər aparıcı ölkələr müxtəlif məqsədlər üçün istiqamətləndirilmiş enerji (lazer) silahlarını hazırlamağa və sınaqdan keçirməyə nail olublar. ABŞ Ordusu 2022-ci ildə yüksəkgüclü lazer silahının prototipinin yaradıldığını və yaxın illərdə onu silahlanmaya qəbul ediləcəyini bildirmişdir [14]. Bu silahın ən böyük üstünlüyü enerjini işıq sürəti ilə ötürərək, hədəfi anında məhv etməsidir. İstiqamətləndirilmiş enerji sayəsində hədəfi vurma dəqiqliyi çox yüksəkdir, həmçinin bu silah atəş vaxtı adi silahlardan fərqli olaraq, səs çıxarmır və geri çəkilmir. Bundan başqa, enerjinin gücünü tənzimləmə mümkünlüyü silahın məsafə ölçmək, hədəfi sıradan çıxarmaq və məhv etmək kimi müxtəlif məqsədlər üçün istifadəsinə imkan verir. Demək olar ki, bu silahlar qeyri-məhdud atəş gücünə malikdir, çünki mümkün atışların sayı yalnız enerji mənbəyinin xüsusiyyətlərindən asılıdır [15]. Hazırda mövcud silahlarda çatışmazlıqların aradan qaldırılması və təkmilləşdirmə işlərinin sürətlə davam etdirilməsi, onların effektivliyini xeyli artıracaqdır. Yaxın gələcəkdə təkmilləşdirilmiş lazer silahı ilə uzaq məsafədən döyüş təyyarələrinin, pilotsuz uçuş aparatlarının, peyklərin və raketlərin vurulması nəzərdə tutulur.

– ***süni zəka.*** Süni zəka, adətən, insan zəkasını tələb edən vizual qavrayış, nitqin tanınması, qərar qəbuletmə və dillər arasında tərcümə kimi vəzifələri yerinə yetirə bilən kompüter sistemlərinin inkişafı kimi müəyyən edilir [16]. Son illərdə süni zəka (AI) sahəsində böyük irəliləyişlər əldə edilmişdir. Bu sahədə əldə edilən son nailiyyətlər əvvəllər elmi fantastika kimi görünənləri həyata keçirməyə imkan verir. Belə ki, süni zəka əsasında çalışan kompüter, robot və digər texnikalar anlıq olaraq irihəcmli informasiyanı emal edir və qərar qəbul edir. Artıq insan müdaxiləsi olmadan süni zəka sayəsində avtonom idarəedilən müxtəlif təyinatlı sistemlərin nümunələri yaradılmış və sınanmışdır. Bununla belə müasir süni zəka ilə insanaməxsus düşünmə, dərketmə, izahetmə və problemi qoymaq kimi fəaliyyətlər hələlik mümkün deyil. Lakin hesab edirik ki, alqoritmlər üzərində aparılan təkmilləşdirmə işləri gələcəkdə süni zəkanın imkanlarını daha da artıracaqdır.

Bütün elmi-texnoloji nailiyyətlərin hərb işində geniş tətbiq olunduğunu nəzərə alsaq, süni zəkanın da silah və silah sistemlərinə inteqrasiyası baş verəcəkdir. Son illər qabaqcıl ordular süni zəka əsasında çalışan "ağıllı" silah sistemlərinin işlənməsinə, inkişafına və tətbiqinə xüsusi diqqət yetirirlər. Aydındır ki, gələcəkdə silahlı qüvvələrin döyüş potensialı, məhz "ağıllı" silah sistemlərin imkanları ilə müəyyən ediləcəkdir. Komanda mərkəzi ilə sinxron çalışacaq "ağıllı" silah sistemləri gələcək döyüşlərin əsas elementi olaraq, müharibənin bütün mərhələlərində mühüm rol oynayacaqdır. Belə ki, "ağıllı" silah sistemləri hərbi əməliyyatların bütün dərinliklərində şəraiti qiymətləndirərək, hədəfin növünə görə müstəqil effektiv zərbə endirmək qabiliyyətinə malik olacaqdır. Belə ki, mürəkkəb alqoritmlər sayəsində süni zəka insan müdaxiləsi olmadan növlərinə, koordinatlarına və məhvetmə ardıcıllığına görə hədəflərə zərbə endirmək üçün uyğun çevik qərar qəbul edəcəkdir. Süni zəka ilə müqayisədə bu fəaliyyət komanda mərkəzində ən peşəkar insanlar tərəfindən belə icra edildikdə daha çox vaxt alacaqdır. Halbuki şəraitin sürətlə dəyişdiyi müasir və gələcək müharibələrdə zaman faktoru atəşlə zərərvurmada çox vacibdir. Məhz bu səbəbdən "ağıllı" silah sistemlərinə malik olan ordular artıq müharibənin əvvəlində üstünlük əldə edəcəklər.

Sözügedən silah sistemləri hal-hazırda işlənib-hazırlanma mərhələsindədir, lakin onların yarı avtonom nümunələri artıq silahlanmadadır. Süni zəka ilə çalışan silah sistemlərinin daha da təkmilləşdirilməsi, avtonom döyüşən robototexnikaların yaradılması, həmin silah sistemlərində yüksək dəqiqliyə malik sursatların istifadə edilməsi həm canlı qüvvə arasında itkini minimuma endirəcək, həm də hədəfləri uzaq məsafədən məhv etməyə imkan verəcəkdir. Belə ki, süni zəka ilə idarəedilən silah sistemləri, o cümlədən hərbi robototexnika avtonom olaraq ərazi, üz və hədəftanıma, koordinat

müəyyənetmə, şəraiti təhlil etmək və qərar qəbuletmə, atəşaçma kimi imkanlara malik olacağından, döyüş meydanında canlı qüvvənin birbaşa tətbiqini böyük ölçüdə azaldacaqdır. ABŞ-ın müdafiə departamentinin mütəxəssislərinə görə, süni zəka silahlı münaqişələrin prinsiplərini bütövlüklə dəyişdirməklə, hərb sənətində barıt və nüvə silahından sonra üçüncü inqilaba səbəb olacaqdır [17]. Lakin onu da qeyd etmək istəyirik ki, süni zəka onun istifadəçilərinə müəyyən problem yaradacaqdır. Bunlar düşmən tərəfindən süni zəkaya müdaxilə edilərək, silahı öz istifadəçisinə qarşı yönəldilməsi, döyüş meydanında düşmən və dost qüvvələrin qarışdırılması, mülki əhali və obyektlərə zərbələr endirilməsi kimi problemlərdir. Gələcək müharibələrdə müvəffəqiyyət əldə etmək üçün silah və texnikada süni zəkanın istifadəsinin səbəb olduğu bu kimi problemlərin həlli mütləqdir.

– ***nanotexnologiya.*** Əslində nanotexnologiya bio və material mühəndisliyi sahəsində əldə edilən böyük inkişafın nəticəsi olaraq yaranmışdır. Bu texnologiya maddə, yaxud maddələr birləşməsinə molekul və ya atom miqyasında müdaxilə edilərək, yeni struktur, cihaz və sistemlərin dizayn edilməsi, yaradılması və istifadəsi ilə məşğul olan elm sahəsi ilə əlaqəlidir [18]. Nanotexnologiya müxtəlif funksiyalara malik kiçik, miniatür cihazların hazırlanmasına və onların bir sistem şəklində istifadə edilməsinə şərait yaradır. Hesab edirik ki, nanotexnologiya əsasında hazırlanmış hərbi təchizat, silah və texnika gələcəkdə geniş şəkildə tətbiq ediləcəkdir. Bu texnologiya sahəsində əldə edilən və gözlənilən böyük inkişaf kiçikölçülü hərbi təyinatlı robotların, dronların, müşahidə cihazlarının, həmçinin yüngül, lakin çoxfunksiyalı geyim və təchizatların, zirehli gödəkcələrin və maskalanma vasitələrinin kütləvi şəkildə istehsalına və tətbiqinə imkan verir. Bundan başqa, artıq nanotexnologiyaların inkişafı nəticəsində müasir elektronikanın aktiv komponentlərinin ölçüləri əhəmiyyətli dərəcədə kiçilmişdir. Həmin komponentlərin ölçüləri 0,1 mikrona qədər və ya daha az kiçilməklə yanaşı, onların yaddaş tutumu 10^{12} bitdən çox artmışdır [19]. Nanotexnologiya sahəsində sürətli inkişaf bu göstəricilərin yaxın gələcəkdə daha da təkmilləşəcəyini göstərir. Bu sahədə əldə edilən uğurların informasiya-kommunikasiya texnologiyalarında geniş tətbiqi göstərir ki, növbəti iki onillikdə əməli yaddaş qurğularının ölçüləri kiçilməklə yanaşı, onların informasiya emal (oxuma, yazma və ötürmə) sürətli təxminən dörd dəfə artacaq, maya dəyəri isə xeyli azalacaqdır. Bu nailiyyətlərin nəticəsi olaraq, süni zəka ilə çalışan müxtəlif, o cümlədən hərbi təyinatlı kiçikölçülü texnika, robot kimi pilotsuz aparatların kütləvi istehsalı və istifadəsi başlayacaqdır. Çünki orduya əsgərlərin həyatlarını riskə atmadan, həmçinin onların aşkar edilmədən düşməni müstəqil məhv edəcək, mina və partlamamış bombaları zərərsizləşdirəcək texnika lazımdır.

Hərbi təyinatlı mini robot və dronlara süni zəkanın inteqrasiya edilməsi onların operatorun müdaxiləsi olmadan döyüş meydanında kütləvi şəkildə istifadəsinə və avtonom zərbə endirməsinə imkan verəcək. Ölçüləri kiçik olduğundan, onları aşkar və məhv etmək çətin olacaq. Eyni zamanda mini robot və dronlar tapşırığın icrası prosesində həm müstəqil, həm də bir-biriləri ilə sıx əlaqədə fəaliyyət göstərəcək, öz aralarında hədəfləri bölüşdürmə və məhvetmə ardıcıllığını müəyyənləşdirmək imkanına malik olacaq. Fikrimizcə, gələcəkdə yüksək enerji fizikası, həmçinin "ağıllı" nanotexnologiyaların kiçik və ortaçaplı silahlara inteqrasiyanı, həmin silahların hədəfi dəqiqliklə vura bilmə imkanlarını qat-qat artıracaqdır. Məsələn, bu silah və sursatların lazer təyinedici və miniatür sensorla təchiz edilməsi planlaşdırılır ki, bu da sığınacaqlarda yerləşən canlı qüvvəni vurmağa imkan verəcək.

– ***informasiya-kommunikasiya texnologiyası.*** Günümüzdə dövlətlər arasında amansız strateji rəqabətin mövcud olduğu bir şəraitdə informasiya vacib rol oynayır. İnformasiya texnologiyalarında meydana gələn inqilabi dəyişiklər sayəsində maddi sərvət və fiziki qüvvəyə əsaslanmış güc sisteminə informasiyaya (biliyə) əsaslanan güc də əlavə olundu. Belə ki, müasir dünyada müvəffəqiyyət qazanmanın birinci şərti informasiyanın vaxtında emal edilərək, düzgün qərarın verilməsindən ibarətdir. Təhlillər göstərir ki, sözügedən texnologiyalarda inqilabi dəyişikliklər iki əsas istiqamətdə baş verir: informasiyanın emalı və informasiyanın ötürülməsi. Artıq bu gün istifadə olunan kompüterlər irihəcmli məlumatları saxlama və bir anda emaletmə imkanlarına malikdir. Gələcəkdə kvant kompüterlərin meydan gəlməsi ilə saxlanılacaq və emal ediləcək informasiyanın həcm və sürətinin indikindən qat-qat çox olacağı gözlənilir. Kvant mexanikasının qanunları əsasında işləyəcək kompüterlərdə adi kompüterlərdən fərqli olaraq, məlumatların bir-bir deyil, eyni anda birgə emalı nəzərdə tutulur. Bunun

nəticəsində emal vaxtı dəfələrlə azalacaqdır. Məsələn, hazırda istifadədə olan ən güclü kompüterdə 30-40 simvoldan ibarət ədədi sadə amillərə parçalamaq üçün milyard il lazımdırsa, kvant kompüteri ilə eyni iş 18 saniyədə yerinə yetiriləcəkdir [20]. İnformasiya texnologiyalarında inqilab irihəcmli məlumatların toplanması, saxlanılması, emalı və təhlil edilməsi üçün zəruri olan hesablama gücünün həndəsi silsilə ilə artımına səbəb olacaqdır. Bundan başqa, bu inqilab sayəsində müxtəlif formada olan gizli informasiya (mətin, audio, video və s.) dünyanın istənilən nöqtəsində, istənilən şəxsə, o cümlədən hərbi əməliyyatlarda iştirak edənlərə real vaxt rejimində ötürüləcək və deşifrə ediləcəkdir. İndiki dövrdə irihəcmli informasiyanın vahid şəbəkə üzərindən böyük məsafələrə ötürülməsi və emalında əldə edilən nailiyyətlər artıq eyni vaxtda müxtəlif əməliyyatların uzaqdan idarə edilməsinə imkan verir. İnformasiya-kommunikasiya texnologiyaları sahəsində davam edən inkişaf gələcəkdə məlumat mübadiləsinin indiki ilə müqayisədə qat-qat sürətlənəcəyini, habelə şəbəkə üzərindən daha mürəkkəb əməliyyatların qısa müddətdə icra ediləcəyini göstərir. Belə bir şəraitdə vaxtında əldə olunmuş və hərtərəfli analiz edilmiş informasiya müvəffəqiyyətin təmin edilməsində böyük rol oynayacaqdır. Bu səbəbdən hərbi əməliyyatların bütün mərhələlərində informasiya məkanına davamlı nəzarət etmək və üstünlüyü qoruyub saxlamaq gələcək müharibələrdə qələbə qazanmanın əsas şərtlərindəndir. Belə ki, informasiya məkanına hakim olan komandirlər real vaxt rejimində yaranmış vəziyyət haqqında məlumat əldə edəcəklər. Bu da onlara vəziyyəti təhlil edərək, vaxtında düzgün qərar qəbul etməyə, qüvvə və vəsaitlərin, o cümlədən yüksək dəqiqliyə malik silahların effektiv tətbiqinə imkan verəcəkdir. Bütün bunlar döyüşün ənənəvi üsul və formalarını dəyişəcəkdir.

Fikrimizcə, informasiya-kommunikasiya texnologiyalarının inkişafı hərb sənətində inqilabi dəyişikliyə səbəb olacaqdır. Yüksək texnologiyaların məhsulu olan şəbəkə, hesablama, müşahidə və "ağıllı" texnologiyaların qoşunların avtomatlaşdırılmış idarəetmə sisteminə inteqrasiyası operatorun müdaxiləsi olmadan, yaxud az müdaxiləsi ilə böyük həcmdə müxtəlif informasiyanın sürətli emalına, əməliyyat şəraitinin proqnozlaşdırılmasına, eyni vaxtda bütün səviyyələrdə döyüş sahəsinin, əməliyyat rayonlarının müşahidəsinə, həmçinin effektiv zərbə endirilməsinə imkan verəcəkdir. Hərbi təyinatlı şəbəkə texnologiyalarının inkişafı "şəbəkə əsaslı müharibə" (Network-centric warfare) anlayışını meydana gətirmişdir. Bu müharibənin konsepsiyası ilk dəfə ABŞ-ın Müdafiə Nazirliyi tərəfindən ötən əsrin 90-cı illərinin sonunda irəli sürülmüşdür və əsasını informasiya-kommunikasiya məkanında əldə edilən üstünlük sayəsində döyüşü qazanmaq fikri təşkil edir [21]. "Şəbəkə əsaslı müharibə"də kəşfiyyat, idarəetmə, naviqasiya, atəş vasitə, sistem və komplekslərinin vahid informasiya-kommunikasiya şəbəkəsinə birləşdirilərək, əməliyyat (döyüş) şəraiti haqqında etibarlı və dolğun məlumatların qəbulu və ötürülməsinin praktiki olaraq real vaxt rejimində həyata keçirilməsi, həmçinin aşkarlanan hədəflərin yüksək sürət və dəqiqliklə məhv edilərək, bölmənin döyüş gücünün artırılması nəzərdə tutulur. Döyüş gücünün effektivliyinin artması güc və vasitələrin idarə edilməsi prosesinin və döyüş tempinin sürətlənməsi, həmçinin döyüş fəaliyyətlərinin sinxronlaşdırılması nəticəsində baş verir. Böyük ərazidə real vaxt rejimində məlumatların qəbulu və ötürülməsi şəbəkə isifadəçilərinə icazə səviyyələrinə uyğun bütün dost və düşmən bölmələrinin cari fəaliyyətlərini elektron xəritədə, yaxud ekranda izləməyə və zərurət yarandıqda döyüş meydanındakı fəaliyyətlərə birbaşa müdaxilə etməyə imkan verir [22].

ABŞ-ın müdafiə nazirinin kommunikasiya və informasiya üzrə köməkçisinin yanında tədqiqatlar ofisinin direktoru David Steven Alberts "Şəbəkə əsaslı müharibə"nin aşağıda göstərilən üstünlüklərini qeyd etmişdir [23]:

1. Güclü və sürətli şəbəkə müharibədə informasiya mübadiləsini və qarşılıqlı əlaqəni böyük ölçüdə yaxşılaşdırır.
2. İnformasiya mübadiləsinin və qarşılıqlı əlaqənin yaxşılaşması informasiyanın etibarlılıq, doğruluq keyfiyyətini, həmçinin ümumi vəziyyət haqqında məlumatlılığı artırır.
3. Ümumi vəziyyət haqqında məlumatlılıq bölmələrin özünü sinxronlaşdırmasına imkan verir.
4. Özünüsinxronlaşdırma isə öz növbəsində fəaliyyətlərin effektivliyini kəskin şəkildə artırır.

Yuxarıda qeyd edilənlərdən diqqət çəkən əsas məqam özünüsinxronlaşdırmadır. Ənənəvi mərkəzləşdirilmiş iyerarxik quruluşa malik hərbi təşkilatlarda komanda, qərar, məlumat, tapşırıq, qarşılıqlı əlaqə qurma məsələləri yuxarıdan aşağıya ötürülür və adətən, bütün fəaliyyətlər yuxarı rəislərin

diktəsi ilə icra olunur. Özünüsinxronlaşdırmada isə bir çox mürəkkəb fəaliyyətlər aşağıdan yuxarıya doğru təşkil edilir və qarşılıqlı əlaqə tənzimlənir. Bunun səbəbi döyüş meydanındakı komandirlərin istər döyüşən əsgərlər, istərsə də müxtəlif səviyyədə olan rəisləri ilə birbaşa qarşılıqlı əlaqə yarada bilməsidir. Bu onlara yaranmış vəziyyət haqqında daim məlumatlı olmağa, həmin məlumatı real vaxt rejimində yuxarı rəislərə ötürməyə, dəyişən şəraitə cəld uyğunlaşmağa, şəraitə uyğun sürətlə müstəqil qərar qəbul etməyə və yerdəyişmə aparmağa, atəş dəstəyi və əlavə güc istəməyə imkan verir. Qısaca, döyüş meydanındakı komandirlər yuxarı komandanlığın niyyətlərinə uyğun, vəzifə və hədəfləri, həmçinin döyüşün aparılma forma və üsulunu özləri müəyyən edəcəklər. Özünüsinxronlaşdırma həm sürət, həm idarəetmə, həm də qəfillik baxımdan düşmən üzərində böyük üstünlük qazandırır. Bu üstünlük döyüş fəaliyyətlərini fasiləsiz aparmağa imkan verir. Nəticədə düşmənin yararlana biləcəyi taktiki və əməliyyat fasilələri aradan qalxır, döyüş fəaliyyətləri daha dinamik, fasiləsiz və qətiyyətli olur. Bölmələrin müstəqil olaraq fəaliyyət göstərə bilməsi, həmçinin yüksək məlumatlılıq taktiki, əməliyyat və strateji səviyyədə döyüş fəaliyyətlərini eyni vaxtda aparmağa imkan verəcəkdir.

Amerikalı mütəxəssislərin fikrincə, "Şəbəkə əsaslı müharibə" coğrafi cəhətdən geniş səpələnmiş, lakin mükəmməl informasiya-kommunikasiya şəbəkəsinə qoşulmuş və döyüş meydanı haqqında yaxşı məlumatlanmış qüvvələrin yaradılmasını nəzərdə tutur [24]. "Şəbəkə əsaslı müharibə" sisteminin əsas komponentləri aşağıdakılardır:

– bütün zəruri məlumatlara real vaxt rejimində çıxış, həmçinin onların sürətlə ötürülməsini təmin edən effektiv informasiya-kommunikasiya şəbəkəsi;

– alınan məlumatların təhlili nəticəsində müəyyənləşdirilən hədəflərə uzaq məsafədən yüksək dəqiqliyə malik silahlarla zərbələrin endirilməsini, həmçinin zəruri yerdəyişmələri təşkil edən yüksək effektivliyə malik komanda-idarəetmə sistemi;

– ətraf mühitdə baş verən hər hansı bir dəyişikliyi ani olaraq aşkarlayan, məlumatları təhlil edərək ötürmə imkanına malik və vahid şəbəkəyə qoşulmuş "sensorlar". Bu sensorlara təyyarə, peyk və pilotsuz uçuş aparatlarına quraşdırılmış, həmçinin stasionar optik-elektron müşahidə sistemləri, fərdi müşahidə kameraları, radiolokasiya qurğuları, teplovizorlar və bədən "sensorları" kimi müxtəlif vasitələr aiddir. Hesab edirik ki, gələcəkdə bu "sensorlar" vasitəsilə nəinki, ətraf mühitdə baş verən hadisələri, həm də əsgərin bədənində gedən fizioloji prosesləri də real vaxt rejimində izləmək mümkün olacaqdır. Bunun nəticəsində komandirlər döyüşdə yaralanan, həlak olan, hətta taqətdən düşən əsgərlər barəsində vaxtında məlumatlı olacaqlar.

Beləliklə, texnologiyaların inkişafı nəticəsində hərb sənətində baş verən inqilabi dəyişiklikləri və bu dəyişikliklərin yaxın gələcəkdə daha da sürətlənməsini nəzərə alaraq, gələcək müharibələrin xüsusiyyətlərini təsvir edə bilərik. Fikrimizcə, yaxın on il ərzində meydana gələcək müharibələrdə döyüşlərin "təmassız", yaxud "məsafədən" aparılma forması artacaq və gələcəyə doğru bu formalar daha da təkmilləşərək, geniş vüsət alacaqdır. Bunların "təmassız", yaxud "məsafədən" adlandırılmasının səbəbi odur ki, müharibənin ilkin və ya əsas mərhələsində düşmənə sarsıdıcı zərbələr təmas xəttindən uzaqda olan (uçan) vasitələrdə yerləşdirilmiş yüksək dəqiqliyə malik silahlarla endiriləcək, yaxud döyüş meydanında uzaqdan və ya avtonom idarəedilən silahlı robototexnika (dron sürüsü və s.) fəaliyyət göstərəcəkdir. Əvvəlki müharibələrdə əsas yük quru qoşunlarının üzərinə düşürdü və düşmənlə birbaşa təmasa girərək onu məhv etmədən və müəyyən ərazini ələ keçirmədən qələbə qazanmaq mümkün deyildi. Hərb sənətində baş verəcək növbəti inqilab isə müharibədə qələbə qazanmağın mahiyyətini əsaslı şəkildə dəyişdirməkdədir. Belə ki, müharibənin əvvəlində uzaq məsafədən yüksək dəqiqliyə malik silahlarla düşmənin mühüm hərbi və mülki obyektlərinə zərbələr endirmək və onun hərbi, iqtisadi və döyüş potensialına ciddi ziyan vurulmaqla, əhali və hərbi qulluqçular arasında qorxu və çaxnaşma yaradılacaqdır. Növbəti mərhələdə artıq qorxu və çaxnaşma içində olan düşmən bölmələri xüsusi təyinatlı qüvvələrin və ya taktiki qrupların sürətli həmləsi ilə məhv ediləcəkdir. Hesab edirik ki, bu mərhələdə süni zəkaya malik və avtonom idarəolunan hərbi robototexnika, dron sürüsünün sözügedən qüvvə və qruplarla birlikdə, yaxud onlarla sinxronlaşdırılmış bir şəkildə istifadəsi yaxın gələcək üçün gözlənilməndir.

Hərb sənətində baş verən inqilab müharibənin həm strateji, həm operativ, həm də taktiki səviyyələri haqqında mövcud olan anlayışlara təsir edərək, onları əhəmiyyətli dərəcədə dəyişəcəkdir. Əgər əvvəlki müharibələrdə taktiki, operativ və strateji səviyyələr arasında ərazi, məkan, zaman, məqsəd və qüvvə baxımdan müəyyən bir sərhəd var idisə, gələcəkdə bu sərhəd silinəcək və səviyyələri təyin etmək çətin olacaqdır. Belə ki, hərbi əməliyyatların əhatə dairəsi ərazi və məkan baxımdan genişlənəcək. Ənənəvi quru, hava və dəniz məkanlarına kosmik və informasiya (kiber) məkanları əlavə olunacaqdır. Hərbi-texnoloji inkişaf hədəfləri eyni anda həm taktiki, həm operativ, həm də strateji dərinlikdə seçməyə və məhv etməyə imkan verəcək. Bununla belə, əgər düşmənlə döyüş meydanında hər hansı bir təmas olacaqsa, bu qısa müddət ərzində baş verəcək. Qeyd edildiyi kimi, əvvəlki ənənəvi müharibələrdə həlledici döyüşlər, əsasən, quru qoşunları tərəfindən yerdə aparılırdı, müəyyən dərinlik və genişliyə malik idi. Bu müharibədə şaquli olaraq yuxarıda və üfüqi olaraq geridə fəaliyyət göstərən qüvvə və vasitələr (hərbi hava, raket-artilleriya bölmələri), adətən, quruda döyüş fəaliyyətlərini aparan qoşunların dəstəyinə verilirdi. Gələcəkdə təmassız müharibələrdə isə hər şey tərsinə olacaqdır.

Ənənəvi müharibələrdə strateji məqsədə nail olmaq üçün taktiki və operativ səviyyədə döyüşlər planlaşdırılır və aparılırdı. Bunun üçün böyük qüvvələrin yerdəyişməsi və yerləşməsi təşkil edilir, ehtiyatlar və təminat nöqtələri yaradılır, hücumda əsas istiqamət, müdafiədə əsas səylərin cəmləşdirilməsi istiqaməti təyin edilir, yaxın, uzaq və sonrakı tapşırıq göstərilir, yaxud dərinlikdə müdafiə təşkil edilirdi. Fikrimizcə, gələcək müharibələrdə bunların bir çoxuna ehtiyac qalmayacaq. Çünki əsas zərbənin və ya təhlükənin haradan gələcəyi və necə olacağı barədə aydın təsəvvür olmayacaqdır. Gələcək müharibələrin müqəddəratını və qalibini yaxşı düşünülmüş, eyni zamanda düzgün seçilmiş strategiya müəyyən edəcəkdir. Bundan başqa, hesab edirik ki, gələcəkdə çox sayda canlı qüvvənin, həmçinin böyük silahlı birlik və birləşmələrin döyüşdə tətbiqi üstünlük deyil, potensial risk yaradacaqdır. Belə ki, müxtəlif yerüstü və havadan (kosmik fəzadan) kəşfiyyat və müşahidə vasitələri ilə aşkar edilən düşmən qüvvə və texnikalarına yüksək dəqiqliyə malik silahlarla zərbələr endiriləcəkdir. Bu şəraitdə effektivlik meyarının yüksəldilməsində kiçik, lakin çoxfunksiyalı dron və robototexnika, həmçinin qabaqcıl müşahidə və informasiya-kommunikasiya sistemləri ilə təchiz edilmiş və yaxşı hazırlanmış mobil taktiki qrupların rolu xeyli artacaqdır.

Döyüş meydanına çox sayda canlı qüvvə cəlb edilmədiyindən, döyüşün ən vacib elementlərindən biri olan atəşlə manevr öz əhəmiyyətini tədricən itirəcəkdir. "Ön xətt", "müdafiə rayonu", "cəbhə", "əsas hücum istiqaməti" kimi terminlər "dəqiq zərbə", "əsas zərbə yeri", "cavabdehlik rayonu", "dəqiq zərbə endirmə məsafəsi", "sürətlə zərbə altına almaq", "şəbəkənin intensivliyi" kimi terminlərlə əvəz olunacaq. Döyüşün nəticəsi bu fəaliyyətlərin effektivliyi ilə müəyyən ediləcək: sürətlə aşkar etmək; sürətlə təhlil etmək; sürətlə qərar qəbul etmək; sürətlə müdaxilə etmək və ya dəqiq zərbə ilə uzaqdan məhv etmək. Məhz bu fəaliyyətlərdə üstünlük əldə edən tərəf gələcək müharibələrdə qələbə qazanacaqdır.

Nəticə

Əhalinin artması, urbanizasiya və ətraf mühitin çirklənməsi fonunda məhdud imkanlar uğrunda gedən gərgin mübarizə, həmçinin millətçilik və etnik zəmində qarşıdurmalar, beynəlxalq terrorizm, qaçqın axını, narkotiklərin qanunsuz dövriyyəsi, kütləvi qırğın silahlarının yayılması gələcəkdə də davam edəcək və yeni müharibələrin yaranmasına səbəb olacaqdır.

Müharibə, bəşər sivilizasiyasının bir hissəsi kimi, şübhəsiz ki, daim inkişafdadır. Nəzərə almaq lazımdır ki, son illərdə bu inkişaf daha da dinamik xarakter almışdır. Belə ki, müşahidə olunan elmi-texniki inqilab insan fəaliyyətinin və sosial münasibətlərin bütün sahələrinə olduğu kimi, silahlı qarşıdurmaların üsul və formalarına da böyük ölçüdə təsir etmişdir. Artıq müasir müharibələr 20 və 10 il bundan əvvəl olmuş münaqişələrdən çox fərqlənir. Zamanımızın müharibələri artıq fiziki məkanlarla (quru, hava, dəniz) yanaşı, informasiya, kiber və kosmik məkanları da əhatə edir. Fikrimizcə, yaxın onillikdə, elmi-texniki sahədə əldə ediləcək nailiyyətlər bu məkanların bir-birinə inteqrasiyasını daha da genişlədərək, müharibələrin xarakterini köklü şəkildə dəyişdirəcəkdir.

Təhlillər göstərdi ki, texnologiyalarda, o cümlədən bio, nano və rəqəmsal texnologiyalarda baş verən və gözlənilən böyük inkişaf hərb sənətində inqilabi dəyişikliyə səbəb olacaqdır. Döyüşün forma və üsulları keçmişlə müqayisədə əhəmiyyətli dərəcədə dəyişəcək. Barıtın və atıcı silahların yaranmasından bugünə qədər uğurla istifadə olunan bir çox forma və üsullar, həmçinin döyüşün əsas komponentləri artıq effektiv olmayacaq. Belə ki, döyüşün bugünə qədər birlikdə tətbiq edilməklə effektivliyi sınanmış atəş, zərbə və manevr kimi əsas komponentlərindən gələcəkdə sadəcə zərbə, vacibliyini qoruyub saxlayacaqdır. Əvvəlki müharibələrdə strateji məqsədlərə nailolmada taktiki və operativ səviyyədə düşmənlə birbaşa təmasa girilərək, onun əsas qüvvələrinin atəş və manevrlə darmadağın edilməsi və ərazinin ələ keçirilməsi vacib şərt sayılırdı. Burada yerüstü əməliyyatlara xüsusi önəm verilirdi. Gələcək müharibələrdə isə rəqibin mühüm obyektlərini, o cümlədən kritik infrastrukturunu, idarəetmə mərkəzlərini, təminat nöqtələrini, hərbi texnikalarını uzaq məsafədən dəqiq zərbə ilə sıradan çıxartmaq və bununla da ona öz istəyini qəbul etdirmək mümkün olacaq. Gələcəkdə müharibə aparmaq üçün qabaqcıl texnologiyalara sahib olmayan, o cümlədən süni zəkanı, uzaqməsafəli yüksək dəqiqliyə malik silahların inkişafına nail olmayan ölkələr bu çatışmazlığı canlı qüvvənin, eləcə də ənənəvi silah və texnikaların sayını çoxaltmaqla əvəz etməyə çalışacaqlar. Bununla belə, hesab edirik ki, gələcək müharibələrdə hazırlıqsız canlı qüvvə və ənənəvi hərbi texnikanın çoxluğu üstünlük deyil, böyük çatışmazlıq olacaqdır. Çünki dəqiq zərbələr nəticəsində idarəetməni və bir neçə ağır texnikanı itirmiş tərəfin şəxsi heyəti arasında çaxnaşma, qorxu və çaşqınlıq yaranacaq, bununla da döyüş qabiliyyəti aşağı düşəcəkdir. Son çarə olaraq, həmin tərəfin kütləvi qırğın silahı, qadağan olunmuş sursatlardan istifadəetmə, yaxud terrorçuluq fəaliyyətlərinə başlama ehtimalı yüksəkdir.

Əlavə olaraq, yüksək dəqiqliyə malik silahlarla yanaşı, süni zəka ilə avtonom idarəedilən müxtəlif robototexnika, pilotsuz uçuş aparatları, o cümlədən dron sürüsü gələcək müharibə meydanında aparıcı rol oynayacaq. Bunların silahlı münaqişələrdə geniş tətbiqi Silahlı Qüvvələrin strukturunu əhəmiyyətli dərəcədə dəyişəcək. Artıq yaxın gələcəkdə Quru, Hava və Dəniz Qüvvələrinə aid müxtəlif səviyyədəki (taktiki, operativ və strateji) ənənəvi qoşun növlərini vahid komanda-idarəetmə şəbəkəsinə qoşulmuş strateji kəşfiyyat-zərbə, zərbə vasitələri, yüksək dəqiqliyə malik silah sistemlərindən ibarət qüvvələr, həmçinin kiçik, lakin mobil, hazırlıqlı, hərtərəfli təchiz edilmiş xüsusi təyinatlı qüvvələr (taktiki qruplar) əvəz edəcək.

Yekun olaraq qeyd edək ki, gələcək müharibələrdə hadisələr sürətlə cərəyan edəcək, vəziyyət tez-tez dəyişəcək, zərbələr qısamüddətli, lakin dəqiq və dağıdıcı olacaqdır. Belə bir şəraitdə döyüşdə qələbə qazanmaq üçün təşəbbüs, bilik, çeviklik, dərin düşünmə, hərtərəfli hazırlıq, güclü motivasiya kimi liderlik keyfiyyətləri ön plana keçəcəkdir.

İstifadə edilmiş ədəbiyyat siyahısı

1. Beverelli, L. Why France Lost in 1940: [Electronic resource] / – War Writers. – October 11, 2020. URL: https://warwriters.com/why-france-lost-in-1940/

2. Walsh, T. The defence review fails to address the third revolution in warfare: artificial intelligence: [Electronic resource] / – The Conversation. – April 28, 2023.
URL: https://theconversation.com/the-defence-review-fails-to-address-the-third-revolution-in-warfare-artificial-intelligence-204619

3. What Are The Main Causes Of War?: [Electronic resource] / – Last updated – August, 2017.
URL:https://resources.finalsite.net/images/v1612766712/dohacollegecom/pxkzaxykcazvtnquk4uf/Arwa-ImmerseTheMainCausesOfWarEssay.pdf

4. Coccia, M. Comparative Theories and Causes of War: [Electronic resource] / – Global Encyclopedia of Public Administration, Public Policy, and Governance (pp.1-7), Publisher: Springer. – December, 2019.
URL:https://www.researchgate.net/publication/337890175_Comparative_Theories_and_-Causes_of_War

5. Finucane, M. İs War Primarily the Product of "Human Nature": [Electronic resource] / – E-International Relations. – October 31, 2013. URL: https://www.e-ir.info/2013/10/13/is-war-primarily-the-product-of-human-nature/

6. Matthew, O. J., Massimo, M. The Reasons for Wars – an Updated Survey: [Electronic resource] / – Handbook on the Political Economy of War. – December, 2009.
URL:https://www.researchgate.net/publication/238529380_The_Reasons_for_-Wars_-_an_Updated_Survey

7. Assumpção, C. Is Huntington's "Clash of Civilizations" a Self-fulfilled Prophecy?: [Electronic resource] / – Dublin City University, E-International Relations. – January 29, 2020.
URL: https://www.e-ir.info/pdf/81197

8. James, M. D. No guarantees when it comes to war: [Electronic resource] / – Association of The United States Army. – August 22, 2018. URL: https://www.ausa.org/articles/no-guarantees-when-it-comes-war

9. Cole, B. Clausewitz's Wondrous Yet Paradoxical Trinity: The Nature of War as a Complex Adaptive System: [Electronic resource]/ The premier professional military and academic publishing house. – February 7, 2020.
URL:https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2076059/clausewitzs-wondrous-yet-paradoxical-trinity-the-nature-of-war-as-a-complex-ada/

10. Waldman, T. War, Clausewitz, and the Trinityhttps: [Electronic resource] / – University of Warwick, Department of Politics and International Studies. – June, 2009.
URL: https://core.ac.uk/download/pdf/40048786.pdf

11. Черных, Г.С., Старостин, А. С. Оружие на новых физических принципах, проблемы защиты населения и территорий от его поражающих факторов // – Москва: Стратегия гражданской защиты: проблемы и исследования, – 2015. № 2(9). – с. 22-37;

12. Безбородов, В. Бесконтактные войны - революция в военном искусстве: [Электронный ресурс] / – Военное обозрение. Мнения. –17 ноябрь, 2014. URL: https://topwar.ru/62636-beskontaktnye-voyny-revolyuciya-v-voennom-iskusstve.html

13. Fernow, R. C. Introduction to experimental particle physics: [Electronic resource] / – Cambridge University Press. – March, 2022. URL: https://library.oapen.org

14. Rodgers, E. Directed-Energy Weapons Come Of Age: [Electronic resource] / – Honeywell, Aerospace Technologıes. – February 13, 2024. URL: https://aerospace.honeywell.com/us/en/about-us/blogs/directed-energy-weapons-come-of-age

15. Bothwell, B. Science & Tech Spotlight: Directed Energy Weapons: [Electronic resource] / – U.S. Government Accountability Office. – May 25, 2023. URL: https://www.gao.gov/products/gao-23-106717

16. Marcin, M. M. What is Artificial Intelligence?: [Electronic resource] / – Conference Paper. – November 2019.
URL: https://www.researchgate.net/publication/337089782_What_is_Artificial_Intelligence

17. Etzioni, A., Etzioni, O. Pros and Cons of Autonomous Weapon Systems: [Electronic resource] / – Military Review. – June 2017. URL: http://www.armyupress.army.mil/Journals/Military-Review/-English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/

18. Matthew, U. What Is Nanotechnology?: [Electronic resource] / – Built In, Expert Contributors. – January 16, 2024. URL: https://builtin.com/hardware/nanotechnology

19. Grewal, D. et al. The future of in-store technology // – Oslo: Journal of the Academy of Marketing Science. – 2020.T. 48. – p. 96-113;

20. Квантовый компьютер: что, зачем, когда: [Электронный ресурс] / – ноябрь 25, 2022. URL: https://vc.ru/future/548157-kvantovyy-kompyuter-chto-zachem-kogda

21. Mallick, P. Network centric warfare: [Electronic resource] / – The Centre for Land Warfare Studies. – October, 2020. URL: https://www.researchgate.net/publication/344737587_network_-centric_warfare

22. Jonjo, R. Modern Militaries and a Network Centric Warfare Approach: [Electronic resource] / – E-International Relations. – January 9, 2014. URL: https://www.e-ir.info/2014/01/09/modern-militaries-and-a-network-centric-warfare-approach/

23. Smith, C.R. Network Centric Warfare, Command, and the Nature of War: [Electronic resource] / Land Warfare Studies Centre, Canberra. – February 2010. URL:https://researchcentre.army.gov.au/sites/default/files/sp318ncwcommandandnatureofwarchristopher_smith.pdf

24. Чижевский, Я. А. Реализация концепции сетецентрических боевых действий в вооруженных силах США // –Военная мысль, – 2019. № 3. – с.116-137.

Аннотация
Характер будущих войн
Гейдар Пириев, Ариф Гасанов, Рашад Тахиров

Сегодняшние военно-политические реалии требуют от Вооруженных Сил быть готовыми к будущим войнам в любой момент в целях обеспечения национальной безопасности страны. Потому что, как и в прошлом, борьба за природные ресурсы, межгосударственная конкуренция, стремление к гегемонии, а также идеологические разногласия и проблемы безопасности, которые приводят к военным конфликтам, продолжатся и в будущем. В то же время достигнутый и ожидаемый большой прогресс в области техники существенно изменит традиционные формы и методы борьбы. Под влиянием научно-технического прогресса формы и способы ведения войн будущего существенно изменятся по сравнению с прошлыми. Таким образом, в будущих войнах события, в том числе боевые действия, будут разворачиваться более динамично, ситуация обмена информацией будет часто меняться, а удары будут кратковременными, но точными и разрушительными. Традиционные виды боя, такие как нападение и оборона, игравшие ключевую роль в достижении целей военных действий в предыдущих войнах и требовавшие непосредственного контакта с противником, потеряют свое значение. Появятся новые методы и формы борьбы. Изучение и умелое применение этих форм и методов в Вооруженных Силах будет одним из главных условий успеха в будущих войнах. По этой причине в целях изучения характера будущих войн, прогнозирования методов и форм военных действий в статье анализируются происходящие и ожидаемые изменения в научно-технической сфере, рассматривается их влияние на военное дело. Кроме того, в начале статьи рассматриваются причины войны, чтобы лучше понять ее природу или характер.

Ключевые слова: война, политическая, мир, конфликт, противоречие, стратегия, гибрид

Abstract
Nature of future wars
Heydar Piriyev, Arif Hasanov, Rashad Tahirov

Today's military-political realities require the Armed Forces to be prepared for future wars at any time in order to ensure the country's national security. Because, as in the past, the struggle for natural resources, interstate competition, the desire for hegemony, as well as ideological differences and security problems that lead to military conflicts will continue in the future. At the same time, the great progress achieved and expected in the field of technology will significantly change traditional forms and methods of struggle. Under the influence of scientific and technological progress, the forms and methods of waging future wars will change significantly compared to the past. Thus, in future wars, events, including fighting, will unfold more dynamically, the situation of information exchange will change frequently, and strikes will be short-lived, but accurate and destructive. Traditional types of combat, such as attack and defense, which played a key role in achieving military objectives in previous wars and required direct contact with the enemy, will lose their importance. New methods and forms of military operation will appear. The study and skillful application of these forms and methods in the

Armed Forces will be one of the main conditions for success in future wars. For this reason, in order to study the nature of future wars, predict methods and forms of military action, the article analyzes ongoing and expected changes in the scientific and technical sphere, and examines their impact on military affairs. In addition, the article begins by examining the causes of war to better understand its nature or character.

Keywords: war, political, peace, conflict, conflict, strategy, hybrid

Məqalə redaksiyaya daxil olmuşdur: 17.04.2024
Təkrar işlənməyə göndərilmişdir: 26.04.2024
Çapa qəbul edilmişdir: 14.05.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 22-33
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 351/354 DOI: 10.30546/9878.2024.2.10.0014.

KİBERCİNAYƏTLƏRİN MİLLİ VƏ BEYNƏLXALQ HÜQUQİ-QANUNVERİCİ ASPEKTLƏRİ

Zahid Oruc
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
zahidoruc@gmail.com

Xülasə. Məqalədə milli və beynəlxalq qanunvericilik təcrübəsinə əsaslanaraq kibercinayətkarlıq və kibertəhlükəsizlik məsələlərinin hüquqi aspektləri, mümkün təhlükələr və bu təhlükələrin mənbələrinin aradan qaldırılması ilə bağlı yanaşmalar təhlil edilir. Həmçinin vurğulanır ki, kibertəhlükəsizlik sahəsində mövcud qanunların və mütərəqqi təcrübələrin qarşılıqlı öyrənilməsi və tətbiqi kibertəhlükəsizliyin təmin olunmasına xidmət edir. Kibercinayətlər "internet cinayətindən" daha geniş anlayışdır, çünki istənilən informasiya və ya telekommunikasiya şəbəkələrindən istifadə etməklə cinayət törətmək imkanlarını özündə ehtiva edir. Kibercinayətkarlıq kompüter sistemləri və ya kompüter şəbəkələrinə, habelə kiberməkana daxil olmaq üçün digər vasitələrdən istifadə etməklə və ya onlar vasitəsilə, kompüter şəbəkələri daxilində saxlanan, emal edilən, yaxud ötürülən məlumatlara qarşı kiberməkanda törədilən cinayətləri əks etdirir. Bununla belə, kibercinayətkarlığın dəqiq və tam başa düşülməsi, habelə onun dünyada qanunvericilik baxımından modifikasiyası, ümumən qəbul edilmiş yanaşma, vahid bitkin təriflər məsələsi hələ də araşdırılmayıb. Tədqiqat nəticəsində məlum olur ki, yalnız qanunvericilik sahəsində deyil, kibercinayətin tərifi ilə bağlı nəzəri, doktrinal yanaşmalarda da alimlər arasında ümumi konsensus hələ də formalaşmayıb. Bu isə kiberməkanda cinayətlərin həm sürətli artımı, həm də cinayət törədilərkən kompüter sistemlərindən istifadənin forma və üsulları ilə bağlıdır.

Açar sözlər: kibercinayət, hüquqi aspektlər, kibertəhlükəsizlik, milli qanunvericilik, beynəlxalq qanunvericilik, hüquqi mübarizə, Azərbaycan

Giriş

İnformasiya texnologiyalarının sürətli inkişafı ilə paralel olaraq, kiberməkanda törədilən cinayətlərin sayı internet və kompüter şəbəkələrindən istifadə edənlərin sayına mütənasib olaraq artır. Hazırkı dövrdə kibercinayətkarlığın çox ciddi qlobal təhdidlərdən olması, onun çoxsaylı formalarının əhatəli təsnifatı, habelə qanunvericilikdə adekvat təsbit edilməsi məsələsini aktuallaşdırır. Yeni cinayətkarlıq fenomeninin qanunverici əsaslarının hazırlanması üçün milli və beynəlxalq səviyyədə səylərin davam etdirilməsinə baxmayaraq, hər ay, yaxud hər il yeni kibercinayət növləri meydana çıxır. Hüquq mühafizə orqanlarının belə cinayətlərin qarşısının alınması üzrə işinin səmərəliliyi isə kibercinayətkarlığın düzgün elmi-hüquqi definisiyası, qanunvericilikdə operativ təsbit və tətbiq edilməsi, cəmiyyətdə hüquqi maarifləndirmənin aparılması ilə bilavasitə bağlıdır.

İnternet istifadəçilərinin sayı artdıqca, bu haldan sui-istifadə edərək, müxtəlif qanun pozuntularına yol verən fırıldaqçıların da sayı çoxalır. Kibercinayətlərin, internet fırıldaqçılığının maraqlı xüsusiyyəti ondan ibarətdir ki, bir çox üsullar açıq şəkildə qanuna zidd olmur və bu, fırıldaqçıların qanun çərçivəsində təqib edilməsini çətinləşdirir. Kiberfırıldaqçılar eyni sxem üzrə fəaliyyət göstərirlər: birincisi, onlar e-poçt və ya sosial şəbəkələr vasitəsilə qurbanla əlaqə qurur, həmçinin e-poçt, telefon, faks və ya hər hansı digər yolla cavab almağa çalışırlar. Cavab alan fırıldaqçılar qurbanın etimadını qazandıqdan sonra müxtəlif bəhanələrlə müxtəlif məbləğdə pul istəyirlər. Belə fırıldaqçıların qurbanı olmamaq üçün onların üsullarını yaxşı bilmək, internetdə hansı fırıldaqçılıq üsullarının mövcud olması ilə bağlı məlumatlı olmaq lazımdır.

Pandemiya dövründə məsafədən və hibrid iş rejimlərinin, biznes platformalarının (ZOOM, Microsoft Teams, Skype və s.) texnoloji-informasiya müstəvisindən genişlənərək, sosial məkan müstəvisinə çevirilməsi və qlobal miqyas alması kibertəhlükəsizliyi, həm də ictimai-sosial təhlükəsizliyin ayrılmaz tərkib hissəsi etmişdir.

Dünyanın əksər ölkələrindəki normativ qaydalar kibercinayətləri cinayət kimi qeydə alır, cərimədən tutmuş ölüm cəzasına qədər cəza növlərini nəzərdə tutur.

Kibercinayətkarlığın hüquqi aspektlərini müəyyən etmək və bu anlayışı sistemləşdirmək üçün hüquqi ədəbiyyatda mövcud olan tərifl ərin təhlili vacibdir. Ümumi olaraq, kibercinayətkarlıq informasiya-kommunikasiya texnologiyalarının istifadəsi ilə informasiya məkanında məsafədən törədilmiş cinayətlər sistemi olan, tarixən dəyişkən, gizli sosial və cinayət hüququnun neqativ hadisəsi kimi başadüşülməlidir. Bütövlükdə, elmi-nəzəri və doktrinal yanaşmaların təhlili, kibercinayətin tərifində alimlər arasında konsensusun mövcud olmadığını göstərir. Eyni vəziyyət, həm də kiberməkanda müxtəlif şərhləri və qanunsuz hərəkətləri törədərkən kompüter sistemlərindən istifadənin forma və üsulları ilə də bağlıdır. Fərqlərə baxmayaraq, araşdırmaçılar kiberməkanda törədilən cinayətlər kimi təsnif edilən qeyri-qanuni hərəkətlərin siyahısı ilə bağlı beynəlxalq və milli qanunvericiliklər arasında əlaqə məsələsinin vacibliyini vurğulayırlar. Hesab edilir ki, "kibercinayət" anlayışı istənilən informasiya-kommunikasiya texnologiyalarından istifadə etməklə törədilən cinayətlərə şamil oluna bilər.

XXI əsrdə texnoloji inkişaf və informasiya inqilabının nailiyyəti nəticəsində formalaşan, ənənəvi olaraq, "real məkan" kimi başa düşülən məkana alternativ olan, sərhədlərinin, demək olar ki, tamamilə aradan qaldırıldığı yeni "virtual məkan" qismində – kiberməkanın mövcudluğu ümumən qəbul edilmişdir. Mobil telefonlar, kompüter və planşetlər və sair hər bir fərdin kiberməkanda təmsilçiliyini təmin edir. İnternet və kompüter vasitəsilə ünsiyyət bütün dünyada insanların məlumat mübadiləsi üsullarını kəskin şəkildə dəyişdirmişdir. İnformasiya texnologiyalarının insanlara verdiyi rahatlıq artdıqca, elektron daşıyıcılardan istifadə də geniş vüsət almış, zaman və məkandan asılı olmayaraq, istənilən məlumatın işləndiyi, saxlandığı, daşındığı və ötürüldüyü mühitlərə əlçatanlıq daha da asanlaşmışdır.

Kibercinayətlərin leqal aspektləri

Virtual məkanda qlobal kibercinayətkarlığın getdikcə yüksələn yeni dalğası, müvafiq olaraq, fərqli reallıqları aşkara çıxarmışdır. Müasir dövrdə heç bir, hətta ən güclü dövlət belə, "Ümumdünya Hörümçək Toru"nda – internetdə cinayətkarlıqla təkbaşına mübarizə aparmaq gücündə deyil. Potensial kibercinayətkarlığın subyekt və obyektlərinin say və miqyasının sürətlə artması, ona qarşı mübarizədə yeni üsul və vasitələrin daha da təkmilləşdirilməsi birgə – hüquqi, texnoloji, siyasi, iqtisadi, elmi, mədəni əməkdaşlıq çərçivəsində – tənzimləmə mexanizmlərinin hazırlanmasını şərtləndirir. Hər bir dövlətin informasiya infrastrukturu qlobal internet şəbəkəsi ilə sıx bağlı olduğundan, yeni cinayətkarlıq növü dövlətin milli təhlükəsizliyinə ciddi təhdidlər yaradır.

Kibercinayətlərlə beynəlxalq mübarizənin səmərəli və mühüm elementləri Birləşmiş Millətlər Təşkilatı (BMT) sistemində həyata keçirilir. Bu cinayətlə mübarizənin daha geniş spektrdə effektivliyinə nail olmaq üçün universal beynəlxalq qurum olan BMT çərçivəsində qəbul edilən sənədlər əsasında bu sahəyə dair təsbit olunmuş müqavilə müddəalarına üzv ölkələrin diqqət yetirməsi zəruri hesab olunur.

Kibercinayətkarlıqla bağlı beynəlxalq hüquq normalarının, xüsusilə "Kibercinayətkarlıq haqqında Budapeşt Konvensiyasının" ölkədaxili implementasiyası beynəlxalq hüquqda təsbit olunan ümumi qaydalara uyğun şəkildə həyata keçirilir. Lakin burada kibercinayətkarlıqla bağlı hüquqi normalar, habelə milli qanunvericiliyin maraqları ilə əlaqədar bəzi spesifik məqamlar nəzərə alınmalıdır.

Budapeşt Konvensiyası kibercinayətkarlıqla mübarizənin aşağıdakı prinsiplərini müəyyən etmişdir:

– geniş əməkdaşlıq prinsipləri;
– köçürmə prinsipi;
– qarşılıqlı yardımın ümumi prinsipi;
– təcili yardım tələblərinin rəhbər tutulması və həyata keçirilməsi prinsipi;
– məxfilik və məhdud istifadə prinsipi;
– müvəqqəti yardım prinsipi;
– yardımın göstərilməsi prinsipi və s. [1, s.14].

Kibercinayətkarlıq transmilli komponentə malikdir və transmilli xarakterinə, nəticələrinin ciddiliyinə görə digər beynəlxalq cinayətlərdən, heç də geri qalmır. Kibercanilər serverdə quraşdırılmış məlumatların, virusların və digər zərərli proqramların təminatçılarıdır. Bu baxımdan kibercinayətkarlığa qarşı hərtərəfli regional əməkdaşlığın qurulması və cinayətlə mübarizə mexanizmlərinin müəyyənləşdirilməsi vacibdir.

Bir çox amillər, kiberməkanın səciyyəvi xüsusiyyətləri, habelə informasiya infrastrukturunun dövlətlə yanaşı, özəl sektor və vətəndaşların əlində cəmlənməsi kibercinayətkarlıqla mübarizədə adekvat institutsional qurumların, elmi-texniki və normativ-hüquqi bazanın formalaşdırılması və təkmilləşdirilməsi ilə yanaşı, dövlət, özəl sektor və vətəndaşlar arasında, həmçinin beynəlxalq səviyyədə tərəfdaşlıq və əməkdaşlığın genişləndirilməsini tələb edir. Qeyd edilənlərin həyata keçirilməməsi (çoxtərəfli və beynəlxalq tərəfdaşlıq və əməkdaşlığın qurulmaması, adekvat mexanizmlərin, zəruri institutların yaradılmaması və s.) kibercinayətkarlıqla mübarizəni daha da çətinləşdirir.

Kiberməkanda insan amili və gündəlik sosial həyat özünün bütün komponentləri ilə təmsil olunur ki, bu da öz növbəsində cinayət fenomeninin tamamilə yeni təzahürlərinə gətirib çıxarır. Texnoloji tərəqqinin nəticəsi olaraq, müsbət sosial təzahürlərlə yanaşı, mənfi təzahürlər, o cümlədən cinayətkarlığın yeni üsul və formaları kiberməkanda yayılaraq qloballaşır. İnternetin yaratdığı imkanların genişləndirdiyi bu yeni cinayətlər kibercinayətlər kimi müəyyən edilir.

Bəzi dövlətlər kibertəhlükəsizliyə mülki və ya iqtisadi məsələ kimi yanaşsalar da, bir çoxları kibertəhlükəsizlik siyasətinin yaradılması və ya həyata keçirilməsinə kəşfiyyat agentliklərini cəlb edirlər. Kibertəhdidlər insanların təhlükəsizlik və milli təhlükəsizlik qaydaları və təcrübələri haqqında fikirlərinə inqilabi dəyişiklikləri şərtləndirir. Kibertəhlükənin bütün ölkələr tərəfindən qəbul edilən vahid və hərtərəfli tərifi mövcud olmasa da, demək olar ki, bütün dövlətlər kiberməkanda təhlükə və risklərin öz milli təhlükəsizlik siyasətinə daxil edilməsi fikrində yekdildirlər. Bu məsələnin tədqiqatçılar tərəfindən öyrənilməsi davam etdirilsə də, onun aktuallığı səngimir. Belə ki, texnologiyaların sürətli inkişafının səbəb olduğu mühitdə siyasətçilər və hüquqşünaslar yaranmış yeni tənzimlənmə problemlərinə çevik cavab vermək üçün çox vaxt dəyişən reallıqla ayaqlaşa bilmirlər [2; 3; 10].

Ayrı-ayrı fərdlər kiberməkanda virtual kimliklərini (virtual identiklik), real dünyadakı kimlikləri ilə eyniləşdirirlər. Bu inteqrasiya ictimai şüurda və psixi strukturlaşmada "dissosiasiya" adlanan prosesləri şərtləndirir. Toplumda insanların şüurunda yaranan yayınmalar, amneziya, diqqətsizlik və affektiv hərəkətliliklə səciyyələnən "dissosiativ təcrübələr" getdikcə kiberməkanda fərdlərin "kiberqurbana" (cyber victims) çevrilməsinə səbəb ola, onları cinayətin şahidi və ya cinayətkar edə bilər. Optimal məsafənin, real və virtual məkanlar arasında sərhədlərin qeyri-müəyyənliyi, kiberməkandakı dissosiativ psixoloji potensial və zəminlər fərdlərin cinayətə üz tutmasını asanlaşdırır. Kibercinayətin hüquqi aspektləri fərdin kiberməkanda olduğu dissosiativ və mobil (dinamik, səyyar) affektiv zəminlərdə qiymətləndirilməlidir. Bütün bu məsələlər, dəyişən sosial-mədəni dinamika qeyd olunan cinayətlərin inkişafı üçün zəmin rolu oynayır. Bu cinayətlərin psixoloji dinamikası cinayətkarın və qurbanın tipologiyasının müəyyən edilməsində, beləliklə də profilaktik tədbirlər planının işlənib hazırlanmasında və davam etdirilməsində mühüm əhəmiyyət kəsb edir.

Digər tərəfdən hüquqi-qanuni çərçivədə "məlumat sisteminə daxil olmaq", "sistemi bloklamaq, məlumatları məhv etmək və ya dəyişdirmək", "bank və ya kredit kartlarından sui-istifadə" və s. kimi əməllər də kibercinayətkarlıqdır. Bütün bunlar "informatika sahəsində cinayətlər" başlığı altında tənzimlənir [4].

Məlumdur ki, cinayətkar və deviant qruplar artıq bir-birindən çox uzaq məsafələrdə belə informasiya mübadiləsi aparmaq üçün forumlar və xəbər qrupları kimi kompüter vasitəsilə işləyən kommunikasiya texnologiyalarından istifadə edə bilirlər.

Əlavə olaraq, hakerlər təhlükəsizlik resurslarına çıxış əldə etmək və məlumatları oğurlamaq üçün demək olar ki, istənilən növ kompüter proqramı və avadanlıqlarından istifadə imkanına malikdirlər [5, s.87].

Kibercinayətlərə qarşı hüquqi mübarizə: bəzi beynəlxalq və milli təcrübələr

Milli, regional və beynəlxalq qanunlar real həyatda olduğu kimi, kiberməkanda da davranışları və kibercinayətlərlə bağlı cinayət mühakiməsi məsələlərini tənzimləyə bilər. Bu qanunlar yalnız baş vermiş hallarla bağlı qayda və gözləntiləri deyil, həm də bu qayda və gözləntilərin pozulması halında əməl edilməli olan prosedurları müəyyən edir. Bununla belə, kibercinayətin əsas növləri ilə bağlı müxtəlif ölkələrin milli qanunvericiliyində təsbit edilən müddəalardakı fərqlər cinayət mühakiməsi və ona qarşı mübarizə sahəsində beynəlxalq əməkdaşlığı mürəkkəbləşdirir. Kibercinayətkarlığa qarşı beynəlxalq əməkdaşlıq, müvafiq olaraq, transmilli mütəşəkkil cinayətkarlıqla mübarizədə beynəlxalq əməkdaşlıq sferasının daha da genişlənməsini tələb edir.

Kibercinayətkarlıqla milli qanunvericiliklərdən bəhs edərkən qeyd olunmalıdır ki, bu hallar mövcud qanunlara kibercinayətkarlıqla bağlı müddəaları əlavə etmək yaxud, dəyişiklik etməklə təmin edilə bilər. Digər tərəfdən, mövcud qanunların bütün hallarda kibercinayətlərə tətbiqi mümkün olmaya bilər. Belə ki, onlar internet və rəqəmsal texnologiyaların yaranmasından əvvəl qəbul edilmiş, yaxud internet və rəqəmsal texnologiyalar nəzərə alınmadan hazırlanmış ola bilər. Buna görə də real həyatdakı cinayətlərlə əlaqədar nəzərdə tutulmuş qanunlar, virtual məkandakı kibercinayətkarlara və informasiya-kommunikasiya texnologiyalarından (İKT) cinayətin törədilməsinin subyekti və ya vasitəsi kimi istifadə edən digər cinayətkarların əməllərinə tətbiq edilməyə, yaxud onlara sadəcə məhdud çərçivədə təsir göstərə bilər. Nəticədə kibercinayətlərlə bağlı xüsusi qanunlara ehtiyac duyulur. Kibercinayətkarlıqla bağlı qanunların qəbul edilib-edilməməsi, milli qanunvericiliyin əhatə dairəsindən, normativ aktların xarakteri və şərhindən asılıdır.

Kibertəhlükə və kiberhücumların getdikcə daha çox yayıldığı bir şəraitdə, nəinki dövlət və qurumlar səviyyəsində, hətta ayrı-ayrı müəssisələr və təşkilatlar səviyyəsində də biznes və informasiya təhlükəsizliyi siyasəti, eləcə də texnoloji siyasətin prioritet hesab edilməsi kibercinayətlərdən qorunmağa ciddi töhfə verə bilər. Təşkilatlardan keçən məlumatlar hüquqi baxımdan fərqli ola bilər. Məsələn, hər hansı bir müəssisə və ya şirkətin bütün işçilərinin məxfi məlumatlara bütövlükdə çıxışı varsa, o zaman "müəssisənin məlumatlarının sızmayacağına necə əmin olmaq olar?".

Kibercinayətlər haqqında qanunun yeri və roluna gəldikdə, bu qəbildən olan qanunlar informasiya və kommunikasiya texnologiyaları (İKT) istifadəçiləri üçün məqbul davranış standartlarını müəyyən edir; kibercinayətlərə görə sosial və hüquqi sanksiyalar müəyyən edir; ümumilikdə İKT istifadəçilərini qoruyur və xüsusilə insanlara, verilənlərə, sistemlərə, xidmətlərə və infrastruktura dəyən ziyanı minimuma endirir və ya qarşısını alır; insan hüquqlarını qoruyur; internetdə (virtual dünyada) törədilmiş cinayətləri araşdırmaq və mühakimə etmək imkanı verir; kibercinayətkarlıq halları üzrə ölkələr arasında əməkdaşlığı təşviq edir [6, s.57].

Kibercinayətkarlıq qanunvericiliyi internetdən, kompüterlərdən və əlaqəli rəqəmsal texnologiyalardan istifadə dövlət və özəl təşkilatların hərəkətlərində davranış qaydaları və standartlarını təmin edir; sübut qaydaları; cinayət prosesinin həyata keçirilməsi qaydaları və cinayət hüququnun kiberməkana aid digər məsələləri; kibercinayətkarlıq halında şəxslərə, təşkilatlara və infrastruktura dəyən riskin azaldılması və ya zərərin azaldılması üçün müddəalar. Beləliklə, kibercinayətkarlıq qanunvericiliyi maddi, prosessual və qabaqlayıcı hüquq normalarını ehtiva edir.

Bəzi ölkələr kibercinayətkarlıqla bağlı yeni spesifik qanunlar hazırlamaq əvəzinə, öz milli qanunlarına və ya məcəllələrinə ayrıca kibercinayətkarlıqla bağlı müddəaları daxil edərək düzəlişlər etmişlər. Digər ölkələr cinayət törətmək üçün informasiya və kommunikasiya texnologiyalarından qeyri-qanuni istifadə ilə bağlı ayrıca qanunvericilik aktlarını qəbul etməyə üstünlük verirlər. Belə ki, cinayəti törədən şəxs saxtakarlıq və ya dələduzluq etmək üçün qeyri-qanuni girişdən istifadə edibsə, belə bir əməl eyni vaxtda iki cinayət təşkil edir.

Bir sıra ölkələrdə kibercinayətkarlıqla mübarizəyə dair ayrıca qanunlar hazırlanmışdır. Məsələn, Almaniya, Yaponiya və Çin kibercinayətkarlıqla mübarizə sahəsində öz cinayət məcəllələrinin müvafiq müddəalarına düzəlişlər etmişlər. Bəzi ölkələr, həmçinin kibercinayətlərin və kibercinayətkarların müəyyən növlərini əhatə etmək üçün mövcud qanunlardan istifadə edirlər.

Hər bir dövlətin kibercinayətkarlıq sahəsində maddi cinayət hüququnun yaradılmasına təsir göstərən öz hüquq sistemi var:

1. Ümumi hüquq (Common law). Burada qanunlar qəbul edilmiş ayrıca qanunlar və presedent hüququ (yəni, məhkəmə qərarları və ya məhkəmə presedentləri əsasında formalaşan qanun) şəklində mövcuddur.

2. Mülki hüquq (Civil law). Belə hüquq sisteminə malik olan ölkələr əsas hüquqların, öhdəliklərin, və davranış gözləntilərinin sərhədlərini müəyyən edən kodifikasiya olunmuş, birləşdirilmiş və hərtərəfli normativ qaydalar və qanunlara malikdirlər. Bu sistemlər, əsasən, qanunvericiliyə və konstitusiyaya əsaslanır.

3. Adi hüquq (Customary law). Bu hüquq sistemlərinə konkret tarixi-mədəni ənənələrin daşıyıcıları tərəfindən qanun kimi qəbul edilən ümumi davranış nümunələri daxildir (opinio juris – qanuniliyə inam). Beynəlxalq hüquqda adət hüququ dövlətlər arasında münasibətləri və praktikanı tənzimləyir və bütün dövlətlər üçün məcburi hesab olunur.

4. Dini hüquq (Religious law). Dini hüquq sistemləri hüququn mənbəyi kimi dini təlimlərə və ya dini ədəbiyyata əsaslanan qaydalardan istifadə edir.

5. Hüquqi plüralizm (Legal pluralism). Bu tip hüquq sistemində yuxarıda qeyd olunan hüquq sistemlərindən iki və ya daha çoxu (məsələn, ümumi hüquq, mülki hüquq, adət hüququ və ya dini hüquq) bir yerdə mövcud ola bilər [7, s.101].

Kibercinayətkarlığın beynəlxalq səviyyəsinə gəldikdə, bu sahədə bir sıra beynəlxalq müqavilələrin bağlandığı qeyd edilə bilər. Ümumiyyətlə, mövcud çoxtərəfli və regional hüquqi sənədlər və milli qanunlar öz tematik məzmunu və kriminallaşma, istintaq tədbirləri və səlahiyyətləri, rəqəmsal sübutların toplanması və istifadəsi, tənzimləmə və risk, yurisdiksiya və beynəlxalq əməkdaşlıq kimi aspektləri əhatəetmə dərəcəsi ilə fərqlənir. Bu müqavilələr, həm də coğrafi əhatə dairəsi (yəni regional və ya çoxtərəfli olması) ilə fərqlənir. Bu cür fərqlər kibercinayətkarların effektiv müəyyən edilməsi, araşdırılması və mühakimə olunmasına, eləcə də kibercinayətkarlığın qarşısının alınmasına maneələr yaradır. İnternet məzmununu və girişi məhdudlaşdıran qanunların qanuni məqsədlər üçün tətbiqini, qanunun aliliyi və insan hüquqları standartlarına uyğunluğunu təmin etmək üçün də təminatların nəzərə alınması lazım gəlir. Bundan əlavə, kibercinayətkarlıq qanunlarının əhatə dairəsi və tətbiqi "bir ölkədə yaradılan və məqbul olan internet məzmunu üçüncü ölkədə əlçatan olduqda" belə məzmunun qeyri-qanuni hesab edildiyi məqamlarda çətinləşir [5, s.128].

Kibercinayətkarlıqla bağlı ayrı-ayrı ölkələrin hüquqi praktikalarına gəldikdə, Çin, ABŞ, Estoniya, Ukrayna, Niderland, İspaniya, Avstriya, Böyük Britaniya və digər ölkələrdə kiberterrorizmlə bağlı xüsusi qanun qəbul edilmiş, həmçinin bir sıra qanunvericiliyə əlavə və dəyişikliklər də edilmişdir.

Kibertəhlükəsizlik siyasətinin həyata keçirilməsi ilə məşğul olan ölkə kimi Estoniyanın təcrübəsi maraqlıdır. Dövlət tərəfindən bu sahədə bir sıra strateji sənədlər hazırlanmış, qəbul edilmiş, müvafiq institusional strukturlar yaradılmışdır. Strateji planlaşdırma bütün kibertəhlükəsizlik arxitekturasının vəhdətini təmin edir. 2008-ci ildə Estoniya Respublikası dünyada ilklərdən biri olaraq beynəlxalq hüquq normaları çərçivəsində yazılmış Milli Kibertəhlükəsizlik Strategiyasını [10] qəbul edib. Estoniya informasiya-kommunikasiya texnologiyalarından istifadəni və "ağıllı həllər"in işlənməsini asanlaşdıran şərait yaratmağa başlamışdır [8].

Çin bir-biri ilə bağlı olan: 2015-ci il iyulun 1-də "Dövlət təhlükəsizliyi haqqında", 2017-ci il iyunun 1-də "Kibertəhlükəsizlik haqqında", 2016-cı ildə "Terrorizmlə mübarizə haqqında" Qanun qəbul etmişdir. Böyük Britaniyanın 2000-ci il "Terrorizm Aktı"na əsasən kompüterlərə, onların sistemlərinə və ya şəbəkələrinə ciddi ziyan vurmaq, yaxud onların kütləvi zorakılıq aksiyalarını təşkil etmək üçün əldə edilmiş kompüter məlumatlarının isifadəsinə dair, Fransa Cinayət Məcəlləsinin 4211 – "İnformatika sahəsindəki hərəkətlərlə bağlı terror aktları"nda kibercinayətkarlığın terror aktlarına bərabər tutula biləcəyi müəyyənləşdirilmişdir [9, s.93].

Rusiya, Ukrayna, Gürcüstan, Qazaxıstan və Estoniyada qəbul edilmiş qanunlarda artıq informasiya texnologiyaları və kommunikasiyaların terrorizmdə rolunu aydın şəkildə müəyyən edir.

Ukraynanın 21 iyun 2018-ci il tarixli 2469-VIII nömrəli "Kibertəhlükəsizliyin təmin edilməsinin əsas prinsipləri haqqında" Qanununun 1-ci maddəsində kiberməkanda və ya ondan istifadə etməklə həyata keçirilən terror fəaliyyəti (kiberterrorizm) ilə bağlı tədbirlər nəzərdə tutulmuşdur.

Xarici ölkələrdə kibercinayətkarlıqla mübarizənin aparılması həvalə edilən sahəvi səlahiyyətli qurumların fəaliyyəti də fərqlidir. Başqa sözlə, bu səlahiyyət Avstraliyada Müdafiə Departamenti, Belçikada Təhlükəsizlik Nazirliyinin Komitəsi, Braziliyada İnformasiya Təhlükəsizliyi Komitəsi, Kanadada Kanada Kompüter Şəbəkəsinin Fövqəladə Hallara Cavab Mərkəzi, Estoniyada İqtisadiyyat, Rabitə və Nəqliyyat Nazirliyi, Finlandiyada, Baş Nazirlik strukturunda Milli Müdafiə Baş Katibliyi, Fransada Milli İnformasiya Təhlükəsizliyi Agentliyi, Almaniyada Federal İnformasiya Təhlükəsizliyi Agentliyi, Macarıstanda İnformatika və Rabitə Nazirliyi, Hindistanda Milli İnformasiya Şurası, İtaliyada Daxili İşlər Nazirliyi, Yaponiyada Nazirlər Kabineti, Koreya Respublikasındakı bütün dövlət təşkilatları və onların törəmə qurumları, Malayziyada Modernləşdirmə və Planlaşdırmanı İdarəetmə Mərkəzi, Niderlandda Daxili İşlər Nazirliyi və Kral İşləri Nazirliyi, Yeni Zelandiyada Kritik İnfrastrukturun Mühafizəsi, Norveçdə Mülki Müdafiə və Böhran Planlaması İdarəsi, Elm və Ali Təhsil Nazirliyi və Daxili İşlər Nazirliyi, Polşada sahəvi idarələr, Sinqapurda İnformasiya Şəbəkələri və Rabitə Təhlükəsizliyi Müdirliyi, İspaniyanın Dövlət İdarəçilik Nazirliyi və Daxili İşlər Nazirliyi, Böyük Britaniyada Nazirlər Kabineti yanında Kibertəhlükəsizlik İdarəsi, həmçinin bir sıra müxtəlif təşkilati bölmələrdə kiberterrorizmlə məşğul olan qurumlar mövcuddur [11, s.35-45].

Macarıstan Respublikasında "Dövlət-Özəl Tərəfdaşlıq Fondu" kibertəhlükəsizlik üçün vəsaitlərin sistemli şəkildə bölüşdürülməsini təmin edir. Həmçinin Macarıstanda kiberterrorizmlə mübarizədə "CERT– Macarıstan Təcili Müdaxilə Qüvvəsi". Hindistanda Hindistan Respublikası Milli Təhlükəsizlik Şurasının Katibliyinin 21-ci üzvü yanında kiberterrorizmlə mübarizə məqsədilə "Hindistanın Milli İnformasiya Şurası" yaradılmışdır. İtaliyada Daxili İşlər Nazirliyi və İnnovasiya və Texnologiyalar Nazirliyi kiberterrorizmlə mübarizə sahəsində dövlət siyasətinin işlənib hazırlanması və həyata keçirilməsi üzrə səlahiyyətli dövlət orqanı kimi müəyyən edilir. Həmçinin İtaliyada poçt polisi xidməti yaradılmışdır və o, milli və regional səviyyələrdə kompüter cinayətlərinə operativ reaksiya mərkəzlərinə nəzarət edir. İtaliyanın "Kritik İnfrastruktur Mütəxəssisləri Assosiasiyası" dövlət və özəl sektorların kibertəhlükəsizlik işini əlaqələndirir [12, s.35-45].

Bütövlükdə, hüquq sistemləri daxilində hüquqi tənzimləmələr kibercinayət qurbanlarının hüquqlarının qorunmasında, günahkarların lazımi sanksiyalarla üzləşməsinin təmin edilməsində və cinayətin reallaşmasının qarşısının alınmasında mühüm rol oynayır.

Artıq qloballaşma və informasiya dövrünün tələblərinə müvafiq olaraq, milli qanunvericilik sistemləri də modern dəyişikliklərə məruz qalmaqdadır.

Bu gün dünyanın əksər ölkələri sürətlə inkişaf edən müasir İKT sistemlərinə nüfuz etdikcə milli qanunvericiliklərdə də müasir beynəlxalq hüquq norma və prinsiplərin tələblərinə uyğun rasional dəyişiklik və inkişaf müşahidə olunur [13, s.98].

Azərbaycanda kibertəhlükəsizliyin təminatı. Azərbaycanda kibertəhlükəsizlik sahəsində hüquqi-tənzimləyici çərçivələr

Ölkəmizdə informasiya-kommunikasiya texnologiyalarının sürətli inkişafı beynəlxalq hüquqi münasibətlərin kibercinayətkarlıq kimi müxtəlif sahələrində beynəlxalq əməkdaşlığa və bu sahədə hüquqi mübadilələrin zəruriliyinə səbəb olmuşdur. Dövlətimiz kibercinayətlərə qarşı mübarizədə Birləşmiş Millətlər Təşkilatı, Avropa Şurası, və Avropa İttifaqı (Aİ) çərçivəsində hüquqi addımlar atmağa başlamışdır.

Digər ölkələr kimi, Azərbaycanda da kibercinayətkarlıqla mübarizədə hərtərəfli əməkdaşlıq çərçivəsində beynəlxalq hüququn milli qanunvericiliyə daxil edilməsi və tətbiqi istiqamətində zəruri tədbirlər həyata keçirilir. Azərbaycan Respublikasında kiberməkandan istifadə, o cümlədən informasiya ehtiyatlarının mühafizəsi və kibercinayətkarlığa qarşı mübarizə milli təhlükəsizlik qədər mühümdür. Bu sahədə beynəlxalq hüququn tətbiqi Azərbaycan Respublikasının milli təhlükəsizlik sahəsinə dair qanunvericiliyində öz əksini tapmışdır [14].

Ölkəmizdə kibertəhlükəsizlik sahəsində mühüm addımlar atılmışdır və Prezident İlham Əliyev bu sahədə uğurlu siyasət həyata keçirir. Budapeşt Konvensiyası kibercinayətkarlıqla bağlı qoşulduğumuz ilk qanunvericilik sənədidir.

Bütün dünyada olduğu kimi, Azərbaycanda da milli kibertəhlükəsizlik siyasətinin inkişaf etdirilməsi zəruri məsələdir. Hökumətin informasiya və kommunikasiya sistemləri, o cümlədən hərbi, texnoloji və kommersiya layihələri kiberhücumlar və kibercasusluğunun hədəfi kimi getdikcə daha həssas qrupu təşkil edir. Bu baxımdan kiberməkanın idarə edilməsinə dövlət səviyyəsində əhəmiyyət verilir.

Qeyd edilən istiqamətdə hüquqi-tənzimləyici məzmunlu (strategiya, qanunlar, doktrinalar və qanunvericiliyin təkmilləşdirilməsi) dövlətin kibertəhlükəsizliyinin, bu sahədə dövlət siyasətinin prinsip və istiqamətlərinin yaradılması üzrə hüquqi və təşkilati çərçivə formalaşdırılmışdır. Buraya, həmçinin dövlət orqanları, müəssisələr, institutlar, təşkilatlar, fərdlər və vətəndaşların sözügedən sferada səlahiyyətləri, eyni zamanda onların fəaliyyətlərinin koordinasiyası üzrə başlıca prinsipləri də daxildir. Azərbaycanın kibertəhlükəsizlik siyasəti ilə bağlı hüquqi-tənzimləyici bazanın inkişafına əsas etibarilə 1999–2000-ci illərdə başlanılıb. Kibertəhlükəsizliklə bağlı ayrıca strategiya, hələlik hazırlanmasa da, müxtəlif sahələrdə dövlət siyasətlərinin həyata keçirilməsində kibertəhlükəsizlik məsələlərinin inkişafı üçün mühüm müddəalar artıq təsbit edilib.

Bu kimi strategiyalara "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014–2020-ci illər üçün Milli Strategiya" və "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016–2020-ci illər üçün Dövlət Proqramı"nı, həmçinin "Azərbaycan 2020 gələcəyə baxış" İnkişaf Konsepsiyasını və "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"ni aid etmək olar. Həmçinin "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" Beynəlxalq Telekommunikasiya İttifaqı (BTİ) və Aİ tərəfindən hazırlanmış bütün təcrübə və tövsiyələri nəzərə alan sənəddir. Strategiyanın əsas məqsədi informasiya cəmiyyətinin qurulması və İKT-nin inkişafı daxil olmaqla ölkənin davamlı sosial-iqtisadi və mədəni səviyyədə yüksəlişi üçün vətəndaşlar, icmalar və dövlət tərəfindən onun imkanlarından səmərəli istifadə etməkdir. Müvafiq strategiyanın həyata keçirilməsi üçün Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi əlaqələndirici qurum təyin edilmişdir. Məqsəd, rəqəmsal məkanda təhlükəsizliyi inkişaf etdirmək, İKT-dən istifadəyə inamı artırmaq, qanunvericilik bazasını təkmilləşdirmək və məlumatlılığı yüksəltməkdir. Bu məqsədlərə çatmaq üçün vəzifələr sırasına isə informasiya təhlükəsizliyi üzrə dövlət siyasətinin hazırlanması, bu istiqamətdə xarici ölkələrdən asılılığın azaldılması, "elektron hökumət" şəbəkələrinin mühafizəsi, kibertəhlükələrin əhəmiyyətinin ölkə miqyasında elan edilməsi, kibertəhlükəsizlik sahəsində texniki peşəkarlığın inkişaf etdirilməsi, uşaqların istifadəsi üçün "təhlükəsiz internet" platformasının gücləndirilməsi, cəmiyyətdə və şirkətlər arasında məlumatlılığın artırılması, eləcə də informasiya təhlükəsizliyi mədəniyyətinin təşviqi daxildir.

Yuxarıda qeyd edilən strategiya hər biri dövlət proqramları ilə müşayiət olunan iki mərhələdə həyata keçirilir. "2016–2020-ci illər üçün Dövlət Proqramı" Milli Strategiyanın tətbiqi istiqamətində yeddi prioritet üzrə konkret addımlardan ibarətdir. İnformasiya təhlükəsizliyinə dair tədbirlər planına əsasən Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi (RİNN), Dövlət Təhlükəsizliyi Xidməti (DTX) və Müdafiə Nazirliyi (MN) kibertəhlükəsizliyə dair normativ hüquqi aktların yenilənməsinə məsul olan qurumlardır. "Telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"nə və İKT sektorunun "SWOT" təhlilinə əsasən şəbəkə və informasiya təhlükəsizliyinə qarşı artan çağırışlar əsas təhlükələr sırasındadır. Bu baxımdan, strateji məqsədlərdən biri, milli kibertəhlükəsizliyə hazırlığın və məlumatlılığın artırılmasıdır.

Qanunvericilik bazasına aid sənədlərin bəziləri kimi aşağıdakılar qeyd edilə bilər:

"Dövlət sirri haqqında" Azərbaycan Respublikasının Qanunu, 2004; Milli Təhlükəsizlik Konsepsiyası, 2007; "Kibercinayətkarlıq haqqında" Konvensiyanın təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, 2009; Azərbaycan Respublikasının Hərbi doktrinası, 2010; "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu, 2010; "İnformasiya təhlükəsizliyi sahəsində

fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2012; "Milli təhlükəsizlik haqqında" Azərbaycan Respublikasının Qanununda dəyişiklik edilməsi barədə Azərbaycan Respublikasının Qanunu, 2012; "Azərbaycan Respublikasının Cinayət Məcəlləsi. Otuzuncu fəsil. Kibercinayətlər", 2012; "Azərbaycan Respublikasının Xüsusi Dövlət Mühafizə Xidmətinin Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi haqqında Əsasnamənin və Agentliyin strukturunun təsdiq edilməsi" barədə Azərbaycan Respublikası Prezidentinin Fərmanı, 2012; "Azərbaycan Respublikasının Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin fəaliyyətinin təmin edilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2012; "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə Azərbaycan Respublikasının Qanunu, 2017; "Rəqəmsal transformasiya sahəsində idarəetmənin təkmilləşdirilməsi haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2021; "Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası", 2021; "Azərbaycan Respublikasının Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti haqqında Əsasnamənin təsdiq edilməsi" barədə Azərbaycan Respublikası Prezidentinin Fərmanı, 2021;"Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində bəzi tədbirlər haqqında" Azərbaycan Respublikası Prezidentinin Fərmanı, 2021.

Bundan əlavə, Azərbaycan Respublikası Prezidentinin 2005 və 2010-cu illərdəki sərəncamları, habelə Azərbaycan Respublikası Nazirlər Kabinetinin 14 may 2010-cu il tarixli sərəncamı ilə Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafına dair Dövlət proqramları təsdiq edilmişdir.

2011-ci ildə "Elektron hökumətin formalaşdırılması üzrə Fəaliyyət Proqramı"nda İKT-nin inkişafı ilə bağlı əməli tədbirlərin həyata keçirilməsi nəzərdə tutulmuşdur.

2014-cü ildə Azərbaycan Respublikası Prezidentinin Sərəncamı ilə kibertəhlükəsizlik strategiyası qəbul edilmişdir. Azərbaycanda informasiya cəmiyyətinin əsaslarını yaratmış İKT üzrə Milli Strategiya vətəndaşlar, cəmiyyət və özəl sektor tərəfindən İKT-dən geniş istifadəni nəzərdə tutur.

Milli Strategiyanın başlıca məqsədi və vəzifələri ölkənin informasiya məkanının təhlükəsizliyinin təmin edilməsi, İKT-dən istifadəyə inamın artırılması, bu sahəni tənzimləyən normativ hüquqi bazanın işlənib hazırlanması, informasiya və maarifləndirmə işinin həyata keçirilməsi ilə bağlıdır.

Strategiyanın məqsədlərinə nailolmanın siyasi istiqamətləri:

a) informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin və hüquqi bazanın təkmilləşdirilməsi;

b) ölkənin milli informasiya məkanının və strateji infrastrukturunun, habelə informasiya infrastrukturunun, informasiya təhlükəsizliyini təmin edən sistemin inkişafı;

c) ölkənin informasiya əlaqələrində texniki və texnoloji asılılığın azaldılması üzrə tədbirlərin həyata keçirilməsi;

d) "elektron hökumət" infrastrukturunun informasiya təhlükəsizliyinin təmin edilməsi;

e) elektron təhlükələr haqqında məlumatın milli səviyyədə həyata keçirilməsi;

f) kibertəhlükəsizliyin gücləndirilməsi sahəsində müvafiq texniki və metodiki vasitələrin yaradılması, tövsiyələrin hazırlanması və metodiki dəstəyin göstərilməsi;

g) uşaqları qeyri-qanuni və təhlükəli məzmundan qorumaq üçün "təhlükəsiz internet" mexanizminin işlənib hazırlanması və tətbiqi;

h) dövlət və qeyri-dövlət informasiya infrastrukturu subyektlərinin kibertəhlükəsizlik üzrə fəaliyyətinin əlaqələndirilməsi;

i) əhalinin, özəl və digər qurumların kibertəhlükəsizlik sahəsində maarifləndirilməsi və informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması, bu sahədə ixtisaslı kadrların hazırlanması;

j) ölkənin informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığının təmin edilməsi.

Milli Strategiyanın icrası prosesində dövlət orqanları, özəl sektor və vətəndaş cəmiyyəti institutları arasında sıx əməkdaşlıq və əlaqələndirilmiş fəaliyyət təmin edilir, informasiya cəmiyyəti ideyalarının geniş yayılması üçün fəal təbliğat aparılır.

Azərbaycanın kibersərhədlərinin mühafizəsi ilə üç əsas dövlət qurumu məşğul olur: Rabitə və İnformasiya Texnologiyaları Nazirliyi (RİTN), Dövlət Təhlükəsizlik Xidməti (DTX) və İnformasiya Texnologiyaları İnstitutu (İTİ). Azərbaycanın Dövlət Departamentləri üzrə kompüter şəbəkələrinin mühafizəsi məqsədilə Xüsusi Dövlət Mühafizə Xidmətinin nəzdində informasiya təhlükəsizliyi insidentlərinə cavab vermək üçün CERT-GOV-AZ18 kompüter fövqəladə hallar qrupu yaradılmışdır.

Dövlət Təhlükəsizlik Xidməti kibercinayətkarlıqla mübarizə üzrə səlahiyyətli orqan kimi təyin olunmuşdur və kibercinayətkarlıq hallarının araşdırılması, bu istiqamətdə yaranan təhlükələrin qarşısının alınması məqsədilə səmərəli mübarizənin aparılması üçün müvafiq addımlar atmaqdadır.

Kibercinayətkarların, xüsusən də kiberterrorizmin artması bu təhlükənin qarşısının alınması üçün Dövlət Təhlükəsizlik Xidmətinin işinin təkmilləşdirilməsi məsələsini daha da aktuallaşdırmışdır. Bu sahədə qeyri-qanuni fəaliyyətlə mübarizə aparmaq üçün müvafiq texniki təchizat, eləcə də yüksək texnologiyalar üzrə xüsusi bilik və bacarıqlar tələb olunur [1, s.204-205].

Ölkəmizdə kibertəhlükəsizliyin təmin edilməsi məqsədilə Azərbaycan Respublikası Prezidentinin 26 sentyabr 2012-ci il tarixli Fərmanının 5-ci hissəsinə uyğun olaraq, Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyinin tabeliyində Kibertəhlükəsizlik Mərkəzi (CERT.GOV.AZ) yaradılmışdır. Kibertəhlükəsizlik Mərkəzi sosial sabitlik və virtual məkanda normal fəaliyyəti təmin edir, kibertəhlükəsizlik sahəsində informasiya infrastrukturunun fəaliyyətini əlaqələndirir, mövcud və potensial elektron təhlükələr barədə aidiyyəti orqanları məlumatlandırır.

Elektron idarəetmənin bu missiyasının davamlılığına nail olmaq üçün hökumətin qarşıya qoyduğu tapşırıqlar [15]:

1. Elektron Hökumət Akademiyasının yaradılması.
2. Elektron Hökumət Araşdırma Mərkəzinin yaradılması.
3. Elektron hökumət üzrə bacarıqların artırılması və biliklərin paylaşılması.
4. Elektron hökumət infrastrukturunun inkişafı (G-Cloud adlı hökumət buludunun tətbiqi).

Prezidentin Fərmanı ilə nəqliyyat, rabitə və yüksək texnologiyalar sahəsində idarəetmənin təkmilləşdirilməsi ilə bağlı əlavə tədbirlər haqqında Azərbaycan Respublikasının 12 yanvar 2018-ci il tarixli sərəncamı ilə Elektron Təhlükəsizlik Xidməti (ETX) kimi Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyinin strukturuna daxil edilmişdir. Ümumiyyətlə, ETX infrastruktur haqqında məlumat verən, ölkə səviyyəsində mövcud və potensial elektron təhlükələr barədə məlumatlılığı, əhalinin, özəl qurumların və digər təşkilatların kibertəhlükəsizlik sahəsində maarifləndirilməsini təmin edən, həmçinin metodiki köməklik göstərən əlaqələndirici dövlət orqanıdır.

Elektron Təhlükəsizlik Xidməti aşağıdakı fəaliyyətləri həyata keçirir:

a) kibertəhlükəsizlik sahəsində informasiya infrastrukturu subyektlərinin fəaliyyətini əlaqələndirmək;

b) istifadəçilərdən, proqram təminatı, aparat və texniki avadanlıq istehsalçılarından, xarici ölkələrdəki analoji strukturlardan və digər mənbələrdən kiberhücumlar, müdaxilələr, zərərli kompüter proqramları (bundan sonra elektron təhlükə və təhdidləri) haqqında məlumatları toplamaq və təhlil etmək;

c) istifadəçilərin kibertəhlükəsizlik məsələlərinə dair məlumatlılığının artırılması məqsədilə mövcud və potensial kibertəhlükələrin bildirilməsini həyata keçirmək;

d) istifadəçiləri təhdid edən proqramlar və texniki vasitələr haqqında təlimat və tövsiyələr hazırlamaq, kibertəhlükələrə qarşı mübarizəyə metodiki dəstək göstərmək;

e) qlobal internet trafikində kiberhücumların dəf edilməsi üçün milli İnternet operatoru və aidiyyətli beynəlxalq qurumlarla birgə qabaqlayıcı tədbirlər həyata keçirmək;

f) kibertəhlükəsizliyə hazırlığı təmin etmək üçün ölkədə fəaliyyət göstərən digər aidiyyəti qurumlarla əməkdaşlıq etmək [4, s.133].

2002-ci ildə yaradılan İnformasiya və Telekommunikasiya Elmi Mərkəzinin (BTRM) əsasında AMEA-da İnformasiya Texnologiyaları İnstitutu (İTİ) fəaliyyətə başlamışdır. İnstitut 2022-ci ildə Elm və Təhsil Nazirliyinə tabe edilmişdir. İnformasiya Texnologiyaları İnstitutu İKT-nin müasir problemlərinə dair innovativ elmi tədqiqatlar aparan təşkilatdır. Burada informasiya texnologiyaları və

informasiya cəmiyyətinin aktual elmi-nəzəri problemləri üzrə tədqiqatların əsası qoyulmuş, yeni elmi-tədqiqat şöbələri və mərkəzləri açılmışdır. İnstitutda mühüm layihələr həyata keçirilir, səmərəli tədqiqat nəticələrinin əldə edilməsi və təşkilatın daha yüksək innovasiya fəaliyyətinin təşkili üçün beynəlxalq standartlara cavab verən bütün imkanlar yaradılır. İnstitut elmi-texniki və innovasiya siyasətinin həyata keçirilməsi istiqamətində uğurlu işlərini davam etdirir.

İnstitutun əsas məqsədləri İKT-nin geniş imkanlarından istifadə etməklə elmi fəaliyyətin müasir tələblərə uyğun təşkili və inkişaf etdirilməsi, elmi idarəetmənin təkmilləşdirilməsi, milli elmi informasiya məkanının formalaşdırılması, beynəlxalq elmi mühitə inteqrasiya və yüksək səviyyəli kadr hazırlığıdır. İnstitutun mühüm elmi nailiyyətləri bunlardır:

a) uyğunlaşan şəbəkələr üçün dəyər və vaxt göstəriciləri üzrə paylanmış optimal autentifikasiya sistemi hazırlanmış və korporativ şəbəkələrdə müxtəlif təhlükələrə qarşı mübarizədə qərarların qəbulu üçün nəzəri oyun modeli təklif edilmişdir;

b) virtual mühitdə informasiya müharibəsinin təzahürünün aşkarlanması üçün üsul və alqoritmlər işlənib hazırlanmışdır. Respublikada elektron elmin formalaşdırılması, idarə olunması və qiymətləndirilməsi, informasiya təhlükəsizliyinin təmin edilməsi üçün model və metodlar təklif edilmişdir;

c) böyük verilənlər bazasının (Data Mining) intellektual təhlili üçün metodlar və alqoritmlər işlənib hazırlanmışdır. Mətn sənədləri dəstlərinin məzmununa görə qruplaşdırılması, onların avtomatlaşdırılmış ümumiləşdirilməsi və xülasələrin qiymətləndirilməsi (Text Mining) üçün çoxsaylı üsullar və alqoritmlər təklif edilmişdir;

d) elektron imza infrastrukturunun yaradılması üçün sonlu sahələr üzərində elliptik əyrilərə əsaslanan kriptoqrafik üsullar və alqoritmlər işlənib hazırlanmışdır.

Nəticə

Məqalədə milli və beynəlxalq qanunvericilik təcrübəsi əsasında kibercinayətkarlıq və kibertəhlükəsizliyin təmin edilməsi, mümkün təhlükələrin və onların mənbələrinin dərk edilməsi məsələlərinə müxtəlif yanaşmaların hüquqi aspektləri təhlil olunmuşdur. Nəticədə kibercinayətkarlıqla bağlı qanunlara olan tələbatın, onların rolunun müəyyən edilməsinə, müzakirə və öyrənilməsinə hələ də ehtiyac olduğu qənaətinə gəlinmişdir. Qeyd etmək lazımdır ki, maddi, prosessual və preventiv-qabaqlayıcı kibercinayətkarlıqla bağlı qanunvericiliyin müəyyənləşdirilməsi, həmçinin sözügedən istiqamətlər arasındakı fərqlərin tədqiqi zəruridir.

Milli, regional və beynəlxalq səviyyəli kibercinayətkarlıq qanunlarının müəyyənləşdirilməsi və müqayisəli dəyərləndirilməsi mübarizənin hüquqi aspektlərinin daha da təkmilləşdirilməsini şərtləndirir.

Qənaətə görə, kibertəhlükəsizliyin təminatında ən yaxşı profilaktik üsullarından biri elmi tədqiqat və hüquqi maarifləndirmə sahəsində beynəlxalq əməkdaşlığın təşkilidir. Demək olar ki, hər bir ölkədə kibercinayətkarlıqla mübarizədə beynəlxalq və milli hüquq sistemlərinin əməkdaşlığının qurulması səmərəli nəticələrin ilkin şərtidir. Təlim və maarifləndirici materialların ictimaiyyətə çatdırılması, o cümlədən bu sahəyə aid məlumatların kütləviləşməsi məqsədilə radio, televiziya və internet resurslarından istifadə, normativ-hüquqi bazaların kütləvi informasiya vasitələri tərəfindən geniş təbliği də bu şərtə daxildir.

İstifadə edilmiş ədəbiyyat siyahısı

1. Convention on Cybercrime. European Treaty Series // – Budapest, –2001 № 185. 23. (XI) – 22 p.: [Electronic resource] / URL: https://rm.coe.int/1680081561

2. Kibertəhlükəsizlik 2021: [Elektron resurs] / URL: http://aggression.az/wp-content/uploads/2019/10/kıtab-kiber-2019-son.pdf

3. Mitra, A., Schwartz, R.L. From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces // Journal of Computer-Mediated Communication's, – 2001, № 1.Vol. 7: [Electronic resource] / URL: http://jcmc.indiana.edu/vol7/issue1/mitra.html.

4. Comprehensive Study on Cybercrime: [Electronic resource] / URL:https:www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrıme_study_210213.pdf
5. Maras, Marie-Helen. Computer Forensics: Cybercriminals Laws, and Evidence / Oxford University Press. – 2014. – 408 p.
6. Maras, Marie-Helen. Counterterrorism. Jones & Bartlett Learning / – 2012. – 148 p.
7. Основы политики безопасности Эстонской Республики: [Электронный ресурс] / URL:http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/julgeolekupoliitika_aluset_2010.pdf
8. Расулев, А. Противодействие кибертерроризму: международно-правовые и уголовно-правовые аспекты. / А. Расулев – 2018. – 253с.
9. Бенджамин, С. Демократическое управление и вызовы кибербезопасности / С.Бенджамин, Ф. Шрайер, Х. Теодор. – Женева: Женевский центр демократического контроля над вооруженными силами, – 2013. – 334с.
10. Həsənov A.H. Kiber Təhlükəsizlik // Hərbi Bilik, Bakı, 2014, № 5, s. 3-7.
11. Талимончик, В. П. Роль двусторонних договоров, заключенных Российской Федерацией, в международном информационном обмене // Правоведение – 2006. № 5. – 220 с.
12. Якимова, Е., Нарутто, С. Международное сотрудничество в борьбе с киберпреступностью. Криминологический журнал Байкальского национального университета экономики и права // –2016.№.2.Т.1.– с.10: [Электронный ресурс] / URL: https://e-qanun.az/framework/5455
13. “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”nın təsdiq edilməsi haqqında // [Elektron resurs] / – qanun.az. URL: https://e-qanun.az/framework/27456
14. Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri // [Elektron resurs] / URL:https://ict.az/uploads/konfrans/info_sec_2018/rs16_problems_of_educatıng_cybersecurıty_specıalısts_ınunıversıtıes.pdf
15. Məcidli, S.T. Kibercinayətlər / S.Məcidli – Bakı, – 2019. – 314 s.

Аннотация
Киберпреступления: национальные и международные правовые-законодательные аспекты
Захид Орудж

В статье анализируются правовые аспекты различных подходов к вопросам киберпреступности и обеспечения кибербезопасности и понимания возможных угроз и их источников на основе национального и международного законодательного опыта. В настоящее время в период бурного развития информационных технологий количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей. В исследовании подчеркивается, что взаимное изучение и применение существующих законов и прогрессивных практик в области кибербезопасности служат обеспечению лучшей кибербезопасности.

Киберпреступность – это более широкое понятие, чем «интернет-преступность», так как оно включает в себя возможность совершения преступлений с использованием любых информационных или телекоммуникационных сетей. Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

Однако вопрос о точном и полном понимании киберпреступности, а также о его законодательном закреплении до сегодняшнего дня остается открытым. Сущность данной проблемы заключается в том, что от правильного понимания киберпреступности зависит эффективность работы правоохранительных органов по предупреждению такого рода преступлений.

Исследование позволило прийти к выводу, что анализ доктринальных подходов не показывает единого мнения среди ученых в определении киберпреступности. Это обусловлено различными трактовками киберпространства и способов использования компьютерных систем при совершении противоправных действий. Несмотря на различия ученые ставят вопрос о соотношении национального и международного законодательства относительно перечня противоправных действий, совершаемым в киберсфере.

Ключевые слова: киберпреступность, правовые аспекты, кибербезопасность, национальное законодательство, международное законодательство, правовая борьба, Азербайджан

Abstract

Cyber crimes: national and international legal-legislative aspects

Zahid Oruj

The article analyzes the legal aspects of various approaches to cybercrime and cybersecurity issues and understanding of possible threats and their sources based on national and international legislative experience. Currently, during the period of rapid development of information technology, the number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks. The study emphasizes that the mutual study and application of existing laws and progressive practices in the field of cybersecurity serve to ensure better cybersecurity.

As a concept, it is noted that cybercrime is a broader concept than "Internet crime", since in the first case it includes the possibility of committing a crime using any information or telecommunication networks. Cybercrime - crimes committed in cyberspace against computer systems or computer networks, as well as computer data stored, announced or transmitted in computer networks using other means of access to cyberspace or through them. However, the issue of an accurate and complete understanding of cybercrime, as well as its modification from the point of view of the legislation in the world, the generally accepted approach and uniform definitions, remains open to this day.

The extremely important significance of this problem lies in the fact that the effectiveness of the activities and mutual cooperation of law enforcement agencies in the direction of preventing such crimes directly depends on the correct understanding of cybercrime, common approaches, and the availability of similar legislation.

The study led to the conclusion that the analysis of doctrinal approaches does not show a consensus among scientists in the definition of cybercrime. This is due to different interpretations of cyberspace and ways of using computer systems when committing illegal acts. Despite the differences, scientists raise the question of the relationship between national and international legislation regarding the list of illegal actions committed in the cyber sphere.

Keywords: cybercrime, legal aspects, cyber security, national legislation, international legislation, legal struggle, Azerbaijan

Məqalə redaksiyaya daxil olmuşdur: 08.01.2024
Təkrar işlənməyə göndərilmişdir: 16.01.2024
Çapa qəbul edilmişdir: 05.02.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 34-44
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 327.7 DOI: 10.30546/9878.2024.2.10.0016.

DÖVLƏTİN MİLLİ GÜCÜNÜ QİYMƏTLƏNDİRMƏ METODU

siy.e.ü.f.d., dosent Vüqar Məmmədzadə
https://orcid.org/0000-0002-5381-0387
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
vuqar.zade1982@gmail.com

tex.e.d., dosent Elxan Səbziyev
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
elkhan.sabziev@gmail.com

tex.ü.f. doktoru, professor, 1-ci dərəcəli kapitan Əsəd Rüstəmov
Azərbaycan Texniki Universiteti,
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
asadrustamov1122@gmail.com

polkovnik-leytenant Elcan İmamverdiyev
https://orcid.org/0009-0005-6394-568X
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
i.eljan85@gmail.com

mayor Cəlil Həsənov
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
jalil.hasanov@hotmail.com

Xülasə. Məqalədə dövlətin milli gücünü (MG) və onu formalaşdıran struktur komponentləri olan əhali (Əh), ərazi (Ər), iqtisadiyyat (İq), hərbi güc (HG), elmi-texniki tərəqqi (ETT), siyasi iradə (Sİ) və geosiyasi amillər (GA) təhlil edilir və hesablama qaydaları nəzərdən keçirilərək, düstur formasına salınır. Sadalanan faktorların qiymətləndirilməsi üçün istifadə olunan "yüksək", "orta", "kafi", "zəif" və "çox zəif" linqvistik qiymətlərinə uyğun olaraq, elmi-texniki tərəqqinin nailiyyətlərindən istifadə əmsalının qiymətləndirilməsində istifadə olunan "böyük", "yaxşı", "qənaətbəxş", "kiçik" və "çox az" linqvistik qiymətləri ekvivalent kimi götürülür. Tədqiqat işinin məqsədi Azərbaycan Respublikasının milli gücünü qeyri-səlis ədədlər şkalasından istifadə etməklə ekspert rəyi əsasında qiymətləndirməkdir. Məqalədə müvafiq olaraq, aşağıdakı vəzifə qarşıya qoyulur: dövlətin milli gücünü qiymətləndirmə mexanizminin hazırlanması. Tədqiqat metodlarından istifadə edilir: müqayisəli təhlil, analiz-sintez və riyazi modelləşdirmə. Aşağıdakı nəticələr əldə edilmişdir: məqalədə dövlətin milli gücünün formalaşmasının struktur təhlili əsasında milli gücün hesablanmasının daha təkmil düsturu irəli sürülür ($MG = Əh + Ər + ETT \times (İq + HG) + Sİ + GA$) və Azərbaycan Respublikasının gücü qeyri-səlis qiymətləndirmə metodu əsasında qənaətbəxş güc kimi xarakterizə olunur. Yekun nəticə: hər bir dövlətin öz daxili və xarici siyasətini mükəmməlləşdirə və siyasi kursunu daha real əsaslarla effektiv şəkildə gerçəkləşdirə bilməsi üçün real milli gücünü qiymətləndirməsi zəruridir.

Açar sözlər: milli güc, əhali, ərazi, iqtisadiyyat, hərbi güc, siyasi iradə, geosiyasi amil, elmi-texniki tərəqqi, qeyri-səlis qiymətləndirmə

Giriş

Müasir dünya Azərbaycan Respublikası və onun vətəndaşlarının maraqlarına dərindən təsir edən əsaslı və dinamik dəyişikliklər yaşayır. Azərbaycan Respublikası bu prosesin fəal iştirakçısı və bütün sahələrdə mühüm potensiala və resurslara malik olmaqla yanaşı, dünyanın aparıcı dövlətləri ilə intensiv əlaqələr saxlayaraq regionda yeni reallıqların formalaşmasına mühüm təsir göstərir.

Milli maraqların təmin edilməsi üçün güclü təməli olan mili dövlətin mövcudluğu vacib şərtdir. Hər bir dövlətin milli təhlükəsizliyinin təminatı onun milli maraqları ilə, onların formalaşması isə bir çox faktorlarla (xüsusilə, milli dəyərlərlə) birbaşa bağlıdır və onun inkişafı uzun tarixi prosesdir. Milli maraqlar prosesi iqtisadi, sosial, etnopsixologiya və digər amillərin əsasında formalaşır [1, s.65] və dövlətin milli gücü ilə sıx bağlıdır.

Beynəlxalq münasibətlər sistemində hər bir ölkənin digərləri ilə yanaşı yaşamaq və bu zaman milli kimliyini qorumaqla müstəqil inkişafetmə imkanı onun milli gücü ilə şərtlənir. Bu baxımdan ölkənin milli gücünün qiymətləndirilməsi mühüm nəzəri və praktik əhəmiyyətə malikdir.

Digər siyasi-iqtisadi göstəricilər kimi milli gücün də qiymətləndirilməsi üçün müəyyən ölçmə sistemi tətbiq olunmalıdır. Nəzərdən keçirilən ölkənin dünya arenasındakı rolundan və milli təhlükəsizliyə qarşı ehtimal olunan təhdidlərdən çıxış edərək, belə fikir söyləmək olar ki, milli gücün qiymətləndirilməsi lokal və nisbi xarakter daşıya bilər. Yəni dünya hegemonluğuna iddialı dövlətlərin milli gücünün qiymətləndirilməsi onların resurs və potensiallarının ümumdünya göstəriciləri ilə həyata keçirilə bilər (məsələn, ölkənin hərbi xərclərinin dünya ölkələrinin ümumi xərclərində payı və s.).

Bu tədqiqatda həmin amilləri də nəzərə alaraq, milli gücün hesablanmasının daha mükəmməl düsturu təklif edilir:

$$\text{MG} = \text{Əh} + \text{Ər} + \text{ETT} \times (\text{İq} + \text{HG}) + \text{Sİ} + \text{GA}. \quad (1)$$

Burada,
- MG – milli gücü;
- Əh – əhalini;
- Ər – ərazini;
- ETT – elmi-texniki tərəqqini;
- İq – iqtisadiyyatı;
- HG – hərbi gücü;
- Sİ – siyasi iradəni;
- GA – geosiyasi amilləri ifadə edir.

Baxılan düsturda Əh, Ər, İq, HG, ETT, Sİ, GA ilə milli gücün formalaşmasına təsir edən əsas faktorlar sırasında əhalinin, ərazinin, iqtisadiyyatın, hərbi gücün, siyasi iradənin və geosiyasi amillərin aparıcı rola malik olduğu nəzərdə tutulmuşdur. ETT əmsalı elmi-texniki tərəqqinin səviyyəsini səciyyələndirir və göstərir ki, onun qiyməti yüksək olduqda, iqtisadi və hərbi güc faktorları milli gücün qiymətini əhəmiyyətli dərəcədə artırır.

R.S. Klayn [2], Ə. Davudoğlu [3], S. Qasımov [4] və digər alimlərin təklif etdiyi milli gücün düsturları kimi (1) düsturu da fəlsəfi xarakterə malikdir. Qeyd edilməlidir ki, bu düstura daxil olan komponentlərin ədədi qiymətləndirilməsi baxılan ölkənin milli gücünü hesablamağa və digər ölkələrlə müqayisə etməyə imkan verə bilər.

Bu məqalədə milli gücün hesablanması və müqayisəsi üçün qeyri-səlis qiymətləndirmə metodundan (şkalasından) istifadə etməklə müxtəlif faktorların ekspert rəyi əsasında müəyyənləşdirilən qiyməti əsasında milli gücü qiymətləndirmə mexanizmi təklif olunur.

Milli gücə təsir edən amillərin linqvistik dəyişənlərlə qiymətləndirilməsi

Humanitar elmlər sahəsində ənənəvi göstəricilərin ədədi qiymətləndirilməsi aktual olmadığından milli gücün hesablanması məqsədilə qeyri-səlis çoxluqlar nəzəriyyəsinin elementlərindən istifadə edilə bilər (məs., [5; 6]).

Qiymətləndirmə sisteminin əsasını tədqiqat obyektinə uyğun olaraq, miqyas və ya prioritetlər sistemi və onların müəyyənləşdirmə mexanizmi təşkil edir. Qeyri-səlis qiymətləndirmə, ilk növbədə ictimai-siyasi mülahizələrə söykənən məntiq əsasında qiymətləndirmə şkalasının təyin olunmasını nəzərdə tutur. Bu tip şkala universal, yaxud tədqiqat mövzusunun spesifikasına uyğun təyin oluna bilər. Tədqiqat obyektinin mahiyyətindən asılı olaraq, bu şkalanın dərəcələnmə, yaxud səviyyələndirmə şkalası şəklində tərtib edilməsi mümkündür.

Aşağıda (1) düsturuna daxil olan hər bir faktor linqvistik qiymətlər adlanan "yüksək", "orta", "kafi", "zəif" və "çox zəif" kimi beş səviyyə üzrə qiymətləndirilir.

Əhali faktoru. Bu faktorun milli gücə təsiri gənc və əmək qabiliyyətli əhalinin sayı, əhalinin ümumi artımda tempi, nikah və boşanma və s. göstəriciləri əsasında təsbit olunur.

2023-cü ildə Azərbaycan Respublikası əhalisinin sayı 10127.1 nəfər artmışdır. Gənc və əmək qabiliyyətli əhalinin sayında və ümumi artımda inkişaf meyillərinə (təbii artım) baxmayaraq, artım tempində azalma qeydə alınır. Azərbaycan Respublikasının əhalisinə əsas mənfi təsirlər isə nikah və boşanma göstəricilərindədir. Belə ki, Ədliyyə Nazirliyinin rayon (şəhər) qeydiyyat şöbələri tərəfindən cari ilin yanvar-noyabr ayları ərzində 49549 nikah və 19761 boşanma halı qeydə alınmışdır. Belə ki, 2022-ci ilin müvafiq dövrü ilə müqayisədə əhalinin hər 1000 nəfərinə nikahların sayı azalaraq, 6.2-dən 5.3-ə düşmüş, boşanmaların sayı isə 1.6-dan 2.1-ə qədər artmışdır [7].

2023-cü ilin 9 ayı ərzində ölkəyə 1 milyon 536 min 378 nəfər giriş, 1 milyon 533 min 47 nəfər isə çıxış etmişdir. Bu dövr ərzində 283 min 21 nəfər olduğu yer üzrə qeydiyyata alınmışdır. Məlumata görə, 2022-ci ilin müvafiq dövrü ilə müqayisədə 2023-cü il ölkə üzrə giriş-çıxış və olduğu yer üzrə qeydiyyat göstəricisi azalmışdır [8].

Beləliklə, Azərbaycan Respublikasının milli gücünün formalaşmasına təsir edən əhali faktoru "orta" linqvistik qiyməti ilə xarakterizə oluna bilər.

Ərazi faktoru. Bu faktorun milli gücə təsiri dövlətin geostrateji mövqeyi, nəqliyyat-kommunikasiya imkanları, zəngin yeraltı və yerüstü sərvətlərə malik olması, geosiyasi dəyərinin artması, ərazi və əhalisinin bir qisminin ölkənin materik hissəsi ilə birbaşa əlaqəsinin olmaması, dost olmayan dövlətlərin əhatəsində yerləşməsi kimi göstəricilərin əsasında təsbit olunur.

Azərbaycan Respublikasının geostrateji mövqeyinin əsas göstəriciləri onun 86.6 min kvadrat kilometr quru, 80 min kvadrat kilometr Xəzər dənizindəki milli su sektoruna, Avropa və Asiyanı birləşdirən avtomobil, dəmir yolu və su nəqliyyatı vasitəsilə Rusiya, Türkiyə, İran, Gürcüstan, Ermənistan, Orta Asiya və Qara dəniz bölgəsi ölkələri ilə nəqliyyat-kommunikasiya imkanlarına, həmçinin gözəl təbiətə, əlverişli iqlim şəraitinə, zəngin yeraltı və yerüstü sərvətlərə malik olmasıdır [9]. Qlobal aləmdə gedən son proseslər (Rusiya–Ukrayna müharibəsi) Orta Dəhliz üzərində yerləşən, böyük tarixi coğrafiyasından (Cənubi Azərbaycandan) zorla qoparılan və dünya azərbaycanlılarını bir araya gətirən yeganə vətən torpağı missiyasını yerinə yetirən Azərbaycan Respublikasının geosiyasi dəyərinin artmasına və xarici ölkələrlə münasibətlərinə müsbət təsir göstərən əsas amillərdən sayılır.

Bununla yanaşı, mürəkkəb, qeyri-sabit, dinamik, dəyişən və xarici təsirlərə açıq coğrafiyada yerləşən Azərbaycan Respublikasının dünya okeanlarına birbaşa çıxışının olmaması, kiçik əraziyə malik olması (coğrafi dərinliyinin olmaması), ərazi (5502.75 kvadrat km) və əhalisinin (461.5 min nəfər) (Naxçıvan Muxtar Respublikası) bir qisminin ölkənin materik hissəsi ilə birbaşa əlaqəsinin olmaması, Rusiya, İran və Ermənistan kimi dost olmayan dövlətlərin əhatəsində yerləşməsi həyati vacib çatışmazlıqlarındandır və onun güc faktoruna mənfi təsir göstərən əsas amillərdəndir.

Beləliklə, Azərbaycan Respublikası milli gücünün formalaşmasına təsir edən ərazi faktoru coğrafi güc olaraq, "kafi" linqvistik qiyməti ilə xarakterizə oluna bilər.

İqtisadiyyat faktoru. Bu faktorun milli gücə təsiri ümumi daxili məhsulun (ÜDM) həcmi, bank sektoru, strateji valyuta ehtiyatları, ölkəyə qoyulan investisiyaların ümumi həcmi, əməkhaqqı və pensiya göstəriciləri əsasında təsbit olunur.

Beynəlxalq Valyuta Fondu (BVF) 2023-cü ildə Azərbaycan Respublikasının ÜDM-nin artımını 2.4%, 2024–2028-ci illərdə isə illik 2.3% səviyyəsində proqnozlaşdırsa da [10], 2023-cü ildə ölkədə istehsal edilmiş ÜDM-nin həcmi əvvəlkinə nisbətən 1.1% artaraq, 123 005,5 milyon manat, neft sektorunda istehsalın həcmi 2022-ci illə müqayisədə 1.7% azalaraq, 45 343.7 milyon manat, qeyri-neft sektoru istehsalın həcmi 2022-ci illə müqayisədə 3.7% artaraq, 77 661.8 milyon manat və 2022-ci ildə qeyri-neft sektorunda yaradılmış ÜDM-nin artım tempi 9.1% olmuşdur [11, s.2].

"Fitch Ratings" beynəlxalq reytinq agentliyi Azərbaycanın bank sektorunun göstəricilərinin davamlı yaxşılaşmasını qeyd edir [12]. Belə ki, 2022-ci ildə bank sektorunda 914.5 milyon, 2023-cü ildə isə 18.5% yəni 1 milyard 84.2 milyon manat xalis mənfəət əldə etmişdir.

2023-cü ilin sonuna Azərbaycan Respublikasının strateji valyuta ehtiyatları 68.5 milyard ABŞ dolları təşkil etmişdir. Bu isə 2022-ci illə müqayisədə 17% çoxdur. 2022-ci il də daxil olmaqla, Azərbaycan Respublikası Mərkəzi Bankının strateji valyuta ehtiyatları 29.1% artaraq, 11.6 milyard ABŞ dollarına çatmışdır [13]. Azərbaycan Respublikası müstəqillik əldə etdikdən sonra ölkəyə qoyulan investisiyaların ümumi həcmi 300 milyard dollardan çox olmuşdur ki, bunun da təxminən 200 milyard dollarını qeyri-neft sektoruna qoyulan investisiyalar təşkil etmişdir [14].

Son 5 ildə ölkədə sosial sahədə minimum əməkhaqqı 2.7 dəfə artırılaraq, 130 manatdan 345 manata, minimum pensiya isə 2.5 dəfə artırılaraq, 110 manatdan 280 manata çatdırılmışdır [15]. Ölkədə ehtiyac meyarının 270 AZN olması, həmçinin sadalanan artımlar iqtisadi göstəricilərlə müqayisədə mənfi hal kimi qiymətləndirilə bilər.

Yuxarıda qeyd edilən faktorlarla yanaşı, ölkə iqtisadiyyatının karbohidrogen sektorundan yüksək asılılığının davam etməsi, bank sisteminin yüksək səviyyədə dollarlaşması və iqtisadi siyasətin proqnozlaşdırılmasının qeyri-kafi səviyyəsini mənfi hal kimi qeyd etmək mümkündür [12].

Beləliklə, Azərbaycan Respublikası üzrə milli gücün formalaşmasına təsir edən iqtisadiyyat faktoru "kafi" linqvistik qiyməti ilə xarakterizə oluna bilər.

Hərbi güc faktoru. Bu faktorun milli gücə təsiri orduda əsgər sayı, dövlətin təhlükəsizlik və müdafiə xərcləri (maliyyə vəziyyəti), Hərbi Dəniz Qüvvələri (HDQ) və Hərbi Hava Qüvvələrinin (HHQ) reytinqi, silah sənayesindəki texnoloji inkişafı, maddi-texniki imkanları, çevikliyi və Müdafiə Sənayesi Nazirliyinin hərbi təyinatlı məhsulun istehsalı kimi göstəricilərin əsasında təsbit olunur.

Azərbaycan Ordusu Quru Qoşunları (QQ), HHQ və HDQ-dən təşkil olunmuşdur. Azərbaycan Ordusunun şəxsi heyətinin tərkibi 126 min fəal və 300 min ehtiyatda olan hərbçilərdən ibarətdir [16].

Azərbaycan Respublikası hər il davamlı olaraq təhlükəsizlik və müdafiə xərclərini artırır. Stokholm Beynəlxalq Sülh Araşdırmaları İnstitutuna (SIPRI) istinadən 2021-ci ildə dünya üzrə Azərbaycan Respublikası ÜDM-də hərbi xərclərin ən yüksək payına malik ölkələr arasında beşinci yerdədir. Belə ki, hazırda SIPRI-nin məlumatına əsasən Azərbaycan Respublikasının hərbi xərclərinin ÜDM-də payı 5.3% təşkil edir [17]. SIPRI-dən hərbi xərclərə dair məlumatlar, sülhməramlı qüvvələr də daxil olmaqla, silahlı qüvvələr üçün bütün cari və əsaslı xərcləri özündə əks etdirən NATO tərifindən əldə edilmişdir.

Beynəlxalq hərbi gücə dair məlumatlar toplayan ABŞ-ın "Global Firepower" saytı 2023-cü il üçün bir çox meyarlar üzrə qiymətləndirmə əsasında hazırladığı siyahıda Azərbaycan Respublikasının HDQ 67-ci [18] və HHQ isə 57-ci yerdə qərarlaşmışdır [19].

"Global Firepower" 2023-cü ildə ən yüksək hərbi gücə malik ölkələrin siyahısında Azərbaycan Respublikasının Silahlı Qüvvələrini 145 ölkə içində 59-cu yerdə qiymətləndirmişdir [20]. Reytinqin tərtib olunması zamanı orduların silah sənayesindəki texnoloji inkişafı, maliyyə vəziyyəti, maddi-texniki imkanları və çevikliyi kimi cəhətlər əsas götürülür.

Hərbi faktorun milli gücə təsirini qiymətləndirmək üçün onu şərtləndirən amillərə diqqət edək. Bu amillər sırasında ölkənin ümumi əhali sayında silahlı qüvvələrin payı, hərbçilər arasında zabitlərin rolu, müasir tank və zirehli texnikanın miqdarı, ümum ordunun şəxsi heyətinin ruh yüksəkliyi, idarəetmə və silah arsenalında müasir texnologiyalarla təchizatın səviyyəsi və digərləri vardır.

Ölkənin müdafiə qabiliyyətinin və milli təhlükəsizliyinin daha da gücləndirilməsi məqsədilə ordunun maddi-texniki təchizatının müasirləşdirilməsi və hərbi potensialın artırılması ilə bağlı tədbirlərin davam etdirilməsi üçün 2024-cü ilin dövlət büdcəsində 3 milyard manat maliyyə təminatının yaradılması nəzərdə tutulur [21]. Bu ədəd 2023-cü ilə görə 6% çoxdur.

Azərbaycan Respublikasının Müdafiə Sənayesi Nazirliyində 1000-dən çox adda hərbi təyinatlı məhsul istehsal edilir ki, bu da İkinci Qarabağ müharibəsində Azərbaycan Ordusunun tələbatının böyük ölçüdə daxili istehsal hesabına təmin edilməsini mümkün etdi və yerli istehsal olan müasir silah-sursat və hərbi texnika, məhz 44 günlük Vətən müharibəsində ilk dəfə real döyüş vəziyyətində uğurla sınaqdan keçdi və Azərbaycan Ordusunun zəfər qazanmasında, həmçinin onun zəngin döyüş təcrübəsi əldə etməsində əhəmiyyətli rol oynadı. Bu faktor ordunun ümumi gücünə müsbət təsir edən vacib amillərdəndir.

Sülhməramlı qüvvələr də daxil olmaqla, silahlı qüvvələr üçün ayrılan bütün cari və əsaslı xərclər, silah sənayesindəki texnoloji inkişaf, maliyyə vəziyyəti, maddi-texniki imkan və çevikliyi kimi cəhətləri qalib Azərbaycan Ordusunun hərbi gücünü "orta" qiymətləndirməyə əsas verir.

Beləliklə, Azərbaycan Respublikası üzrə milli gücün formalaşmasına təsir edən hərbi güc faktoru "orta" linqvistik qiyməti ilə xarakterizə oluna bilər.

Geosiyasi amillər. Bu faktorun milli gücə təsiri Cənubi Qafqazda konfiqurasiyanın dəyişməsi, regionda Türkiyə–Rusiya tandemi, Rusiya–Ukrayna münaqişəsi, Qərbin Rusiya və İrana sanksiyaları, Avropa dövlətlərinin Azərbaycan Respublikasının karbohidrogen resurslarına ehtiyacının artması, dövlətin əsas geosiyasi resursları, diaspora və lobbi fəaliyyəti kimi faktorların əsasında təsbit olunur.
Cənubi Qafqaz regionunda son 30 ildə konfiqurasiyanın dəyişməsi və Türkiyə–Rusiya tandemi Azərbaycan Respublikasının İkinci Qarabağ müharibəsində qələbə qazanmasını təmin edən əsas xarici siyasi amil olmuşdur. Əgər bu cütlükdən Rusiya Federasiyası kənarlaşsa, o zaman tandem dağılacaq və bu faktor regionda yeni geosiyasi konfiqurasiyanın yaranmasına səbəb olacaqdır [22].

Rusiya–Ukrayna münaqişəsi, Rusiya və İranın Qərbin ağır sanksiyalarına məruz qalması amilləri geosiyasi sferada Azərbaycan Respublikasının mövqeyini gücləndirir. Belə ki, Qərbin Rusiya və İranın neft-qaz sektoruna tətbiq etdiyi sanksiya və embarqo siyasəti Avropanın Azərbaycan Respublikasının karbohidrogen resurslarına ehtiyacının artması faktoru rəsmi Bakının geosiyasi mövqeyinə müsbət təsir göstərir.

Qlobal layihələrin həyata keçirilməsində və beynəlxalq iqtisadi-siyasi proseslərdə Azərbaycanın aparıcı qüvvəyə çevrilməsi rəsmi Bakının mövqeyinin güclənməsi ilə müşayiət olunur və onu qlobal miqyasda qaz ixrac edən ölkəyə çevirir [23; s.88].

Azərbaycan Respublikasının İslam Əməkdaşlıq Təşkilatının, Türk Dövlətləri Təşkilatının, Qoşulmama Hərəkatının aktiv iştirakçısı olması, habelə Türkiyə, Pakistan və İsrail kimi müttəfiqlərə malik olması dövlətin əsas geosiyasi resurslarından sayılır.

Azərbaycan Respublikasının xarici ölkələrdə diasporasının yetərli qədər təsirli olmaması, həmçinin coğrafi baxımdan Rusiya, İran və Ermənistan kimi dövlətlərin əhatəsində yerləşməsi dövlətin milli gücünə mənfi təsir edən geosiyasi amillərdən hesab edilir.

Beləliklə, Azərbaycan Respublikası üzrə milli gücün formalaşmasına təsir edən geosiyasi amillərin rolu "orta" linqvistik qiyməti ilə xarakterizə oluna bilər.

Siyasi iradə. Bu faktorun milli gücə təsiri xarici siyasi təzyiq, müstəqil siyasət aparması, işğal faktı ilə barışmaması, ölkə ərazisində uzun müddət mövcud olan separatizmə son qoyması, Azərbaycanın dövlət sərhədlərinin və ərazi bütövlüyünün bərpa etməsi kimi göstəricilərin əsasında təsbit olunur.

Siyasi iradə siyasi şüurun və davranışın təzahür forması, subyektin daxili və xarici maneələri dəf etməklə, şüurlu şəkildə qarşıya qoyulmuş məqsədləri ardıcıl surətdə həyata keçirmək bacarığıdır. Dövlət başçılarının siyasi iradəsinin olmaması çox vaxt siyasi məsələlərin öz həllini tapmamasına səbəb olur.

Dövlətin xarici siyasəti daxili siyasətin davamıdır. Hazırda Azərbaycan Respublikasının xarici siyasəti öz bütövlüyü və müstəqilliyi ilə seçilir. Bunun da əsas səbəbi, təbii ki, güclü siyasi iradə faktorunun olmasıdır [24]. Azərbaycan Respublikası dünyada davam edən barışmaz geosiyasi mübarizə arenasında bütün güc mərkəzlərindən məsafəli qalmaqla, çoxvektorlu və müstəqil siyasət yeridir.

Prezident İlham Əliyevin siyasi iradəsi Azərbaycan Respublikasının Avrasiyanın ən uğurlu ölkələrindən biri kimi formalaşmasında həlledici amil olmuşdur. Bu barədə Xəzər Strateji Araşdırmalar İnstitutunun (Rusiya) baş direktoru İqor Korotçenko bildirmişdir: *"Azərbaycan Respublikasına misli görünməmiş xarici siyasi təzyiqlər edilməsinə baxmayaraq, bu cəhdlər uğurlu olmamışdır. Ölkədə vəziyyəti sarsıtmaq, Azərbaycan Respublikasına təsir etmək, Bakını manipulyasiya etmək üçün dövlətin tərkibində separatçı anklavın saxlanmasına yönəlmiş çox güclü mövqelər mövcud olsa da, 19-20 sentyabr 2023-cü ildə 24 saatdan az müddətdə Azərbaycan Respublikası lokal antiterror tədbiri keçirməklə, tam hərbi qələbə əldə etməsi reallığı rəqiblərini rəsmi Bakıya qarşı xarici təsir rıçaqlarından məhrum etdi"* [25].

Azərbaycan Respublikası ərazilərinin 20%-i işğal altında olduğu dövrdə İ. Əliyevə işğal faktı ilə barışın mesajları verilirdi [26]. Lakin o, bütün təzyiqlərə sinə gələrək dövlətin milli maraqlarını güzəştə

getməyərək, prinsipial mövqeyində qalaraq və güclü iradə nümayiş etdirərək, 30 il ərzində həll edilməyən Ermənistan–Azərbaycan münaqişəsini qısa zaman ərzində kökündən həll etmiş və ölkə ərazisində uzun müddət mövcud olan separatizmə son qoymuşdur [27]. Bununla da Azərbaycanın dövlət sərhədlərinin və ərazi bütövlüyünün bərpasına və regionda geosiyasi reallıqların Azərbaycan Respublikasının xeyrinə dəyişməsinə nail olmuşdur.

Beləliklə, Azərbaycan Respublikası üzrə milli gücün formalaşmasına təsir edən siyasi iradənin rolu "yüksək" linqvistik qiyməti ilə xarakterizə oluna bilər.

Elmi-texniki tərəqqi faktorunun milli gücün formalaşmasına təsiri ixtira və patentlərin göstəricilərinin dinamikası, dövlət büdcəsindən təhsil sektoruna ayrılan vəsait, ölkədə professor-müəllim heyətinin sayı, tam və orta təhsilli əhalinin sayı, Azərbaycan Respublikası alimlərinin beynəlxalq indeksli elmi jurnallarda dərc olunan məqalələr üzrə reytinq göstəriciləri əsasında təsbit olunur.

Elmi-texniki tərəqqi – elmin nailiyyətlərindən istifadə etməklə istehsalın texniki səviyyəsinin yüksəldilməsi, istehsal proseslərinin səmərə və keyfiyyətinin artırılması, insanların tələbatlarının daha yaxşı ödənilməsi məqsədilə müxtəlif sahələrdə elm, texnika və texnologiyanın tətbiqidir.

SSRİ-nin süqutundan sonra (xüsusilə, 1990-cı illərdə) alimlərin və yüksəkixtisaslı mütəxəssislərin elmi sferadan uzaqlaşaraq, yüksəkgəlirli başqa fəaliyyət sahələrinə axın etməsi, eyni zamanda beyin axınının xarici ölkələrə miqrasiyası, elmin nüfuzdan düşməsi və elmtutumlu istehsal müəssisələrinin tamamilə və ya qismən fəaliyyətinin dayandırması və s. kimi problemlər ölkədə elmin inkişafına mənfi təsir göstərmişdir.

Lakin 2000-ci ildə bu göstərici Azərbaycan Respublikası üçün 1.8%-ə qədər azalmışdır. Bu səbəbdən Dünya Bankının iqtisadçıları Azərbaycanı Respublikasını beyin axınının ən aşağı səviyyədə reallaşdığı ölkələr siyahısına daxil etmişdir [28].

Hazırda ölkədə ETT-nin yüksək səviyyədə olmamasının əsas səbəbi bu sferada tətbiq edilən stimullaşdırma sisteminin müasir tələblərə cavab verməməsi faktı dayanır. Dövlət büdcəsindən elmin inkişafına ayrılan vəsaitin optimal səviyyədə yüksəldilməsi bu sahənin populyarlaşmasına, elmi-tədqiqat işlərinin kəmiyyət və keyfiyyəti göstəricilərinin yüksəldilməsinə və gənc mütəxəssislər arasında elmə münasibətin radikal şəkildə dəyişməsinə gətirib çıxara bilər.

Azərbaycan Respublikasında 2010-2019-cu illər üzrə ixtiralarla bağlı mütləq göstəricilərin dinamikası düşməkdədir. Qüvvədə olan ixtira patentlərin sayı 2010-cu illə (496) müqayisədə 2019-cu ildə (236) aşağı düşmüşdür ki, bu da ixtiraçıların mühafizə sənədlərinin qüvvədə saxlanılma maraqlarının olmadığını və mövcud patentlərə tələbatın zəif olduğunu göstərir [29, s.16].

2024-cü il dövlət büdcəsindən təhsil bölməsi üzrə 102 tədbiri əhatə edən 10 proqramın həyata keçirilməsi üçün 4549.9 milyon manat məbləğində vəsaitin yönələcəyi proqnozlaşdırılıb. Bu ədəd 2023-cü illə müqayisədə 3.2% çoxdur [30].

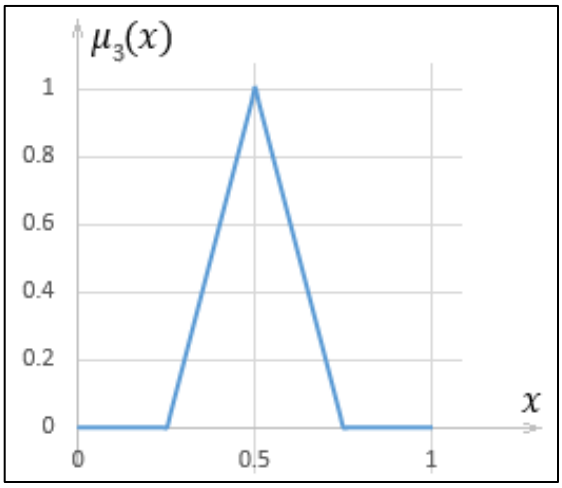
Qeyd etmək lazımdır ki, Dövlət Statistika Komitəsinin yaydığı məlumata görə, 2021-2022-ci tədris ili üçün ölkədə professor-müəllim heyətinin sayı 14393 nəfər təşkil edir [31]. 2023-cü il nəticələrinin əsasında Azərbaycan Respublikasının alimləri beynəlxalq indeksli elmi jurnallarda məqalə reytinqinə görə, "Scopus h-index 166, Web of Science h-index 145, Google Scholar h-index186"-cı yerdə qərarlaşmışdır [32]. Azərbaycan Respublikasında 15 və yuxarı yaşda olan əhalinin hər 1000 nəfərdən 974-nün tam və orta təhsilli olması [33] faktoru müsbət göstərici sayılır.

Beləliklə, Azərbaycan Respublikasının iqtisadi və hərbi potensialı üzrə elmi-texniki tərəqqinin nailiyyətlərindən istifadə əmsalı "kiçik" linqvistik dəyişəni ilə ifadə oluna bilər.

Milli gücün qeyri-səlis qiymətləndirilməsi

Milli gücün qiymətləndirilməsində yuxarıda təklif olunan (1) düsturuna riyazi məna vermək üçün ilk növbədə linqvistik dəyişənlərə uyğun qeyri-səlis ədədləri qurmaq lazımdır. Bu addım isə qeyri-səlisləşdirmə (fuzzification) adlanır. Mahiyyətinə görə, baxılan bütün faktorlar (əhali, ərazi, iqtisadiyyat, hərbi güc, siyasi iradə, geosiyasi amillər), həmçinin elmi-texniki tərəqqidən istifadə əmsalının daşıyıcısı eyni $[-0.25, +1.25]$ intervalında verilən qeyri-səlis ədədlərlə təyin edilə bilər.

Göstərilən faktorların qiymətləndirilməsində istifadə olunan "yüksək", "orta", "kafi", "zəif" və "çox zəif" linqvistik qiymətlərinə elmi-texniki tərəqqinin nailiyyətlərindən istifadə əmsalının qiymətləndirilməsi üçün istifadə olunan "böyük", "yaxşı", "qənaətbəxş", "kiçik" və "çox az" linqvistik qiymətlərini ekvivalent hesab etmək olar. Ona görə də onlara fərq qoymadan sadalanan linqvistik dəyişənlərə uyğun, qeyri-səlis ədədlərin mənsubiyyət funksiyalarını qurmaq mümkündür. Burada sadəlik üçün mənsubiyyət funksiyaları hissə-hissə xətti funksiya kimi verilir.



Şəkil 1. "Kafi" linqvistik qiymətinə uyğun qeyri-səlis ədədin mənsubiyyət funksiyasının qrafiki

"Yüksək" (böyük), "orta" (yaxşı), "kafi" (kafi), "zəif" (kiçik) və "çox zəif" (çox az) linqvistik qiymətlərinə uyğun olaraq, mənsubiyyət funksiyasını $j = 5, 4, 3, 2, 1$ kimi nömrələyirik. j ədədinin mənsubiyyət funksiyası aşağıdakı formada təyin edilir:

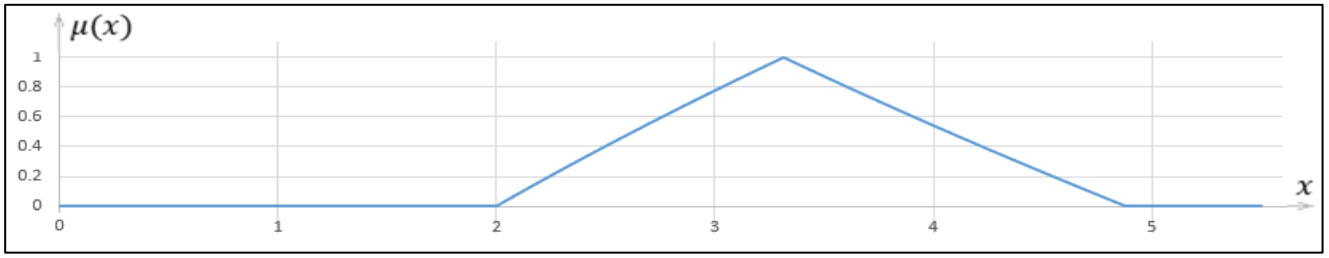
$$\mu_j(x) = \begin{cases} 0, & x \le (j-2)/4, \\ 4x + 2 - j, & (j-2)/4 < x \le (j-1)/4, \\ j - 4x, & (j-1)/4 < x \le j/4, \\ 0, & j/4 < x. \end{cases}$$

Nümunə üçün "kafi" qiymətinə uyğun qeyri-səlis ədədin mənsubiyyət funksiyasının qrafiki şəkil 1-də verilmişdir. (1) düsturunun komponentləri üzrə yuxarıda şərh olunmuş ekspert qiymətlərindən çıxış edərək, milli gücün qeyri-səlis ifadəsi üçün aşağıdakı mənsubiyyət funksiyası yazıla bilər:

$$\mu(x) = \mu_4(x) + \mu_3(x) + \mu_2(x) \times [\mu_3(x) + \mu_4(x)] + \mu_4(x) + \mu_5(x). \quad (2)$$

$\mu(x)$ funksiyasının qeyri-səlis ədədlər üzərində hesabi əməliyyatlar qaydasına uyğun olaraq, hesablanmış ifadəsi aşağıdakı şəkildə yazılır [5, s.97]:

$$\mu(x) = \begin{cases} 0, & x \le 2, \\ \sqrt{6.5625 + 8x} - 4.75, & 2 < x \le 3.3125, \\ -\sqrt{6.5625 + 8x} + 6.75, & 3.3125 < x \le 4.875, \\ 0, & 4.875 < x. \end{cases} \quad (3)$$



Şəkil 2. (2) düsturu üzrə hesablanan qeyri-səlis ədədin mənsubiyyət funksiyasının təsviri

Əyanilik üçün onun qrafiki şəkil 2-də verilir və burada görmək olar ki, $\mu(x)$ funksiyalarının daşıyıcısı $[-0.25, +6.25]$ intervalında təyin olunur. Bu intervalı əhatə edən qiymətləndirmə şkalası aşağıdakı kimi daxil edilmişdir:

$$\text{linqvistik dəyişən} = \begin{cases} \text{"çox zəif güc"} & əgər \quad \mu_o \leq 1, \\ \text{"zəif güc"} & əgər \quad 1 < \mu_o \leq 2, \\ \text{"orta güc"} & əgər \quad 2 < \mu_o \leq 3, \\ \text{"qənaətbəxş"} & əgər \quad 3 < \mu_o \leq 4, \\ \text{"yüksək güc"} & əgər \quad 4 < \mu_o \leq 5, \\ \text{"çox yüksək güc"} & əgər \quad 5 < \mu_o, \end{cases} \tag{4}$$

Nəticənin (4) şkalası üzrə linqvistik qiymətlərlə ifadəsi üçün (3) ədədinin defazzifikasiyası həyata keçirilməlidir. Bu məqsədlə mənsubiyyət funksiyasının məhdudlaşdırdığı intervalın mərkəzinə nəzərən defazzifikasiya tətbiq edilsə, (2) üzrə hesablanan ədədə uyğun olaraq, $\mu_o \approx 3.375$ alınır. Bu isə (4) şkalasına uyğun olaraq, qiymətləndirilən "qənaətbəxş" güc kimi xarakterizə olunur.

Beləliklə, milli gücün qiymətləndirilməsi üçün təklif olunan (1) formulu qiymətləndirilmə xarakterinə malik düstur olur.

Nəticə

Məqalədə dövlətin milli gücünün formalaşma strukturu – əhali, ərazi, iqtisadiyyat, hərbi güc, elmi-texniki tərəqqi, siyasi iradə və geosiyasi amillərin təhlili əsasında milli gücün hesablanmasının daha təkmil düsturu irəli sürülür və dövlətin gücü qeyri-səlis qiymətləndirmə metodu əsasında qənaətbəxş güc kimi xarakterizə olunur.

Həmçinin dövlətin milli gücünün əsasını təşkil edən bütün komponentlərin paralel və balanslı inkişafı daxili sabitliyi təmin edir, ölkənin beynəlxalq nüfuzunu möhkəmləndirir, onu regional güc mərkəzinə çevirir və qlobal miqyasdakı rolunu artırır.

Beləliklə, hər bir dövlət milli gücünü qiymətləndirməklə, öz daxili və xarici siyasətini mükəmməlişdirə və siyasi kursunu daha real əsaslarla gerçəkləşdirə bilər. Real milli gücə əsaslanmayan dövlət siyasəti təmin oluna bilməz və onu inkişafa deyil, tənəzzülə sürükləyər.

İstifadə edilmiş ədəbiyyat siyahısı

1. Məmmədzadə, V., İmamverdiyev, E. Milli maraqlar milli təhlükəsizliyin təmin olunması kontekstində // – Bakı: Elmi Əsərlər jurnalı, − 2023. № 3(21).− s. 65-69.
2. Cline, R. World Power Assessment 1977: A Calculus of Strategic Drift // – Colorado: Westview Press, − 1977. − 206 p.
3. Davutoğlu, A. Strateji derinlik. Türkiye'nin uluslararası konumu // – İstanbul: Kurtiş Matbaacılık, – 2010. – 584 s.
4. Qasımov, S. Azərbaycan Respublikasının Milli Maraqları Sistemində geosiyasi amil / siyasi elmlər üzrə fəlsəfə doktoru dis. avtoreferatı. / – Bakı: – 2017. – 29 s.
5. Klir, G.J., Bo, Y.. Fuzzy sets and fuzzy logic: theory and applications // – New Jersey: Prentice hall, –1995. – 574 p.
6. Emami, M.R., Turksen. I.B., Goldenberg, A.A. A unified parameterized formulation of reasoning in fuzzy modeling and control // – Fuzzy Sets and Systems, − 1999. − V. 108, − p. 59-81.
7. 2023-cü ilin 11 ayı ərzində qeydə alınan nikah və boşanmaların sayı bəlli oldu: [Elektron resurs] / – 17 yanvar 2024. URL: https://1news.az/az/news/20240117124439780-2023-cu-ilin-11-ayi-erzinde-qeyde-alinan-nikah-ve-boshanmalarin-sayi-belli-oldu
8. Bu il Azərbaycana giriş və ölkədən çıxış üzrə statistika açıqlanıb: [Elektron resurs] / – 16 noyabr 2023. URL: https://naxcivanxeberleri.com/public/index.php/bloq/bu-il-azerbaycana-giris-ve-olkeden-cixis-uzre-statistika-aciqlanib-24651

9. Həsənov, Ə. Azərbaycanın Milli Dövlət Quruculuğu və Geosiyasi İnkişaf Xarakteristikası: Keçilmiş Yol, Mövcud İmkanlar və Perspektivlər. // – Bakı: Geosiyasət jurnalı, − 2016. № 06 (36). – s.3-13.

10. Azerbaijan Staff Concluding Statement of the 2023 Article IV Mission: [Electronic resource] / – December 11, 2023. URL: https://www.imf.org/en/News/Articles/2023/12/11/mcs121123-azerbaijan-staff-concluding-statement-of-the-2023-article-iv-mission

11. Sənayenin əsas göstəriciləri: [Elektron resurs] / – URL:https://economy.gov.az/storage/files/files/6287/qGBwjvM7XWstYF9PdAnyzDCFxBfmBEKxhpxuMnvp.pdf

12. Fitch подтвердило рейтинг Азербайджана на уровне "BB+": [Электронный ресурс] / – 1 апреля, 2023. URL: https://www.interfax.ru/business/893938

13. Обнародована сумма стратегических валютных резервов Азербайджана: [Электронный ресурс] / – 31 января, 2024. URL: https://report.az/ru/finansy/obnarodovana-summa-strategicheskih-valyutnyh-rezervov-azerbajdzhana/

14. Президент Ильхам Алиев: Общий объем инвестиций в Азербайджан превысил 300 млрд долларов: [Электронный ресурс] / – 26 октябрь, 2023. URL:https://azertag.az/ru/xeber/prezident_ilham_aliev_obshchii_obem_investicii_v_azerbaidzhan_prevysil_300_mlrd_dollarov-2802391

15. Minimum əməkhaqqı 345 manata çatdırıldı, Vahid Tarif Cədvəli üzrə əməkhaqları artırıldı: [Elektron resurs] / – 5 yanvar 2023. URL: https://sosial.gov.az/media/xeberler/Minimum-emekhaqqi-345-manata-catdirildi-Vahid-Tarif-Cedveli-uzre-emekhaqlari-artirildi_644009?hl=az

16. Azerbaijan leader in South Caucasus for military power index: [Electronic resource] / – January 18, 2021. URL: https://www.azernews.az/nation/175160.html

17. SIPRI Fact Sheet. Trends In World Military Expenditure: [Electronic resource] / – April, 2022. URL: https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf

18. Dünyanın ən güclü donanmalarının 2023-cü il siyahısı – Türkiyə və Azərbaycan donanmaları neçənci yerdədir?: [Elektron resurs] / – 6 noyabr 2023. URL: https://ordu.az/az/news/290088/dunyanin-en-guclu-donanmalarinin-2023-cu-il-siyahisi--turkiye-ve-azerbaycan-donanmalari-necenci-yerdedir-

19. Hərbi Hava Qüvvələri Reytinqi: [Elektron resurs] / – 18 avqust 2023. URL: https://transqafqaz.com/h%C9%99rbi-hava-quvv%C9%99l%C9%99ri-reytinqi/

20. 2024 Azerbaijan Military Strength: [Electronic resource] / – May 1, 2024. URL: https://www.globalfirepower.com/country-military-strength-detail.php?country_id=azerbaijan

21. Gələn il üçün müdafiə və milli təhlükəsizlik xərcləri açıqlanıb: [Elektron resurs] / – 21 sentyabr 2023. URL:https://azertag.az/xeber/gelen_il_uchun_mudafie_ve_milli_tehlukesizlik_xercleri_achiqlanib-2757235

22. Türkiyə-Rusiya tandemi, qələbəmizi təmin edən əsas xarici siyasi amil oldu –Tofiq Zülfüqarov: [Elektron resurs] / – 4 yanvar 2021. URL: https://visiontv.az/article/turkiye-rusiya-tandemi-qelebemizi-temin-eden-esas-xarici-siyasi-amil-oldu-tofiq-zulfuqarov

23. 23. Məmmədzadə V., İskəndərov X. Azərbaycanın enerji siyasəti və transregional layihələrinin təhlükəsizliyi // – Bakı: Milli Təhlükəsizlik və Hərbi Elmlər jurnalı, − 2019. № 3. Cild 5, − s. 82-90.

24. Речь Ильхама Алиева на пятом совещании руководителей органов дипломатической службы Азербайджана: [Электронный ресурс] / – 7 июля 2014. URL: https://president.az/ru/articles/view/12392

25. Политическая воля Президента Ильхама Алиева стала решающим фактором в становлении Азербайджана одной из самых успешных стран Евразии – Игорь Коротченко: [Электронный ресурс] / – 7 ноября, 2023. URL: https://turkic.world/ru/articles/politics/166554

26. İlham Əliyev: "Biz istənilən halda axıra qədər gedəcəyik, məqsədimiz dəyişməz qalır": [Elektron resurs] / – 11 oktyabr 2020. URL: https://1news.az/az/news/20201011030745817-Ilham-Eliyev-Biz-istenilen-halda-axira-qeder-gedeceyik-meqsedimiz-deyishmez-qalir

27. Президент: Сепаратизму на наших землях положен конец, это – показатель нашей сильной политической воли: [Электронный ресурс] / – 29 сентября 2023. URL:https://report.az/ru/vnutrennyaya-politika/prezident-separatizmu-na-nashih-zemlyah-polozhen-konec-eto-pokazatel-nashej-silnoj-politicheskoj-voli/

28. Dünyada və Azərbaycanda Beyin Axını (Brain Drain, World and Azerbaijan): [Elektron resurs] / – July, 2018. URL:https://www.researchgate.net/publication/326583840_Dunyada_v_Azrbaycanda_Beyin_Axini_Brain_Drain_World_and_Azerbaijan

29. Azərbaycan Respublikasının Əqli Mülkiyyət Agentliyi. Azərbaycanda ixtiraçılıq və patent analitikası / – Bakı: – 2020. − 88 s.: [Elektron resurs] / URL:https://copat.gov.az/docs/Nesrler/AZE/%C6%8Fqli%20M%C3%BClkiyy%C9%99t/Ixtira%C3%A7%C4%B1l%C4%B1q_v%C9%99_patent_analitikas%C4%B1_az.pdf?_t=1619523881

30. Azərbaycanda elm və təhsilə ayrılan vəsait ilbəil artır. "Davamlı Artım Ölkədə Bu Sahənin Prioritet Olduğunu Göstərir": [Elektron resurs] / – 27 oktyabr, 2023. URL: https://525.az/news/240533-azerbaycanda-elm-ve-tehsile-ayrilan-vesait-ilbeil-artir

31. On dörd mindən çox professor olan ölkədə elmin səviyyəsi – Yeni qaydalar nəyi dəyişəcək: [Elektron resurs] / – 9 yanvar 2023. URL: https://sputnik.az/20230109/on-dord-minden-cox-professor-olan-olkede-elmin-seviyyesi---yeni-qaydalar-neyi-deyisecek-450282645.html

32. Azerbaijan National H-index Ranking 2023: [Electronic resource] / URL: https://az.h-index.com/az

33. Əhali. Azərbaycanın demoqrafik göstəriciləri: [Elektron resurs] / – 28 noyabr 2023. URL: https://stat.gov.az/source/demoqraphy/

Аннотация

Метод оценки национальной мощи государства

Вугар Мамедзаде, Эльхан Сабзиев, Асад Рустамов,
Эльджан Имамвердиев, Джалил Гасанов

В статье анализируются национальная мощь (НМ) государства и его формирующие структурные компоненты, включающее в себя население (Нас), территория (Терр), экономика (Экон), военная мощь (ВМ), научно-технический прогресс (НТП), политическая воля (ПВ) и геополитический фактор (ГФ). Согласно правилам, проводится оценка национальной мощи государства и предлагается его новая формула. Для перечисленных факторов, используемых по языковым значениям оценки - «высокий», «умеренный», «достаточный», «слабый» и «очень слабый», эквивалентно принимаются как лингвистическая оценка «отличный», «хороший», «удовлетворительный» «слабый» и «очень слабый». Целью исследования является оценка национальной мощи на основе экспертного мнения Азербайджанской Республики с использованием шкалы нечетких чисел. Соответственно, в статье ставится следующая задача: разработка механизма оценки национальной мощи государства. Использованы методы исследования: сравнительный анализ, анализ-синтез и математическое моделирование. Были получены следующие результаты: в статье на основе структурного анализа формирования национальной мощи государства предложена более совершенная формула расчета национальной мощи ($НМ = Нас + Терр + НТП \times (Экон + ВМ) + ПВ + ГФ$) Азербайджанской Республики характеризуется как удовлетворительная сила на основе нечеткого метода оценки. Вывод: каждому государству необходимо оценить свою реальную национальную мощь, чтобы усовершенствовать свою внутреннюю и внешнюю политику и эффективно реализовать свой политический курс на более реалистичной основе.

Ключевые слова: национальная мощь, население, территория, экономика, военная сила, политическая воля, геополитический фактор, научно-технический прогресс, метод нечеткой оценки

Abstract
Method for Assessing the National Power of the State
Vugar Mammadzada, Elkhan Sabziyev, Asad Rustamov,
Eljan Imamverdiyev, Jalil Hasanov

In the article, the national power (NP) of the state and the structural components that form it are population (Pop), territory (Terr), economy (Econ), military power (MP), scientific and technical progress (STP), political will (PW) and geopolitical factors (GF) is analyzed and put into the form of a formula by considering the rules of calculation. According to the "high", "moderate", "sufficient", "weak" and "very weak" linguistic values used for the evaluation of the listed factors, "great", "good", "satisfactory" used in the evaluation of the coefficient of use of the achievements of scientific and technical progress ", "small" and "very small" linguistic values are taken as equivalent. The purpose of the research work is to evaluate the national power of the Republic of Azerbaijan on the basis of expert opinion using a scale of fuzzy numbers. Accordingly, the following task is set in the article: development of a mechanism for assessing the national power of the state. Research methods are used: comparative analysis, analysis-synthesis, mathematical modeling. The following results were obtained: the article proposes a more advanced formula for calculating national power based on the structural analysis of the formation of the state's national power ($NP = Pop + Terr + STP \times (Econ + MP) + PW + GF$) and the power of the Republic of Azerbaijan as a satisfactory power based on the fuzzy assessment method it is characterized. The bottom line: each state needs to assess its real national power in order to perfect its domestic and foreign policy and effectively implement its political course on a more realistic basis.

Keywords: national power, population, territory, economy, military power, political will, geopolitical factor, scientific and technical progress, fuzzy evaluation method

Məqalə redaksiyaya daxil olmuşdur: 29.02.2024
Təkrar işlənməyə göndərilmişdir: 11.03.2023
Çapa qəbul edilmişdir: 08.04.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 45-51
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 351/354 DOI: 10.30546/9878.2024.2.10.0017.

THE WAY OF ACHIEVING STRATEGIC ENDS IN THE COMPLEX ENVIRONMENT – POSITIONAL SUPERIORITY MODEL

Colonel Elnur Alasgarli
National Defence University
elnuralasgarli@yahoo.com

Abstract. The changing, uncertain, complex and ambiguous characteristics of the strategic environment in the modern era often lead to the failure of activities carried out to achieve strategic goals. This requires the review of approaches to strategy formulation, including the strategy model, which is used as a tool for achieving strategic goals. Given the interconnectedness of strategies with the environment in which they are implemented, a new approach and model is required to reflect the characteristics of the modern strategic environment and allow the actor's flexible actions.

The similarity of the characteristics of the virtual environment formed in the game of chess and the real security environment shows that this game can be considered for the formulation of a new strategy model. In addition, in the game of chess, the focus of the main efforts is not on the strategic goal, but on the superior position that helps to achieve it, the consistent application of strategy and tactics, and the possibility of changing the initial strategic goal in the course of the game can play an important role in ensuring the flexibility of the model to be developed.

In the preparation of the model, the activities carried out by the Republic of Azerbaijan on the restoration of its territorial integrity are used as an example. This shows the possibility of applying the mentioned model in the formulation of a real strategy.

Keywords: national security, strategy, tactics, positional superiority, global security environment

Introduction

Every country implements strategic activities based on different approaches to ensure its security and sustainable development within the framework of its national interests. One of them is strategy. With optimal management, a well-designed strategy can concentrate common efforts on the main goal, use resources efficiently and purposefully, and provide conditions for strategic impact at the right time. In addition, having a strategy allows actors to anticipate and respond to changes in the competitive environment.

However, a strategy is implemented in an environment that contains factors beyond the control of those who develop it. For this reason, in order to be successful, a developed strategy must meet the characteristics of the environment formed by those factors. Constantly increasing complexity of the environment can be considered one of the biggest obstacles to development and implementation of the strategy.

Important changes are currently taking place in the global security environment. The number of actors and trends affecting the security environment in the world is increasing day by day. Strategic processes such as globalization, rapid technological development and the increasing irregularity of relations between the world's leading states that influence each other, further complicates the global security environment by increasing uncertainty. It is not a coincidence that the Secretary General of the United Nations, A. Guterres, noted at the Environmental Security Conference that a more complex and dangerous environment is being formed in the world [1].

The increasing level of complexity of the security environment negatively affects [2, p.52] the implementation of strategies developed based on the traditional "Ends, Ways, Means" strategy-making model. This approach is basically designed for clear or complicated environments rather than complex ones. Recent events show that the traditional strategy-making model based on goal-oriented, linear approach has limitations in coping with modern challenges [3, p.38].

Due to the complexity of the security environment, tactical actions are increasingly being used as another approach to achieve the ultimate goals, nowadays. However, they bring more short-term solutions, which are insufficient in achieving long-term strategic goals, and do not provide a comprehensive and systematic approach to the issue.

In general, the abovementioned approaches are accompanied by significant weaknesses either by not reflecting the dynamic and increasingly complex nature of the current environment [4, p.8] or by not being sufficient in achieving long-term strategic goals in the modern era. Each environment-specific problem becomes increasingly difficult to answer with the strategy-making approach used for a simpler environment.

The current state of the modern security environment requires the application of flexible approaches to the implementation of strategic activities.

The continuous complication of the global security environment and its complex character requires the application of more flexible approaches to achieve the strategic ends.

I. The basis of a new approach

To develop a strategy that reflects the characteristics of a complex security environment the game theory, especially the game of chess, which has been successfully tested in virtual practice to make a strategy, can be used as a new model. Its strategy-making philosophy based on the concept of "positional advantage" [5, p.32], the method of achieving the end state can provide prominent ways in this regard.

Similarities between the virtual environment created in the game and the modern real environment in terms of complexity, and the fact that they both require serious planning are the main reasons for choosing it as a model. In chess, the number of possible combinations increases after each move and calculation becomes more difficult, which makes the establishment of a superior position the purpose of strategy instead of checkmate. The high level of uncertainty in the security environment theoretically shows the possibility of applying this approach to achieve strategic ends in the modern era.

1.1. Components of the superiority

The increasingly intertwining socio-political, economic and military processes, since the beginning of the 21st century, the requirement of more collaborative [6, p.302] action rather than coordination and interaction especially in the current complex security environment stipulates the creation of positional superiority not in the areas, but in specific directions, depending on the characteristics of the main object of the strategy.

However, it is important to prioritize the areas of actions to increase the efficiency of the strategy to be prepared and to harmonize joint efforts in the complex strategic environment. Considering the resolution of the conflicts, the foreign policy, economy, military, social public and information fields can be defined as associated areas of ensuring national interests (Figure 1).

Figure 1. Areas of action

On the other hand, identifying specific directions will contribute to the synchronic application of the force, space and time elements of the strategy and to the simultaneous acquisition of superiority in different areas in order to create the necessary strategic impact.

Considering the characteristics of modern conflicts, its external and internal aspects, as well as the opponent, the formation of opinion, the creation of a strong side and unbalancing an opponent can be determined as the directions of action covering the actual issues that can create appropriate conditions for joint action.

The analysis of the Karabakh conflict allows us to say that the Republic of Azerbaijan has been implementing a complex of long-term and purposeful measures in these areas of activity. The following examples can be considered some of those activities:

– One of the successful elements of Azerbaijan's foreign policy during the Second Karabakh war was the formation of an opinion. Activities in this direction included gaining foreign and domestic support for the de-occupation of Azerbaijani territories, the return of internally displaced people to their native lands, and the need for a possible military operation to restore justice. By persuasively conveying its position on the issue Azerbaijan managed to get most countries of the world to accept that Karabakh is the historical territory of Azerbaijan. This also created the legal grounds for the liberation of Karabakh and adjacent 7 regions which were occupied during the First Karabakh war.

– Taking into account the characteristics of modern warfare, while ensuring the necessary combat readiness of the Armed Forces, the Republic of Azerbaijan has managed to create strong sides by developing certain military capabilities that had a serious impact on the course of the military operations. New methods combat activities, including Special Forces on the battlefield, as well as modern technologies such as armed UAVs and high-precision strike systems are a few examples. It is no coincidence that foreign experts say that the Azerbaijani side bought certain types of weapons on purpose in the last ten years, prepared selected units for use in special types of operations, and prepared a joint operational plan in order to isolate the battlefield [7].

– The Azerbaijani side purposefully and effectively used all the opportunities affecting its economic potential to reduce the budget revenues that could be directed to the development of the defense potential of Armenia. Azerbaijan has succeeded in preventing Armenia's economic development by excluding it from important international projects, including the oil and gas pipelines from Azerbaijan to Turkey and Europe, the railway line connecting China to Europe, communications connecting Iran and Russia, or by making its projects unpromising. At the same time, the closure of the borders with Turkey has given an additional impetus to the isolation of Armenia, hence the deterioration of its economic situation and emigration. Armenia's poor economic situation and lack of human resources did not allow it to strengthen militarily, which became one of the main factors determining its defeat in the war.

Positional superiority is created by gaining a decisive advantage over the opponent. This involves convincing the opponent that the continuation of the conflict is ineffective, creating a significant deterrence and prompting the rational opponent to make the desired decision on the resolution of the conflict. In some cases, the advantage created in chess forces the opponent to resign without waiting for the end. Sometimes the created superior position for various reasons may not be enough to force the irrational opponent to resolve the conflict. This determines the transition to the next stage, the realization of superiority through military operations. For example, the superiority created by the Republic of Azerbaijan was not enough to force the Armenian authorities to hand over the occupied territories peacefully. The Armenian side fell into the illusion that its army is invincible and its allies will protect it. Therefore, instead of trying to solve the problem they continued the provocations on the ground and by presenting the concept of "new war for new territories" [8] and the strategy of "active deterrence" [9]. Finally, Armenia's military provocation on September 27, 2020 forced Azerbaijan to realize its positional advantage.

1.2. The model of reaching the end state

New strategy-making model can be formulated by taking into account the conceptual basis of the complex strategic environment and the characteristics of the chess game. This time, the stages of chess can be transformed into stages of the model. The game of chess consists of the opening, midgame and endgame stages. The opening stage mainly involves the strengthening of the existing position, as well as the preparations for creating a superior position with dual-purpose attacks. Based on created position in the midgame, activities are carried out to achieve a decisive superiority over the opponent for the endgame, and to achieve the main goal at the end of the game. For this reason, the stages of "Establishing positional superiority", "Realization of superiority" and "Achieving strategic ends" can be defined in sequence (Figure 2).

In terms of application in real strategy, the position created at the end of the opening game is called "Positional superiority", and the position in the midgame is called "Special superiority". So, sometimes the created Positional superiority may not be enough to push the unrealistic actor to resolve the existing conflict for various reasons. This also necessitates the transition to the next stage, the creation of a special superiority. Here, positional superiority includes a complex of non-military activities, while special superiority includes military actions.

Figure 2. Modelling the game of chess

A strategy and tactics are used to achieve the end state in the game of chess. Here, strategy is used to create an advantage, while tactics are used to achieve a strategic goal using an existing advantage. Positional advantage created as a result of good strategic play lays bases for tactical action by presenting new opportunities.

In chess, there are many cases where advantage is created by tactical activities. However, this can lead to the desired result either against a very weak opponent or if the opponent makes a mistake. Against a strong opponent, this approach is considered to be unsuccessful. Besides, separate tactical successes unaligned with strategic goals may not be enough to achieve the end state. There is a need for a strategy to ensure that the actions are moving in the right direction.

It might be the case in real-time strategies as well. In today's security environment, tactical activities can be more focused on immediate targets and have a short-term strategic impact. However, it is important to align tactical successes with strategic goals to ensure that resources are being used effectively and that the organization is moving towards its desired end state.

For example, the superior position established by the Republic of Azerbaijan, during the Second Karabakh War, has created a foundation for the strategic goal of ensuring its sovereignty throughout the

country. In this context, Azerbaijan's initiative to conclude a peace agreement with Armenia can be evaluated as tactical activity arising from a superior position.

In order to create positional superiority, strategic objectives are defined in the directions of activity. At this time, they are formed based on the transformation of the end state by adapting it to the current realities. However, the end state is always kept in mind during the implementation of the strategy. This will play the role of a lighthouse, preventing activities from deviating from it and guiding the determination of the next steps.

The strategic objectives of positional superiority differ significantly from the medium-term objectives of traditional strategies. Thus, achieving the medium-term objectives of traditional strategies only provides an opportunity to advance to the main goal. However, positional superiority can be used to achieve different goals. For example, the superior position achieved by the Republic of Azerbaijan as a result of the Second Karabakh war created a basis for pursuing a different strategic goal, such as forming its more reliable partner status capable of diversifying Eurasian transport and communication connections in an unstable world. In this context, Azerbaijan's initiative to open the Zangezur corridor can be evaluated as strategic activity arising from a superior position.

Conclusion

Strategy is one of the approaches used to achieve strategic goals. Since it is implemented in an environment that contains factors beyond the control of those who develop it, the success of the strategy is closely related to its adequacy to the characteristics of that environment. In the modern era, the degree of complication of the global security environment is continuously increasing and becoming complex that negatively affects the success rate of strategies developed based on traditional approaches designed for simpler environments. Currently, a more flexible approach is required to achieve strategic goals.

The similarity between the characteristics of the modern security environment and the virtual environment of chess makes it possible to develop a new approach based on this strategy game. Its strategy-making philosophy of concentrating the main efforts not on the strategic goal, but on the strategic objectives of superior position, achieving the end state not only with strategy, also with tactical activities, and presenting an opportunity to change strategic goals in the implementation process are the main features that distinguishes this approach from others. In the framework of the new approach, strategy is used to create a superior position, and tactical activities are used to achieve the end state. Depending on the situation, gained superiority can be used to achieve either the original or different strategic goal.

In the study, the activities carried out by the Republic of Azerbaijan during the Second Karabakh War, before and after it to ensure the territorial integrity and sovereign rights in all its territories are analyzed from the perspective of the positional superiority approach. It can be said that to achieve its strategic goals, the Republic of Azerbaijan first established a positional advantage, then realized it in the war against an irrational opponent, and pursued its ultimate and other strategic goals by tactical activities.

In general, it is evaluated that the presence of an appropriate approach to developing a strategy for each level of the environment will facilitate the successful implementation of strategies. In this regard, the application of a superiority-based approach, and consistent use of strategy and tactics to achieve the end state could provide the necessary flexibility to meet the requirements of a complex security environment characterized by its dynamism and high uncertainty.

References

1. UN Secretary-General press release. “Threat to Global Security More Complex, Probably Higher Than during Cold War, Secretary-General Warns Munich Security Conference”: [Electronic resource] / – Munich, Germany. – 18 February, 2022. –
URL: https://press.un.org/en/2022/sgsm21146.doc.htm

2. Ivančić, V. Strategy implementation – external environment alignment / V.Ivančić, M.Ivan, L.Jelenc, Ž.Dulčić // – Croatia: Management: journal of contemporary management issues – 2017. №22. – p.51-67.

3. Alasgarli, E. How much successful the traditional strategy-making models in the contemporary strategic environment? The analysis of the Ends, Ways and Means formula // –Romania: Journal of Defense Resources Management (JoDRM) – 2019. №2. – p. 30-39.

4. . Cerami, J.R. Holcomb, J.F. Jr. US Army War College Guide to Strategy / – Carlisle, PA: Strategic Studies Institute, – 2001. – p.8.

5. Lasker, E. Common sense in chess / E.Lasker – New York: Dover Publications, – 1965. – p.43.

6. McLeod, J., Childs, S. The Cynefin framework: A tool for analyzing qualitative data in information science? // – Norman, Oklahoma, United States of America: Library & information science research – 2013. №4(35). – p. 299-309.

7. Gressel, G. Military lessons from Nagorno-Karabakh: Reason for Europe to worry The European Council on Foreign Relations (ECFR): [Electronic resource] /– November 24, 2020. URL: https://ecfr.eu/article/military-lessons-from-nagorno-karabakh-reason-for-europe-to-worry/

8. Wilson, J. Caucasus: Armenia's New war for new territories: [Electronic resource] / –July 2, 2020. URL: https://www.euractiv.com/section/azerbaijan/opinion/caucasus-armenias-new-war-for-new- territories/

9. Abramyan, E. Rationalizing the Tonoyan Doctrine: Armenia's Active Deterrence Strategy: [Electronic resource] / – May 2, 2019. URL: https://jamestown.org/program/rationalizing-the-tonoyan-doctrine-armenias-active-deterrence-strategy

Xülasə

Kompleks mühitdə strateji məqsədlərə nail olmanın yolu –
mövqe üstünlüyü modeli

Elnur Ələsgərli

Müasir dövrdə strateji mühitin dəyişkən, qeyri-müəyyən, kompleks və müxtəlif cür yozula bilən xüsusiyyətləri strateji məqsədlərə nail olmaq üçün həyata keçirilən fəaliyyətlərin sıxlıqla uğursuz olmasına gətirib çıxarır. Bu da strateji məqsədlərə nailolma aləti kimi istifadə edilən strategiyanın hazırlanması üzrə yanaşmaların, o cümlədən strategiya modelinin nəzərdən keçirilməsini şərtləndirir. Strategiyaların icra olunduğu mühitlə sıx bağlılığını nəzərə alsaq, yeni yanaşma və modelin müasir strateji mühitin xüsusiyyətlərinə və aktorun çevik fəaliyyətinə uyğun olmasını tələb edir.

Real təhlükəsizlik mühiti və şahmat oyununda formalaşan virtual mühitin xüsusiyyətlər baxımından oxşarlığı şahmat oyunundakı əsas məqsədə nailolma üsulunun yeni strategiya modeli kimi nəzərdən keçirilməsini şərtləndirir. Bu halda əsas səylərin strateji məqsədə deyil, ona nail olmağa kömək edən üstün mövqeyə yönəlməsi, strategiya və taktikanın ardıcıl tətbiqi, ilkin strateji məqsədin dəyişdirilməsinin mümkünlüyü hazırlanacaq modelin çevikliyinin təmin edilməsində mühüm rol oynaya bilər.

Modelin hazırlanmasında Azərbaycan Respublikası tərəfindən ərazi bütövlüyünün bərpa edilməsi və qorunub saxlanması məqsədilə həyata keçirilən fəaliyyətlər əsas götürülür. Bu isə sözügedən modelin həqiqi strategiyanın formalaşdırılmasında tətbiqinin mümkünlüyünü göstərir.

Açar sözlər: milli təhlükəsizlik, strategiya, taktika, mövqe üstünlüyü, qlobal təhlükəsizlik mühiti

Аннотация

Достижение стратегических целей в комплексной среде –
модель позиционного превосходства

Эльнур Алескерли

Изменчивый, неопределенный, комплексный и неоднозначный характер стратегической среды в современном этапе часто приводит к провалу мероприятий, осуществляемых для

достижения стратегических целей. Это требует пересмотра подходов к формулированию стратегии, в том числе модели стратегии, которая используется как инструмент достижения стратегических целей. Учитывая взаимосвязь стратегий со средой, в которой они реализуются, необходимы новый подход и модель, отражающие характеристики современной стратегической среды и позволяющие гибкие действия актора.

Сходство характеристик виртуальной среды, формируемой при игре в шахматы, и реальной среды безопасности заставляет рассматривать способ достижения основной цели в игре в шахматы как новую модель стратегии. В этом случае важную роль в обеспечении гибкости могут сыграть сосредоточение основных усилий не на стратегической цели, а на превосходящей позиции, способствующей ее достижению, последовательное применение стратегии и тактики, возможность изменения исходной стратегической цели. модели, которую предстоит разработать.

При подготовке модели за основу взяты мероприятия, осуществляемые Азербайджанской Республикой в целях восстановления и сохранения территориальной целостности. Это показывает возможность применения указанной модели при формулировании реальной стратегии.

Ключевые слова: национальная безопасность, стратегия, тактика, позиционное преимущество, глобальная среда безопасности.

Məqalə redaksiyaya daxil olmuşdur:16.04.2024
Təkrar işlənməyə göndərilmişdir: 22.04.2024
Çapa qəbul edilmişdir: 03.05.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 52-61
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 355/359 DOI: 10.30546/9878.2024.2.10.0021.

GEOPOLITICAL AND MILITARY-STRATEGIC ASPECTS OF RUSSIAN-UKRAINIAN WAR

ScD in History, Professor Nurulla Aliyev
Military Scientific Research İnstitute
nurullaliyev@mail.ru

Lieutenant Colonel Anar Musayev
Military Scientific Research İnstitute
anar_az83@yahoo.com

Abstract. The article shows the growing importance of the Black Sea-Caspian region with the historical development of human civilization and outlines the history of the struggle of the leading world powers, whose geostrategic interests intersected in this region. An assessment is made of the geopolitical rivalry between modern emerging geostrategic centers in the Black Sea-Caspian basin for the right to control the situation in it. The article analyzes military-political events in the conditions of the Russian-Ukrainian war, revealing its geopolitical and military-strategic aspects. The purpose of the study is to assess the geopolitical sphere and methods of geopolitical struggle for control over oil and gas pipelines passing through the region, transport corridors and communication lines. In the course of studying this problem, the main responsibilities were the analysis of the geopolitical processes taking place in the Black Sea-Caspian region and its historical aspects, the main goals of the rivalry between the leading world powers in the Russian-Ukrainian war. The article used historical, chronological and comparative research methods to reveal the problem posed. In the final part of the article, it is predicted that the Russian-Ukrainian war, acting as a factor in the formation of a new world order, will allow the balance of forces to be distributed between geopolitical centers.

Keywords: modern world order, regional security, natural resources, socio-political system

Introduction

At the end of the 20th century, with the collapse of the USSR, a number of changes occurred in the world. With the end of the Cold War, the main centers of power in international relations decided to adapt their activities to existing conditions, based on new geopolitical realities and, along with the collapse of the old system of international relations, they began to create the foundations of a new world order. These transnational processes, as in other post-Soviet republics, have confronted the Ukrainian state with the task of formulating, creating and implementing a general strategy for its own national development and security policy. However, the Russian-Ukrainian war changed the global geopolitical landscape, political geography and ideological foundations of the world order, and due to all its indicators and cumulative nature, increased the risk of this conflict moving into the phase of the Third World War [1].

Russia's military intervention in Ukraine, which began on February 24, 2022, is considered the largest war that occurred in Europe after World War II and caused major changes in the global and regional war security system [2]. This war was very comprehensive as it affected everything from economics to politics, from security to energy. This has been one of the most common moments of systemic crisis, as many countries, including China, the UK, Europe, the USA and Turkey, reassess their global positions and try to adapt to the new situation [3]. At the same time, the Russian-Ukrainian war put on the agenda the creation of a new international security system.

In addition, this war intensified the geopolitical struggle of world powers for control of the Black Sea-Caspian basin and its heartland, Ukraine. The current situation in Ukraine is considered a period of “transition to a new world order” [4].

Considering the importance of the geostrategic position of the Black Sea-Caspian region for Russia, as well as for Western countries and the processes taking place there, the topic under discussion is of great interest from the point of view of relevance.

1. The Black Sea-Caspian basin and geopolitical aspects of the Russian-Ukrainian war

An analysis of the military-political events that took place in Ukraine in antiquity and the Middle Ages shows that the historical fate of the peoples living in these territories has always been connected with the Black Sea. As before, Ukraine, due to its geographical location and natural resources, is considered one of the main participants in the center of geopolitical processes in Central Eurasia, especially in the Black Sea-Caspian basin.

Formed on the basis of basic geopolitical principles, "telluric dualism" (land power), "thalassocracy" (sea power) and the centuries-long West-East conflict continued in a military-political form. As a result of this, two types of cultural and historical civilization arose - democracy and ideocracy. One of the main centers of this conflict was and remains the Black Sea-Caspian basin. According to the theory of H. Mackinder, a dynamic historical process of development manifests itself around the "Pivot Area" and the HEARTLAND or continental internal Eurasian space, which includes the basins of the Arctic Ocean and the Mediterranean Sea [5].

An analysis of events in Central Eurasia showed that the process of continuous expansion and contraction of this huge monolith as a geopolitical space occurred over the course of centuries. The clash between the geopolitical forces of East and West had varying degrees of success. World history has recorded the experience of "military-civilizational" aggression of the West on this mega-region. In the last centuries of the first millennium BC, the thalassocratic West, although unsuccessfully, tried to overcome the ethnic and religious isolation of the tellurocratic East by "Hellenizing" it.

This region, which has a strong geopolitical space called the "Heart of Eurasia", as before, due to its geographical location, inexhaustible natural resources and demographic potential, is subject to a clash of geostrategic interests of world powers such as Russia and the United States.

According to Z. Brzezinski, the geostrategic importance of this region, which is part of the "Eurasian Balkans," has increased even more. During the XX–XXI centuries, the region again became one of the important geopolitical factors due to its rich reserves and natural resources, trade and transport routes passing through it, as well as strategic communications" [6].

Thus, after the collapse of the USSR, the Black Sea-Caspian basin and Ukraine in particular were considered the sphere of influence of Russia, but the processes taking place here recently have led to a change in the geopolitical balance. Ukraine was one of the active participants in the geopolitical struggle in the region. Along with the main leading world powers – the West (USA, Great Britain and the European Union) and the East (Russia and China), the countries of the region - Turkey, Iran and others - also took part in this competition.

As mentioned above, the growing interest of neighboring countries in this region, along with many centers of power, is associated not only with the presence in the region of a wide transit route, road communications and rich natural resources, but also with the geospatial role of the region in the struggle of regional forces [6]. The geopolitical conflict between states is gradually moving from Eastern Europe and the Mediterranean basin to the Black Sea-Caspian basin, and from there to the Caucasus-Caspian region, the Central Asian region and China. Under these conditions, the geopolitical imperatives of NATO, on the one hand, and China, Russia and Iran, on the other, came to the fore.

One of the most pressing problems for both Ukraine and neighboring countries (Georgia, Moldova, etc.) has become the replacement of transit routes for the transportation of natural resources imported with the help of Russian and Western companies into the Black Sea-Caspian basin.

Russian analysts talk about the geostrategic importance of this basin and consider attempts by British-American transnational companies to control the strategic highways and natural resources passing through it as one of the most pressing geopolitical problems for Russia. Thus, according to the famous Russian ideologist A. Dugin, "Full control over the entire Black Sea-Caspian basin is one of the

strategic goals of the global conflict between Atlanticism and Eurasianism" [7]. A. Dugin believes that "the main task facing Moscow is, first of all, to achieve its centuries-old geostrategic goal by forming the Moscow-Tehran axis, that is, to break the "anaconda ring", gaining access to warm seas" [5].

Currently, Iran, which is anti-American, anti-Atlantic, geopolitically active and coincides with Russia's interests in many issues, has also strengthened its efforts to penetrate this region. Thus, in the Moscow-Tehran axis that was formed, Armenia was considered to be an important strategic link that completed the union of Russia with Iran and separated Turkey from the intra-continental Eurasian space, taking the path of military conflict with Azerbaijan. However, since 2014, Russia's military operations in Ukraine have changed the geopolitical environment in the Caspian-Black Sea basin and the implementation of new projects in the region, including the "lifeway" connecting the Mediterranean, Caspian and Black Sea basins via Nakhchivan (Baku-Tbilisi-Kars transport future connection of the road line with the Zangezur corridor, etc.) promised new development prospects. Azerbaijan's victory in the 44-day war with Armenia had an impact on the balance of forces in the military and political spheres in the Caucasus-Caspian region. Azerbaijan actually changed the line of confrontation on the geopolitical level and increased the importance of the Black Sea-Caspian basin [8].

In such a global scenario, Azerbaijan did not ensure the interests of either the West or Russia, but stood guard over its own national interests. It played the role of a middle, unifying force between the West and Russia and was distinguished by its impartial position in relation to world powers. In addition to the fact that Azerbaijan took a decisive and tough position to ensure its economic and political independence and territorial integrity, Azerbaijan, as the leader of the South Caucasus region, created new geopolitical realities, implemented projects of global significance in its geography, and tried to strengthen its place among the winning states in the emerging world order of the future. Currently, Azerbaijan continues to attach great importance to the restoration of all economic and transport ties, strategic communications and corridors in the region.

It should be noted that corridors, in addition to being of great importance, are considered the most sensitive point of states. Ambitious states sometimes did not even hesitate to use force to control these corridors. The struggle for corridors passing through the Black Sea-Caspian basin is taking on a more fierce form. From this point of view, the Russian-Ukrainian conflict is considered a clear factor in the struggle for the corridors.

At the same time, the importance of the corridors is increasing day by day against the backdrop of sanctions imposed by the West against Moscow as a result of the Russian-Ukrainian war. These sanctions have limited Russia's effectiveness in overland trade relations between the European Union and China. In this context, the Middle Corridor (Trans-Caspian International Transport Route) has begun to attract the attention of Chinese, EU and regional governments as a potential alternative route for rail trade.

Since the beginning of the war, the volume of traffic in the Middle Corridor has increased dramatically. During January-March 2022, 266.3 thousand tons of cargo passed along this route, which is 123 percent more than during the same period in 2021. Container turnover amounted to 584,720-foot container equivalent units (TEU), which is 19 percent more than in January-March 2021. Currently, the Middle Corridor accounts for 3-5 percent of total China-EU rail freight traffic. Arousing great interest, it is expected that, in the future, about 10 percent of this volume can be easily transported along this corridor [9].

Despite the increasing importance of the Middle Corridor as a potential route to compensate for the relatively significant losses of the Northern Corridor through Russian territory, various problems have prevented the effective use of the alternative passage. Problems on the Central Asian section of the route, especially at the China-Kazakhstan border, have led to delays and increased shipping costs, reducing the route's reliability.

Another serious dilemma was related to the Black Sea and Caspian sections of the route. Limited port capacity and ferry services have proven to be the most significant challenges causing delays and making it difficult to accurately manage delivery times. The latest problem was transport issues related

to the railway route and the part of the corridor passing through Turkey. Limited capacity in the Istanbul region, especially at Halkali station, prevented efficient transportation in bottlenecks, as well as great uncertainty in setting delivery times. As a result, national governments and local companies have come together to address these challenges and effectively optimize transportation along the Middle Corridor, while also demonstrating their commitment to creating a secure environment in parts of the Black Sea-Caspian Basin.

It can be said that the intense geopolitical competition between the newly formed geostrategic centers around the Black Sea-Caspian basin has been expanding for almost a century. To help the horizontal consolidation of the states of the Black Sea, Central Asia and the South Caucasus, the West decided to create a new main communication artery bypassing Russia according to the Turkey-Ukraine-Moldova-Georgia-Azerbaijan scheme. This plan included a number of Central Asian states. Examples include the successful implementation of the Baku-Tbilisi-Ceyhan oil pipeline, the TANAP and TAP projects, the commissioning of the strategic route Baku-Tbilisi-Kars, the restoration of the Great Silk Road, the opening of the international transport trans-Caspian route, the Turkish project "New Asia" [10] and so on. The Russian side responds to this by forming a vertical axis of Russian-Armenian-Iranian states. This, in turn, created real prospects for the transformation of the Black Sea-Caspian basin into a decisive "arena of military operations" in the Atlantic-Eurasian geopolitical conflict of the 21st century. The first military conflict occurred at the beginning of the twentieth century in Karabakh (1991–1994), South Ossetia (1991–1992), Abkhazia (1992–1993), Chechnya (1995–1996), and in 2008 it broke out again in South Ossetia. As a continuation of these processes, we can name the Armenian-Azerbaijani war in 2020 (September 27-November 10), the First Russian-Ukrainian War in 2014 and the Second Russian-Ukrainian War in 2022 [5].

In general, the Black Sea-Caspian basin, located at the center of the geopolitical turning point of the Central Eurasian post-Soviet space, has since the 1990s become an integral part of the "great geostrategic game", conducted according to the classical rules of geopolitics in world politics. In addition to the fact that the Black Sea-Caspian space is considered the most unstable, conflict-ridden, but at the same time the most important geopolitical space on Earth, the geopolitical, geo-economic and military-geostrategic interests of the countries of the world, various civilizations, religious denominations, cultures and ethnic interests are taken into account here. This region has become the hottest line where the interests of Russia and the West collide. Ukraine, which for centuries has been one of the important links in geopolitical relations in Central Eurasia, has found itself at the center of international geostrategic competition in the Caspian-Black Sea basin. As a result of the ongoing geopolitical struggle, the Russian-Ukrainian conflict has led to a redefinition of the future foreign policy contours of Ukraine, with the military-power factor becoming the determining factor in this geopolitical competition.

2. Military-strategic aspects of the Russian-Ukrainian war

Events in Ukraine have strengthened the geopolitical significance of NATO and Eastern Europe in the region and their influence on the policies of these states, causing a new qualitative change in the balance of power. The country, which exercises control over the Black Sea-Caspian basin, is open to roads leading to Europe, the Caucasus-Caspian region and Central Asia. Russia's inclusion of Crimea and Sevastopol into the constituent entities of the federation on March 18, 2014, and on April 7 of the same year, pro-Russian separatists proclaimed the unrecognized "Donetsk People's Republic" and "Luhansk People's Republic" in Eastern Ukraine, with the support of Russia, created the basis for the policy neo-Eurasianism and led to increased power of Russia in this region [11].

Both participants in the war pursue radically different goals. Russia assesses its actions as a special military operation aimed at protecting its national security, while Ukraine's goal is the withdrawal of Russian troops from its territory (Crimea, Donbass and regions that the Russian Armed Forces entered after February 24).

At the same time, the main reason for Russia's war against Ukraine was the destruction of the development model that was growing in its cultural geography and was considered dangerous from the

point of view of its internal politics. This model was seen as a new socio-economic structure of society, where one could be culturally Slavic and Orthodox, but politically and economically Western. Although Russia tried to block the development of this model in Ukraine in 2014, Moscow backed down after demonstrations in Kyiv. Then Russia unjustly annexed Crimea and Sevastopol. Although Russia seems to have won, increasing its influence in Donetsk and Lugansk, it was unable to put an end to this political and social model, which is deepening day by day in Ukraine. Russia's main idea was related to the threat of the influence of this model on the economic and political order in Russia, as well as the desire and determination of Ukraine to join the NATO alliance [12]. To prevent this, from 2021 Russia began to deploy its military forces near the border with Ukraine, including in neighboring Belarus. Russian President Vladimir Putin has criticized NATO expansion and opposed Ukraine's joining the military alliance, questioning Ukraine's right to exist and its independent activities.

To protect the territorial integrity and sovereignty of Ukraine, from attempts by the strong to forcefully keep the weak under their influence, the West and many countries of the world showed solidarity with Ukraine and mobilized all of Europe against Russia. Even during the Cold War, Russia was not subject to such large-scale sanctions. European air and sea ports were closed to Russian planes and ships, huge Western companies and brands left the Russian market, and most large companies ceased trade and cooperation with Moscow. The war in Ukraine has reached the climax of confrontation between Russia and the West.

Since February 24, 2022, Ukraine’s stubborn struggle to restore its territorial integrity and ensure its future as an independent state [13] led to tough measures from Russia: according to the results of pseudo-referendums held on September 23-27 in Donetsk, Lugansk, Zaporozhye and Kherson, these territories were recognized as part of Russia (they covered 15% of the territory of Ukraine), and in 7 months a total of more than 108,800 km2 of Ukrainian territory (for example, as much as Cuba alone, or slightly less than Bulgaria) was occupied by Russia. Thus, Ukraine’s actual membership in NATO, although not formalized de jure, upset the balance, and persistent efforts towards the West led to the annexation of four regions to Russia [14].

Both the United States and Russia, seeking to secure their core national interests, gave priority to pursuing offensive policies to protect these interests. In particular, Russia's interventions in neighboring states have been shaped by the military threat posed by NATO's eastward expansion and by Russia's historical view of this geography as part of its territory.

To maintain its influence over the architectural, historical and cultural structure of its cultural geography in Ukraine, Russia has announced the possibility of stationing and using nuclear weapons in its only ally in Eastern Europe, Belarus. This was seen as a new step in the nuclear weapons threat from Moscow, which opposes Western countries sending heavy weapons to Kyiv. When asked about the possibility of using these weapons, Putin replied: “Why should we threaten the whole world? I have already said that if there is a danger to the Russian state, then we can resort to extreme measures” [15].

Russia, which threatened the West and Ukraine with the deployment of huge forces, actually demonstrated the idea of forcing the Kyiv administration to surrender, and Western countries to reduce aid and keep the situation as it is.

The analysis showed that real politics is shaped by the relations between alliances created by the Big Five states: Russia founded the Commonwealth of Independent States (CIS), the Eurasian Economic Union, the Collective Security Treaty Organization (CSTO) in its geography of interests, China created the Shanghai Cooperation Organization, France and Germany founded the European Union, and The USA and Great Britain created NATO. However, over the 30-year period from the 90s to the 2020s, tectonic cracks formed inside these blocks. Disunities and ruptures moved the rocks of the international order, laying the groundwork for events that led to a new world order in the struggle for new bases and new zones of economic and political influence.

As a natural result of these factors, Ukraine prepared its army according to NATO standards, providing it with modern equipment, ensuring a number of victories on the battlefield, and also created the conditions for the formation of a new geopolitical configuration in the region [16]. Tensions between

Russia and Ukraine will continue until the end of this year, and after Ukraine receives sufficient support from Western countries, the war will reach a military-strategic level. Russia, mobilizing its resources, will further increase defense spending and try to modernize its army. The conduct of Russia's military strategy serves to achieve control over the main strategic communications and corridors located in the Black Sea-Caspian basin, especially to control the lands in the east and south of Ukraine [17], as well as to destroy the economy and infrastructure of Ukraine, by strengthening the blockade of sea ports [18]. This strategy would involve forcing Kyiv to end the war and cede control of some of its territories to Russia. Various means will be used to achieve this, including creating political and economic instability, increasing poverty in Ukraine, and reducing popular support for the war. Russia's new tactics and missile attacks will prolong the war and lead to increased military spending and resource use.

This is aimed at forcing Ukraine to make concessions and, with more support from Western countries, push it into an endless war and increase its own military spending to show its European neighbors that Russia remains a serious threat to the continent. The current situation will force Russia to continue its tactics of destroying infrastructure with the threat of using tactical nuclear weapons.

This conflict between Russia and the West will escalate into political and economic wars, followed by a race to modernize and reconfigure all aspects of their military, including advanced and nuclear equipment, to ensure deterrence.

Despite limited public opposition to the war in Russia and sanctions against it, Moscow is likely to continue the war. Despite the fact that the Russian-Ukrainian war has been going on for more than two years, the West will continue to support Ukraine’s position both morally and militarily until the end of the war [19].

3. Military-political aspects of the Russian-Ukrainian war in 2024

The course of recent events in the Russian-Ukrainian war shows that the main strategic plans of the United States and the West are aimed at defeating Russia in this war. However, one cannot ignore that in the West there are certain contradictions regarding the models of Russia’s defeat. This is largely due to the acute clash of interests in the West regarding the new world order. At the same time, representatives of some Western countries, including the United States, believe that a quick defeat of Russia may allow it to gather strength and later make plans for revenge. Therefore, the West seeks to condemn Russia to a protracted war, gradually weakening it and preventing it from gaining strength again. This clearly demonstrates that the complete depletion of Russia’s military-economic potential and resources is included in the long-term strategic plans of the West [20].

Recently, despite weakening support for Ukraine from Western countries and declining interest in the Russian-Ukrainian war due to the Israeli-Palestinian conflict, NATO countries' agenda for 2024 still predicts that this war will still continue. Because with the military occupation of Ukraine, there is a possibility that European countries could become a direct target of Russia. Trying to bring this factor to the fore, some military and political circles in the Ukrainian government are trying to intensify attacks on the positions of the Russian army. It is emphasized that it is impossible to reach peace negotiations in the context of such intense hostilities. Because in order to sit down at the truce table, it is first necessary to create calm in the combat zone. On the other hand, the Russian side believes that as a result of a long war, the resources in the Ukrainian army’s arsenal will be completely exhausted. It is assumed that if this happens, a Russian military victory will be inevitable and the Kremlin will not enter into negotiations on a peace agreement with the collective West.

According to available data, Russia has already begun to think about the prospect of annexing not part of, but the entire territory of Ukraine to Russia. If this happens, Russia will also try to dictate its geopolitical terms to the United States and the West. The current situation forces the collective West to resume military support for Ukraine with the same intensity in 2024 and change the strategy of the United States and European countries towards Ukraine. The reasons for the need for a new strategy include the failure of Ukraine’s counter-offensive in 2023 and weakening support for Ukraine in the US Congress [21]. In December 2023, Pentagon chief Lloyd Austin, at a joint press conference in the United

States with Ukrainian President Vladimir Zelensky, assured that the United States would help Ukraine create Armed Forces capable of containing Russia.

Russia's large-scale military intervention in Ukraine has changed the security environment in Europe and forced continental states to reconsider their military-political strategies. Thus, in the Strategic Concept adopted by NATO in 2022 and 2023, it is possible to show the implementation of the policy of increasing military power both by the North Atlantic bloc and by individual members of the bloc.

At the same time, the United States and its European allies are "slowly changing their strategy" towards Ukraine and are discussing a transition to a defensive posture in the east of the country. Wherein, NATO emphasizes the strengthening of Ukraine's air defense systems, the construction of fortifications, anti-tank barriers and trenches along the northern border with Belarus, as well as the intention to help Ukraine quickly restore its military-industrial complex to produce the necessary weapons. During 2024, it is considered necessary to maintain the defenses and current positions of the Ukrainian side, increase reserves of forces and weapons, intensify attacks on Russian bases in Crimea, and create conditions for the war to transfer to Russian territory. This Ukrainian strategy is designed to prevent any new attack from Russia. The goal is to create a credible threat and force Russia to agree to peace talks. Among other things, the main goal of the strategy of the Ukrainian military command is to weaken Russia's offensive tactics through attacks on Russian arms factories, weapons and ammunition depots, and transport railways. Such long-range attacks on Russian bases in Crimea could disrupt its dominance in the Black Sea and help Ukraine win at sea.

Thus, an analysis of events shows that tensions between Russia and Ukraine will continue until the end of this year, and it is predicted that the war will reach a military-strategic level after Ukraine receives sufficient support from Western countries.

Conclusion

Thus, the Russian-Ukrainian war is predicted to determine the balance of power between the main military-political centers of power in the world, and will also become the main factor in the formation of a new world order. It is likely that after the war in Ukraine, Russia's use of existing corridors in the Black Sea-Caspian basin will be limited, including the suspension of the transportation of natural resources and the export of hydrocarbon resources from the territory of Ukraine, which will definitely lead to a weakening of the world order and the single-center economic and financial structure. As a result, the foundation will be laid for global restructuring and the beginning of a new multipolar order.

Unfortunately, in this competition, Ukraine took on the role of an international testing ground. The main military-strategic plans of the United States and the West are based on the goal of defeating Russia. However, the West sees certain positional contradictions around the models of Russia's defeat in the war. This is largely due to the acute clash of interests in the West regarding the new world order. At the same time, some countries of the West and East, led by the United States, are not positive about Russia's quick defeat. On the contrary, representatives of this pole believe that a quick defeat of Russia may allow the Kremlin to make plans for revenge in the future. Therefore, Russia should be doomed to a long war, gradually weakened and not given a chance to strengthen again. That is, military-strategic plans are being formed aimed at completely exhausting the military-economic potential and resources of Russia.

All this will raise the geopolitical risk index to high values in the Black Sea-Caspian basin and adjacent regions, and world powers will enter a new phase of geopolitical competition.

References

1. Rusiya-Ukrayna qarşıdurması – növbəti dünya müharibəsi: [Elektron resurs] / – 10 may, 2022. URL: https://report.az/analitika/rusiya-ukrayna-qarsidurmasi-novbeti-dunya-muharibesi

2. Rusiya-Ukrayna müharibəsinin bir ili – Azərbaycandan ekspert baxışları: [Elektron resurs] / – 23 fevral, 2023. URL: https://www.amerikaninsesi.org/a/6975456.html

3. Ukrayna-Rusiya müharibəsinin uzanmasının səbəbləri və mümkün ssenarilər: [Elektron resurs] / – 16 mart, 2023. URL: https://ordu.az/az/news/256904

4. Yeni dünya nizamında Azərbaycan regional güc və birləşdirici amil kimi: [Elektron resurs] / – 22 oktyabr, 2022. URL: https://musavat.com/news/yeni-dunya-nizaminda-azerbaycan-regional-guc-ve-birlesdirici-amil-kimi_930621.html

5. Əliyev, N.A. Cənubi Qafqazda geotəhlükəsizlik mühiti və Azərbaycan postmüharibə dövründə. Dərs vəsaiti. / N.A.Əliyev, V.M.Məmmədzadə – Bakı: AfpoliqrAF – 2023. – 112 s.

6. Бжезинский, З. Великая шахматная доска. / З. Бжезинский, – Москва – 1999, – 256 с.

7. Дугин, А. Основы геополитики. / А.Дугин – Москва. – 1999. – 608 с.

8. Азербайджан укрепляет позиции в международных транспортных потоках – новые перспективы для экономического развития: [Электронный ресурс] / – 12 июля, 2023. URL: https://news.day.az/politics/1580779.html

9. Orta Dəhliz Layihəsi kritik əhəmiyyət kəsb edir – Bəs optimallaşdırma necə aparılır? [Elektron resurs] / – 25 avqust, 2022. URL: https://ordu.az/az/news/228915/orta-dehliz-layihesi-kritik-ehemiyyet-kesb-edir-bes-optimallasdirma-nece-aparilir

10. Чавушоглу рассказал о внешнеполитических приоритетах на всех континентах: [Электронный ресурс] / 1 ноября, – 2022. URL: https://vestikavkaza.ru/analytics/cavusoglu-rasskazal-o-vnesnepoliticeskih-prioritetah-na-vseh-kontinentah.html

11. Yaremenko, B. Military build-up of Crimea / B.Yaremenko, T.Huchakova, A. Klymenko, O.Korbut, Y.Smelianskyi // Black Sea Security. – Kyiv: – 2017. № 2(30). – p. 14-34.

12. Qaribaşvili Rusiya-Ukrayna müharibəsinin səbəbini açıqlayıb: [Elektron resurs] / – [Elektron resurs] / – 30 may, 2023. URL: https://ikisahil.az/post/424599-qaribashvili-rusiya-ukrayna-muharibesinin-sebebini-achiqlayib

13. Ukrayna yoxsa Rusiya?: [Elektron resurs] / – 3 aprel, – 2021. URL: https://teref.az/siyaset/186984-ukrayna-yoxsa-rusiya-siyasi-tehlil.html

14. Wiegrefe, K."NATO's Eastward Expansion: Is Vladimir Putin Right?". [Electronic resource] / – 15 February – 2022. URL: https://spiegelşde/international/world/nato-s-eastward-expansion-is-vladimir-putin-right-a-bf318d2c-7aeb-4b59-8d5f-1d8c94e1964d

15. Rusiya Ukrayna müharibəsində nüvə silahından istifadə edə bilər?: [Elektron resurs] / – 05 iyul, 2023. URL: https://ordu.az/az/news/271990/rusiya-ukrayna-muharibesinde-nuve-silahindan-istifade-ede-biler—-analiz-

16. Ukraynanın gələcəyi NATO-dadır və bu müzakirə mövzusu deyil: [Elektron resurs] / – 16 iyul, 2023. URL: https://modern.az/dunya/422057/ukraynanin-geleceyi-nato-dadir-ve-bu-muzakire-mvzusu-deyil-sallivan/

17. 2023-cü ildə geosiyasi münaqişələr dünya üçün hansı təhlükələri yaradacaq?: [Elektron resurs] / – 09 yanvar, 2023. URL: https://ordu.az/az/news/247294/2023-cu-ilde-geosiyasi-munaqiseler-dunya-ucun-hansi-tehlukeleri-yaradacaq-

18. Xersonda Rusiya Ukraynaya məxsus 3 kateri batırıb: [Elektron resurs] / – 15 iyul, 2023. URL: https://ikisahil.az/post/438647-xersonda-rusiya-ukraynaya-mexsus-3-kateri-batirib

19. Rusiya-Ukrayna müharibəsinin görünməyən tərəfləri – Amerikalı eksperti: [Elektron resurs] / – 13 iyul, – 2022. URL: https://oxu.az/world/622344

20. Məmmədli, M. Rusiya–Ukrayna müharibəsinin yaratdığı hərbi-siyasi reallıqlarda NATO-nun təhlükəsizlik siyasətinin əsas aspektləri / M.Məmmədli. – Bakı: «Beynəlxalq Münasibətlərin Təhlili Mərkəzi», – iyun, – 2023.

21. Abdullayev, M. Rusiya–Ukrayna müharibəsi: yeni dağıntılar və itkilər // Xalq qəzeti. – 2023,10 avqust, – səh.5

Xülasə

Rusiya–Ukrayna müharibəsinin geosiyasi və hərbi-strateji aspektləri

Nurulla Əliyev, Anar Musayev

Məqalədə bəşər sivilizasiyasının tarixi inkişafı ilə Qara dəniz–Xəzər regionunun artan əhəmiyyəti və bu regionda geostrateji maraqları kəsişən aparıcı dünya dövlətlərinin mübarizə tarixi göstərilir. Qara dəniz–Xəzər hövzəsində vəziyyətə nəzarət hüququ uğrunda formalaşan müasir geostrateji mərkəzlər arasında geosiyasi rəqabət dəyərləndirilir. Məqalədə Rusiya–Ukrayna müharibəsi şəraitində hərbi-siyasi hadisələr təhlil edilir, onun geosiyasi və hərbi-strateji aspektləri üzə çıxarılır. Tədqiqatın məqsədi regiondan keçən neft-qaz kəmərlərinə, nəqliyyat dəhlizlərinə və kommunikasiya xətlərinə nəzarət uğrunda geosiyasi sferanı və geosiyasi mübarizə üsullarını qiymətləndirməkdir. Bu problemin öyrənilməsi zamanı əsas vəzifələr Qara dəniz–Xəzər regionunda baş verən geosiyasi proseslərin və onun tarixi aspektlərinin təhlili, Rusiya–Ukrayna müharibəsində aparıcı dünya dövlətləri arasında rəqabətin əsas məqsədləri olmuşdur. Məqalədə qoyulan problemi üzə çıxarmaq üçün tarixi, xronoloji və müqayisəli tədqiqat metodlarından istifadə edilmişdir. Məqalənin yekun hissəsində yeni dünya düzəninin formalaşmasında amil kimi çıxış edən Rusiya–Ukrayna müharibəsinin qüvvələr balansının geosiyasi mərkəzlər arasında bölüşdürülməsinə imkan verəcəyi proqnozlaşdırılır. Güman edilir ki, müharibədən sonra Rusiyanın mövcud nəqliyyat dəhlizlərinə çıxışı məhdudlaşdırılacaq, təbii və karbohidrogen ehtiyatlarının Ukrayna ərazisindən daşınması dayandırılacaqdır. Bu da mərkəzləşdirilmiş iqtisadi və maliyyə sisteminin zəifləməsinə gətirib çıxaracaq, eləcə də qlobal restrukturizasiya və dünya nizamının yeni çoxqütblü sisteminin formalaşması üçün əsas yaradacaqdır.

Açar sözlər: müasir dünya nizamı, regional təhlükəsizlik, təbii sərvətlər, ictimai-siyasi sistem

Аннотация

Геополитические и военно-стратегические аспекты Российско-Украинской войны

Нурулла Алиев, Анар Мусаев

В статье показано возрастающее значение Черноморско–Каспийского региона по мере исторического развития человеческой цивилизации, изложена история борьбы ведущих мировых держав, геостратегические интересы которых пересекались в этом регионе. Дана оценка геополитического соперничества между современными формирующимися геостратегическими центрами в Черноморско-Каспийском бассейне за право контролировать ситуацию в нём. В статье проведён анализ военно-политических событий в условиях Российско-Украинской войны, раскрывается его геополитические и военно-стратегические аспекты. Цель исследования является оценка геополитической сферы и методы геополитической борьбы за обладанием контроля над проходящими в регионе нефтегазовыми трубопроводами, транспортными коридорами и коммуникационными линиями. В ходе исследования данной проблемы основными обязанностями были анализ происходящих в Черноморско-Каспийском регионе геополитических процессов и его исторические аспекты, основные цели соперничества ведущих мировых держав в Российско-Украинской войне. В статье для раскрытия поставленной проблемы использовалось историко-хронологический и сравнительный методы исследования. В заключительной части статьи прогнозируется, что Российско-Украинская война, выступая как фактор формирования нового мирового порядка позволит распределить соотношение сил между геополитическими центрами. Предполагается, что после войны доступ России к существующим транспортным коридорам будет ограничено, в том числе приостановка использования украинской территории для транспортировки природных и карбогидрогенных ресурсов приведёт к ослаблению централизованной системы экономическо-финансовой структуры, а также глобальной реструктуризации и основы для формирования новой многополярной системы миропорядка.

Ключевые слова: современный миропорядок, региональная безопасность, природные ресурсы, общественно-политическая система

Məqalə redaksiyaya daxil olmuşdur:17.04.2024
Təkrar işlənməyə göndərilmişdir: 29.04.2024
Çapa qəbul edilmişdir:14.05.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 62-69
HƏRBİ NƏZƏRİ ELMLƏR ***MILITARY THEORETICAL SCIENCES***

UOT 371 DOI: 10.30546/9878.2024.2.10.0023.

HƏRBİ ALİ TƏHSİL MÜƏSSİSƏLƏRİNDƏ MÜHƏNDİS HAZIRLIĞININ DİDAKTİK LAYİHƏLƏNDİRİLMƏSİNİN ƏSASLARI

e.o. kapitan Amil Dadaşov
Heydər Əliyev adına Hərbi İnstitut
amilodas@gmail.com

Xülasə. Məqalədə hərbi ali təhsil müəssisələrində mühəndis hazırlığının didaktik layihələndirilməsinin əsasları və bu əsaslar üzrə həyata keçirilən işlərin məzmunu araşdırılır. Tədqiqat işinin məqsədi hərbi mühəndis hazırlığı üzrə didaktik layihələndirmənin nəzəri əsaslarını, didaktik yanaşmanın hərbi elmi-pedaqoji təhlilinin xüsusiyyətlərini və didaktik layihələndirmədə sistemli yanaşmanı vurğulamaqdır. Hərbi ali təhsil müəssisələri potensial çağırışları qabaqlaya və təlim proqramlarını vaxtında uyğunlaşdıra bilərlər. Bu məqsədlə yeni yaranan texnologiyalar, inkişaf edən təhdidlər və dəyişən əməliyyat tələblərini müəyyən etmək üçün mövcud vəziyyət hərtərəfli tədqiqat və təhlillərin aparılmasını aktuallaşdırır. Məqalədə, həmçinin didaktik layihələndirmə prosesinin elmi pedaqoji cəhətdən səmərəliliyinin elmi fikir və müddəalarla müəyyən edilməsi üsullarına nəzər salınır. Problemin araşdırılmasında nəzəri təhlil tədqiqat metodundan istifadə edilmişdir. Əldə olunan nəticəyə görə didaktik layihələndirmə təlim proqramının mahiyyətini, məzmun və strukturunu özündə ehtiva edir. Bu proses, verilən təhsilin səmərəliliyinin yüksəldilməsində həlledici rol oynayır. Məqalədə yer alan elmi fikirlər və müddəalar hərbi ali təhsil müəssisələrində mühəndis hazırlığının didaktik layihələndirmə prosesinin mahiyyətini, məzmun və strukturunun əhəmiyyətini, eyni zamanda rasionallığını əsaslandırmağa imkan verir.

Açar sözlər: hərbi təhsil, təlim prosesi, hərbi institut, mühəndis hazırlığı, didaktik əsaslar

Giriş

Didaktik layihələndirmə prosesi hərbi ali təhsil müəssisələrində (HATM) mühəndis hazırlığının vacib tərkib hissəsidir. Bu prosesin mahiyyət, məzmun və strukturunun əsasını təlim məqsədlərinin hərbi tələblərə uyğunlaşdırılması və fəal təlimi təşviq edən pedaqoji yanaşmalar da daxil olmaqla, hərtərəfli qiymətləndirmə strategiyalarının hazırlanması təşkil edir. HATM-lər yaxşı hazırlanmış didaktik prosesi həyata keçirməklə, mühəndis hazırlığı proqramlarının hərbi mühəndislik sahəsinin xüsusi əhəmiyyətli vəzifələrinin icrasına və mürəkkəb problemlərin həllinə qadir olan, səriştəli, eyni zamanda uyğunlaşmağı bacaran hərbi mühəndislərin hazırlanmasına nail ola bilər.

Mühəndislik təhsilinin didaktik layihələndirilməsi işinin icrasında mühüm olan ilk element fənn proqramının (kurikulumun) strukturudur. Hərbi mühəndislər üçün təlim proqramlarının tərtibi pedaqoji prinsiplərin, ixtisas sahəsinin vəzifə və öhdəliklərinin diqqətlə nəzərdən keçirilməsini tələb edir. Mükəmməl tərtib edilmiş fənn proqramı hərbi ixtisasın tələblərini nəzərə almaqla, göstərilən əsas məqsədləri təmin etməlidir: təməl mühəndislik elminin nəzəriyyəsini; hərbi ehtiyaclara uyğunluğu; hərtərəfli praktiki tətbiqləri [1]. Fənn proqramları nəzəri biliklər və praktiki təcrübələr arasında balans yaratmalı, ixtisas üzrə təhsilalanları real mühəndislik problemlərinin öhdəsindən gəlməyə hazırlamalıdır [2]. Bu istiqamətdə görülən işlər çərçivəsində Azərbaycanın milli təhlükəsizlik və xüsusi hərbi elm sahələrini, hərbi elm təhsil sistemini gücləndirmək üçün beynəlxalq əməkdaşlığa və inteqrasiyaya mühüm yer verilməkdədir. Ötən illərdə görülən işlərin nəticəsinə əsasən Türkiyə, NATO və digər beynəlxalq təşkilatlarla hərbi və çoxşaxəli əməkdaşlıq təkcə hərbi təhsil sistemində müasir elmi nailiyyətlərə aparan bilik mübadiləsinə, fənn proqramlarının hazırlanmasına və fakültə hazırlığına əsaslı töhfələr vermişdir [3]. Müasir ali pedaqoji fəaliyyət planı, yalnız müvafiq bilik və bacarıqlara malik şəxsiyyət yox, həm də müasir tələblərə cavab verməyə qadir müasir nəsil və dünyagörüşü formalaşdırmağa yönəldilməli, bu tendensiyalarla gələcəyə doğru irəliləməlidir [4].

Daha yaxşı nəticələrə nail olmaq üçün ali hərbi təhsil müəssisələrində tədris prosesinin təşkili onun optimallığını təmin etməlidir. Pedaqoji işin elmi təşkilinə əsaslanmaqla həll edilməli olan məsələlər arasında təlim və tədrisin layihələndirilməsi və didaktik layihələndirmə aparıcı rol oynayır. Elmi pedaqogikada təlim və tədrisin layihələndirilməsi sahəsində müxtəlif tədqiqatçı alimlərin istifadə etdiyi konseptual fikirlər mövcuddur. "Bloom"un yenilənmiş təhsil məqsədləri taksonomiyasına əsaslansaq, layihələndirmə prosesinin düşüncənin təkmilləşdirmə, yaratma və yenidən hazırlama, yadda saxlama, anlama, tətbiqetmə, təhliletmə, qiymətləndirmə və ixtira da daxil olmaqla bütün idrak fəaliyyətləri ilə əhatələndiyinə əmin olarıq [5]. Müasir pedaqogika elminin banisi L.S.Vıqotski iddia edir: *"Pedaqogika insan inkişafının dünənki deyil, sabahkı gününə istiqamətlənməlidir"*. Pedaqoji cəhətdən professional layihələndirmə elmi fənnin layihələndirilməsi prosesi kimi (Instructional Design), daha effektiv, rasional və rahat tədris üsul, metod və sistemlərinin işlənib hazırlanmasına əsaslanır [6]. Hərbi mühəndislik pedaqogikası təbiət elmləri, humanitar elmlər və tətbiqi biliklər arasında spesifik qarşılıqlı əlaqəni özündə əks etdirən metodoloji əsaslı sistemdir. Bəzi mənbələrdə mühəndis pedaqogikasının, həm də fundamental və tətbiqi elm olduğu qeyd edilir, çünki onun kateqoriyaları və konsepsiyaları elmi statusa malikdir və mühəndis kadrlarının hazırlanması üçün metodoloji əsas rolunu oynaya bilər [7]. Qeyd edildiyi kimi, bu fikirlər hərbi mühəndislərin hazırlanması və didaktik layihələndirmə prosesinin məzmun xəttinin genişləndirilməsi üçün faydalı hesab olunur.

HATM-lərdə mühəndis hazırlığı proqramı silahlı qüvvələrin müdafiə sektorunda üzləşdiyi müxtəlif mühəndislik problemlərinə adekvat kadrların hazırlanmasında mühüm əhəmiyyətə malikdir. Bu təlim proqramı üzrə didaktik layihələndirmə, biliklərin ötürülməsinin effektivliyinə, bacarıqların inkişafına və hərbi mühəndislərin ümumi səriştəsinə müsbət təsir göstərir. Məqalənin elmi yeniliyi ondan ibarətdir ki, xüsusi hərbi elmi sahəsində (hərbi mühəndislik) potensial töhfələrə diqqət yetirilir, HATM-də mühəndis hazırlığının didaktik layihələndirilməsinin nəzəri əsasları-vurğulanır.

Mühəndis hazırlığının didaktik layihələndirilməsinin nəzəri əsasları

HATM-də hərbi mühəndislik təhsili bərpa quruculuq işlərinin yerinə yetirilməsi, işğaldan azad olunmuş ərazilərin tam təmizlənməsi, ordunun mühəndis cəhətdən təminatı kimi mühüm vəzifələrin və müxtəlif sahələrdə mürəkkəb problemlərin öhdəsindən gəlməyə qadir olan yüksəkixtisaslı mütəxəssislərin hazırlanmasının əsasını təşkil edir [8]. Hərbi kontekstdə mühəndislik işi silahlı qüvvələrin mühəndis təminatının təşkili, daha çox qabaqcıl mühəndis silahlandırma vasitələrinin və silah sistemlərinin tətbiqi, hərbi infrastrukturun qurulması və əməliyyatların aparılması üçün olduqca vacibdir. Hərtərəfli nəzəri biliklərə, praktiki bacarıq və tənqidi düşünmə qabiliyyətinə, eləcə də liderlik keyfiyyətlərinə malik mühəndis ixtisaslı zabitlərin hazırlanması ilə hərbi institutlar, həm də onların formalaşan əməliyyat bacarıqları sayəsində gələcəkdə baş verə biləcək təhlükələri effektiv həll edə bilməsinə nail olar. Hərbi mühəndislik peşə sahəsi xüsusi təlim yanaşmaları tələb edən xüsusi sənət növü olmaqla, unikal problemlərin həllinə kömək edir. Mülki mühəndislikdən fərqli olaraq, hərbi mühəndislik: sahə bilikləri və bacarıqlarına yiyələnmiş; uyğunlaşmaya, komanda tərkibində fəaliyyət göstərməyə (bölmə, qrup), inteqrasiyaya; liderliyə və yüksəkstressli mühitlərdə işləmək qabiliyyətinə malik güclü əzm, iradə və s. xüsusiyyətlərin olmasını tələb edir. İnsan faktorlarını araşdıran mütəxəssislər mühəndis hazırlığının didaktik layihələndirilməsi və ixtisasçı kadrların peşə sahəsinə hazırlanması zamanı hərbi mühəndis vəzifələrinin nəzərə alınmasında mühüm olan xüsusiyyətləri qeyd edirlər [9]. Bu xüsusiyyətlərə daxildir:

- yüksək texnoloji sistemlərdə ixtisas təcrübələri;
- stressli iş şəraiti;
- sərt ekoloji ekstremal şərait;
- tez-tez icra ediləcək tapşırıqlarla həddindən artıq yüklənməsi şəraiti;
- tez və dəqiq qərar qəbuletmə tələbi;
- həssas şəraitdə davranış tərzləri;
- operativlik.

HATM-də mühəndis hazırlığı üçün didaktik layihələndirmə prosesində qarşıya qoyulan tapşırıqların icrası zamanı hərbi əməliyyatların mürəkkəbliyi və çətinliyini nəzərə alaraq, müvafiq mühəndis təminatı biliklərinin aşılanması mühüm əhəmiyyət kəsb edir. Bu baxımdan peşə vəzifələrinin öhdəsindən gələ biləcək mühəndislər hazırlamaq üçün qeyd edilən fərqli tələb və vəzifələr nəzərə alınmalıdır [10].

Didaktik layihələndirmə prosesinin mahiyyəti isə onun mühəndislik təhsilinə strukturlaşdırılmış və sistemli yanaşma qabiliyyətindən ibarətdir. Bu qabiliyyətlər hərtərəfli hərbi mühəndislərin hazırlanması üçün həm nəzəri bilikləri, həm də praktik vərdişləri özündə ehtiva etməlidir. Ali təhsil proqramlarının layihələndirilməsi təhsilalanların ixtisas sahəsinə və xarakteristikasına müvafiq olaraq, ali təhsil pilləsi üzrə hərbi institutların kafedralarında tədris planı əsasında hazırlanır [11].

Didaktik layihələndirmə prosesinin anlamaq üçün aşağıdakı amillərə üstünlük verməlidir:

1. Hərbi mühəndislik üzrə ixtisas proqramının (kurikulumun) inkişafı üçün milli kurikulumun məzmunu. Bunun üçün zəruri olan mühəndislik bacarıqlarının formalaşdırılması vacib hesab edilir. Çünki milli kurikulum mühəndislik prinsiplərini və hərbi xüsusi fənləri özündə birləşdirən xüsusi hərbi məqsədlərə uyğunlaşdırılmalıdır. Hərbi mühəndis hazırlığı ixtisasına yiyələnmədə informasiya texnologiyaları, elektronika və telekommunikasiya, hərbi əməliyyatların idarə edilməsi, hərbi coğrafi sistemlər, mühəndis texnologiyaları, idarəetmə, logistika və strateji planlaşdırma kimi xüsusi və fundamental fənlərin inteqrasiyası mövcuddur.

2. Aktiv öyrənmə və praktik təlim modelləri üzrə metodologiyanın yaradılması. Didaktik layihələndirmə prosesində akademik heyət, təhsilalanların problemlərini (tapşırıqları) həll etmək üçün ilk növbədə onun metodoloji əsaslarını müəyyənləşdirməli və bu metodoloji əsaslar üzrə fəaliyyətini davam etdirməlidir. HATM-nin kursantlarına verilən məlumatlar müəyyən edilmiş tədris işinin növlərinə və metodoloji əsasların modellərinə istinad etməklə tətbiq olunmalıdır. Aktiv öyrənmədə tənqidi düşünmə və qərar qəbuletmə fəaliyyətlərinə təşviq edən fəal təlim metodologiyalarına diqqət yetirməlidir. Praktik təlimdə isə hərbi texnika, sahə təlimləri və simulyasiyalarla praktiki təcrübə təmin etmək çox vacibdir. Real həyat ssenarilərini daxil etməklə, kursantlar hərbi mühəndislikdə tələb olunan zəruri bacarıqları, praktiki və qərar qəbuletmə bacarıqlarını inkişaf etdirə bilərlər [12].

3. Liderlik, əməkdaşlıq və komanda işi üzrə fəaliyyət modelinin tətbiqi. Bu model üzrə verilən biliklər sayəsində hərbi mühəndislər arasında liderlik, idarəetmə, əməkdaşlıq və komanda işi olmaqla, bir sıra bacarıqların formalaşdırılmasına və səmərəli inkişafına nail olmaq mümkündür. Qrup layihələri üzrə verilən tapşırıqlar və komanda əsaslı fəaliyyətlər təhsilalanlara effektiv ünsiyyət, koordinasiya və liderlik qabiliyyətlərini inkişaf etdirməyə imkan verir. Bu bacarıqlar mühəndisləri tez-tez digər hərbi müəssisə və qurumlarla, mütəxəssislərlə, eyni zamanda sənaye ilə sıx əməkdaşlıq etməyə istiqamətləndirir və mühəndislik üçün yeni innovasiyaların tətbiqi təcrübələrini qazandırır.

4. Hərbi dəyərlərin, etik normaların və mənəvi keyfiyyətlərin formalaşdırılması. HATM-nin kursantlarının peşə sahələrində müvəffəqiyyətli olması üçün etik normaların, əxlaqi-mənəvi keyfiyyətlərin aşılanması da mühüm əhəmiyyət kəsb edir. Peşə və texniki bacarıqlara əlavə olaraq didaktik prosesdə etik və əxlaqi təlim də vurğulanmalıdır. Hərbi dəyərlərin aşılanması mühəndislərin yüksək etik və ictimai davranış, peşəkarlıq və dürüstlük standartlarına riayət etmələrini şərtləndirir. Gələcəyin komandirlərinin qərar qəbuletmə prosesinə etika təlimləri və praktiki ssenarilərin daxil edilməsi hərbi mühəndislikdə tələb olunan dəyərləri aşılamağa kömək edəcəkdir. Hərbi pedaqogikanın predmeti olan hərbi etika yüksək mənəvi dəyərlərə sahib, dünyagörüşlü zabitlərin və hərbi liderlərin hazırlanmasında mühüm rol oynayır. Etika və əxlaq normalarına sahib hərbi rəhbərlər qoşunların rifahını yüksəldir və qanunsuzluqların, çatışmazlıqların qarşısını alır. Əlbəttə, ilkin mərhələdə planlaşdırılıb keçirildikdə, hərbi liderlərin formalaşdırılmasına kömək edir və təlimin növbəti mərhələlərində vəzifələrin uğurla yerinə yetirilməsi üçün vacibdir [13].

Didaktik yanaşmanın hərbi elmi-pedaqoji təhlilinin xüsusiyyətləri

Müstəqillik qazandığımız ilk dövrlərdən hazırkı dövrə qədər olan müddətdə fənn modullarının və işçi tədris planlarının hazırlanması, həmçinin didaktik layihələndirmənin müxtəlif mərhələlərlə təkmilləşməsi prosesinə nəzər salsaq, oxşar və fərqli cəhətlərin olduğunu görərik [3]. Ümumilikdə elmi pedaqoji təkamülün akademik göstəricilərinin təhlilindən aydın olur ki, ötən dövrlərdə didaktik yanaşmaların metodologiyasında, milli və ümumbəşəri dəyərlərin əks etdirilməsində ciddi dəyişiklər baş vermişdir. Azərbaycanda hərb təhsilinin dünya hərb təhsilinə – NATO və Türkiyə modelinə inteqrasiyası baxımından fənn modullarının tərtib edilməsi və tətbiqi müsbət qiymətləndirilir. Məlumdur ki, hərb elmi və hərbi təhsilin modernləşdirilməsi və inkişafı istiqamətində hazırda ciddi işlər görülür. Bu da hərbi təhsilin bütün pillələrində təlimin qanun və qanunauyğunluqlarına, prinsiplərinə, metodlarına, təşkili formalarına, bütövlükdə didaktik əsasların qoyuluşu və tətbiqinə yeni müasir mövqedən yanaşmanı tələb edir. Didaktik yanaşmaların təkmilləşdirilməsi isə təhsilalanların hərbi təlimə olan maraqlarını və meyillərini artırmış olur [14].

Mühəndis hazırlığı ixtisası üzrə xüsusi hərb elminin mənimsənilməsi üçün bir sıra elm sahələri üzrə fənlərin tədrisi zəruridir. Bunun üçün əsas mühəndislik fənləri sırasına riyaziyyat, fizika, mexanika, elektronika, materialşünaslıq və kompüter elmləri kimi fundamental mühəndislik fənləri ilə yanaşı, sosialyönümlü, humanitar və milli təhlükəsizlik sahələrinin fənn modulları daxil edilməlidir. Ona görə ki, bu fənlər qabaqcıl mühəndislik bilikləri ilə inteqrasiya üçün vacib hesab edilir. Eyni zamanda hazırkı proqramlarda hərbi mühəndislik biliklərinin tədrisində bir sıra dəstəkləyici və hərəkətverici fənn mövzularına üstünlük verilmişdir. Bura daxildir: döyüş mühəndisliyi, hərbi əməliyyatların idarə edilməsi, informasiya texnologiyaları, elektronika və telekommunikasiya, hərbi coğrafi sistemlər, mühəndis texnologiyaları, mühəndis qrafikası, idarəetmə, logistika və onun əsasları, strateji planlaşdırma.

Bu fənlər mühəndisləri hərbi vəzifələrinin səmərəli icrası üçün zəruri olan xüsusi bilik və bacarıqlarla təchiz edir.

Fənlərarası tədqiqatların aparılması çox faydalıdır. Belə ki, mühəndislik proqramının layihələndirmə prosesində fənlərarası əlaqələrin tədqiqi, inteqrasiyası hərbi mühəndislərin psixologiya, sosiologiya, siyasi elmlər və iqtisadiyyat kimi digər sahələrə olan maraqlarını artırmış olur. Bu isə daha geniş perspektivdə mühəndislik işlərinin sosial, siyasi və iqtisadi nəticələrini başa düşməyə imkan verir.

Hərbi mühəndislər üçün peşəkarlığın inkişaf etdirilməsi onların hərbi xidməti sahəsindəki qazana biləcəyi uğurlarında faydalı olacaqdır. Çünki peşəkarlığın artırılması mühəndislərin komandalara rəhbərlik etmək, effektiv ünsiyyət qurmaq, layihələri idarə etmək və etik problemləri həll etmək bacarığını formalaşdırır.

HATM-də mühəndis hazırlığı üçün didaktik layihələndirmə prosesi aşağıdakı elementləri özündə birləşdirir:

1. Ehtiyacların qiymətləndirilməsi. Proqramların tərtib edilməsindən əvvəl HATM-nin xüsusi tələblərini və hərbi mühəndislərin arzuolunan bacarıq və səriştələrini müəyyən etmək üçün ehtiyacların hərtərəfli qiymətləndirilməsi aparılmalıdır. Bu qiymətləndirmə təlim prosesini HATM-nin məqsədlərinə uyğunlaşdırmağa kömək edir və fənn proqramlarının buna uyğun tərtib olunmasını təmin edir.

2. Öyrənmə məqsədləri. Layihələndirmə prosesinə rəhbərlik etmək üçün aydın və ölçülə bilən təlim məqsədləri müəyyənləşdirilməlidir. Bu məqsədlər kursantların təlim proqramını başa vurduqdan sonra əldə etməli olduqları bilik, bacarıq və münasibətləri ifadə etməlidir.

3. Tədris strategiyaları. Tədris strategiyalarının tərkib hissələrindən biri olan fənn proqramlarının layihələndirmə prosesi fənlərin keçirilmə formasını – mühazirələr, müzakirələr, laboratoriya işləri, real nümunələr, simulyasiyalar və praktiki sahə məşqləri də daxil olmaqla, müxtəlif tədris strategiyalarını özündə birləşdirməlidir. Bu strategiyalar müxtəlif öyrənmə üslublarına uyğunlaşır və aktiv əlaqəni təşviq edir.

4. Qiymətləndirmə metodları. Kursantların materialı başa düşməsini, tətbiq etməsini və mənimsəməsini qiymətləndirmək üçün imtahanlar, layihələr, təqdimatlar, praktiki nümayişlər və fəaliyyətin qiymətləndirilməsi də daxil olmaqla, bir sıra metodlardan istifadə olunmalıdır.

5. Davamlı inkişaf. Didaktik işin layihələndirilməsi prosesi davamlı təkmilləşdirmə mexanizmlərini özündə birləşdirməlidir. Təhsilalanlardan, təlimatçılardan və hərbi mütəxəssislərdən mütəmadi rəylər toplanmalı, sorğu və müsahibələr keçirilməlidir. Əldə olunan nəticələrin təhlili tədris planının və təlim metodlarının təkmilləşdirilməsi üçün istifadə olunmalı, təlimin aktuallığı təmin edilməlidir.

Didaktik layihələndirmədə sistemli yanaşma

Didaktik layihələndirmə prosesi təhsilverənlərin fəaliyyətlərinin optimallaşdırılmasını, təhsilalanların isə bilik və bacarıqlarının mənimsənilməsini asanlaşdırmaq və praktik vərdişlərini inkişaf etdirmək üçün qəbul edilmiş sistematik yanaşmaya aiddir. O, təhlil, layihələndirmə, həyata keçirmə və qiymətləndirmə daxil olmaqla, bir-biri ilə əlaqəli olan bir sıra mərhələləri əhatə edir. HATM-də mühəndis hazırlığı kontekstində didaktik layihələndirmə prosesi hərbi mühəndislərin unikal ehtiyac və tələblərinə uyğunlaşdırılır.

Təhlil: bu mərhələ, mühəndis hazırlığı proqramının məqsədləri, vəzifələri və məhdudiyyətlərinin, eyni zamanda çətinliklərinin müəyyən edildiyi didaktik layihələndirmə prosesinin ilkin mərhələsidir. Hərbi kontekstdə bu mərhələ hərbi mühəndislərin öz vəzifələrini səmərəli şəkildə yerinə yetirmələri üçün tələb olunan bacarıq, bilik və səriştələrin hərtərəfli qiymətləndirilməsini nəzərdə tutur. Təhlil mərhələsi, həmçinin hərbi mühəndislərin üzləşdiyi xüsusi əməliyyat kontekstlərini və çətinlikləri nəzərə alır, təlim proqramının real dünya ssenarilərinə uyğun olmasını təmin edir.

Tərtibat: didaktik layihələndirmə prosesinin tərtibetmə mərhələsi təhsilalanlara müəyyən edilmiş məqsədlərə nail olmağa imkan verir və didaktik fəaliyyətlərinin strukturlaşdırılmasını təmin edir. Mühəndis hazırlığında bu mərhələ nəzəri bilikləri, praktiki bacarıqları və praktiki təcrübəni əhatə edən əlaqəli işçi proqramların hazırlanmasını nəzərdə tutur. Tərtibetmə mərhələsi, həmçinin təlim nəticələrini optimallaşdırmaq üçün müvafiq təlim strategiyalarının, resurslarının və qiymətləndirmə metodlarının seçilməsini özündə birləşdirir.

Tətbiq: icra mərhələsi, hazırlanmış işçi proqramların hərəkətə gətirilməsi və birbaşa tətbiqinin aparılmasıdır. Mühəndis hazırlığında bu mərhələ mühazirələrin, praktiki məşğələlərin, simulyasiyaların və sahə təlimlərinin xüsusi ayrılmış siniflərdə, auditoriya və təlim mərkəzli laboratoriya və sahələrdə keçirilməsini nəzərdə tutur. Tətbiq mərhələsi, həmçinin öyrənmə təcrübəsini artırmaq üçün virtual reallıq və ya kompüter əsaslı təlim sistemləri kimi qabaqcıl texnologiyaların istifadəsini əhatə edə bilər. Bundan əlavə, icra mərhələsi hərbi mühəndislik sahəsində həm akademik biliklərə, həm də praktik təcrübəyə malik ixtisaslı professor-müəllim və təlimçilərin fəaliyyətini nəzərdə tutur.

Qiymətləndirmə: nəticələrin əldə edilməsi, səmərəliliyin yoxlanması mərhələsi mühəndis hazırlığı proqramının effektivliyinin ölçülməsində, qiymətləndirilməsində və lazımi təkmilləşdirmələrin aparılmasında mühüm əhəmiyyət kəsb edir. Bu mərhələdə kursantların müəyyən edilmiş məqsədlərə nail olmasını ölçmək üçün yazılı imtahanlar, klassik, praktiki və sahələr üzrə fəaliyyətin yoxlanılması kimi müxtəlif qiymətləndirmə üsullarından istifadə edilir. Qiymətləndirmə həm öyrənənlər, həm də müəllim-professor, təlimatçılar tərəfindən rəy bildirməyə imkan verir. Bütün zamanlarda olduğu kimi, qiymətləndirmələr həm tədris və təlimin formal təkmilləşdirilməsi, həm də təhsilverənlərin, HATM-lərin və onlara rəhbərliyi həyata keçirənlərin yekun hesabatının qiymətləndirilməsi üçün dəstək funksiyasını icra edir. Həmçinin təlim proqramının davamlı təkmilləşdirilməsinə kömək edir və nəticədə əlavə diqqət tələb edən sahələri müəyyənləşdirir [15].

Bütün bunlar deməyə əsas verir ki, didaktik işin layihələndirilməsi prosesinin bir sıra üstünlükləri vardır. Onları aşağıdakı kimi qruplaşdırmaq olar:

1. Tədris məqsədlərinə uyğunlaşma: didaktik layihələndirmə prosesinin strukturlaşdırılmış xarakteri mühəndis hazırlığı proqramının hərbi mühəndislərin xüsusi təlim məqsədlərinə uyğun olmasını təmin edir. Təlim proqramı zəruri bacarıq və bilikləri müəyyən etməklə, hərbi əməliyyatların və infrastrukturun inkişafının tələblərini səmərəli şəkildə həll edə bilər.

2. Kontekstlə əlaqəlilik: didaktik layihələndirmə prosesi hərbi mühəndislərin üzləşdiyi real ssenarilərin və problemlərin inteqrasiyasına imkan verir. Bu, təlim proqramını öyrənənlərin gələcək tapşırıqların mürəkkəbliyi və tələblərinə hazırlığını, həmçinin əməliyyat hazırlığını təmin edir.

3. Resurslardan optimal istifadə: diqqətli təhlil və layihələndirmə vasitəsilə didaktik layihələndirmə prosesi resurslardan, o cümlədən hərbi mütəxəssislərdən, təlimatçılardan, qurğulardan və avadanlıqlardan səmərəli istifadəyə imkan verir. Əlavə olaraq, HATM-lərə büdcə məhdudiyyətləri daxilində effektiv təlimlərin keçirilməsini təmin edir.

4. Davamlı təkmilləşdirmə: didaktik layihələndirmə prosesinin qiymətləndirmə mərhələsi mühəndis hazırlığında davamlı təkmilləşmə mədəniyyətini təşviq edir. Təlim proqramlarının nəticələrinin, güclü və zəif tərəflərinin müntəzəm olaraq qiymətləndirilməsi, çatışmazlıqların aşkarlanaraq aradan qaldırılması baxımından mühüm əhəmiyyət kəsb edir.

Göründüyü kimi, HATM-də mühəndis hazırlığının didaktik layihələndirilməsi prosesi, hərbi mühəndislər tərəfindən bilik və bacarıqların səmərəli şəkildə mənimsənilməsini təmin edən strukturlaşdırılmış və sistemli yanaşma fəaliyyətidir. Təhlil, layihələndirmə, həyata keçirmə və qiymətləndirmə mərhələləri vasitəsilə bu proses təlim proqramlarının təlimin məqsədlərinə, kontekstlə uyğunlaşdırılmasına, resursların optimal istifadəsinə və davamlı təkmilləşdirilməsinə imkan verir.

Nəticə

Hərbi ali təhsil müəssisələrində mühəndis hazırlığının didaktik layihələndirilməsi işinin məqsədyönlü və mütəşəkkil həyata keçirilməsi, hərbi pedaqoji işin elmi təşkili prosesinin davamlı təkmilləşdirilməsini təmin etmiş olar. Bu prosesin səmərəli təşkili və keçirilməsi, bacarıqlı və peşəkar hərbi mühəndislərin hazırlanması üçün çox vacibdir. Hərbi ali təhsil müəssisələrində mühəndis hazırlığının didaktik layihələndirilməsinin mahiyyəti, məzmunu, məqsəd və vəzifələri strukturlaşmış fəaliyyətlərin aparılması və tətbiqini ehtiva edir. Layihələndirmə prosesinin davamlı tətbiqi və təkmilləşdirilməsi mühəndis hazırlığının səmərəliliyinin artırılmasında və cari vəzifələrin ordunun inkişaf edən ehtiyaclarına uyğunluğunun təmin edilməsində mühüm rol oynayır. Eyni zamanda bu proses mühəndis kadrlarını hərbi mühəndislik peşəsinin unikal çağırışlarına cavab verməyə hazırlayır. Fənn proqramlarının didaktik layihələndirməsi aktiv öyrənmə, əməkdaşlıq, etik təlim, strukturlaşdırılmış təlimatlara və əsasnamələrə diqqət yetirməklə təmin oluna bilər. Vurğulanan elmi yanaşmalar HATM-lərə öz təlim proqramlarını optimallaşdırmağa və onların inkişaf edən ehtiyaclarının və problemlərinin həllində effektivliyini təmin etməyə imkan verir. Layihələndirilmə prosesinin tətbiqi ilə HATM-lər mühəndis hazırlığının müasir təlim texnologiyalarının mənimsənilməsinə, ordunun inkişaf edən ehtiyaclara uyğunlaşmasına və səmərəliliyini artırılmasına nail ola bilərlər. Məqalənin məzmunu, orada yer alan fikirlər və əsas elmi ideyalardan HATM-nin bakalavriat, magistratura pilləsində təhsil alanlar, doktorantlar (adyunkt) və müəllimlər istifadə edərək faydalana bilərlər.

İstifadə edilmiş ədəbiyyat siyahısı

1. Dadaşov, A.S., Designing military engineering training based on the model of didactic justification / Journal of Defense Resources Management 14:2(2023): 87-96.
URL: http://www.jodrm.eu/issues/Volume14_issue2/8_dadashov.pdf

2. Dadaşov, A.S., Hərbi institutda mühəndis hazırlığının didaktik layihələndirilməsi vəziyyətinin təhlili // – Bakı: Azərbaycan Respublikasının Təhsil İnstitutunun Elmi əsərləri, -2023, №4, -s. 47-51.

3. Dadaşov, A.S., Azərbaycan Respublikasında hərbi – mühəndis təhsili tarixinin – pedaqoji təhlili // – Bakı: Azərbaycan Respublikasının Təhsil İnstitutunun Elmi əsərləri – 2023. №6. – s. 227-231.

4. Bəşirov, V. Pedaqoji fəaliyyətin hədəfləri: [Elektron resurs] / Azərbaycan müəllimi – Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin orqanı / – Online qəzet.– 6 sentyabr, 2019. URL: https://muallim.edu.az/news.php?id=7240

5. Anderson, L. W. and Krathwohl, D. R. A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. – MA Boston: Allyn & Bacon. – 2001, p.7: [Electronic resource] / URL:https://quincycollege.edu/wp-content/uploads/Anderson-and-Krathwohl_Revised-Blooms-Taxonomy.pdf

6. Məhsimova, S. Tədrisdə universal layihələndirmə: [Elektron resurs] / Azərbaycan müəllimi-Azərbaycan Respublikasının Elm və Təhsil Nazirliyinin orqanı / – Online qəzet.– 19 oktyabr, 2018. URL: https://muallim.edu.az/news.php?id=2713

7. Кондратьев, В.В. Инженерная педагогика как основа системы подготовки преподавателей технических университетов // Москва: Высшее образование в России. – 2018. №2. (220). – с. 29-38.

8. Azərbaycan Respublikası Müdafiə Nazirliyi Azərbaycan Ordusunun hərbi elm və təhsil sistemi (14 yanvar 2024-ci il): [Elektron resurs] / URL:https://mod.gov.az/az/azerbaycan-ordusunun-herbi-elm-ve-tehsil-sistemi-326/

9. Gerald, P.K. Military Engineering Psychology: Setting the Pace for Exceptional Performance: [Electronic resource] / – January, 2012. URL:https://www.researchgate.net/publication/282932688_Military_Engineering_Psychology_Setting_the_Pace_for_Exceptional_Performance

10. Silahlı Qüvvələrdə mühəndis təminatı üzrə Təlimat // – Bakı: Hərbi Nəşriyyat – 2015. – 228 s.

11. Xüsusi təyinatlı təhsil müəssisələrinin təhsil fəaliyyətinin təşkili haqqında Təlimat // – Bakı: Hərbi Nəşriyyat, – 2015. – 90 s.

12. Piriyev, H. Hərbi təhsildə təlim metodları. Metodiki vəsait / H.K.Piriyev, M.P.Həmidov, E.Q.Həşimov // – Bakı: Hərbi Nəşriyyat, – 2017. – 52 s.

13. Piriyev, H.K. The role of military ethics and morale as a subject of pedagogy in the leadership training of officers for multinational environment / Romania: Journal of Defense Resources Management – 2019. 10:2: – p.21-29: [Electronic resource] / URL:http://www.jodrm.eu/issues/Volume10_issue2/02_military%20ethics%20_Heydar%20Piriyev_AZE.pdf

14. Sadıqov, F.B. Didaktika. Ali məktəblər üçün dərs vəsaiti. / F.B.Sadıqov, Q.Q.Həsənli – Bakı: Elm və Təhsil – 2015. – 269 s.

15. Brown, G.T. The past, present and future of educational assessment: [Electronic resource] / – A transdisciplinary perspective. Frontiers Education-Conceptual analysis. November 11, 2022. DOİ: https://doi.org/10.3389/feduc.2022.1060633

Аннотация

Сущность, содержание, цели и обязанности дидактического проектирования инженерной подготовки в военном институте

Амиль Дадашов

В статье рассмотрены основы дидактического проектирования инженерной подготовки в военных вузах и содержание работ, проводимых на этих основах. Цель научно-исследовательской работы - подчеркнуть теоретические основы дидактического проектирования подготовки военных инженеров, особенности военного научно-педагогического анализа дидактического подхода и системного подхода в дидактическом проектировании. Военные высшие учебные заведения могут предвидеть потенциальные проблемы и вовремя адаптировать программы обучения. С этой целью текущая ситуация требует комплексных исследований и анализа для выявления новых технологий, развивающихся угроз и меняющихся оперативных требований. В статье говорится об основах дидактического проектирования инженерной подготовки в военных вузах и содержании работ, проводимых на этих основах. Также в статье рассматриваются способы определения эффективности научно-педагогической деятельности

процесса дидактического проектирования с использованием научных идей и положений. При исследовании проблемы был использован метод теоретического анализа. По полученному результату показано, что дидактический проект содержит сущность, содержание и структуру программы обучения. Этот процесс играет решающую роль в повышении эффективности предоставляемого образования. Научные идеи и положения, содержащиеся в статье, призваны обосновать важность и рациональность дидактического проектирования процесса инженерной подготовки в военных вузах.

Ключевые слова: военное образование, учебный процесс, военный институт, инженерная подготовка, основы дидактики

Abstract
Principles of didactic design of engineer training
in military higher education institutions
Amil Dadashov

In the article, the basics of the didactic design of engineering training in military higher education institutions and the content of the works carried out on these bases were examined. The purpose of the research work is to emphasize the theoretical foundations of didactic design for military engineer training, the features of the military scientific-pedagogical analysis of the didactic approach, and the systematic approach in didactic design. Military higher education institutions can anticipate potential challenges and adapt training programs in time. To this end, the current situation calls for comprehensive research and analysis to identify emerging technologies, evolving threats, and changing operational requirements. The article talks about the basics of the didactic design of engineering training in military higher education institutions and the content of the works carried out on these bases. The article also looks at the ways of determining the efficiency of the scientific pedagogical activity of the didactic design process with scientific ideas and provisions. The theoretical analysis research method was used in the investigation of the problem. According to the obtained result, it is shown that didactic design contains the essence, content and structure of the training program. This process plays a crucial role in improving the efficiency of the education provided. The scientific ideas and propositions contained in the article try to justify the importance and rationality of the didactic design process of engineering training in military higher education institutions.

Keywords: military education, training process, military institute, engineer training, didactic basics

Məqalə redaksiyaya daxil olmuşdur:26.02.2024
Təkrar işlənməyə göndərilmişdir: 05.03.2024
Çapa qəbul edilmişdir:02.04.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 70-82
HƏRBİ XÜSUSİ ELMLƏR ***MILITARY SPECIAL SCIENCES***

UOT 93/94 DOI: 10.30546/9878.2024.2.10.0025.

AZƏRBAYCAN XALQ CÜMHURİYYƏTİ DÖVRÜNDƏ HƏRBİ DİPLOMATİYA

Mehman Süleymanov
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
smehman@mail.ru

Xülasə. Ölkənin hərbi təhlükəsizliyinin təmin edilməsi sahəsində Azərbaycan Xalq Cümhuriyyəti hökumətinin qarşısında duran başlıca vəzifələrdən biri də beynəlxalq hərbi əməkdaşlığın qurulması idi. 23 ay davam edən müstəqillik illərində Cümhuriyyət hökuməti bu istiqamətdə bir sıra işlər görməyə müvəffəq oldu. İlk növbədə Osmanlı Türkiyəsi ilə hərbi əməkdaşlıq sahəsində praktiki tədbirlər həyata keçirildi. Mövcud olan təhlükənin aradan qaldırılması, Azərbaycanın müstəqilliyinin və ərazi bütövlüyünün təmin edilməsi ilə bağlı bu əməkdaşlıq səmərəli nəticələr verdi. Bu mövzu kifayət qədər geniş mövzu olsa da, onun müəyyən tərəfləri məqalədə öz əksini tapmışdır. Məqalədə, eyni zamanda Gürcüstanla qurulan beynəlxalq hərbi əməkdaşlıq sahəsində təhlil aparılmışdır. Xüsusilə Osmanlı hərbi qüvvələrinin Azərbaycanı tərk etməsindən sonra Gürcüstanla hərbi əməkdaşlığın genişləndirilməsinə diqqət artırıldı. Məqalədə, həmçinin Böyük Britaniya və Avropanın digər dövlətləri, o cümlədən İtaliya və Fransa ilə Azərbaycan Xalq Cümhuriyyəti arasında qurulan hərbi əməkdaşlıq məsələlərinə də toxunulmuşdur. Cümhuriyyət dövründə hərbi diplomatiyanın ümumiləşdirilmiş şəkildə araşdırılması ilk dəfədir ki, tədqiqat mövzusuna çevrilmişdir. Bu mənada əldə edilmiş nəticələr də mövzu baxımından yenidir.

Açar sözlər: cümhuriyyət, müstəqillik, milli ordu, hərbi siyasət, hərbi əməkdaşlıq

Giriş

Birinci Dünya müharibəsinin hərbi-siyasi nəticələri, çar Rusiyasının süqutu Cənubi Qafqaz bölgəsində, o cümlədən Azərbaycan hüdudlarında mürəkkəb bir şəraitin meydana gəlməsinə yol açdı. Bölgə ilə bağlı geosiyasi və iqtisadi maraqlarını təmin etməyə çalışan böyük dövlətlərin, böyük güclərə arxalanaraq kütləvi şəkildə silahlanan və yad ərazilərdə öz dövlətini qurmaq istəyən erməni millətçi təcavüzkar dairələrinin bölgədə fəallaşması Azərbaycan xalqının mövcudluğuna ciddi təhlükə yaratdı. Ona görə Azərbaycanın milli-azadlıq hərəkatının liderləri və fəalları bu təhlükədən xilas olmaq və etibarlı müdafiə imkanlarına malik müstəqil bir dövlət qurmaq üçün səmərəli yollar axtarmağa başladılar. Azərbaycan Xalq Cümhuriyyəti elan ediləndən sonra isə hökumət tərəfindən təhlükəsizlik sahəsində beynəlxalq əməkdaşlığın qurulması istiqamətində səmərəli siyasət həyata keçirilməyə başlandı. Bu istiqamətdə hökumət tərəfindən prioritetlər müəyyənləşdirildi, Azərbaycanın hərbi təhlükəsizliyinin təmin edilməsi üçün hökumət və parlament tərəfindən razılaşdırılmış bir siyasət ortaya qoyuldu. Belə bir siyasətin uğurlu şəkildə həyata keçirilməsi həm beynəlxalq təcrübənin öyrənilməsi, həm də ordunun texniki təchizatının təkmilləşdirilməsi baxımından mühüm əhəmiyyət kəsb edirdi.

Türkiyə ilə hərbi əməkdaşlıq

Müstəqilliyin əldə edilməsindən sonra Azərbaycan hökumətinin hərbi əməkdaşlıq qurmağa çalışdığı ilk dövlətlərdən biri Türkiyə idi və bu münasibətlərin əsası 1918-ci il iyunun 4-də Batumda Osmanlı dövləti ilə Azərbaycan Xalq Cümhuriyyəti hökuməti arasında imzalanan müqavilə ilə qoyuldu. Həmin müqavilənin 4-cü maddəsində bildirilirdi ki, ölkə daxilində nizam və asayişin yaradılması üçün müraciət edildiyi təqdirdə, Osmanlı dövləti Azərbaycana hərbi yardım göstərə bilər [1, v.43-45].

Azərbaycan hökuməti də bu imkandan istifadə edərək dərhal hərbi kömək üçün Osmanlı dövlətinə müraciət etdi. Həmin müraciət əsasında ilkin olaraq, Osmanlı Ordusunun 5-ci Qafqaz piyada diviziyası Azərbaycana gəldi. Azərbaycanın milli hərbi qüvvələri ilə Osmanlı hərbi qüvvələrinin bazasında Qafqaz İslam Ordusu yaradıldı və türk zabiti general-leytenant Nuru paşa bu ordunun komandanı təyin edildi. Mövcud tarixi şəraitin xüsusiyyətləri nəzərə alınmaqla, Azərbaycan hökumətinin qərarına əsasən

Cümhuriyyət Ordusunun formalaşdırılmasına rəhbərlik də Qafqaz İslam Ordusu komandanına həvalə edildi.

1918-ci ilin iyulunda Azərbaycanla Osmanlı Türkiyəsi arasında uzunmüddətli hərbi ittifaqın yaradılması haqqında da müqavilə layihələri hazırlanmışdı [2, s.555; 3, s.290-295]. Bu layihələr iki variantda idi və hər ikisi "Mukavile-i Askeriyye" adlanırdı. 14 maddədən ibarət olan birinci müqavilənin 90, 8 maddədən ibarət olan ikinci müqavilənin isə 20 illik müddətə bağlanması nəzərdə tutulmuşdu. Həmin müqavilələrin əsas məzmunu ondan ibarət idi ki, Azərbaycanın Milli Ordusu bütünlüklə Osmanlı hərbi qüvvələrinin əməliyyat tabeliyinə verilməli, Osmanlı dövləti isə Azərbaycan Milli Ordusunun təchizatını, onun kadr hazırlığını öz üzərinə götürməli idi [4, s.295]. Lakin bu müqavilələr imzalanmadı. Çox güman ki, buna səbəb beynəlxalq vəziyyətin dəyişməsi və tezliklə Qafqaz İslam Ordusunun ləğv edilməsi olmuşdu.

Azərbaycanla Türkiyə arasında mövcud hərbi əməkdaşlığın ən mühüm tarixi nəticəsi, sözsüz ki, müştərək hərbi qüvvələrin iştirakı ilə 1918-ci il sentyabrın 15-də Bakı şəhərinin və sonrakı ay isə Azərbaycanın Qarabağ bölgəsinin bolşevik-daşnak işğalından azad edilməsi oldu. Nəzərdə tutulmuşdu ki, Qafqaz İslam Ordusu qüvvələrinin köməyi ilə Azərbaycanın cənubunda da respublikanın suverenliyi təmin edilsin və həmin bölgə orada nəzarəti ələ keçirmiş ağqvardiyaçı qüvvələrdən təmizlənsin. Bu məsələ 1918-ci il noyabrın 1-də Bakıda Nuru paşanın Lənkəran bölgəsi əhalisinin nümayəndələri ilə görüşündə də müzakirə edilmişdi [5]. Lakin tezliklə türk hərbi qüvvələrinin Azərbaycanı tərk etməsi səbəbindən Lənkəran bölgəsində respublika hakimiyyətinin bərqərar edilməsi təxirə salınmalı oldu.

Milli Ordunun təşkilatlanması sahəsində hərbi əməkdaşlığın nəticələrinə gəlincə isə milli zabit kadrlarının yetişdirilməsində, ordu hissələrinin hərbi-texniki təchizində, hərbi strukturların yaxşılaşdırılmasında Türkiyə tərəfindən Azərbaycana böyük kömək göstərildi. Belə ki, Qafqaz İslam Ordusu komandanının əmrinə əsasən, 1918-ci il avqust ayının 13-də Əlahiddə Azərbaycan Korpusunun yenidən qurulmasına başlanıldı [6, s.185]. Azərbaycan korpusunun təşkilatlanması və qısa zamanda döyüşə hazır vəziyyətə gətirilməsi üçün onun tərkibinə daxil olan hissələrin Azərbaycan–Türk hərbi qüvvələrindən komplektləşdirilməsi qərara alındı[7, s.303]. Nuru paşa Azərbaycan hökumətinə göndərdiyi raportlardan birində bildirirdi ki, qarışıq tərkibdə yaradılmış hərbi strukturların sıravi heyətinin yarısı, zabit heyətinin isə böyük hissəsi türk hərbçiləridir. Həmin raportda həmçinin qeyd edilir ki, türk hərbçilərinin köməyi ilə Azərbaycanda iki diviziyadan ibarət bir korpus, dörd alaydan ibarət bir süvari diviziyası, Zəngəzurda əlahiddə atlı bölüyü, Gəncədə bir təlim taboru və bir pulemyot təlim taboru, üç tabordan ibarət bir sərhəd alayı, Ordubadda bir piyada taboru və bir topçu taqımı təşkil olunmuşdur [8, s.396].

Gəncədə açılmış olan Milli Hərbiyyə Məktəbinə rəhbərlik təcrübəli türk zabiti olan qayməqam Atıf bəyə tapşırılmışdı və 1918-ci il oktyabrın 27-də bu məktəbin ilk buraxılışı oldu [9]. Cümhuriyyət Ordusu hissələrinin hərbi-texniki təchizatının daha da yaxşılaşdırılması üçün Türkiyədən xeyli sayda silah və sursat Azərbaycana göndərildi. Bu sahədə əməkdaşlığın gələcəkdə də davam etdirilməsi planlaşdırılmışdı [10, s.279].

1918-ci il oktyabrın 30-da Egey dənizinin Lemnos adasının Mundoros limanında Osmanlı Türkiyəsi ilə Böyük Britaniya arasında Birinci Dünya müharibəsinin nəticələrini özündə əks etdirən barışığa görə Osmanlı Türkiyəsinin məğlubiyyəti rəsmiləşdirildi. Həmin barışığın 11-ci və 15-ci maddələrinə əsasən Osmanlı dövləti öz qoşunlarını Azərbaycandan çıxardı və Azərbaycan ingilis qoşunlarının nəzarətinə keçdi [11, s.170; 12, s.157-158].

Osmanlı hərbi qüvvələrinin Azərbaycanı tərk etməsi və Qafqaz İslam Ordusunun ləğv edilməsi reallığa çevriləndə Nuru paşa 1918-ci il noyabrın 4-də Qafqaz İslam Ordusunun ləğv edilməsi və onun Azərbaycan Ordusu adlandırılması haqqında xüsusi bir əmr imzaladı. Həmin gün imzaladığı digər bir əmrdə isə Nuru paşa özünü Azərbaycan Ordusunun komandanı kimi təqdim etdi [13, s.365-366]: yəni 1918-ci il noyabrın 4-dən etibarən Nuru paşa Qafqaz İslam Ordusunun deyil, Azərbaycan Ordusunun komandanı olaraq fəaliyyətini davam etdirəcəkdi.

Noyabrın 4-də Nuru paşa bu ad altında həm də "Azərbaycan hökuməti ilə burada qalacaq zabitan üçün əqd edilən müqavilə şəraiti" adlı bir müqavilə layihəsini imzaladı. Bu müqavilədə onun özü də

daxil olmaqla, könüllü olaraq Azərbaycanda qalıb Azərbaycan Ordusunda xidmət edəcək türk hərbçilərinin hüquq və səlahiyyətləri təsbit olunmuşdu [13, s.365-366].

Azərbaycan Ordusu komandanlığı elan ediləndə əlahiddə Azərbaycan korpusu ləğv edilməmişdi [14, s.373]. Ona görə də ilk baxışdan belə bir qənaətə gəlinir ki, Nuru paşa Azərbaycan korpusunu və əlavə olaraq Azərbaycanda qalacaq türk hərbçilərindən təşkil edilmiş bölmələrdən formalaşdırılan ümumi bir Azərbaycan Ordusunun komandanı vəzifəsini öz üzərinə götürmüşdü. Amma Azərbaycan Ordusu strukturu ilə 1918-ci il noyabrın 1-də bərpa edilmiş Hərbi Nazirlik arasındakı əlaqə, yəni Azərbaycan Ordusunun Hərbi Nazirliyə paralel, yoxsa onun tabeliyində bir struktur olduğu haqqında dəqiq bir fikir söyləmək hələlik çətindir.

Nuru paşa Osmanlı Hərbi Nazirliyinə ünvanladığı 12 noyabr 1918-ci il tarixli məktubunda Azərbaycan Ordusunun komandanı vəzifəsində Azərbaycan hökumətinin xidmətinə daxil olduğunu bildirirdi[15, s.403]. Bu məlumata əsasən Nuru paşanın Azərbaycan Ordusunun komandanı təyin edilməsinin Azərbaycan hökumətinin razılığı ilə olduğu ehtimal edilir. 1918-ci il noyabrın 23-də imzaladığı bir əmrdə Nuru paşa Azərbaycan Ordusunun komandanı kimi Gəncədə fəaliyyətini davam etdirdiyini yazırdı. Buradan belə bir qənaətə gəlmək olar ki, Azərbaycan Ordusunun komandanlığının qərargahı Gəncədə təsis edilmişdi [16, s.416]. Bir gün sonra, yəni noyabrın 24-də imzalanmış əmrdə isə Nuru paşa artıq Azərbaycan Ordusunun deyil, Azərbaycandakı Osmanlı Qüvvələrinin komandanı kimi fəaliyyətini davam etdirməyə başlamışdı [17, s.418]. Həmin əmrdə Nuru paşa aydın şəkildə yazırdı ki, müttəfiq dövlətlər adından Azərbaycana gəlmiş ingilis hərbi qüvvələrinin rəhbərliyi türk hərbçilərinin heç bir halda Azərbaycanda qalmasına icazə verməmişdir. Buradan belə nəticəyə gəlinir ki, Nuru paşa və digər türk hərbçiləri Azərbaycan Ordusu tərkibində xidmət edə bilməzdilər. Ona görə də Nuru paşa Azərbaycan Ordusunun komandanı vəzifəsindən kənarlaşmağa məcbur oldu.

Beləliklə, sənədlərə görə Nuru paşa 20 gün ərzində Azərbaycan Ordusunun komandanı oldu. Lakin bu müddət ərzində onun hansı səlahiyyətlərə malik olması, bu strukturla Hərbi Nazirlik arasındakı münasibətlərin necə qurulması haqqında yetərli məlumat mövcud deyil. Hər bir halda Cümhuriyyət Ordusunun tarixində türk hərbçilərinin rəhbərliyi altında belə bir strukturun olması maraqlı bir faktdır və heç şübhəsiz ki, gələcəkdə elmi dövriyyəyə gətirilə biləcək yeni sənədlər bu faktla bağlı daha yetərli fikir söyləməyə imkan verəcəkdir.

Bununla belə, mövcud məlumatlar onu göstərir ki, türk hərbi qüvvələri Azərbaycanı tərk etdikdən sonra bir neçə türk kiçik zabit milli ordu sıralarında qalmağa nail olmuşdu. 1918-ci ilin dekabrın son günlərində Cümhuriyyət Ordusunun Ağdamda yerləşən 1-ci piyada diviziyasının bəzi bölmələrində hərbi rəhbərliyə qarşı bir itaətsizlik halı baş vermişdi. Hərbi nazir Səməd bəy Mehmandarovun 1919-cu il fevralın 25-də Azərbaycan parlamentində etdiyi çıxışı zamanı bu itaətsizlik hadisəsində 10-a yaxın türk əsilli kiçik zabitin də iştirak etdiyini bildirirdi [18, s.92]. Bu türk zabitlərinin sonrakı taleyi haqqında konkret məlumat olmasa da, intizamsızlıqlarına görə milli ordu sıralarından kənarlaşdırıldıqları ehtimal oluna bilər. Çünki 1920-ci ilin əvvəllərinə aid olan məlumatlarda Cümhuriyyət Ordusunda 6 nəfər türk əsilli zabitin xidmət etməsi haqqında məlumat vardır, onlar isə kiçik zabitlər deyildilər. Bu zabitlərin Azərbaycan Ordusuna gəlməsi Türkiyədə yaranmış mürəkkəb tarixi şəraitlə bağlı idi. Belə ki, Birinci Dünya müharibəsində məğlub olan Türkiyə Ordusunun hərbi qulluqçuları müttəfiq dövlətlər tərəfindən ciddi təqiblərə məruz qalmışdılar. Onların müəyyən hissəsi Azərbaycana sığınmaq qərarına gəlmişdilər. Bu zabitlərin bir neçəsi Cümhuriyyət Ordusunda xidmətə qəbul edilmişdilər. Həmin zabitlər kornet Faik Cevdetoğlu (parlament mühafizə bölüyü), kapitan Nüsrət bəy (7-ci Şirvan piyada alayı), podporuçik İbrahim İsmayıloğlu (İstehkam məktəbi), kapitan Məcid Seyidoğlu (8-ci Ağdaş piyada alayı), ştabs-kapitan Necət Mustafa (6-cı Göyçay piyada alayı) və podporuçik Məhəmməd Şefik Taksinoğlu (3-cü Gəncə piyada alayı) idilər [19, s.764].

Türkiyədən Azərbaycana pənah gətirən türk hərbçilərinin sayı çoxaldıqda Azərbaycan hökuməti 1920-ci ilin əvvəllərində Hərbi Nazirliyin tabeliyində onlardan ibarət yardım alayı adlı bir hissənin təşkilinə qərar verdi. Lakin sonradan bu alay Daxili İşlər Nazirliyinin tabeliyinə keçirildi.

Bu hərbçilərin maliyyə təminatı Azərbaycan hökuməti tərəfindən həyata keçirilirdi. Azərbaycan hökuməti, hətta xidmətə alınmayan türk zabitlərini hərtərəfli qayğı ilə əhatə etməyə çalışır və onlara

aylıq maliyyə vəsaitləri ayırırdı [20, s.269]. Lakin məlumdur ki, bu alayın şəxsi heyəti sonradan güclü bolşevik təbliğatına məruz qaldı və Azərbaycanın bolşevik qoşunları tərəfindən işğal edilməsi bu alay tərəfindən də dəstəkləndi.

Azərbaycan–Böyük Britaniya hərbi əməkdaşlığı

Mundoros müqaviləsinin şərtlərinə əsasən, Cənubi Qafqaz, o cümlədən də Azərbaycan müttəfiq dövlətlərinin nəzarəti altına düşməli idi. Adı çəkilən müqavilənin imzalanmasından bir gün sonra, yəni 1918-ci il oktyabrın 31-də Böyük Britaniyanın Hərbi Nazirliyi Mesopotamiyada yerləşən ingilis qüvvələri komandanlığına Bakı şəhərinin dərhal işğal edilməsi barəsində əmr göndərdi. Bu əmrə əsasən Bakı şəhərinin işğal edilməsi, o zaman İranın şimalında dislokasiya olunmuş ingilis qüvvələrinin komandanı general-mayor V.Tomsona həvalə olundu [21, s.21]. General V.Tomsonun rəhbərliyi altında Bakıda hərbi idarəçilik yaradılmalı və o, Bakının general-qubernatoru elan edilməli idi. Yeni şəraitdə Azərbaycanın müstəqilliyinin qorunmasına və tanınmasına nail olmaq üçün general V.Tomson, hələ İranda olarkən, onun yanına Azərbaycan hökumətinin rəsmi nümayəndə heyəti göndərildi. Amma bu heyətlə general V.Tomson arasında aparılan danışıqlar gözlənilən nəticəni vermədi. General V.Tomson Bakı şəhərinin işğal olunacağını, Azərbaycanın müstəqilliyinin tanınmayacağını, Azərbaycan xalqının iradəsi ilə yaradılmış bir respublikanın mövcud olmadığını və Azərbaycan hökumətinin Türkiyə hərbi qüvvələrinin intriqaları ilə yaradılmış bir hökumət olduğunu birmənalı şəkildə bəyan etdi [11, s.171; 21, s.21; 22, s.278].

General V.Tomson onu müşayiət edən hərbi qüvvələrlə 1918-ci il noyabrın ayının 17-də Bakıya daxil oldu. Mövcud məlumata görə, onun rəhbərliyi altında Bakıya 5 min nəfərlik ingilis hərbi qüvvələri gətirildi və onlar Bakı şəhərini bütünlüklə nəzarət altına aldılar [23, s.119].

Bakı üzərində nəzarəti gücləndirmək üçün V.Tomson şəhərdə olan bütün milli hərbi qüvvələrin, onların idarəetmə orqanlarının Bakı şəhərini tərk etməsini tələb etdi. Bunun nəticəsi idi ki, Hərbi Nazirlik Bakı şəhərini tərk etdi və Gəncə şəhərinə yerləşdi. Bundan başqa, Azərbaycan hökumətinə məxsus olan "Qars", "Ərdəhan" kanoner gəmiləri və digər hərbi gəmilər Denikinin rəhbərliyi altında olan qüvvələrin sərəncamına verildi. Bildirildi ki, bu qərar bolşevizmin qarşısının alınması üçün Denikin rəhbərliyi altında olan qüvvələrin möhkəmləndirilməsi üçün edilmişdir.

Azərbaycan hökuməti general V.Tomson administrasiyası ilə fəal siyasət aparırdı və bunun nəticəsi idi ki, general V.Tomson Azərbaycan hökumətinin doğrudan da Azərbaycan xalqının iradəsini əks etdirdiyini və bu hökumətin real müstəqilliyə malik olduğunu gördü. Ona görə tezliklə V.Tomsonun Azərbaycanın müstəqilliyinə münasibəti dəyişdi və tərəflər arasında daha faydalı əməkdaşlığın qurulmasına başlandı.

Bu əməkdaşlığın bir istiqamətini də hərbi sahədə anlaşmanın və qarşılıqlı fəaliyyətin yaradılması təşkil edirdi. Bu əməkdaşlığın düzgün qurulmasının nəticəsi idi ki, 1919-cu ilin fevral ayında artıq V.Tomson məhdud sayda milli hərbi qüvvələrin Bakıya qayıtmasına etiraz etmədi [24, s.467]. Ona görə də 1919-cu il aprelin 5-də Azərbaycanın məhdud sayda hərbi qüvvələri Bakı şəhərinə daxil oldular [25, v.53].

Hərbi əməkdaşlıq sahəsində qarşılıqlı münasibətlərin düzgün qurulmasının nəticəsi idi ki, ingilis qüvvələri Azərbaycanı tərk etmədən əvvəl Azərbaycanın Hərbi Nazirliyi, Baş Qərargah və digər hərbi idarəetmə strukturları 1919-cu ilin yayında Bakıya qayıtdılar, Bakı şəhərində bir piyada diviziyasının yerləşdirilməsinə icazə verildi və Bakıda Azərbaycan hökumətinin hərbi fəaliyyəti tam şəkildə bərpa edildi.

Azərbaycan hökuməti ilə ingilis komandanlığı arasında Azərbaycana məxsus hərbi gəmilərin geri qaytarılmaması ilə bağlı bir qarşıdurma yaransa da, ingilis komandanlığı bu məsələyə Böyük Britaniyanın bölgədəki ümumi siyasəti çərçivəsindən yanaşırdı. Bu siyasətin mahiyyəti isə general Denikinin rəhbərliyi altında olan hərbi qüvvələrə kömək etməklə, Rusiyanın bolşevikləşməsinin qarşısını almaq idi. Azərbaycanın hərbi gəmiləri də bu siyasətin həyata keçirilməsi üçün Denikin qüvvələrinin tabeliyinə verilmişdi [21, s.33].

Bütün bunlara baxmayaraq, hərbi sahədə fəal əlaqələrin yaradılması ingilis komandanlığının

Azərbaycanın müstəqilliyinə daha loyal münasibət bəsləməsinə yol açdı. İngilis komandanlığının Denikinçi qüvvələri dəstəkləməsinə baxmayaraq, Azərbaycan hökuməti Denikin qoşunlarının respublikaya müdaxilə planlarının qarşısının alınması üçün ingilis komandanlığının imkanlarından da istifadə etməyə çalışırdı. Bunun nəticəsi idi ki, Denikin qoşunlarının Azərbaycan üzərinə hücum etməyəcəyinə bir ümid də yaranmışdı. Azərbaycan hökumətinin müraciətindən sonra ingilis komandanlığının səyləri ilə Denikin qoşunları və Azərbaycan arasında demarkasiya xətti müəyyənləşdirildi. Böyük Britaniya hökumətinin razılığı ilə müəyyənləşdirilmiş həmin demarkasiya xətti Dağıstan ərazisində Petrovsk şəhərinin 5 mil cənubundan keçirdi. İngilis komandanlığı ilə razılaşdırılmışdı ki, Böyük Britaniya ilə sıx əlaqədə olan Denikin qoşunları bu demarkasiya xəttindən cənuba, yəni Azərbaycan istiqamətinə hərəkət etməyəcəklər [22, s.305]. Əslində, ilkin olaraq, demarkasiya xəttinin bir qədər də şimalda müəyyənləşdirilməsi qərara alınmışdı. Lakin Denikinçi qoşunlar bu tələbə əməl etmədilər və onlar Dağıstanın cənubuna, yəni Azərbaycan sərhədlərinə doğru irəliləməyə başladılar.

Azərbaycan hökumətinin apardığı müzakirələrdən sonra ingilis komandanlığı 1919-cu ilin avqustunda yeni demarkasiya xəttini razılaşdırdı. Bu xətt Azərbaycanın şimal sərhədi boyunca keçirdi [21, s.33]. Bununla, Denikin qoşunları Azərbaycan sərhədinə daha da yaxınlaşmaq imkanı əldə etdi. Lakin ingilis komandanlığı Azərbaycan hökumətinə bəyan etdi ki, bu qoşunlar Azərbaycan sərhədlərinə təcavüz etməyəcək.

Respublika daxilində hərbi-siyasi şəraitin sabitləşməsi üçün ingilis komandanlığı ilə yaxşı münasibətlər qurulmuşdu. Belə ki, müstəqilliyin elan edilməsindən sonra da Azərbaycan türklərinin qədim yurdu İrəvan ərazisində respublika yaradılmasına nail olan Ermənistan hökuməti Azərbaycana qarşı əsassız ərazi iddiaları irəli sürməyə davam edirdi. Həm Ermənistanın hökumət qüvvələri, həm də qeyri-hökumət silahlı dəstələri Azərbaycanın Zəngəzur və Qarabağ bölgəsinə silahlı basqınlar edir, azərbaycanlı əhalini sıxışdıraraq, bu bölgələri Ermənistana birləşdirmək istəyirdilər. Məsələnin mahiyyəti ilə bağlı Azərbaycan hökuməti ingilis komandanlığı ilə müzakirələr apardı. Azərbaycan ərazilərinin və əhalisinin erməni silahlı dəstələrinin qanunsuz və haqsız təcavüzünə məruz qalması ingilis komandanlığının, xüsusən general Tomsonun diqqətinə çatdırıldı. General Tomson dərhal silahsız azərbaycanlı əhalini erməni silahlı dəstələrinin basqınlarından qorumaq üçün qətiyyətli mövqe nümayiş etdirərək, azərbaycanlılar yaşayan məntəqələr üzərinə daha çox basqınlar edən, erməni silahlı dəstələrindən birinin rəhbəri Andronikə teleqram göndərdi və onu silahlı basqınlardan çəkindirməyə çalışdı. General Tomsonun razılığı ilə Azərbaycan hökuməti Qarabağ bölgəsini əhatə edən Qarabağ general-qubernatorluğu yaratdı. Bu general-qubernatorluğun nəzdində ingilis hərbçilərindən ibarət bir nəzarət missiyası da təşkil edildi və həmin missiyaya rəhbərlik mayor Monk-Mezona tapşırıldı. Ermənistan hökumətinin bu qərara etirazı ilə qarşılaşan Bakıda yerləşən ingilis komandanlığı xüsusi bir bəyanatla çıxış etdi. İngilis qüvvələrinin Bakıdakı komandanı, polkovnik Şatelvort bəyanatında bildirirdi: *"İngilis komandanlığı Şuşa, Zəngəzur, Cəbrayıl və Cavanşir qəzalarının əhalisinə məcburi icra üçün aşağıdakıları elan edir:*

1. Azərbaycan hökumətinin 15 yanvar 1919-cu il tarixli qərarına əsasən doktor Sultanov Şuşa, Zəngəzur, Cəbrayıl və Cavanşir qəzalarının general-qubernatoru təyin olunub və o, ingilis komandanlığının dəstəyinə malikdir.
2. Mövcud qanunlara görə, bütün əhalinin ehtiyaclarının ödənməsi üçün general-qubernator yanında 6 nəfər hadisələrdən məlumatlı erməni və müsəlmandan ibarət şura yaradılır.
3. İngilis komandanlığının nümayəndəsi kimi şuraya bir nəfər ingilis missiyasının zabiti daxil ola bilər.
4. General-qubernatorluq daxilində bütün işçilərin maaşı və başqa xərcləri Azərbaycan xəzinəsindən ödənilir.
5. Bütün mübahisəli məsələlər öz qəti həllini sülh konfransında tapacaq.
6. General-qubernatorluq daxilində hərbi hissələrin hər cür yerdəyişməsi haqqında əvvəlcədən ingilis missiyasının diqqətinə çatdırılmalıdır.

7. Bu müraciətlə ingilis komandanlığı bildirir ki, general-qubernatorluq hüdudlarında qanunçuluq və sakitliyin yaradılması üçün general-qubernatora həvalə olunan vəzifələrin icrası zamanı general-qubernator və onun orqanlarına aid olan bütün sərəncamlar və tədbirlər sözsüz icra olunmalıdır. İngilis komandanlığı bütün qanuni fəaliyyətə tam dəstək verir" [26, s.295].

Yəni ingilis komandanlığı bir tərəfdən Azərbaycan hökumətinin Qarabağda vəziyyətin sabitləşdirilməsi üçün izlədiyi siyasəti dəstəklədiyini bildirir, digər tərəfdən də ərazi mübahisələri ilə bağlı məsələlərin həllinin Paris sülh konfransının öhdəsinə buraxılmasını lazım bilirdi.

1919-cu ilin avqustunda Böyük Britaniya hökuməti ingilis hərbi qüvvələrinin Azərbaycandan çıxarılması haqqında qərar qəbul etdi. Qeyd edildiyi kimi, müəyyən məsələlərdə, o cümlədən Azərbaycanın hərbi gəmilərinin Denikinin tabeliyinə verilməsində, denikinçi zabitlərin Azərbaycan daxilində ingilislər tərəfindən himayə olunmasında Azərbaycan hökuməti ilə ingilis hərbi komandanlığı arasında bir anlaşılmazlıq qalmaqda idi. Bununla belə, Azərbaycanın müstəqilliyinin müdafiəsi sahəsində tərəflər arasında faydalı əməkdaşlıq yaradıldığından Azərbaycan hökuməti ingilis hərbi qüvvələrinin Azərbaycanı tərk etməsini istəmirdi. Buna görə də Azərbaycan hökuməti ingilis hərbi qüvvələrinin Azərbaycandan çıxarılmaması ilə bağlı Böyük Britaniya hökumətinə müraciət etmək haqqında qərar qəbul etdi və Azərbaycanın xarici işlər naziri olan Məmməd Yusif Cəfərov bu qərarı Böyük Britaniya hökumətinə göndərdi. Eyni zamanda o, hərbi qüvvələrin Bakıdan çıxarılması ilə bağlı qərara yenidən baxılması üçün ingilis hərbi qüvvələrinin Bakıdakı yeni komandanı polkovnik Şatelvorta məktub göndərdi [22, s.308]. Lakin yaranmış tarixi şəraitlə əlaqədar olaraq, Böyük Britaniya hökuməti ingilis hərbi qüvvələrinin Azərbaycandan çıxarılması qərarını dəyişmədi.

İngiltərədən silah, sursat və hərbi geyim alınması məsələsini müzakirə etmək üçün Hərb naziri S.Mehmandarov 1919-cu ilin payızında İngiltərənin Bakıdakı Ali Komissarının siyasi nümayəndəsi polkovnik Stoksla görüşdü. Bu görüş zamanı İ.Usubovun rəhbərliyi altında Azərbaycan nümayəndə heyətinin İtaliyaya yollanmasına işarə edən S.Mehmandarov İngiltərə tərəfinin Azərbaycanla hərbi əməkdaşlığa razı olacağı təqdirdə, İtaliya ilə əldə edilə biləcək bütün razılaşmalara yenidən baxılacağını Stoksa bildirdi [27, s.113].

Azərbaycan Xalq Cümhuriyyətinin xarici işlər naziri Fətəli xan Xoyski də 1920-ci il yanvar ayının 7-də İngiltərənin Ali Komissarlığının Bakıda olan siyasi nümayəndəsi polkovnik Stoksla görüşərək, Azərbaycana silah və hərbi geyim yardımı göstərilməsi məsələsini müzakirə etdi. Polkovnik Stoks Azərbaycan tərəfinin müraciətlərinə rəğbətlə yanaşaraq, İngiltərənin ali hakimiyyət orqanları qarşısında Azərbaycana silah və hərbi geyim yardımı edilməsinin vacibliyi məsələsini qaldırdı [27, s.78].

İngiltərənin hərbi-siyasi rəhbərliyi də bolşevik qoşunlarının Cənubi Qafqaza müdaxiləsinin qarşısının alınması üçün Azərbaycanın hərbi qüvvələrinə yardım göstərilməsini vacib hesab edirdi. Bununla bağlı İngiltərənin hərbi komandanlığı bu ölkənin Aralıq dənizində yerləşən hərbi dəniz qüvvələrinin komandanına Xəzər buxtasındakı topların çatışmayan ehtiyat hissələri ilə təmin edilməsi barədə göstəriş verdi[27, s.85].

Paris sülh konfransının müzakirələrində iştirak edən Azərbaycan nümayəndə heyətinin müraciətindən sonra Antanta ölkələrinin Ali Hərbi Şurası da 1920-ci ilin yanvar ayında Cənubi Qafqaz respublikalarına, o cümlədən Azərbaycana hərbi yardım göstərilməsi məsələsini müzakirə etdi. Bu məsələ ilə bağlı Ali Hərbi Şuraya təqdim olunmuş memorandumda da Cənubi Qafqaz respublikaları ilə yanaşı, Azərbaycana da ərzaq və hərbi yardımın göstərilməsi məqsədəuyğun sayılırdı. Eyni zamanda konfransda Denikin Ordusunun təmini üçün nəzərdə tutulmuş silah-sursatın da Cənubi Qafqaz respublikalarına verilməsi təklifi irəli sürüldü [27, s.86-87].

1920-ci ilin fevralında İngiltərənin hərbi nümayəndələri mövcud hərbi ehtiyacların müəyyənləşdirilməsi üçün Cənubi Qafqaza, o cümlədən də Azərbaycana səfər etdilər. Onlar lazım olan məlumatları topladıqdan sonra İstanbuldan keçməklə geri qayıtdılar. Aparılan danışıqlardan sonra bir sıra özəl ingilis şirkətləri Azərbaycanla əməkdaşlıq etmək niyyətində olduqlarını bildirdilər. Paris sülh konfransındakı Azərbaycan nümayəndə heyətinin üzvlərinin verdiyi məlumata görə, bu şirkətlərlə müvafiq müqavilələrin imzalanması üçün İtaliyada olan Azərbaycanın hərbi nümayəndə heyətinin rəhbəri general İ.Usubovun İngiltərəyə gedərək zəruri olan təchizatın müəyyənləşdirməsinə ehtiyac var

idi. Lakin 1920-ci ilin fevralından başlayaraq Qarabağda hərbi vəziyyətin mürəkkəbləşməsi, Azərbaycanın müharibə vəziyyətinə olması, habelə bölgədə cərəyan edən hərbi-siyasi proseslər İngiltərə ilə hərbi əməkdaşlıq sahəsində müvafiq sənədlərin imzalanmasına imkan vermədi [27, s.114].

Gürcüstanla hərbi əməkdaşlıq

Müdafiə qüvvələrinin təşkilatlandırılması istiqamətində Azərbaycanla qonşu Gürcüstan arasında qurulmuş hərbi əməkdaşlıq da Cümhuriyyət Ordu quruculuğu üçün xüsusi əhəmiyyət daşıyırdı. Yaranmış tarixi şəraitdən irəli gələrək eyni vaxtda dövlət müstəqilliklərini elan etmiş Azərbaycanla Gürcüstan arasında qarşılıqlı dostluq münasibətlərinin bərqərar olması Azərbaycan Xalq Cümhuriyyətinin xarici siyasətinin mühüm istiqamətlərindən birini təşkil edirdi.

Azərbaycan və Gürcüstan arasında hərbi əlaqələrin tənzimlənməsi üçün 1919-cu ilin yazında Tiflisdə Azərbaycanın hərbi attaşeliyi təsis edildi və polkovnik-leytenant Məmməd bəy Əliyev bu vəzifəyə təyin edildi [28, s.32]. Həmin ilin avqust ayında isə Gürcüstanın Azərbaycanda Hərbi Attaşeliyi təsis edildi və polkovnik Navasalov bu vəzifəyə təyin olundu [29, s.132].

Hərbi əməkdaşlığın qarşılıqlı fayda üzərində daha da genişləndirilməsi üçün 1919-cu il iyunun 16-da Azərbaycanla Gürcüstan arasında hərbi saziş imzalandı. Sazişi Azərbaycan hökuməti tərəfindən Xarici İşlər naziri M.Cəfərov, hərbi nazir S.Mehmandarov və Baş Qərargah rəisi M.Sulkeviç imzaladılar. Tiflisdə üç il müddətinə imzalanmış həmin sazişin əsas mahiyyəti ondan ibarət idi ki, respublikaların hər hansı birinə xarici müdaxilə olacağı halda, digər respublika ona hərbi kömək göstərsin [30, s.105-106].

Bu sazişin imzalanması Azərbaycanın dövlət və hökumət rəhbərliyi, habelə siyasətçiləri tərəfindən son dərəcə yüksək qiymətləndirildi. 1919-cu il iyunun 27-də parlamentin fövqəladə iclasında həmin saziş ratifikasiya olundu. Bununla bağlı çıxış edən parlament üzvləri və xarici işlər naziri M.Cəfərov Azərbaycanın və bütünlükdə bölgənin təhlükəsizliyinin təmin edilməsində sazişin əhəmiyyətini vurğulayaraq, bu günü hər iki respublikanın tarixində önəmli bir gün kimi xarakterizə etdilər. Xarici işlər naziri M.Cəfərovun fikrincə, həmin saziş Cənubi Qafqaz üçün real təhlükə sayılan Denikin təcavüzünün qarşısının alınmasında təsirli bir addım olmaqla, həm də Cənubi Qafqaz xalqlarının birliyi istiqamətində imzalanmış tarixi bir anlaşma idi. Sazişin hər iki xalqın həyatındakı praktiki əhəmiyyəti nəzərə alındığı üçün parlamentin müzakirələrində Gürcüstanın nümayəndə heyəti də iştirak edirdi.

Bu sazişə əlavə olaraq, iki dövlət arasında hərbi-texniki əməkdaşlıq haqqında da sənəd imzalandı ki, həmin sənədə müvafiq olaraq, Gürcüstan həm hərbi-texniki və sursat sahəsində, həm də hərbi kadrların hazırlanması istiqamətində Azərbaycana kömək göstərməli idi. Adları çəkilən sənədlər imzalandıqdan dərhal sonra onların icrasına başlanıldı. Bu da Azərbaycanın qoşun hissələrinin, o cümlədən Denikin təhlükəsinə qarşı şimal sərhədləri boyunca yerləşdirilmiş bölmələrin maddi-texniki təchizatını xeyli yaxşılaşdırdı.

Gürcüstandan alınacaq hərbi əmlakın qəbul edilməsi üçün Azərbaycanın Hərbi Nazirliyində xüsusi komissiya yaradıldı və general-mayor M.Tlexas bu komissiyanın rəhbəri təyin edildi [31, s.7]. General Tlexasın rəhbərlik etdiyi komissiyanın səmərəli fəaliyyəti nəticəsində Azərbaycan Ordusunun təchizatı üçün böyük əhəmiyyət kəsb edən iki eşelon hərbi-texniki vasitə və ərzaq 1919-cu il iyulun 11-də Azərbaycana göndərildi. Bu eşelonlarda 12 ədəd dağ topu, dağ topları üçün 10 yeşik partladıcı maddə, 1500 ədəd tüfəng, toplar və tüfənglər üçün böyük sayda ehtiyat detallar var idi. İyulun 19-da yola salınan digər eşelonda isə 8 ədəd yüngül top, toplar üçün 16 ədəd partladıcı maddə, 1500 ədəd tüfəng, toplar və tüfənglər üçün ehtiyat detallar, 12885 rubl məbləğində dərman və tibb ləvazimatı, habelə topoqrafiya əşyaları var idi. İyulun 21-də bir eşelon, əsasən, mühəndis- istehkam ləvazimatı Tiflisdən Gəncəyə göndərildi [32, s.237].

İyulun 18-dən etibarən komissiya çoxlu sayda mətbəx arabalarının, dördçarxlı arabaların qəbuluna başladı. Şəxsi adamlardan 20 min rubl həcmində çoxlu sayda top detalları alındı. Bütün əmlak üçün gürcü tərəfinə 80 min rubl avans verildi. Gürcüstandan alınacaq hərbi əmlakın dəyərinin bir hissəsinin neftlə ödənilməsi haqqında da razılıq əldə edildi [33, s.174].

Gürcüstanla 1919-cu il iyun ayının 16-da imzalanmış "Hərbi-müdafiə" sazişinə əsasən tərəflər bütün silahlı qüvvələri və hərbi vasitələri ilə razılığa gələn respublikaların birinin və ya hər ikisinin müstəqilliyini və ya ərazi bütövlüyünü təhdid edən hər hansı hücuma qarşı birgə çıxış etməyi öhdələrinə götürmüşdülər. Zərurət yarandığı halda, Gürcüstana belə bir köməyin göstərilməsi üçün Azərbaycan tərəfindən qüvvə və vəsaitlər ayrılmış, onların Gürcüstan ərazisinə çatdırılması planları hazırlanmışdı. Bu plana əsasən nəzərdə tutulurdu ki, Gürcüstan hərbi müdaxiləyə məruz qalsa, onun köməyinə bir piyada diviziyası və bir süvari briqadası göndərilsin. Piyada diviziyası kimi 1-ci piyada diviziyasının Gürcüstana göndərilməsi planlaşdırılırdı. Diviziyanın 1-ci Cavanşir alayı Xankəndindən, 2-ci Zaqatala alayı Zaqataladan, 3-cü Gəncə alayı Gəncədən, 1-ci topçu briqadasının 1-ci batareyası Xankəndindən, 2-ci və 3-cü batareyaları Gəncədən, 4-cü batareyası isə Xankəndindən Gürcüstana yola salınmalı idi. Gürcüstana göndərilməli olan süvari briqadası isə mövcud süvari diviziyasının bazasında formalaşdırılmalı idi. Bu briqadanın tərkibinə 2-ci Qarabağ süvari alayının, 3-cü Şəki süvari alayının və dağ-atlı batareyasının verilməsi planlaşdırılırdı. Bu qüvvələrin Gürcüstana çatdırılması onların səfər hazırlığından və daşınmaların təşkilindən asılı idi. Xüsusən, daşınmalar üçün zəruri olan vaqonların vaxtında ayrılması planlaşdırılan işlərin icrası üçün xüsusi əhəmiyyət kəsb edirdi. Gürcüstana göndərilməli olan hissələrdən yalnız 2-ci Zaqatala piyada alayı piyada olaraq qonşu respublikanın ərazisinə keçməli idi. Çünki Gürcüstan sərhədinə yaxınlıq buna imkan verirdi. Digər hissə və bölmələr isə dəmir yolu ilə daşınmalı idi. Aparılan hesablamalara görə, hərbi yardım üçün nəzərdə tutulmuş qüvvə və vasitələrin daşınması üçün 940 ədəd vaqon lazım idi. Əldə edilən məlumata görə, respublikada kifayət qədər vaqon olsa da, bütün yükləri götürə biləcək 10 eşelonun hərəkətə gətirilməsi üçün kifayət qədər parovoz yox idi. Bu məsələ həll olunacağı təqdirdə nəzərdə tutulan bütün qüvvə və vasitələrin 4 gün ərzində Gürcüstan ərazisinə çatdırılması mümkün idi. Belə bir hazırlıq işləri Gürcüstan tərəfindən də aparılmışdı və Azərbaycan üzərinə hərbi müdaxilə olacağı təqdirdə Gürcüstan tərəfindən Azərbaycana müvafiq hərbi kömək göstərməli idi [34, s.370-371].

İki ölkə arasında hərbi əməkdaşlığın uğurlu davamı kimi, 1920-ci il yanvarın 20-də Azərbaycan və Gürcüstan arasında müştərək Hərbi Şura təsis edildi. Bu müştərək Hərbi Şura hər iki ölkə üçün ehtimal olunan düşmənləri və hərbi əməliyyatlar rayonunu öyrənməli, məqsədəuyğun müdafiə və dislokasiya planını hazırlamalı, hər iki ölkənin hərbi qüvvələrinin döyüş hazırlığı vəziyyətini nəzarət altında saxlamalı idi.

Hərbi Şuraya hər tərəfdən iki nəfər daxil etməli və hökumətlərin qarşılıqlı razılaşması əsasında onlardan biri Şuranın sədri seçilməli idi. Şuranın iclaslarına hər iki respublikanın məsul vəzifəli şəxsləri dəvət oluna bilərdilər. Bu orqanın qəbul etdiyi strateji və hərbi-texniki yönümlü qərarların icrası hər iki tərəf üçün məcburi xarakter daşımalı idi. Hər hansı bir qərarın qəbulundan sonra onun icrası ilə bağlı zəruri hallarda işçi iclasları keçirilə və bu iclaslarda qəbul olunmuş qərarların icra mexanizmi müəyyənləşdirilə bilərdi. Belə iclaslarda fikir ayrılığı yarandığı halda, bu hala səbəb olmuş məsələ hökumət rəhbərlərinə məruzə olunmalı və onların iştirakı ilə razılıq əldə edilməli idi [35, s.18].

Qeyd etmək lazımdır ki, Azərbaycan tərəfdən bu Şuraya artilleriya generalı Əliağa Şıxlinski və Baş Qərargah rəisi Məmməd bəy Sulkeviç, Gürcüstan tərəfindən isə N.Odoşelidze və Kutetaladze seçilmişdilər [36, s.25].

İki dövlət arasında imzalanan sənədlərə uyğun olaraq, hərbi mütəxəssislərin hazırlanması üçün Gürcüstana azərbaycanlı hərbi qulluqçular ezam olundular. Onlardan 6 zabit təyyarəçilik kurslarında, 4 zabit və 10 nəfər əsgər isə radioteleqraf kurslarında hazırlıq keçməli idilər.

Eyni zamanda 14 gürcü zabit hərbi nazirin 1919-cu il 15 iyul tarixli əmri ilə Cümhuriyyət Ordusu sıralarına qəbul edildi [37, s.27-28]. Bu proses sonralar da davam etdirilmişdi.

Azərbaycanda milli zabit kadrlarının çatışmadığı bir vaxtda gürcü zabitlərindən istifadə edilməsi qoşun hissələrinin formalaşdırılmasında mühüm rol oynayırdı Qarşılıqlı razılaşmaya əsasən gürcü zabitlər Azərbaycan Ordusunda xidmət edə bilsələr də, Azərbaycan ərazisində aparılan döyüşlərdə iştiraketmə hüququna malik deyildilər. Razılaşmaya əsasən, Cümhuriyyət Ordusu sıralarında xidmət edərkən gürcü zabitlərin əvvəlki imtiyazları, o cümlədən onların rütbələri, iş stajları və bundan irəli gələn imtiyazlar saxlanılırdı.

Xidmət təcrübələri nəzərə alınmaqla, çox sayda gürcü zabiti Cümhuriyyət Ordusu sıralarında çox məsul vəzifələrə təyin olunmuşdular. Məsələn, podpolkovnik Svanadze Gəncə şəhərinin komendantı vəzifəsinə, polkovnik Çxeidze əvvəlcə 4-cü Quba piyada alayının komandiri olmuş, sonradan isə Hərbiyyə Məktəbinin rəisi təyin edilmişdi. Cümhuriyyət Ordusu sıralarında gürcü millətindən olan beş nəfər general xidmət edirdi: general-mayor Amaşukeli, general-mayor Sisianov, general-mayor Purseladze, general-mayor Karqaleteli və general-mayor Çxeidze. Karqaleteli və Çxeidze Azərbaycan hökumətinin qərarı ilə bu ali hərbi rütbəyə layiq görülmüş son Cümhuriyyət generalları idilər.

Adları çəkilən gürcü generalların hər birinin Cümhuriyyətin ordu quruculuğunda böyük rolu vardır. Hərbi nazir Səməd bəy Mehmandarov onlardan biri olan general-mayor Amaşukelinin Cümhuriyyət Ordusu sıralarındakı xidmətini belə qiymətləndirirdi: *"Süvari diviziyasının komandiri vəzifəsini icra edən, diviziyanın qərargah rəisi general Amaşukelidən daxil olan vəsatətə görə, o, öz arzusu ilə xidməti tərk edir və qoşunların siyahısından çıxarılır. 7 ay əvvəl orduda quruculuq işlərinin çox gərgin vaxtında süvari diviziyasının qərargah rəisi vəzifəsinə qəbul edilən general Amaşukeli, əslində, beş aydan çox diviziya komandir vəzifəsini icra etmişdi. Hərb işini yaxşı bilən və onu sevən general Amaşukeli hərbi hissələrdə xidmətin tələblərini həyata keçirməkdə enerjisi və xüsusi qətiyyətliliyi ilə fərqlənirdi və işə böyük xeyir gətirirdi. General Amaşukeli ilə təəssüflə vidalaşaraq, ona ordu sıralarındakı əla və səmərəli xidmətlərinə görə öz səmimi minnətdarlığımı bildirirəm"* [38, s.121].

Gürcü hərbi mütəxəssisləri, həmçinin konkret məsələlər üzrə məsləhətlərin alınması məqsədilə Azərbaycana dəvət edilirdilər. Məsələn, general-leytenant M.Sulkeviçin xahişi ilə 1919-cu il avqustun sonunda gürcü generalları Kutalaşvili və Takayşvili Bakıya gəldilər [39, s.20]. Bu təcrübəli generallar Bakı şəhərinin müdafiə sisteminin qurulması ilə bağlı öz yardımlarını göstərdilər.

General Takayşvilinin rəhbərliyi altında Bakı və onun ətrafının müdafiəsi planı hazırlandı. Bu plan iki hissədən ibarət idi: birincisi – Abşeron yarımadasının müdafiəsi, ikincisi – Bakı şəhərinin müdafiəsinin mühəndis-istehkam işlərinin təşkili. Abşeron yarımadasının müdafiəsi üçün görülməli olan istehkam işləri Badamdardan Masazır gölünə qədər uzanırdı. Bu xətt üzrə 7 dayaq müdafiə qrupu yerləşdirilməli idi. İkinci müdafiə xətti isə Biləcəri–Böyük Şor–Razin dağı–Əhmədli ərazisi boyunca keçməli idi. Bu xətt boyunca 6 dayaq müdafiə qrupu yerləşdirilməli idi [40, s.61-62].

1919-cu ilin noyabr ayında general Takayşvili yenidən Bakıya gəldi. O, Bakının və Abşeron yarımadasının müdafiəsinin təşkili ilə bağlı hazırladığı planın icrası ilə tanış oldu. Gürcü generalı müdafiə işlərinin sürətini və keyfiyyətini artırmaq üçün tövsiyələrini hazırlayıb Azərbaycanın Hərbi Nazirliyinin rəhbərliyinə təqdim etdi.

Gürcü zabitlərinin bir qrupu da şimal sərhədlərinin müdafiəsinin gücləndirilməsi məqsədilə aparılan mühəndis-istehkam işlərinin icrasında iştirak edirdilər. Bu istiqamətdə aparılan mühəndis-istehkam işlərinə ştabs-kapitan Sereteli rəhbərlik edirdi. Həmin işlərin aparılması ilə bağlı ştabs-kapitan Sereteli çox müfəssəl bir raport hazırlayıb Hərbi Nazirliyə təqdim etmişdi [41, s.8-9].

Gürcüstandan olan zabitlərinin məişət qayğılarının daha yaxşı həlli üçün hərbi naziri S.Mehmandarovun 28 fevral 1920-ci il tarixli əmri ilə onlara ayrılan ezamiyyət pullarının miqdarı da artırıldı. Hərbi Nazirliyin rəhbərliyi çalışırdı ki, bu zabitlər Azərbaycanda heç bir çətinliklə rastlaşmadan xidmət etsinlər. Qeyd etmək lazımdır ki, bu zabitlərin köməyi ilə qısa müddət ərzində xeyli işlər görülmüş və Denikin təhlükəsinə qarşı Azərbaycanda çox güclü müdafiə sistemi yaradılmışdı.

İtaliya və Fransa ilə hərbi əməkdaşlıq məsələləri

Ölkənin müdafiə qüdrətinin artırılması və ordunun təchizat səviyyəsinin daha da yaxşılaşdırılması üçün Azərbaycan hökumətinin və Hərbi Nazirliyinin beynəlxalq fəaliyyətinin mühüm istiqamətlərindən birini də inkişaf etmiş Avropa dövlətləri ilə hərbi əməkdaşlığın yaradılması təşkil edirdi. Belə bir əməkdaşlığın uğurla qurulması Cümhuriyyət Ordusu üçün zəruri olan keyfiyyətli təchizatın əldə edilməsinə imkan verə bilərdi. Həmin istiqamətdə atılan addımlardan biri də İtaliya ilə hərbi əməkdaşlığın yaradılmasına göstərilən cəhd idi. Bu məqsədlə xüsusi komissiya təşkil edildi. Komissiyaya 2-ci piyada diviziyasının komandiri general İbrahim ağa Usubov rəhbərlik edirdi. Hərbi Nazirliyin rəhbərliyi, xüsusən general Usubov İtaliyanın Soloniki şəhərinə yollanmalı və orada

İtaliyanın Hərbi Nazirliyi ilə Cümhuriyyət Ordusu üçün zəruri olan topçu, istehkam, tibb, geyim və s. əşyaların əldə edilməsi üçün müzakirələr aparmalı idi. İtaliyadan 25 min dəst hərbi geyim alınması və Azərbaycana gətirilməsi nəzərdə tutulmuşdu [36, s.159].

1919-cu ilin oktyabrında İtaliyaya yola düşən general İ.Usubovun rəhbərlik etdiyi komissiya Romada İtaliyanın Hərbi Nazirliyi ilə danışıqlara başladı. Hərbi Nazirliyin Azərbaycan tərəfinin tələbini ödəyəcək məhsulları təmin etmək imkanında olmadığı məlum olduqda İtaliyanın özəl şirkətləri ilə müzakirələrə başlanıldı. 1919-cu ilin noyabr ayı ərzində Genuya, Milan, Turin, Verona və Triento şəhərlərinin şirkətləri ilə danışıqlar aparıldı və nəticədə Kiono, Qello və Ko şirkətləri ilə müvafiq razılaşma əldə edildi. Bu şirkətlərin rəhbərliyi anbarlarında 20 min dəst hazır hərbi geyim olduğunu bildirdi və az bir vaxta daha 5 min dəst hərbi geyim, habelə general və zabitlər üçün 500 dəst geyim hazırlayacaqlarını vəd etdi. 1919-cu il noyabrın 23-də Azərbaycan heyəti ilə adı çəkilən şirkətlər arasında razılaşdırılmış təchizatın satın alınması haqqında müqavilə imzalandı. Həmin müqaviləyə əsasən hərbi geyim əşyalarının 1919-cu il dekabrın 20-də İtaliyanın Turin şəhərindən Bakıya yola salınması nəzərdə tutulmuşdu [36, s.159].

Lakin İtaliyada mövcud olan ictimai-siyasi vəziyyətin mürəkkəbləşməsi səbəbindən bu ölkədən alınmış hərbi əmlakın Azərbaycana vaxtında göndərilməsi mümkün olmadı. Nəticədə İtaliyadan göndərilən hərbi təchizat Cümhuriyyətin süqutu ərəfəsində Azərbaycana çatdı və həmin əmlak Azərbaycana müdaxilə etmiş bolşevik ordusunun əlinə keçdi [42, s.42].

Cümhuriyyət Ordusunun hərbi təchizatla təminatının yüksəldilməsi üçün Antanta hərbi qüvvələrinin komandanlığı ilə əlaqə yaradılması cəhdləri haqqında da məlumatlar mövcuddur. Həmin məlumatlara əsasən, İtaliyaya göndərilmiş nümayəndə heyətinin rəhbəri general-mayor İ.Usubov Avropada olarkən, Antanta qüvvələrinin komandanlığı ilə də əlaqə saxlamış, Antanta ölkələrinin hərbi rəhbərliyi Cümhuriyyətin Hərbi Nazirliklə əməkdaşlıq etməkdən imtina etməmişdi. Lakin Antantanın hərbi anbarlarında olan hərbi geyim ehtiyatları rumın, çex və polyak hərbi qüvvələrinə paylandığından çox az miqdarda qalmışdı və bu miqdar Azərbaycan tərəfini qane etmədiyindən İ.Usubovun rəhbərlik etdiyi nümayəndə heyəti İtaliya ilə əməkdaşlığa üstünlük verdi·

Azərbaycan hökuməti və Hərbi Nazirliyin rəhbərliyi ordunun təchizatının daha da yaxşılaşdırılması üçün Fransa ilə də əlaqələr yaratmağa cəhd göstərdi. Bunun nəticəsi kimi, tərəflər arasında aparılan danışıqlardan sonra 1920-ci il martın 9–12-də fransalı zabitlər mayor Nonankur və dəniz qüvvələri leytenantı Deforj da Bakıda olmuş və Azərbaycana hərbi yardım göstərilməsi imkanlarını araşdırmışlar. Adları çəkilən zabitlər Azərbaycanın hərbi-dəniz qüvvələrinin mövcud imkanlarını nəzərdən keçirmişlər. Öz rəhbərliklərinə göndərdikləri raportda həmin zabitlər bildirirdilər ki, Azərbaycanın hərbi dəniz qüvvələrinin yaxşılaşdırılması üçün buraya hərbi əmlakla yanaşı, həm də hərbi təlimatçıların göndərilməsinə ehtiyac vardır [27, s.121-123].

Lakin 1920-ci il aprel ayının sonlarında bolşevik qoşunları Azərbaycana daxil olduqdan sonra hərbi sahədə Avropa ölkələri ilə planlaşdırılan əməkdaşlıq məsələlərinin həyata keçirilməsi mümkün olmadı.

Nəticə

Azərbaycan xalqının XX əsrin əvvəllərində yaratdığı ilk respublika cəmi 23 ay mövcud oldu. Bölgədə və dünyada gedən siyasi proseslər səbəbindən Azərbaycanın müstəqilliyini qorumaq mümkün olmadı və 1920-ci il aprel ayının 28-də Azərbaycan bolşevik Rusiyası tərəfindən işğal olundu. Mövcud olduğu dövr ərzində Azərbaycan Xalq Cümhuriyyətinin əldə etdiyi mühüm nəticələrdən biri də yetərli döyüş qabiliyyətinə malik olan milli ordunun yaradılması oldu. Qısa müddət ərzində Azərbaycan hökuməti ölkənin daxili imkanlarını səfərbərliyə almaqla bərabər, həm də dünya dövlətləri ilə hərbi əməkdaşlıq sahəsində səmərəli bir siyasət həyata keçirə bildi. Müasir və demokratik dəyərlərə üstünlük verən Azərbaycan hökuməti hərbi sahədə də səmərəli bir siyasət yeritməyə çalışırdı. Bu siyasət beynəlxalq normalara, eyni zamanda milli maraqlara cavab verirdi. Nəticədə həm ordunun, həm də ölkənin möhkəmləndirilməsi istiqamətində səmərəli işlər görmək mümkün oldu. Ən əsası isə cümhuriyyət dövründə Azərbaycanın hərbi diplomatiyasının əsası qoyuldu.

İstifadə edilmiş ədəbiyyat siyahısı

1. Osmanlı imperator hökuməti və Azərbaycan Respublikası arasında dostluq müqaviləsi // Azərbaycan Respublikası Prezidentinin İşlər İdarəsinin Siyasi Sənədlər Arxivi, Fond № 277, siyahı № 2, iş № 9.
2. Birinci Dünya harbinde türk harbi Kafkas cebhesi 3ncü ordu harekatı. – Ankara: Genelkurmay basım evi, – cilt II. – 1995, – 686 s.
3. Osmanlı-Azərbaycan hərbi müqavilə layihələri / V.Qafarov, Q.Şükürov. Azərbaycan Cümhuriyyəti tarixi (1918-1920-ci illər) // Osmanlı arxiv sənədləri əsasında, Elmin inkişaf fondu, – 2017, – 520 s.
4. Azərbaycan Cümhuriyyəti tarixi. 1918-1920-ci illər / V.V.Qafarov, Q.E.Şükürov (Osmanlı arxiv sənədləri əsasında). Bakı, Elmin İnkişafı Fondu – 2017. – 520 s.
5. Nuri paşa həzrətləri hüzurunda Lənkəran nümayəndəsi // Azərbaycan qəzeti – 1918, 3 noyabr. № 29.
6. Təmim. // – Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı) – 2020.№ 148, – 472 s.
7. Ordu əmr-i yevmisi. Numro 28. Kafkas İslam Ordusu (Azerbaycan harekatı) // – Ankara Askeri tarih belgeleri dergisi. – 2020. № 148, – 472 s.
8. Azerbaycan Hükumeti Heyeti Vükəla Riyasst-i Aliyyesinez. // – Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı) – 2020. №148. – 472 s.
9. Elçi. Gəncədə milli zabitan təftiş və imtahan mərasimi // Azərbaycan qəzeti, – 1918, 5 noyabr. – s. 2.
10. Azərbaycan Xalq Cümhuriyyəti və Qafqaz İslam Ordusu. // (Redaktorlar M. Rıhtım və M. Süleymanov) – Bakı: Nurlar, –2008, – 696 s.
11. İsgenderli, A. Realities of Azerbaijan: 1917-1920 / A.İsgenderli, – USA: Xlibris Corporation – 2011, – 370 s.
12. Yüceer, N. Birinci Dünya savaşında Osmanlı Ordusunun Azerbaycan ve Dağıstan harekatı./ N.Yüceer, – Ankara: Genelkurmay Basım evi, – 1996 – 202 s.
13. Azerbaycan Hükûmeti ile burada kalacak zâbitân için akd edilen mukavele şerâiti // –Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). – 2020.№148, – 472 s.
14. Azerbaycan Kolordusu Kumandanlığına // – Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). – 2020.№148 – 472 s.
15. Ordu Dâiresine // – Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). – 2020.№148, – 472 s.
16. Şimâlî Kafkas Kumandanlığına ve Reîs-i Cumhûr Abdülmecîd Çermoyef Hazretlerine // – Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). – 2020.№148, – 472 s.
17. Gence'den Başkumandanlık Vekâlet-i Celîlesi Erkân-ı Harbiyye-i Umûmiyye Riyâsetine / – Ankara: Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). Askeri tarih belgeleri dergisi. Kafkas İslam Ordusu (Azerbaycan harekatı). – 2020.№148, – 472 s.
18. Süleymanov, M.S. Səməd bəy Mehmandarov / M.S. Süleymanov, – Bakı: Hərbi Nəşriyyat, – 2000, – 376 s.
19. Azərbaycan Cümhuriyyəti Ordusunun zabit və məmurları / A.Şahbazov, – Bakı: Maarif, – 2020. – 814 s.
20. Baykara, H. Azərbaycan istiqlal mübarizəsi tarixi. / H.Baykara, – Bakı: Azərbaycan Dövlət Nəşriyyatı, –1992. – 276 s.
21. Юсифзаде, С. Азербайджано-британское отношения в начале XX века. / С.Юсифзаде, – Баку: Тахсил, –2008, –128 s.
22. Azərbaycan tarixi. [8 cilddə].. – Bakı: Elm, – c.5 – 2008, – 696 s.
23. Azərbaycan Cümhuriyyəti (1918-1920). / – Bakı: Elm, –1998, – 336 s.

24. Qafqaz və Bakı ərazisinə dair məlumatlardan çıxarışlar / Qasımlı M. Birinci Dünya müharibəsi illərində böyük dövlətlərin Azərbaycan siyasəti. Üç hissədə. III hissə. – Bakı – 2004. –532 s.

25. Отношение М.Сулькевича С.Агабекову об организации контрразведки в Баку в связи с прибытием азербайджанских войск. №1539, Гянджа 31 марта 1919 г. // Azərbaycan Respublikasının Dövlət Arxivi, Fond №894, siyahı №2, iş №88

26. Нагорный Карабах в международном праве и мировой политике. Документы и комментарий (Составитель проф. Ю.Г. Барсегян). [В двух томах] – Москва: Круг –т.1. – 2008. – 944 s.

27. Топчубаши, А.М. Парижский архив. В четырех книгах. Книга первая. 1919-1921. – Москва: Художественная литература, – 2016, – 568 s.

28. Приказ по военному ведомству Азербайджанской Республики, № 148, 26 марта 1919 года // Azərbaycan Respublikasının Dövlət Arxivi, Fond № 2894, siyahı №1, iş №3

29. Приказ по военному ведомству Азербайджанской Республики, №365, 17 августа 1919 года // Azərbaycan Respublikasının Dövlət Arxivi. Fond №2894, siyahı №1, iş №40

30. Военно-оборонительное соглашение, заключенное между правительствами Азербайджана и Грузии и утвержденное парламентом 27 июня 1919 г. Азербайджанская Демократическая Республика (1918-1920) /– Баку, – 1998, – 440 s.

31. Приказ С.С.Мехмандарова об объявлении благодарности членам комиссии, приобретшим вооружение и военное имущество в Республике Грузии, №421, 19 сентября 1919 г. // Azərbaycan Respublikasının Dövlət Arxivi, Fond №2900, siyahı №1, iş № 1

32. Süleymanov, M. Azərbaycan Ordusu (1918-1920). / M.Süleymanov, – Bakı: Hərbi nəşriyyat, – 1998. – 488 s.

33. Süleymanov, M. Azərbaycan Ordusunun tarixi: [5 cilddə]. / M.Süleymanov,– Bakı: Maarif – c.2. – 2018. – 728 s.

34. Süleymanov, M. Hərb tarixindən. / M.Süleymanov, – Bakı: Maarif, – 2020, – 608 s.

35. Положение о Союзном военном совете республик Азербайджана и Грузии. 18 января 1920 г.//Azərbaycan Respublikasının Dövlət Arxivi, Fond №970, siyahı №.1, iş №64

36. Süleymanov, M. Azərbaycan Xalq Cümhuriyyətinin hərb tarixi. [2 cilddə] / M.Süleymanov, – Tehran: Firuzan, – c.2. – 2014. – 696 s.

37. Приказ по военному ведомству Азербайджанской Республики, № 323, 15 июля 1919 года // Azərbaycan Respublikasının Dövlət Arxivi, Fond №2894, siyahı №1, iş №5

38. Приказ по военному ведомству Азербайджанской Республики, № 347, 03 августа 1919 года // Azərbaycan Respublikasının Dövlət Arxivi, Fond №2894, siyahı 1, iş №24

39. Сообщение военного инженера ген.-м. Такаишвили В. к Д.Каргалетели о необходимых мерах для начала работ по укреплению обороны Баку. Август 1919 г. // Azərbaycan Respublikasının Dövlət Arxivi, Fond 2898, siyahı №1, iş №13

40. Доклад М.А.Сулькевича С.С.Мехмандарову о мерах, необходимых для укрепления подступом к Баку с моря. Август 1919 г. // Azərbaycan Respublikasının Dövlət Arxivi, iş 13

41. Доклад шт.-кап. В.Церетели к Д.Каргалетели о ходе работ по инженерному оборудованию позиций на северной границе Азербайджана. 29 августа 1919 г. // Azərbaycan Respublikasının Dövlət Arxivi, Fond 2898, siyahı №1, iş №6

42. Стеклов, А.А. Армия мусаватского Азербайджана. /А.А.Стеклов, – Баку: Азгосиздат, – 1928. – 52 s.

Аннотация
Военная дипломатия в период
Азербайджанской Демократической Республики
Мехман Сулейманов

Одной из основных задач, стоящих перед правительством Азербайджанской Демократической Республики в области обеспечения военной безопасности страны, было налаживание международного военного сотрудничества. За 23 месяца независимости правительству республики удалось провести плодотворную политику в этом направлении. Прежде всего, удалось достичь хорошие результаты в области военного сотрудничества с Османской Турцией. Это сотрудничество дало эффективные результаты в деле устранения существующей угрозы, обеспечения независимости и территориальной целостности Азербайджана. Хотя эта тема достаточно широка, в статье отражены отдельные ее аспекты. В статье также проанализирована сфера международного военного сотрудничества, сложившаяся с Грузией. В частности, после того как турецкие военные силы покинули Азербайджан, было усилено внимание на расширение военного сотрудничества с Грузией В статье также затронуты вопросы военного сотрудничества, установившегося между Великобританией и другими европейскими государствами, в том числе Италией и Францией, и Азербайджанской Демократической Республикой.

Ключевые слова: Азербайджан, независимость, национальная армия, военная политика, военное сотрудничество

Abstract
Military diplomacy during the period of the
Azerbaijan Democratic Republic
Mehman Suleymanov

One of the main tasks facing the government of the Azerbaijan Democratic Republic in the field of ensuring the military security of the country was the establishment of international military cooperation. Over the 23 months of independence, the government of the republic managed to pursue a fruitful policy in this direction. First of all, good results were achieved in the field of military cooperation with Ottoman Turkey. This cooperation has produced effective results in eliminating the existing threat, ensuring the independence and territorial integrity of Azerbaijan.

Although this topic is quite broad, the article reflects some of its aspects. The article also analyzes the sphere of international military cooperation that has developed with Georgia. In particular, after Turkish military forces left Azerbaijan, there was an increased focus on expanding military cooperation with Georgia. The article also touches on the issues of military cooperation established between Great Britain and other European states, including Italy and France and the Azerbaijan Democratic Republic.

Keywords: Azerbaijan, independence, national army, military policy, military cooperation

Məqalə redaksiyaya daxil olmuşdur: 18.04.2024
Təkrar işlənməyə göndərilmişdir: 22.04.2023
Çapa qəbul edilmişdir: 06.05.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 83-93
HƏRBİ XÜSUSİ ELMLƏR ***MILITARY SPECIAL SCIENCES***

UOT 629.076:623.426 DOI: 10.30546/9878.2024.2.10.0027.

ANALYSIS OF THE PROPERTIES OF MILITARY VEHICLES

PhD in technical sciences, Associate Professor Anatoly Kovtun
National Guard Military Academy of Ukraine

PhD in technical sciences, Associate Professor Volodymyr Tabunenko
National Air Force University Ivan Kozhedub Kharkiv, Ukraine
tabunenko55@ukr.net

PhD in technical sciences, Associate Professor Sergey Nesterenko
National Aerospace University ("KhAI"), Ukraine
nesterenko.geo@gmail.com

Konstantin Borisenko
National Air Force University Ivan Kozhedub Kharkiv, Ukraine
kostya.bo.bo.01@gmail.com

Abstract. With the beginning of military aggression, the arsenal of military vehicles of the Armed Forces of Ukraine was replenished with modern and highly effective models from NATO countries. Current documents on the organization and operation of military vehicles need to determine some of the indicators for the use of vehicles. The indicators used do not allow us to assess the degree of combat effectiveness of vehicles during combat operations. The article analyzes various types (modifications) of the main properties of military vehicles and obtains dependencies to assess their combat capability when performing assigned tasks in the conduct of combat operations. The essence and content of the category of "combat capability of military automotive equipment" are defined and a common understanding of the properties included in this category has been developed. The paper proposes mathematical dependencies to determine the indicators of individual properties of the combat capability of military vehicles, which allows to create a mathematical apparatus for its assessment and forecasting, which makes it possible to build mathematical models of combat (operation) that will correspond to the real processes of armed struggle as much as possible. The objective of the study is to determine the indicators of the main properties of new models of military vehicles. The following theories were used as a research method for assessing the level of combat capability of military vehicles: the reliability of weapons and military vehicles, the effectiveness of the use of military vehicles, the survivability of military vehicles, the technical operation of military vehicles, probabilities and mathematical statistics.

Keywords: military automotive equipment, efficiency of application weapon systems, basic properties and combat capability of automotive equipment.

Introduction

Since the beginning of Russia’s full-scale invasion of Ukraine, the arsenal of the Armed Forces of Ukraine (AFU) has been replenished with modern high-performance models of military vehicles. These means are designed to dramatically increase the effectiveness of the use of weapons systems of military formations of the security and defense sector of Ukraine, reduce the aggressor's capabilities, and force the enemy to be defeated on the battlefield.

Military vehicles are the most popular means of equipment in the army and, thanks to their technical capabilities, ensure the fulfillment of assigned tasks at the tactical and operational levels. The need to provide military units of the Armed Forces of Ukraine with modern automotive equipment is associated with the increase in the tasks assigned to the troops.

With the help of military automotive equipment (MAE), various combat missions are solved:

– effective use of weapons placed on vehicles;

– ensuring fast transportation of personnel;
– delivery of ammunition, petroleum products and other material resources;
– evacuation, towing and repair of military equipment and weapons;
– placement of means of engineering support, communication, electronic warfare, protection and defense of areas;
– conducting reconnaissance;
– medical support and others.

To accomplish these tasks, there is a need to create various modifications of MAE. There is a need to adapt MAE samples to changes on the battlefield. At the same time, it is necessary to ensure the justification of the requirements for MAE in the changed conditions. Current documents on the organization and operation of automotive equipment need to determine some of the indicators of the use of MAE, namely:

– coefficient of technical readiness of machines;
– fleet utilization rate,
– load capacity utilization rate,
– mileage utilization rate, etc.

However, these indicators do not make it possible to assess the degree of combat capability of the automotive equipment of the military unit (subdivision).

Therefore, determining the indicators of the main properties of new MAE models for the Armed Forces of Ukraine (AFU) for further modernization of vehicles in order to meet the needs of military units is an urgent task.

Analysis of the latest research and publications. The scientific basis for research on the assessment of the level of combat capability of are the theories of reliability of weapons and military equipment, effectiveness of the use of MAE, survivability of military equipment, technical operation of combat vehicles, probabilities and mathematical statistics [1-5]. The basic terms and definitions of equipment reliability and reliability forecasting based on the results of testing and operation of equipment are given in the works [1; 2]. The papers [6-11] provide methodological bases for the development of models for assessing the expected effectiveness of performance of service and combat tasks by military units and subdivisions and features of assessing the effectiveness of systems in combat operations using probabilistic models.

The paper [12] analyzes the renewal of the fleet of wheeled vehicles of the armies of NATO member states from 2012 to 2022. The paper [13] substantiates the tactical and technical requirements for the development of promising models of "light" armored vehicles.

However, the results presented in the considered works do not make it possible to assess the combat capability of military vehicles during the performance of assigned tasks in the conduct of hostilities.

The aim of the article is to determine the main properties of MAE for their different types (modifications) and to obtain dependencies for assessing the combat capability of MAE during the performance of assigned tasks in the conduct of combat operations.

Statement of the main material. Multi-purpose wheeled vehicles are the most common type of MAE of the US Army (Table 1) and NATO member states. The main program in the field of improvement of multi-purpose wheeled vehicles of the US Army for the period up to 2025 is the "Army Tactical Wheeled Vehicles (TWV) Strategy" [13;15].

The purpose of this program is to:

– adapt existing MAE models to new changes on the battlefield, as well as reduce the risks of uncertainty that will be caused by new threats;
– to change the structure of the MAE fleet to perform new tasks.

Table 1. Type and number of tactical wheeled vehicles as of the beginning of 2022 in the US Armed Forces

Tactical vehicles of the US Armed Forces			Quantity, units	Total, units
1.	Light Tactical All-Terrain Vehicle LTATV (Light Tactical All-Terrain Vehicle)	Polaris MRZR X	20	2053
		MRZR-4 LTATV and MRZR-2	2033	
2.	Light tactical vehicles-LTV (Light Tactical Vehicle), carrying capacity up to 2 tons	HMMWV with reinforced armor protection (UAH)	50 thousand	119 thousand
		General purpose HMMWV (Utility)	35 thousand	
		HMMWV (obsolete)		
		Joint Light Tactical Vehicle (JLTV)	34 thousand	
3.	Medium tactical vehicles MTV (Medium Tactical Vehicles), carrying capacity 2.5-5 tons	Series: M35; M809; M939	76 thousand	
	Medium tactical vehicles FMTV (Family of Medium Tactical Vehicles), carrying capacity 2.5-5 tons	M1078A1 (4×4)		
		M1083A1 (6×6)		
	MTVR (Oshkosh Defense)	MTVR (6×6)		
4.	Heavy tactical vehicles - HTV (Heavy Tactical Vehicle), carrying capacity over 5 tons	Multifunctional high-mobility heavy tactical trucks NEMTT (Heavy Expanded Mobility Tactical Truck)	34 thousand	
		Transporter of heavy military equipment NET (Heavy Equipment Transporter), a family of cars with a packaged loading system PLS (Palletized Load System)		
		The family of cars of the M915 series		
5.	A family of vehicles with anti-mine protection from a hidden attack - MRAP (Mine-Resistant Ambush Protected)	Modernization of machines developed under the JMVP program (Joint MRAP Vehicle Program)	15 thousand	
The total number of			246053	

In addition to significant investments in the development and production of a new generation of MAE, it is also planned to finance the improvement of the existing JSC fleet in the following areas:

– modernization of the power drive (use of hybrid and electric drives);
– suspension reinforcement aimed at increasing the mobility of vehicles in off-road conditions;
– installation of improved ballistic and mine protection;
– ensuring counteraction to means of electronic warfare;
– development of new materials and technologies that reduce the weight of machines and fuel consumption [13].

Problems in equipping the Armed Forces of Ukraine are caused by the fact that a significant number of samples of the existing fleet of MAE have a long service life, are morally and physically obsolete and need to be modernized or replaced with new models. According to the order of the Cabinet

of Ministers of Ukraine dated 14.06. 2017 No. 398–p "On Approval of the Main Directions of Development of Weapons and Military Equipment for the Long Term" it is required: "To provide military units (subdivisions) with modern models of automotive equipment for various purposes, created on the basis of unified models with a wheel arrangement of 4×4, 6×6, 8×8 with increased mobility characteristics, cross-country ability, autonomy, economy and protection of personnel".

Units and military units are armed with the following types of armored vehicles:

– *the first type* – armored highly maneuverable passenger cars designed for:
– conducting reconnaissance and sabotage raids in areas where the enemy is concentrated;
– covert persecution;
– frontal observation of the battlefield and fire adjustment;
– patrolling sections of the state border and districts;
– withdrawal and evacuation of reconnaissance and sabotage units, as well as rescue operations;
– *the second type* – armored off-road vehicles, made on the chassis of trucks and designed to transport personnel in armored modules (container bodies);
– *the third type* – armored off-road vehicles, designed to place various special equipment (reconnaissance, communication systems and complexes, etc.) on their chassis;
– *the fourth type* is armored off-road vehicles designed to accommodate weapons (guns, mortars, missiles and air defense systems, etc.) on their chassis. The main purpose of the vehicle is fire support for the actions of troops in various combat conditions.
– *the fifth type* is armored and lightly armored heavy wheeled chassis of increased cross-country ability, designed for the installation of weapons systems, towing and transportation of bulky cargo and heavy armored vehicles.
– *the sixth type* – armored off-road vehicles designed for the evacuation of the wounded and sick, providing first aid in various combat conditions.

Military formations of the security and defense sector of Ukraine receive military assistance from the allies. Among the provided samples of foreign MAE, a significant place is occupied by American highly mobile multipurpose wheeled vehicles of the HMMWV type. HMMWVs are versatile vehicles that can perform a variety of tasks in combat conditions.

The military formations of the security and defense sector of Ukraine receive the following modifications of HMMWV vehicles (Table 2).

Table 2. Modifications of HMMWV machines that belong to different types of MAE

Types of armored vehicles	**General view of HMMWV machines**		
1	**2**		
1.			
2.			

followed

1	2		
3.			
4.			
5.			
6.			

These vehicles have different purposes, so they must have different properties that characterize their adaptability to conduct (support) combat operations.

One of the main properties of MAE is their combat capability.

The combat capability of military vehicles is its ability to function with the parameters established by the operational documentation [4; 5]. The combat capability of military equipment is ensured by its reliability and survivability.

Let us consider these properties for different types of MAE.

Reliability of MAE is its ability to maintain the values of all parameters that characterize the ability to perform the required functions in the specified modes and conditions of application, maintenance, repair, storage and transportation in time and established limits.

As one of the possible indicators of the reliability of the MAE, it is possible to use the complex indicators of the reliability of the MAE, i.e. the coefficient of operational readiness of machines. The coefficient of operational readiness of machines is the probability that the machines will be in working condition at any point in time, and, starting from this moment, will work flawlessly for a given period [4]:

$$K_{or(t)} = \frac{T_0}{T_0 + T_{ra}} e^{-\frac{t}{T_0}},$$

where,

T_0 – is the average uptime of machines, hours;

T_{ra} – random recovery time of machines, hours;

t – is the time of use of machines, hours.

The survivability of the bat is a complex property of the bat to maintain the values of combat capability indicators in terms of time (mileage, operating time) (even with a possible decrease in the value of these indicators below the established limits) in certain conditions of the enemy's combat impact (and emergency situations) and to restore them after the end (repair during) of the enemy's combat impact [5].

The survivability of the MAE is ensured by the strength of structures, resistance to the effects of shock waves, high temperatures and penetrating radiation, giving products streamlined, ricocheted shapes, reducing dimensions, applying camouflage painting, duplication of control devices and energy sources, creating a reliable system of biological protection of the crew (service) and facilitating the restoration of equipment.

The main components of the survivability of MAE: – secrecy of movement; – mobility; – maneuverability; – security; – cross-country ability, – autonomy.

Stealth is a property in which it is possible to keep secret from the enemy data the location, task, and combat capabilities of the MAE, etc. Indicators of secrecy characterize the adaptability of military equipment to conceal its deployment (probability of detection, average detection time, level of unmasking radiation, etc.).

The probability of detecting an object RB is calculated by the formula [11,13]:

$$R_i = R_{i.o.} + R_{i.s.} - R_{i.o.} \cdot R_{i.s.},$$

where,

$R_{i.o.}$ – is the probability of detecting the object without taking into account the shadow of the object;

$R_{i.s.}$ – is the probability of detecting the shadow of the object.

Mobility is a property that characterizes the ability of a MAE to move quickly, deploy in the area of combat use and move during combat operations. Quantitative indicators of MAE's mobility are:

– average speed of movement *Vser*.,
– the time of deployment of the MAE, t_{dep}.,
– the time of removal from the position and the readiness to move the $t_{tak.pos.}$.

The average speed of movement on the section of the path $V_{ser.}$ is the ratio of the length S of this section to the time interval t in which this section is traversed by the machine:

$$V_{ser.} = \frac{S}{t},$$

Autonomy is the property of MAE to function without the help of auxiliary external systems (energy sources, controls, support, etc.).

New vehicles under development for a long time during operation must be in the field at a considerable distance from the point of permanent deployment (being in areas of concentration, combat use). A quantitative indicator of autonomy is the term of autonomy – a certain time during which the MAE can perform a combat mission at the expense of its own resources without replenishing consumables (fuel and lubricants, coolant, water, etc.).

One of the quantitative indicators of MAE's mobility is the power reserve coefficient

$$C_{p.r.} = \frac{P_{ri}}{P_{rmax}},$$

where,

P_{ri} – is the current indicator of the power reserve of the i–th vehicle, km; P_{rmax} – is the maximum possible indicator of the vehicle's power reserve, km.

Maneuverability is the ability of the JSC to quickly change the speed and direction of movement on the ground, depending on the complexity of the situation. The manoeuvrability of wheeled vehicles depends on the turning radius and lane width, speed range, engine power, and controllability.

One of the quantitative indicators of the maneuverability of the MAE is the agility coefficient (the agility of the car is characterized by the turning radius, that is, the distance from the instantaneous center of turn to the longitudinal axis of the K_t car:

$$K_t = \frac{R_{ti}}{R_{tmax}},$$

where R_{ti} – is the turning radius of the i-th machine, m;

R_{tmax} – is the maximum possible turning radius of the machine, m.

Security is a property of resistance to external influences which characterizes the ability of JSC to maintain combat capability under natural and combat influences. A quantitative indicator of security is the probability of not hitting the vehicle.

The probability of not hitting the vehicle is determined by the expression:

$$P_{n.def.} = 1 - P_{def.}, \quad (1)$$

(a) When small arms are used, the following may be used:

– the probability of hitting the target with one Ruhr shot $P_{def.}$:

$$P_{def.} = p' \cdot G, \quad (2)$$

where,

p' – is the probability of hitting the target with one shot;

G – is the probability of hitting the target with one hit.

Given a known average number of hits required k:

$$P_{def.} = \frac{p'}{k}, \quad (3)$$

– probability of hitting the target with n independent Ruhr shots:

$$P_{def.} = 1 - \prod_{i=1}^{n}(1 - p_i), \quad (4)$$

where,

p_i – is the probability of hitting the target with the i-th shot.

– the probability of hitting the target with dependent Ruhr shots $P_{def.}$:

$$P_{def.} = p + (P_n - p)\sqrt{1 - r^2}, \quad (5)$$

where,

P, P_n – are the probabilities of defeat with one and n independent shots;

r – is the correlation coefficient of shots.

(b) For ground artillery, the probability of hitting an elemental target not observed by the $P_{def.}$:

$$P_{def.} = \hat{\Phi}\left(\frac{l_x}{E_{X_E}}\right) \cdot \hat{\Phi}\left(\frac{l_Y}{E_{Y_E}}\right), \quad (6)$$

where,

l_x, l_Y are the dimensions of the target in terms of range and direction;

E_{X_E}, E_{Y_E} – median errors of the shot in range and direction.

Dynamism is the property of a car to move at the highest possible average speed, which is characterized by the maximum speed, the intensity of acceleration to a given speed and the intensity of braking.

One of the quantitative indicators of the dynamism of the MAE is the coefficient of the dynamism of the movement K_d:

$$K_d = \frac{V_{p.i}}{V_{p.max}},$$

where,

$V_{p.i}$ – is the maximum speed of the first vehicle, km/h;

$V_{p.max}$ – is the maximum possible speed for cars of this type, km/h.

Cross-country ability of a car is the ability of a car to move on low-quality roads and outside the road network, as well as to overcome artificial and natural obstacles without the use of aids.

The cross-country ability of the car depends on many factors, the main of which are the traction properties and geometric parameters of the car.

One of the quantitative indicators of the cross-country ability of JSC is the coefficient of ground clearance of the car $K_{g.c.}$

$$K_{g.c.} = \frac{h_{g.c.i}}{h_{g.c.max}},$$

where,

$h_{g.c.i}$ – is the current ground clearance of the i-th car, cm;

$h_{g.c.max}$ – is the maximum possible ground clearance of the machine, cm.

Vehicle stability is the ability of a vehicle to maintain movement along a given trajectory, counteracting the forces that cause it to drift and overturn in various road conditions at high speeds and maintain combat capability under combat impacts.

One of the quantitative indicators of the stability of BAT is the stability coefficient $K_{dur.}$:

$$K_{dur.} = \frac{P_i}{P_{max}},$$

where,

P_i – is the overpressure of the shock wave of the explosion on the body of the i-th machine, Pa;

P_{max} – is the maximum possible overpressure of the shock wave of the explosion on the body of a machine of this type, Pa.

Vehicle handling is the ability of the car to move in the direction set by the driver. One of the characteristics is the property of the car to change direction when the steering wheel is stationary.

It is evaluated according to the following criteria: critical speed, ratio of steering angles, stabilization of steered wheels, angular oscillations.

One of the quantitative indicators of the controllability of the MAE is the controllability coefficient of the machine $K_{con.}$:

$$K_{con.} = \frac{V_{crit.i}}{V_{crit.max}},$$

where,

$V_{crit.i}$ – is the critical speed of the first vehicle, km/h;

$V_{crit.max}$ – is the maximum possible critical speed for vehicles of this type, km/h.

With the help of the method of expert analysis for armored wheeled vehicles (AWV) of different types, the weight coefficients of individual properties were determined. To substantiate the weighting coefficients of individual properties of different types of AWV, the provisions of the method of expert assessments were used. To determine the weighting coefficients of individual properties of different types AWV involved leading specialists of research centers, teachers, and practitioners on the problems

of assessing the level of technical perfection of MAE samples. The value of the concordance coefficient depending on the property was in the range of (0.8-0.9), which indicates a sufficient level of consistency of the results [13].

The value of the location of individual properties for AWV of different types is given in table 3.

Table 3. The importance of individual properties for different types of AWV

№	Properties	Machine Groups					
		Combat Vehicles	Reconnaissance vehicles	Angle grinder	Transport Vehicles	Machines with special equipment	Ambulances
1.	Reliability	1	1	1	1	1	1
2.	Security	2	4	3	4	2	3
3.	Dynamism	3	5	4	2	8	5
4.	Agility	4	6	5	6	6	6
5.	Cross-country ability	5	3	6	3	5	2
6.	Concealment	6	2	2	9	4	10
7.	Resistance	7	7	7	5	7	7
8.	Battery life	8	8	8	10	3	9
9.	Handling	9	9	9	7	9	8
10.	Fluency	10	10	10	8	10	4

Conclusions

1. The main properties of JSC for their different types are determined and dependencies for assessing the combat capability of JSC during the performance of assigned tasks in the conduct of combat operations are obtained.

2. The essence and content of the category "combat capability of MAE" are defined, a common understanding of the properties that are included in the category of "combat capability of MAE" is developed, which meets the interests of both the further development of military science and the solution of practical problems facing the troops.

3. Mathematical dependencies are proposed to determine the indicators of individual properties of the combat capability of MAE, which allows to create a mathematical apparatus for its assessment and forecasting. This, in turn, makes it possible to build mathematical models of combat (operations) that will correspond as much as possible to the real processes of armed struggle, which will be a promising direction for further research.

References

1. State standard of Ukraine. Reliability of equipment. Terms and definitions. DSTU 2860 – 1994. – 15 p.

2. National Standard of Ukraine. Reliability of equipment: Evaluation and prediction of reliability based on the results of testing and/or operation in conditions of low number of failures. DSTU 8647:2016.

3. Maksymenko, O.G., Military Automobile Transportation / O.G.Maksymenko, O.M.Tovkach, O.V.Yaroshenko, – Kyiv: NUBIPU. – 2008. – 138 p.

4. Ivanchenko, O.V. Systematization of the properties of military automobile equipment / O.V.Ivanchenko, A.V.Kovtun, A.O.Ivanchenko, O.I.Shapovalov // – Kyiv: Collection of scientific

papers of the National Academy of the State Border Guard Service of Ukraine series: military and technical sciences. – 2022. № 3 (88). – p.270-285.

5. Ivanchenko, O.V. Determining the survivability index of armored vehicles during implementation of measures to ensure state security / O.V. Ivanchenko, A.V. Kovtun, S.A. Kudimov // – Kyiv: Honor and law. –2020. –№74. Vol.3. – p.20 – 26.

6. Chabanenko, P.P. Regularities and features of evaluating the effectiveness of systems in combat operations using probabilistic models/ P.P. Chabanenko // – Kyiv: Science and defense. – 2016. – №4. – p.16 – 22.

7. Davydich, Yu.O. Synopsis of lectures on the discipline "Transport efficiency" / Yu.O. Davydich, G.I. Faletska, M.V. Olkhova // Kharkiv: National city university farm named after O.M. Beketova. –2019. – 74 p.

8. Prokudin, H.S. Methodology for assessing the quality and efficiency of transport services for the population of suburban areas / H.S. Prokudin, V.P. Kuzmich, N.V. Kopyak // Kharkiv: Collection of Scientific Papers of KNUZT named after Acad. V. Lazaryan. – 2020. –№19. – p.76 – 82.

9. Borovyk O.V., Kupelskyi V.V. "Metodika otseniya efektyvnosti voyennoho perevozen' kolonoj tekhniki" [Methods of evaluation of the effectiveness of military transportation by a column of technology]. – 2019. – No 67. – P.25–35.

10. Tabunenko, V.A. Methods of determining the effectiveness of the use of armored vehicles by units of the National Guard of Ukraine for the protection of public order in peacetime / V.A. Tabunenko, O.V. Ivanchenko, V.I. Kuzhelovich, P.D. Buryak // – Kharkiv: Honor and Law. – 2018. –№67. Vol.4. – p.82 – 87.

11. Sydorenko, R.G. Methods of evaluating the effectiveness of masking measures in the visible range of wave lengths / R.G. Sydorenko, G.V. Akulinin, S.A. Bezverkhyi, G.M. Safarova // – Kyiv: Science and technology of the Air Forces of the Armed Forces of Ukraine. – 2020. – №4. – p. 31-37.

12. Kokhan, V.F. The structure of the development and renewal of the fleet of wheeled equipment of the armies of NATO member countries from 2012 to 2022 / V. F. Kokhan // – Kyiv: Weapon systems and military equipment. – 2022. – №2(70). – p.6 – 15.

13. Budyanu, R.G. Justification of tactical and technical requirements for the development of promising models and further modernization of domestic "light" armored vehicles / R.G. Budyanu // – Kyiv: Scientific Bulletin of the National Forestry University of Ukraine. – 2015. – №25.3 – p.156 – 165.

Xülasə
Hərbi avtomobillərin xüsusiyyətlərinin təhlili
Anatoli Kovtun, Vladimir Tabunenko,
Sergey Nesterenko, Konstantin Borisenko

Hərbi təcavüzün başlaması ilə Ukrayna Silahlı Qüvvələrinin hərbi avtomobil texnikasının (HAT) arsenalı NATO ölkələrinin müasir, yüksək effektiv modelləri ilə tamamlandı ki, bu da düşməni döyüş meydanında məğlubiyyətə uğratmaqla ordunun silah sistemlərindən istifadəsi effektivliyini kəskin şəkildə artırdı. Avtomobil texnikasının təşkili və istismarı üzrə mövcud sənədlər HAT-nin istifadəsi üçün bəzi göstəriciləri müəyyən etməlidir. Hazırda istifadə olunan göstəricilər döyüş əməliyyatları zamanı avtomobil texnikasının döyüş effektivliyinin dərəcəsini qiymətləndirməyə imkan vermir. Məqalədə hərbi nəqliyyat vasitələrinin əsas xassələrinin müxtəlif növləri təhlil edilir və onların döyüş effektivliyini qiymətləndirmək üçün riyazi asılılıqlar əldə olunur. “Hərbi nəqliyyat vasitələrinin döyüş qabiliyyəti” kateqoriyasının mahiyyəti və məzmunu müəyyənləşdirilir, bu kateqoriyaya daxil olan xassələrin vahid anlayışı hazırlanır. Məqalədə hərbi maşınların döyüş qabiliyyətinin fərdi xüsusiyyətlərinin göstəricilərini müəyyən etmək üçün riyazi asılılıqları təklif edilmişdir ki, bu da onun qiymətləndirilməsi və proqnozlaşdırılması üçün riyazi aparat yaratmağa, eləcə də döyüşün (əməliyyatların) riyazi modellərini qurmağa imkan verir. Tədqiqatın məqsədi hərbi hissələrin ehtiyaclarını ödəmək üçün Ukrayna Silahlı Qüvvələri üçün NATO ölkələrinin hərbi avtomobil texnikasının yeni modellərinin əsas xüsusiyyətlərinin göstəricilərini müəyyən etməkdir. Məqalənin məqsədi müxtəlif növlər

(modifikasiyalar) üçün hərbi texnikanın əsas xassələrini müəyyən etmək və döyüş şəraitində nəzərdə tutulmuş tapşırıqları yerinə yetirərkən hərbi texnikanın döyüş effektivliyinin qiymətləndirilməsi üçün riyazi asılılıqları əldə etməkdir. Hərbi maşınların döyüş qabiliyyətinin səviyyəsini qiymətləndirmək üçün tədqiqat metodu kimi aşağıdakı metod və nəzəriyyələrdən istifadə edilmişdir: silah və hərbi texnikanın etibarlılığı, hərbi texnikadan istifadənin effektivliyi, hərbi texnikanın dayanıqlılığı, hərbi maşınların texniki istismarı, ehtimallar və riyazi statistika.

Açar sözlər: hərbi avtomobil texnikası, silah sistemlərindən istifadənin effektivliyi; avtomobil texnikasının əsas xassələri və döyüş effektivliyi

Аннотация
Анализ свойств военной автомобильной техники
Анатолий Ковтун, Владимир Табуненко,
Сергей Нестеренко, Константин Борисенко

С началом военной агрессии арсенал военной автомобильной техники (ВАТ) Вооруженных Сил Украины (ВСУ) пополнился современными высокоэффективными образцами стран НАТО, которые резко повысили эффективность применения систем вооружения военных формирований, заставив противника потерпеть поражение на поле боя. Действующие документы по организации и эксплуатации автомобильной техники нуждаются в определении некоторых из показателей применения ВАТ. Используемые показатели не позволяют оценить степень боеспособности автомобильной техники при ведении боевых действий. В статье проведен анализ различных типов (модификаций) основных свойств военной автомобильной техники и получены зависимости для оценки их боеспособности. Определены сущность и содержание категории «боевая способность военной автомобильной техники», разработано единое понимание свойств, входящих в эту категорию. В работе предложены математические зависимости для определения показателей отдельных свойств боевой способности военной автомобильной техники, позволяющей создать математический аппарат ее оценки и прогнозирования, позволяющий строить математические модели боя (операции), которые будут максимально соответствовать реальным процессам вооруженной борьбы, что является перспективным направлением дальнейших исследований. Задачей исследования является определение показателей основных свойств новых для ВСУ образцов ВАТ стран НАТО в целях обеспечения потребностей воинских подразделений. Целью статьи есть определение основных свойств ВАТ для различных типов (модификаций) и получение зависимости для оценки боеспособности ВАТ при выполнении задач по назначению в условиях ведения боевых действий. Методом исследований оценки уровня боеспособности военной автомобильной техники использованы теории: надежности вооружения и военной техники, эффективности применения ВАТ, живучести боевой техники, технической эксплуатации боевых машин, вероятностей и математическая статистика.

Ключевые слова: военная автомобильная техника, эффективность применения систем вооружения; основные свойства и боеспособность автомобильной техники

Məqalə redaksiyaya daxil olmuşdur: 30.01.2024
Təkrar işlənməyə göndərilmişdir: 12.02.2024
Çapa qəbul edilmişdir: 27.03.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 94-105
HƏRBİ XÜSUSİ ELMLƏR ***MILITARY SPECIAL SCIENCES***

UOT 623 DOI: 10.30546/9878.2024.2.10.0031.

İDARƏOLUNAN ZENİT RAKETLƏRİNİN SÜRƏTLİ BALLİSTİK RAKETLƏRƏ YÖNƏLDİLMƏSİ

t.e.d., professor Bayram İbrahimov
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
i.bayram@mail.ru

m.t.h.e.ü.f.d., dosent, polkovnik Yalçın İsayev
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
timuchinumud@gmail.com

polkovnik Eldar Əliyev
Hərbi İdarəetmə İnstitutu

dosent Əhəd İsayev
Heydər Əliyev adına Hərbi İnstitut
keshikten@mail.ru

Xülasə. Məqalədə "İsgəndər" sinfinə daxil olan əməliyyat-taktiki raket komplekslərinin imkanlarının nümunəsində onların yüksəksürətli ballistik hədəflərə qarşı yönəldilməsinin əsas xüsusiyyətlərindən bəhs edilir. Bundan əlavə, kalman süzgəci əsasında ballistik obyektin koordinatlarının təyin edilməsinin statistik işlənməsi üçün rekurrent alqoritmin, raketin fəzada vəziyyətinin, sürət komponentlərinin və ballistika əmsalının təyin edilməsi dəqiqliyinin qiymətləndirilməsi nəzərdən keçirilmişdir. Tədqiqat işinin məqsədi radiolokasiya stansiyası (RLS) məlumatlarının Kalman süzgəci vasitəsilə emalının, o cümlədən raketin ballistik və aerodinamik hədəflərə yönəldilməsinin modelləşdirilməsinin həyata keçirilməsidir. Məqsədə nail olmaq üçün qarşıya qoyulmuş vəzifələr aşağıdakılardır: Yer atmosferində ballistik hədəfin ağırlıq mərkəzinin hərəkət tənliyinin təyin edilməsi; radiolokasiya stansiyasının ballistik hədəfi müşayiətmə səhvlərinin qiymətləndirilməsi; ballistik hədəfin məhv edilmə ehtimalının qiymətləndirilməsi; idarəolunan zenit raketinin ballistik hədəflə qarşılaşma nöqtəsinin koordinatının hesabatının aparılması; ballistik hədəfin məhvedilmə ehtimalının qiymətləndirilməsi. Problemləri həll etmək üçün nəzəri təhlil, riyazi modelləşdirmə, riyazi statistika tədqiqat metodlarından istifadə olunur. Tədqiqat işində nəticə olaraq: Kalman süzgəcinin radiolokasiya stansiyasında məlumatların emalı üçün optimal süzgəc olduğu müəyyən edilmişdir. Ballistika əmsalı və hədəfin xüsusiyyətlərinin obyektiv qiymətləndirilməsi vasitəsilə yalançı hədəflərin seleksiyası modelləşdirilmişdir. Modelləşdirmənin nəticələrinə əsaslanaraq, aerodinamik hədəflərin tutulması zamanı özüyönələn başlıqla raketin müşayiət vaxtının 5-7 saniyəyə qədər uzadılması və radiolokasiya stansiyasının hədəfi müşayiət edən siqnal tezliyinin 20 Hs-ə qədər artırılması təklif olunmuşdur.

Açar sözlər: ballistik hədəf , aerodinamik hədəf, özüyönələn başlıq, alqoritmik-proqram təminatı, yerli yer koordinat sistemi, çoxməqsədli radiolokasiya stansiyası , effektiv əksetdirmə sahəsi, mühərrik qurğusu, döyüş başlığı

Giriş

XXI əsrin hava hücum silahlarının hazırlanmasında əsas istiqamətlərdən biri də ballistik və aerodinamik pilotsuz uçuş aparatlarının hazırlanması və istehsalı olmuşdur. Bu tendensiya pilotsuz uçuş vasitələrinin istehsalı üçün xərclərin əhəmiyyətli dərəcədə aşağı olması ilə əlaqələndirilir. Bununla əlaqədar olaraq, RLS-lər və onların alqoritmik-proqram təminatının (APT) təkmilləşdirilməsi kimi bir vəzifə ortaya çıxır. Ballistik raket (BR) – uçuşunun çox hissəsini ballistik trayektoriya üzrə qət edən, nəzarətsiz hərəkətdə olan bir raketdir.

Uçuş üçün tələb olunan sürət və istiqamət ballistik raketin mühərrik qurğusuna (MQ) onun uçuşunun aktiv hissəsində çatdırılır. MQ öz işini bitirdikdən sonra raketin faydalı yükü olan döyüş hissəsi uçuş marşrutunun qalan hissəsində ballistik trayektoriya üzrə hərəkətini davam etdirir. Ballistik raketlər çoxpilləli ola bilər, bu halda, raket tələb olunan sürətə çatdıqdan sonra işlənmiş pillələr ayrılır.

Ballistik obyekt koordinatlarının Kalman süzgəci əsasında statistik emaletmə nəzəriyyəsi hələ keçən əsrin 60–70-ci illərində işlənib hazırlanmışdır. Lakin matris nisbətlərinin hesablanmasının mürəkkəbliyi alınan alqoritmlərin tam həcmdə real hava hücumundan müdafiə (HHM) sistemlərinə daxil edilməsinə imkan vermirdi. Zaman keçdikcə hesablama texnikasının sürətli inkişafı bu çatışmazlığın aradan qaldırılmasına geniş imkan yaratdı.

Kalman süzgəci əvvəlcədən məlum olan dinamik sistemin vəziyyət vektorunu rekursiv qiymətləndirmək üçün nəzərdə tutulmuşdur, yəni sistemin cari vəziyyətini hesablamaq üçün cari ölçməni, həmçinin süzgəcin özünün əvvəlki vəziyyətini bilmək vacibdir.

Beləliklə, Kalman süzgəci, digər rekursiv süzgəclər kimi, tezlik görünüşündə deyil, zaman görünüşündə reallaşdırılıb. Lakin digər oxşar süzgəclərdən fərqli olaraq, Kalman süzgəci, Bayesin şərtli ehtimal düsturuna əsaslanaraq, yalnız vəziyyətin qiymətlərindən ilə deyil, vəziyyət vektorunun qeyri-müəyyən qiymətlərindən (yəni ölçmələrin səhvləri) də yararlanır. Vəziyyət vektorunun qiymətlərinə əsasən ballistik hədəfin trayektoriyası prolonqasiya edilir və idarəolunan zenit raketinin ballistik hədəflə qarşılaşma nöqtəsinin koordinatları müəyyən edilir. İdarəolunan zenit raketinin (İZR) hədəflə görüşündən bir qədər əvvəl özüyönələn başlıq (ÖYB) ballistik hədəf BH-dən əksolunan siqnalı avtomatik müşayiətə götürür və İZR-nin ballistik hədəfə doğru özüyönəlməsi prosesi başlayır.

1. Yer atmosferində ballistik hədəfin ağırlıq mərkəzinin hərəkətinin tənliyi

Qiymətlər vektoru və kovariasiya matrisinin proqnozlaşması üçün ballistik hədəfin hərəkət modelinin ifadəsi zəruridir. O, göstərilən differensial tənliklərlə ifadə edilir:

$$\ddot{x} = -\frac{g_0}{R}\left(\frac{R_y}{R}\right)^2 x - \gamma\,\frac{\rho V}{2}\,\dot{x} + W_{xk} + W_{xn};$$

$$\ddot{y} = -\frac{g_0}{R}\left(\frac{R_y}{R}\right)^2 (y + R_y) - \gamma\,\frac{\rho V}{2}\,\dot{y} + W_{yk} + W_{yn}; \quad (1)$$

$$\ddot{z} = -\frac{g_0}{R}\left(\frac{R_y}{R}\right)^2 z - \gamma\,\frac{\rho V}{2}\,\dot{z} + W_{zk} + W_{zn};$$

burada,

g_o – Yer kürəsi səthindəki cazibə qüvvəsinin təcili;
R_y – Yer kürəsinin radiusu;
R – ballistik hədəfin Yer kürəsinin mərkəzindən uzaqlaşması;
ρ – ballistik hədəfin uçuş hündürlüyündə atmosferin sıxlığı;
V – ballistik hədəfin sürəti;
W_{zk} ,W_{yk} , W_{xk} – koriolis təcilin komponentləri,
W_{xn}, W_{yn}, W_{zn}, – ötürülən təcilin komponentləri.
Koriolis və ötürülmə təcilləri aşağıdakı kimi təyin edilir:

$$W_{xi} = -\Omega_y^2 \cdot \sin(\varphi) \cdot \left((y + R_y) \cdot \cos(\varphi) - x \cdot \sin(\varphi)\right);$$

$$W_{yi} = -\Omega_y^2 \cdot \cos(\varphi) \cdot \left((y + R_y) \cdot \cos(\varphi) - x \cdot \sin(\varphi)\right);$$

$$W_{zi} = -\Omega_y^2 \cdot z; \quad (2)$$

$$W_{xk} = -2 \cdot \Omega_y \cdot \sin(\varphi) \cdot \dot{z};$$

$$W_{yk} = -2 \cdot \Omega_y \cdot \cos(\varphi) \cdot \dot{z};$$

$$W_{zk} = -2 \cdot \Omega_y \cdot (\dot{y}\cos(\varphi) - \dot{x}\sin(\varphi)),$$

burada,

Ω_y = 7,292115·10-51/c – Yer kürəsinin fırlanmasının bucaq sürəti;

R_y = 6371210 м. – Yer kürəsinin radiusur;

φ – RLS-nin yerləşmə enliyidir (YYKS koordinatların başlanğıcı).

Ballistika əmsalı aşağıdakı düsturla ifadə olunur:

$$\gamma = C_x \frac{S}{m}, \quad (3)$$

burada,

C_x – ön müqavimətinin aerodinamik əmsalı;

S – Midel sahəsi;

m – ballistik obyektin çəkisidir.

Qiymətləndirmə vektorunun daha dəqiq ekstrapolyasiyasının əldə edilməsi üçün ballistika əmsalının (BƏ) aproksimasiyasını daxil etmək zəruridir. BƏ Max ədədi M-dən, hücum bucağı α və Reynolds ədədindən R asılıdır:

$$\gamma = f(M, \alpha, R) \quad (4)$$

Yuxarıda göstərilən asılılığa əlavə olaraq, uçuş trayektoriyasını müəyyən edən ballistika əmsalı, döyüş başlığının (DB) formasından, onun qızması və yanması zamanı BH-nin (və ya pilləsinin) kütləsinin dəyişməsindən asılıdır.

Buna görə də ballistika əmsalının ön müqavimət əmsalından, Midel sahəsindən və statistik işləmə alqoritmində BH-nin (və ya pillləsinin) kütləsindən asılılığı haqqında dəqiq qeydiyyat aparmaq məqsədəuyğun deyil, çünki BH-nin xüsusiyyətlərinin dəqiq müəyyən edilməsi mümkün deyil. BƏ əhəmiyyətli dərəcədə Max ədədi M-dən asılıdır. Əgər hipersəs sürətinə malik BH ($M > 6$) üçün bu asılılıq o qədər də böyük deyilsə, səsdən yuxarı ($1 \leq M \leq 6$) sürətli BH-lər üçün bu asılılıq mühüm əhəmiyyət kəsb edir.

BƏ, səs sürətinə qədər ($0 < M < 1$) sürətlərdə uçarkən, Max ədədinin artması ilə demək olar ki, sabit qalır, sonra isə artır. Təkrarlanan (rekurent) alqoritmdə Max ədədindən asılı olaraq, iki mərhələdə γ aproksimasiyası daxil edilir. Birinci mərhələdə Max ədədinin yüksək qiymətlərində BƏ γ_∞ təyin edilir. Sonra isə BƏ-nin ekstrapolyasiya olunmuş qiyməti $\hat{\gamma}_t$ hesablanır.

BƏ γ_∞ hesablanması aşağıdakı tənliklə aparılır:

$$\gamma_\infty = \gamma^*, M > 6 \; olduqda;$$

$$\gamma_\infty = \frac{\gamma^*}{1+(6-M)^2/18}, 1 \leq M \leq 1 \; olduqda; \quad (5)$$

$$\gamma_\infty = \frac{\gamma^*}{1{,}5+3{,}55(M-0{,}75)}, 0{,}75 \leq M < 1 \; olduqda;$$

$$\gamma_\infty = \frac{2}{3}\gamma^* \; M < 0{,}75 \; olduqda.$$

Burada,

γ^* – ballistika əmsalının qiyməti;

M – γ^* qiymətinin alınması zamanı Max ədədidir.

Max ədədindən və ekstrapolyasiya zamanı istifadə olunan γ_∞ asılı olaraq, BƏ-nin aproksimasiyası aşağıdakı üsulla təyin olunur:

$$\hat{\gamma} = \gamma_\infty, M > 6 \; olduqda;$$

$$\hat{\gamma} = \gamma_\infty + \gamma_\infty(6 - M)^2/18, 1 \le M \le 6 \; olduqda; \quad (6)$$

$$\hat{\gamma} = \gamma_\infty (1{,}5 + 3{,}55\,(M - 0{,}75)), 0{,}75 \le M < 6 \; olduqda;$$

$$\hat{\gamma} = \frac{3}{2}\gamma_\infty, M < 0{,}75 \; olduqda;$$

Burada,

$\hat{\gamma}$ – BƏ-nin ekstrapolyasiya olunmuş qiymətidir.

2. Ballistik hədəflərin əsas xarakteristikaları

Tətbiq sahəsinə görə BR taktiki (TBR), əməliyyat-taktiki (ƏTBR) və orta məsafəli (OMBR) ballistik raketlərə bölünür. Taktiki və əməliyyat-taktiki raketlər kiçikməsafəli raketlərə (20-1000 km), OMBR isə ortaməsafəli raketlərə (1000-5500 km) aiddir. BR-nin uçuş sürəti 250-5500 m/s həddində dəyişir.

Digər vacib xassələrdən biri də BR effektiv əksetdirmə sahəsidir (EƏS). EƏS – raketin əksetdirici xüsusiyyətlərini, onun konfiqurasiyasını, materialının elektrik xassələrini və raketin ölçüsünün dalğa uzunluğuna olan nisbətindən asılılığnı nəzərə alaraq, kvadrat metrlərlə ifadə olunan bir qiymətdir. Ballistik raketlərin EƏS 0,04 – 1 м^2 həddində dəyişir. "Stels" texnologiyalarının tətbiqi zamanı BR EƏS-si daha kiçik ola bilər [1].

Yüksəksürətli ballistik hədəflərin əsas xarakteristikalarını "İsgəndər" tipli əməliyyat-taktiki raket kompleksinin xüsusiyyətlərinin nümunəsində araşdıraq. Tuşlama üsulundan asılı olaraq, hədəfdən dairəvi sapması 1–30 m arasında dəyişir. Raketin start kütləsi 3800 kq, ondan 480 kq döyüş hissəsi təşkil edir. Raketin uzunluğu 7,2 m, diametri isə 920 mm təşkil edir. Uçuş trayektoriyasının başlanğıc hissəsindən sonra, bu tip raketlərin sürəti 2100 m/s çatır. Təsir uzaqlığı 50–500 km arasında olur. Raketlərin buraxılması arasında interval bir dəqiqə təşkil edir. Kompleks –50°C +50°C temperaturlarda işləmək qabiliyyətini saxlayır [2].

Döyüş başlıqlarının növləri.

Adi təchizatda:

– kontaktsız partlayan 54 ədəd qəlpəli döyüş elementli kaset (yerin səthinə çatmadan təqribən 10 m hündürlükdə işə düşür);
– kumulyativ qəlpəli döyüş elementli kaset;
– özü tuşlanan döyüş elementli kaset;
– həcm-partlayışlı təsirli kaset;
– qəlpəli-fuqas;
– yandırıcı-fuqas;
– nüfuzedici;
– xüsusi (nüvə).

9M723K1 tipli raket kompleksi bərk yanacaqlı və tək pilləlidir. Raketin uçuş trayektoriyası trayektoriyanın başlanğıc və son hissələrində manevr etməklə kvaziballistikdir. Uçuş zamanı raket aerodinamik və qazodinamik sükanlardan istifadə etməklə idarə olunur. Radiolokasiya görünüşünün azaldılması (Stels texnologiya) texnologiyalarının geniş tətbiqi ilə istehsal olunub: kiçik əksetdirmə səthi, xüsusi örtüklər, kiçikölçülü çıxıntı hissələr və s. Uçuşun çox hissəsi təxminən 50 km hündürlükdə baş verir. Raket uçuşun son mərhələsində 20 g vahid yüklənməsi ilə intensiv raket əleyhinə manevretməni həyata keçirə bilər. Qarışıq tuşlama sistemi: inersial – uçuşun başlanğıc və orta mərhələsində; optik – uçuşun son mərhələsində, bununla da xətası 5–7 metr təşkil edən dəqiqlik əldə edilir. İnersial tuşlama sistemi ilə yanaşı, GPS/GLONASS-nin istifadəsi mümkündür.

3. Çoxməqsədli radiolokasiya stansiyası (ÇRLS) ilə ballistik hədəfin müşayiət etməsinin səhvlər modeli.

Səhvlər modelinə daxildir:

– sistematik səhvlər;
– küy səhvləri;
– bucaq səhvləri.

Sistematik səhvlər RLS antenasının üfüqün yanlarına qeyri-dəqiq bağlaması və RLS qeyri-şaqulilik vericilərinin (datçiklərin) qeyri-dəqiq göstəriciləri ilə şərtlənir. Həmçinin sistematik səhvlər bucaq koordinatlarına görə:

– bucaq koordinatları üzrə $\sigma_{\varepsilon,\beta} \approx 2 \div 6$ dərəcə/dəqiqə;
– dekart koordinatları üzrə $\sigma_{\Delta x,y,\,z} \approx 5 \div 10$ m;
– küy səhvləri əsasən siqnal/küy nisbəti ilə təyin olunur.
– bucaq koordinatları üzrə:

$$\sigma_{\kappa\varphi_{\ddot{u}}\varphi_{ş}} = \frac{\Delta\theta\,\varphi_{\ddot{u}}\varphi_{ş}}{K_{\varphi}\sqrt{\rho}} \tag{7}$$

Burada,
$\Delta\theta\,\varphi_{ü}\,\varphi_{ş}$ – şüanın eni;
ρ – siqnal/küy nisbəti;
K_{φ} – RLS-nin konstruktiv əmsalıdır.
Uzaqlığa görə:

$$\sigma_r = \frac{\Delta r}{k_r\sqrt{\rho}} \tag{8}$$

Burada,
Δr – strobun eni;
k_r – RLS-nin uzaqlığa görə konstruktiv əmsalıdır.
Dopler sürətinə görə:

$$\sigma_{\dot{r}} = \frac{\Delta\dot{r}}{k_{\dot{r}}\sqrt{\rho}} \tag{9}$$

Burada,
$\Delta\dot{r}$ – RLS Dopler süzgəcinin zolağı;
$k_{\dot{r}}$ – konstruktiv əmsaldır.
Konstruktiv əmsallar RLS keyfiyyətini xarakterizə edirlər, əmsalların göstəriciləri nə qədər çox olarsa, o qədər keyfiyyətli RLS icra edilər.

Devid Noks Bartonun fikrincə, əmsalların 1,5 göstəriciləri olduqca əlverişlidir. Maksimal qiymətləri isə ≈ 3. Siqnal/küy nisbəti:

$$\rho = k_m \frac{S}{R^{y}} \tag{10}$$

Burada,
K_m – güc üzrə konstruktiv əmsal;
R – ballistik hədəfə qədər məsafə;
S – effektiv əksetdirmə sahəsidir.

BH-nin müşayiəti $\rho \geq 13$ dB zamanı baş verir. BH-nin modelində EƏS loq-normal təsadüfi prosesin paylanması qanuna uyğun verilir.

Bucaq səhvləri RLS yerləşdiyi yerdən müşahidə edildikdə, bucaqlara çevrilmiş BH-nin xətti ölçüləri ilə müəyyənləşdirilir. R məsafəsində bucaq səhvləri göstərilən düsturla müəyyən ediləcək:

$$\sigma_{\varphi} = \frac{\Delta l}{R} \tag{11}$$

Burada,
Δl – ballistik hədəfin xətti ölçüləridir.

4. Ölçmələrin statistik emalı alqoritmi

Yuxarıda qeyd edildiyi kimi, RLS ilə ölçülən koordinatlar Kalman süzgəcindən istifadə edilərək işlənilir. O, sistemin dinamik modelindən, məlum qarşılıqlı idarəetmə təsirləri və optimal vəziyyət qiymətlərinin əmələ gəlməsi ilə bağlı ardıcıl ölçmələrdən istifadə edir. Alqoritm iki təkrar mərhələdən ibarətdir: qabaqcadan məlumatvermə və ölçmələrdə düzəlişin edilməsi. Birinci mərhələdə vaxtın növbəti anı üçün ilkin məlumat hesablanır. İkinci mərhələdə isə RLS-dən gələn yeni məlumat qabaqcadan verilən məlumatı dəqiqləşdirir.

Problemin xətti formallaşma halı üçün ölçü xətalarının paylanmasının normal qanunu və hərəkətin dəqiq fərq tənlikləri ilə təkrarlanan alqoritm, kriteriyaya uyğun olaraq, optimal qiymətləri əldə etməyə imkan verir [5]:

$$\min j = \sum_{k=1}^{m} \sigma_k^2 \tag{12}$$

Burada,

m – faza vektoru komponentlərin sayı;

σ_k^2 – k-faza vektoru komponentinin qiymətlər dispersiyasıdır.

Yuxarıda qeyd edilənlər riyazi olaraq sübut olunmuşdur. Beləliklə, aydın olur ki, tapşırığın heç bir alqoritmi Kalman süzgəcinin təkrarlanan (rekurent) alqoritmdən daha dəqiq qiymətləri verə bilməz.

Kalman süzgəcinin üstünlüklərinə aiddir: təkrarlanma və optimallıq, əvvəlcədən olan məlumatların istifadəsi, ilkin hərəkət modeli, qeyri-bərabər ölçü xətalarının statistik xüsusiyyətləri, məhdud "yaddaş"ın toplanması, ölçülərin alınmasının qeyri-bərabər vaxtı və onun işləməsinin mümkünlüyü, bütün ölçülər cəmindən istifadə, müasir RLS tərəfindən həyata keçirilən dopler sürətinin ölçülməsi. Kalman süzgəci faza koordinatları ilə yanaşı, onların seleksiya tapşırıqlarının həlli və qiymətlərinin kompleksləşdirilməsi üçün istifadə olunan dispersiyanın qiymətlərini də hesablayır. Təkrarlanan alqoritmin əsas formula asılılıqları aşağıdakı matris münasibətləridir:

– faza vektoru və onun kovariasiya matrisinin ekstrapolyasiya tənliyi:

$$D_{i/_{i-1}} = F_i\, D_{i-1} F_i^T; \tag{13}$$

$$\hat{X}_i = \Phi(X_{i-1}^*);$$

– qiymətlər vektoru və onun i – vaxt anı üçün kovariasiya matrisinin hesablanması tənliyi:

$$S_i = D_{i/_{i-1}} H_i^T (H_i\, D_{i-1} H_i^T + Q_i)^{-1};$$

$$X_i^* = \hat{X}_i + S_i(Y_i - H_i(\hat{X}_i)); \tag{14}$$

$$D_i = D_{i/_{i-1}} - S_i H_i D_{i/_{i-1}},$$

burada,

i – ölçü vektoru və alqoritm sayının takt nömrəsi;

$X_i^* - x_i^*, y_i^*, z_i^*, \dot{x}_i^*, \dot{y}_i^*, \dot{z}_i^*, \gamma_i^*$ komponentləri ilə qiymətlər vektoru;

$\hat{X}_l$ – alqoritmin takt sayına ekstrapolyasiya olunmuş qiymətlər vektoru;

Y_i – x, y, z, $\dot{r}$ komponentləri ilə ölçmələr vektoru;

D_i – X_i^* qiymətləndirmələrin vektorunun kovariasiya matrisi;

S_i – çəki matrisi;

Q_i – Y_i ölçmələr vektorunun kovariasiya matrisi;

F_i – faza vektorunun evolyusiya matrisi;

$H_i(\hat{X}_i)$ – t_i vaxtın anı üçün gözlənilən ölçü vektorunun hesablama üsulu;

$D_{i/_{i-1}}$ – ekstrapolyasiya olunmuş $\hat{X}_l$ vektorunun matrisi;

$\Phi(X_{i-1}^*)$ – t_i vaxtın anı üçün X_{i-1}^* vektorunun ekstrapolyasiya üsulu.

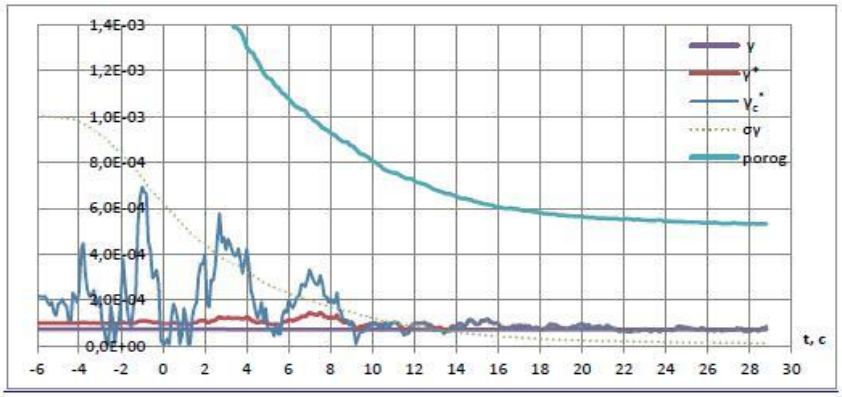
Diferensial tənliklər ballistika əmsalındakı uyğunsuzluqlar və döyüş başlığının mümkün qızması və yanması səbəbindən ballistik hədəfin hərəkəti ilə dəqiq uyğunlaşa bilmir ki, bu da dinamik xətalara və yaxud alqoritmin divergensiyasına səbəb olur. Bu neqativ nəticələrin aradan qaldırması üçün hər bir ölçmənin alınması taktında sürət komponentinin dispersiyasına və ballistika əmsallarına sabit kəmiyyətlər əlavə olunur. Bu ümum qəbul edilmiş üsul rekurent süzgəcin yaddaşını da məhdudlaşdırır.

Rekurent alqoritm, hədəfgöstərmə, yaxud ölçmələrin ilkin emalı zamanı ballistika əmsalının qiymətləndirməsi məqsədilə alınmış faza vektorunun göstəricisi olan yerləşmə və sürət qiymətlərindən istifadə edir. Faza vektorunun başlanğıc qiymətlərinə uyğun olaraq, onun kovariasiya matrisinin başlanğıc elementləri seçilir. İlk kovariasiya D matrisinin qismində diaqonal matrisdən istifadə təklif olunur. Vəziyyət vektoru komponentlərinin dispersiyası kimi, hədəfgöstərmə qiymətlərinin aprior dispersiyaları və ya dekart koordinat ölçmələri, sürət komponentlərinin dispersiyaları kimi sürət komponentlərinin qiymətləndirilməsi dispersiyaları, ballistik əmsalın dispersiyası kimi dispersiyasının apriori dəyəri götürülür. Kiçik EƏS olan BH müşayiəti zamanı əks olunmuş siqnalın fedinqinə (zəifləmə) görə ölçmələr bir neçə takt ərzində olmaya bilər. Ölçmələri olmayan zaman alqoritmin işini təmin edən üsullarından biri S_i çəki matrisin sıfırlanması sayılır. Koordinatların statistik işlənməsinin alqoritminə xəta (dayanma) ölçmələrinin qeydiyyat mexanizminin daxil edilməsi təklif olunur. Əgər $Y_i - H_i\hat{X}_i$ uyğunsuzluqlar vektorunun komponentinin kvadratı verilmiş komponentin dispersiyasının n qat qiymətləndirilməsindən yüksəkdirsə, onda S_i (n əmsalı modelləşmə nəticəsinə görə seçilir) çəki matrisinin sıfırlanması baş verir. Uyğunsuzluqlar vektorunun komponentlərinin dispersiyalarının qiymətləri $H_i\, D_{i-1} H_i^T + Q_i$ matrisinin diaqonal elementlərini özündə əks etdirir.

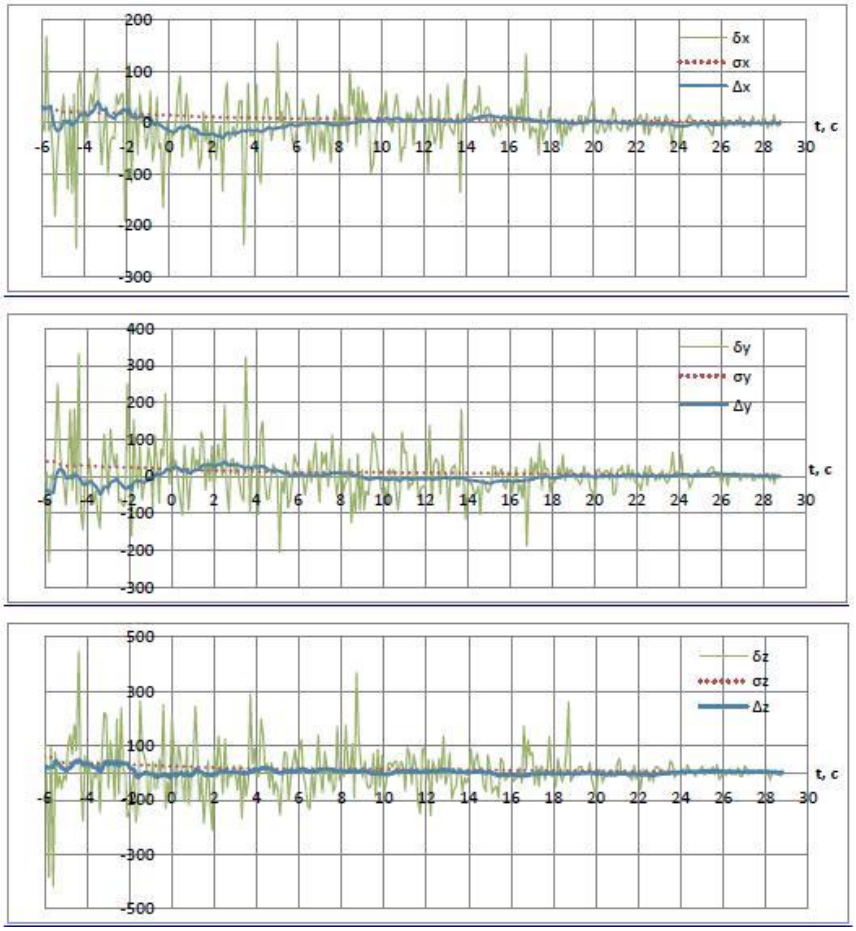
5. Ballistik hədəfin ağırlıq mərkəzinin hərəkətinin prolonqasiyası.

Hərəkətin uzun müddət davamiyyəti (ekstrapolyasiya) 1-ci başlıqda əvvəl göstərilmiş tənliklərdən istifadə etməklə 4-cü dərəcəli Runqe – Kutt metodu ilə həyata keçirilir. Şəkillərdə (Şəkil 1; 2 və 3) $V \approx 2000\ m/san$ sürəti ilə hərəkət edən BH-nin modelləşməsinin nəticələri təqdim olunmuşdur. Şəkillərdə göstərilir:

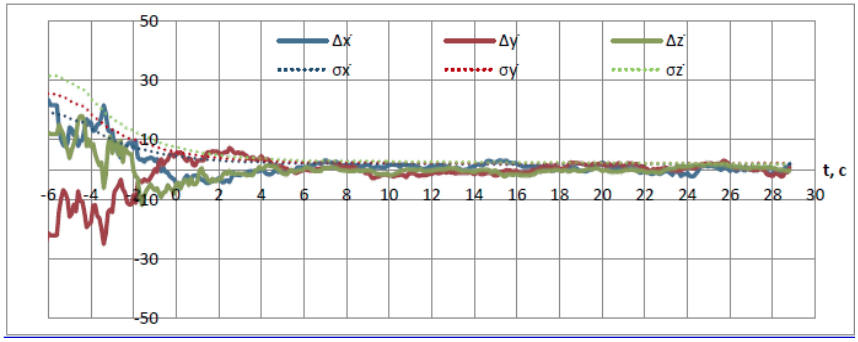
– γ – ballistika əmsalı;
– γ^* – raketin yönəltməsi üçün istifadə olunan BƏ-nın qiyməti;
– γ_s^* – seleksiya üçün istifadə olunan BƏ-nın qiyməti;
– σ_γ – BƏ qiymətinin orta kvadratik səhvi (OKS);
– *porog* – seleksiya üçün istifadə olunan həddi göstərici;
– *Δx, Δy, Δz* – koordinat səhvlərinin qiymətləri;
– *δx, δy, δz* – RLS ölçmələrin səhvləri;
– $\sigma_x, \sigma_y, \sigma_z$ – təkrarlanan süzgəci ilə hesablanmış koordinat səhvləri qiymətlərinin orta kvadratik sapması;
– $\Delta\dot{x}, \Delta\dot{y}, \Delta\dot{z},$ – sürət vektorunun komponent səhvlərinin qiymətləri;
– $\sigma_{\dot{x}}, \sigma_{\dot{y}}, \sigma_{\dot{z}}$ – təkrarlanan alqoritmlə hesablanmış sürət komponentlərinin səhv qiymətinin orta kvadratik sapması.



Şəkil 1. Ballistika əmsalı, onun qiymətləri və orta kvadratik səhv



Şəkil 2. Koordinatların ölçmələri səhvi, qiymətlər və onların OKS



Şəkil 3. Sürət komponentləri qiymətlərin səhvləri və onların OKS

Görüş anı üçün hədəfin hərəkətinin uzun müddət davamiyyət dəqiqliyinin qiymətləndiriməsi aşağıdakı kimi həyata keçirildi. Prolonqasiya alqoritminin girişinə hədəf koordinatların qiymətləri x^*, y^*, z^*, hədəf koordinatlarının törəmələrinin qiymətləri $\dot{x}^*, \dot{y}^*, \dot{z}^*$ və γ^* ballistika əmsalının qiyməti daxil olurdu. Alqoritmin çıxışında τ vaxtı ərzində uzun müddət təkrarlanan koordinatların, sürət komponentləri və ballistika əmsalının qiyməti işlənildi. BH-nin daha dəqiq prolonqasiya edilməsi üçün BH koordinatlarının statistik işlənməsi alqoritmində olduğu kimi eyni BH aproksimasiya alqoritmi istifadə olunmuşdu. Prolonqasiya alqoritmində 4-cü dərəcəli Runqe – Kutt ədədi inteqrasiya üsulu istifadə olunmuşdu. Prolonqasiya intervalı, hər birində faza vektorunun qiyməti hesablamaqla, dörd bərabər hissəyə bölünürdü. Görüş nöqtəsində Kalman süzgəci əsasında alqoritm qiymətlərinin prolonqasiyası zamanı səhvlərin qiymətləndirilməsi riyazi model üzərində həyata keçirilmişdir. Kalman süzgəcindən əldə edilən koordinatın qiymətləri konstanta ilə müəyyənləşdirilmiş cari və görüş vaxtı arasındakı fərqə bərabər zamana prolonqasiya edilmişdir. Nəticədə səhvlərin

prolonqasiya zamanından asılılıqları əldə olunmuşdur. Prolonqasiya səhvlərinin davranış xarakterini aşağıdakı kimi şərh etmək olar. Yüksək atmosfer sahəsindəki prolonqasiya və sürətin hesablanması səhvləri, qismən də hədəfin ballistika əmsalının həqiqi qiyməti ilə apriori arasındakı uyğunsuzluqdan asılıdır. Atmosferin sıx qatlarına daxil olduqdan sonra BƏ-nin dəqiqləşməsi başlayır, lakin onun prolonqasiya olunmuş faza vektoruna təsiri artdığından, prolonqasiya səhvləri də artır. BH-nin atmosferin daha sıx qatlarına daxil olması ilə səhvlər azalır [7].

6. İdarəolunan zenit raketinin ballistik hədəflə görüş nöqtəsinin koordinatının hesabatı

İZR-nin BH ilə qarşılaşma nöqtəsinin koordinatlarının hesablanması iterasiyaetmə metodu ilə həyata keçirilir. Bu zaman təsbit edilən zaman və növbəti an üçün görüşün koordinatları hesablanır. Bu üsulda hədəf və raketin hərəkətinin prolonqasiyası aparılır və yeni alınmış nəticələr istifadə edilir.

Belə hesablamalar zamanın hər bir anı üçün aparılır. Görüş nöqtəsi 10-20 Hs tezliyi ilə rekursiv olaraq hesablanır. Bu tezliklə raketdən görüş nöqtəsinə qədər olan məsafə və ona çatma vaxtı yenidən hesablanır. Görüş nöqtəsinə edilən düzəlişlərdən asılı olaraq, ona çatmaq üçün də vaxt korrektə edilir. Bunun səbəbi aşağıdakılardan irəli gəlir:

$$\Delta\tau = -\frac{\Delta x\Delta\dot{x}+\Delta y\Delta\dot{y}+\Delta z\Delta\dot{z}}{V_{nisb.}^2} \quad (15)$$

Burada,

$\Delta x, \Delta y, \Delta z$ – qarşılaşma anında BH və raket nisbəti yerləşməsi koordinatları;

$\Delta\dot{x}, \Delta\dot{y}, \Delta\dot{z}$ – qarşılaşma anında nisbəti sürətinin komponentləridir.

$\Delta\tau$ qiyməti, τ düsturunun köməyi ilə hesablanma zamanının korrektə edilməsində istifadə olunur.

$$\tau_к = \tau_{к-1} + \Delta\tau_к \quad (16)$$

Görüş nöqtəsinin hesablanmış koordinatları sabit dəyərlər deyil, çünki onlar informasiya yığıldıqca daim yenilənir.

Qeyd etmək lazımdır ki, belə düzəlişlər ətraf mühitin şəraitinə və digər amillərlə sıx bağlıdır.

7. Ballistik hədəfin məhvedilmə ehtimalının qiymətləndirilməsi.

İZR döyüş tətbiqi metodundan asılı olmayaraq, funksional effektivliyin əsas göstəricisi tək hədəfə bir raket atılan zaman hədəfin məhv olunması ehtimalı olacaq. Bir İZR ilə hədəfinin məhv edilməsinin ardıcıl vaxtda baş verən iki təsadüfi hadisədən ibarət mürəkkəb hadisə kimi qiymətləndirilməsi mümkündür. İlkin təsadüfi hadisə ondan ibarətdir ki, raketin döyüş hissəsinin partlaması h yanılması ilə fəzanın məhz bu verilən nöqtəsində baş verib. Bu hadisənin ehtimalı atəş zamanı yaranan tuşlama səhvləri və səhvlərin idarə edilməsi $\varphi(h)$ qanunu ilə müəyyən olunur. Bu səhvlər, təcrübələrdən göründüyü kimi, hədəfin mərkəzi ilə üst-üstə düşən, dairəvi $(\sigma_y = \sigma_z = \sigma)$ olana yaxın bir qanunla paylanır, o cümlədən yayınmalar paylanması ehtimalının sıxlığı Reley qanununa tabe olur:

$$\varphi(h) = \frac{h}{\sigma^2} e^{-\frac{h^2}{2\sigma^2}} \quad (17)$$

Burada,

σ – hədəfdən yayınmanın orta kvadratik qiymətidir.

İkinci təsadüfi hadisə ondan ibarətdir ki, raketin döyüş hissəsinin zərərvurma elementlərinin h yayınması anında partlayış hədəfə zərər vuracaq. Bu hadisənin ehtimalı hədəfin məhv edilməsinin şərti $p(h)$ qanunu ilə təyin edilir və $p(h)$ qanununun bir funksiyadır:

– raketin döyüş hissəsinin növü və xüsusiyyətlərinin;
– radiopartlayıcının parametrlərinin;
– hədəflə raketin qarşılaşma şərtlərinin (raket və hədəfin sürət vektorunun istiqaməti və modulu, və s.)
– hədəfin zəifliklərinin.

İdarəetmə və yönəltmə xətalarının dairəvi paylanması ilə hədəfin məhv edilməsinin şərti qanunu təqribi asılılıqla təsvir olunur.

$$p(h) = e^{-\frac{h^2}{2R_0^2}} \quad (18)$$

Burada,

R_0 – hədəfin şərti vurulma ehtimalı 0,606 olan zaman yayınmanın qiymətinə ədədi bərabər olan şərti qanunun parametridir.

Mürəkkəb hadisənin tam ehtimalı olacaq:

$$W = \int_0^\infty \varphi(h)p(h)dh = \int_0^\infty \frac{h}{\sigma^2}\, e^{-\frac{h^2}{2}\left(\frac{R_0^2+\sigma^2}{R_0^2\sigma^2}\right)}\, dh \quad (19)$$

Əvəzetmə ilə:

$$t = \frac{h^2}{2}\left(\frac{R_0^2+\sigma^2}{R_0^2+\sigma^2}\right) \quad (20)$$

Alırıq:

$$W = \frac{R_0^2}{R_0^2+\sigma^2}\int_0^\infty e^{-t}\, dt, \quad (21)$$

Nəticə olaraq:

$$W = \frac{R_0^2}{R_0^2+\sigma^2} \quad (22)$$

8. ZİR-nin ballistik raketlərə tuşlaması xüsusiyyətləri.

İZR-nin BH-nə bəzi tuşlama xüsusiyyətlərini qeyd etmək lazımdır:

1. AH-dən fərqli olaraq, kiçik EƏS səbəbindən BH-dən əksolunan siqnalın alınmasının çətinliyi.
2. Atmosferdə hərəkət edən zaman tuşlamanı çətinləşdirən böyük yüklənmələr.
3. Faza vektoru qiymətlərinin alınmasının çətinliyi.
4. Zəruri olan keçid kompleksləşdirmə rejimi ilə RLS və ÖYB-dən gələn verilənlərin BH-ni tutma çətinliyi.
5. AH-nin tutulması zamanı yönəlmə vaxtının kiçik olması (bu vaxt nə qədər az olsa yayınma qiyməti də o qədər artar) BH tutulması üçün yönəltmə vaxtının 1,5 – maksimum 2 saniyyə çərçivəsində saxlanmasına tövsiyyə olunur.
6. 10 Hs aşağı göstəricidə olan koordinatların dəyişməsi tezliyi. Onun 20 Hs göstəricisinə yüksəldilməklə kəskin aşağı enmənsini təmin edir.

Nəticə

Məqalədə İZR-nin yüksəksürətli ballistik hədəflərə yönəldilməsinin əsas prinsiplərinə baxılmış və Kalman süzgəcinin radiolokasiya stansiyasında məlumatların emalı üçün ən uyğun süzgəc olduğu müəyyən edilmişdir. RLS məlumatlarının Kalman süzgəci vasitəsilə emalının modelləşdirilməsi aparılmışdır. O cümlədən raketin ballistik və aerodinamik hədəflərə yönəldilməsinin modelləşdirilməsi həyata keçirilmişdir. Nəticə olaraq avtomatik idarəetmə sisteminin iki məsələsinə baxılmışdır:

– obyektin trayektoriya parametrlərinin müəyyən edilməsi;
– obyektə doğru İZR-nin yönəldilməsi (tuşlanması).

Birinci məsələnin həlli zamanı ballistika əmsalı və hədəfin xüsusiyyətlərinin obyektiv qiymətləndirilməsi yolu ilə yalançı hədəflərin seleksiyası modelləşdirilmişdir.

Modelləşdirmənin nəticələrinə əsaslanaraq, aerodinamik hədəflərin tutulması zamanı özüyönələn başlıqla raketin müşayiət vaxtının 5-7 saniyəyə qədər uzadılması və radiolokasiya stansiyasının hədəfi müşayiət edən siqnal tezliyinin 20 Hs-ə qədər artırılması imkanlarının nəzərdən keçirilməsi təklif olunur.

İstifadə edilmiş ədəbiyyat siyahısı

1. İsayev, Y.S., Aydemir, M.E., İsayev, Ə.M. Radar Cross Section identification of air targets using the cosine transform and neural networks // – Bakı: Milli təhlükəsizlik və Hərbi elmlər, – 2016. №1 (2). – s. 43- 48.
2. İsayev, Y.S. Hərbi təyinatlı radiotexniki sistemlərin əsas taktiki xarakteristikaları haqqında // – Bakı: Milli Təhlükəsizlik və Hərbi Elmlər, – 2019. № 3(5). – s. 11-18.
3. Barton, D. K., Radar system analysis and modeling / D. K. Barton – Boston, London: Artech House, – 2004. – 545 p.
4. Blackman, S. S. Design and analisys of modern tracking systems / S. S. Blackman. – London: Artech House, – 1999. – 1185 p.
5. Шахтарин, Б.И. Фильтры Винера и Калмана. Учебник для вузов / Б.И. Шахтарин – Москва: Горячая линия –Телеком, – 2014. – 396 с.
6. Бартон, Д. К., Справочник по радиолокационным измерениям / Д.К.Бартон, Г.Р.Вард. – Пер. с англ. под ред. М. М. Вейсбейна. – Москва: Советское радио, – 1976. – 392 с.
7. Вторая научно-техническая конференция молодых ученых и специалистов. 2011. Сборник докладов / Под ред. Созинова П.А. – Москва: Радиотехника – 2012. – 392 с.
8. Демидов, В. П., Кутыев, Н. Ш. Управление зенитными ракетами. 2-е изд., перераб. и доп. – Москва: Воениздат – 1989. – 335 с.
9. Косарев, В. И. 12 лекций по вычислительной математике (вводный курс): Учеб. пособие: Для вузов. Изд. 2-е, испр. и доп. – Москва: Изд-во МФТИ, – 2000 – 204 с.

Аннотация

Наведение зенитных управляемых ракет на скоростные баллистические цели

Байрам Ибрагимов, Ялчин Исаев, Эльдар Алиев, Ахад Исаев

В статье на примере возможностей оперативно-тактических ракетных комплексов, входящих в класс «Искандер», рассмотрены основные особенности их направления по высокоскоростным баллистическим целям. Кроме того, были рассмотрены рекуррентный алгоритм статистической обработки определения координат баллистического объекта на основе фильтра Калмана, оценка точности определения положения ракеты в пространстве, составляющих скорости и баллистического коэффициента. Целью научно-исследовательской работы является моделирование обработки данных РЛС средствами фильтра Калмана, включая моделирование баллистического и аэродинамического наведения ракеты. Для достижения цели были поставлены следующие задачи: Определение уравнения движения центра тяжести баллистической цели в атмосфере Земли; оценка модели ошибок радиолокационной станции сопровождения баллистической цели; оценка вероятности поражения баллистической цели; Проведение доклада координаты места встречи управляемой зенитной ракеты с баллистической целью; Оценка вероятности поражения баллистической цели. Для решения задач используются следующие методы исследования: теоретический анализ, математическое моделирование, математическая статистика. В результате исследовательской работы: определено, что фильтр Калмана является оптимальным фильтром для обработки данных на радиолокационной станции. Выбор ложных целей моделировался посредством объективной оценки характеристик цели с помощью баллистического коэффициента. По результатам моделирования предлагалось увеличить время сопровождения ракеты до 5-7 секунд и увеличить частоту сигнала радиолокационной станции до 20 Гц при захвате аэродинамических целей.

Ключевые слова: радиолокационная станция, баллистическая цель, аэродинамическая цель, зенитная управляемая ракета, самонаводящаяся боевая часть, программно-алгоритмическое обеспечение, противовоздушная оборона, локальная местная система координат, многоцелевая радиолокационная станция, эффективная площадь отражения, среднеквадратическая ошибка, двигательная установка, баллистический коэффициент, боевая часть

Abstract

Guiding anti-aircraft guided missiles at high-speed ballistic targets

Bayram Ibragimov, Yalchin Isaev, Eldar Aliyev, Ahad Isaev

Using the example of the capabilities of operational-tactical missile systems included in the Iskander class, the article examines the main features of their direction against high-speed ballistic targets. In addition, a recurrent algorithm for statistical processing of determining the coordinates of a ballistic object based on the Kalman filter, an assessment of the accuracy of determining the position of the missile in space, components of velocity and ballistic coefficient were considered. The purpose of the research work is to simulate the processing of radar data using the Kalman filter, including the simulation of ballistic and aerodynamic missile guidance. To achieve the goal, the following tasks were set: Determination of the equation of motion of the center of gravity of a ballistic target in the Earth's atmosphere; assessment of the error model of a ballistic target tracking radar; assessing the probability of hitting a ballistic target; Conducting a report on the coordinates of the meeting point of a guided anti-aircraft missile with a ballistic target; Estimation of the probability of hitting a ballistic target. To solve problems, the following research methods are used: theoretical analysis, mathematical modeling, mathematical statistics. As a result of the research work it was determined that the Kalman filter is the optimal filter for data processing at a radar station. The selection of decoys was modeled by objectively assessing target characteristics using a ballistic coefficient. Based on the modeling results, it was proposed to increase the missile tracking time to 5-7 seconds and increase the frequency of the radar signal to 20 Hz when capturing aerodynamic targets.

Keywords: ballistic target, aerodynamic target, self-directed warhead, software and algorithmic support, local coordinate system, multi-purpose radar station, effective reflection area, mean square error, propulsion system, warhead

Məqalə redaksiyaya daxil olmuşdur: 08.01.2024
Təkrar işlənməyə göndərilmişdir: 15.01.2024
Çapa qəbul edilmişdir: 12.03.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 106-115
MİLLİ TƏHLÜKƏSİZLİK ***NATIONAL SECURITY***

UOT 355/359 DOI: 10.30546/9878.2024.2.10.0032.

İNFORMASİYA MÜHARİBƏSİ VƏ MİLLİ TƏHLÜKƏSİZLİK

polkovnik-leytenant Rəşadət Orucov
Milli Müdafiə Universitetinin Hərbi Elmi Tədqiqat İnstitutu
orujovrashadat@gmail.com

Xülasə. Məqalədə informasiya müharibəsinin milli təhlükəsizlikdə rolu və milli təhlükəsizliyə təsiri, informasiya müharibəsinə konseptual baxış, eləcə də informasiya müharibəsinə qarşı mübarizə strategiya nümunələri öz əksini tapır. Münaqişələrdə üstünlük əldə etmək və ya strateji məqsədlərə nail olmaq üçün informasiya və kommunikasiya texnologiyalarından istifadənin əhəmiyyəti, strateji kommunikasiya sistemlərinin fəaliyyətinə və nəticələrə mənfi təsir göstərmək üçün məlumatın manipulyasiyası, istismarı və yayılması kimi məsələlərə toxunulur. O cümlədən informasiya üstünlüyü uğrunda mübarizənin milli təhlükəsizlik kontekstində həlledici rol oynadığı izah edilir. Tədqiqatın məqsədi vətəndaşlar arasında media və rəqəmsal savadlılığı və tənqidi düşüncənin artırılması, fərdlərdə yanlış məlumatı müəyyən və ayırd etmək bacarığının formalaşdırılmasıdır. Bu çərçivədə təhsil proqramları fərdlərə mənbələri qiymətləndirməyə, məlumatı və faktları yoxlamağa, məzmunu tənqidi təhlil etməyi öyrənməyə imkan verir. Məqalədə həmçinin dövlətlərin və beynəlxalq təşkilatların informasiya müharibəsi ilə kollektiv mübarizədə normalar, qanunlar və vahid çərçivələrin yaradılması üçün kəşfiyyat məlumatlarının mübadiləsi, kiberhücumlara cavab tədbirlərinin əlaqələndirilməsi və informasiya məkanında məsuliyyətli davranışın təşviqi sahəsində əməkdaşlığından bəhs edilir.

Açar sözlər: strateji kommunikasiya, milli təhlükəsizlik, informasiya müharibəsi, kommunikasiya texnologiyaları, məlumat mübadiləsi

Giriş

Son illər informasiya müharibəsinin milli təhlükəsizliyin təmin olunması istiqamətində ciddi problemlərə gətirib çıxardığının şahidi oluruq. Müasir rəqəmsal əsrdə məlumatın manipulyasiyası və mənfi yönümlü istifadəsi xalqların sabitliyi və təhlükəsizliyinə əhəmiyyətli dərəcədə təsir göstərmə gücünə malikdir. Bu məqalə informasiya müharibəsi anlayışını və onun milli təhlükəsizliyə təsirini işıqlandırmaq məqsədi daşıyır. Məqalədə, həmçinin informasiya müharibəsinə qarşı mübarizə strategiyaları araşdırılır və onun təzahürlərini əks etdirən real dünya nümunələri öz əksini tapır.

İnformasiya müharibəsi münaqişələrdə üstünlük əldə etmək və ya strateji məqsədlərə nail olmaq üçün informasiya və kommunikasiya texnologiyalarından istifadə edən bir sıra fəaliyyətləri əhatə edir. O, qavrayışları formalaşdırmaq, strateji kommunikasiya sistemlərinin fəaliyyətinə mənfi təsir göstərmək və nəticələrə təsir etmək üçün məlumatın manipulyasiyası, istismarı və yayılmasını ehtiva edir. Dünyada baş verən hadisələr fonunda informasiya üstünlüyü uğrunda mübarizə milli təhlükəsizlik kontekstində həlledici rol oynayır.

İnformasiya müharibəsinin milli təhlükəsizliyə təsiri geniş və çoxşaxəlidir. O, siyasi fəaliyyətlərə və demokratik proseslərə informasiya sisteminin boşluqlarından istifadə edilməklə mənfi təsir göstərə bilər. İctimai rəyin manipulyasiyası, yalan məlumatların yayılması və dövlət qurumlarına inamın azalmasını informasiya müharibəsinin nəticəsi hesab etmək olar. İnformasiya müharibəsinə qarşı mübarizə və milli təhlükəsizlik maraqlarının qorunması ilə bağlı effektiv strategiyaların hazırlanması üçün bu təsirləri dərk etmək və onların həlli yollarını müəyyənləşdirmək zəruridir.

İnformasiya müharibəsinə qarşı mübarizə fəal tədbirləri, müdafiə mexanizmlərini və birgə səyləri özündə birləşdirən hərtərəfli yanaşmanı əks etdirməlidir. İnformasiya müharibəsinə qarşı mübarizə strategiyalarına kritik infrastrukturun qorunması üçün kibertəhlükəsizlik tədbirlərinin gücləndirilməsi, fərdlərin media savadlılığının və rəqəmsal vətəndaşlıq təhsilinin təşviqi, norma və çərçivələrin yaradılmasında beynəlxalq əməkdaşlığa sövq edilməsi, effektiv əks-təbliğat və strateji kommunikasiyanın inkişaf etdirilməsi daxildir. Bu strategiyalar informasiya müharibəsinin risk və

təsirlərini azaltmaq, milli təhlükəsizlik maraqlarını və informasiya ekosisteminin bütövlüyünü qorumaq məqsədini daşıyır.

Qeyd etmək lazımdır ki, dünyada baş vermiş hadisələr fonunda informasiya müharibəsində tətbiq edilən taktikaların və xalqların üzləşdiyi nəticələrə dair konkret nümunələrin öyrənilməsi mühümdür. Belə ki, Rusiyanın 2016-cı il ABŞ prezident seçkilərinə müdaxiləsi, kritik infrastruktura kiberhücumlar, İraq–Şam İslam Dövlətinin (İŞİD) təbliğatı və terror təşkilatına cəlbetmə, seçkilərdə dezinformasiya kampaniyaları kimi bariz nümunələr informasiya müharibəsinin müxtəlif təzahürlərini nümayiş etdirir. Bu nümunələri araşdırmaqla siyasətçilər, təhlükəsizlik mütəxəssisləri və tədqiqatçılar informasiya müharibəsi ilə mübarizədə mürəkkəb vəziyyəti və yaranan problemlərin həlli yollarını tapmağa kömək edə bilər.

Nəticə etibarilə, informasiya müharibəsi qloballaşan dünyada milli təhlükəsizliyə ciddi problemlər yaradır. Onun konseptual əsaslarını dərk etmək, təsirini qiymətləndirmək, onunla mübarizə aparmaq üçün effektiv strategiyaların işlənib hazırlanması və bu istiqamətdə dünyada baş vermiş hadisələrin araşdırılması milli təhlükəsizlik maraqlarının qorunmasında mühüm əhəmiyyət kəsb edir. Dövlət və ona bağlı qurumlar informasiya müharibəsinin manipulyativ və istismarçı aspektlərini aradan qaldırmaqla, proaktiv tədbirlər hazırlaya, kibertəhlükəsizliyi inkişaf etdirə, media savadlılığını təşviq edə, beynəlxalq əməkdaşlığı inkişaf etdirə və milli təhlükəsizliyin qorunması və informasiya ekosistemlərinin bütövlüyünün qorunması məqsədilə effektiv əks-tədbirlər həyata keçirə bilər.

İnformasiya müharibəsinə konseptual baxış

İnformasiya müharibəsi milli təhlükəsizliyi formalaşdıran müasir münaqişələrin mühüm aspekti kimi meydana gəlmişdir. Texnoloji tərəqqi və qarşılıqlı əlaqə ilə müəyyən edilən bir dövrdə informasiya üstünlüyü uğrunda mübarizə həlledici xarakter almışdır. Bu bölmədə informasiya müharibəsinə konseptual baxış, onun təbiəti, məqsədləri, dövlət və qeyri-dövlət subyektləri tərəfindən istifadə olunan strategiyalar araşdırılır.

İnformasiya müharibəsi münaqişələrdə üstünlük əldə etmək və ya strateji məqsədlərə nail olmaq üçün informasiya və kommunikasiya texnologiyalarından istifadəni ehtiva edir. O, qavrayışlara təsir etmək, kommunikasiya sistemlərinin fəaliyyətinə zərər vurmaq və nəticələri formalaşdırmaq üçün məlumatın manipulyasiyası, istismarı və yayılmasını əhatə edir. İnformasiya müharibəsindən qarşı tərəfi aldatma, inandırma və ya pozucu fəaliyyət vasitəsi kimi istifadə edilir. Bundan əlavə, informasiya müharibəsi taktiki, əməliyyat və ya strateji məqsədlərə nail olmaq üçün informasiyanın və onunla əlaqəli texnologiyaların istifadəsi kimi də qəbul edilə bilər. Bu, kiberhücumlar, psixoloji əməliyyatlar, təbliğatın yayılması, dezinformasiya kampaniyaları və sosial mühəndislik daxil olmaqla, geniş fəaliyyət spektrini əhatə edir [1].

İnformasiya müharibəsi cəlb olunan aktorların motivasiya və niyyətindən asılı olaraq, bir sıra məqsədlərə xidmət edir. Bu məqsədlərə aşağıdakılar aid edilə bilər:

– təsir və inandırma. İnformasiya müharibəsi təbliğat, dezinformasiya və ya məlumatların məqsədli yayılması yolu ilə ictimai rəyi formalaşdırmaq, qərar qəbuletmə proseslərinə təsir etmək və qavrayışları dəyişdirmək məqsədini daşıyır. Aktorlar ictimai əhval-ruhiyyəyə təsir etməklə, öz məqsədlərinə dəstək əldə etməyə, düşmənləri gözdən salmağa və ya öz hərəkətlərinə haqq qazandırmağa çalışırlar;

– təhlükə və inkar. İnformasiya müharibəsi informasiya sistemləri, şəbəkələri və ya kritik infrastrukturun fəaliyyətinə zərər vurmaq və ya onu məhdudlaşdırmaq üçün istifadə edilə bilər. Kiberhücumlar, informasiya manipulyasiyası və ya yalan məlumatların yayılması məlumatın bütövlüyünü pozmaq, onun etibarlılığına zərər vurmaq və çaşqınlıq yaratmaq, xaosla və ya dövlət qurumlarına inamın itirilməsi ilə nəticələnə bilər;

– casusluq və kəşfiyyat məlumatlarının toplanması. İnformasiya müharibəsi kibercasusluq, müşahidə və ya sosial mühəndislik vasitəsilə həssas və ya məxfi məlumatların toplanmasını əhatə edə bilər. Bu məlumatlar strateji üstünlük, kəşfiyyat məqsədləri və ya rəqiblərin imkanları və niyyətləri barədə məlumat toplamaq məqsədilə istifadə edilə bilər [2];

– psixoloji əməliyyatlar. Əhalinin rəftarı, inancı və davranışlarına təsir etmək məqsədini daşıyır. Təbliğat, aldatma və ya qavrayış idarəçiliyi kimi taktikalardan istifadə etməklə, informasiya müharibəsi çaşqınlıq yaradır, düşmənləri ruhdan salır və ya əməliyyatları həyata keçirən aktorun maraqlarına üstünlük vermək üçün rəy formalaşdırır [3].

İnformasiya müharibəsi informasiya sistemləri və şəbəkələrindəki boşluqlardan istifadə etməklə, bir çox yanaşmaları özündə əks etdirir. Bəzi ümumi yanaşmaları aşağıdakı kimi qruplaşdırmaq olar:

– kiberhücumlar – məlumat sistemlərini, şəbəkələri və ya kritik infrastrukturun fəaliyyətini dayandırmaq və ya məhdudlaşdırmaq üçün zərərli proqramların, hakerlərin və ya xidmətdən imtina hücumlarının (DDOS) istifadəsini əhatə edir. Kiberhücumçular (hakerlər) icazəsiz giriş əldə etmək, məlumatları oğurlamaq, əməliyyatları məhdudlaşdırmaq və ya ziyan vurmaq üçün texnologiyanın zəif tərəflərindən istifadə edir [4].

– dezinformasiya və təbliğat. Dezinformasiya kampaniyaları hədəf auditoriyasını aldatmaq üçün bilərəkdən yalan və ya yanlış məlumat yaymaq məqsədini daşıyır. Burada təbliğat qavrayışlarını formalaşdırmaq, ictimai rəyi manipulyasiya etmək və ya müəyyən səbəb və ya ideologiyaya dəstək vermək üçün qərəzli, yaxud seçmə məlumatların yayılması nəzərdə tutulur.

– sosial mühəndislik. Bu taktika etibardan sui-istifadə etmək, həssas məlumatları oğurlamaq, sistemlərə və ya şəbəkələrə icazəsiz giriş əldə etmək üçün insan psixologiyasının manipulyasiyasını nəzərdə tutur. Fiziki və hüquqi şəxsləri aldatmaq məqsədilə, adətən, "fişinq" kimi üsuldan istifadə edilir [5].

– qavrayışın idarə edilməsi – ictimai rəyə təsir etmək üçün məlumatların və rəylərin formalaşdırılmasını və məlumat axınına nəzarəti əhatə edir. Media manipulyasiyası, strateji mesajlaşma və ya rəylərin idarə edilməsi, eyni zamanda məlumatın yayılmasını istiqamətləndirmək üçün sosial media platformalarından istifadə etməklə həyata keçirilə bilər [6].

İnformasiya müharibəsi təsir və çətinlikləri özündə ehtiva edir. Bu təsir və çətinliklərə aşağıdakılar şamil edilə bilər:

– sürətli texnoloji tərəqqi. Texnologiyanın daim inkişaf edən təbiəti potensial təhlükələri qabaqlamaqda bir çox çətinliklər yaradır. İnformasiya müharibəsi ilə məşğul olan aktorlar davamlı olaraq, ayıq-sayıq olmalı və yeni texnologiyalardan istifadə etməklə, onları öz fəaliyyət tərzlərinə uyğunlaşdırmalıdır;

– sahələrarası təsir. İnformasiya müharibəsi siyasi, iqtisadi və sosial sahələrdə fəaliyyət göstərir. O, ənənəvi hərbi arenalardan kənara çıxaraq ictimai rəy, iqtisadi sabitlik, sosial birlik və siyasi proseslərə təsir edə bilər. Bu sahələrarası təsirləri qavramaq və problemləri həll etmək milli təhlükəsizlik istiqamətində cavab tədbirləri üçün vacibdir;

– tanınma problemləri. İnformasiya müharibəsi fəaliyyətinin mənbəyini müəyyən etmək mühüm problemdir. Çətin aktorlar tez-tez gizli şəkildə "bot" şəbəkələrindən istifadə edir və ya müəyyən dərəcədə anonimliyi təmin edən vasitələrlə öz həqiqi şəxsiyyətini maskalamaq üçün bir çox yanaşmalardan istifadə edir. Bu isə hücumların dəqiq mənbəyini müəyyən etməyi və onlara qarşı müvafiq cavab tədbirlərini çətinləşdirir;

– inkişaf etməkdə olan tənzimləyici çərçivələr. İnformasiya müharibəsinin sürətlə artması möhkəm hüquqi və tənzimləyici çərçivələrin işlənib hazırlanmasını tələb edir. Kiberməkanı idarə etmək, informasiya texnologiyalarından yanlış məqsədlər üçün istifadə olunması ilə mübarizə məqsədilə norma, qayda və protokolların yaradılmasında beynəlxalq əməkdaşlıq həyati əhəmiyyət kəsb edir. İnformasiya müharibəsinin inkişaf edən təbiəti hüquqi bazaların təkmilləşdirilməsi və gücləndirilməsi üçün davamlı olaraq, səylər tələb edir [7].

Yuxarıda qeyd edilən məqamlara əsasən milli təhlükəsizlik kontekstində informasiya müharibəsinin mürəkkəb və çoxşaxəli sahədə yayılmasını qeyd etmək olar. Onun konseptual əsaslarını anlamaq effektiv cavab tədbirlərinin görülməsində və müdafiə fəaliyyətlərinin həyata keçirməsində önəmlidir. Göründüyü kimi, informasiya texnologiyaları inkişaf etdikcə informasiya müharibəsində istifadə olunan taktika və strategiyalar da inkişaf edəcəkdir. İnformasiya müharibəsinin məqsədlərini, strategiyalarını və nəticələrini dərk etməklə, dövlət və ona bağlı olan qurumlar, o cümlədən təşkilatlar

milli təhlükəsizlik maraqlarını qorumaq üçün fəal tədbirlər hazırlaya bilər. Əməkdaşlıq, texnoloji tərəqqi, beynəlxalq əməkdaşlıq və möhkəm hüquqi bazaların inkişafı informasiya müharibəsinə qarşı mübarizədə, eləcə də rəqəmsal əsrdə dövlətin təhlükəsizliyi və sabitliyinin təmin edilməsi üçün vacibdir.

İnformasiya müharibəsinin milli təhlükəsizliyə təsiri

Rəqəmsal əsrdə informasiya müharibəsi milli təhlükəsizlik üçün əhəmiyyətli problem kimi ortaya çıxmışdır. Qloballaşan dünyada informasiya üstünlüyü uğrunda mübarizə dövlətlərin təhlükəsizliyi və sabitliyi üçün vacib amildir. Bu məqalə informasiya müharibəsinin milli təhlükəsizlik fonunda siyasi, iqtisadi, sosial və digər sahələrə təsirlərini tədqiq edir.

Siyasi təsir. İnformasiya müharibəsi güc, idarəetmə və beynəlxalq münasibətlərin dinamikasına təsir edə bilir. Bu təsirlərə aiddir:

– seçkilərə müdaxilə. Rəqib aktorlar seçki proseslərinə müdaxilə etmək üçün informasiya müharibəsi taktikalarından məharətlə istifadə edir. Onlar dezinformasiya yaymaq, kiberhücumlar həyata keçirmək və ya ictimaiyyətə təsir kampaniyaları vasitəsilə ictimai rəyi formalaşdırmaq, demokratik proseslərə inamı sarsıtmaq və seçkilərin nəticələrini manipulyasiya etmək kimi fəaliyyətləri həyata keçirir;

– dövlətin sabitliyinin pozulması. İnformasiya müharibəsi nifaq salmaq, sosial iğtişaşları qızışdırmaq və ya ictimai etimadı pozmaq kimi fəaliyyətlərlə dövlətin sabitliyinə xələl gətirə bilər. Məlumatların manipulyasiyası mövcud ictimai parçalanmalardan istifadə edə, dövlətin legitimliyini zəiflədə və siyasi qarışıqlıq yarada bilər;

– siyasi proseslərə təsir. İnformasiya müharibəsi siyasi proseslərə təsir göstərə bilər. Aktorlar ictimai rəyi manipulyasiya etməklə gündəmi formalaşdıra, siyasi qərarları idarə edə və effektiv idarəçiliyə mane ola bilər. Yanlış məlumat və təbliğat kampaniyaları ictimai əhval-ruhiyyəni dəyişdirə, yanlış qərarların qəbul edilməsinə səbəb ola bilər [8].

İqtisadi təsir. İnformasiya müharibəsi sənaye, maliyyə sistemləri və iqtisadi sabitliyə təsir edən iqtisadi problemlər yaradır. Bu təsirlərə aşağıdakılar aid edilə bilər:

– kritik infrastruktura qarşı fəaliyyətlər. Elektrik şəbəkələri, nəqliyyat sistemləri və ya kommunikasiya şəbəkələri kimi kritik infrastrukturu hədəfə alan kiberhücumlar iqtisadi təsirlərə səbəb ola bilər. Potensial nəticələrə maliyyə itkilərini və ictimai təhlükəsizliyin pozulmasını aid etmək olar;

– əqli mülkiyyət oğurluğu. İnformasiya müharibəsi əqli mülkiyyət oğurluğuna, innovasiyalara və iqtisadi rəqabət qabiliyyətinə təhlükə yarada bilər. Dövlət tərəfindən maliyyələşdirilən aktorlar və ya kibercinayətkarlar əqli mülkiyyətə, ticarət, tədqiqat və sənaye sirlərinə, həmçinin inkişafedici məlumatlara icazəsiz giriş əldə etmək üçün biznesləri, tədqiqat institutlarını və ya dövlət qurumlarını hədəfə alır [9];

– maliyyə bazarının manipulyasiyası. Yanlış məlumatların yayılması və ya maliyyə sistemlərinə koordinasiyalı şəkildə hücumların həyata keçirilməsi kimi informasiya müharibəsi taktikaları bazar sabitliyini və investorların inamını sarsıda, dəyişkənlik, iqtisadi itki və maliyyə institutlarına olan inamın azalmasına səbəb ola bilər [10; 90].

Sosial təsir. İnformasiya müharibəsi ictimai əhval-ruhiyyəyə, cəmiyyətin birliyi və fərdi davranışa təsir edən əhəmiyyətli sosial təsirlərə malikdir. Müəyyən əsas təsirlərə aşağıdakılar daxildir:

– ictimai rəyin manipulyasiyası. İnformasiya müharibəsi dezinformasiya, təbliğat yaymaq və ya məlumatlara təsir etməklə ictimai rəyi manipulyasiya edə bilər. Bu, cəmiyyətlərin qütbləşməsinə, sosial bölünmələrin artmasına, institutlara və mediaya olan inamın azalmasına səbəb ola bilər;

– sosial media platformalarının istismarı. Sosial media platformaları informasiya müharibəsi fəaliyyətləri üçün əlverişli şəraitə çevrilmişdir. Rəqib aktorlar bu platformalardan yanlış məlumat yaymaq, ictimai müzakirələri manipulyasiya etmək və mövcud ictimai disbalansın pozulmasını artırmaq məqsədilə istifadə edir ki, bu da cəmiyyətdə iğtişaşlara və gərginliyə gətirib çıxarır;

– məxfilik və şəxsi təhlükəsizliyə təhdidlər. İnformasiya müharibəsi şəxslərin məxfiliyini poza və şəxsi təhlükəsizliyinə zərər vura bilər. Kiberhücumlar şəxsi məlumatların oğurlanması və ya yayılması, nüfuza xələl gəlməsi, maliyyə itkisi, hətta fiziki zərərlə nəticələnə bilər [10, s.103-107].

Digər sahələrə aid təsirlər. İnformasiya müharibəsinin milli təhlükəsizliyə təsiri geniş yer alır. O, dövlət sistemlərinə, hərbi əməliyyatlara və kəşfiyyat orqanlarının bütövlüyünə zərər vura bilər. Bu istiqamətdə bəzi əsas təsirlərə aşağıdakılar aid edilir:

– müdafiə sistemlərinin zəiflədilməsi. İnformasiya müharibəsi hərbi şəbəkələri hədəf alaraq, məxfi məlumatları əldə edə, komandanlıq və idarəetmə imkanlarına zərər vuraraq, müdafiə sistemlərinin fəaliyyətini sarsıda bilər. Beləliklə, bir dövlətin təhlükəsizlik təhdidlərinə effektiv cavab vermək qabiliyyətinə maneə yarada bilər.

– hibrid müharibə. İnformasiya müharibəsi çox vaxt ənənəvi hərbi taktikaları qeyri-hərbi üsullarla birləşdirilərək, hibrid müharibə strategiyalarının bir hissəsi kimi istifadə olunur. Hibrid müharibə fonunda hərbi və qeyri-hərbi sahələrin mürəkkəb qarşılıqlı fəaliyyəti milli təhlükəsizliyə öz təsirini göstərir [11].

– kritik milli infrastruktur üçün təhdidlər. İnformasiya müharibəsi elektrik şəbəkələri, nəqliyyat şəbəkələri və rabitə sistemləri də daxil olmaqla, kritik milli infrastruktur üçün əhəmiyyətli risklər yaradır. Sistemlərin fəaliyyətlərinin məhdudlaşdırılması və ya pozulması milli və ictimai təhlükəsizliyə, həmçinin iqtisadi sabitliyə ardıcıl təsir göstərir [4].

İnformasiya müharibəsi milli təhlükəsizlik fonunda siyasi, iqtisadi, sosial və digər sahələrə təsir edir, idarəetmə, demokratik proseslər, iqtisadi sabitlik, cəmiyyətin birliyi və hərbi hazırlıq üçün potensial problemlər yaradır [12]. Bu təsirləri nəzərə alaraq, milli təhlükəsizlik maraqlarını qorumaq üçün effektiv strategiyalar və əks-tədbirlər planı işlənib hazırlanmalıdır. Dövlətlərarası və beynəlxalq əməkdaşlıq, kibertəhlükəsizliyin təkmilləşdirilməsi, media savadlılığı proqramları, təkmilləşdirilmiş qanunvericilik bazaları informasiya müharibəsi təhdidləri qarşısında risklərin azaldılması, xalqların təhlükəsizliyinin təmin edilməsi və sabitliyin qorunub saxlanması üçün vacibdir.

İnformasiya müharibəsinə qarşı mübarizə strategiyaları

Rəqəmsal dünyada informasiya hökmranlığı uğrunda gedən mübarizənin milli təhlükəsizliyə təsirləri danılmazdır. İnformasiya müharibəsinin geniş vüsət alması məlumatların manipulyasiyası, yayılması və istismarına qarşı effektiv strategiyalara ehtiyac olduğunu göstərir. Bu bölmədə proaktiv tədbirləri, müdafiə mexanizmlərini və birgə səyləri əhatə edən informasiya müharibəsinə qarşı mübarizə üçün bir-biri ilə sıx əlaqəli bir sıra strategiyalar tədqiq olunur.

Maarifləndirmə və təhsil. Maarifləndirmə və təhsilin təşviqi informasiya müharibəsinə qarşı mübarizə üçün mühüm strategiyadır. Vətəndaşlar arasında media savadlılığı, tənqidi düşüncə və rəqəmsal savadlılığın artırılması nəticəsində fərdlər yalan və ya yanlış məlumatı müəyyən və ayırd etmək üçün daha məlumatlı olur. Təhsil proqramları fərdlərə mənbələri necə qiymətləndirməyi, məlumatı, faktları yoxlamağı və məzmunu tənqidi təhlil etməyi öyrənməyə imkan verir. Dövlət, təhsil müəssisələri və vətəndaş cəmiyyəti təşkilatları media savadlılığının təşviqi üçün resurs və kampaniyaların təmin edilməsində mühüm rol oynayır. Bundan əlavə, media savadlılığının və rəqəmsal vətəndaşlıq təhsilinin təşviqi informasiya müharibəsinə qarşı mübarizədə uzunmüddətli strategiya hesab edilir. Bu təhsil təşəbbüsləri tənqidi düşünmə bacarıqları, media savadlılığı və etik "onlayn" davranışı inkişaf etdirmək üçün müxtəlif yaş qruplarını hədəf alaraq, tədris müəssisələrinin kurikulumlarına inteqrasiya edilməlidir. Media savadlılığı proqramları fərdlərə etibarlı mənbələri necə müəyyən etməyi, məlumatı düzgün qiymətləndirməyi, manipulyasiya üsullarını aşkarlamağı və rəqəmsal platformalarda məsuliyyətlə naviqasiya etməyi öyrədir. Bu, fərdlərə informasiyanın məlumatlı istehlakçısı və informasiya müharibəsinə qarşı mübarizədə fəal iştirakçı olmaq imkanını verir.

Əməkdaşlıq və tərəfdaşlıq. İnformasiya müharibəsi beynəlxalq əməkdaşlıq və koordinasiya tələb edən transmilli çağırışdır. Dövlətlər və beynəlxalq təşkilatlar informasiya müharibəsi ilə kollektiv şəkildə mübarizədə normalar, qanunlar və vahid çərçivələrin yaradılması üçün kəşfiyyat məlumatlarının mübadiləsi, kiberhücumlara cavab tədbirlərinin əlaqələndirilməsi, informasiya məkanında məsuliyyətli davranışın təşviqi sahəsində əməkdaşlıq etməlidir. İnformasiya müharibəsinə qarşı mübarizədə beynəlxalq əməkdaşlığı inkişaf etdirmək üçün dialoq və əməkdaşlıq platformaları yaradılmalıdır. Bundan əlavə, informasiya müharibəsinə qarşı mübarizədə dövlətlər, kəşfiyyat agentlikləri, texnologiya

şirkətləri, vətəndaş cəmiyyəti təşkilatları arasında əməkdaşlıq və tərəfdaşlığın olması zəruridir. Bu tərəfdaşlıqlar məlumat mübadiləsi, səylərin əlaqələndirilməsi və informasiya müharibəsi təhdidlərinə birgə cavab tədbirlərini özündə cəmləşdirir. Əməkdaşlıq təşəbbüsləri kəşfiyyat xarakterli məlumatların paylanılması, birgə araşdırmaların aparılması, texnoloji həllərin işlənib hazırlanması və informasiya müharibəsini kollektiv şəkildə həll etmək üçün siyasət çərçivələrinin həyata keçirilməsini əhatə edə bilər.

Kibertəhlükəsizlik tədbirlərinin gücləndirilməsi. İnformasiya müharibəsinə qarşı mübarizədə əsas strategiyalardan biri sayılır. Qabaqcıl şifrləmə üsullarının, güclü audentifikasiya protokollarının, müdaxilənin aşkarlanması sistemlərinin və təhlükəsizlik auditlərinin tətbiqi kimi gücləndirilmiş kibertəhlükəsizlik tədbirləri informasiya sistemləri, şəbəkələri və kritik infrastrukturu kiberhücumlardan qoruyur. Müntəzəm qiymətləndirmələr və monitorinq sistemi zəif tərəfləri müəyyən etməyə və riskləri azaltmağa kömək edir. Dövlətlər, özəl sektor və beynəlxalq təşkilatlar arasında əməkdaşlıq kibertəhlükəsizlik sahəsində mükəmməl təcrübələrin işlənib hazırlanması və icrasında mühüm əhəmiyyət kəsb edir.

Əks-təbliğat və strateji ünsiyyət. Dezinformasiya, təbliğat və manipulyasiyaya qarşı proaktiv kommunikasiya strategiyalarının işlənib hazırlanması informasiya müharibəsinə qarşı mübarizədə çox vacibdir. Effektiv əks-təbliğat yalan məlumatların aşkarlanması, doğru məlumatın təbliği və manipulyasiya üsullarını ifşa etməyi özündə birləşdirir. Dövlətlər və təşkilatlar şəffaf və etibarlı kommunikasiya kanalları vasitəsilə ənənəvi və rəqəmsal media platformalarından istifadə edərək, düzgün məlumat vermək və problemləri operativ şəkildə həll etmək üçün ictimaiyyətlə əlaqə saxlamalıdır. İnformasiya müharibəsinin təsirlərinə qarşı mübarizədə ictimai etimadın və qarşılıqlı əlaqənin yaradılması vacibdir.

Tədqiqat və inkişaf. Tədqiqat və inkişafa sərmayə qoymaq informasiya müharibəsinə qarşı mübarizədə olduqca vacibdir. Dövlətlər, özəl sektor qurumları və akademik dairələrdə yaranan təhlükələri araşdırmaq, qabaqcıl texnologiyaları inkişaf etdirmək, informasiya müharibəsi taktikalarını müəyyənləşdirmək və onlara adekvat cavab vermək üçün analitik imkanları artırmaq məqsədilə resurslar ayırmalıdır. Tədqiqat zamanı informasiya müharibəsinin təsirini aşkar və təhlil edə, həmçinin effektivliyini aşağı sala bilən vasitə və texnikalar hazırlamaq üçün süni intellekt, məlumat analitikası və maşının öyrənilməsi kimi sahələrə diqqət yetirilməlidir.

Qanunvericilik və siyasət çərçivələri. İnformasiya müharibəsinə qarşı mübarizə üçün dayanıqlı qanunvericilik və siyasət çərçivələrinin hazırlanması zəruridir. Qanunlar dezinformasiyanın yayılması, şəxsi həyatın toxunulmazlığının qorunması, kibercinayətkarlıq və seçkilərə müdaxilə kimi məsələlərin hüquqi bazasının olması vacibdir. Dövlətlər, həmçinin məzmunun moderasiyası, alqoritmlərdə şəffaflıq və məlumat mübadiləsi üçün təlimatlar və standartların yaradılmasında texnologiya şirkətləri ilə birgə fəaliyyət göstərilməlidir.

Beynəlxalq norma və standartlar. İnformasiya müharibəsinə qarşı mübarizədə informasiya məkanında məsuliyyətli davranış qaydaları, kritik infrastrukturu hədəf alan kiberhücumlara qarşı normalar və məlumat mübadiləsi, əməkdaşlıq haqqında sazişlərin yaradılması kimi beynəlxalq norma və standartları təşviq etmək üçün səylər göstərilməlidir. Birləşmiş Millətlər Təşkilatı (BMT) və regional qurumlar kimi beynəlxalq təşkilatlar dialoqun təşviqində, normaların işlənib hazırlanmasında və millətlərarası əməkdaşlığın asanlaşdırılmasında mühüm rol oynayır.

Davamlı monitorinq və qiymətləndirmə. Hazırlanan strategiyaları uyğunlaşdırmaq və təkmilləşdirmək üçün əks-tədbirlərin effektivliyinin monitorinqi və qiymətləndirilməsi vacibdir. Dövlətlər və təşkilatlar informasiya müharibəsi fəaliyyətlərinə nəzarət etmək, əks-tədbirlərin təsirini qiymətləndirmək və yaranan təhlükələri müəyyən etmək üçün mexanizmlər hazırlamalıdır. Müntəzəm qiymətləndirmələr strategiyaların daim inkişaf edən informasiya məkanında aktual və effektiv qalmasını təmin edir.

İnformasiya müharibəsinə qarşı mübarizə fəal tədbirləri, müdafiə mexanizmlərini və birgə səyləri birləşdirən çoxşaxəli yanaşmanı tələb edir. Yuxarıda göstərilən yanaşmalar effektiv əks-informasiya müharibəsi strategiyasının mühüm komponentləridir. Bu strategiyaları həyata keçirməklə dövlətlər,

təşkilatlar və fərdlər informasiya müharibəsinin yaratdığı riskləri azaltmaq, milli təhlükəsizlik təhdidini aradan qaldırmaq və informasiya ekosistemlərinin bütövlüyünü saxlamaq məqsədilə birgə fəaliyyət göstərə bilərlər.

Tədqiqat istiqaməti: real dünya nümunələri

İnformasiya müharibəsinin real dünya nümunələri bu fenomenin mürəkkəbliyi və milli təhlükəsizliyə təsirləri haqqında hərtərəfli fikirlərin formalaşması üçün əhəmiyyətlidir. Bu nümunələrin araşdırılması tətbiq olunan taktikaları, onların müxtəlif sahələrə təsirini və informasiya müharibəsinə qarşı mübarizədə çətinlikləri dərk etməyə kömək edir. Bu bölmədə informasiya müharibəsi ilə milli təhlükəsizliyin kəsişməsini göstərən vacib nümunələr tədqiq olunur.

1. Rusiyanın 2016-cı il ABŞ prezident seçkilərinə müdaxiləsi. Bu hal informasiya müharibəsi haqqında mühüm fikirlərin yaranmasına gətirib çıxarır. Sosial media manipulyasiyası, hakerlik və dezinformasiya kampaniyaları vasitəsilə rus aktorlar ictimai rəyə təsir etmək, nifaq salmaq və demokratik proseslərə olan inamı sarsıtmaq məqsədi güdürdülər. Yalan xəbərlərin yayılması, məqsədyönlü mesajlaşma və siyasi disbalansın gücləndirilməsi informasiya müharibəsinin seçki sistemlərinə və demokratik institutlara potensial təsiri qaçılmaz etdi [13].

2. Kritik infrastruktura kiberhücumlar. 2010-cu ildə kəşf edilən “Stuxnet” adlı kompüter qurdu kritik infrastrukturu hədəfə alan informasiya müharibəsi ilə bağlı əhəmiyyətli nümunədir. Birləşmiş Ştatlar və İsrailin birgə hazırladığı “Stuxnet” xüsusilə İranın nüvə obyektlərini hədəfə almışdı. Kompüter qurdu sənaye nəzarət sistemlərini sıradan çıxardaraq, sentrifuqlara ziyan vurmuş və İranın nüvə zənginləşdirmə imkanlarına ciddi maneə yaratmışdır. Bu nümunə araşdırıldığı zaman onun informasiya müharibəsinin kritik infrastruktura potensial təsiri və hücumların anonimliyi kimi çətinliklər ortaya çıxır [14].

3. İŞİD-in təbliğatı və terrorçuluğa cəlb edilməsi. İŞİD təbliğat kampaniyaları və sosial media platformaları vasitəsilə ekstremist ideologiyaları yaymaq, zorakılıq hərəkətlərini nümayiş etdirmək və dünyanın müxtəlif yerlərindən insanları öz sıralarına cəlb etmək məqsədinə nail olmağa çalışır. Bu nümunənin araşdırılmasında məqsəd fərdləri radikallaşdırmaqda, zorakılığı qızışdırmaqda və əhəmiyyətli milli təhlükəsizliyə təhdid yaratmaqda olan informasiya müharibəsinin gücünü göstərməkdən ibarətdir [15].

4. Seçkilərdə dezinformasiya kampaniyaları. Müxtəlif ölkələrdə, o cümlədən Fransa və Almaniyada müşahidə olunan bu kampaniyalar yalan məlumatların yayılmasını, məlumatların manipulyasiyasını və seçki nəticələrinə təsir etmək üçün süni “onlayn” personajların yaradılmasını nəzərdə tutur. Burada məqsəd, şübhə və fikir ayrılığı yaratmaq, demokratik proseslərə ictimai inamı sarsıtmaqdır. Bu nümunə araşdırmaları seçki sistemlərinin və demokratik təsisatların bütövlüyünü qorumaq üçün informasiya müharibəsinə qarşı mübarizənin vacibliyini vurğulayır [16].

5. Çinin kibercasusluq əməliyyatları. Çinin kibercasusluq fəaliyyəti milli təhlükəsizlik baxımından digər dövlətlərə ciddi problemlər yaradır. Çin aktorlar bütün dünyada dövlət qurumlarını, müdafiə sənayesi şirkətlərini və tədqiqat institutlarını hədəfə alan müxtəlif haker qruplarından ibarətdir. Bu kiberəməliyyatlar həssas məlumatları, əqli mülkiyyəti oğurlamaq və strateji üstünlüklər əldə etmək məqsədi daşıyır. 2015-ci ildə ABŞ-ın milyonlarla federal əməkdaşının şəxsi məlumatlarının ələ keçirildiyi “Personal İdarəetmə Ofisi” fəaliyyətinin məhdudlaşdırılması fonunda baş vermiş hadisə informasiya müharibəsinin milli təhlükəsizliyə təsirini və güclü kibertəhlükəsizlik tədbirlərinə zərurət olduğunu göstərir [2].

6. Ukraynada hibrid müharibə. Ukraynadakı münaqişəni informasiya müharibəsi elementlərini özündə birləşdirən hibrid müharibə nümunəsi kimi görmək olar. Rusiya Ukraynanın şərqindəki separatçı hərəkatları dəstəkləmək üçün hərbi güc, təbliğat, dezinformasiya kampaniyaları və kiberhücumlardan istifadə edirdi. Yalan məlumatların yayılması, manipulyasiyası və Ukrayna infrastrukturunu hədəf alan kiberhücumlar informasiya müharibəsi taktikalarının ənənəvi hərbi strategiyalara inteqrasiyasını nümayiş etdirir [17].

Real dünya nümunələri informasiya müharibəsinin milli təhlükəsizliyə təsiri haqqında dəyərli fikirləri özündə ehtiva edir. Yuxarıda qeyd olunan nümunələr informasiya müharibəsinin müxtəlif taktika və nəticələrini əks etdirir. Bu araşdırmalar informasiya müharibəsinə qarşı mübarizədə çətinlikləri, məsələn, yalan məlumatın sürətlə yayılması və ictimai rəyin manipulyasiyasını tədqiq edir. Dövlətlər və tərəflərarası əməkdaşlıq, gücləndirilmiş kibertəhlükəsizlik tədbirləri, media savadlılığı proqramları, beynəlxalq əməkdaşlıq və möhkəm qanunvericilik bazalarının inkişafı daxil olmaqla, effektiv strategiyalar informasiya müharibəsinin yaratdığı təhlükələrə qarşı mübarizədə mühüm əhəmiyyət kəsb edir. Bu istiqamətdə dünyada baş vermiş insidentləri öyrənməklə, dövlətlər informasiya müharibəsinin mürəkkəbliklərini daha yaxşı anlaya və milli təhlükəsizlik maraqlarının qorunması üçün hərtərəfli yanaşmalar inkişaf etdirə bilər.

Nəticə

İnformasiya müharibəsinin milli təhlükəsizliyə əsas təhdid kimi ortaya çıxması onun konseptual əsasları, təsirləri, ona qarşı mübarizə strategiyaları və real dünya nümunələrinin hərtərəfli başa düşülməsini tələb edir. Bu məqalə Milli təhlükəsizlik maraqlarının qorunmasında informasiya müharibəsi ilə mübarizənin əhəmiyyəti məqalədə vurğulanmış və müvafiq aspektləri işıqlandırmışdır.

İnformasiyanın manipulyasiyası və istismarı ilə səciyyələnən informasiya müharibəsi siyasi, iqtisadi və sosial sahələrə geniş təsir göstərir. O, demokratik prosesləri sarsıdır, kritik infrastrukturun fəaliyyətinə zərər vurur və ictimai inamı sarsıdır. Texnologiyanın sürətli təkamülü və rəqəmsal dünyanın qarşılıqlı əlaqəsi informasiya müharibəsinə qarşı mübarizə ilə əlaqəli problemləri daha da gücləndirir. Bu təhlükəni effektiv həll etmək üçün informasiya müharibəsinə qarşı mübarizə strategiyaları fəal, əməkdaşlıq çərçivəsində qurulmalı və çoxölçülü olmalıdır. Kritik infrastrukturu və informasiya sistemlərini kiberhücumlardan qorumaq üçün kibertəhlükəsizlik tədbirlərinin gücləndirilməsi vacib amillərdən hesab olunur. Media savadlılığının və rəqəmsal vətəndaşlıq təhsilinin təşviqi fərdlərə məlumatları tənqidi qiymətləndirməyə və manipulyasiya üsullarını aşkar etməyə imkanı verir. Beynəlxalq əməkdaşlıq məlumat mübadiləsini, birgə cavabları, norma və çərçivələrin yaradılmasını asanlaşdırır. Əks-təbliğat və strateji kommunikasiya təşəbbüsləri yalan məlumatların üzə çıxarılmasında və düzgün məlumatın təbliğində mühüm rol oynayır.

Real dünya nümunələri informasiya müharibəsinin milli təhlükəsizliyə təsirinin konkret nümunələrini özündə əks etdirir. Bu nümunə araşdırmaları informasiya müharibəsinə qarşı effektiv mübarizə aparmaq üçün adaptiv və hərtərəfli strategiyalara olan zərurəti tədqiq edir.

Nəticə olaraq, informasiya müharibəsinə qarşı mübarizə fəal tədbirlər, birgə səylər və davamlı adaptasiya tələb edən mürəkkəb və çoxşaxəli prosesdir. Dövlətlər, təşkilatlar və fərdlər kibertəhlükəsizlik tədbirlərini gücləndirməli, media savadlılığını və beynəlxalq əməkdaşlığı təşviq etməli, effektiv əks-tədbirlər görməlidir. Bu fəaliyyətlərin həyata keçirilməsi milli təhlükəsizlik maraqlarını və informasiya ekosistemlərinin bütövlüyünü qoruya, qloballaşan dünyada xalqların sabitliyi və rifahını təmin edə bilər.

İstifadə edilmiş ədəbiyyat siyahısı

1. Brazzoli, M.S. Future prospects of information warfare and particularly psychological operations // – South African army vision, – 2020, – p. 217-232.

2. Grages, T.H. Playing the Long Game: How Cyber Will Facilitate China's Long-Term Economic Espionage Campaign and Information Warfare Objectives: / PhD diss. / – Utica College, 2020 – 130 p.

3. Bolton, D. Targeting ontological security: Information warfare in the modern age // Political psychology, – 2021. № 1 (42) – p. 127-142.

4. Taddeo, M. Information warfare: A philosophical perspective // Philosophy and Geography, – 2011. №1 (25) – p. 105-120.

5. Paterson, T., Lauren, H. Political warfare in the digital age: cyber subversion, information operations and ‘deep fakAustralian Journal of International Affairs, – 2020. №4 (74). – p. 439-454.

6. Bârgăoanu, A. Godzimirski, J., Ioniță D. Information Warfare and information operations in the black sea area // – New Strategy Center, Norwegian Institute of International Affairs, – 2020, p. 3-34.
7. Usmonov, M. Information War // – International Journal of Academic and Applied Research (IJAAR), –2021. №1 (5). – p. 79-82.
8. Harknett, R.J and Max S. Cyber campaigns and strategic outcomes // – Journal of Strategic Studies, – 2022. №4 (45) – p. 534-567.
9. Acton, J.M. Cyber warfare & inadvertent escalation // – Daedalus, – 2020. №2 (149). – p. 133-149.
10. Christopher, W. In Information warfare in the age of cyber conflict. Social media as information warfare / W.Christopher, T.Trevor, M.M.Brian, J.Prier – Abingdon, Oxfordshire: Published by Routledge, – 2020. – 270 p.
11. Clark, M. Russian hybrid warfare // – Washington, DC: Institute for the Study of War – 2020, – p. 8-33.
12. A.H.Həsənov, R.R.İmanov, V.Z.İsayeva. Hibrid müharibələrdə informasiya hücumları // Strateji təhlil jurnalı, Bakı, 2018, № 1-2 (23-24), s. 485-495.
13. McCombie.S, Allon.J.U, Morrison, S. The US 2016 presidential election & Russia's troll farms // – Intelligence and National Security, – 2020, №1 (35). – p. 95-114.
14. Plėta,T., Tvaronavičienė, M., Silvia, D.C., Agafonov, K. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases // – Vilnius: Entrepreneurship and Sustainability Center, – 2020.№3(2) – p. 703-715.
15. Mitts, T., Gregoire, P., Barbara, F.W. Studying the impact of ISIS propaganda campaigns // – The Journal of Politics, – 2022. №2 (84). – p. 1220-1225.
16. Baumann, M. Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in Russia-West relations – Contemporary Politics, – 2020. №3 (26) – p. 288-307.
17. Bachmann, S.D, Dries, P., Duczynski, G. Hybrid warfare and disinformation: A Ukraine war perspective // – Global Policy, – 2023. №2 (14). – p. 3-5.

Аннотация
Информационная война и национальная безопасность
Рашадат Оруджев

В статье на реальных примерах отражены роль информационной войны в национальной безопасности, концептуальный взгляд на информационную войну, влияние информационной войны на национальную безопасность, стратегии борьбы с информационной войной. Рассматривается важность использования информационных и коммуникационных технологий для получения преимущества в конфликтах или достижения стратегических целей, а также манипулирования, эксплуатации и распространения информации с целью отрицательного воздействия на функционирование стратегических коммуникационных систем и влияния на результаты, а также борьба за информационное превосходство в контексте национальной безопасности. Объясняется, что оно играет решающую роль. Основная цель данного исследования – повышение медиаграмотности, критического мышления и цифровой грамотности граждан, а также формирование у личности способности выявлять и отличать ложную информацию. В этих рамках образовательные программы позволяют людям научиться оценивать источники, проверять информацию, факты и критически анализировать контент. В статье также упоминается сотрудничество государств и международных организаций в области обмена информацией, координации реагирования на кибератаки и продвижения ответственного поведения в информационном пространстве для создания норм, законов и единых рамок коллективной борьбы с информационной войной.

Ключевые слова: стратегическая коммуникация, национальная безопасность, информационная война, коммуникационные технологии, обмен информацией

Abstract
Information warfare and national security
Rashadat Orujov

In the article, the role of information warfare in national security, a conceptual view of information warfare, the impact of information warfare on national security, and strategies for combating information warfare are reflected in real-world examples. The importance of using information and communication technologies to gain advantage in conflicts or achieve strategic goals, as well as the manipulation, exploitation, and dissemination of information to adversely affect the functioning of strategic communication systems and influence outcomes, are addressed, and the struggle for information superiority in the context of national security. It is explained that it plays a decisive role. The main goal of this study is to increase media literacy, critical thinking and digital literacy among citizens, and to form the ability to identify and distinguish false information in individuals. In this framework, educational programs enable individuals to learn how to evaluate sources, check information, facts, and critically analyze content. The article also mentions the cooperation of states and international organizations in the field of information sharing, coordination of responses to cyber attacks, and promotion of responsible behavior in the information space for the creation of norms, laws and unified frameworks for the collective fight against information warfare.

Keywords: strategic communication, national security, information warfare, communication technologies, information exchange

Məqalə redaksiyaya daxil olmuşdur:25.04.2024
Təkrar işlənməyə göndərilmişdir:06.05.2024
Çapa qəbul edilmişdir: 03.06.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 116-122

UOT 351/354 DOI: 10.30546/9878.2024.2.10.0034.

THE IMPORTANCE OF CYBER DEFENSE FOR AZERBAIJANI NATIONAL SECURITY

mayor Mehrac Huseynov
National Defence University
mehrac77@yahoo.com

Abstract. This article offers a comprehensive exploration of cyber defense's significance for Azerbaijan's national security across three sections. The first section outlines Azerbaijan's importance and recent developments in cyberspace. The second section delves into the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack case study, analyzing its execution, focus on national power elements, and consequential impacts through diplomatic, informational, military, and economic lenses. Finally, the third section provides insights into necessary capabilities to enhance Azerbaijan's cyber defense posture.

The purpose of this research is to assess the importance of cybersecurity in bolstering Azerbaijan's national security framework, with a specific focus on recent developments and vulnerabilities in cyberspace. A combination of analysis and synthesis research methods is employed, including literature review, case study analysis, stakeholder interviews, comparative analysis, and scenario planning. These methods enable a comprehensive examination of cybersecurity in Azerbaijan, encompassing existing literature, in-depth case studies such as the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack, stakeholder insights, comparative assessments with other nations, and scenario-based analysis to anticipate cyber threats. The research yields crucial findings, emphasizing the necessity for robust cybersecurity measures in Azerbaijan due to its escalating reliance on cyberspace and the vulnerabilities exposed by incidents like the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack. Furthermore, it underscores the interconnected nature of cyber threats across diplomatic, informational, military, and economic domains, advocating for investments in technology, human capital, and international collaboration to fortify Azerbaijan's cyber defence posture and enhance cyber resilience.

Keywords: cybersecurity, Baku-Tbilisi-Ceyhan Pipeline, geopolitics, cyber threats, national security

Introduction

The Republic of Azerbaijan is located at the crossroads of Eastern Europe and Western Asia. “Despite its limited size and small population, Azerbaijan, with its vast energy resources, is also geopolitically critical. It is the cork in the bottle containing the riches of the Caspian Sea basin and Central Asia” [1].

Despite the political chaos and economic paralysis created by the collapse of the Soviet Union in the early 1990s and the recently ended conflict in the Karabakh region, Azerbaijan's economy has experienced a significant transformation and development. The economy of Azerbaijan is based on oil and natural gas, and the Baku-Tbilisi-Ceyhan Oil Pipeline is one of the biggest post-Soviet government projects. It is one of the leading projects that increased Azerbaijan’s geopolitical importance, was constructed to carry Azerbaijani oil to the west, and was completed in 2005. As a result, Azerbaijan is the most powerful country in the Caucasus region economically and militarily. However, economic improvement and strengthening of the infrastructure has created many challenges and threats. The country's location and its natural resources, coupled with its balanced policy to be neutral and cooperate with both the East and West, makes Azerbaijan vulnerable as a geopolitical pivot. Azerbaijan tries to maintain its status as a sovereign and independent country by avoiding alliances with any geopolitical bloc, but instead opts for economic, energy, and military cooperation with both West and East [2]. This economic development brought information technology to the country and made its infrastructure basically digital. The digitization of the functions and structures of state institutions and private

companies provides many benefits to the government, businesses, customers, and citizens. However, the ever-increasing use of information and communication technology moved society into the rapidly evolving cyber world. This transformation shows all the institutions, organizations, and functions of the society, and how the systems and processes of society are constructed and executed. The information and technology connected to the cyber environment are vulnerable to various security threats. Hence, the security of information as well as the security of the technology structures and infrastructure systems has become a serious issue. The State Security Service of Azerbaijan believes that the cyber-security threats are prevailing in Azerbaijan due to the digitalization of society and the development of non-oil state infrastructure [3].

Baku-Tbilisi-Ceyhan (BTC) Pipeline Cyber Attack

The term cyberspace is not only associated with the internet and connected computer systems, but it is also linked with the electronic devices and the systems connected directly or indirectly to it [4]. The security of cyberspace usually refers to the protection of cyberspace infrastructure, which contains the four features, computer hardware, telecommunication structure, the control systems of operating devices, and digital devices such as laptops or desktop computers [4]. Science fiction society termed the word, cyberspace, and now it is a mainstream term used to describe the domain of the global information technology environment.

We live in an increasingly networked world, from personal banking to government infrastructure. Protecting these networks is no longer optional; instead, it is mandatory and requires a great deal of investment. [5] Moreover, it is not only about the investment in technology, but also about personal awareness and about how to remain secure in cyberspace. Cyber security has become a primary challenge to all countries and organizations. It consists of threats that are generally unknown to the public and is strongly connected to strategic interests and information security.

Due to increased dependence on the availability of information communication technologies and the ever-growing number of internet users (now 40 percent of the world’s population) cyber security is now much more important in the world. Statistics and reports show that cyber threats are on the rise. The potential yearly financial impact on the global economy due to cybercrime exceeds $455 billion. [6] Developing countries are most at risk to cyber-attacks due to the broader use of information and communication technologies. Security is crucial for the socio-economic wellbeing of a country in the adoption of new technologies. Considering that Azerbaijan is among developing countries and uses the latest technologies in the field of energy, it is inevitable that cyber security is important for the country.

Traditional security has always been a priority of Azerbaijan’s foreign and domestic policies due to the Armenian occupation of Nagorno-Karabakh, which has recently ended, concerns about the Caspian Sea’s energy security, and the antagonistic neighbouring states of clerical Iran and nuclear Russia. However, the well-known Stuxnet case, which aimed to delay the Iranian nuclear program, focused Azerbaijan’s and other affected world states’ attention on cyber security [3]. Stuxnet mainly targeted Iranian computers; however, it also affected other states. Even though this incident did not severely damage the infrastructure and the economy, it showed the existing cyber security gaps in Azerbaijan. In Azerbaijan, the legal basis for cyber security should be strengthened because cyber weapons (such as the Stuxnet virus) have attempted to destroy the government infrastructures. Economic development and neighbouring threats on the borders show the significance of cyber security in all critical areas. Hence, cyber security has become vital concern to protect Azerbaijan's national security.

Baku-Tbilisi-Ceyhan (BTC) pipeline carries oil from Caspian Sea across Azerbaijan, Georgia and Turkey. The Sangachal terminal situated on the Caspian Sea coastline within Azerbaijan's borders is connected to the Ceyhan marine terminal located along the Turkish Mediterranean coast. Moreover, the pipeline facilitates the transportation of crude oil from Turkmenistan. Since October 2013, it has also recommenced the conveyance of Tengiz crude oil from Kazakhstan via the BTC pipeline [7]. The pipeline, which commenced operations in June 2006, was constructed by the Baku-Tbilisi-Ceyhan pipeline company, which is operated by British Petroleum.

The BTC pipeline incident is associated with the cyber-attack that took place on August 6, 2008, in close proximity to the town of Refahiye within Turkey. Hackers planned a combined physical and cyber-attack on the pipeline that caused an explosion and fire with flames as high as 50 meters [8]. The cyberattack carried out in 2008 on the BTC oil pipeline on Turkish soil created an explosion that ignited a fire, which blazed for over 20 days. Along the way, millions of dollars were lost in material and revenue. The physical rupture, which led to an explosion that resulted in a fire that was extinguished by firefighters on 7 August 2008. The pipeline was out of commission until reopened on 25 August 2008 [8].

The Kurdistan Workers' Party (PKK) terrorist group, battling with Turkey since 1984, claimed responsibility for the attack [9]. Despite the fact that PKK claimed responsibility for the attack, another interesting fact was that the incidence happened during a period of escalating tensions between Russia and Georgia, leading toward the brink of armed conflict. Two days after the pipeline explosion, Russia formally deployed troops into the Russian-Georgian conflict. The BTC pipeline runs through Georgia and it represented a threat to Russia's energy policy. In some reports, it was observed that attackers consisted of a team of two with laptops near the pipeline [8].

The BTC pipeline has been reported to have a new IP-based camera system network along the pipeline. The attack was made through an unprotected wireless network, making disconnections of security alarms and survey cameras. Cyber attackers had access to the control system of the pipeline and suppressed the alarms, manipulated the process and blunted the system operators [8]. Although the control systems in use at the BTC pipeline have not been disclosed, it is reasonable to assume that the security of the pipeline was very weak and the only observation of the pipeline occurred through the surveillance camera network installed along the pipeline and linked to the surveillance centre via the internet. The attackers identified these weaknesses and were able to exploit these vulnerabilities and penetrate the technical control system to access the alarm management server [9]. After disabling the alarms and all communication tools with local teams (by interfering with wireless communication,) they took control of industrial systems and created excessive pressure resulting in an explosion in the pipeline [9]. The described attack scenario is lacking details, but reports suggests that the attackers might have used a wireless Internet connection to gain access to the security camera network. Other details indicate physical access to field controllers may have also been necessary [8].

The scenario describes the attack as targeting industrial computers at valve stations to change pressure and misreport results back to the control room [8]. This information may point to direct physical access to control components at remote locations. This information suggests that there was direct physical access to control components at remote locations. The assault on the camera system might have solely aimed to obstruct the pipeline operator's view, potentially facilitating physical intrusions to gain access to field components.

This event is an example of an industrial system attack, which may have been partly supported by a foreign government. When we analyse this attack from the Diplomatic, Information, Military, and Economic (DIME) perspective, the most affected national power was economy. Three elements of national power were covered in one paragraph.

Diplomatic-Information-Military: PKK's proclamation and the rise of Russian – Georgian tensions infer that Diplomatic issues may have been the basis of this attack but tangible evidence that can prove it does not exist. In addition, no observable diplomatic consequence arose from this attack other than the proclamation of PKK's responsibility for the attack. Generally, it is known that PKK's aim is getting diplomatic power in Turkey and divide the country as they represent themselves as freedom fighters of the Kurdish population. It is possible that they tried to send a message to the Turkish government with this attack by demonstrating their capabilities. Countries and companies are strong as long as they are able to hide their information and secrets, which they have to protect. Damaging these institutions and countries is going to be a great deal easier when they are unable to defend critical information and infrastructure. A terrorist organization attacking an industrial system with a combination

of physical and cyber-attacks, demonstrates advanced capabilities perhaps associated with a military, but none of these attacks were aimed at a specific military installation.

Economic: The researcher would like to start the analysis with BCT throughput capacity – one million barrels per day from March 2006 to March 2009 [7]. The pipeline has significantly boosted the economies of the host countries, as Georgia and Turkey receive substantial annual transit fees, amounting to large sums of money. In the early years of operation, Turkey is anticipated to receive around $200 million annually in transit fees, with projections suggesting that these fees could rise to $290 million per year from 2017 to 2040. Additionally, Turkey gains from heightened commercial activity in the port of Ceyhan and other areas of eastern Anatolia, a region that had witnessed a notable decline in economic activities since the Gulf War in 1991 [10]. This data shows us how big the economic damage is in this attack. If one only takes into consideration the transfer fee lost, it is approximately equal to $11 million USD.

On the other hand, Georgia and Azerbaijan also were affected economically by this attack. Georgia is projected to receive an average of $62.5 million annually in transit fees [10]. Twenty-day downtime means about $3.5 million loss of income for Georgia. This attack also created a significant economic loss for Azerbaijan. As mentioned earlier, one million barrels per day of oil were flowing through BTC; this means that the 20-day interruption caused 20 million barrels of oil loss.

What capabilities are needed to improve Azerbaijan's cyber defence posture?

The purpose of this paragraph is to answer: What capabilities are needed to improve Azerbaijan's cyber defence posture? This question has been answered under four main headings: Improve Education on Cyber-Security, Awareness of Cyber Situations, Cyber-Security Partnerships, and Strong Cyber-Deterrence.

To improve education on cyber-security, basic cyber security should be taught at the school level, from beginning levels to university level. Training programs should focus on increasing the number of incident response teams. Education would focus on prevention of attacks and key is a strong defence. Prevention is expensive in terms of time and money but recovery is very costly and international credibility cannot be rebuilt overnight. Cyber hygiene courses should be created for the governmental entities and should be mandatory for all employees as a prerequisite course.

If Azerbaijan does not know who the attacker is (successfully or unsuccessfully), Azerbaijan cannot protect itself. New laws should require that certain types of cyber-incidents must be reported to appropriate authorities. Government policy must incentivize and encourage sharing of attack data by victims, not inhibit or unnecessarily penalize/publicize. A framework must be built to predict the impact of new cyber-attacks on other parts of the Azerbaijan internet infrastructure in order to take immediate corrective action.

Cyber-Security Partnerships must be made. Cyber-defence partners could include Turkey, Georgia as well as Pakistan. Due to sharing BTC pipeline and other strategic planned projects, with Turkey and Georgia, it is inevitable to create partnerships in cyberspace. On the other hand, Pakistan is one of the most powerful military partners of Azerbaijan and relations at government level are based on very strong ties.

Strong cyber-deterrence is important and robust cyber-attack capability must be created. Respondents must know that Azerbaijan has strong cyber-deterrence capabilities. Cyber threats can be categorized in many ways, and each category will have different motivations and cyber skills or abilities. The government's ability to deter each cyber-hostile group should be variable.

Over all DIME Analysis showed that, cyber threat is very harmful and very possible for Azerbaijan due to its industrial-based economy. In order to protect the industrial-based economy and infrastructure against cyber-attacks, cyber defence has vital importance in the national security of Azerbaijan. Moreover, analysis has shown that the most affected instrument of national power in possible cyber-attacks to Azerbaijan is the economy. National defence measures will mitigate the damage of cyber hazards. First of all, it can be ensured that the critical infrastructures of country work with the network

independent of the internet. The intranet system can be implemented to prevent attacks from the internet. National security policy should be determined and local software should be created and focused on that. The software produced by the foreign country may not be secure. In critical infrastructure systems and software, the possibility of espionage can be weakened by using national products. In order to identify vulnerabilities and hazards, attack threat detection mechanisms should be used and strengthened. General participation can be achieved by emphasizing the importance of national cyber exercises. The support of universities and private institutions in cyber defence strategies must be increased. National Strategy, Laws and Recommendations, and cooperation with partner countries are important factors in increasing the country's cyber power.

In conclusion, the Republic of Azerbaijan stands at a critical juncture, balancing its geopolitical significance as an energy hub with the increasing challenges posed by cyber threats. The country's economic transformation, driven by its oil and natural gas resources, has elevated its status in the Caucasus region. However, this development has exposed Azerbaijan to vulnerabilities in the rapidly evolving cyber world.

The Baku-Tbilisi-Ceyhan (BTC) pipeline cyber-attack serves as a poignant example of the potential risks Azerbaijan faces in the digital era. The combined physical and cyber assault orchestrated by the PKK terrorist group not only caused a significant economic setback but also underscored the weaknesses in Azerbaijan's cyber security infrastructure. This incident emphasizes the need for a robust cyber defense posture to safeguard the nation's critical assets.

Conclusion

Azerbaijan's response to cyber threats requires a multifaceted approach. Primarily, enhancing education on cyber security from schools to universities is imperative. Building a skilled workforce and incident response teams will contribute to preventing and mitigating cyber-attacks. Additionally, fostering awareness of cyber situations and implementing reporting mechanisms for cyber incidents are crucial steps in bolstering the nation's cyber resilience.

Cyber-security partnerships with neighboring countries like Turkey, Georgia, and strong allies such as Pakistan are essential. Given the interconnectedness in the region, collaborative efforts can strengthen collective defenses and provide a united front against cyber threats. Moreover, establishing a strong cyber-deterrence capability is paramount. Azerbaijan must highlight its ability to defend against cyber-attacks, thereby dissuading potential adversaries.

The Diplomatic, Information, Military, and Economic (DIME) analysis underscores the economic repercussions of cyber-attacks on Azerbaijan. The country's industrial-based economy makes it susceptible to disruptions, and protecting against cyber threats becomes integral to national security.

In conclusion, Azerbaijan's journey towards economic development and geopolitical prominence necessitates a proactive and comprehensive approach to cyber security. By investing in education, fostering awareness, building strategic partnerships, and establishing a formidable cyber-deterrence capability, Azerbaijan can fortify its defenses in the cyber domain. In doing so, the nation can continue to thrive in the digital age while safeguarding its critical infrastructure and economic prosperity.

References

1. Brezinski, Z. The Grand Chessboard. American Primacy and Its Geostrategic Imperatives / Z.Brezinski – NY: Basic Books – 1997. – 240 p.

2. Strîmbovschi, S. Azerbaijan’s Balanced Foreign Policy Trapped in a Volatile Geopolitical Context: [Electronic resource] / – europolity.eu. – Bucharest, Romania, 2015.
URL: http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.121-134.pdf

3. Makili-Aliyev, K and Attiq-ur-Rehman. Cyber-security objective: Azerbaijan in the digitalized world: [Electronic resource] / – sam.az. – November 2013.

URL:http://sam.az/uploads/PDF/SAM%20comments%20and%20review%20publications/Cyber%20Security%20objective%20Azerbaijan%20in%20the%20digitalized%20world.pdf.

4. Fischer, E.A. Creating a National Framework for Cybersecurity: An analysis of issues and options / E.A. Fischer. – New York: Nova Science Publishers, – 2019. – 92 p.

5. Detlev, G., Bertrand, L., Orzechowski, D. Cyber risk: Why cyber security is important: [Electronic resource] / – coursehero.com, – 2019.
URL:https://www.coursehero.com/file/42218407/Explain-What-Cybersecurity-Is-and-Why-We-Should-Care-revisiondocx/

6. Reuters. Cyber security: [Electronic resource] / – reuters.com. – 10 December, 2018.
URL:https://www.reuters.com/article/us-cybersecurity-mcafee-csis/cyber-crime-costs-global-economy-445-billion-a-year-report-idUSKBN0EK0SV20140609

7. BP.com. Baku-Tbilisi-Ceyhan pipeline: [Electronic resource] / – bp.com.
URL: https://www.bp.com/en_az/caspian/operationsprojects/pipelines/BTC.html.

8. Lee, R.M, Assante. M.J., Conway T. Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack: [Electronic resource] / – ICS Defense Use Case (DUC.) SANS Institute. – Bethesda, MD, USA, 20 December, 2014.
URL:https://scholar.google.com/citations?view_op=view_citation&hl=en&user=mqu2hhyaaaaj&citation_for_view=mqu2hhyaaaaj:mvmsd5a6bfqc

9. The Sentryo Files: Industries vs. cyber-attacks Episode 2. Attack on the BTC oil pipeline in 2008: [Electronic resource] / – Sentryo.net. – 17 August, 2017.
URL: https://www.sentryo.net/the-sentryo-files-industries-vs-cyberattacksepisode-2-attack-on-the-btc-oil-pipeline-in-2008/.

10. Iqbal, M. Z., Shah, N. The Baku-Tbilisi-Ceyhan Pipeline: Political and Economic Impacts for the Region // – Islamabad: Pakistan Horizon, – 2015. № 68(1). – p. 69-81.

Xülasə
Azərbaycanın milli təhlükəsizliyi üçün kibermüdafiənin əhəmiyyəti
Mehrac Hüseynov

Məqalənin hər üç bölməsində Azərbaycanın milli təhlükəsizliyi üçün kibermüdafiənin əhəmiyyətinin hərtərəfli tədqiqi əks olunur. Birinci bölmədə son illərdə kiberməkanda baş verən hadisələr vurğulanır. İkinci bölmədə Bakı–Tbilisi–Ceyhan boru kəmərinə kiberhücum araşdırılır, diplomatik, informasiya, hərbi və iqtisadi milli güc elementləri də nəzərə alınaraq, bu hücumun təsiri təhlil edilir. Üçüncü bölmədə Azərbaycanın kibermüdafiə sahəsindəki gücünün artırılması üçün lazım olan imkanlar barədə məlumatlar öz əksini tapır. Tədqiqat işində məqsəd Azərbaycanın milli təhlükəsizlik sisteminin gücləndirilməsində kibertəhlükəsizliyin əhəmiyyətini vurğulamaq, kiberməkanda baş verən son hadisələri qiymətləndirmək və bu sahədəki zəiflikləri müəyyən etməkdən ibarətdir. Məqalədə təhlil, sintez və müqayisəli təhlil tədqiqat metodlarından istifadə edilmişdir. Bu üsullar Azərbaycanda kibertəhlükəsizliyin hərtərəfli tədqiqinə, mövcud ədəbiyyatların təhlilinə, Bakı–Tbilisi–Ceyhan boru kəmərinə edilən kiberhücumun analizinə, maraqlı tərəflərin rəylərinə, digər ölkələrlə müqayisəli qiymətləndirmə aparmağa və ssenari əsasında təhlilə imkan verir. Tədqiqat işində kiberzəifliklərin ağır nəticələrinin qarşısının alınmasında kibertəhlükəsizlik tədbirlərinə ehtiyac olduğu vurğulanır və bununla bağlı tədbirlər planı təklif edilir. Bundan əlavə, tədqiqat işində diplomatik, informasiya, hərbi və iqtisadi sahələrdə kibertəhlükələrin bir-biri ilə əlaqəli xarakteri, eyni zamanda Azərbaycanın kibermüdafiə imkanlarını gücləndirmək və kiberdavamlılığını artırmaq üçün texnologiyaya, insan kapitalına və beynəlxalq əməkdaşlığa sərmayələrin yatırılmasının əhəmiyyəti əsaslandırılır.

Açar sözlər: kibertəhlükəsizlik, Bakı-Tbilisi-Ceyhan boru kəməri, geosiyasət, kibertəhdidlər, milli təhlükəsizlik

Аннотация
Значение киберзащиты для национальной безопасности Азербайджана
Мехрадж Гусейнов

В данной статье в трех разделах описывается комплексное исследование значимости киберзащиты для национальной безопасности Азербайджана. В первом разделе отражается важность Азербайджана и развития в киберпространстве за последние годы. Во втором разделе рассматривается пример кибератаки на трубопровод Баку-Тбилиси-Джейхан, анализируется ее реализация, основное внимание уделяется элементам национальной мощи и полученным эффектам через дипломатическую, информационную, военную и экономическую призму. И наконец, в третьем разделе дается представление о необходимых возможностях для укрепления потенциала киберзащиты Азербайджана. Целью данного исследования является оценка значимости кибербезопасности в укреплении системы национальной безопасности Азербайджана, с особым акцентом на последние события и уязвимости в киберпространстве. В анализе и синтезе используется сочетание исследовательских методов, включая анализ литературы и работы, интервью с заинтересованными сторонами, сравнительный анализ и сценарное планирование. Эти методы позволяют провести всестороннее исследование кибербезопасности в Азербайджане, проанализировать существующую литературу, углубленные тематические исследования, такие как кибератака на трубопровод Баку-Тбилиси-Джейхан, мнения заинтересованных сторон, сравнительные оценки с другими странами, а также анализ на основе сценариев для преждевременного прогнозирования кибербезопасности. Исследование дает важные результаты, которые подчеркивают необходимость принятия строгих мер по кибербезопасности из-за уязвимостей, трубопровода Баку-Тбилиси-Джейхан подверженных инцидентам кибератак в Азербайджане и уязвимости к кибератакам. Кроме того, он подчеркивает взаимосвязанный характер киберугроз в дипломатической, информационной, военной и экономической сферах, пропагандируя инвестиции в технологии, человеческий капитал и международное сотрудничество для укрепления потенциала киберзащиты Азербайджана и повышения киберустойчивости.

Ключевые слова: кибербезопасность, трубопровод Баку-Тбилиси-Джейхан, геополитика, киберугрозы, национальная безопасность

Məqalə redaksiyaya daxil olmuşdur: 15.01.2024
Təkrar işlənməyə göndərilmişdir: 26.01.2024
Çapa qəbul edilmişdir: 07.03.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 123-132
MİLLİ TƏHLÜKƏSİZLİK ***NATIONAL SECURITY***

UOT 004 DOI: 10.30546/9878.2024.2.10.0036.

PRESERVING CONFIDENTIAL INFORMATION: A COMPREHENSIVE ANALYSIS OF SECURITY AND PRIVACY CONCERNS IN INTERNET OF THINGS (IOT) SYSTEMS

mayor Elshan Tanriverdiyev
National Defence University
elshantanriverdiyev@gmail.com

Abstract. This research paper conducts a thorough analysis of security and privacy concerns within internet of things (IoT) systems, aiming to identify vulnerabilities across its various layers perception, network, transport, and application – and develop strategies to mitigate these risks. The study is structured to first categorize major security threats and privacy issues within each IoT layer, followed by a comprehensive literature review to understand existing challenges and solutions. Further tasks include analyzing common attack vectors and assessing the effectiveness of proposed security measures through simulations and real-world case studies.

A variety of research methods were employed, including systematic literature reviews, case studies, experimental research, and simulation modeling to test and predict effectiveness of the solution.

The research results reveal key vulnerabilities within each IoT layer and catalog a comprehensive range of potential attack vectors by their targets and threat nature. It highlights significant shortcomings in existing security measures, and emphasizes the need for enhanced solutions tailored to these specific vulnerabilities.

The outcome of the research is the development of recommended security measures and best practices, specifically designed for IoT systems. These recommendations encompass layered security protocols, enhanced encryption methods, and dynamic authentication mechanisms. The study also proposes a framework for continuous security assessment and adaptation, aiming to foster the development of more resilient and secure IoT environments. This comprehensive approach not only addresses current security challenges but also prepares for future threats.

Keywords: internet of things, IoT Systems, IoT security issues, IoT security attacks

Introduction

In the realm of future technologies, the Internet of Things (IoT) has become a ubiquitous and frequently discussed concept. IoT comprises a network of intelligent objects, with these nodes serving as the central actors in the IoT network. Their primary function is information exchange and facilitating user communication. IoT stands at the forefront of the ongoing expansion of internet services, as it aims to integrate and connect an extensive array of objects and devices [1]. IoT entities encompass a wide range of devices, including laptops, smartphones, smartwatches, televisions, and automobiles. Each individual IoT node within the network possesses its distinct identity and designated role. The seamless cooperation among these nodes results in the formation of a robust and collaborative IoT network. Within IoT, objects are integrated into the physical environment and initiate data collection and sharing autonomously, free from human intervention. It was projected that the quantity of interconnected objects on the internet would soar to approximately 25 billion by the year 2020 [2]. IoT devices exhibit intelligence due to their access to data and information from interconnected devices, providing them with the capability to make real-time decisions and execute their functions intelligently. Figure 1 illustrates the fundamental concept of IoT systems [3]. In the near future, the proliferation of IoT networks is anticipated to continue, expand in scope, and assume greater significance within the realm of technology. As IoT continues to evolve, fresh security and privacy concerns emerge, alongside the exacerbation of conventional security and privacy issues. Two primary drivers of this phenomenon are the vast number of connected objects and the increasing diversity within the IoT landscape [4]. Within

IoT development communities, there is a diverse group of developers, some of whom possess limited familiarity with security standards. The inherent complexity and ambiguity surrounding IoT have consequently elevated IoT security to the top priority for both end-users and institutions [5].

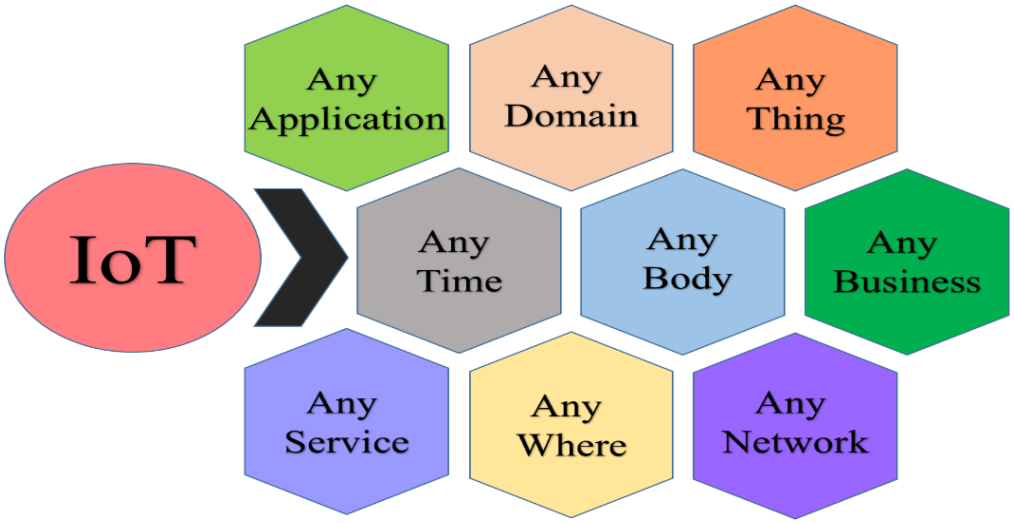


Figure 1. The fundamental concept of IoT systems

Much like any other technology, IoT is susceptible to attacks from malicious users or hackers. The extensive and intricate architecture of IoT creates vulnerabilities that hackers can identify and exploit, potentially leading to network breaches. These breaches can manifest in various ways, including network disruption, data misuse, and more. Given the critical role of IoT networks, it is imperative to fortify their security and address all potential vulnerabilities. Users are increasingly seeking the highest levels of security and privacy when utilizing IoT networks, given the sensitive information exchanged within these networks. Consequently, the subject of IoT security and privacy has gained prominence due to the integral role of IoT in our daily lives. IoT technology is omnipresent, appearing in forms such as smart wearables (e.g., smartwatches), smart homes, autonomous vehicles, precision agriculture systems, healthcare solutions, and more.

Security concerns within IoT networks stem from multiple sources. Some of these issues in security and privacy result from attacks on different layers of the IoT architecture. Additionally, attacks may exploit the network's communication characteristics to infiltrate and compromise network components, weakening their integrity. This paper conducts a thorough examination of IoT security and privacy issues, delving into their complexities. It seeks to shed light on the types of attacks that can target IoT systems, detailing how these attacks have detrimental effects. Furthermore, the paper outlines measures to prevent attacks and fortify IoT systems against potential threats. It serves the purpose of providing comprehensive insights into the state of IoT security and the possible risks faced by IoT users, thereby aiding in the development of stronger and more secure IoT systems, given their expanding use in everyday life.

1. Security and privacy concerns at different layers of IoT:

IoT consists of four primary layers, namely, the perception layer, network layer, transport layer (commonly referred to as the Middleware Layer), and the application layer. Each of these layers introduces its distinct privacy and security considerations. This section will provide an in-depth exploration of these IoT layers, highlighting the respective issues, challenges, and security aspects. Figure 2 illustrates the composition of IoT layers.

The perception layer encompasses distinct sets of data, divided into two primary components: the perception node and the perception network. The perception node assumes the role of data collection, while the perception network manages the transmission and administration of data. Within the perception layer, a diverse array of sensor technologies are integrated, such as Radio Frequency Identification (RFID) [6].

RFID systems encounter security and privacy challenges. The perception layer encompasses a variety of control and data collection modules, including sound sensors, vibration sensors, and temperature sensors. Within this layer, the primary role is to gather data from the environment through the use of sensors and actuators.

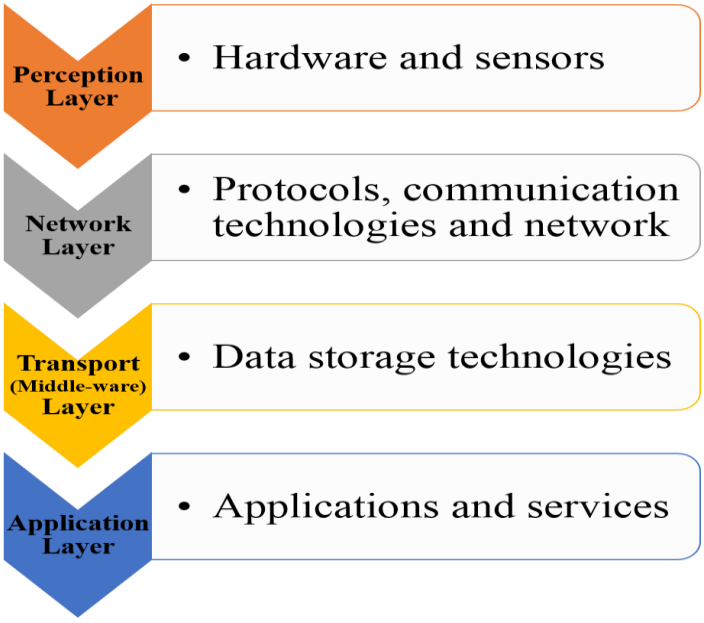


Figure 2. IoT layers

Subsequently, the perception layer undertakes the tasks of data verification, collection, and processing before forwarding the information to the subsequent layer, which is the network layer. It is worth noting that data collected within the perception layer may undergo pre-processing before transmission to the network layer. Additionally, this layer is responsible for regulating data sources, with IoT nodes serving as the primary data origin [7].

1.1. Perception layer security and privacy issues:

IoT nodes face significant susceptibility to attacks, which has led to the development of a security node within the architecture of the perception layer (referred to as SNPL). The application layer primarily encompasses hardware components and sensors. Within the perception layer, there are various security and privacy concerns, which are outlined as follows:

1.1.1. Tag Cloning:

Tags are affixed to various objects, and, through certain hacking techniques, the data on these objects can be accessed, read, and even altered. This situation can result in tag cloning, where individuals with ill intent can effortlessly capture tags and produce duplicates, making it challenging for users to distinguish between the compromised and authentic tags.

1.1.2. Eavesdropping:

Eavesdropping refers to the interception of information exchanged between two nodes or communication devices, often involving a process known as data sniffing. The wireless nature of RFID technology renders it vulnerable to eavesdropping, making it relatively easy for hackers to intercept sensitive information flowing between the tag and the reader, or vice versa. Within the realm of wireless surveillance, there are two primary categories of eavesdropping attacks: passive and proactive. Proactive eavesdropping is employed with the aim of intensifying the eavesdropping rate.

1.1.3. Spoofing:

These attacks involve the transmission of inaccurate and deceptive information to the RFID system, with the intent of falsely representing it as originating from an authenticated and genuine source. This deceptive tactic grants attackers full access to the system, rendering it vulnerable. Spoofing attacks are a type of assault that can result in the creation of routing loops. Such attacks have the capability to both truncate and elongate source routes, achieved by either repelling or enticing network selection by

nodes. Spoofing attacks encompass various forms, including IP spoofing and RFID spoofing. RFID spoofing takes place when an attacker attempts to deceive the system and gain access to records, subsequently sending harmful data by employing the identification of an authorized tag. Attackers employ tactics aimed at persuading the application that they are genuine users, with the objective of assuming control over the IoT application.

1.1.4. RF Jamming:

Radio Frequency (RF) Jamming involves a deliberate non-compliance with lower-level protocols to disrupt ongoing legitimate communication. RF jamming can have various detrimental effects on communication by transmitting signals with diverse patterns. In this type of attack, RFID tags are compromised through a Denial of Service (DoS) attack, which introduces RF signals mixed with noise signals, disrupting communication. The source initiating jamming attacks may vary in power, from very potent, capable of damaging the entire network, to less powerful, causing harm to specific network segments. Security attacks and threats are pertinent across all layers of IoT. These attacks fall into two broad categories: active attacks, which directly impede service, and passive attacks, which observe IoT network information without obstructing network functions. Security attacks can also be categorized based on their source of origin, with external attacks stemming from sources outside the network, and internal attacks initiated by insiders. At all IoT layers, IoT objects and services are susceptible to Denial of Service (DoS) attacks, which aim to render the network inaccessible to authorized users [8].

Within the perception layer, three primary security issues are prominent. The first issue pertains to the strength of wireless signals. In this layer, signals are transmitted between sensors using wireless technologies, and the effectiveness of this communication can be compromised by interference from disruptive waves. The second issue is associated with IoT devices, where sensor nodes can be incapacitated either by the device owner or by potential attackers. This vulnerability is due to the outdoor and external nature of IoT systems, making them susceptible to physical attacks on both the IoT nodes and the IoT system. The third issue revolves around the dynamic nature of network topology within IoT. IoT nodes frequently move across various locations, resulting in a constantly shifting network topology. In the perception layer, RFID and sensors play a critical role. However, these components have limited storage, power capacity, and computational capabilities, making them susceptible to security breaches and attacks.

Altering, spoofing, or replaying the identity information of an IoT device can instigate a replay attack [9]. In a timing attack, hackers scrutinize the time required for encryption to deduce the encryption key. Node capture attacks transpire when an attacker gains control over IoT nodes, capturing their data and information. Attackers exploit the confidentiality of the perception layer by employing replay attacks, timing attacks, and node capture attacks. To threaten the integrity of data in the perception layer, assailants may add an extra node that transmits malicious data to the IoT network. Initiating a Denial of Service (DoS) attack is attainable by draining the energy of IoT nodes and preventing them from entering sleep mode, which is designed to conserve energy. Security issues within the perception layer can be mitigated through the implementation of point-to-point or end-to-end encryption measures.

The perception layer constitutes the foundational tier in IoT systems, situated at the lowest level of the IoT layer hierarchy. This layer serves multiple security functions and serves four primary purposes: safeguarding data privacy and sensitive information, enabling authentication, and assessing potential risks. Authentication is a crucial security objective essential for safeguarding systems against intrusion from hackers and malicious entities. Cryptography provides a means to implement authentication, employing algorithms capable of generating digital signatures to fortify protection against attacks, including collision attacks and brute force attempts. The protection and security of data are paramount during both collection and transmission to subsequent layers. Achieving data privacy can be accomplished through the utilization of symmetric and asymmetric encryption algorithms. These encryption algorithms are particularly advantageous for sensor deployment due to their minimal power consumption. Ensuring location anonymity and identity protection is essential for securing sensitive information. This can be effectively accomplished through the K-Anonymity approach, which shields

user data, identity, and location information from potential exposure and harm. Risk assessment holds a significant role within IoT security, primarily because it aids in the identification of novel threats to systems. Furthermore, it assists in the formulation of security strategies that can be categorized as optimal, ultimately serving as a preventative measure against potential security breaches. In the event that an intrusion is detected, the RFID reader issues a kill-command to the RFID tag to halt unauthorized access to the data stored on the tag [10].

2. IoT Network Layer security and privacy issues:

Following the perception layer in the IoT layers framework, the subsequent layer is the network layer. This layer assumes responsibility for ensuring the security of information and facilitating the transmission of data within the network.

The network layer encompasses a spectrum of technologies including mobile devices, the internet, and cloud computing. Within this layer, Wireless Sensor Networks (WSN) are responsible for reliably transmitting data from sensors to their intended destinations. It also plays a crucial role in facilitating data exchange between IoT devices and hubs and serves as the foundation for data routing. Various technologies such as WiFi, Bluetooth, 3G, and LTE are employed in the network layer to manage internet operations, including switching, routing, and gateways. Network gateways act as intermediaries between IoT nodes, facilitating the process of transmitting, aggregating, and filtering data. The network layer consists of an array of protocols, communication technologies, and the corresponding hardware. In practice, the network layer plays a pivotal role in establishing connections between IoT nodes and IoT applications, allowing for data flow and interaction. Each node or device within the IoT system has a unique identity to enable data traceability. Network components like switches, hubs, routers, and gateways are crucial in connecting IoT nodes and devices with each other. One of the primary security concerns at the network layer is the potential for a Denial of Service (DoS) attack. These attacks are initiated by malicious actors with the intent of rendering services unavailable to legitimate users.

2.1. Sybil Attack:

A Sybil attack involves an attacker attempting to compromise the system by manipulating a node to possess multiple identities, leading to the dissemination of false information. In a Sybil attack, malicious entities can employ multiple identities within the same network, often presenting duplicated or erroneous identification for the purpose of deceiving other IoT nodes.

2.1.1. Sinkhole Attack:

A sinkhole attack revolves around the strategy of making compromised nodes appear appealing to nearby nodes, causing data to be directed toward these compromised nodes and, ultimately, leading to dropped packets. The system, under the influence of this attack, falsely assumes that data has been successfully transmitted to its destination, while, in reality, the system's traffic is disrupted. Sinkhole attacks can potentially trigger a Denial of Service (DoS) scenario due to the increased energy consumption associated with routing through malicious nodes. In a sinkhole attack, a malicious node can deceive IoT nodes by providing fraudulent routing information, redirecting the packets of other nodes through it. The process of a sinkhole attack operates in a clandestine manner, typically escaping the network's detection mechanisms, as attackers aim to mislead the system into believing that all transmitted data has reached its intended receiver.

2.1.2. Denial of Service (DoS) Attack:

A Denial of Service (DoS) attack transpires when an attacker seeks to inundate a network with an excessive volume of meaningless traffic, depleting the system's resources. As a result, the system's network becomes inaccessible to its users. In this type of attack, the attacker sends a barrage of requests to a server, overwhelming it with requests, ultimately causing the server to become unresponsive or go offline.

2.1.3. Malicious code injection:

A malicious code injection attack transpires when an attacker attempts to manipulate a sensor node into introducing malicious code into the system, resulting in network shutdown. This subsequently grants the attacker complete control over the network. Code injection enables attackers to incorporate malicious

code into input fields, allowing them to execute the code and gain unauthorized access to the application. This form of attack can manifest when injecting malicious JavaScript code into an HTML document, potentially leading to hijacking and the spread of botnets.

2.1.4. Man-in-the-Middle Attack:

The Man-in-the-Middle attack is akin to an eavesdropping attack, with its focus centered on the communication channel. In this attack, an unauthorized user can intercept and manipulate communication between two other parties. Additionally, the unauthorized user has the capacity to assume the identity of the victim and utilize the channel for information acquisition.

In a Passive Man-in-the-Middle attack, an eavesdropper taps into the communication using a Poisson channel. In the context of traffic analysis, passive monitoring and eavesdropping can compromise the privacy and confidentiality of IoT networks. These three attacks are frequent due to the remote access mechanism and data exchange. Man-in-the-Middle and eavesdropping attacks are especially likely to occur in the network layer. The security of communication channels becomes compromised if the keying material of IoT devices is intercepted.

IoT communication fundamentally differs from typical internet communication because IoT extends beyond machine-to-human interactions to include machine-to-machine communication. This expansion introduces compatibility and security challenges, particularly in the context of heterogeneous network components [10]. Standard network protocols are often inadequate for addressing these diverse elements. In an IoT network, various objects are interconnected to gather information about users, a feature that malicious actors may exploit to misuse user information. Consequently, safeguarding IoT network objects is as crucial as protecting the network itself. These objects should possess the capability to take proactive measures in self-defense against network-initiated attacks. This requires the implementation of robust protocols and software within the network, enabling objects to respond to abnormal behaviors or conditions that threaten both the objects and network security.

Network layers encompass both wired and wireless communication capabilities. The openness of wireless communication channels exposes the network layer to a multitude of potential attacks. Security within the network layer can be categorized into three types: authentication, routing security, and data privacy. The implementation of authentication and encryption measures is effective in thwarting unauthorized access to nodes, consequently preventing the dissemination of false information. The most common threat encountered is the Denial of Service (DoS) attack, which disrupts the network by flooding it with an excess of meaningless traffic within communication channels. Routing algorithms play a crucial role in ensuring the privacy of data transmitted between sensors and the system. To enhance the system's error detection capabilities and fortify it against potential failures, multiple data routing paths need to be established. Security control mechanisms must be integrated to monitor the system and shield it from various forms of intrusion. To verify that received data at one end matches the original data transmitted from the other end, data integrity methods should be implemented. The security issues within the transport layer can be categorized as follows:

2.2. IoT Transport (Middle-ware) Layer security and privacy issues:

Following the network layer in IoT systems, the subsequent layer is the Transport (Middle-ware) Layer. Within this layer, data storage technologies, such as cloud computing, are employed. This layer facilitates ubiquitous access for the perception layer, and it is divided into three distinct layers: local area, core network, and access network.

2.2.1. Unauthorized Access:

Unauthorized system access may transpire when an attacker engages in data deletion or restricts access to IoT services, thereby inflicting harm on the IoT system. The Transport (Middle-ware) layer offers dual interfaces, one for data storage and another for applications. Attackers can gain unethical entry to infiltrate the network by exploiting misconfigured access control rights.

2.2.2. DoS Attack:

A Denial of Service (DoS) attack is characterized by the generation of a substantial volume of superfluous traffic aimed at incapacitating the system. Attackers execute these attacks to render the

network service unavailable for a specific duration [10]. Numerous DoS attacks can be launched to target the IoT system, with their objective being the depletion of service provider resources and network bandwidth. The complexity and heterogeneity of IoT networks render the transport layer susceptible to DoS attacks.

2.2.3. Malicious Insider:

Insiders possess the capability to manipulate and modify data to serve their personal interests. A Malicious Insider attack transpires when an insider manipulates data for their personal gain or the benefit of third parties. One potential method to safeguard IoT systems against malicious insider attacks involves the implementation of the Isabelle insider framework. This framework is designed to identify any policy violations that may occur [11].

2.3. IoT Application Layer security and privacy issues:

The final layer within the IoT framework, subsequent to the Transport (Middle-ware) Layer, is the application layer. This layer plays a vital role in structuring the application layer's services, is visible to end users, and represents the topmost layer. Its purpose is to fulfill the vision of creating smart environments and IoT-based systems, ensuring authenticity, integrity, and confidentiality. However, security issues can arise due to the absence of standardized processes for managing application development and their interactions [12]. It becomes challenging to guarantee data privacy and authentication for applications that employ diverse authentication mechanisms. The application layer encompasses various service domains, such as connected cars and healthcare, each of which must address its specific security threats and establish corresponding security measures. The Application Layer provides user access to IoT applications. Security measures can be integrated into the application layer by incorporating security policies in the functional architecture. Security concerns within the application layer can be mitigated through the implementation of security measures such as firewalls, antivirus software, and intrusion detection systems. These security issues within the application layer can be categorized as follows:

2.3.1. Malicious Code Injection:

Malicious code injection transpires when an attacker inserts malicious code into the system to pilfer user data. Hackers initiate this attack by exploiting vulnerabilities in the system's graphical user interface (GUI), either within the software or on the device itself, to execute actions such as Cross-Site Scripting (XSS) attacks, deploying Trojans that disrupt normal operations, or executing remote code. Unlike traditional attacks that can be deterred with antivirus tools, malicious code injection presents a challenge since it may either activate automatically or necessitate the attacker's intervention to initiate the attack on the system.

2.3.2. DoS Attack:

In recent times, Denial of Service (DoS) attacks have evolved to become more sophisticated than their earlier counterparts. These attacks employ a smokescreen tactic to carry out their malicious activities, deceiving users regarding the actual location of the attack. This strategy leads users to believe that the attack is occurring in a different part of the system, ultimately diverting their attention [13]. As a consequence, DoS attacks can place unencrypted sensitive user information into the hands of hackers. DoS attacks operate within the application layer, much like their actions across other layers, with the shared objective of disrupting service availability. DoS attackers possess the capability to undermine the availability of services or applications.

2.3.3. Spear-Phishing Attack:

The Spear-Phishing attack begins when an attacker attempts to launch an assault on users through emails sent to the victims. The goal is to entice victims into opening the email, with the aim of acquiring additional sensitive data from them. Spear-Phishing is a multi-step procedure that entails the attacker gathering information about a specific target or a group of targets.

2.4. Sniffing Attack:

A Sniffing attack happens when an attacker introduces a sniffer application into the system, allowing them to gather information about the network, ultimately compromising the system. Sniffing

can take various forms, including DNS poisoning, ARP poisoning, DHCP attacks, MAC flooding, and password sniffing [14]. Sniffers initiate their monitoring activities at the data link layer, and once the data link layer is compromised, other upper layers become involved in the sniffing process.

There are no universally applicable rules and standards in place to regulate the development and interactions of IoT applications. This lack of uniformity gives rise to several security concerns related to IoT applications. These applications employ diverse authentication mechanisms, making it challenging to ensure data privacy, identity verification, and seamless integration of various IoT applications. As the number of connected devices participating in information sharing within the IoT network increases, it places a growing burden on applications responsible for data analysis. This, in turn, affects the availability of services. When designing IoT applications, three critical considerations must be addressed: understanding how users interact with the application, managing the volume of data, and determining the system administrator. IoT application users should be equipped with tools that grant them control and management over their data disclosure preferences. Users should also possess knowledge about the usage, timing, and entities accessing their data.

Security measures within the Transport (Middle-ware) layer and application layer are categorized into four distinct areas: risk assessment, authentication, data security, and intrusion detection. Authentication serves as a safeguard against malicious users attempting to gain unauthorized access to the system by verifying their identities. The Middle-ware layer leverages various key technologies, such as cloud technologies, which can be susceptible to compromise and insider threats. Additionally, virtualization, a technology utilized in this layer, is exposed to data security threats and DoS attacks. Intrusion detection technologies function by raising alerts when any unusual events occur within the system. This is achieved by continuously logging and monitoring the activities of potential intruders. Intrusion detection technologies encompass various approaches, including data mining and anomaly detection. Risk assessment plays a pivotal role in justifying security strategies and enhancing the overall security structure. Encryption technologies can be deployed to prevent data theft and misuse, serving as a means to safeguard data and thwart malicious activities initiated by attackers and malicious users.

Conclusion

IoT technology significantly enhances communication capabilities and interactions among users, driving advancements in smart homes, agriculture, and other areas vital for modern living. Despite these advantages, the susceptibility of IoT systems to security breaches by malicious entities poses a severe risk, particularly in terms of accessing and compromising sensitive data. This reality highlights the urgent need to develop robust security strategies and measures to protect IoT infrastructures and the private data they handle. Security and privacy issues within IoT are critical concerns that vary widely in severity and nature, including both internal and external threats. Although the forms of these attacks differ, they uniformly threaten substantial damage. This research paper thoroughly reviews the literature on IoT security and privacy, addressing the specific security concerns within each layer of IoT architecture and detailing the types of security attacks and their preventive countermeasures. Additionally, it critically assesses the ongoing challenges in IoT security and privacy, emphasizing the need for continuous improvement in security practices to safeguard against evolving threats.

References

1. Singh, D., G. Tripathi, and A.J. Jara, “A survey of Internetof Things: Future Vision, Architecture, Challenges and Services,” 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, Mar 2014.

2. Alsamani, B., Lahza, H. A Taxonomy of IoT: Security and Privacy Threats // 2018 International Conference on Information and Computer Technologies (ICICT) / – USA, – March, – 2018, – p. 72-77,

3. Solangi, Z. A., Solangi, Y. A., Chandio, Aziz, Abd., Hamzah, M. S., Shah., A. The future of data privacy and security concerns in Internet of Things // 2018 IEEE International Conference on Innovative Research and Development (ICIRD, – Thailand, – May – 2018, – p. 1-4

4. Zhang, Z. K., Yi Cho, M. C., Wang, C. W., Hsu, C. W., Chen, C. K., Shieh, S. IoT Security: Ongoing Challenges and Research Opportunities // IEEE 7th International Conference on Service-Oriented Computing and Applications, – Japan, – November 17-19, – 2014, – p. 230-234.

5. Sarrab, M., S. Alnaeli, M. Critical Aspects Pertaining Security of IoT Application Level Software Systems // 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON Vancouver, BC, Canada, November 2018, – p. 960-964.

6. Alabaa, F. A., Internet of Things security: A survey / F.Alabaa, A.M.Othmana, I.A.T.Hashema, F.Alotaibi // – Amsterdam: Journal of Network and Computer Applications – 2017. April.Vol. 88, – p. 10-28.

7. Yang, Y. A Survey on Security and Privacy Issues in Internet-of-Things / Y.Yang, L.Wu, GYin, L.Li, H.Zhao // – New York: IEEE Internet of Things Journal – 2017. № 5. Vol.4. – p. 1250-1258.

8. Wang, Y., Attebury, G., Ramamurthy, B. A Survey of Security Issues In Wireless Sensor Networks // – USA: IEEE Communications Surveys & Tutorials – 2006. № 2. Vol.8, – p. 2-23.

9. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures // 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), – London, – December 14-16, – 2015, – p. 336-341.

10. Farooq, M.U. A Critical Analysis on the Security Concerns of Internet of Things (IoT) / M.U.Farooq, Waseem, M., Khairi,A., Mazha,r S // USA: International Journal of Computer Applications (0975 8887), – 2015. №7. Vol.111. – p. 1-6.

11. Khan, A. Y. Malicious Insider Attack Detection in IoTs Using Data Analytics / A.Khan, Y.R.Latif, S.Latif, S.Tahir, T.Saba // – New York: – 2020. January. Vol. 8. – p. 11743-11753.

12. Assiri, A., Almagwashi, H. IoT Security and Privacy Issues // Riyadh: 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), – April – 2018, – p. 1-5.

13. Ortiz, V. B. Internet of Things (IoT): A Survey on Privacy Issues and Security // – New York: International Journal of Scientific Research – 2015. №3. Vol.1. – p. 168-173.

14. Anu, P., Vimala, Dr.S. A survey on sniffing attacks on computer networks // 2017 International Conference on Intelligent Computing and Control (I2C2), – India, – June – 2017, – p. 1-5.

Xülasə
Məxfi məlumatların qorunması: əşyaların interneti (IoT) sistemlərində təhlükəsizlik və məxfilik problemlərinin ətraflı təhlili
Elşən Tanrıverdiyev

Tədqiqat işinin məqsədi əşyaların interneti (IoT) sistemləri daxilində təhlükəsizlik və məxfilik problemlərinin hərtərəfli təhlil edilməsi, onun müxtəlif təbəqələrində – qavrayış, şəbəkə, nəqliyyat və tətbiqetmədə boşluqların müəyyənləşdirilməsi və bu risklərin azaldılması məqsədilə strategiyanın hazırlanmasıdır. Məqsədə müvafiq olaraq, tədqiqat işində əvvəlcə hər bir IoT təbəqəsi daxilində əsas təhlükəsizlik təhdidlərini müəyyən etmək və məxfilik problemlərini kateqoriyalara ayırmaq, mövcud problemləri və həlli yollarını anlamaq üçün mövcud ədəbiyyatların nəzərdən keçirilməsi kimi vəzifələr qarşıya qoyulur. Əlavə vəzifələrə ümumi hücum vektorlarının təhlili və simulyasiyalar, real dünya nümunələri vasitəsilə təklif olunan təhlükəsizlik tədbirlərinin effektivliyinin qiymətləndirilməsi daxildir.

Təhlükəsizlik həllinin effektivliyini yoxlamaq və proqnozlaşdırmaq üçün nəzəri və müqayisəli təhlil, eksperiment və simulyasiya modelləşdirmə də daxil olmaqla, müxtəlif tədqiqat metodlarından istifadə edilmişdir.

Aşağıdakı nəticələr əldə edilmişdir: Hər bir IoT təbəqəsindəki əsas boşluqlar aşkar edilmiş, potensial hücum vektorlarının geniş spektri müəyyən olunmuşdur. Mövcud təhlükəsizlik tədbirlərindəki əhəmiyyətli çatışmazlıqlar aşkarlanaraq uyğun təkmil həllər təklif olunmuşdur.

Tədqiqatın yekun nəticəsi olaraq, IoT sistemləri üçün nəzərdə tutulmuş tövsiyə olunan təhlükəsizlik tədbirləri və ən yaxşı təcrübələr işlənib hazırlanmışdır. Bu tövsiyələr laylı təhlükəsizlik protokollarını, təkmil şifrələmə üsullarını və dinamik audentifikasiya mexanizmlərini əhatə edir. Tədqiqatda, həmçinin daha davamlı və təhlükəsiz IoT mühitlərinin inkişafını təşviq etmək məqsədilə təhlükəsizliyin qiymətləndirilməsi və uyğunlaşdırılması üçün həllər təklif edilir. Qeyd olunan kompleks yanaşmanın yalnız mövcud təhlükəsizlik məsələlərinə deyil, həm də gələcək təhdidlərdən qorunmaq üçün effektivliyi qeyd olunmuşdur.

Açar sözlər: əşyaların interneti, IoT Sistemləri, IoT təhlükəsizlik problemləri, IoT təhlükəsizlik hücumları

Аннотация

Защита конфиденциальной информации: комплексный анализ вопросов безопасности и конфиденциальности в Системах Интернета Вещей (IoT)

Эльшан Танрывердиев

Это исследовательская работа проводит тщательный анализ проблем безопасности и конфиденциальности в системах Интернета вещей (IoT), целью которого является выявление уязвимостей на различных слоях IoT – восприятие, сеть, транспорт и приложения, и разработка стратегий для снижения этих рисков. Исследование начинается с категоризации основных угроз безопасности и проблем конфиденциальности на каждом слое инфраструктуры IoT, за которой следует всесторонний обзор существующих исследований по безопасности IoT для понимания текущих вызовов и решений. Дополнительные задачи включают анализ распространенных векторов атак и оценку эффективности предложенных мер безопасности посредством симуляций и исследований реальных случаев.

Были использованы различные методы исследования, включая систематические обзоры литературы, кейс-стади, экспериментальные исследования и моделирование симуляций для тестирования и прогнозирования эффективности решений по безопасности.

Результаты исследования раскрывают ключевые уязвимости на каждом слое архитектуры IoT и составляют подробный каталог потенциальных векторов атак, классифицируя их по целям и характеру угроз. Он подчеркивает значительные недостатки в существующих мерах безопасности, подчеркивая необходимость в усиленных решениях, адаптированных к этим конкретным уязвимостям.

Итогом исследования стала разработка рекомендованных мер безопасности и передовых практик, специально предназначенных для систем IoT. Эти рекомендации включают в себя слоистые протоколы безопасности, усовершенствованные методы шифрования и динамичные механизмы аутентификации. Исследование также предлагает рамки для постоянной оценки и адаптации мер безопасности, направленные на создание более устойчивых и безопасных сред IoT. Этот комплексный подход не только решает текущие проблемы безопасности, но и подготавливает к будущим угрозам.

Ключевые слова: интернет вещей, интернет вещей системы, проблемы безопасности интернета вещей, атаки на безопасность интернета вещей.

Məqalə redaksiyaya daxil olmuşdur:29.01.2024
Təkrar işlənməyə göndərilmişdir:12.02.2024
Çapa qəbul edilmişdir: 02.04.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 133-140
MİLLİ TƏHLÜKƏSİZLİK ***NATIONAL SECURITY***

UOT 004 DOI: 10.30546/mk.2024.2.049.

НОРМАТИВНО-ПРАВОВАЯ БАЗА, РЕГЛАМЕНТИРУЮЩАЯ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В АРМЕНИИ

Илаха Чирагова
Центр имени Топчибашева
ilaha.chiragova@gmail.com

Аннотация. Первые сравнительно серьезные сигналы, сопутствующие развитию нормативно-правовой базы, начали поступать в 2001 году с объявлением правительства сферы информационных технологий приоритетом экономического развития страны. Затем определенный промежуток в законодательстве были приняты общеустановленные нововведения. С приходом к власти Серж Саргсяна начались происходить изменения, что с еще более ускоренными темпами было продолжено правительством Никола Пашиняна. В данной статье проводится многосторонний анализ нормативно-правовой базы, регламентирующей информационные технологии в Армении. В исследовании вкратце охватывается процесс формирования нормативно-правовой базы в вышеперечисленной сфере, анализируются приоритетные сектора развития, наряду с нововведениями. Отдельно дается краткий обзор предпринятых шагов в секторе электронного правительства, цифровизации, кибербезопасности, военной промышленности и космической деятельности. Статья завершается описанием текущей правительственной программы 2021–2026 и планируемыми армянским правительством шагами. Анализ позволяет сделать вывод о чрезмерном интересе армянского правительства к различным секторам информационных технологий, ибо законодательство является явным тому примером. В результате укрепления законодательной базы Армения стремится достичь создание рабочих мест, инновационной и конкурентоспособной экономики, приток инвестиций, развитие научного и технического потенциала, способного отразится на качестве вооруженных сил и усовершенствовании военной промышленности.

Ключевые слова: информационные технологии, кибербезопасность, военная промышленность, Армения, нормативно-правовая база, закон

Введение

Нормативно-правовая база, имея регулирующую функцию, устанавливает конкретные правила поведения, регламентирует и стимулирует развитие деятельности определенных, в данном контексте, сфер. Основная нормативно-правовая база Армении в сфере информационных технологий стала сформировываться в начале текущего столетия. Первоначально она несла примитивный характер, регулируя лишь законодательную базу в узком смысле, что начало постепенно меняться с приходом к власти Сержа Саргсяна. Несмотря на наличие толчка развития, нормативно-правовая база все еще не достигала того уровня проработки, которая была зафиксирована у стран-членов Евразийского экономического союза. Ситуация стала относительно меняться с приходом Никола Пашиняна, нацеленного на развитие данной сферы: нормативно-правовая база начала расширяться, правовые документы были более детально описаны, новые сектора были освоены.

Правительство Никола Пашиняна намерено продолжает способствовать развитию инновационной системы и комплексному инвестированию в различные сферы. Ими же планируется разработать стратегию развития сектора высоких технологий, направленную на увеличение объемов сектора высоких технологий, повышение вовлеченности в отрасль, обеспечение роста доходов от операционной деятельности компаний и увеличение доли этого показателя по отношению к ВВП, коммерциализации инновационных идей, развитию

предпринимательства, технологическому прогрессу и широкому применению технологических решений в экономике и общественной сфере.

Цель данной статьи – предоставление всеобъемлющей картины нормативно-правовой базы Армении в сфере информационных технологий. В статье будут рассмотрены законодательные проекты, документы и нормативно-правовые акты, регулирующие тот или иной сектор, на базе которых вырабатывается основная политика армянского правительства в ИТ сфере. Учитывая количество документов, в исследовании изучены законоемкие документы, отражающие основные положения касательно тот или иной сферы. Нормативно-правовая база была исследована методом изучения документов. Статья начинается с анализа формирования нормативно-правовой базы в сфере информационных технологий, затем в более узком спектре изучаются электронное правительство, цифровизация, кибербезопасность, военная промышленность, космическая деятельность, а также правительственная программа 2021–2026 годов и планируемые шаги.

Сформирование нормативно-правовой базы

В опубликованном в июне 2001 года концептуальном документе армянское правительство открытым текстом объявило сферу информационных технологий приоритетом экономического развития страны [1]. В соответствии с указом президента правительство создало Совет поддержки развития ИКТ – консультативный орган под председательством премьер-министра, который стал коммуникационной платформой для заинтересованных сторон, позволяющей предлагать и обсуждать вопросы в области политики и регулирования телекоммуникаций [2]. Затем в 2003 году правительство запустило инициативу “Электронная Армения”. Однако прогресс в реализации инициативы и концептуального документа был прерван парламентскими выборами в 2003 году, вслед за этим и президентскими выборами в 2004 году. С тех пор в возобновлении обеих инициатив был достигнут незначительный прогресс.

Летом 2008 года правительство утвердило десятилетнюю Концепцию развития сектора ИКТ в Армении, которая также содержит концептуальные положения и график формирования электронного общества в РА, основанные на анализе и сравнении международных практик. В отличие от Концептуального документа 2001 года, в первом изложены краткосрочные и долгосрочные планы действий с фиксированными графиками для развития информационного общества и обеспечения конкурентоспособности сектора. В концепции зафиксированы векторы модернизации сферы информационных технологий. Здесь же описаны потенциальные препятствия и шаги к их устранению, а также дальнейшие интенции (финансовые механизмы, технологичное образование, инфраструктура, привлечение капиталов, электронное управление, наращивание электронной науки, а также оснащение армянского населения технологическим оборудованием и недорогим интернетом). Что касается интернета, в 2013 году была разработана концепция о “Принципах управления интернетом”, где началось формирование политики и основных принципов управления интернетом [3]. Во исполнение распоряжений с 2014 года во главе с заместителем министра транспорта, коммуникаций и информационных технологий начал свою деятельность неформальный консультационный орган – Совет по управлению интернетом. Советом регулировались вопросы киберпространства, новые и старые законодательства, конструирование определенной политики. Являясь, как и Совет поддержки развития ИКТ, коммуникационной платформой, Совет по управлению интернетом состоял из чиновников, гражданского общества и лиц частного сектора.

Электронное правительство

База для публичного доступа к данным правительства с соответствующим законодательством, директивой и решениями, была закреплена в сентябре 2003 года законом “О свободе информации”. Учитывая необходимость разработки комплексной программы

формирования электронного общества в РА, 25 февраля 2010 года была разработана и принята “Концепция формирования электронного общества в Республике Армения”. Согласно видению электронного правительства Республики Армения, основной целью предоставления электронных услуг является улучшение предоставления государственных услуг пользователям и сделать их доступными и удобными для каждого гражданина. Координация электронного правительства велась на основе программных документов вплоть до 2014 года, пока правительство не разработало особый нормативный документ “Стратегическая программа развития электронного правительства (2014–2018)”, включающий единое видение с созданием основ рамочного взаимодействия, модификацию нормативно-правовой базы, конструирование совместной технологической платформы, наряду с учреждением портала для электронного правительства [4].

Согласно постановлению от октября 2012 года “об утверждении внедрения сайта **e-gov.am**”, государственные электронные услуги были объединены и электронное правительство начало свою деятельность. Основными ответственными органами электронного правительства на тот момент являлись созданный в 2009 году Центр внедрения инфраструктуры электронного правительства (EKENG) и Министерство экономики, под председательством которого функционировал центр. В конечном счете была создана система электронных инструментов правительства (**www.e-gov.am**). Платформа объединяет услуги, включая недвижимость (**www.e-cadastre.am**), государственные платежи (**www.e-pays.am**), электронную регистрацию организаций (**www.e-register.am**), электронную подачу налоговой отчетности (**file-online.taxservice.am**) электронные системы, единую платформу для электронных запросов (www.e-request.am). Существуют также другие системы, обслуживающие процессы получения разрешений на строительство (**www.e-permits.am**), единый электронный реестр лицензий РА (**www.e-license.am**) и национальной стратегии по правам человека (**e-rights.am**).

Концепция внедрения электронного правительства 2014 года была сформулирована на основе фундаментального, к тому времени, постановления от 2014 года “Стратегическая программа перспективного развития Республики Армения на 2014–2025 годы”. Относительно сферы информационных технологий, стратегическая программа предусматривает содействие ИТ компаний, сконцентрированных на инновациях, налоговой политики для упрощения экспорта, создание инфраструктур, включая инкубаторы, технопарки, а также соответствующих лабораторий.

Цифровизация

После принятия закона “Об электронном документе и электронной цифровой подписи”, важным документом в развитии цифровизации стала “Стратегия цифровизации Армении (2021–2025 гг.)”. В общем, стратегия цифровизации построена на трех различных направлениях: государство, экономика, общество. В область государственного управления входят основные институты цифровизации, единые стандарты, единая структура, интеграция, доступность цифровых систем, реестр цифровых систем. К экономическому направлению приписывают повышение осведомленности о цифровых технологиях в частном секторе, программа продвижения использования цифровых решений, обзор законодательства в области цифрового бизнеса, поощрение и устранение барьеров для электронной коммерции, цифровизация промышленности. Изучив практику различных стран, армянское правительство в общественное направление вносит включение курса цифровых навыков в систему общего образования, интерактивного обучения пожилых людей и лиц, не обладающих передовыми технологическими навыками, учебную программу по киберграмотности, информацию о доступных цифровых платформах [5].

Ранее в результате отсутствия единой политики и единых подходов к цифровой трансформации в государственной системе цифровизация, в основном носила децентрализованный характер с частичными решениями. Предыдущие инициативы цифрового

развития Армении в целом не предусматривали определение общих стандартов и принципов для цифровых платформ. Одной из возможных причин упомянутой проблемы было отсутствие соответствующего отдела или структуры для поддержания ключевых принципов, определяющих и контролирующих разработку и функционирование систем. В результате многие цифровые платформы в настоящее время разрабатываются на основе разных принципов, как с точки зрения операционных систем, так и технологий программирования, баз данных, управления ими и доступа к ним. Для ряда систем отсутствует соответствующая документация и стандарты безопасности. Большинство проектов выполняются и поставляются без архитектуры программного обеспечения, плана тестирования, дизайна пользовательского опыта, руководства пользователя и т. д.

В соответствующем документе так же повествуется о ряде проблем, существующих в процессе цифровизации внутренних функций государства. На данный момент государственные органы используют около 300 цифровых платформ и сайтов. Одна из проблем заключается в том, что многие из внутренних цифровых систем не связаны напрямую с госуслугами, что является препятствием для предоставления быстрых и эффективных госуслуг. Несмотря на наличие внутренних систем, многие сферы государственного управления еще не цифровизированы, например, управление проектами, финансовыми потоками, человеческими ресурсами, складами и товарно-материальными запасами и т.д. Действующая система электронного документооборота построена просто по принципу передачи документов через цифровую платформу с сохранением ее бумажной логики.

Кибербезопасность

Официально видение об информационной безопасности в Армении начало выстраиваться с 2009 года, в этом же году оно легально было закреплено соответствующей концепцией. Поддержание и стимулирование кибербезопасности нашло свое место в “Национальной программе по повышению эффективности борьбы с организованной преступностью” от 2010 и “Национальной стратегии о борьбе с терроризмом” от 2012 года, а также соответственно в стратегическом плане 2014 года. В 2017 году представлена программа об усовершенствовании систем ИБ. Среди компетентных органов, ответственных за кибербезопасность, Служба национальной безопасности Республики Армения, наряду с Полицией и Министерством обороны.

Для преодоления вызовов в сфере кибербезопасности Министерство высокотехнологической промышленности планирует разработать комплексную политику и план действий по кибербезопасности, которые будут включать создание центра кибербезопасности, управление рисками и механизмы быстрого реагирования в ходе стихийных бедствий, чрезвычайных ситуаций и войны. Кроме того, для того, чтобы следовать постоянному развитию, изменениям технологий и угрозам кибербезопасности ключом к достижению соответствующей модернизации армянское правительство считает тесное межведомственное сотрудничество и сотрудничество с частным сектором, межгосударственное сотрудничество и членство в международных структурах безопасности, локализация международного опыта, а также учет международных стандартов кибербезопасности.

Военная промышленность

Основным и первоначальным законом о военно-промышленном комплексе является закон “О промышленном комплексе”. Целью закона является создание основ стабильной, системной, правовой, экономической, социальной, а также научной и научно-технической кадровой политики военно-промышленного комплекса Республики Армения и реализация амбициозных государственных и военно-технических программ вооружения Вооруженных Сил и других войск Армении. Закон регулирует цели, принципы и задачи военно-промышленной политики в

Республике Армения, отношения между государством и другими органами и организациями, входящими в состав оборонно-промышленного комплекса, порядок формирования и размещения государственного заказа на военные нужды, методика регулирования цен на товары, работы и услуги [6]. С приходом к власти Никола Пашиняна, в закон несколько раз были внесены определенные поправки.

Космическая деятельность

Целью закона “О космической деятельности” от 2020 года является развитие экономики, науки, технологий в сфере космической деятельности, укрепление безопасности, расширение международного сотрудничества с Республикой Армения [7]. По закону принципами космической деятельности являются содействие поддержанию международной безопасности и мира посредством использования достижений и технологий космической науки; обеспечение безопасности космической деятельности и охраны окружающей среды; обеспечение равноправного и взаимовыгодного сотрудничества Республики Армения в сфере космической деятельности; обеспечение международной ответственности Республики Армения в области космической деятельности; обеспечение рационального сочетания и сбалансированного развития космической техники, используемой в научных, социально-экономических целях. В законе так же освещены экономические условия, государственное регулирование космической деятельности, космические средства, техника, и инфраструктура, безопасность космической деятельности, возмещение убытка и государственный контроль [8]. В этом контексте стоило бы отметить и другие юридические документы, регулирующие космическую деятельность, а точнее постановление правительства РА об утверждении порядка использования (эксплуатации), обработки, создания, испытаний космической техники и сооружений, наряду с постановлением об определении порядка использования космической техники и объектов, являющихся вышедшей с эксплуатации государственной собственностью [9].

Правительственная программа 2021–2026 годов и планируемые шаги

В настоящее время одним из текущих юридических нормативно-правовых актов является программа 2021–2026 годов, при содействии которой армянское правительство намерено реализовать определенные шаги в сфере высоких технологий [10]. В программе отмечены качественное и количественное улучшение технологического образования в сфере высоких технологий, постоянное увеличение возможностей по привлечению необходимых инвестиций в высокотехнологичные компании (стартапы) и привлечению финансовых инструментов для обеспечения их дальнейшего развития и экспорта на мировой рынок, в том числе через программы государственной поддержки. Среди шагов перечисляются реализация мер, направленных на содействие иммиграции технологического потенциала, обеспечение применения технологических решений в высокотехнологичном секторе и во всех отраслях экономики путем финансирования стартап-компаний в рамках грантовых программ, реализация образовательных и акселерационных программ с целью обеспечения притока знаний и навыков из технологических, образовательных, исследовательских центров мира, содействия развитию технологического сектора, привлечения инвестиций.

В течение 2021–2026 годов планируется улучшение возможностей существующих технологических центров (технопарков, акселераторов и инкубаторов) в Армении, а также создание новых центров в регионах Республики Армения в целях территориального сбалансированного развития, в том числе на основе международного сотрудничества. В этом контексте имеется в виду создание и развитие специальных инженерно-промышленных зон на примере “Инженерного города”.

В программе предусматривается обеспечение и продвижение присутствия армянского высокотехнологичного сектора (компаний) в мире, в том числе на престижных международных выставках и мероприятиях, содействие эффективному сотрудничеству технологических компаний и университетов для поступательного развития сектора путем подготовки новых специалистов и предоставления возможности переспециализации специалистам других областей, а так же реализация программ, направленных на развитие бизнес-возможностей компаний отрасли.

Заключение

Исходя из рассмотренного, можно сделать выводы о приоритетном восприятии сферы информационных технологий, в частности кибербезопасности, космической деятельности, цифровизации, электронного правительства, военной промышленности. Правительство Армении намерено продолжать усовершенствование нормативно-правовой базы, конструирование новой базы в сфере искусственного интеллекта на основе освоения международного опыта, сотрудничества извне и научно-исследовательского потенциала Армении. Власти Армении надеются, что разработанная правительством политика поощрения инвестиций и создание совместных предприятий также создадут благоприятную среду для развития сектора. Эта политика, ссылаясь на последних, основана на совершенствовании налоговых и административных процедур, привлечении иностранных инвестиций, а также государственном, частном и международном сотрудничестве. Следуя правительственной программе, армянское правительство поставило перед собой задачу трудоустроить к 2026 году около 35 тысяч человек в секторе высоких технологий и увеличить оборот сектора до 500 млрд драмов, что составит 6–7% ВВП Армении. По данным 2020 года этот показатель составляет 4%. В Армении надеются на то, что, таким образом, в стране будет создано не менее 16 тысяч новых высокотехнологичных рабочих мест. Таким образом, с помощью усовершенствования нормативно-правовой базы, армянское правительство достигает несколько целей: достижение инновационной и конкурентоспособной экономики, приток инвестиций, создание рабочих мест, развитие научного и технического потенциала, способного отразится на качестве вооруженных сил и усовершенствовании военной промышленности.

Список использованной литературы

1. Պարսյան Ս., SS ոլորտը Հայաստանում միջին խավ է ձևավորում [էլեկտրոնային ռեսուրս] // – Երևան. – 2021.
URL: https://evnreport.com/arm/economy-arm/the-it-sector-in-armenia-is-forming-a-middle-class-2/
2. Տեղեկատվական Տեխնոլոգիաների զարգացմանն աջակցող խորհրդի անհատական կազմը հաստատելու մասին [էլեկտրոնային ռեսուրս] // 2003 թվականի հուլիսի 26-ի. – Երևան. – 2003. URL: https://www.irtek.am/views/act.aspx?tid=13969&sc=p16#p16
3. Հայաստանի Հանրապետության կառավարության նիստի արձանագրությունից քաղվածք, ինտերնետ կառավարման սկզբունքներին հավանություն տալու մասին [էլեկտրոնային ռեսուրս] // 2014 թվականի օգոստոսի 14-ի. – Երևան. – 2014.
URL: https://www.irtek.am/views/act.aspx?aid=77996
4. Էլեկտրոնային կառավարման զարգացման ռազմավարական ծրագիր (2014-2018 թթ.) [էլեկտրոնային ռեսուրս] // 2014 թվականի ապրիլի 10-ի. – Երևան. – 2014.
URL: https://www.e-gov.am/u_files/file/decrees/arc_voroshum/2104/04/14-44_1ardz.pdf
5. ՀՀ կառավարության որոշումը հայաստանի թվայնացման ռազմավարությանը, ռազմավարության միջոցառումների ծրագրին եվ արդյունքային ցուցանիշներին հավանություն տալու մասին [էլեկտրոնային ռեսուրս] // 2021 թվականի փետրվարի 11-ի. –Երևան. – 2021.
URL: https://www.arlis.am/DocumentView.aspx?DocID=149957

6. ՀՀ օրենքը ռազմարդյունաբերական համալիրի մասին [էլեկտրոնային ռեսուրս] // 2015 թվականի մարտի 25-ի. – Երևան. – 2015.
URL: https://www.arlis.am/DocumentView.aspx?DocID=178244
7. ՀՀ օրենքը տիեզերական գործունեության մասին [էլեկտրոնային ռեսուրս] // 2020 թվականի մարտի 6-ի.– Երևան. – 2020.
URL: https://www.arlis.am/DocumentView.aspx?DocID=140629
8. ՀՀ կառավարության որոշումը տիեզերական տեխնիկայի եվ օբյեկտների օգտագործման (շահագործման), մշակման, ստեղծման, փորձարկման կարգը հաստատելու մասին [էլեկտրոնային ռեսուրս] // 2022 թվականի օգոստոսի 24-ի. – Երևան. – 2022.
URL: https://www.arlis.am/DocumentView.aspx?docid=167818
9. ՀՀ կառավարության որոշումը շահագործումից հանված պետական սեփականություն հանդիսացող տիեզերական տեխնիկայի եվ օբյեկտների օգտագործման կարգը սահմանելու մասին [էլեկտրոնային ռեսուրս] // 2021 թվականի փետրվարի 4. – Երևան. – 2021.
URL: https://www.arlis.am/DocumentView.aspx?docid=149656
10. ՀՀ ազգային ժողովի որոշումը ՀՀ կառավարության ծրագրին հավանություն տալու մասին [էլեկտրոնային ռեսուրս] // 2021 թվականի օգոստոսի 26-ի. – Երևան. – 2021.
URL: https://www.arlis.am/documentview.aspx?docID=155373

Xülasə
Ermənistanda informasiya texnologiyaları sahəsini tənzimləyən normativ-hüquqi baza
İlahə Çıraqova

İlk, nisbətən ciddi siqnallar 2001-ci ildə hökumətin informasiya texnologiyaları sektorunu ölkənin iqtisadi inkişafı üçün prioritet elan etməsi ilə gəlməyə başladı. Daha sonra müəyyən müddət ərzində qanunvericilikdə ümumi müəyyən edilmiş yeniliklər qəbul edildi. Serj Sarkisyanın hakimiyyətə gəlməsi ilə dəyişikliklər müşahidə olundu və bunlar da Nikol Paşinyan hökuməti tərəfindən daha da sürətlə davam etdirildi. Bu məqalə Ermənistanda informasiya texnologiyalarını tənzimləyən hüquqi bazanın çoxşaxəli təhlilini təqdim edir. Tədqiqat yuxarıda qeyd olunan sahə üzrə normativ-hüquqi bazanın formalaşması prosesini qısa şəkildə əhatə edir, innovasiyalarla yanaşı, prioritet inkişaf sektorlarını təhlil edir. Ayrı-ayrılıqda elektron hökumət, rəqəmsallaşma, kibertəhlükəsizlik, hərbi sənaye və kosmik fəaliyyətlər sektorlarında atılan addımların qısa icmalı verilir. Məqalə hazırkı 2021 – 2026-cı illər hökumət proqramının və Ermənistan hökumətinin planlaşdırdığı addımların təsviri ilə bitir. Təhlil belə qənaətə gəlməyə imkan verir ki, Ermənistan hökuməti informasiya texnologiyalarının müxtəlif sektorları ilə həddindən artıq maraqlanır və qanunvericilik bunun bariz nümunəsidir. Qanunvericilik bazasının gücləndirilməsi nəticəsində Ermənistan yeni iş yerlərinin yaradılmasına, innovativ və rəqabətqabiliyyətli iqtisadiyyata, investisiya axınına, hərbi sənayeyə, silahlı qüvvələrin keyfiyyətinə və ordunun təkmilləşdirilməsinə təsir göstərə biləcək elmi-texniki potensialın inkişafına nail olmağa çalışır.

Açar sözlər: informasiya texnologiyaları, kibertəhlükəsizlik, hərbi sənaye, Ermənistan, normativ-hüquqi baza, qanun

Abstract
Regulatory framework for information technology in Armenia
Ilaha Chiragova

The first relatively serious signals set off to be received in 2001, with the government declaring the information technology sector a priority for the country's economic development. Then, for a certain period of time, generally accepted innovations were adopted in the legislation. With Serzh Sargsyan coming to power, changes began to occur, which was continued at an even more accelerated pace by the government of Nikol Pashinyan. This article provides a diversified analysis of the legal framework for information technology in Armenia. The study briefly covers the process of formation of the regulatory

framework in the above area, analyzes priority development sectors, along with innovations. Separately, a brief overview of the steps taken in the sectors of e-government, digitalization, cybersecurity, military industry and space activities is given. The article ends with a description of the current government program 2021-2026 and the steps planned to be implement by the Armenian government. The analysis allows us to conclude that the Armenian government is overly interested in various sectors of information technology, since legislation is a clear instance of this. As a result of strengthening the legislative framework, Armenia strives to achieve job creation, an innovative and competitive economy, an influx of investments, and the development of scientific and technical potential that can affect the quality of the armed forces and the improvement of the military industry.

Keywords: information technology, cybersecurity, military industry, Armenia, regulatory framework, law

Məqalə redaksiyaya daxil olmuşdur: 19.01.2024
Təkrar işlənməyə göndərilmişdir: 24.04.2024
Çapa qəbul edilmişdir: 25.04.2024

Milli Təhlükəsizlik və Hərbi Elmlər – National Security and Military Sciences
№2(10)/2024, səh. 141-148

HƏRBİ TƏBABƏT ***MILITARY MEDICINE***

UOT 578; 579 DOI: 10.30546/9878.2024.2.10.0037.

BAĞIRSAQ MİKROBİOTASININ ƏHƏMİYYƏTİ VƏ MÜASİR DİAQNOSTİKA ÜSULLARI

t.ü.f.d. Hafizə Mansurova
ATU Tibbi mikrobiologiya və immunologiya kafedrası
departament.microbiology@amu.edu.az

t.ü.f.d. Səidə Hacıyeva
ATU Tibbi mikrobiologiya və immunologiya kafedrası
saida.hadjiyeva@gmail.com

b.e.d. prof. Gülər Seyidova
ATU Tibbi mikrobiologiya və immunologiya kafedrası
departament.microbiology@amu.edu.az

b.e.d. prof. Emma Ağayeva
ATU Tibbi mikrobiologiya və immunologiya kafedrası
departament.microbiology@amu.edu.az

b.ü.f.d. Yeganə Baxışova
ATU Tibbi mikrobiologiya və immunologiya kafedrası
departament.microbiology@amu.edu.az

tibb xidməti polkovniki Şahin Süleymanov
Hərbi tibb fakültəsinin Tibbi profilaktika kafedrası
departament_medical_prophylaxis@amu.edu.az

Xülasə. Məqalədə bağırsaq mikrobiotasının insan orqanizmi üçün əhəmiyyəti və helikobakter pilorinin eradikasiya terapiyasından (HPET) sonra onda baş verən dəyişikliklər araşdırılır. Bağırsaq mikrobiotası immun sistemin formalaşması, aminturşu və vitamin sintezi, həzmi stimullaşdırmaq, patogen mikroorqanizmlərə qarşı kolonizasiya rezistentliyi və s. yaratmaqla insan sağlamlığı üçün zəruri olan bir çox fizioloji proseslərdə iştirak edir. Mikrobiomanın tərkibi metagenomik analiz üsulları – hədəflənmiş metagenomika (16s rRNT, 18s rRNT, ITS təyin olunur), ov tüfəngi metagenomikası, YNS və s. ilə öyrənildikdən sonra bu nəticəyə gəlinmişdir ki, HPET-dən sonra antibiotiklərin təsirindən bağırsaq mikrobiotasının tərkibində obliqat anaerobların (actinobacteria, bacteroides, akkermansia muciniphila, faecalibacterium prausnitzii və s.) sayının azalması və fakültativ aerob mikroorqanizmlərin artımında dəyişikliklər yaranır və disbioz baş verir. HP-nin rasional eradikasiya müalicəsi, alternativ fitopreparatlar, faq və ya probiotiklərlə aparılarsa, disbioz problemi vaxtında müəyyən edilərək aradan qaldırıla bilər.

Aparılmış araşdırmada HP infeksiyalarının antibiotik müalicəsindən bağırsaq mikroflorasının tərkibində bakteriyaların nisbi miqdarı sekvenirləşmə üsulu ilə əldə edilən məlumatlar əsasında müəyyən edilmişdir. Bifidobacterium, lactobacillus, escherichia və clostridium cinslərinin nümayəndələrinə təsirini müəyyən etmək üçün klinik materialın metagenomik analizindən istifadə edilmişdir. Məlum olmuşdur ki, bağırsağın mikrob tərkibi lactobacillus, escherichia və clostridium cinsinə aid olan bakteriyaların müalicədən sonra müvafiq olaraq xəstələrin 76,5%, 51,3% və 55,2%-də, yəni cəmi 0,5% dəyişiklik baş vermişdir. Bifidobacterium miqdarı xəstələrin 60,5%-də əhəmiyyətli dərəcədə azalmışdır. HPET bağırsaq mikroflorasında "açar" bakteriyalar olan əsas nümayəndələrinin sayına çoxistiqamətli təsir göstərir,bu baxımından müalicənin nəticələrinin risklərini proqnozlaşdırarkən antibiotiklərin istifadəsi zamanı nəzərə alınmalıdır.

Açar sözlər: bağırsaq mikrobiotası, microbioma, Helicobacter pylori, eradikasiya müalicəsi, metagenomik analiz

Giriş

Mikroorqanizmlər insan orqanizminin biokütləsinin əhəmiyyətli hissəsini təşkil edərək, onunla mürəkkəb simbiotik ekosistem yaradır. Bağırsaq mikrobiotasının normal tərkibi və funksiyası immun sistemin formalaşması, stimullaşması (bağırsağın selikli qişasının gücləndirilməsi/ß-defensin istehsalı), vitamin sintezi (B1, B2, B6, B12 və K), həzmi dəstəkləmək (həzm olunması çətin olan liflərin və karbohidratları parçalanması), bağırsağın epitel hüceyrələrində enerji mənbəyi kimi qısa zəncirli yağ turşularının (asetat və butirat) sintezi, iltihab əleyhinə və selikli qişalara qoruyucu (butiratlar və s.), detoksifikasiya (ekzogen maddələrin parçalanması və çıxarılması), aminturşu sintezi, patogen mikroorqanizmlərə qarşı kolonizasiya rezistentliyi və s. təsirlərlə insan sağlamlığı üçün zəruri olan bir çox fizioloji proseslərdə iştirak edir. Çox hissəsi bakteriyalar, göbələk, virus və protozoalardan ibarət olan bu populyasiya insan hüceyrələrindən 10 dəfə çox mikrob hüceyrəsinə, insan genomundan 150 qat daha çox genə malikdir. İnsan orqanizmində yaşayan kommensal, simbiotik mikroorqanizmlərin yaratdığı bu ekoloji birliyə "mikrobiota", bu mühitdə yaşayan "mikrobiota"nın sahib olduğu genetik materiala isə "mikrobioma" deyilir. Mikroorqanizmlərin stabil tərkibi bir yaşından sonra formalaşır. Onun tərkibinə ətraf mühit faktorları, antibiotiklər, pəhriz, genetika, iltihab, gigiyenik aspektlər, həyat tərzi və s. təsir göstərir. Onu da qeyd etmək lazımdır ki, bu gün ənənəvi nəcis analizlərini əvəz edən müasir molekulyar-genetik üsullarla bağırsaq mikrobiotasının tərkibini öyrənmək mümkündür. Bu analizlərlə mikrobiomanın hər bir fərd üçün spesifik və nisbi stabil olması müəyyən edilmişdir. "İnsanın mikrobiom proyekti" (Human Microbiome Project, 2007) sayəsində insanın sağlamlığında çox əhəmiyyətli rolu olan mikrobiota daim hərtərəfli öyrənilməkdədir [1; 2; 3; 4].

Mikrobiotanın taksonomiyası 5 əsas tipdən (phylum) – aktinobakteria (5%), proteobakteria (8%), firmicutes (>250 cins, 40-65%; lactobacillus, mycoplasma, bacillus, clostridium), bacteroides (~20 cins, 25-60%), verrucomicrobia (1%) ibarətdir. Fərdlərdə mikrobiotada rast gəlinən 160 bakteriya növündən 124-ü tədqiq edilmişdir [5].

Helikobakter pilori bakteriyası dünya əhalisinin təxminən yarısında mədədə bakteriya gəzdiriciliyə səbəb olur. Bu bakteriya qastrit, mədə xorası, adenokarsinoma və mədə selikli qişası ilə əlaqəli limfoid toxuma limfoması **(**mucosa-associated lymphoid tissue – MALT lymphoma) kimi xəstəliklərə səbəb olur. Dünya miqyasında yayılan patogen olmaqla yanaşı, H. pylori getdikcə daha yüksək antibiotiklərə davamlılıq nümayiş etdirir və bu bakteriyaya qarşı yeni terapevtik strategiyaların işlənib hazırlanması zərurətini yaradır. H. pylori-nin eradikasiya terapiyası (HPET) infeksiyadan dərhal sonra başlansa, mədə selikli qişasının zədələnməsi və yetkinlik dövründə mədə xərçənginin yaranma riski azala bilər. Bunu nəzərə alaraq, bir çox ölkələrdə ilkin profilaktik tədbir kimi gənclər arasında H.pylori-nin skrininqinə başlanılmışdır [6, 7].

HPET Maastrixt Konsensusunun protokoluna uyğun olaraq, kompleks bir sxemə əsaslanan amoksisillin 1000 mq, klaritromisin 500 mq, o cümlədən proton pompası inhibitoru və vismut subsalisilatının istifadəsi ilə həyata keçirilir. HPET tərkibində olan antibiotiklər bağırsaq mikrobiotasına təsir göstərərək onun tərkibinin kəmiyyət və keyfiyyətcə dəyişməsinə səbəb olur. Bu müalicənın bağırsaq mikrobiotasına təsirini müəyyən etmək üçün faydalı (obliqat, autoxton) və patogen bağırsaq mikroflorasının sayının qiymətləndirilməsi lazımdır [8; 9].

HPET aparılmış xəstələrdə diqqət bağırsaq mikroflorasının əsas nümayəndələrinin kəmiyyətcə miqdarına yönəldilir – bifidobacterium, lactobacillus, escherichia və clostridium – bakteriya cinsləri bağırsaq mikrobiotasının əhəmiyyətli hissəsini təşkil edir. Eyni zamanda faecalibacterium prausnitzii və akkermansia muciniphila kimi anaerob bakteriyalar mikrobiotanın ən böyük populyasiyasını təşkil edən növlərdir, adi üsullarla aşkarlana bilməsələr də, metabolik funksiyalarına və genoma görə ayırd edilirlər [10;11; 12, 13].

HPET sonra baş vermiş disbiozun diaqnostikası üçün əvvəllər istifadə edilən, klassik üsul bağırsaq tərkibinin (nəcisin) kultivasiyası aparılaraq öyrənilirdi. Lakin bağırsaqda yaşayan əksər mikroorqanizmlərin kultivasiyası üçün uyğun şərait yaratmaq mümkün olmadığından (xüsusilə, anaeroblar üçün) bu üsulun geniş istifadəsi mümkün deyil. Hazırda müasir molekulyar genetik

analizlərdən istifadə edərək, bağırsaq mikrobiotasında çoxlu sayda aerob və anaerob bakteriyaları və metabolik əlaqəli qruplarını müəyyən etmək mümkündür [14; 15; 16].

Tədqiqat işində tərəfimizdən H.pylori-nin eradikasiya terapiyasından sonra xəstələrdə bağırsaq mikrobiotasının tərkibindəki dəyişikliklər araşdırılmışdır.

Material və təhlil metodları

Bağırsaq mikrobiotasının tərkibini müəyyənləşdirmək üçün xəstələrdən 200 mq çəkidə nəcis nümunələri toplanılır və müxtəlif üsullarla müayinə edilir. Bu məqsədlə mikroskopik, kultural (aerob/anaerob NextGen kullturası), molekulyar-genetik (ZPR və s.), metabolit zülalların təyini (MS, ELISA), molekulyar texniki (Sanger, NGS) üsullar istifadə olunur. Metagenomik analizlərdən (MA) istifadə edərək, nümunələrdə mikrobiomanın tərkibindəki mikroorqanizmlərinin kultivasiya aparmadan nuklein turşusunu təyin etməklə birbaşa identifikasiyası mümkündür. Bu üsullardan istifadənin səbəblərindən biri mikrobiotada mövcud olan çoxlu sayda anaerob bakteriyalar qrupunun kultivasiya yolu ilə aşkarlanmasının çox zəhmətli və əksər hallarda mümkün olmamasıdır. Mikrobiomanın tərkibi aşağıdakı müasir üsullarla öyrənilir: mikrobiomun profilləşdirilməsi (16S rRNA, 18S rRNA, ITS2, funksional marker genləri), proqnozlaşdırılan funksional profilləşdirmə (16S rRNT gen məlumatlarına əsaslanaraq), ov tüfənginin metagenomikası, metatranskriptomika, filogenetik analiz. Nəcisdə yüksək miqdarda DNT izolyasiya inhibitorlarının olması səbəbindən DNT təcrid proseduru üçün adətən, xüsusi ekstraksiya dəsti (QIAmp DNA Stool Mini Kit, QIAgen, GERMANY) istifadə olunur. Mikrobiom məlumatlarının təhlili nümunələrdə metagenomik analizlər, müqayisəli taksonomik və funksional profillər öyrənilərək aparılır. Mikrob metatranskriptomikası – kompleks nümunə daxilində bir qrup mikroorqanizm tərəfindən kodlanan bütün RNT-lərin təhlilidir. Hədəflənmiş metagenomikada müəyyən konservativ (qorunan) bölgələr (16s rRNT, 18s rRNT, ITS (Internal Transcribed Spacer – Daxili transkripsiya aralığı)) zəncirvari polimeraza reaksiyası (ZPR) praymerləri ilə amplifikasiya olunur və ardıcıllıq təyin edilir. ~1500 bp uzunluğunda 16S rRNT geni ilə bakteriyaların identifikasiyası hazırda standartlaşdırılmış bir prosedurdur. Tək genin müxtəlifliyinə əsaslanan unimodal filogenetik analizdən fərqli olaraq, 16S rRNT geni, metagenomik analizi mikrob populyasiyasının multimodal genetik tərkibini sistemləşdirir və beləliklə, daha düzgün taksonomik təyin və genomik məlumat verir. Metagenomika mikrob populyasiyasının tərkibinin təkamül profillərini yaratmaqla yanaşı, funksiyanı filogenetika ilə əlaqələndirməyə kömək edir. 16S rRNT ardıcıllığı verilmiş nümunədə mövcud olan bakteriyaları müəyyən və müqayisə etmək üçün istifadə olunur [17; 18; 19].

Mikrobiotanın test panelinə aşağıdakılar daxildir – Enterotiplər: (Bacteroides, Prevotella, Ruminococcus, Lachnospiracea); Mucin-/Butirat əmələ gətirən: (Akkermansiya, Faecalibacterium); Mucin-/Butirat-/H2S- əmələ gətirən: (Akkermansia, Faecalibacterium, SRB (sulfat azaldan bakteriyalar)); Firmicutes-Bacteroidetes-Ratio (piylənmə, qıcıqlanan bağırsaq): Bacterioides, Bifidobacterium, Eubacterium; həzm pozğunluğu (mədə pozğunluğu): pankreatik elastaza, öd turşusu.

Klinik nümunələrdəki bakteriya genomları molekulyar-genetik texniki üsulu olan DNT sekvenirləşmə ilə aşkar edilir. Proses zamanı, xüsusilə bakteriyalardan gələn siqnallar qeydə alınır. Nümunədə neçə fərqli bakteriya genomunun olduğu 16S rRNT ardıcıllığı zəncirvari polimeraza reaksiyası (ZPR) ilə çoxaldılaraq təyin edilir. Bu üsullarla mikrobiomdakı spesifik genlər aşkarlanaraq funksional məlumatlar verilir və bakterial bioçeşidlilik təhlil olunur [19].

Sekvenirləşmə (ardıcıllıq) üsullarından olan ov tüfəngi (Shotgun) metagenomikası qeyri-diskriminantdır, mikroorqanizmlərin növ səviyyəsinə qədər kəmiyyətini, hətta taksonomiyasını müəyyən edir. İstənilən mikroorqanizm olan nümunə kompleksində bütün genlərin DNT ardıcıllığını təyin etməyə imkan verir. Mikrobiomun metagenomik ov tüfəngi ardıcıllığı nəticəsində bakteriyaların 16S rRNT bölgəsi üçün spesifik praymerlər hədəf bölgənin amplifikasiyası məqsədilə istifadə edilir. Uzun nukleotidin oxunması ilə daha dəqiq nəticələr əldə olunur. Massive Bioinformatics Illumina sistemlərindən istifadə edilərək, standartlaşdırılmış metagenomik analizlər, həmçinin Oxford Nanopore texnologiyası ilə sintez olunan uzun amplikonlarla analizlər yerinə yetirilir [20].

Yeni nəsil sekvenirləşmə (YNS (Next-generation sequencing – NGS)) genetik texnologiyası ilə bir nümunədən götürülən milyonlarla hissəyə ayrılmış DNT molekulunun hər bir hissəsinin eyni vaxtda paralel oxunmasına əsaslanır. Mikrobiomun tərkibinin öyrənilməsində uğurla tətbiq olunur. Hüceyrədəki DNT, RNT, mikro-RNT kimi molekullar haqqında böyük həcmdə məlumatların az xərclə, tez və paralel şəkildə əldə olunmasını təmin edir. Son zamanlar müasir YNS – metagenomik ov tüfəngi ardıcıllığı üsulu yavaş-yavaş klassik Sanger ardıcıllığını əvəz etmişdir. Həm 454/Roche, həm də Illumina/Solexa sistemləri çoxçeşidli mühitlərdə metagenomik nümunələrin təhlili üçün geniş şəkildə istifadə olunur [21; 22; 23].

ZPR üsulundan bakteriyaların kəmiyyətcə fərdi fərqlərini müəyyən etmək və klassik kultivasiya üsullarını dəstəkləmək üçün istifadə olunur. Xüsusi praymerlər vasitəsilə nuklein turşusu (spesifik hədəf) amplifikasiya olunaraq fərdlərin bağırsaq mikrobiotasında olan mikroorqanizmlərin növ və miqdarı təyin edilir. Nümunə toplanması, MutaCLEAN® Mag RNT/DNT köməyi ilə nukleotidlərin ekstraksiyası, (Real time PCR: MutaPLEX®) spesifik mikrobiomun amplifikasiyası (xüsusi Ct-dəyərləri bakteriya növləri) KƏV-nin hesablanması, növlərin nisbətinin müəyyən edilməsi (standart əyri ilə ölçülməsi, xüsusi nömrələri ilə ifadə edilməsi = KƏV) Xüsusi Diaqnostika Xidməti (Special Diagnostic Service – SDS) standartlarına uyğun aparılır [19].

İntestinal mikrobiomun təhlili nəticəsində insanın bağırsaq florasında yerləşən 3 əsas enterotip müəyyən edilmişdir. Enterotiplər qidalanma vərdişlərindən asılı olaraq fərqlənir, əsasən, Bacteriodes (enterotip 1), Prevotella (enterotip 2), ve Ruminococcus (enterotip 3) növlərindən ibarətdir. Tipik metabolik xüsusiyyətlərə görə enterotipin hansı bakterial qrupa aid olduğunu təyin etmək mümkündür.

Tədqiqatın təhlili

Beləliklə, standart məlumatlara istinad edərək, mikroorqanizmləri müəyyən etmək və terapevtik tədbirlər üçün fərdi tövsiyələr vermək mümkündür. Mikrobiom analizində Actinobacteria, Bacteroides, Firmicutes, Akkermansia muciniphila və nadir hallarda Fusobacterium filumunun tərkibi nəzərə alınır. Tipik klinik nümunələr bu taksonomik təsnifata uyğun olaraq, müəyyən edilir. Məsələn, Firmicutes/Bacteroidetes nisbətinin artması və ya Proteobacterium-un üstünlüyü müxtəlif klinik fərqlər yaradır. Bağırsaq mikrobiomu tədqiqatında "yaxşı bakteriyalar" diqqət mərkəzindədir. Sağlam bağırsaq üçün vacib bakteriyalardan biri olan Akkermansia muciniphila – Qram-mənfidir, anaerob, çöpşəkilli olub bağırsaq endotelində musini deqradasiya edərək, selikli qişadakı musin təbəqəsini yeniləyir və s. Bağrsağın digər normal mikrobiota nümayəndəsi faecalibacterium prausnitzii – Qram-müsbətdir, nəcisin 1% KBE = Bacteroides + Eubacteriumdan sonra üçüncü ən çox rast gəlinən bağırsaq bakteriyasıdır. Butirat sintez edir, iltihab əleyhinə (NF-kB-aktivasiya + IL-8 sintezini blokada etməklə) təsir göstərir [5; 24].

Nəticə

HPET tərkibinə amoksisillinin daxil olduqda xəstə qrupunun bağırsaq mikroflorasında Enterococcus spp., Enterobacteriaceae spp. və Peptostreptococcus spp.-nin kəmiyyətcə artması, həmçinin Enterobacteriaceae fəsiləsinin rezistent ştammlarının da çoxalması müşahidə edilmişdir. Anaerob mikrobiotadan Bifidobacterium spp., Clostridium spp. əhəmiyyətli dərəcədə azalır. Bəzi xəstələrdə maya göbələkləri (əsasən Candida albicans) aşkar edilir. Bəzi hallarda müalicədən 4 həftə sonra mikrobiotanın tərkibi bərpa olunur. Klaritromisin qəbul edən xəstələrdə Bifidobacterium spp., Clostridium spp., Bacteroides spp.-də azalma, Enterococcus spp.-nin miqdarında isə artma baş vermişdir. Amoksisillin və klaritromisinin Enterococcus spp. və Enterobacteriaceae spp.-yə qarşı minimum inhibisiya konsentrasiyası (MİK) nəcis nümunələrində əhəmiyyətli dərəcədə artmışdır. Bacteroides spp.-yə qarşı klaritromisinin MİK əhəmiyyətli dərəcədə artmış, amoksisillin üçün əhəmiyyətli dəyişikliklər müşahidə edilməmişdir. Bacteroides spp.-nin klaritromisinə davamlı ştammlarının tərkibində antibiotik terapiyası fonunda 2%-dən 76%-ə qədər artma müəyyən edilmiş, müalicədən 4 həftə sonra onların nisbəti 59% təşkil etmişdir. Müəlliflər belə qənaətə gəlirlər ki, H.pylori-

nin eradikasiya sxemlərinin bir hissəsi kimi antibakterial preparatların istifadəsi bütün mədə-bağırsaq traktının mikroflorasının tərkibinin dəyişməsinə gətirib çıxarır və disbiozla nəticələnir [25; 26; 27;28].

Həmçinin antibakterial müalicə aparıldıqda patogen bakteriyalar və onlarla yanaşı, normal mikroflora nümayəndələri arasında rezistentlik genləri yayılır. Məlum olduğu kimi, bakteriyalarda rezistentlik mutasiya və ya horizontal ötürülmə ilə qazanılır. Nəticədə bağırsaq mikroflorası rezistentlik genlərinin potensial rezervuarı olur. HPET tərkibində uzunmüddətli antibiotik müalicəsinin aparılması antibiotiklərə davamlı bakteriya ştammlarının seleksiyası ilə nəticələnir. HPET preparatları, antibiotiklər və proton pompası inhibitorları mədə-bağırsaq traktının mikrobiotasında uzunmüddətli disbiotik dəyişikliklərə səbəb olur. Qarşısını almaq üçün probiotiklərin, prebiotiklərin və mikrob metabolitlərinin (məsələn, butirat +) müalicə sxeminə daxil edilməsi eradikasiyanın mənfi təsirlərini azaldır [27]. Bundan əlavə, antibiotik istifadəsi məhdudlaşdırılmalıdır və alternativ eradikasiya vasitələri (məs.,bakteriofaq) [30], autoprobiotiklər [29], fitopreparatlar daxil olmaqla təbii agentlər, üsullar inkişaf etdirilməli və tədqiq olunmalıdır. Qeyd etmək lazımdır ki, H. pylori-nin litik faqlarının müəyyən edilməsi, onun aradan qaldırılması üçün alternativ yanaşma kimi faq terapiyasını nəzərdən keçirməyə imkan verir [30].

HPET zamanı bağırsaq mikrobiotasının tərkibinin öyrənilməsi, məsləhət və müalicə yanaşmaları fərdi şəkildə həyata keçirilir. Nəticə olaraq qeyd etmək lazımdır ki, H. pylori-nin rasional eradikasiyası aparılarsa, probiotiklər, faq və fitopreparataın istifadəsi ilə bağırsaq mikrobiotasının disbiozunun qarşısını almaq mümkündür.

İstifadə edilmiş ədəbiyyat siyahısı

1. The Human Microbiome Project Consortium. A framework for human microbiome research // – London: Nature. – 2012. № 486(7402). – p.215-221: [Electronic resource] / URL: http://dx.doi.org/10.1038/nature11209

2. Willem, M de Vos, Herbert, T, Matthias, Van Hul, Patrice, D Cani. Gut microbiome and health: mechanistic insights //– London. – Nature. – 2022. №71(5) – p.1020-1032. PMID: 35105664 PMCID: PMC8995832 DOI: 10.1136/gutjnl-2021-326789.

3. Turnbaugh, P.J. The Human Microbiome Project / P.J.Turnbaugh, R.E.Ley, M.Hamady, C.M.Fraser-Liggett, R.Knight, J.I.Gordon // – London: Nature – 2007 №449. – p. 804-810.

4. Jane Peterson, Susan Garges, Maria Giovanni, Pamela McInnes, Lu Wang, Jeffery A. Schloss, Vivien Bonazzi. The NIH HMP Working Group et al: The NIH Human Microbiome Project. In: Genome Res. 19, Published in Advance October 9, – 2009, – p.2317-2323, DOI:10.1101/gr.096651.109

5. Wu, G.D. Linking Long-Term Dietary Patterns with Gut Microbial Enterotypes / G.D.Wu, J.Chen, C.Hoffmann, K.Bittinger, Y.Y.Chen, S.A.Keilbaugh, M.Bewtra, D.Knights, W.A.Walters, R.Knight // – United States: Science. – 2011; №334. – p.105-108. DOI: 10.1126/science.1208344.

6. Cuomo, P., An Innovative Approach to Control H.pylori-Induced Persistent Inflammation and Colonization. Microorganisms / P. Cuomo, M.Papaianni, A.Fulgione, F.Guerra, R.Capparelli, , C.Medaglia // – PubMed. – 2020. №10; 8(8). DOI: 10.3390/microorganisms8081214.

7. Guo, Y, Cao, X-S, Guo, G-Y, Zhou, M-G, Yu B (2022) Effect of Helicobacter Pylori Eradication on Human Gastric Microbiota: A Systematic Review and Meta-Analysis. Front. Cell. Infect. Microbiol. 12:899248. DOI: 10.3389/fcimb.2022.899248. Meta-Analysis PMID: 35601105 PMCID: PMC9114356

8. Zagari, R.M, Romano, M., Ojetti, V., Stockbrugger, R., Gullini, S., Annibale, B., Farinati, F., Ierardi E, Maconi G, Rugge M, Calabrese C, Di Mario F. Guidelines for the management of Helicobacter pylori infection in Italy: The III Working Group Consensus Report 2015. Dig Liver Dis. – 2015 Nov;47(11):903-12. DOI: 10.1016/j.dld.2015.06.010. Epub 2015 Jul 6. PMID: 26253555

9. Malfertheiner P, Management of Helicobacter pylori infection-the Maastricht V / P.Malfertheiner, F.Megraud, C.A. O'Morain et al. // Gut.: BMJ journal – 2017. №66(1). – p. 6-30.

10. Luyi, Ch., Wenli, X., Allen, L., Jiamin, H. The impact of Helicobacter pylori infection, eradication therapy and probiotic supplementation on gut microenvironment homeostasis: An open-

label, randomized clinical trial –LondonEBioMedicine – 2018. №35. – p. 87-96. DOI: 10.1016/j.ebiom.2018.08.028. Epub 2018

11. Y.Guo, C.Xue-Shan, Yi Guo G., G.Z. Meng Y.Bo Effect of Helicobacter Pylori Eradication on Human Gastric Microbiota: A Systematic Review and Meta-Analysis./ – USA: Front Cell Infect Microbiology. American Society for Microbiology. – 2022 May 4:12:899248. DOI: 10.3389/fcimb.

12. Mao, L. Q., Zhou, Y. L., Wang, S. S., Chen, L., Hu, Y., Yu, L. M., et al. (2021). Impact of Helicobacter Pylori Eradication on the Gastric Microbiome. Gut pathogens 13 Article number: 60 (2021).

13. Bull, M.J., Plummer, N.T. Part 1: The Human Gut Microbiome in Health and Disease // Integrative Medicine: A Clinician's Journal, – 2014. №13(6). – p. 17-22.

14. Leonard, M.M. et all. Microbiome signatures of progression toward celiac disease onset in at-risk children in a longitudinal prospective cohort study / – USA: Proc Natl Acad Sci – 202. – 118 s.

15. Sandi, Y.J. Johnson, S. Metagenomics: a path to understanding the gut microbiome. – Germany. ISSN: 1432-1777, 0938-8990 (Print) – 2021; № 32(4). – p.2 82–296. DOI: 10.1007/s00335-021-09889-x

16. Almeida, A. A unified catalog of 204,938 reference genomes from the human gut microbiome. // – London: Nature Biotechnol – 2020. 39(1). – p. 105-114

17. Franzosa, EA. Species-level functional profiling of metagenomes and metatranscriptomes // – New York: Nature Methods. – 2018; №15. – p. 962–968. DOI: 10.1038/s41592-018-0176-y. Corpus ID: 53115339

18. Fox, G.E. Classification of methanogenic bacteria by 16S ribosomal RNA characterization. / G.E. Fox, L.J. Magrum, W.E.Balch, R.S.Wolfe, C.R. Woese // – USA: Proc. Nat. Acad. Sci. – 1977. №74. – p.4537–4541.

19. Shailesh, K.S., Z.Kasra, V.G. Natalya, K.M.Ashutosh. Microbiota Analysis Using Two-step PCR and Next-generation 16S rRNA Gene Sequencing. // – USA: PubMed. JVis Exp –2019 Oct. 15(152). DOI: 10.3791/59980.

20. Francesco Durazzi, Claudia Sala, Gastone Castellani, Gerardo Manfreda, Daniel Remondini & Alessandra De Cesare Comparison between 16S rRNA and shotgun sequencing data for the taxonomic characterization of the gut microbiota. Scientific Reports volume 11, Article number: 3030 (2021) C

21. Goig GA, Blanco S, Garcia-Basteiro AL, Comas I. Contaminant DNA in bacterial sequencing experiments is a major source of false genetic variability. BMC Biol. 2020; 18:24.

22. Gu W, et al. Rapid pathogen detection by metagenomic next-generation sequencing of infected body fluids. – Nature Med.– 2021. №2. – p.115-124.

23. Levy SE, Myers, RM. Advancements in next-generation sequencing // Annu Rev Genom Hum Genet. – 2016. №17. – p.95-115.

24. Manimozhiyan Arumugam, Jeroen Raes, Eric Pelletier, Denis Le Paslier, Takuji Yamada, Daniel R. Mende, Gabriel R. Fernandes, Julien Tap, Thomas Bruls et all. Enterotypes of the human gut microbiome Nature. 2011 May 12; 473(7346): – p.174-180.

25. Ye, Q., Shao, X., Shen, R., Chen, D., Shen, J. (2020). Changes in the Human Gut Microbiota Composition Caused by Helicobacter Pylori Eradication Therapy: A Systematic Review and Meta-Analysis. Helicobacter 25 (4), e12713. DOI: 10.1111/hel.12713

26. Schulz, C., Schutte, K., Koch, N., Vilchez-Vargas, R., Wos-Oxley, M. L., Oxley, A. P. A., et al. (2018). The Active Bacterial Assemblages of the Upper GI Tract in Individuals With and Without Helicobacter Infection. Gut 67 (2), 216–225. DOI: 10.1136/gutjnl-2016-312904

27. Yuan, Z., Xiao, S., Li, S., Suo, B., Wang, Y., Meng, L., et al. (2021). The Impact of Helicobacter Pylori Infection, Eradication Therapy, and Probiotics Intervention on Gastric Microbiota in Young Adults. Helicobacter 26 (6), e12848. DOI: 10.1111/hel.12848

28. Butorova, L.I., Ardatskaya, M.D., Osadchuk, M.A., Kadnikova, N.G., Lukianova, E.I., Plavnik, R.G., Sayutina, E.V., Topchiy, T.B., Tuayeva, E.M. [Comparison of clinical-metabolic efficacy

of pre- and probiotics in the conducted optimized protocols of eradication therapy of Helicobacter pylori infection] Ter Arkh. – 2020. № 92– p.64–69.

29. Suvorov, A., Karaseva, A, Kotyleva, M, Kondratenko, Y, Lavrenova, N, Korobeynikov, A, Kozyrev, P, Kramskaya, T., Leontieva, G., Kudryavtsev, I., Guo, D., Lapidus, A., Ermolenko, E. Autoprobiotics as an Approach for Restoration of Personalised Microbiota. – Front Microbiol – 2018.9:1869.

30. Angela B. Muñoz, Johanna Stepanian, Alba Alicia Trespalacios, and Filipa F. Vale. Bacteriophages of Helicobacter pylori Published online – 2020 Nov 12. – 2020. – 11 p.

Аннотация

Значение кишечной микробиоты и методы их современной диагностики

Хафиза Мансурова, Саида Гаджиева, Гюлер Сеидова, Эмма Агаева, Егана Бахышова, Шахин Сулейманов

В статье рассмотрено значение микробиоты кишечника для организма человека и изменения, происходящие в ней после эрадикационной терапии Helicobacter pylori (ГПЭТ). Кишечная микробиота участвует в формировании иммунной системы, синтезе аминокислот и витаминов, стимуляции пищеварения, колонизационной устойчивости к патогенным микроорганизмам и др. Она участвует во многих физиологических процессах, необходимых для здоровья человека. Изучив состав микробиома с помощью методов метагеномного анализа - таргетной метагеномики (16s рРНК, 18s рРНК, ITS), метагеномики дробовика, YNS и других, был сделан вывод, что облигатные анаэробы (Actinobacteria, Bacteroides, Akkermansia muciniphila, Faecalibacterium prausnitzii и др.) возникает уменьшение численности и изменение роста факультативных аэробных микроорганизмов и дисбактериоз. Если провести рациональное эрадикационное лечение HP альтернативными фитопрепаратами, фагом или пробиотиками, проблему дисбактериоза можно своевременно выявить и устранить.

В проведенных исследованиях на основании данных, полученных методом секвенирования, определяли относительное количество бактерий в микрофлоре кишечника при лечении антибиотиками HP-инфекций. Метагеномный анализ клинического материала был использован для определения влияния на представителей родов бифидобактерий, лактобактерий, эшерихий и клостридий. Установлено, что после лечения бактериями рода лактобацилл, эшерихий и клостридий микробный состав кишечника изменился у 76,5%, 51,3% и 55,2% больных, т.е. всего у 0,5%. Содержание бифидобактерий было достоверно снижено у 60,5% больных. ГПЭТ оказывает разнонаправленное влияние на количество ключевых представителей микрофлоры кишечника, что следует учитывать при применении антибиотиков при прогнозировании рисков исходов лечения.

Ключевые слова: микробиота кишечника, микробиом, Helicobacter pylori, эрадикационная терапия, метагеномный анализ.

Abstract

Importance of intestinal microbiota and modern diagnostic methods

Hafiza Mansurova, Saida Hajiyeva, Gular Seyidova, Emma Aghayeva, Yegana Bakhishova, Shahin Suleymanov

The article examines the importance of intestinal microbiota for the human body and the changes that occur in it after Helicobacter pylori eradication therapy (HPET). Intestinal microbiota is involved in the formation of the immune system, synthesis of amino acids and vitamins, stimulation of digestion, colonization resistance against pathogenic microorganisms, etc. It participates in many physiological processes necessary for human health. After studying the composition of the microbiome using metagenomic analysis methods - targeted metagenomics (16s rRNA, 18s rRNA, ITS), shotgun metagenomics, YNS, and others, it was concluded that obligate anaerobes (actinobacteria, bacteroides)

in the gut microbiota after HPET were affected by antibiotics, akkermansia muciniphila, faecalibacterium prausnitzii and others) decrease in number and changes in the growth of facultative aerobic microorganisms and dysbiosis occurs. If the rational eradication treatment of HP is carried out with alternative phytopreparations, phage or probiotics, the problem of dysbiosis can be identified and eliminated in time.

In the conducted research, the relative number of bacteria in the intestinal microflora from the antibiotic treatment of HP infections was determined based on the data obtained by the sequencing method. Metagenomic analysis of clinical material was used to determine the effect on representatives of the genera bifidobacterium, lactobacillus, escherichia and clostridium. It was found that after the treatment of bacteria belonging to the genus lactobacillus, escherichia and clostridium, the microbial composition of the intestine changed in 76.5%, 51.3% and 55.2% of patients, i.e. only 0.5%. Bifidobacterium content was significantly reduced in 60.5% of patients. HPET has a multidirectional effect on the number of key representatives of intestinal microflora, which should be taken into account when using antibiotics while predicting the risks of treatment outcomes.

Keywords: intestinal microbiota, microbiome, helicobacter pylori, eradication treatment, metagenomic analysis

Məqalə redaksiyaya daxil olmuşdur:20.12.2023
Təkrar işlənməyə göndərilmişdir:15.01.2024
Çapa qəbul edilmişdir: 19.02.2024

ELMİ MƏQALƏLƏRİN TƏRTİB EDİLMƏSİNƏ DAİR TƏLƏBLƏR

Təqdim edilən məqalələr jurnalın elmi istiqamətinə (hərbi-nəzəri elmlər, hərbi-xüsusi elmlər, hərbi təbabət, milli təhlükəsizlik) uyğun, aktual elmi problemlərə aid tədqiqatların ilk dəfə dərc olunması üçün nəzərdə tutulmuş materiallara malik olmalıdır. Məqalələr elektron variantda üç dildə (Azərbaycan, rus və ya ingilis) təqdim edilə bilər.

Məqalə MS WORD mətn redaktorunda 12-lik Times New Roman şrifti ilə yığılmalı, sətirlərarası məsafə 1 olmalıdır. Məqalənin strukturuna uyğun olaraq UOT, məqalənin adı, müəllif haqqında tam məlumat, xülasə, açar sözlər, giriş, əsas hissə (metodologiya və əldə olunan nəticələr), nəticə, istifadə edilmiş ədəbiyyat siyahısı, və əlavələr (ehtiyac olarsa) ardıcıl və sistemli şəkildə təqdim olunmalıdır. Məqalənin birinci səhifəsinin yuxarı sol tərəfində UOT indekslər göstərilməlidir. Mətnin əvvəlində məqalənin adı, müəllif(lər) haqqında məlumat (adı və soyadı tam şəkildə, elmi dərəcəsi, elmi adı və hərbi xidmətdə olanlar üçün hərbi rütbəsi), ORCİD indeks(lər) (əgər varsa), müəllif(lər)in işlədiyi müəssisə(lər), müəllif(lər)in elektron poçt ünvan(lar)ı, telefon nömrələri, həmçinin qonorar ödənilməsi üçün onların Azərbaycan Beynəlxalq Bankının hesab rekvizitləri göstərilməlidir. Bu məlumatlardan sonra məqalənin yazıldığı dildə 150 – 250 sözdən ibarət xülasə verilməlidir. Xülasədə tədqiqat işinin mahiyyəti, müəllif(lər)in aldıqları elmi nəticələr, işin elmi cəhətdən yeniliyi, tətbiqi əhəmiyyəti və s. yığcam şəkildə öz əksini tapmalıdır. Xülasədən sonra 5 – 8 sözdən ibarət açar sözlər göstərilməlidir.

Məqalənin mətni 6 – 12 səhifə (A4 formatında) həcmində olmalı, səhifələrdə isə bütün tərəflərdən 20 mm boş məsafə saxlanmalıdır. Səhifələrin nömrəsi səhifənin aşağı orta hissəsində qoyulmalıdır.

İllüstrasiyalar, cədvəllər, qrafiklər, diaqramlar mətndə yerləşdirilərkən (sayı birdən artıqdırsa) ardıcıl olaraq ərəb rəqəmləri ilə nömrələnməlidir. Cədvəl – cədvəlin yuxarısında sağdan (məs., Cədvəl 1), şəkil isə şəklin altında ortadan (məs., Şəkil 2.) və mətn hissədən (yuxarıdan və aşağıdan) 1 boş sətir buraxmaqla nömrələnməli, həmçinin elə yerləşdirilməlidir ki, məqaləni döndərmədən və ya saat əqrəbinin hərəkəti istiqamətində döndərdikdə onlara baxmaq, yaxud oxumaq mümkün olsun.

Mətndə verilən riyazi ifadələr MS Word proqramının düstur redaktoru (Equation) ilə tərtib olunmalıdır. Düstur sətrin ortasında, nömrəsi isə sağda mötərizədə yazılmalıdır.

Elmi məqalədə mövzu üzrə qısa təhlil verilməli, onun aktuallığı əsaslandırılmalı, həll olunmalı məsələlər açıqlanmalı və onların həlli yolları göstərilməli, əldə edilən nəticələr, işin elmi cəhətdən yeniliyi, tətbiqi əhəmiyyəti, iqtisadi səmərəsi və s. aydın şəkildə verilməlidir.

Elmi mənbələrə edilən istinadlar mətndə kvadrat mötərizədə verilməlidir (məsələn, [1] və ya [1, s.119]). Məqalənin sonunda verilən ədəbiyyat siyahısı istinad olunan ədəbiyyatların mətndəki ardıcıllığına uyğun şəkildə nömrələnməlidir. Ədəbiyyat siyahısında son 10 ildə nəşr edilmiş elmi məqalələrə, monoqrafiyalara və digər etibarlı mənbələrə üstünlük verilməlidir. İstinad olunan mənbənin biblioqrafik təsviri verilərkən Azərbaycan Respublikasının Prezidenti yanında Ali Attestasiya Komissiyası Rəyasət Heyətinin 29 oktyabr 2019-cu il tarixli qərarı ilə təsdiq edilmiş, 7 may 2021-ci il, 9 dekabr 2022-ci il tarixli qərarı ilə dəyişiliklər edilmiş "Dissertasiyanın tərtibi qaydası"nın tələbləri əsas götürülməlidir. "İstifadə edilmiş ədəbiyyat siyahısı"ndan sonra məqalənin və müəllifin adı, xülasə və açar sözlər (məqalənin yazıldığı dildən əlavə, yuxarıda qeyd edilmiş daha iki dildə) verilməlidir.

Redaksiyaya daxil olmuş məqalələrin çapa tövsiyə olunması jurnalın redaksiya heyətinin anonim rəyindən və plagiatlığın mövcudluğunun yoxlanılmasından sonra müəyyən edilir. Redaksiyaya təqdim olunan məqalə çapa tövsiyə olunmadıqda bu barədə müəllif(lər)ə məlumat göndərilir.

Jurnalın bir nömrəsində eyni müəllif(lər)in iki məqaləsi dərc oluna bilməz. Yuxarıda qeyd edilən tələblərə cavab verməyən məqalələr dərc edilmir və nəşr edilmiş məqalələrin əlyazmaları geri qaytarılmır.

ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ НАУЧНЫХ СТАТЕЙ

Представленные для публикации в журнале статьи должны соответствовать научным направлениям (военно-теоретические науки, военно-специальные науки, военная медицина, национальная безопасность) журнала и содержать материалы, отражающие результаты исследований научно-актуальных проблем, предназначенные для первичной публикации. Статьи

могут быть представлены в электронном варианте на одном из следующих языков: азербайджанском, русском или английском.

Статья должна быть набрана в текстовом редакторе MS WORD шрифтом Times New Roman 12, междустрочный интервал – 1.

Согласно структуре статьи УДК, название статьи, полная информация об авторе, аннотация, ключевые слова, введение, основная часть (методология и полученные результаты), заключение, список использованной литературы, и приложения (при необходимости) должны быть представлены последовательно и системно. Индексы УДК должны отображаться в левой верхней части первой страницы статьи. В начале текста указывается название статьи, сведения об авторе(ах) (полное имя и фамилия, ученая степень, ученое звание и воинское звание для военнослужащих), ORCID индекс(ы) (при наличии), учреждении(ях), в котором работает(ют) автор(ы), адрес(а) электронной почты автора(ов), номера телефонов, а также реквизиты счета Международного Банка Азербайджана для уплаты гонорара. После этой информации следует дать аннотацию объемом 150–250 слов на том языке, на котором написана статья. В аннотации следует отразить кратко: суть научно-исследовательской работы, научные результаты, полученные автором(ами), научная новизна работы, важность применения и т.п. После аннотации следует перечислить ключевые слова из 5–8 слов.

Текст статьи должен составлять 6–12 страниц (формата A4), страницы должны иметь свободное пространство по 20 мм со всех сторон. Номера страниц должны быть размещены в центре внизу страницы.

При размещении в тексте иллюстраций, таблиц, схем, диаграмм (если их количество больше одной) их следует нумеровать последовательно арабскими цифрами. Нумерация должна быть вверху таблицы справа (например, Таблица 1.), а на странице с рисунком – внизу посередине (например, Рисунок 2.) и 1 пустая строка от текстовой части (сверху и снизу). Изображение должно располагаться таким образом, чтобы его можно было рассматривать или читать не поворачивая, а также при повороте по часовой стрелке.

Математические выражения, приведенные в тексте, должны быть составлены с помощью редактора формул (Equation) программы MS Word. Формулу следует писать посередине строки, а их номера в скобках справа.

В научной статье должен быть дан краткий анализ темы, обоснована её актуальность, разъяснены решаемые вопросы и указаны пути их решения. Должны быть чётко представлены полученные результаты, научная новизна работы, её прикладная значимость, экономическая эффективность и т.п.

Ссылки на научные источники в тексте должны быть даны в квадратных скобках (например, [1] или [1, стр.119]). Список литературы, приведенный в конце статьи, должен быть пронумерован в соответствии с порядком цитирования литературы в тексте. В списке литературы предпочтение следует отдавать научным статьям, монографиям и другим достоверным источникам, опубликованным за последние 10 лет. При даче библиографического описания цитируемого источника, за основу должны приниматься требования «Правила составления диссертации», которые были утверждены решением Президиума ВАК при Президенте Азербайджанской Республики от 29 октября 2019 года и внесены и дополнены постановлением от 7 мая 2021-го, 9 декабря 2022-го годов. После «Списка использованной литературы» следует указывать название статьи и автора, аннотацию и ключевые слова (помимо языка, на котором написана статья, на двух других языках, упомянутых выше).

Рекомендация к публикации статей, входящих в редакцию, определяется после анонимного заключения редакционной коллегии журнала и проверки на наличие плагиата. Если поступившая в редакцию статья не рекомендуется к публикации, информация об этом отправляется автору(ам).

Две статьи одного и того же автора(ов) не могут быть опубликованы в одном номере журнала. Статьи, не соответствующие вышеуказанным требованиям, не будут опубликованы, а рукописи опубликованных статей не будут возвращены.

REQUIREMENTS FOR THE COMPILATION OF SCIENTIFIC ARTICLES

Submitted articles should have materials intended for the first publication of researches related to current scientific problems, in accordance with the journal's scientific direction (military-theoretical sciences, military-special sciences, military medicine, national security). Articles can be submitted electronically in three languages (Azerbaijani, Russian or English).

The article should be typed in MS WORD text editor with Times New Roman font 12, line spacing should be 1. Universal decimal classification (UDC) according to the structure of the article, ORCID indexes (if any) title of the article, full information about the author, abstract, keywords, introduction, main part (methodology and results obtained), conclusion, list of references used, and supplements (if needed) should be presented in a consistent and systematic manner. UDC indexes should be displayed on the upper left side of the first page of the article. At the beginning of the text, the title of the article, information about the author(s) (full name and surname, academic degree, academic title and military rank for those in military service), institution(s) where the author(s) works, e-mail address(es), telephone numbers, as well as account details of the International Bank of Azerbaijan for the payment of fees. After this information, a summary of 150-250 words should be given in the language in which the article was written. In the summary, the essence of the research work, the scientific results obtained by the author(s), the scientific novelty of the work, the importance of application, etc. should be concisely reflected. After the summary, keywords of 5-8 words should be listed.

The text of the article should be 6-12 pages (in A4 format), and the pages should have 20 mm free space on all sides. Page numbers should be placed in the lower middle of the page.

When placing illustrations, tables, charts, diagrams in the text (if the number is more than one), they should be numbered consecutively with Arabic numbers. Table – should be numbered at the top of the table from the right (e.g., Table 1), and the figure should be numbered from the middle (e.g., Figure 2.) and 1 blank line from the text part (top and bottom), and should be placed in such a way that the article is not rotated or clockwise so that they can be viewed or read when turned in the direction of the movement of the hand.

Mathematical expressions given in the text should be compiled with the formula editor (Equation) of the MS Word program. The formula should be written in the middle of the line, and the number should be written in parentheses on the right.

In a scientific article, a brief analysis of the topic should be given, its relevance should be justified, the issues to be resolved should be explained and their solutions should be indicated, the results obtained, the scientific novelty of the work, its application importance, economic efficiency, etc. should be given clearly.

References to scientific sources should be given in square brackets in the text (for example, [1] or, [1, p.119]). The list of references given at the end of the article should be numbered according to the order of the cited literature in the text. Scientific articles, monographs and other reliable sources published in the last 10 years should be preferred in the literature list. When giving the bibliographic description of the referenced source, the "Procedure for the preparation of the Dissertation" approved by the decision of the Presidium of the Higher Attestation Commission under the President of the Republic of Azerbaijan dated October 29, 2019, and amended by the decision dated May 7, 2021, December 9, 2022 requirements should be taken into account. The title of the article and the author, abstract and keywords (in addition to the language in which the article is written, in two other languages mentioned above) should be given after the "referenced literature list".

The recommendation for publication of the articles included in the editorial board is determined after the anonymous opinion of the editorial board of the magazine and after checking the presence of plagiarism. If the article submitted to the editors is not recommended for publication, information is sent to the author(s).

Two articles by the same author(s) cannot be published in one issue of the journal. Articles that do not meet the above-mentioned requirements will not be published, and manuscripts of published articles will not be returned.

Çapa imzalanıb 02.05.2025. Ofset çap üsulu.
Formatı 60/84 ⅛. Fiziki ç.v. 19. Sifariş 188.

Hərbi Nəşriyyatın mətbəəsində çap olunmuşdur.
Bakı, akad. Ş.Mehdiyev 144,
“Qızıl Şərq” hərbi şəhərciyi

№ 2(10)/2024