

Ali Hərbi Təhsil Sistemində Kibertəhlükəsizlik üzrə Təhsil və İnnovasiya

Müjkan Məmmədzaadə

Hərbi Elmi Tədqiqat İnstitutu, Bakı, Azərbaycan
mujkan@mail.ru

Xülasə— Məqalədə ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin müasir vəziyyəti, nəzəri əsasları və inkişaf istiqamətləri təhlil olunur. Kibertəhlükəsizliyin müasir hərbi təhlükəsizlik mühitində strateji rolu əsaslandırılır və bu sahədə kadr hazırlığının əhəmiyyəti vurğulanır. Beynəlxalq təcrübə, xüsusilə NATO və digər qabaqcıl ölkələrin modelləri nəzərdən keçirilir. Təhsildə innovativ yanaşmalar – simulyasiya mühitləri, süni intellekt, adaptiv təlim sistemləri və oyun əsaslı metodlar ətraflı təhlil olunur. Eyni zamanda, Azərbaycan ali hərbi təhsil sistemində mövcud vəziyyət, problemlər və çağırışlar müəyyənləşdirilir. Məqalədə kibertəhlükəsizlik üzrə təhsilin təkmilləşdirilməsi üçün praktik və elmi əsaslandırılmış təkliflər irəli sürülür və bu istiqamətin milli təhlükəsizlik baxımından əhəmiyyəti göstərilir.

Açar sözlər— kibertəhlükəsizlik; ali hərbi təhsil; innovativ təlim; kibertəlim poliçonu; milli təhlükəsizlik.

I. GİRİŞ

XXI əsr informasiya cəmiyyətinin formalaşması ilə xarakterizə olunur və bu proses dövlətlərin təhlükəsizlik sistemlərinə fundamental təsir göstərir. Rəqəmsallaşma, süni intellekt texnologiyalarının sürətli inkişafı, böyük verilənlər (big data) və bulud texnologiyalarının geniş tətbiqi nəticəsində həm mülki, həm də hərbi sahədə informasiya resurslarının rolu əhəmiyyətli dərəcədə artmışdır. Bu kontekstdə təhlükəsizlik anlayışı ənənəvi çərçivədən çıxaraq kiberməkani da əhatə edən kompleks və çoxşaxəli məzmun qazanmışdır. Artıq müasir təhlükəsizlik mühiti yalnız fiziki sərhədlərin qorunması ilə məhdudlaşmır, eyni zamanda dövlətlərin informasiya infrastrukturalarının, kommunikasiya şəbəkələrinin və rəqəmsal sistemlərinin mühafizəsini də özündə birləşdirir.

Hibrid müharibə konsepsiyasının yayılması kibertəhlükəsizlik sahəsinin aktuallığını daha da artırmışdır. Hibrid müharibələrdə ənənəvi hərbi vasitələrlə yanaşı, informasiya və kiberməkan üzərindən həyata keçirilən təsir mexanizmləri geniş istifadə olunur. Bu isə hərbi kadrların hazırlığında yeni bilik və bacarıqların formalaşdırılmasını zəruri edir. Müasir hərbi mütəxəssis yalnız fiziki əməliyyatları deyil, həm də informasiya və kiberməkanda baş verən prosesləri analiz etmək və idarə etmək qabiliyyətinə malik olmalıdır. Bu səbəbdən ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin təşkili strateji əhəmiyyət daşıyır.

Ali hərbi təhsil müəssisələri milli təhlükəsizlik sisteminin intellektual bazasını formalaşdırən əsas institutlar kimi çıxış edir. Bu müəssisələrdə kibertəhlükəsizlik üzrə tədrisin məqsədi yalnız nəzəri biliklərin verilməsi deyil, eyni zamanda praktik

bacarıqların, analitik düşüncənin və operativ qərarvermə qabiliyyətlərinin inkişaf etdirilməsidir. Xüsusilə real senarilər əsasında qurulan təlim modelləri, simulyasiya mühitləri və “cyber range” (kibertəlim poliçonu) texnologiyaları təhsilalanların peşəkar hazırlıq səviyyəsinin yüksəldilməsində mühüm rol oynayır. Bununla yanaşı, süni intellekt və maşın öyrənməsi kimi innovativ texnologiyaların tədris prosesinə inteqrasiyası kibertəhlükəsizlik sahəsində yeni imkanlar açır.

Azərbaycan Respublikasında da informasiya təhlükəsizliyinin təmin olunması dövlət siyasətinin prioritet istiqamətlərindən biri kimi müəyyən edilmişdir. Bu istiqamətdə qəbul edilmiş strateji sənədlər, o cümlədən “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası” kibertəhlükəsizlik sahəsində institusional və kadr potensialının inkişafını mühüm vəzifə kimi qarşıya qoyur [1]. Eyni zamanda, ölkədə rəqəmsal transformasiya proseslərinin sürətlənməsi kibertəhlükəsizlik üzrə ixtisaslaşmış kadrların hazırlanmasına olan tələbatı artırır.

Bununla belə, ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin təşkili bir sıra çətinliklərlə müşayiət olunur. Bu çətinliklərə texnoloji dəyişikliklərin sürəti, müasir tədris infrastrukturunun məhdudluğu, ixtisaslı pedaqoji kadrların çatışmazlığı və beynəlxalq təcrübənin yetərinə tətbiq olunmaması daxildir. Mövcud problemlərin aradan qaldırılması üçün təhsildə innovativ yanaşmaların tətbiqi, beynəlxalq əməkdaşlığın genişləndirilməsi və praktiki yönümlü təlim mühitlərinin yaradılması xüsusi əhəmiyyət kəsb edir.

Ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin inkişafı müasir təhlükəsizlik mühitinin tələblərinə adekvat cavab verən kadr hazırlığının təmin olunması baxımından mühüm elmi və praktiki əhəmiyyətə malikdir. Bu istiqamətdə aparılan tədqiqatlar və tətbiq olunan innovasiyalar gələcəkdə dövlətlərin müdafiə qabiliyyətinin gücləndirilməsinə mühüm töhfə verə bilər.

II. KİBERTƏHLÜKƏSİZLİK ANLAYIŞI VƏ HƏRBİ KONTEKSTDƏ ROLU

Kibertəhlükəsizlik anlayışı müasir informasiya cəmiyyətində ən vacib təhlükəsizlik kateqoriyalarından biri kimi formalaşmışdır və informasiya sistemlərinin, şəbəkələrin, proqram təminatının və məlumatların icazəsiz girişdən, dəyişdirilmədən və ya məhv edilmədən qorunmasını təmin edən texniki, təşkilati və hüquqi tədbirlər kompleksini əhatə edir. Ədəbiyyatda kibertəhlükəsizlik çox vaxt “informasiya təhlükəsizliyinin” tərkib hissəsi kimi təqdim olunsada, onun

əhatə dairəsi daha genişdir və kiberməkanda baş verən bütün təhlükə və riskləri özündə birləşdirir [2]. Beynəlxalq standartlara əsasən kibertəhlükəsizlik konfidensiallıq, bütövlük və əlçatanlıq (CIA triadası) prinsiplərinin təmin edilməsinə yönəlmiş fəaliyyətlər sistemidir [3].

Müasir dövrdə kiberməkan dövlətlərin fəaliyyətinin ayrılma tərkib hissəsinə çevrilmiş və ənənəvi əməliyyat mühitləri – quru, hava, dəniz və kosmosla yanaşı beşinci əməliyyat sahəsi kimi qəbul edilmişdir. ABŞ Müdafiə Nazirliyinin “Cyber Strategy” sənədində kiberməkanın hərbi əməliyyatların planlaşdırılması və icrasında strateji əhəmiyyət daşıdığı xüsusi olaraq vurğulanı [4]. Bu yanaşma göstərir ki, kibertəhlükəsizlik artıq yalnız texniki müdafiə mexanizmi deyil, həm də hərbi-strateji üstünlüyün əldə olunmasında əsas vasitələrdən biridir.

Hərbi kontekstdə kibertəhlükəsizliyin rolu bir neçə əsas istiqamətdə özünü göstərir. İlk növbədə, bu sahə hərbi informasiya sistemlərinin və komanda-idarəetmə (C2 – Command and Control) strukturlarının qorunmasını təmin edir. Müasir orduların fəaliyyətində qərarların qəbul olunması, əməliyyatların koordinasiyası və məlumat mübadiləsi tam şəkildə rəqəmsal sistemlərə əsaslandığından bu sistemlərin təhlükəsizliyi birbaşa əməliyyat effektivliyinə təsir göstərir. İkincisi, kibertəhlükəsizlik kəşfiyyat və əks-kəşfiyyat fəaliyyətində mühüm rol oynayır. Kibercasusluq vasitəsilə rəqib tərəfin informasiya resurslarına çıxış əldə etmək və ya öz informasiya mühitini qorumaq müasir müharibələrin ayrılmaz komponentinə çevrilmişdir [5].

Digər mühüm istiqamət kiberməkanda hücum və müdafiə əməliyyatlarının həyata keçirilməsidir. Müasir münaqişələr göstərir ki, kritik infrastruktur obyektlərinə – enerji sistemlərinə, nəqliyyat şəbəkələrinə, rabitə və maliyyə sektoruna yönəlmiş kibercasusluq dövlətlərin milli təhlükəsizliyi üçün ciddi təhdid yaradır. NATO-nun yanaşmasına görə, kiberməkanda baş verən hücumlar müəyyən hallarda kollektiv müdafiə mexanizmlərinin işə salınmasına səbəb ola bilər [6]. Bu isə kibertəhlükəsizliyin hərbi-siyasi səviyyədə nə qədər əhəmiyyətli olduğunu göstərir.

Kibertəhlükəsizlik həmçinin hibrid müharibə konsepsiyası çərçivəsində xüsusi əhəmiyyət kəsb edir. Hibrid müharibələrdə informasiya manipulyasiyası, dezinformasiya kampaniyaları və psixoloji təsir vasitələri kiberməkan üzərindən həyata keçirilir. Bu kontekstdə kibertəhlükəsizlik yalnız texniki müdafiə deyil, həm də informasiya mühitinin qorunması, ictimai rəyin manipulyasiyasının qarşısının alınması və strateji kommunikasiya fəaliyyətlərinin təmin edilməsi kimi funksiyaları da yerinə yetirir [7].

Azərbaycan Respublikasında da kibertəhlükəsizlik milli təhlükəsizlik siyasətinin mühüm istiqamətlərindən biri kimi müəyyən edilmişdir. “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası”da dövlət informasiya resurslarının qorunması, kibertəhdidlərin qarşısının alınması və bu sahədə insan resurslarının inkişafı prioritet vəzifələr kimi qeyd olunur [1]. Bu baxımdan hərbi təhsil sistemində kibertəhlükəsizlik üzrə bilik və bacarıqların formalaşdırılması strateji əhəmiyyət daşıyır.

Kibertəhlükəsizlik müasir hərbi təhlükəsizlik sisteminin

ayrılmaz komponenti olmaqla yanaşı, dövlətlərin müdafiə qabiliyyətinin təmin olunmasında həlledici rol oynayır. Onun hərbi kontekstdə əhəmiyyəti yalnız müdafiə funksiyası ilə məhdudlaşmır, eyni zamanda hücum, kəşfiyyat və informasiya üstünlüyünün təmin edilməsi kimi çoxşaxəli istiqamətləri əhatə edir. Bu isə ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə hazırlığın gücləndirilməsini və bu sahədə elmi-tədqiqat fəaliyyətlərinin genişləndirilməsini zəruri edir.

III. KIBERTƏHLÜKƏSİZLİK ÜZRƏ TƏHSİLDƏ İNNOVATİV YANAŞMALAR

Müasir dövrdə kibertəhlükəsizlik sahəsində baş verən sürətli texnoloji dəyişikliklər təhsil sisteminin də çevik və innovativ yanaşmalar əsasında qurulmasını zəruri edir. Ənənəvi tədris metodları kiberməkanda dinamik şəkildə dəyişən təhdidlərə adekvat cavab verməkdə kifayət etmir. Bu baxımdan ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə hazırlığın səmərəliliyinin artırılması üçün innovativ təlim texnologiyalarının və metodlarının tətbiqi xüsusi əhəmiyyət kəsb edir. Bu yanaşmalar təhsilalanların yalnız nəzəri biliklərini deyil, həm də praktik bacarıqlarını, analitik düşünmə qabiliyyətini və operativ qərarvermə bacarıqlarını inkişaf etdirməyə yönəlmişdir.

Kibertəhlükəsizlik üzrə təhsildə ən mühüm innovativ vasitələrdən biri simulyasiya əsaslı təlim mühitləri və “cyber range” platformalarıdır. Bu platformalar real şəbəkə infrastrukturunu modelləşdirərək müxtəlif kibercasusluq və müdafiə ssenarilərinin modelləşdirilməsinə imkan yaradır. Belə mühitlərdə təhsilalanlar real şəraitə maksimum dərəcədə yaxın olan vəziyyətlərdə qərar qəbul etməyi öyrənir və risklərin idarə olunması bacarıqlarını inkişaf etdirirlər. NATO-nun Kooperativ Kibercasusluq üzrə Mükəmməllik Mərkəzi (CCDCOE) tərəfindən təşkil olunan təlimlərdə bu tip simulyasiya mühitlərindən geniş istifadə olunur ki, bu da onların effektivliyini təsdiq edir [6]. Eyni zamanda, ABŞ və Avropa ölkələrinin hərbi təhsil müəssisələrində “cyber range” laboratoriyaları kibertəhlükəsizlik təhsilinin əsas komponentlərindən biri kimi tətbiq edilir.

Digər mühüm innovativ yanaşma süni intellekt (Sİ) və maşın öyrənməsi texnologiyalarının tədris prosesinə inteqrasiyasıdır. Süni intellekt əsaslı sistemlər kibertəhdidlərin aşkarlanması, təhlili və proqnozlaşdırılması sahəsində geniş imkanlar yaradır. Tədris prosesində bu texnologiyaların tətbiqi təhsilalanların müasir alətlərlə işləmə bacarıqlarını inkişaf etdirir və onları real əməliyyat mühitinə hazırlayır. Tədqiqatçılar qeyd edirlər ki, süni intellekt yalnız texniki vasitə deyil, həm də qərarvermə proseslərini optimallaşdıran strateji alətdir [8]. Bu baxımdan Sİ-nin kibertəhlükəsizlik təhsilində tətbiqi innovativ və perspektivli istiqamət kimi qiymətləndirilir.

Kibertəhlükəsizlik üzrə təhsildə fərdiləşdirilmiş və adaptiv təlim sistemləri də mühüm yer tutur. Bu sistemlər təhsilalanların bilik səviyyəsini, öyrənmə tempini və fərdi xüsusiyyətlərini nəzərə alaraq tədris prosesini optimallaşdırır. Adaptiv platformalar vasitəsilə hər bir təhsilalan üçün fərdi təlim trayektoriyası müəyyən edilir ki, bu da təhsilin effektivliyini artırır və biliklərin daha dərinlən mənimsənilməsinə şərait yaradır. Xüsusilə hərbi təhsil kontekstində fərdi hazırlıq səviyyəsinin nəzərə alınması əməliyyat effektivliyinin

yüksəldilməsi baxımından vacibdir.

Oyun əsaslı təlim (gamification) və yarış formatlı öyrənmə metodları da kibertəhlükəsizlik təhsilində geniş tətbiq olunan innovativ yanaşmalardandır. “Capture The Flag” (CTF) tipli yarışlar təhsilənlərin praktiki biliklərini sınaqla yanaşı, onların motivasiyasını artırır və komandada işləmə bacarıqlarını inkişaf etdirir. Bu cür yarışlar real hücum və müdafiə ssenarilərinə əsaslandığından öyrənmə prosesini daha interaktiv və effektiv edir. ABŞ Milli Təhlükəsizlik Agentliyi (NSA) tərəfindən dəstəklənən akademik proqramlarda bu tip fəaliyyətlər geniş şəkildə tətbiq olunur [9].

Bundan əlavə, virtual və artırılmış reallıq (VR/AR) texnologiyalarının tədris prosesinə inteqrasiyası da innovativ yanaşmalar sırasına daxildir. Bu texnologiyalar vasitəsilə kompleks kibermühitlər vizuallaşdırılır və təhsilənlərə daha aydın və interaktiv öyrənmə imkanı təqdim olunur. Xüsusilə mürəkkəb şəbəkə strukturlarının və hücum mexanizmlərinin vizual təqdimatı öyrənmə prosesini əhəmiyyətli dərəcədə asanlaşdırır.

Kibertəhlükəsizlik üzrə təhsildə innovativ yanaşmalar tədris prosesinin keyfiyyətini yüksəltməklə yanaşı, müasir təhlükəsizlik mühitinin tələblərinə cavab verən peşəkar kadrların hazırlanmasına imkan yaradır. Simulyasiya texnologiyaları, süni intellekt, adaptiv təlim sistemləri və oyun əsaslı metodların inteqrasiyası ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə hazırlığın effektivliyini artıran əsas amillər kimi çıxış edir. Bu yanaşmaların sistemli şəkildə tətbiqi gələcəkdə kiberməkanda üstünlüyün təmin olunmasına və milli təhlükəsizliyin gücləndirilməsinə mühüm töhfə verə bilər.

IV. AZƏRBAYCAN ALİ HƏRBİ TƏHSİL SİSTEMİNDƏ MÖVCUD VƏZİYYƏT

Azərbaycan Respublikasında kibertəhlükəsizlik sahəsi son illərdə dövlət siyasətinin prioritet istiqamətlərindən biri kimi formalaşmış və bu istiqamətdə institusional, hüquqi və təhsil mühitində mühüm addımlar atılmışdır. Xüsusilə rəqəmsal transformasiya proseslərinin sürətlənməsi, elektron hökumət xidmətlərinin genişlənməsi və kritik informasiya infrastrukturunun inkişafı kibertəhlükəsizlik üzrə ixtisaslaşmış kadrların hazırlanmasını strateji zərurətə çevirmişdir. Bu kontekstdə ali hərbi təhsil sistemi də müasir çağırışlara uyğun olaraq kibertəhlükəsizlik sahəsində tədris və tədqiqat fəaliyyətlərini genişləndirməyə başlamışdır.

Azərbaycanın ali hərbi təhsil müəssisələrində kibertəhlükəsizlik üzrə hazırlıq əsasən informasiya texnologiyaları, rabitə və avtomatlaşdırılmış idarəetmə sistemləri istiqamətləri çərçivəsində həyata keçirilir. Bu sahədə tədris proqramları təhsilənlərə şəbəkə təhlükəsizliyi, kriptografiya, informasiya mühafizəsi və kibər hücumların qarşısının alınması kimi əsas bilik və bacarıqları aşılamağa yönəlmişdir. Bununla yanaşı, son illərdə kibertəhlükəsizlik ayrıca ixtisas və ya ixtisaslaşma istiqaməti kimi də inkişaf etdirilir. Ali hərbi təhsil müəssisələrində kibertəhlükəsizlik üzrə proqramların tətbiqi bu sahədə ümumi kadr potensialının formalaşmasına müsbət təsir göstərir.

Dövlət səviyyəsində qəbul olunmuş strateji sənədlər ali təhsil sistemində kibertəhlükəsizlik üzrə hazırlığın inkişafına

mühüm təkan verir. “Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizlikə dair 2023 – 2027-ci illər üçün Strategiyası”da insan resurslarının inkişafı və bu sahədə mütəxəssislərin hazırlanması əsas prioritetlərdən biri kimi müəyyən edilmişdir [1]. Eyni zamanda, “Azərbaycan 2030: sosial-iqtisadi inkişafa dair Milli Prioritetlər” sənədində rəqəmsal transformasiya və informasiya təhlükəsizliyi məsələləri xüsusi yer tutur ki, bu da ali təhsil sisteminin, o cümlədən hərbi təhsilin bu istiqamətdə modernləşdirilməsini zəruri edir [10].

Bununla belə, mövcud vəziyyətin təhlili göstərir ki, ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin inkişafı bir sıra problemlərlə müşayiət olunur. İlk növbədə, praktiki təlim mühitlərinin, xüsusilə “cyber range” tipli laboratoriyaların məhdudluğu diqqəti cəlb edir. Müasir kibertəhsil yalnız nəzəri biliklərlə məhdudlaşmadığından praktiki ssenarilər əsasında qurulan təlim infrastrukturuna mühüm əhəmiyyət daşıyır. İkinci mühüm problem yüksək ixtisaslı pedaqoji kadrların çatışmazlığı ilə bağlıdır. Kibertəhlükəsizlik sahəsi sürətlə inkişaf etdiyindən bu sahədə müasir bilik və bacarıqlara malik mütəxəssislərin hazırlanması xüsusi yanaşma tələb edir.

Beynəlxalq əməkdaşlığın məhdudluğu da diqqət çəkən məsələlərdəndir. Halbuki NATO, Avropa İttifaqı və digər beynəlxalq qurumların kibertəhlükəsizlik üzrə təlim proqramlarında iştirak təcrübə mübadiləsi baxımından mühüm əhəmiyyət kəsb edir [6]. Azərbaycan bu istiqamətdə müəyyən addımlar atsa da, ali hərbi təhsil müəssisələrinin beynəlxalq kibertəlim şəbəkələrinə inteqrasiyası daha da genişləndirilməlidir.

Digər tərəfdən, müsbət tendensiyalar da müşahidə olunur. Son illərdə ölkədə kibertəhlükəsizlik sahəsində fəaliyyət göstərən qurumların – o cümlədən Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin və Elektron Təhlükəsizlik Xidmətinin fəaliyyəti bu sahədə institusional inkişafı sürətləndirmişdir. Bu qurumların ali hərbi təhsil müəssisələri ilə əməkdaşlığı praktiki təlim imkanlarının genişləndirilməsi baxımından mühüm perspektivlər açır.

Azərbaycan ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə mövcud vəziyyət inkişaf mərhələsində olmaqla yanaşı, həm də yeni çağırışlar və imkanlarla xarakterizə olunur. Mövcud potensialın daha səmərəli istifadəsi, innovativ tədris metodlarının tətbiqi və beynəlxalq təcrübənin inteqrasiyası bu sahədə keyfiyyətə yeni mərhələyə keçidi təmin edə bilər. Bu isə öz növbəsində milli təhlükəsizlik sisteminin gücləndirilməsinə və kiberməkanda davamlı müdafiə qabiliyyətinin formalaşdırılmasına xidmət edəcəkdir.

V. PROBLEMLƏR VƏ ÇAĞIRIŞLAR

Ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin təşkili və inkişafı müasir dövrün tələblərinə uyğun olaraq bir sıra mürəkkəb problemlər və çağırışlarla müşayiət olunur. Bu çağırışlar həm texnoloji, həm institusional, həm də pedaqoji xarakter daşıyır və onların kompleks şəkildə təhlili effektiv həll yollarının müəyyənləşdirilməsi baxımından mühüm əhəmiyyət kəsb edir.

Əsas problemlərdən biri kibertəhdidlərin sürətlə dəyişən və mürəkkəbləşən təbiəti ilə bağlıdır. Müasir dövrdə kibər hücumları

getdikcə daha daha mürəkkəb xarakter alır, süni intellekt və avtomatlaşdırılmış alətlər vasitəsilə həyata keçirilir. Bu isə təhsil proqramlarının daimi yenilənməsini və çevikliyini tələb edir. Lakin ali hərbi təhsil müəssisələrində kurikulumların yenilənməsi prosesi çox vaxt texnoloji dəyişikliklərin sürətindən geri qalır. ENISA-nın hesabatında qeyd olunur ki, kibertəhlükəsizlik üzrə təhsil proqramlarının aktual saxlanması üçün dinamik və modul əsaslı yanaşmaların tətbiqi zəruridir [7].

Digər mühüm problem ixtisaslı kadr çatışmazlığı ilə bağlıdır. Kibertəhlükəsizlik sahəsində həm müəllim heyəti, həm də praktiki təlim mütəxəssislərinin sayı məhduddur. Bu sahədə yüksək ixtisaslı mütəxəssislərin özəl sektorda daha cəlbəedici əmək şəraiti ilə təmin olunması ali təhsil müəssisələrində kadr axınına səbəb olur. Nəticədə tədris prosesində müasir bilik və bacarıqların ötürülməsi çətinləşir. Bu problem qlobal xarakter daşıyır və müxtəlif beynəlxalq hesabatlarda kibertəhlükəsizlik üzrə peşəkar çatışmazlığının ciddi səviyyədə olduğu vurğulanır.

Texniki infrastrukturun məhduddluğu da diqqət çəkən məsələlərdəndir. Müasir kibertəhsil praktiki yönümlü olduğundan "cyber range", simulyasiya platformaları və laboratoriya mühitlərinin mövcudluğu vacibdir. Lakin bir çox hallarda bu cür texnoloji bazanın yaradılması yüksək maliyyə resursları tələb etdiyindən ali hərbi təhsil müəssisələrində bu imkanlar kifayət qədər inkişaf etmə laboratoriya mühitləriəməşdür. NATO-nun Kooperativ Kibermüdafiə Mükəmməllik Mərkəzinin (NATO CCDCOE) təcrübəsi göstərir ki, effektiv kibertəlim yalnız real ssenarilərə əsaslanan simulyasiya mühitlərində mümkündür.

Bununla yanaşı, normativ-hüquqi və institusional çərçivələrin tam formalaşmaması da müəyyən çətinliklər yaradır. Kibertəhlükəsizlik çoxşaxəli sahə olduğundan onun tədrisi hüquq, beynəlxalq münasibətlər və texnologiya sahələrinin inteqrasiyasını tələb edir. Bu isə kurikulumların hazırlanmasında kompleks yanaşmanın tətbiqini zəruri edir. Azərbaycan Respublikasında bu istiqamətdə müəyyən addımlar atılsa da, ali hərbi təhsil sistemində vahid standartların və metodoloji bazanın daha da təkmilləşdirilməsinə ehtiyac vardır.

Digər mühüm çağırış beynəlxalq əməkdaşlığın yetərli səviyyədə olmamasıdır. Kibertəhlükəsizlik qlobal xarakter daşıdığından bu sahədə təcrübə mübadiləsi və birgə təlimlər xüsusi əhəmiyyət kəsb edir. Lakin ali hərbi təhsil müəssisələrinin beynəlxalq kibertəlim proqramlarına inteqrasiyası hələ də məhdudd səviyyədədir. Bu isə qabaqcıl təcrübələrin mənimsənilməsini çətinləşdirir və təhsilin keyfiyyətinə təsir göstərir.

Nəhayət, kibertəhlükəsizlik sahəsində etik və psixoloji məsələlər də aktual problemlər sırasındadır. Kiberməkanda fəaliyyət göstərən mütəxəssislərin yüksək etik standartlara malik olması və informasiya ilə məsuliyyətli davranması vacibdir. Eyni zamanda, kibercümləmələrin psixoloji təsirləri və informasiya müharibələrinin yaratdığı risklər təhsilənlərin kompleks hazırlığını tələb edir.

Ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin inkişafı çoxsaylı və çoxşaxəli problemlərlə müşayiət olunur. Bu problemlərin aradan qaldırılması üçün kurikulumların mütəmadi yenilənməsi, kadr potensialının gücləndirilməsi, texniki infrastrukturun inkişaf etdirilməsi və beynəlxalq əməkdaşlığın

genişləndirilməsi zəruridir. Yalnız bu halda müasir təhlükəsizlik mühitinin tələblərinə cavab verən yüksək ixtisaslı hərbi mütəxəssislərin hazırlanması mümkün olacaqdır.

NƏTİCƏ

Aparılan təhlillər göstərir ki, müasir təhlükəsizlik mühitində kibertəhlükəsizlik ali hərbi təhsil sisteminin ayrılmaz və strateji əhəmiyyətli istiqamətlərindən birinə çevrilmişdir. Rəqəmsallaşmanın dərinləşməsi, hibrid müharibə elementlərinin geniş yayılması və kritik infrastrukturun informasiya texnologiyalarından asılılığının artması hərbi kadrların hazırlığında yeni yanaşmaların tətbiqini zəruri edir. Bu baxımdan kibertəhlükəsizlik üzrə təhsilin yalnız nəzəri biliklərlə məhduddlaşmaması, praktiki bacarıqlar, analitik düşüncə və operativ qərarvermə qabiliyyətləri ilə tamamlanması xüsusi əhəmiyyət daşıyır.

Məqalədə göstəriləndiyi kimi, innovativ təlim texnologiyalarının – xüsusilə simulyasiya mühitlərinin, süni intellekt əsaslı sistemlərin və adaptiv tədris modellərinin tətbiqi kibertəhsil prosesinin effektivliyini əhəmiyyətli dərəcədə artırır. Eyni zamanda, beynəlxalq təcrübənin öyrənilməsi və qabaqcıl modellərin milli təhsil sisteminə inteqrasiyası bu sahədə keyfiyyət dəyişikliklərinə səbəb ola bilər. Azərbaycan ali hərbi təhsil sistemində bu istiqamətdə müəyyən irəliləyişlər müşahidə olunsada, mövcud problemlərin – kadr çatışmazlığı, texniki infrastrukturun məhduddluğu və tədris proqramlarının müasir tələblərə tam uyğunlaşmaması kimi məsələlərin həlli hələ də aktual olaraq qalır.

Tədqiqatın praktik əhəmiyyəti ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə tədris prosesinin təkmilləşdirilməsi üçün elmi əsaslandırılmış yanaşmalar təqdim etməsindəndir. Məqalədə irəli sürülən təklif və yanaşmalar kibertəhlükəsizlik sahəsində peşəkar hərbi kadrların hazırlanması, innovativ təlim texnologiyalarının tətbiqi və praktiki yönümlü tədris mühitinin formalaşdırılması baxımından faydalı ola bilər. Eyni zamanda, əldə olunan nəticələr ali hərbi təhsil müəssisələrində kurikulumların yenilənməsi və beynəlxalq təcrübənin inteqrasiyası üçün metodoloji baza kimi istifadə edilə bilər. Tədqiqatın nəticələri dövlətin informasiya təhlükəsizliyi siyasətinin həyata keçirilməsi və kiberməkanda müdafiə qabiliyyətinin gücləndirilməsi istiqamətində də praktik əhəmiyyətə malikdir.

Nəticə etibarilə, ali hərbi təhsil sistemində kibertəhlükəsizlik üzrə təhsilin inkişafı kompleks və davamlı yanaşma tələb edir. Bu istiqamətdə həyata keçiriləcək məqsədyönlü tədbirlər, o cümlədən innovasiyaların tətbiqi, institusional əməkdaşlığın gücləndirilməsi və insan kapitalının inkişafı milli təhlükəsizliyin möhkəmləndirilməsinə və kiberməkanda dayanıqlı müdafiə qabiliyyətinin formalaşdırılmasına mühüm töhfə verəcəkdir.

ƏDƏBİYYAT

- [1] Azərbaycan Respublikası Prezidentinin, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası" haqqında Sərəncamı, Bakı, Azərbaycan, 2023. <https://president.az/az/articles/view/60949>
- [2] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Harlow, U.K.: Pearson, 2018. <https://www.emgywomenscollege.ac.in/templateEditor/kcfinder/upload/files/Network-security-essentials.pdf>

- [3] ISO/IEC 27032:2012, Guidelines for Cybersecurity. Geneva, Switzerland: International Organization for Standardization, 2012. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>
- [4] U.S. Department of Defense, Cyber Strategy Summary. Washington, DC, USA, 2026. <https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf>
- [5] M. Bishop, Computer Security: Art and Science. Boston, MA, USA: Addison-Wesley, 2019. https://books.google.az/books?id=pfdBiJNfWdMC&printsec=frontcover&redir_esc=y#v=onepage&q&f=false
- [6] NATO, "Cyber Defence Training and Exercises," 2024. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>
- [7] ENISA, Cybersecurity Education and Training Guide, 2022. <https://ru.scribd.com/document/656127289/ENISA-Cybersecurity-education-initiatives-in-MS>
- [8] M. Məmmədşadə, "Hərbi təhsildə innovativ yanaşma: süni intellektlə inteqrasiya olunmuş təlim texnologiyaları," in Süni intellekt texnologiyaları və aerokosmik problemlər: III Beynəlxalq elmi-praktik konfransın materialları, Bakı, Azərbaycan, Jul. 2025, pp. 87–91.
- [9] National Security Agency, "National Centers of Academic Excellence in Cybersecurity," 2023. <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/>
- [10] Azərbaycan Respublikası, "Azərbaycan 2030: sosial-iqtisadi inkişafa dair Milli Prioritetlər," Bakı, Azərbaycan, 2021. <https://president.az/az/articles/view/50474>

Cybersecurity Education and Innovation in the System of Higher Military Education

Mujkan Mammadzade

Military Scientific Research Institute, Baku, Azerbaijan
mujkan@mail.ru

Abstract – The article analyzes the current state, theoretical foundations, and development directions of cybersecurity education within the system of higher military education. The strategic role of cybersecurity in the modern military security environment is substantiated, and the importance of training qualified personnel in this field is emphasized. International experience, particularly the models of NATO and other advanced countries, is examined. Innovative approaches in education—such as simulation environments, artificial intelligence, adaptive learning systems, and game-based methods—are comprehensively discussed. At the same time, the current situation, existing problems, and challenges in the higher military education system of Azerbaijan are identified. The article proposes practical and scientifically grounded recommendations for improving cybersecurity education and highlights its significance in ensuring national security.

Keywords – cybersecurity; higher military education; innovative learning; cyber range; national security.