

Adaptiv Süni İntellekt Təlimi Vasitəsilə Kursantların Kibertəhlükəsizlik Maarifləndirilməsinin Təkmilləşdirilməsi

Aysu Qafarlı

Milli Müdafiə Universiteti, Naxçıvan Hərbi Kolleci, Naxçıvan, Azərbaycan
gafarliaysu49@gmail.com

Xülasə— Müasir dövrdə kibertəhlükələr təhsil müəssisələri, xüsusilə hərbi kolleclər üçün ciddi risklər yaradır və informasiya təhlükəsizliyi üzrə davamlı maarifləndirməni zəruri edir. Məqalədə kursantların kibertəhlükəsizlik üzrə bilik və bacarıqlarının artırılması məqsədilə süni intellekt əsaslı adaptiv təlim modeli təqdim olunur. Təklif edilən sistem istifadəçilərin bilik səviyyəsini ilkin olaraq qiymətləndirir, nəticələrə uyğun fərdiləşdirilmiş tədris məzmunu formalaşdırır və real vaxt rejimində əks əlaqə yaradır. Bu yanaşma kursantların öyrənmə motivasiyasının, praktik hazırlığının, rəqəmsal intizamının və təhlükəsizlik davranışlarının əhəmiyyətli dərəcədə gücləndirilməsinə imkan verir.

Açar sözlər— adaptiv təlim; hərbi təhsil; informasiya təhlükəsizliyi; kibertəhlükəsizlik; kursant hazırlığı; süni intellekt.

I. GİRİŞ

Müasir rəqəmsal dövrdə kibertəhlükələr təhsil müəssisələri üçün əsas risk faktorlarından birinə çevrilmişdir. Xüsusilə hərbi kolleclərdə istifadə olunan kompüter şəbəkələri, elektron resurslar və daxili informasiya sistemləri yüksək təhlükəsizlik tələblərinə malikdir. Bu səbəbdən kursantların kibertəhlükəsizlik sahəsində bilik və bacarıqlarının erkən mərhələdə formalaşdırılması strateji əhəmiyyət daşıyır. Ənənəvi təlim metodları bütün öyrənmələrə eyni məzmun təqdim etdiyindən fərdi ehtiyacları tam qarşılamır.

Son illərdə Süni İntellekt (Sİ) texnologiyalarının təhsildə tətbiqi fərdiləşdirilmiş və çevik öyrənmə imkanları yaratmışdır. Adaptiv Sİ əsaslı sistemlər istifadəçilərin nəticələrini təhlil edərək onlara uyğun məzmun təqdim edir, zəif sahələri müəyyənləşdirir və real-vaxt rejimində əks-əlaqə yaradır. Bu yanaşma kibertəhlükəsizlik təlimlərində daha yüksək effektivlik əldə etməyə imkan yaradır [1, 2].

Hərbi təhsil mühitində intizam, məxfilik və operativ hazırlıq əsas prioritetlərdən hesab olunur. Buna görə kursantların fişinq hücumları, zəif parollar, sosial mühəndislik və məlumat sızmaları kimi risklərə qarşı hazır olması vacibdir [3]. Təklif olunan adaptiv təlim modeli bu sahədə kursantların rəqəmsal davranışlarını inkişaf etdirməyə, təhlükəsizlik mədəniyyətini gücləndirməyə və təlim nəticələrini artırmağa yönəlmişdir.

Bu məqalənin məqsədi hərbi kolleclərdə kursantların kibertəhlükəsizlik maarifləndirilməsinin artırılması üçün süni intellekt əsaslı adaptiv təlim modelinin üstünlüklərini, tətbiq imkanlarını və perspektivlərini araşdırmaqdır.

II. ADAPTİV TƏLİM SİSTEMİNİN SEÇİMİ VƏ İSTİFADƏ RAHATLIĞI

A. Adaptiv Təlim Modelinin Seçilməsi

Hərbi kolleclərdə kibertəhlükəsizlik üzrə təlim proqramı seçilərkən sistemin istifadə rahatlığı, təhlükəsizlik səviyyəsi və öyrənmələrin ehtiyaclarına uyğunluğu nəzərə alınmalıdır. Ənənəvi təlim üsulları sabit məzmun təqdim etdiyi halda, adaptiv Süni İntellekt əsaslı platformalar kursantların bilik səviyyəsinə uyğun fərdiləşdirilmiş öyrənmə mühiti yaradır. Bu yanaşma təlim müddətinin daha səmərəli istifadəsinə və nəticələrin yüksəlməsinə imkan verir.

Adaptiv Sİ əsaslı təlim modelinin əsas üstünlükləri Cədvəl I-də təqdim edilmişdir.

Seçilən sistem istifadəçi dostu interfeysə malik olmalı, qısa müddətdə mənimsənilməli və məhdud texniki resurslarla işləyə bilməlidir. Xüsusilə hərbi təhsil müəssisələrində daxili şəbəkələrdə işləmə qabiliyyəti və məxfi məlumatların qorunması əsas meyarlardan hesab olunur. Bu səbəbdən proqram təminatının həm funksional, həm də təhlükəsiz olması vacibdir [4].

CƏDVƏL I. ADAPTİV SÜNİ İNTELLEKT ƏSASLI TƏLİM MODELİNİN ƏSAS FUNKSIONAL XÜSUSİYYƏTLƏRİ VƏ GÖZLƏNİLƏN NƏTİCƏLƏRİ

Komponent	Təsviri	Gözlənilən Nəticə
İlkin qiymətləndirmə	Kursantın bilik səviyyəsinin yoxlanılması	Fərdi təlim planı
Adaptiv məzmun	Səviyyəyə uyğun dərs modulları	Daha sürətli öyrənmə
Simulyasiya	Real kibertəhlükə ssenariləri	Praktiki bacarıq
Əks-əlaqə	Ani səhv analizi və tövsiyə	Davamlı inkişaf
Analitika	Təlim nəticələrinin izlənməsi	Effektiv idarəetmə

B. Texniki Bütövlüyün Saxlanılması

Adaptiv təlim sistemlərinin effektiv fəaliyyəti üçün texniki bütövlüyün qorunması mühüm əhəmiyyət daşıyır. Server infrastrukturunun sabitliyi, məlumat bazalarının mühafizəsi və istifadəçi hesablarının təhlükəsiz idarə olunması sistemin dayanıqlığını təmin edir. Müntəzəm yenilənmələr, ehtiyat nüsxələrin yaradılması və giriş nəzarəti tədbirləri mümkün

riskləri minimuma endirir. İnformasiya sistemlərinin təhlükəsizliyinin təmin edilməsində standartlaşdırılmış kibertəhlükəsizlik çərçivələrinin tətbiqi mühüm əhəmiyyət daşıyır [4].

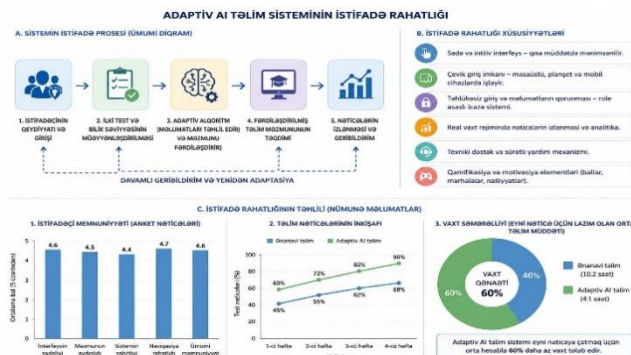
Bundan əlavə, sistemdə təqdim olunan tədris materiallarının düzgün işləməsi, test nəticələrinin itirilməməsi və analitik hesabatların dəqiq formalaşdırılması vacibdir. Əgər platformada texniki nasazlıq yaranarsa, kursantların təlim motivasiyası azala və ümumi nəticələrə mənfi təsir göstərə bilər. Buna görə texniki dəstək mexanizmləri əvvəlcədən planlaşdırılmalıdır.

C. İstifadəçi Təcrübəsinin Yaxşılaşdırılması

Kursantların sistemdən aktiv istifadə etməsi üçün sadə menyular, aydın vizual elementlər və sürətli keçidlər təmin olunmalıdır. Təlim tapşırıqları mərhələli formada təqdim edildikdə istifadəçi yorğunluğu azalır və maraq artır. Qamifikasiya elementləri, ballar və mərhələ göstəriciləri motivasiyanın yüksəlməsinə müsbət təsir göstərir.

Beləliklə, istifadə rahatlığı yüksək olan adaptiv sistemlər həm tədris keyfiyyətini yüksəldir, həm də kibertəhlükəsizlik vərdişlərinin daha davamlı formalaşmasına şərait yaradır.

Adaptiv Sİ təlim sisteminin istifadə rahatlığı və səmərəliliyinin qiymətləndirilməsi Şəkil 1-də təqdim olunmuşdur.



Şəkil 1. Adaptiv Sİ əsaslı təlim sisteminin istifadə rahatlığı və səmərəliliyinin qiymətləndirilməsi.

Adaptiv təlim sisteminin seçilməsi üçün əsas texniki və funksional meyarlar Cədvəl II-də verilmişdir.

CƏDVƏL II. ADAPTİV TƏLİM SİSTEMİNİN SEÇİLMƏSİ ÜÇÜN ƏSAS TEXNİKİ VƏ FUNKSIONAL MEYARLAR

Meyar	Təsviri	Əhəmiyyəti
Təhlükəsizlik	Məlumatların qorunması	Yüksək
Sadə interfeys	Rahat istifadə	Yüksək
Adaptivlik	Fərdi məzmun təqdimatı	Yüksək
Oflayn imkanlar	Məhdud şəbəkədə işləmə	Yüksək
Analitika	Nəticələrin izlənməsi	Orta

III. TƏKLİF OLUNAN ADAPTİV TƏLİM MODELİ

Kursantların kibertəhlükəsizlik üzrə hazırlığının artırılması məqsədilə təklif olunan adaptiv təlim modeli çoxmərhələli yanaşmaya əsaslanır. Modelin əsas üstünlüyü hər bir istifadəçinin bilik səviyyəsinə, öyrənmə sürətinə və nəticələrinə uyğun fərdiləşdirilmiş təlim mühiti yaratmasıdır. Ənənəvi təlimlərdə bütün iştirakçılara eyni məzmun təqdim olunduğu halda, bu sistem hər kursant üçün fərqli inkişaf xətti formalaşdırır.

Modelin birinci mərhələsində ilkin qiymətləndirmə aparılır. Bu mərhələdə kursantların fişinq hücumları, təhlükəsiz parol yaradılması, sosial mühəndislik, məlumat məxfiliyi və şəbəkə təhlükəsizliyi üzrə bilikləri test edilir. Nəticələr əsasında sistem kursantları müxtəlif səviyyələrə ayırır və uyğun məzmun təqdim edir. Kibertəhlükəsizlik üzrə maarifləndirmə təlimlərinin effektivliyinin qiymətləndirilməsi bu cür ilkin bilik səviyyəsinin müəyyənəşdirilməsini və təlim nəticələrinin sistemli şəkildə izlənilməsini tələb edir [5].

İkinci mərhələdə adaptiv məzmun təqdimatı həyata keçirilir. Baza səviyyəsində olan kursantlara fundamental anlayışlar, yüksək nəticə göstərənlərə isə mürəkkəb ssenarilər təqdim olunur. Bu yanaşma vaxt itkisini azaldır və təlim prosesini daha səmərəli edir.

Üçüncü mərhələdə simulyasiya əsaslı öyrənmə tətbiq edilir. Sistem real həyatda rast gəlinən saxta e-poçt hücumları, şübhəli keçidlər, zəif giriş parolları və məlumat paylaşımı riskləri kimi ssenarilər yaradır. Kursantlar bu situasiyalarda düzgün qərar qəbul etməyi praktiki şəkildə öyrənirlər. Kibertəhlükəsizlik üzrə təhsil və təlim proqramlarında praktiki hazırlığın və sərəfələrin inkişaf etdirilməsi mühüm istiqamətlərdən biridir [6].

Dördüncü mərhələdə real-vaxt əks-əlaqə təqdim olunur. İstifadəçi səhv etdikdə sistem səbəbi izah edir, düzgün yanaşmanı göstərir və əlavə tövsiyələr verir. Bu üsul öyrənməni sürətləndirir və səhvlərin təkrarlanma ehtimalını azaldır.

Nəhayət, sistem analitik hesabatlar formalaşdırır. Təlim nəticələri, zəif mövzular və ümumi inkişaf göstəriciləri rəhbərlik və müəllim heyəti üçün faydalı məlumat mənbəyi yaradır. Bu da gələcək təlim strategiyalarının daha düzgün planlaşdırılmasına imkan verir. Qlobal kibertəhlükəsizlik göstəricilərinin və beynəlxalq təcrübənin nəzərə alınması kibertəhlükəsizlik üzrə təlim strategiyalarının təkmilləşdirilməsinə əlavə imkanlar yaradır [7].

NƏTİCƏ VƏ GƏLƏCƏK PERSPEKTİVLƏR

Adaptiv süni intellekt əsaslı kibertəhlükəsizlik təliminin tətbiqi kursantların nəzəri bilik və praktik bacarıqlarında müsbət dəyişiklik yarada bilər. Fərdiləşdirilmiş yanaşma sayəsində kursantlar öz səviyyələrinə uyğun materiallarla işlədiklərindən onların öyrənmə motivasiyası yüksəlir. Bu isə ümumi tədris effektivliyinə birbaşa təsir göstərir.

Praktik simulyasiya tapşırıqları kursantların real riskləri daha yaxşı anlamasına kömək edir. Xüsusilə fişinq hücumlarının tanınması, təhlükəsiz parol seçimi və məlumat paylaşımı zamanı ehtiyatlı davranış kimi bacarıqlar daha sürətli formalaşır.

Bununla yanaşı, sistemin tətbiqində bəzi çətinliklər də mövcuddur. Texniki infrastrukturun kifayət qədər güclü olması, məlumatların qorunması və platformanın davamlı yenilənməsi

əsas tələblər sırasındadır. Eyni zamanda, Sİ sistemləri insan nəzarəti ilə birlikdə istifadə olunmalı və yekun qərarlar yalnız avtomatlaşdırılmış şəkildə qəbul edilməməlidir.

Adaptiv Sİ əsaslı kibertəhlükəsizlik təlim sistemlərinin tətbiqi bir sıra üstünlüklərlə yanaşı, müəyyən çağırışları da ehtiva edir. İlk növbədə, hərbi təhsil müəssisələrində istifadə olunan informasiya sistemlərinin məxfiliyi və təhlükəsizlik standartları yüksək səviyyədə olmalıdır. Bu səbəbdən xarici bulud platformalarından istifadəyə məhdudiyyətlər yarana bilər və lokal server həllərinə üstünlük verilməsi tələb oluna bilər.

İkinci mühüm məsələ texniki infrastrukturla bağlıdır. Adaptiv təlim platformalarının fasiləsiz işləməsi üçün sabit şəbəkə bağlantısı, təhlükəsiz verilənlər bazaları və müasir kompüter avadanlıqları vacibdir. Əgər texniki imkanlar zəif olarsa, sistemin səmərəliliyi azala bilər. Buna görə ilkin mərhələdə pilot tətbiqlərin həyata keçirilməsi və mərhələli inteqrasiyanın təmin olunması daha məqsədəuyğun hesab olunur.

Üçüncü məsələ insan amili ilə əlaqədardır. Bəzi istifadəçilər yeni texnologiyalara ehtiyatla yanaşır və ənənəvi təlim üsullarına üstünlük verə bilərlər. Bu baxımdan müəllim heyəti və kursantlar üçün maarifləndirici seminarların təşkili vacibdir. Süni intellekt sisteminin müəllimi əvəz etmədiyi, əksinə, onu dəstəklədiyi aydın şəkildə izah olunmalıdır.

Gələcək perspektivlər baxımından bu sistemlər daha da inkişaf etdirilə bilər. Səsli virtual təlimçi, davranış analitikası, fərdi risk profilləri və real vaxt rejimində kibertəhlükə simulyasiyaları gələcək versiyalarda tətbiq oluna bilər. Bundan əlavə, mobil platformalar vasitəsilə dərsləndirici tədris imkanlarının yaradılması kursantların davamlı inkişafına töhfə verə bilər.

Təklif olunan adaptiv kibertəhlükəsizlik təlim modelinin hərbi kolleclərdə praktik tətbiqi mərhələli şəkildə həyata keçirilə bilər. İlk mərhələdə kursantlar üçün ilkin bilik qiymətləndirməsi aparılır və onların mövcud hazırlıq səviyyəsi müəyyən edilir. Bu qiymətləndirmənin nəticələrinə əsasən kursantlar başlanğıc, orta və irəli səviyyələr üzrə qruplaşdırılır.

İkinci mərhələdə sistem hər bir kursant üçün fərdiləşdirilmiş təlim planı yaradır. Başlanğıc səviyyəsində olan istifadəçilərə parol təhlükəsizliyi, məlumat məxfiliyi və fişinq hücumlarının tanınması kimi fundamental mövzular təqdim edilir. Daha yüksək səviyyədə olan kursantlara isə şəbəkə təhlükəsizliyi, risk qiymətləndirilməsi və rəqəmsal insidentlərə cavab tədbirləri öyrədilir.

Üçüncü mərhələdə simulyasiya əsaslı məşğələlər təşkil olunur. Kursantlara saxta elektron poçt mesajları, şübhəli keçidlər və məlumat sızması ssenariləri təqdim edilir. Onların qərarları sistem tərəfindən qiymətləndirilir və dərhal əks əlaqə verilir. Bu üsul real təhlükələrə qarşı praktik hazırlığın artırılmasına kömək edir.

Dördüncü mərhələdə müəllim heyəti üçün analitik hesabatlar formalaşdırılır. Hesabatlarda kursantların ümumi nəticələri, zəif sahələri və inkişaf dinamikası göstərilir. Bu

məlumatlar növbəti təlim planlarının hazırlanmasına və fərdi dəstək tədbirlərinin təşkilinə imkan yaradır.

Beləliklə, adaptiv Sİ əsaslı sistem həm kursantlar, həm də tədris heyəti üçün səmərəli və ölçülə bilən təlim mühiti yaradır. Bu modelin tətbiqi kibertəhlükəsizlik üzrə hazırlığın davamlı inkişafına şərait yaradır.

Nəticə etibarilə, adaptiv Sİ əsaslı kibertəhlükəsizlik təlimi yalnız bugünkü ehtiyaclarla deyil, gələcək rəqəmsal təhlükələrə qarşı da hazırlıq yaradan innovativ yanaşmadır. Hərbi kolleclərdə bu cür sistemlərin tətbiqi təhlükəsizlik mədəniyyətinin gücləndirilməsi baxımından strateji əhəmiyyət daşıyır.

ƏDƏBİYYAT

- [1] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Hoboken, NJ, USA: Pearson, 2021.
- [2] A. Smith and J. Brown, "Adaptive learning systems in higher education," *Journal of Educational Technology*, vol. 15, no. 2, pp. 44–56, 2022.
- [3] W. Stallings, *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Boston, MA, USA: Addison-Wesley, 2019.
- [4] National Institute of Standards and Technology, *Cybersecurity Framework 2.0*. Gaithersburg, MD, USA, 2024.
- [5] M. Brown, "Cyber awareness training effectiveness in academic institutions," *Information Security Review*, vol. 10, no. 1, pp. 18–29, 2023.
- [6] European Union Agency for Cybersecurity, *Cybersecurity Education and Training Guidelines*. Heraklion, Greece, 2023.
- [7] International Telecommunication Union, *Global Cybersecurity Index 2024 Report*. Geneva, Switzerland, 2024.

Enhancing Cadets' Cybersecurity Awareness Through Adaptive Artificial Intelligence Training

Aysu Gafarli

National Defense University, Nakhchivan Military College,
Nakhchivan, Azerbaijan
gafarliaysu49@gmail.com

Abstract- In the modern era, cyber threats pose significant risks to educational institutions, particularly military colleges, making continuous cybersecurity awareness and training increasingly essential. This article presents an adaptive artificial intelligence-based training model designed to enhance cadets' cybersecurity knowledge and competencies. The proposed system initially evaluates users' knowledge levels, generates personalized instructional content based on the assessment results, and provides real-time feedback throughout the learning process. As a result, the proposed approach can significantly improve cadets' learning motivation, practical preparedness, digital discipline, and cybersecurity awareness.

Keywords- adaptive learning; artificial intelligence; cadet training; cybersecurity; information security; military education.