Kibertəhlükəsizlik üzrə Təhsil, İnnovasiya və Əməkdaşlıq

Mahir Talıbov
Dövlət Təhlükəsizliyi Xidməti, Bakı, Azərbaycan
mahirtalibov5@gmail.com

***Xülasə*—Rəqəmsal transformasiyanın sürətləndiyi müasir dövrdə ixtisaslı kibertəhlükəsizlik mütəxəssislərinə olan tələbat kəskin artmışdır. Tədqiqatda Azərbaycanda kibertəhlükəsizlik üzrə mövcud təhsil modelləri, kadr hazırlığının problemləri, akademiya-sənaye-dövlət əməkdaşlığının vəziyyəti təhlil edilir. Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyasının kadr hazırlığına töhfəsi ayrıca araşdırılır. Süni intellekt texnologiyalarına əsaslanan yeni tədris metodologiyaları, beynəlxalq əməkdaşlıq mexanizmləri və ixtisaslaşmış laboratoriya infrastrukturunun yaradılması üzrə tövsiyələr irəli sürülür. Nəticələr göstərir ki, kompleks yanaşma - kurikulumun modernləşdirilməsi, sertifikasiya sisteminin gücləndirilməsi və çoxtərəfli əməkdaşlıq çərçivəsinin formalaşdırılması — sahədə kadr çatışmazlığını aradan qaldırmaq üçün zəruri şərtdir.**

Açar sözlər— kibertəhlükəsizlik təhsili; innovativ tədris metodologiyaları; akademiya-sənaye-dövlət əməkdaşlığı;, kadr hazırlığı; rəqəmsal bacarıqlar; CTF yarışmaları; süni intellekt.

I. GİRİŞ

Rəqəmsal texnologiyaların sürətli inkişafı kiberhücumların miqyasını və mürəkkəbliyini əhəmiyyətli dərəcədə artırmışdır. Dünya İqtisadi Forumunun 2024-cü il hesabatına əsasən, kibertəhlükəsizlik sahəsindəki qlobal işçi qüvvəsi açığı 3,4 milyona yaxınlaşmışdır [1]. Bu rəqəm mütəxəssis hazırlığında sistemli yanaşmanın nə qədər vacib olduğunu açıq şəkildə ortaya qoyur. Eyni zamanda, Cybersecurity Ventures agentliyinin məlumatlarına görə, 2025-ci ilə qədər kibertəhlükəsizlik sahəsindəki iqtisadi itkilər illik 10,5 trilyon ABŞ dollarına çatacaqdır [2].

Azərbaycan Respublikası «Rəqəmsal Azərbaycan» strategiyası çərçivəsində informasiya infrastrukturunun qorunmasını prioritet istiqamətlərdən biri kimi müəyyən etmişdir. Ölkədə e-hökumət xidmətlərinin genişlənməsi, maliyyə sektorunun rəqəmsal transformasiyası və kritik infrastrukturun avtomatlaşdırılması kibertəhlükəsizlik mütəxəssislərinə olan tələbatı xeyli artırmışdır. Bu kontekstdə ixtisaslı kadrların hazırlanması, mövcud təhsil modullarının müasirləşdirilməsi və beynəlxalq standartlara uyğunlaşdırılması strateji əhəmiyyət kəsb edir.

Azərbaycan Respublikası Dövlət Təhlükəsizliği Xidmətinin Heydər Əliyev adına Akademiyası bu prosesdə xüsusi yer tutur: akademiya həm dövlət strukturları üçün ixtisaslı kadr hazırlayır, həm də kibertəhlükəsizlik sahəsində tətbiqi tədqiqatların aparılmasına zəmin yaradır. Onun ali təhsil müəssisələri və tədqiqat institutları ilə əlaqələndirilmiş fəaliyyəti sahədə sinergini əhəmiyyətli dərəcədə artıra bilər.

Bu məqalədə üç əsas sual araşdırılır: (1) Azərbaycanda kibertəhlükəsizlik təhsilinin mövcud vəziyyəti necədir? (2) Akademiya-sənaye-dövlət əməkdaşlığı bu sahədə hansı imkanları açır? (3) İnnovasiya və süni intellekt texnologiyaları tədris prosesini necə transformasiya edə bilər? Tədqiqatın nəticələri həm akademik, həm də siyasət qərarları qəbuledici üçün praktiki əhəmiyyət daşıyır.

II. AZƏRBAYCANDA KİBERTƏHLÜKƏSİZLİK TƏHSİLİNİN MÖVCUD VƏZİYYƏTİ

A. Təhsil Müəssisələri və Proqramlar

Azərbaycanda kibertəhlükəsizlik üzrə ixtisaslaşmış bakalavr və magistr proqramları əsasən Azərbaycan Texniki Universiteti (AzTU), Bakı Dövlət Universiteti (BDU) və UNEC-də həyata keçirilir. ETN İnformasiya Texnologiyaları İnstitutu tətbiqi tədqiqatlar sahəsində aparıcı rol oynayır. Dövlət Təhlükəsizliği Xidmətinin Heydər Əliyev adına Akademiyası isə dövlət sektoru üçün ixtisaslaşmış kadr hazırlığında müstəsna yer tutur. Cədvəl I-də bu müəssisələrin kibertəhlükəsizlik sahəsindəki əsas fəaliyyət istiqamətlərinin müqayisəsi verilmişdir.

CƏDVƏL I. AZƏRBAYCANDA KİBERTƏHLÜKƏSİZLİK ÜZRƏ ƏSAS TƏHSİL VƏ TƏDQİQAT MÜƏSSİSƏLƏRİ

Müəssisə	Proqram növü	Əsas istiqamət	Sektor
AzTU	Bakalavr/Magistr	Şəbəkə, kriptoqrafiya	Ali təhsil
BDU	Bakalavr/Magistr	İnformasiya təhlükəsizliyi	Ali təhsil
ETN İTİ	Tədqiqat/ Doktorantura	Tətbiqi kibertəhlükəsizlik	Dövlət/Elmi
DTX Akademiyası	İxtisas kursları	Milli kiber müdafiə, ekspertiza	Dövlət/Hüquq-mühafizə

Mövcud kurikulumlarda bir sıra struktur çatışmazlıqlar müşahidə olunur: nəzəri biliklərin praktiki bacarıqlarla balanslaşdırılmaması; sürətlə dəyişən təhdid mənzərəsinə uyğun kurikulum yeniləmələrinin ləngiməsi; ixtisaslaşmış laboratoriya və simulyasiya mühitlərinin məhdudluğu. Bu çatışmazlıqlar kibertəhlükəsizlik mütəxəssislərinin peşəkar hazırlıq səviyyəsini birbaşa təsir edir.

B. Sertifikasiya və Beynəlxalq Standartlar

CompTIA Security+, CEH (Certified Ethical Hacker), CISSP (Certified Information Systems Security Professional) kimi beynəlxalq sertifikatlar sahə mütəxəssisləri arasında getdikcə daha çox tanınır. Lakin bu sertifikatların əldə edilməsini dəstəkləyən institusional mexanizmlər - hazırlıq kursları, maliyyə dəstəyi, imtahan mərkəzlərinin sayı - hələ kifayət qədər inkişaf etməmişdir. Azərbaycanda mövcud

DOI: 10.25045/forensic.gov.2026.75

sertifikasiya mərkəzlərinin sayı məhdud olmaqla, sertifikasiya xərclərinin orta əməkhaqqına nisbəti əhəmiyyətli maneə yaradır.

Müqayisəli analizlər göstərir ki, qabaqcıl ölkələrdə - Estoniya, İsrail, Sinqapur - dövlət-özəl sektor tərəfdaşlığına əsaslanan sertifikasiya proqramları kadr potensialını əhəmiyyətli dərəcədə artırmışdır [3]. Estoniyada, məsələn, dövlət qulluqçularının 60%-dən çoxu kibertəhlükəsizlik üzrə əsas sertifikatlara malikdir. Bu göstərici Azərbaycan üçün hədəf kimi götürülə bilər.

III. İNNOVASİYA: MÜASİR TƏDRİS METODOLOGİYALARI

A. Oyunlaşdırma və CTF Yarışmaları

Capture The Flag (CTF) formatı kibertəhlükəsizlik təhsilinin ən effektiv praktiki komponentlərindən biri kimi qəbul edilir. Bu format tələbələrə real dünya ssenarilərinə uyğun mühitdə şəbəkə kəşfiyyatı, zəifliklərin istismarı, kriptoqrafik tapmacanın həlli, əks mühəndislik kimi bacarıqlar qazandırır. PicoCTF, Hack The Box, TryHackMe kimi platformalar tədris prosesinin ayrılmaz hissəsinə çevrilmişdir.

CTF yarışmalarının akademik mühitə inteqrasiyası beynəlxalq miqyasda uğurla sınaqdan keçirilmişdir. Carnegie Mellon, MIT, Georgia Tech kimi universitetlər CTF-i fənn proqramlarının məcburi elementi kimi tətbiq etmişdir. Azərbaycan kontekstində milli CTF yarışmalarının institutsionallaşdırılması, universitetlər arası müsabiqə formatının yaradılması və beynəlxalq yarışmalara iştirakın dəstəklənməsi prioritet tədbirlər kimi tövsiyə olunur. DTX Akademiyasının bu yarışmalarda metodoloji rəhbərlik rolu üstlənməsi xüsusilə məqsədəuyğundur.

B. Süni İntellekt Əsaslı Fərdiləşdirilmiş Təlim

Süni intellekt (Sİ) texnologiyaları tədris prosesini köklü şəkildə dəyişdirir. Adaptiv öyrənmə sistemləri tələbənin bilik səviyyəsini real-vaxt rejimində qiymətləndirir və fərdi öyrənmə yolları təklif edir. Kibertəhlükəsizlik sahəsində Sİ-nin tədrisə tətbiqi aşağıdakı istiqamətlərdə inkişaf edir:

- Simulyasiya mühitlərinin yaradılması: Sİ əsaslı kiberhücum simulyatorları tələbələrə nəzarətli şəraitdə real hücum və müdafiə ssenariləri keçməyə imkan verir. Bu simulyatorlar real şəbəkə davranışını modelləşdirir və hücumçunun taktikasını dinamik şəkildə dəyişdirir.
- Avtomatik qiymətləndirmə: Sİ modellər tələbənin laboratoriya tapşırıqlarını, kod keyfiyyətini və problem həll strategiyalarını qiymətləndirir, müəllimə ətraflı analitika təqdim edir.
- Təhdid kəşfiyyatı simulyasiyası: Böyük verilənlər toplusuna əsaslanan Sİ modellər tələbələrə real kiber insidentlərin analizi üzrə praktiki bacarıqlar qazandırır.

C. Cyber Range — Virtual Poliqon İnfrastrukturu

Kibertəhlükəsizlik laboratoriyaları - Cyber Range adlanan virtual poliqonlar - sahənin ən vacib infrastruktur elementlərindən biridir. Bu platformalar real şəbəkə topologiyalarını, zərərli proqram nümunələrini və hücum ssenarilərini təhlükəsiz mühitdə modelləşdirməyə imkan verir. Fərdi simulyasiya mühitindən fərqli olaraq, Cyber Range platformaları çoxtərəfli qarşıdurma ssenariləri - qırmızı komanda (hücumçu) və mavi komanda (müdafiəçi) - üzərindən komanda əməkdaşlığı bacarıqlarını inkişaf etdirir.

Cədvəl II-də seçilmiş ölkələrin Cyber Range infrastrukturunun müqayisəsi verilmişdir. Cədvəldən göründüyü kimi, Azərbaycan Cyber Range inkişafında regionun digər ölkələrindən geri qalır. Bu boşluğun aradan qaldırılması üçün dövlət investisiyası və beynəlxalq tərəfdaşlıq zəruri şərtdir.

CƏDVƏL II. SEÇİLMİŞ ÖLKƏLƏRDƏ CYBER RANGE İNFRASTRUKTURUNUN MÜQAYİSƏSİ

Ölkə	Platforma	İstifadəçi	Maliyyə	İnteqrasiya
Estoniya	NATO CCDCOE CR	5 000+	NATO/ Dövlət	Yüksək
İsrail	CyberGym	10 000+	Özəl/ Hökumət	Yüksək
Sinqapur	CSTAR/CSA	8 000+	Dövlət	Orta-yüksək
Gürcüstan	CERT-Georgia CR	2 000+	AB/Dövlət	Orta
Azərbaycan	Pilot mərhələ	< 500	Dövlət	Aşağı

IV. AKADEMİYA SƏNAYE-DÖVLƏT ƏMƏKDAŞLIĞI

A. Üçtərəfli Tərəfdaşlıq Modeli

Beynəlxalq təcrübə göstərir ki, kibertəhlükəsizlik sahəsindəki ən effektiv kadr hazırlığı proqramları üçtərəfli - akademiya, özəl sektor və dövlət - tərəfdaşlıq modelinə əsaslanır. Bu modelin Azərbaycan üçün uyğunlaşdırılmış variantında ETN İnformasiya Texnologiyaları İnstitutu elmi-metodoloji koordinasiyanı, AzTU və BDU akademik hazırlığı, özəl şirkətlər praktiki bacarıq inkişafını, DTX Akademiyası isə dövlət sektoru üçün ixtisaslaşmış kadr hazırlığını üzərinə götürür.

Modelin effektiv işləməsi üçün aşağıdakı mexanizmlər zəruridir:

- sənayenin kurikulum formalaşmasına aktiv şəkildə cəlb edilməsi;
- praktikant proqramlarının strukturlaşdırılması və kredit sisteminə inteqrasiyası;
- birgə tədqiqat layihələrinin maliyyələşdirilməsi üçün fond yaradılması;
- sertifikasiya xərclərinin dövlət tərəfindən subsidiyalaşdırılması.

B. DTX Akademiyasının Rolu

Azərbaycan Respublikası Dövlət Təhlükəsizliği Xidmətinin Heydər Əliyev adına Akademiyası kibertəhlükəsizlik sahəsində dövlət sektoru üçün ixtisaslaşmış kadr hazırlığının əsas dayağıdır. Akademiya aşağıdakı istiqamətlərdə fərqlənir: milli kiber insidentlərə operativ müdaxilə üzrə praktiki təlim proqramları; kritik informasiya infrastrukturunun qorunması üzrə ixtisaslaşma; rəqəmsal kriminalistika və hüquqi-texniki ekspertiza sahəsində kadr yetişdirilməsi.

Akademiyanın ali təhsil müəssisələri ilə əlaqələndirilmiş birgə tədris proqramları həyata keçirməsi bir neçə əsas üstünlük verir: tələbələr real dövlət kibertəhdid ssenariləri üzərindən praktik bacarıq qazanır; akademik tədqiqatlar operativ

ehtiyaclara uyğun istiqamətləndirilir; məzunlar milli kibertəhlükəsizlik sisteminə daha sürətlə inteqrasiya olunur [4].

C. Beynəlxalq Əməkdaşlıq Mexanizmləri

NATO Kibermüdafiə Mükəmməllik Mərkəzi (CCDCOE), ENISA (Avropa Birliyi Kibertəhlükəsizlik Agentliyi) və ITU (Beynəlxalq Telekommunikasiya İttifaqı) ilə əməkdaşlıq Azərbaycanın kibertəhlükəsizlik potensialının artırılmasında mühüm rol oynaya bilər. Locked Shields, Crossed Swords kimi beynəlxalq kibermüdafiə təlimlərinə iştirak milli komandaların bacarıqlarını əhəmiyyətli dərəcədə artırır [5]. DTX Akademiyasının bu cür beynəlxalq məşqlərə cəlb edilməsi ölkənin regional kibertəhlükəsizlik mövqeyini gücləndirər.

Bundan əlavə, postsovet məkanındakı ortaq kiber insidentlər müstəvisində Gürcüstan, Ukrayna və Baltik dövlətlərinin müvafiq qurumları ilə məlumat mübadiləsi mexanizmlərinin qurulması regionda kiberdayanıqlığın artırılmasına töhfə verə bilər.

V. MÜZAKİRƏLƏR

Aparılmış tədqiqat əsasında Azərbaycanda kibertəhlükəsizlik üzrə təhsilin inkişafı üçün beş strateji istiqamət müəyyənləşdirilmişdir. Hər bir istiqamət konkret tədbirlər toplusu ilə müşayiət olunur.

Kurikulumun modernləşdirilməsi**:** Mövcud proqramlara bulud təhlükəsizliyi, süni intellekt əsaslı kibertəhdid analizi, OT/ICS sistemlərinin mühafizəsi, sıfır güvən (zero-trust) arxitekturası kimi aktual modulların əlavə edilməsi vacibdir. Kurikulum yeniləmələri ildə ən azı bir dəfə sənaye tərəfdaşları ilə birgə nəzərdən keçirilməlidir.

Milli CTF ekosisteminin yaradılması: Universitetlər arası milli CTF çempionatının institutsionallaşdırılması, ən yaxşı iştirakçıların beynəlxalq yarışmalara göndərilməsi üçün dövlət təqaüdlərinin ayrılması tövsiyə olunur. DTX Akademiyası bu yarışmaların metodoloji koordinatoru qismində çıxış edə bilər.

Cyber Range infrastrukturu: AzTU, BDU, ETN İTİ və DTX Akademiyasının birgə istifadə edəcəyi milli Cyber Range platformasının yaradılması üçün dövlət investisiyasının cəlb edilməsi strateji prioritet hesab edilir. Gürcüstanın CERT-Georgia təcrübəsi bu sahədə faydalı model kimi götürülə bilər.

Müəllim hazırlığı: Kibertəhlükəsizlik fənnlərini tədris edən müəllimlərin müntəzəm olaraq beynəlxalq sertifikasiya proqramlarından keçirilməsi, sənaye mütəxəssislərinin qonaq mühaziçi kimi cəlb edilməsi, DTX Akademiyasının praktikantlarının ali məktəb laboratoriyalarında köməkçi müəllim qismində fəaliyyəti.

DTX Akademiyası ilə inteqrasiya: Akademiyanın praktiki təcrübəsinin ali təhsil müəssisələrinin tədris proqramlarına inteqrasiyası, birgə laboratoriya infrastrukturundan istifadə, hüquqi-texniki ekspertiza, rəqəmsal kriminalistika üzrə ortaq kurs proqramlarının hazırlanması.

NƏTİCƏ

Bu məqalədə Azərbaycanda kibertəhlükəsizlik üzrə təhsil, innovasiya və əməkdaşlığın mövcud vəziyyəti sistemli şəkildə təhlil edilmiş, inkişaf perspektivləri müəyyənləşdirilmişdir. Azərbaycan Texniki Universiteti, ETN İnformasiya Texnologiyaları İnstitutu, Azərbaycan Kibertəhlükəsizlik Təşkilatları Assosiasiyası və DTX Akademiyasının mövcud potensialı birlikdə dəyərləndirilərək tədqiq edilmişdir.

Tədqiqat göstərdi ki, sahədəki kadr çatışmazlığını aradan qaldırmaq üçün tək bir tədbirlə deyil, kompleks yanaşma ilə hərəkət etmək lazımdır. Kurikulumun müasirləşdirilməsi, CTF mədəniyyətinin yayılması, Cyber Range infrastrukturunun yaradılması, beynəlxalq əməkdaşlığın genişləndirilməsi, DTX Akademiyasının sistem daxilindəki inteqrasiyası və akademiya-sənaye-dövlət tərəfdaşlığının institutsionallaşdırılması — bu istiqamətlərin sinergiyası Azərbaycanı regional kibertəhlükəsizlik liderinə çevirmək üçün zəruri zəmini yarada bilər. Gələcək tədqiqatlar üçün tövsiyə olunan istiqamətlər: kibertəhlükəsizlik üzrə gender bərabərsizliyinin aradan qaldırılması, orta məktəb səviyyəsindən başlayan kiberhəssaslıq maarifləndirməsi proqramları, Azərbaycanın ENISA Tədris Çərçivəsinə inteqrasiyası və DTX Akademiyası əsasında regional kibertəhlükəsizlik mərkəzinin yaradılması.

ƏDƏBİYYAT

[1] World Economic Forum, "Global Cybersecurity Outlook 2024," WEF Report, Geneva, 2024.

[2] Cybersecurity Ventures, "2023 Cybercrime Report," Cybersecurity Ventures, Northport, NY, 2023.

[3] E. Luiijf and M. Kernkamp, "Sharing cyber security information: Good practice stemming from the Dutch public-private-participation approach," in Proc. Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1-8, 2015.

[4] Azərbaycan Respublikası Dövlət Təhlükəsizliği Xidmətinin Heydər Əliyev adına Akademiyası, Rəsmi sayt, Bakı, 2024. https://academy.dtx.gov.az

[5] NATO CCDCOE, "Cyber Exercises," Cooperative Cyber Defence Centre of Excellence, Tallinn, 2023. https://ccdcoe.org/exercises/

Cybersecurity Education, Innovation and Collaboration

Mahir Talibov
State Security Service, Baku, Azerbaijan
mahirtalibov5@gmail.com

Abstract–In the era of rapid digital transformation, demand for qualified cybersecurity specialists has grown sharply. The study analyzes existing cybersecurity education models in Azerbaijan, personnel training challenges, and the state of academia-industry-government cooperation. The contribution of the Academy named after Heydar Aliyev of the State Security Service to professional training is examined separately. New AI-based teaching methodologies, international cooperation mechanisms, and recommendations for specialized laboratory infrastructure are proposed. Results indicate that a comprehensive approach — curriculum modernization, strengthening certification systems, and multilateral cooperation frameworks — is essential for addressing the talent shortage in the field.

Keywords– cybersecurity education; innovative teaching methodologies; academia-industry-government collaboration; personnel training; digital skills; CTF competitions; artificial intelligence.