

İnformasiya Təhlükəsizliyi İxtisası üzrə Kadr Hazırlığının Mövcud Vəziyyəti və Bəzi Problemləri

Akif Orucaliyev¹, Fərid Süleymanov²

^{1,2}Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası, Bakı, Azərbaycan

¹akiforucaliyev@gmail.com, ²faridsuleymanov2@gmail.com

Xülasə— İnformasiya təhlükəsizliyi ixtisası üzrə bakalavr hazırlığı üçün Azərbaycan Respublikası Təhsil Nazirliyinin Dövlət Standartında nəzərdə tutulmuş təhsil proqramında yer alan humanitar, ixtisas, eləcə də seçmə fənlərinin bu ixtisas üzrə mütəxəssis hazırlığında real vəziyyətin araşdırılmasına ehtiyac vardır. Bu məqsədlə təqdim olunan məqalə “İnformasiya təhlükəsizliyi” ixtisası üzrə təhsil verən ali məktəblərin tədris planlarında yer alan ixtisas və humanitar fənlərinin mövcud tədrisinin bəzi aspektləri araşdırılır, daha savadlı kadr hazırlığı üçün Azərbaycan Respublikasının müvafiq strategiya və tədbirləri əsasında nəyə daha çox diqqət yetirilməli olan məsələlər analiz edilir.

Açar sözlər— təhsil proqramı; informasiya təhlükəsizliyi; təhlükəsizlik; kriptografiya; kadr hazırlığı.

I. GİRİŞ

Müasir dövrdə dövlətin informasiya suverenliyinin qorunması və kritik infrastrukturun təhlükəsizliyinin təmini birbaşa yüksək ixtisaslı kadr potensialından asılıdır. Azərbaycan Respublikasında "İnformasiya təhlükəsizliyi" ixtisası üzrə kadr hazırlığı, profil üzrə bakalavriat səviyyəsinin Ali Dövlət Təhsil Standartları çərçivəsində tənzimlənir. Lakin sürətlə inkişaf edən kibertəhdidlər və texnoloji transformasiyalar fonunda, mövcud təhsil proqramlarının məzmunu ilə real bazar tələbləri arasında müəyyən disbalansın yarandığı müşahidə olunur.

Tədqiqatın əsas obyektini 240 kreditlik təhsil proqramının strukturu, ixtisas fənlərinin paylanma nisbəti və tədris metodologiyasının səmərəliliyi təşkil edir. Xüsusilə, "Azərbaycan Respublikasının İnformasiya Təhlükəsizliyi və Kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası"nda qarşıya qoyulan strateji hədəflər — milli kriptografik alqoritmlərin yaradılması və yüksəkixtisaslı mütəxəssis bazasının formalaşdırılması — təhsil proqramındakı mövcud saat bölgüsü ilə ciddi şəkildə qarşılaşdırılmalıdır.

Məqalədə, proqramda yer alan "Kriptografiyanın əsasları" kimi fundamental fənlərin kredit azlığı, laboratoriya mühitinin çatışmazlığı və təcrübə saatların nəzəriyyəyə nisbətdə qeyri-mütənasibliyi akademik müstəvidə təhlil edilir. Əsas məqsəd, ali təhsil müəssisələrində aparılan hazırlıq prosesinin formal xarakterdən uzaqlaşaraq, təbiiq vərdislərə söykənən real kadr hazırlığına çevrilməsi üçün zəruri olan metodoloji dəyişiklikləri əsaslandırmaqdır.

II. ALI DÖVLƏT TƏHSİL STANDARTINDA KREDİT BÖLGÜSÜNÜN ANALİZİ

“İnformasiya təhlükəsizliyi” ixtisası üzrə kadr hazırlayan hər bir ali məktəb aydın məsələdir ki, bu ixtisas üzrə Azərbaycan Respublikası Təhsil Nazirliyinin bakalavriat səviyyəsinin Ali Dövlət Təhsil Standartına əsaslanmalıdır. 4 illik təhsil üçün nəzərdə tutulmuş bu təhsil proqramına diqqət yetirsək 240 krediti əhatə edən təhsil proqramında ilk növbədə profil üzrə zəruri fənlər deyil Azərbaycan tarixi, Azərbaycan dilində işgüzar və akademik kommunikasiya, xarici dildə işgüzar və akademik kommunikasiya kimi sözsüz vacib fənləri əhatə edən (cəmi 24 kredit), eləcə də seçmə fənlər blokuna daxil olan 7 fənni, yəni psixologiya, sosiologiya, hüququn əsasları, mühəndis etikası, kritik düşünmə, sahibkarlığın əsasları və biznesə giriş və təhsil və karyera planlaması fənlərini əhatə edən cəmi 6 kreditli ümumi fənlər blokunu görürük. Bütövlükdə bu blok Cəmi 30 krediti, yəni 450 saatlıq tədrisi nəzərdə tutur.

Təhsil proqramında verilmiş növbəti blok 120 krediti əhatə edən ixtisas fənləri blokudur. Bu bloka ixtisas yönümlü fundamental fənlər olan riyazi analiz, xətti cəbr, diskret riyaziyyat və ehtimal nəzəriyyəsi fənləri (cəmi 22 kredit), eləcə də informasiya təhlükəsizliyinin, proqramlaşdırmanın, kibertəhlükəsizliyin, kompüter şəbəkələrinin, kriptografiyanın, rəqəmsal kriminalistikanın əsasları fənləri, həmçinin əməliyyat sistemləri, şəbəkə, verilənlər bazalarının, veb, bulud, elektronikanın əsasları və İoT-nin və sənaye idarəetmə sistemlərinin təhlükəsizliyi fənləri və bir neçə ixtisas fənləri daxildir. Bütövlükdə ixtisas fənləri 120 kreditli tədrisi nəzərdə tutur (1800 saat).

Təhsil proqramının axırında ali təhsil müəssisəsinə tövsiyyə edilən 27 seçmə fənnin daxil olduğu blok (cəmi 60 krediti əhatə edən) və 30 krediti əhatə edən təcrübə bölmələri gəlir. İxtisas fənləri blokuna daxil olan fənlər aşağıdakılardır:

Əməliyyat Sistemləri (5 kredit), Şəbəkələrin əsasları-(6 kredit), Şəbəkə təhlükəsizliyi (5 kredit), Veb təhlükəsizlik (5 kredit), Proqramlaşdırmanın əsasları (6 kredit), Verilənlər bazalarının təhlükəsizliyi (5 kredit), İnformasiya təhlükəsizliyinin əsasları (6 kredit), Kiber təhlükəsizliyin əsasları (6 kredit), İnformasiya təhlükəsizliyinin idarəedilməsi sistemləri (5 kredit), İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquq aspektləri (5 kredit), Kriptografiyanın əsasları (5 kredit), Bulud təhlükəsizliyi-(5 kredit), Nüfuzetmə signallarının əsasları (8 kredit), Elektronikanın əsasları və İoT təhlükəsizliyi (5 kredit),

Təhlükəsiz proqramlaşdırma (5 kredit), Rəqəmsal kriminalistikanın əsasları (8 kredit), Sənaye idarəetmə sistemləri təhlükə (5 kredit), Mülki müdafiə (3 kredit), Cəmi 120 kredit.

Qalan saatlar Seçmə fənlər arasında bölünüb-60 kredit.

II. DİNAMİK TEKNOLOJİ DƏYİŞİKLİKLƏR VƏ AKADEMİK UYGUNLAŞMA PROBLEMLƏRİ

Bu fənlər və onlara ayrılan saatlar informasiya təhlükəsizliyi üzrə mütəxəssis yetişdirilməsinə kifayət edirmi?

Hər şeydən əvvəl qeyd etmək ki, Dövlət Standartı gələcək mütəxəssis hazırlığına minimal tələbləri təyin edir. Deməli ehtiyac varsa tədris planına müəyyən əlavələr edilə bilər. Lakin akkreditasiya məsələsi səbəbindən bu məsələdə ali məktəblər standartı pozmaqdan ehtiyat edirlər.

Məlumdur ki, “İnformasiya təhlükəsizliyi” ixtisası üzrə tədris planında tədrisi nəzərdə tutulan ixtisas fənlərinin böyük əksəriyyətinin məzmunu bu fənlərin əsaslandığı texnologiyaların dinamik dəyişməsi ilə ayaqlaşması demək olar ki, mümkün deyildir. Başqa sözlə desək bu ixtisas fənlərində tədris olunan nəzəri və praktiki materiallar müasir İnformasiya texnologiyalarının sürətli inkişafından geri qalır.

Biz diqqəti Təhsil proqramının ixtisas fənləri blokuna daxil olan “Kriptografiyanın əsasları” fənninə yönəltmək istəyirik. “Azərbaycan Respublikasının İnformasiya Təhlükəsizliyi və Kibertəhlükəsizliyə dair 2023 – 2027-ci illər üçün Strategiyası”nın həyata keçirilməsi ilə bağlı tədbirlər planı”nda göstərilir.” [1].

“Kriptografiyanın əsasları” fənninin bu strategiyada qarşıya qoyulmuş mütəxəssis hazırlığını nə dərəcədə təmin edə bilməsinə diqqət etmək. Cəmi 5 krediti əhatə edən bu fənnin tədrisinə qoyulan tələblərdə deyilir: “Bu kurs çərçivəsində tələbələr ənənəvi kriptografiyanın yaranması və inkişafına dair qısa tarixi, aktuallığını, tətbiq sahələrini və mövcud problemlərini, həmçinin müasir kriptosistemlər və şifrləmə üsulları ilə birlikdə kriptografiyanın informasiya təhlükəsizliyinin hansı prinsiplərini necə təmin etdiyini öyrənirlər. Kursda blok, axın və açıq açarlı şifrləmə alqoritmləri ilə yanaşı qabaqcıl kriptografik alqoritmlər icmal edilir. Bu alqoritmlərin praktiki tətbiqləri ilə əlaqəli məlumat verilir” [2]. Göründüyü kimi kifayət qədər riyazi mürəkkəbliyə malik müasir simmetrik və asimmetrik kriptosistemləri icmal etmək onlar haqqında heç nə deməyə ekvivalentdir. Axı laboratoriya işləri ilə təmin olunmayan bu kriptografik alqoritmlərin tədrisi fiktiv tədris deməkdir. Təəssüf ki, təhsil proqramında laboratoriya işləri haqqında heç nə deyilmir.

Təhsil proqramının “Kriptografiyanın əsasları” fənni üzrə təlim nəticələri haqqında deyilir:

FTN 1 – Klassik və müasir kriptografiya arasındakı fərqləri bilməli, klassik şifrlərin kriptanalizi metodları ilə tanış olmalıdır. Simmetrik və asimmetrik şifrləmə sistemlərinin fərqlərini bilməlidir. FTN 2 – İnformasiya təhlükəsizliyi prinsiplərindən konfidensiallıq və tamlığın, o cümlədən auditenfikasiya və idrak edilməmə prinsiplərinin kriptografik üsullarla necə təmin olunduğunu bilməlidir. FTN 3 – Blok şifrlər və axın şifrlər arasındakı fərqləri, onlara uyğun alqoritmlər və bu alqoritmlərin tətbiq sahələrini bilməlidir. FTN 4 – Açıq açarlı şifrlərlə əlaqəli alqoritmləri, onların

tətbiqlərini bilməlidir. Açıq açar infrastrukturunu haqqında məlumatlı olmalıdır. FTN 5 – Heş funksiyaların xüsusiyyətlərini bilməli, onlardan istifadə edərək tamlığın necə təmin edildiyini və rəqəmsal imzalardakı mahiyyətlərini bilməlidir. FTN 6 – Qabaqcıl kriptografik protokolları və onların tətbiqlərini bilməlidir [2].

Cəmi 5 kreditli tədrisdə müasir kriptografik üsulları tədris etməklə paralel onların özləri qədər heçdə az riyazi mürəkkəbliyi olmayan kriptanalizi üsullarını səmərəli tədris etmək mümkün deyildir. Belə tədris kriptografiya və kriptanaliz haqqında ibtidai təsəvvürdən başqa bir şey deyildir. Və belə tədrislə milli kriptografik alqoritmlər yarada bilən mütəxəssis yetişdirmək olmaz. Fikrimizcə “Kriptografiyanın əsasları” fənni ilə bərabər həm kriptografik üsulların, həm də steqanoqrafik üsulların kriptozanalizini əhatə edən “Kriptozanaliz” fənni də tədris olunmalıdır.

Maksimum 75 saatlıq nəzəri və praktiki tədrisdə klassik kriptografiyanı, XX əsr kriptografiyasını və müasir simmetrik və asimmetrik kriptosistemlərini, eləcə də müasir postkvant kriptosistemlərinin mahiyyətini, praktiki aspektlərini, laboratoriya mühitində (əgər belə laboratoriya varsa) tədris etmək, yəni azı minimum bilik vermək üçün qeyri-münasib hesab edirik. Nəzərə alsaq ki, bəzən 75 saatlıq auditoriya tədrisi azaldılaraq 60 saata da endirilə bilər, onda informasiya təhlükəsizliyi üzrə mütəxəssis hazırlığını tam hazırlıq hesab etmək düzgün olmazdı. Bəzi ali məktəblərdə, misal üçün BANM-da kriptografiya fənni kriptografiyaya giriş (5 kredit), tətbiqi kriptografiya (5 kredit), tədris olunur. ADNSU-da “Kriptografiyanın əsasları” fənni (30s müh.,30 lab) və “Kriptografiya və şifrləmə (magistraturada) (30 müh +15 lab) kimi tədris olunur.

“Kriptografiyanın əsasları” fənni informasiya təhlükəsizliyi üzrə bakalavr hazırlığında fundamental əsaslardan birini təşkil edir. Bu fənni tədris edən müəllim gələcək mütəxəssisin riyazi təfəkkürünün tələb olunan səviyyədə formalaşdırır. İnformasiya təhlükəsizliyi üzrə bakalavr hazırlığında riyaziyyatsız kriptografiya yol verilməzdir. Bu iş müxtəlif mütəxəssislərin komanda işi olmalıdır.

III. PRAKTIKA VƏ LABORATORİYA İŞLƏRİ HAQQINDA

“İnformasiya təhlükəsizliyi” ixtisası üzrə Dövlət Standartında təcrübə üçün 30 kredit (450 saat - 5 günlük təhsil həftəsi üzrə) ayrılmışdır. Dövlət Standartının Təcrübə bölümündə qeyd edilir: “Təcrübə tələbənin nəzəri biliklərinin praktikada tətbiqi, eləcə də peşə bacarıqlarının gücləndirilməsi baxımından önəmlidir”.

O fakt aydındır ki, müəyyən sahə üzrə mütəxəssis hazırlığı kadrlardan, laboratoriyalardan, praktika və akademik düzgün tədrisdən asılıdır. Belə ki, bu işdə yalnız nəzəriyyə ilə kifayətlənmək düzgün deyil. Bu zaman ən optimal model fundamental müəllimlər, tətbiqi mütəxəssislər və sənayedən gəlmiş mütəxəssislərlə bu işi qurmaq olar.

Bu mənada dövlət proqramına baxsaq təcrübəyə cəmi 15 həftə vaxt ayrılıb ki, bu da nəzəri təlimə ayrılmış həftələrdən 7 dəfə azdır. Bəs tələbə (kursant) praktiki vərdisləri haradan alacaqdır? Deməli tələbə yüklənir və biliyini yoxlamaq üçün yer tapa bilmir. O da mümkündür ki, 15 həftə təcrübə kifayət

edər, əgər proqramda yazıldığı kimi, müasir stend və müvafiq təlim vasitələri ilə təmin olunmuş laboratoriyalar olsa. Proqram təminatı ilə bu sahədə boşluğu doldura bilmək olar, lakin proqram-aparat vasitələr təminatı olmadan mümkün deyildir.

Humanitar fənləri və ya xarici dil fənlərini müəyyən faiz şişirtməklə, kriptografiya fənninin saatlarını azaltmaqla, təcrübi biliklərin əldə olunmasına az yer verməklə təhsil proqramının məzunu formal olaraq Dövlət standartına uyğun gəlir, lakin savadlı mütəxəssis kimi yox.

İxtisas fənlərində praktikaya çox yer verilməlidir.

İxtisas fənlərinin məqsədi yalnız nəzəri bilikləri tələbələrə ötürmək deyil, həm də onların real iş mühitində tətbiq edilə biləcək praktik bacarıqlarını formalaşdırmaqdır. Xüsusilə kibertəhlükəsizlik sahəsində ixtisas fənləri, məsələn, şəbəkə təhlükəsizliyi, kriptografiya, təhlükəsizlik auditi, penetrasiya testləri, sistem və tətbiq təhlükəsizliyi, CTF və laborator məşğələlər tələbənin həm müdafiə, həm də hücum təfəkkürünü inkişaf etdirir.

Praktik məşğələlər aşağıdakı funksiyaları yerinə yetirməlidir:

1) Təcrübə əsaslı öyrənmə: Tələbələr nəzəri bilikləri real sistemlər üzərində sınaq olaraq onların məntiqini və tətbiq imkanlarını daha dərindən mənimsəyirlər.

2) Hücum-müdafiə bacarıqları: CTF, pentest və laborator ssenarilər tələbələrdə hücum və müdafiə strategiyalarını planlaşdırmaq və həyata keçirmək bacarığını formalaşdırır.

3) Problem həll etmə və analitik düşüncə: Real tapşırıqlar tələbələri tək-cə proseduru izləməyə deyil, həm də kritik analiz aparmağa öyrədir.

4) Komanda işi və layihə yönümlü təcrübə: Praktik tapşırıqlar tələbələrə komanda şəklində işləmə və sənaye standartlarına uyğun layihələri idarə etmə bacarıqlarını aşılayır.

Əgər ixtisas fənlərində praktiki məşğələlər üçün kifayət qədər vaxt ayrılmasa, proqram yalnız nəzəriyyəyə əsaslanan “deklarativ” tədris modelinə çevrilir. Bu halda məzunlar real iş mühitində tətbiq olunacaq bacarıqlara malik olmur, audit, risk qiymətləndirilməsi, təhlükəsizlik planlaşdırılması və pentest kimi əsas proseslərdə səmərəli fəaliyyət göstərə bilmirlər.

Beləliklə, ixtisas fənlərində praktiki hazırlığa ciddi yer ayrılması proqramın əsas prioritetlərindən biri olmalıdır. Bu yanaşma tələbələrdə nəzəri biliklərin real tətbiqini təmin edir və kibertəhlükəsizlik üzrə peşəkar, ixtisaslaşmış kadrların yetişdirilməsini mümkün edir.

Ədəbiyyat haqqında. “İnformasiya təhlükəsizliyi” ixtisası üzrə, bütövlükdə kibertəhlükəsizlik sahəsində müvafiq fənlər üzrə dərslilər və dərs vəsaitləri ya yoxdur, yada ki, çox azdır. Bundan başqa mövcud dərslilər və dərs vəsaitlərinin əhatə etdiyi tədris materialları təhlükəsizlik texnologiyalarının sürətindən geri qaldığı üçün yetərli hesab edilə bilməz.

Azərbaycanda informasiya və kibertəhlükəsizlik sahəsində kadr potensialının gücləndirilməsi məqsədilə ixtisaslaşmış laboratoriyaların ali təhsil müəssisələrinin bazasında yaradılması dövlətin əsas prioritetlərindən biridir.

NƏTİCƏ

Aydın məsələdir ki, yalnız güclü IT bazası olan, müvafiq kadrları olan praktiki laboratoriyaları və müvafiq infrastrukturunu olan ali məktəb bu işin öhdəsindən gələ bilər. Əgər ali təhsil müəssisəsinin kriptografiya üzrə müvafiq müəllimi yoxdursa, informasiya təhlükəsizliyi üzrə praktikləri yoxdursa necə hazırlaya bilər? Bu istiqamətdə ən azı bir kriptograf, şəbəkə mütəxəssisi, əməliyyatlar üzrə mütəxəssis, CTF/pentest üzrə praktik olmalıdır. Bunlarsız tədris proqramı deklarativ məzmunla çevriləcəkdir. İnformasiya təhlükəsizliyi ixtisası üzrə mütəxəssis hazırlığı formal aparıla bilməz. Bizə fiktiv mütəxəssis hazırlığı lazım deyildir. Əgər ali məktəbin müvafiq laboratoriyaları yoxdursa, şəbəkə analizi aparılmırsa, bəzi ixtisas fənləri, o cümlədən kriptografiya fənni keçilmirsə və ya cəmi bir semestr keçilirsə belə mütəxəssis hazırlığı məqbul sayılmamalıdır. Başqa sözlə desək, İnformasiya təhlükəsizliyi ixtisası üzrə mütəxəssis hazırlığında əsas güc yalnız nəzəriyyəyə verilsə, praktik təlimə olduqca az yer verilsə, hücum təfəkkürü yoxdursa, CTF/pentest yoxdursa, kriptografiya yoxdursa belə tədris proqramı kibertəhlükəsizlik üzrə mütəxəssis hazırlığında yetərli qəbul edilə bilməz. Bu istiqamətdə kadr hazırlığını təhlükəsizlik laboratoriyaları olmadan baş verən tədrisi öyrədilmiş hesab etmək olmaz.

ƏDƏBİYYAT

- [1] “Azərbaycan Respublikasının İnformasiya Təhlükəsizliyi və Kibertəhlükəsizliyə Dair 2023 – 2027-ci illər üçün Strategiyası”nın həyata keçirilməsi ilə bağlı tədbirlər planı. Keçirilməsi keçirilməsi ilə bağlı tədbirlər planı.
- [2] Azərbaycan Respublikası Təhsil Nazirliyinin Bakalavriat səviyyəsinin “İnformasiya təhlükəsizliyi” ixtisası üzrə təhsil proqramı

The Current State of Human Resource Training in the Field of Information Security and Some Existing Problems

Akif Orucaliyev¹, Farid Suleymanov²

The Academy of the State Security Service of the Republic of Azerbaijan named after Heydar Aliyev, Baku, Azerbaijan

Abstract— There is a need to examine the actual state of how humanitarian, major, and elective courses included in the curriculum stipulated by the State Standard of the Ministry of Education of the Republic of Azerbaijan contribute to undergraduate training in the field of Information Security. For this purpose, the present article analyzes certain aspects of the current teaching of major and humanitarian subjects included in the curricula of higher education institutions that provide education in the “Information Security” specialization, and, based on the relevant strategies and measures of the Republic of Azerbaijan, identifies and evaluates the issues that require greater attention in order to train more competent professionals.

Keywords— educational program; information security; security; cryptography; personnel training.