Ali məktəblərdə kibertəhlükəsizlik üzrə mütəxəssis hazırlığı problemləri

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@iit.science.az

***Xülasə*— Məqalədə beynəlxalq təşkilatların və inkişaf etmiş bir sıra ölkələrin kibertəhlükəsizlik ixtisası üzrə bakalavr və magistr səviyyələrində ali təhsil standartları və qabaqcıl universitetlərin informasiya təhlükəsizliyi sahəsində təhsil proqramları analiz edilmişdir.**

Açar sözlər— informasiya təhlükəsizliyi, kibertəhlükəsizlik, təhsil standartı, peşə standartı; kurrikulum

I. GİRİŞ

Kibertəhlükəsizliyin etibarlı təmin edilməsi bütün ölkələr üçün prioritet məsələdir və bu məsələnin həllində əsas elementlərdən biri kibertəhlükəsizlik sahəsində yüksək ixtisaslı, öz biliklərini real şəraitdə tətbiq etməyə və yeni meydana çıxan kibertəhdidlərə çevik cavab verməyə qabil mütəxəssislərin hazırlanmasıdır. Hazırda əmək bazarında kibertəhlükəsizlik üzrə mütəxəssislərə böyük tələbat vardır [1]. Elektron xidmətlərin inkişafı, kiber-qoşunların formalaşdırılması, kiber-təhlükəsizlik sənayesinin qurulması, 4-cü sənaye inqilabının gətirdiyi yeni texnologiyalar bütün ölkələrdə belə mütəxəssislərə kəskin tələbat vardır.

Azərbaycan Respublikasında da kibertəhlükəsizlik sahəsində ali təhsilli mütəxəssislərin hazırlığı aktualdır və bu sahədə əlaqədar qurumlar tərəfindən müəyyən addımlar atılır. Qeyd etmək lazımdır ki, kibertəhlükəsizlik sahəsində universitetlərdə mütəxəssis hazırlığı sisteminin formalaşdırılması məsələlər kompleksinin həllini tələb edir: müvafiq peşə və təhsil standartlarının, təhsil proqramlarının hazırlanması, müasir tələblərə cavab verən müvafiq maddi-texniki bazanın yaradılması, müvafiq dərsliklərin və onlayn təhsil resurslarının yaradılması, elmi-pedaqoji kadrların hazırlanması, ali təhsil müəssisələrinin akkreditasiyası sisteminin yaradılması və s.

Bu məsələləri həll etmək üçün ilk addımlardan biri qabaqcıl dünya ölkələrində bu sahədə toplanmış təcrübənin analizidir. Təqdim olunan işdə kibertəhlükəsizlik sahəsində ali təhsilli peşəkar mütəxəssislərin hazırlanması problemlərinə baxılır.

II. KİBERTƏHLÜKƏSİZLİK ÜZRƏ KURRİKULUMLARIN ANALİZİ

Kompüter elmləri, proqram mühəndisliyi və informasiya texnologiyaları üzrə ali təhsil standartlarının hazırlanmasına ACM (Association for Computing Machinery) və IEEE-CS (IEEE Computer Society) xüsusi töhfələr vermişdir. ACM informasiya təhlükəsizliyi üzrə bilik sahələrinin kompüter elmləri üzrə kurrikuluma daxil edilməsinə ilk dəfə cəhdlər etmişdi. Orta məktəbdən sonrakı təhsil səviyyələrində kibertəhlükəsizlik proqramları üçün kurrikulum tövsiyələri (CSEC) 2017-ci ildə işləmişdir [2].

CSEC2017 kurrikulumu

CSEC2017 kurrikulumu dörd təşkilatın nümayəndələrinin daxil olduğu işçi qrup tərəfindən işlənmişdir:

- ACM
- IEEE-CS (IEEE Computer Society)
- AIS (Association for Information Systems)
- IFIP WG 11.8 (International Federation for Information Processing).

CSEC2017 səkkiz əsas bilik sahəsi üzrə təşkil olunub: Verilənlərin təhlükəsizliyi; Proqram təminatının təhlükəsizliyi; Komponentlərin təhlükəsizliyi; Əlaqələrin təhlükəsizliyi; Sistemləri təhlükəsizliyi; İnsanların təhlükəsizliyi; Təşkilatların təhlükəsizliyi; Cəmiyyətin təhlükəsizliyi. Kurrikulumda hər bir bilik sahəsi çərçivəsində tələbələrin bilməli olduqları spesifik əsas konsepsiyaların siyahısı verilir. Məsələn, Verilənlərin təhlükəsizliyi bilik sahəsində tələbələr baza kriptoqrafiya, verilənlərin tamlığı və autentifikasiya kimi əsas konsepsiyaları bilmələrini nümayiş etdirməlidirlər. Əlaqələrin təhlükəsizliyi bilik sahəsində tələbələr birləşməyə və ötürməyə yönəlmiş hücumlar sahəsində bilik və bacarıqlara malik olmalıdırlar.

Daha detallı səviyyədə CSEC2017 əhatə edilməli mövzulara aid deskriptorlar verməklə müəllimləri kurs işləri işləməyə yönləndirir. Məsələn, Verilənlərin təhlükəsizliyi bilik sahəsində Girişə nəzarət əsas konsepsiyası çərçivəsində mövzu deskriptorlarında tələbələrin tanış edilməli olduqları girişə nəzarətin bir neçə növü sadalanır.

Bilik sahələri və əsas konsepsiyalar ilə birlikdə kurrikulum fənləri başa düşmək üçün zəruri olan nəzəri və konseptual bilikləri, həmçinin bacarıqlar qazanmaq üçün praktiki tapşırıq imkanlarını da şərh edir.

CSEC2017 o faktı da əks etdirir ki, adətən, tələbələr kibertəhlükəsizlik ixtisasına Computing sahəsində beş əsas istiqamətdən birini öyrəndikdən sonra baş vururlar. Bu istiqamətlərə kompüter elmləri, kompüter mühəndisliyi,

DOI: 10.25045/NCInfoSec.2018.16

informasiya sistemləri, informasiya texnologiyaları və proqram mühəndisliyi daxildir.

CSEC2017-nin Fənn profilləri (ing. Lens) bölməsi pedaqoqları tələbənin özək fənni əsasında kibertəhlükəsizlik üzrə kurs işinə yanaşmaya, kontentin dərinliyinə və təlim nəticələrinə təsir etməklə istiqamətləndirir.

NATO kibertəhlükəsizlik kurrikulumu (*Cybersecurity: A Generic Reference Curriculum*) 2016-cı ildə hərbi akademiyalar və təhlükəsizlik sahəsində tədqiqat institutları üçün işlənmişdir [3]. Kurrikuluma aşağıdakı dörd mövzu daxildir:

Mövzu 1: Kiberfəza və kibertəhlükəsizliyin əsasları

Mövzu 2: Risk vektorları

Mövzu 3: Kibertəhlükəsizlik üzrə beynəlxalq təşkilatlar, prinsiplər və standartlar

Mövzu 4: Milli kontekstdə kibertəhlükəsizliyin menecmenti

Hər bir mövzu bloklara bölünür, təbii ki, bloklar da bölünə bilər. Məsələn, Mövzu 1 aşağıdakı bloklara bölünür:

- M1-B1: Kibertəhlükəsizlik və kiberfəza – giriş
- M1-B2: İnformasiya təhlükəsizliyi və risklər
- M1-B3: İnformasiya fəzasının strukturu: İnternetin magistral şəbəkəsi və dövlətin şəbəkə infrastrukturu
- M1-B4: Protokollar və platformalar
- M1-B5: Şəbəkə təhlükəsizliyinin arxitekturası və təhlükəsizliyin təmin edilməsi proseslərinin idarə edilməsi

Bloklar ayrıca fənlərə bölünür. Hər bir fənn baza blokları çərçivəsində öyrənilir, onların da hər biri öz növbəsində mühazirələr, təqdimatlar, konkret senarilər üzrə çalışmalar və s. kimi tədris modullarına bölünə bilər. Baxılan kurrikulumun yerli şəraitə uyğunlaşdırılması nəzərdə tutulduğu üçün əksər hallarda modulların və mühazirələrin konkret tərkibi verilmir, onlar yerli ehtiyacdan asılı olaraq detallaşdırılmalıdır. Bunun əvəzində, hər bir mövzuda müxtəlif bloklar əhatə olunur ki, onlar da əldə olunacaq məqsədləri və nəticələri tövsiyə edirlər.

Kurrikulum müəllifləri qeyd edirlər ki, kurrikulum əsasında vahid kursun yaradılması zamanı xüsusi narahatlıq doğuran üç element olacaq: kursun məqsəd və vəzifələri; nəzərdə tutulan tələbələr, xüsusilə onların texniki bilikləri və işlərinin mahiyyəti; kursa ayrılan müddət. Bu üç element texniki detallaşdırmanın səviyyəsini və təlim çalışmalarının xarakterini (mühazirələr, misallar, təlim-tanışlıq səfərləri, hərbi oyunlar və s.) müəyyən etməlidir.

Kibertəhlükəsizlik kurrikulumlarının dizaynı

Bəzi tədqiqatçılar informasiya təhlükəsizliyi kurrikulumlarının dizayn edilməsinə yuxarıdan aşağıya yanaşmaya tərəfdar çıxırlar. Bu yanaşmada gələcək mütəxəssisin görəcəyi işin tipi müəyyənləşdirilir, sonra isə iş rollarının əsasında kurrikulum dizayn edilir [4]. Digər tədqiqatçılar kurrikulum freymvorkları təqdim edirlər və biliyin ümumi sahələrini müzakirə edirlər [4]. Tədqiqatçıların əksəriyyəti informasiya təhlükəsizliyi kurrikulumuna informasiya sistemləri və kompüter elmləri aspektlərinin, həmçinin təhlükəsizliyin əsaslarının daxil edilməsini vacib sayırlar [5]. [4]-də təklif edilir ki, informasiya təhlükəsizliyi kurrikulumu 18 sahəni əhatə etməlidir: 1: İnformasiya təhlükəsizliyi qanunvericiliyi və standartları; 2: İnformasiya sistemlərinin analizi və layihələndirilməsi; 3: Sistemlərin təhlükəsizlik texnologiyaları; 4: Verilənlər bazaları; 5: Əməliyyat sistemləri; 6: Şəbəkə təhlükəsizliyi; 7: Müdaxilələrin aşkarlanması və qarşısının alınması; 8: Şəbəkə; 9: Şəbəkə təhlükəsizliyi texnologiyaları; 10: Virus; 11: Hakinq; 12: Veb təhlükəsizlik; 13: E-kommersiyanın təhlükəsizliyi; 14: Mühasibatlıq və maliyyə; 15: Statistika; 16: Risk analizi; 17: Qərarqəbuletmə nəzəriyyəsi; 18: Kriptologiya. Tələbələr əvvəlcə sistem təhlükəsizliyi kursunu götürməli, sonra isə onu şəbəkə təhlükəsizliyi və tətbiqi proqram təhlükəsizliyi kursları ilə davam etdirməlidir.

[5]-də ABŞ və Çin qabaqcıl universitetlərinin informasiya təhlükəsizliyi üzrə magistr kurrikulumlarının analizi aparılır. Vurğulanır ki, Çində kurrikulumlar telekommunikasiya, kompüter elmləri və informasiya təhlükəsizliyi texnologiyalarına geniş diqqət ayrılır. ABŞ-da isə kompüter elmləri və informasiya təhlükəsizliyi texnologiyalarına əlavə olaraq kurrikulumda müəssisə səviyyəsində təhlükəsizlik strategiyası və siyasəti, informasiya təhlükəsizliyi menecmenti və kiberhüquqa önəm verilir. Bu fərqlərin əhəmiyyətli olduğu və həm informasiya təhlükəsizliyi mütəxəssislərinin qavrayış və bacarıqlarına, həm də dövlət və özəl təşkilatlarda informasiya təhlükəsizliyinin menecmentinə təsir vedəcəyi qənaətinə gəlirlər.

ABŞ-da informasiya təhlükəsizliyi kurrikulumlarının işlənməsinə mühəndislik təşkilatları (ACM, IEEE və s.), Çində isə Təhsil Nazirliyi rəhbərlik edir. Çində İnT kurrikulumu texnologiyaların öyrənilməsinə fokuslanır, ABŞ-da isə iş fəaliyyətinin dəstəklənməsinə yönəlir.

[6]-da qabaqcıl universitetlərin 21 kibertəhlükəsizlik magistr proqramları analiz edilmişdir, əsas diqqət kursların məzmunu, strukturu, qəbul tələbləri, müddəti, qurtarma və evolyusiya üçün tələblərə yönəlmişdir.

III. NICE TƏŞƏBBÜSÜ

National Initiative for Cybersecurity Education (NICE) [7] təşəbbüsü ABŞ Ticarət Nazirliyinin tabeçiliyində olan NIST tərəfindən idarə edilir, kibertəhlükəsizlik təhsili, təlimi və işçi qüvvəsinin yetişdirilməsi üzrə hökumət, ali məktəblər və özəl sektor arasında tərəfdaşlıq təşəbbüsüdür.

NICE freymvorku NIST tərəfindən hazırlanmışdı, kibertəhlükəsizlik sahəsində iş rollarını təsvir etmək üçün taksonomiya müəyyən edir. Freymvorka üç müxtəlif komponent daxildir (mötərizədə sayları göstərilib):

- kateqoriya (7) – kibertəhlükəsizlik funksiyalarını yuxarı səviyyədə təsvir edir;
- ixtisas sahəsi (33) – kibertəhlükəsizlik sahələrini təsvir edir;

- iş rolu (52) – hər bir iş rolunun tələb edildiyi spesifik bilik, bacarıq və vərdişlərə uyğun olaraq kibertəhlükəsizlik rolunu ətraflı təsvir edir.

Hər bir kateqoriyaya daxil olan ixtisas sahələri haqqında qısa məlumatı [8]-də əldə etmək olar:

IV. QABAQCIL ÖLKƏLƏRİN TƏCRÜBƏSİ – QISA QEYDLƏR

A. Amerika Birləşmiş Ştatları (ABŞ)

ABŞ-da əksər bilik sahələri üzrə təhsil standartları və mütəxəssislərin hazırlanması keyfiyyətinin sertifikatlaşdırılması sistemi mərkəzləşdirilməyib və ştatlar səviyyəsində təşkil olunub (regional akkreditasiya komissiyaları). Bununla yanaşı, ABŞ-da informasiya təhlükəsizliyi sahəsində mütəxəssis hazırlığının standartları və sertifikatlaşdırılması ilə federal orqan – Mühəndislik və Texnologiya üzrə Akkreditasiya Şurası (ing. Accreditation Board for Engineering and Technology, ABET) məşğul olur [9]. İlk növbədə, bura kompüter elmləri, kompüter mühəndisliyi və sistem mühəndisliyi aiddir.

ABŞ-da informasiya təhlükəsizliyi sahəsində bakalavr dərəcəsi ilə təhsil proqramlarında ən çox tələb edilənlər: kompüter insidentlərinin təhqiqatı, informasiya təhlükəsizliyi, kompüter təhlükəsizliyi, kompüter şəbəkələrinin təhlükəsizliyidir. Magistratura təhsil proqramlarında isə informasiya təhlükəsizliyinin menecmenti və informasiya təhlükəsizliyinin iqtisadiyyatı (MBA dərəcəsi verilir) istiqamətləri də vardır.

Bir qayda olaraq, magistraturanın sonunda tələbənin informasiya təhlükəsizliyi sahəsində peşə sertifikatlarından birini almaq imkanı olur (məsələn, CİSSP), bu əmək bazarında onun rəqabət qabiliyyətini artırır.

B. Böyük Britaniya

Böyük Britaniyada ali məktəblərdə bakalavr hazırlığı proqramlarının əksəriyyətində kibertəhlükəsizlik və kompüter insidentlərinin təhqiqatı istiqamətləri üstünlük təşkil edir. Magistr proqramlarında isə kibertəhlükəsizlik, İT-təhlükəsizlik və kompüter insidentlərinin təhqiqatı istiqamətləri üstünlük təşkil edir.

Təhsil proqramlarının keyfiyyətinə müəyyən zəmanət vermək üçün bakalavr və magistr proqramları təqdim edən universitetlərin Milli Kibertəhlükəsizlik Mərkəzi (MKM) tərəfindən akkreditasiyası nəzərdə tutulub. MKM 2016-cı ildə Hökumət Rabitəsi Mərkəzinin tərkibində yaradılıb. Lankaster, London, Oksford, Edinburq, Surrey, Krenfild universitetlərinin və Hollovey Kral Kollecinin magistr hazırlığı proqramları həmin mərkəz tərəfindən sertifikatlaşdırılıb (universitetlərin tam siyahısı ilə MKM-in saytında tanış olmaq olar). Sertifikatlaşdırma zamanı dərəcəni verən akademik komanda, tədris olunan fənlər, tələbələrin qiymətləndirilməsi metodları, dərəcə üçün qəbul tələbləri, dissertasiya nümunələri, tələbələrin sayı, tələbələrin aldığı qiymətlər və tələbələrin əks-əlaqə rəyləri nəzərə alınır.

Böyük Britaniyada kibertəhlükəsizlik sahəsində tədqiqatları dəstəkləmək üçün MKM müvafiq qiymətləndirmədən sonra universitetlərə ACE-CSR (Academic Centres of Excellence in Cyber Security Research) statusu verir (4 il müddətinə) və doktorantları bu sxem üzrə dəstəkləyir. 2017-ci ildə 17 universitet bu statusu qazanmışdır. 2021-ci ilə kimi təxminən 150 yeni doktorantın bu sxemdən yararlanaraq vacib kibertəhlükəsizlik mövzularında tədqiqatlarını başa çatdıracaqları gözlənilir.

C. Almaniya

Almaniya ali məktəblərində kibertəhlükəsizlik üzrə mütəxəssis hazırlığı sisteminin fərqləndirici xüsusiyyəti tələbələrin kursları seçməsində nisbi sərbəstliyidir. Ali məktəb hansı kursların məcburi olduğunu müəyyən edir, həm də məcburi fənlərin siyahısı digər ölkələrlə müqayisədə kifayət qədər azdır [10].

Bolonya prosesinin prinsipləri kursların seçimlə olmasını təşviq edir, buna görə müəllimlər rəqabət şəraitində olurlar və öz kurslarını tələbələr üçün cəlbedici etməlidirlər. Müəllimlər öz fənlərinə elmi tədqiqat elementləri daxil etməyə cəhd edirlər, xüsusilə magistraturada elmi-tədqiqat yönümlü kurslar çoxdur. Bakalavr və magistr dərəcələri üçün dissertasiyalar da elmi-tədqiqatların nəticələri üzərində qurulur.

Təhsil formaları klassik xüsusiyyətlərə malik olsa da (mühazirələr, seminarlar, tələbələrin çıxışları və s.), fərqli xüsusiyyətləri də var – informasiya təhlükəsizliyi ilə əlaqəli konkret layihələrin yerinə yetirilməsi zamanı kiçik qruplarda müstəqil işə üstünlük verilir.

D. Fransa

Fransada informasiya təhlükəsizliyi sahəsində mütəxəssis hazırlığı sistemi kriptoqrafiya, şəbəkə təhlükəsizliyi və informasiya sistemlərinin auditi ilə əlaqəli məsələlərin daha dərindən öyrənilməsinə yönəlib. Tələbələrə kriptologiya və kompüter təhlükəsizliyinin riyazi aspektlərini öyrənmək üçün ciddi riyazi təhsil verilir. Şəbəkə təhlükəsizliyinin öyrənilməsi real şəbəkələrin, şəbəkə arxitekturalarının modellərində, real avadanlığın istifadə edilməsi üzərində qurulur [11].

ABŞ, Böyük Britaniya və Almaniyadan fərqli olaraq kompüter təhlükəsizliyi insidentlərinin təhqiqatı və sübutların toplanması ilə bağlı fənlərə az diqqət yetirilir.

Qeyd etmək lazımdır ki, Fransada informasiya təhlükəsizliyi sahəsində mütəxəssis hazırlığı ilə məşğul olan ali məktəblərin sayı azdır və əsasən magistraturada cəmlənib. Riyaziyyat və İnformatika ixtisası üzrə diplom lisenziyası olan istənilən şəxs magistraturaya daxil ola bilər.

Peşə lisenziyasının alınması 460 saat (13 həftə) auditoriya məşğələlərini, layihə üzərində 150 saat (4 həftə) işi və 16 həftə ərzində təcrübə keçməsini nəzərdə tutur. Qəbul edən şirkətin axtarışını tələbə özü yerinə yetirir və bu, lisenziya alınmasına hazırlığın məcburi hissəsidir. Məzunlar şirkətlərin sifarişləri ilə tədris mərkəzində təhsili və yenidən hazırlığı davam etdirə bilərlər.

E. Rusiya Federasiyası (RF)

Rusiya Federasiyasında (RF) informasiya təhlükəsizliyi sahəsində ali təhsilli mütəxəssislərin hazırlanmasına 1992-ci ildən başlanmışdır. Hazırda 100-dən çox alı məktəbdə bu sahədə mütəxəssis və bakalavr hazırlığı həyata keçirilir.

İnformasiya təhlükəsizliyi üzrə bakalavriat proqramları üçün 7 istiqamət (profil) müəyyən edilmişdir: 1) Kompüter sistemlərinin təhlükəsizliyi; 2) İnformasiya mühafizəsinin təşkili və texnologiyası; 3) İnformasiyalaşdırma obyektlərinin kompleks mühafizəsi; 4) Avtomatlaşdırılmış sistemlərin təhlükəsizliyi; 5) Telekommunikasiya sistemlərinin təhlükəsizliyi; 6) Maliyyə monitorinqinin informasiya-analitika sistemləri; 7) İnformasiyanın texniki mühafizəsi.

Qeyd etmək lazımdır ki, 2011-ci ildə Rusiya təhsil sistemi ikisəviyyəli (bakalavriat-magistratura) modelə keçsə də, birsəviyyəli model (o cümlədən, spesialitet) də saxlanmışdır. Təhsil proqramlarında məcburi fənlərin analizi göstərir ki, RF təhsil proqramları informasiya təhlükəsizliyinin təmin olunmasına kompleks yanaşmanı nəzərə alır. Belə ki, proqramların əksəriyyətində tələbələr informasiya mühafizəsinin təşkilati, hüquqi, texniki, proqram-aparat və kriptoqrafik metodları ilə əlaqəli fənləri öyrənirlər. Bütün proqramlarda çox sayda məcburi fənlər var və təhsil müəssisələrinin əksəriyyəti əvvəlki standartda nəzərdə tutulmuş məcburi fənləri də siyahıda saxlayırlar. Bir sıra ali məktəblər özlərinin tədris planlarına informasiya təhlükəsizliyi mütəxəssislərinin fəaliyyət spesifikasına aid olmayan təsadüfi fənlər (kulturologiya, nitq mədəniyyəti) də salırlar.

İnformasiya təhlükəsizliyi sahəsində mütəxəssislərin kvalifikasiya tələblərinin təsviri peşə standartlarında öz əksini tapır. RF Əmək və sosial müdafiə nazirliyi tərəfindən 2016-cı ildə 8 belə peşə standartı hazırlanmışdır, onlardan 3-ü məxfilik qrifinə malikdir, qalan 5-i isə konfidensial deyil və istifadəyə açıqdır.

Qeyd etmək lazımdır ki, əcnəbi vətəndaşların hətta ödənişli əsaslarla da informasiya təhlükəsizliyi üzrə 7 texniki ixtisasdan yalnız birinə qəbul edilməsinə icazə verilir.

Daha bir xüsusi cəhət kimi informasiya təhlükəsizliyi üzrə magistrlərin hazırlığı üçün böyük sayda büdcə yerləri ayrılmasını qeyd edək. Məsələn, 2019-cu ildə təkcə İTMO (İnformasiya Texnologiyaları, Mexanika və Optika) Universitetinə 155 büdcə yeri ayrılmışdır.

NƏTİCƏ

Kiberfəzada ölkələrin virtual sərhədlərinin qorunması əsas prioritetlərdən biridir və bu prioritetin həyata keçirilməsi strategiyasının əsas elementlərindən biri kibertəhlükəsizlik sahəsində maarifləndirmə, təlim və təhsildir.

Ölkəmizdə kibertəhlükəsizlik sahəsində yüksək ixtisaslı mütəxəssislərin hazırlığı üçün bu sahədə əlaqədar qurumlar arasında kooordinasiyanın gücləndirilməsi, onların səylərinin birləşdirilməsi, təcrübə mübadiləsi, tədris proqramlarının və elektron resursların, virtual laboratoriyaların yaradılması, kiber-hücum və müdafiə üzrə yarışların təşkili, kibertəhlükəsizlik sahəsində tədris aparan pedaqoji kadrların ixtisasının artırılması, elmi tədqiqatların daha da intensivləşdirilməsi olduqca vacibdir.

ƏDƏBİYYAT

[1] Cybersecurity workforce study – ICS(2). 2018. https://www.isc2.org/Research/Workforce-Study

[2] The CSEC2017 Joint Task Force, “Cybersecurity Curricula 2017,” version 0.95 report, 13 November 2017. www.csec2017.org.

[3] T.Tagarev, “A generic reference curriculum on cybersecurity,” Information & Security, vol. 35(2), pp. 181-184, 2016.

[4] K. Y. Kim, & K. Surendran, “Information security management curriculum design: A joint industry and academic effort,” Journal of Information Systems Education, vol. 13(3), pp. 227-236, 2002.

[5] H. Chen, S.B. Maynard, & A. Ahmad, “A comparison of information security curricula in China and the USA,” The Proc. of 11th Australian Information Security Management Conference, pp. 21-34, 2013.

[6] K. Cabaj, D. Domingos, Z. Kotulski, A. Respício, “Cybersecurity education: Evolution of the discipline and analysis of master programs,” Computers & Security, v. 75, pp. 24-35, 2018.

[7] NIST Special Publication 800-181: National Initiative for Cybersecurity Education. (NICE). The national cybersecurity workforce framework. 2017. https://doi.org/10.6028/NIST.SP.800-181

[8] L. González-Manzano, & J.M. de Fuentes, “Design recommendations for online cybersecurity courses,” Computers & Security, 80, pp. 238-256, 2019.

[9] R. Greenlaw, A. Phillips, & A. Parrish, “Is it time for ABET cybersecurity criteria?” ACM Inroads, vol. 5(3), pp. 44-48, 2014.

[10] М.С. Чванова, М.С. Анурьева? “Система высшего образования в ФРГ. Подготовка специалистов в области информационной безопасности,” Вестник Тамбовского университета. Серия: Гуманитарные науки, №110(6), с. 78-84, 2012.

[11] М.С. Чванова, М.С. Анурьева, “Подготовка специалистов в области информационной безопасности во Франции,” Вестник Тамбовского университета. Серия: Гуманитарные науки, № 111(7), с. 159-165, 2012.

PROBLEMS OF EDUCATİNG CYBERSECURİTY SPECİALİSTS İN UNİVERSİTİES

Yadigar İmamverdiyev

Institute of Information Technology of ANAS,

Baku, Azerbaijan

yadigar@iit.science.az

Abstract – The article analyzes educational standards of higher education for bachelor’s and master’s degrees from international organizations and developed countries in the field of cyber security, as well as curricula for information security at leading universities.

Keywords – information security, cybersecurity, educational standard, professional standard; curriculum.