AZƏRBAYCAN RESPUBLİKASI
ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Respublikası Elm və Təhsil Nazirliyinin
22.08 2024-cü il tarixli
2-29/3-2-540F/2024 nömrəli əmrinə
7 nömrəli əlavə

VƏTƏNDAŞLARA XİDMƏT VƏ SƏNƏDLƏRLƏ İŞ ŞÖBƏSİ
TƏSLİLƏ DÜZDÜR

Kiber təhlükəsizlik

TƏHSİL PROQRAMI (KURİKULUM)

BAKI – 2024

1. Ümumi müddəalar

1.1. Subbakalavr peşə-ixtisas dərəcəsi verən “Kiber təhlükəsizlik” ixtisasının təhsil proqramı “Təhsil haqqında” və “Peşə təhsili haqqında” Azərbaycan Respublikasının qanunlarına, Azərbaycan Respublikası Nazirlər Kabinetinin “və Təhsil Nazirliyinin müvafiq qərarları ilə təsdiq edilmiş subbakalavr peşə hazırlığını həyata keçirən tədris proqramlarının hazırlanmasını tənzimləyən müvafiq hüquqi sənəd və qaydalara uyğun hazırlanmışdır.

1.2. Yüksək texniki peşə təhsili proqramları (kurikulumlar) təlim nəticələri və məzmun standartlarını, tədris fənn/modullarını, həftəlik dərs və dərsdənkənar məşğələ saatlarının miqdarını, pedaqoji prosesin təşkili, təlim nəticələrinin qiymətləndirilməsi sistemini özündə əks etdirən sənəddir.

1.3 Təhsil Proqramı (kurikulum) tabeliyindən, mülkiyyət növündən və təşkilati-hüquqi formasından asılı olmayaraq Azərbaycan Respublikasında fəaliyyət göstərən və həmin ixtisas üzrə subbakalavr hazırlığını həyata keçirən bütün peşə təhsili müəssisələri üçün məcburidir.

1.4 Strukturda istifadə olunan işarələr:
İTP – ixtisas üzrə Təhsil Proqramı
ÜK – ümummədəni kompetensiyalar
PK – peşə kompetensiyaları

1.5 **Kiber təhlükəsizlik** ixtisası üzrə təhsil proqramlarının mənimsənilməsinin normativ müddəti və məzunlara verilən ixtisas dərəcəsi:

İxtisasın şifri və adı:	030219 Kiber təhlükəsizlik
İxtisas qrupu / İqtisadi sektorlar:	İnformasiya-kommunikasiya texnologiyası və hesablama texnikasının təmiri və servis xidməti
İxtisas dərəcəsi:	“Kiber təhlükəsizlik” ixtisası üzrə subbakalavr
Peşə təhsili səviyyəsi	Yüksək texniki peşə təhsili
Kreditlərin sayı:	180
AzMKÇ səviyyəsi:	5
İSCED kodu:	0612 Information technology security
İstinad edilən kvalifikasiya standartları və kodları:	
Təhsil forması və müddəti:	Əyani, Tam orta təhsil bazasından 3 il; Ümumi orta təhsil bazasından 4 il.
Məşğulluq imkanları:	müxtəlif yerli və beynəlxalq təşkilat və şirkətlər, dövlət qurumlarıda informasiya təhlükəsizliyi sahəsində

030219 Kiber təhlükəsizlik ixtisası Azərbaycan Respublikasının Azərbaycan Respublikasının ömürboyu təhsil üzrə Milli Kvalifikasiyalar Çərçivəsi”nin (AzMKÇ) 5-ci səviyyəsinə uyğundur.

1.6 Təhsil proqramı üzrə bir semestrə 30 kredit müəyyənləşdirilir. Bir kredit tələbənin auditoriya və auditoriyadankənar 30 saatlıq işinə bərabərdir. Tələbənin 5 (beş) günlük iş rejimində həftəlik auditoriya və auditoriyadan-kənar yükünün ümumi həcmi 45 saatdır.

Tələbənin həftəlik işinin həcmi 1,5 kreditdir. Buraxılış dövlət və semestr imtahanlarına hazırlığa, imtahanın verilməsinə və təcrübələrin keçirilməsinə ayrılmış hər bir həftə 1,5 kreditə bərabərdir. Tələbə üçün hər semestrdə 30 kreditə qədər modul və fənlərin tədrisi müəyyənləşdirilir. Müvəffəqiyyətlə təhsil alan tələbələrə əlavə ödəniş etmədən təhsil aldığı ixtisas üzrə əlavə modul (modullar) seçməyə icazə verilir və bütün hallarda bir semestrdə tələbənin götürdüyü kreditlərin sayı 40-dan çox olmamalıdır.

1.7 Müəyyən olunmuş kreditin tələbə tərəfindən yığılması məcburidir. Kreditləri müəyyən səbəblərdən qazanmayan (qazana bilməyən) tələbənin həmin modul/fənn üzrə akademik borcu qalır. Cari semestrdə müəyyən səbəbdən imtahanda (imtahanlarda) iştirak etməyən və (və ya) həmin semestrdə akademik borcu yaranmış tələbəyə növbəti semestrin dərsləri başlayanadək bir dəfə həmin imtahanı (imtahanları) vermək imkanı yaradılır. Əlavə olaraq tələbə hər bir semestrdə modul (fənni) dinləmədən akademik borcu əvvəlki semestrdə (semestrlərdə) yaranmış iki modul üzrə (hər moduldan bir dəfə olmaqla) də imtahanda iştirak edə bilər.

2. Kiber təhlükəsizlik ixtisası üzrə məzunların ixtisas xarakteristikası və kompetensiyası

2.1 Subbakalavrın ixtisas xarakteristikası.

Kiber təhlükəsizlik mütəxəssisi informasiya texnologiyaları təhlükəsizliyi və ya elektron məlumat təhlükəsizliyi kimi də tanınan, kompüter təhlükəsizliyi, kompüterlərin, serverlərin, mobil qurğuların, elektron sistemlərin, şəbəkələrin və məlumatların rəqəmsal hücumlardan qorunmasını təmin edən və istifadə zamanı ortaya çıxa biləcək riskləri idarə edən şəxsdir.

2.1.1 Peşə fəaliyyətinin əsas istiqamətləri (vəzifə və funksiyalar):

- Dövlət idarəçiliyi, bank, nəqliyyat, milli təhlükəszilik və digər sistemlərin təkmilləşdirilməsi;
- Kibermüdafiə tədbirlərinin genişləndirilməsi;
- Təhlükəsizlik boşluqları və zəifliklərı nəzərə almaq, məlumat və hesabat vermək;
- İnformasiya texnologiyaları təhlükəsizliyi və ya elektron məlumat təhlükəsizliyi kimi də tanınan, kompüter təhlükəsizliyi, kompüterlərin, serverlərin, mobil qurğuların, elektron sistemlərin, şəbəkələrin və məlumatların rəqəmsal hücumlardan qorunması;
- Fərqli hücum növlərinə görə tədbirlər görmək;
- Müxtəlif yerli və beynəlxalq təşkilatlarda, dövlət orqanlarının informasiya ehtiyatlarının qorunması;
- Təhdidlərin qarşısının alınması, təhlili və qabaqlanması;
- Kibertəhlükəsizlik sahəsində risklərin qiymətləndirilməsi və idarə olunması.

2.1.2 Peşə fəaliyyəti üzrə hazırlıq səviyyəsinə qoyulan tələblər:

İxtisas üzrə:

- İnformasiya texnologiyaları təhlükəsizliyi sahəsində biliklər
- Əməliyyat sistemləri və şəbəkələr sahəsi üzrə biliklər
- C və Python proqramlaşdırma dilləri üzrə biliklər
- Kiberhücumlar və müdafiə metodları üzrə biliklər
- Zəifliklərin aşkarlanması, qiymətləndirilməsi
- Mobil avadanlıqların təhlükəsizliyi

Yumşaq bacarıqlar (soft skills):

- Zamanın idarə olunması
- Problem həll etmə
- Yaradıcılıq

2.1.3. “Kiber təhlükəsizlik” ixtisasının hazırlanmasında bu istiqamət üzrə WSC2019_WSSS54 standartının tələbləri nəzərə alınmışdır. Müvafiq standartın aşağıdakı standartlar proqram ilə əhatə edilmiş və müvafiq sərişlərin formalaşmasında əsas götürülmüşdür.

Bilik	Bacarıq
İşin təşkili və idarə edilməsi	
• Səmərəli komanda işinin qurulması və tətbiqi • Kompüter sisteminin prinsipləri, xüsusiyyətləri	• Işi ilə bağlı rast gəlinən problemlərin optimal həll axtarışı • Vaxt məhdudluğu və işin təhvili üzrə təyin edilmiş vaxta əməl edilməsi

• Problemlər üzrə müxtəlif həllərin təklif edilməsi mövcud alətlərdən istifadə etməklə problemlərin həllini tapmaq	
Kommunikasiya və şəxslər arası ünsiyyət bacarığı	
• İş icrasında problemlərin düzgün kommunikasiyası • Tapşırıqların icrası üzrə iş axını cədvəllərinin hazırlanması • Proqram təminatı dizayn konsepsiyasının düzgün təsviri • Kiber təhlükəsizlik üzrə yoxlamalar və tədbirlərin və nəticələrin düzgün sənədləşdirilməsi	• Kiber təhlükəsizlik üzrə yoxlamalar və tədbirlər üzrə sənədləşmənin düzgün tətbiqi • Standart və tələbləri başa düşür və tətbiq üçün düzgün şərh edir • Müştəri irad və qeydlərini anlayır və müvafiq həllər formalaşdırır • Biznes ehtiyaclara uyğun müvafiq konsepsiya düşünür • İnformasiya sistemlərinin təhlükəsizliyinin təmini üçün siyasət və prosedurların öyrənilməsi və tətbiqi
Təhlükəsiz İT sistem dizaynı və yaradılması	
• İT risk idarə etmə standartları, qayda və prosedurları • Kiber müdafiə və zəiflik yoxlama alətləri və onların imkanları • Əməliyyat və şəbəkə sistemləri və tənzimləmələri • Proqramlaşıdrma konseptləri, proqramlaşdırma dilləri, testlər, fayl tipləri • Proqram təminatı hazırlanmasında kiber təhlükəsizlik prinsipləri və metodları	• Kiber təhlükəsizlik prinsiplərinin təşkilatın xüsussiyyəti və tələbinə uyğun tətbiqi • Xüsusi tələblərə uyğun olaraq sistemin yoxlanması üzrə həllər hazırlayır və tətbiq edir • Mövcud proqram təminatı və sistem üzrə modifikasiyaları icra edir • Mövcud və ya yeni proqram təminatı və sistemin təhlükəsizlik təhlilini aparır və nəticələri təqdim edir •
Sistem əməliyyatları və texniki qulluğun təhlükəsizliyi	
• Məlumat bazası və SQL dili • Şəbəkə protokolları (TCP/IP, DNS və s.) • Şəbəkə təhlükəsizliyi arxitekturası, tipologiya, protokollar, komponenetlər • Sistem inzibatçılığı, şəbəkə və əməliyyat sistemi təhlükəsizliyinin möhkəmləndirmə texnikaları • Avtorizasiya, müəyyənləşdirmə və istifadə hüququ vermək metodları • Kiber müdafiə prinsipləri	• Şəbəkə infrastrukturu qurulması, konfiqurasiyası, test edilməsi və idarə edilməsi • Məlumat mübadilə proqramlarının idarə edilməsi • əsas server konfiqurasiyası quraşdırılması • Hesabların idarə edilməsi, parol yaratma və idarə etmə • Risk, uyğunsuzluqların ölçülməsi və monitorinqi metodları • İT proqramların auditi
Sistem təhlükəsizliyi və müdafiəsinin təmini	
• Fayl sistem tətbiqləri • Sistem fatlların əhatə etdiyi məlumatlar • Şəbəkə təhlükəsizliyi arxitekturası konsepti, topologiya, protokollar, komponentlər	• Təhlükəsizlik tədbirləri üçün məlumat toplanması və hesabat və məlumatların təhlili • Şəbəkə resurslarının effektiv fəaliyyəti üçün hardvare və proqram təminatı infrasktrukturunun test

• Təhlükəsizlik yoxlamalarının aparılması, altələr, hüquqi tənzimləmə və tətbiq metodologiyası • Kiber müdafiə alətləri və imkanları • Təhlükəsizlik risklərinə qarşı kontra tədbirlərin dizaynı və təşkili	edilməsi, tətbiqi və texniki qulluq işləri • Şəbəkədə təsdiqlənməmiş fəaliyyətlərin monitorinqi • Krizis vəziyyətlər ilə bağlı təcili tədbirlərin icrası • Müdaxilə və boşluqların qiymətləndirilməsi
Əməliyyatlar və İdarə etmə	
• Kiber müdaxilə aktyorları, metodlar və texnikaları • Şəbəkə təhlükəsizliyinin əsasları • Sistem faylllarını iş mexanizmi, funskiyası • İstifadə edilən alətlər (sniffers, keyloggers) və texnikaların (backdoor Access və s.) strukturu, yanaşma və strategiyaları • Daxili (internal) taktikalar • Daxili və kənar partnyorların kiber əməliyyatlar imkan və alətləri	• Kiber cinayətlərin müəyyənləşdirilməsi • Müdaxilələr və boşluqların təyini üçün məlumatların təhlili
Intelektual məlumat toplanması və təhlil	
• Kiber cinayətkarlar və xarici müdaxilələrin təyini • Müxtəlif mənbələrdən olan məlumat və hesabatların əldə etmək və təhlili • Məlumat və sistem bərpası metod və mexanizmləri	• Kiber cinayətkarlar və xarici müdaxilələrin müəyyənləşdirilməsi • Məlumat və sistem bərpası üzrə fəaliyyətlər
Təhlükəsizlik yoxlamaları və rəqəmsal cinayətkarlıq	
• Yoxlama və hesabat alətləri və hüquq tənzimləmər • Malvare təhlili konsepti və metodologiyası • Kiber müdaxilə sənəf tipləri və onların toplanması • Rəqəmsal kiriminal fəaliyyətlər və məlumatlar tətbiqi və onlara qarşı mübarizə praktikası	• S • Collect, process, preserve, analyse, and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations

2.2. Proqramın mənimsənilməsi nəticəsində məzunun kompetensiyasına qoyulan tələblər.

2.2.1 Məzun aşağıdakı ümummədəni kompetensiyalara (**ÜK**) yiyələnməlidir:

- kollektivdə işləmək **(ÜK-1);**
- öz sahəsi və digər sahələrin mütəxəssisləri ilə ünsiyyətdə olmaq **(ÜK-2);**
- etik normalara malik olmaq **(ÜK-3);**
- sağlam həyat tərzini gözləmək **(ÜK-4);**
- tənqid və özünətənqidə dözümlülük göstərmək **(ÜK-5);**
- problemli şəraitlərdə təşəbbüskarlıq göstərmək və məsuliyyəti öz üzərinə götürmək **(ÜK-6);**

- dövlət dilində sərbəst danışmaq **(ÜK-7);**
- xarici dildə ünsiyyətdə olmağı və fikrini ifadə etməyi bacarmaq **(ÜK-8);**
- İKT-dən istifadə etməyi bacarmaq **(ÜK-9);**
- Karyera planlaması və karyera yüksəlişi üçün öz inkişafına, peşəkarlığının artırılmasına çalışmaq **(ÜK-10);**
- fikrini düzgün və yığcam ifadə etmək **(ÜK-11);**
- Peşə fəaliyyəti və gündəlik həyatda əmək təhlükəsizliyi və sağlamlıq qaydalarına riayət etmək və digər şəxslərə məlumatlandırmaq **("ÜK-12).**
- Xidmət göstərdiyi fəaliyyəıt sahəsi üzrə daim yenilikləri araşdırmaq **(ÜK-13)**

2.2.2 Məzun aşağıdakı peşə kompetensiyalarına (**PK**) yiyələnməlidir:

- fəaliyyət sahəsinə aid olan, peşəsinə və ixtisas dərəcəsinə uyğun gələn istənilən istehsal sahələrinin, təşkilatların, idarələrin, müəssisələrin, şirkətlərin və s. əsas problemlərini sistemləşdirməyi bacarmaq, onların kompleks təhlilini aparmaq və idarəetmə məqsədləri üçün konkret nəticə çıxarmaq və aradan qaldırmaq **(PK-1);**
- mövcud tələbləri müvəffəqiyyətlə müəyyənləşdirə bilmək və uyğun bir həll metodu seçmək və tətbiq etmək **(PK-2);**
- peşə fəaliyyətində İKT-dən istifadə etmək **(PK-3);**
- müəyyən vəzifələr qoymağı, onları həll etmək üçün uyğun metodları seçməyi və tətbiq etməyi bacarmaq **(PK-4);**
- İxtisasla əlaqəli əsas anlayış və terminlərin mənasını bilmək və praktikada tətbiq etmək **(PK-5).**
- ixtisasla bağlı müxtəlif layihələrin planlaşdırılması və icrasında iştirak etmək **(PK-6);**
- ixtisasla bağlı aşağıdakı bilik, bacarıq və səritşərlərə yiyələnmək **(PK-7)**.
    - C və Python proqramlaşdırma dilləri funksiyaları bilmək və əməliyyatları icra etmək;
    - Dark Web, Anonimlik və İOT-ların mühafizəsinin təşkil etmək;
    - IT Sistemlərind (Windows Server) təhlükəsizliyin idarəolunması
    - Kiberhücumlar və müdafiə üsullarının tətbiq etmək;
    - Zəifliklərin aşkarlanması, qiymətləndirilməsi üzrə fəaliyyətlər;
    - Mobil avadanlıqların təhlükəsizliyinin təmn etmək.

3.“Kiber təhlükəsizlik" ixtisası üzrə təhsilin məzmununa və səviyyəsinə qoyulan minimum tələblər

Humanitar və baza modulları bölümünə daxil olan modullar Azərbaycan Respublikası Nazirlər Kabinetinin 11.03.2019-cu il tarixli, 85 №-li qərarı ilə təsdiq olunmuş «Peşə təhsilinin dövlət standartları»nda əks olunan “ömürboyu təhsil” prinsipinə uyğun müəyyənləşdirilmişdir.

Humanitar və baza modulları bölümü üzrə təhsilalan “ömürboyu təhsil” prinsipinə uyğun olaraq aşağıdakı bilik və bacarıqlar əldə edəcəkdir:

- ixtisas üzrə peşə fəaliyyətini təmin edən ana dilində və xarici dildə yazılı və şifahi ünsiyyət qurmaq üçün nəzəri və təcrübi biliklərə malik olmalı;
- ixtisas üzrə qazanılmış biliklərdən istifadə etməli;
- informasiyanın toplanması və emalında müasir üsullardan istifadə etməli, müxtəlif hesablamaları aparmalı;
- ixtisas sahəsinin əsas problemlərini dərk etmək, onların konkret tətbiq sahələrini bilməli;
- peşə fəaliyyəti dairəsinə aid olan məlumatların işlənilməsində və saxlanılma-sında kompyuter texnologiyasından istifadə etməli;
- peşə fəaliyyətində sahibkarlıq düşüncəsini və ideyalarını əsas götürməli;
- peşə fəaliyyətində peşənin tələb etdiyi işgüzar etika və davranış qaydalarına əməl etməli;
- peşə fəaliyyətində “ömür boyu” öyrənmə prinsiplərini rəhbər tutaraq şəxsi inkişafa və düzgün karyera planlamasını əsas götürməlidir.

İxtisas üzrə baza biliklərin formalaşmasını imkan verəcək aşağıdakı modulların tədrisi də bu bölümdə icra edilir (məs. Layihə İdarə edilməsi, İstehsalatın İdarəedilməsi və s.). Bu təhsilalana texniki biliklərin formalaşması, həmçinin gələcək iş prosesində müəyyən idarəçilik funksiyalarının icrası üçün tələb olunan səriştələrin əldə edilməsinə istiqamətlənir.

3.1 İxtisas üzrə modul və fənn bölümləri, modul və fənn mənimsənilməsi (təlim) nəticələri (bilik, bacarıq və yanaşma baxımından) və kreditləri, qazanılması nəzərdə tutulan kompetensiyaların kodları:

3.1.1 Ümumtəhsil fənlər bölümü:

Ümumtəhsil fənləri bölməsinə daxil olan fənlər 29 mart 2019-cu il 1532-VQ nömrəli "Ümumi təhsil haqqında" Azərbaycan Respublikasının Qanunun və "Azərbaycan Respublikasında ümumi təhsilin dövlət standartları" haqqında Azərbaycan Respublikası Nazirlər Kabinetinin 2020-ci il 29 sentyabr tarixli 361 nömrəli Qərarının tələblərinə uyğun müəyyənləşdirilmişdir.

Ümumi orta təhsil bazasından qəbul olunmuş qruplarda tədrisin birinci ilində ümumtəhsil fənləri tədris olunduğu üçün kredit sisteminə daxil edilmir.

Fənn bölümünün kodu	**Fənlərin adı**	**Saat miqdarı (həftəlik)**
ÜF-B01	Azərbaycan dili	3
ÜF-B02	Xarici dil	4
ÜF-B03	Riyaziyyat	4
ÜF-B04	Fizika	1
ÜF-B05	Kimya	1
ÜF-B06	Ədəbiyyat	1
ÜF-B07	Azərbaycan tarixi	2
ÜF-B08	Coğrafiya	1
ÜF-B09	Ümumi Tarix	1
ÜF-B10	Biologiya	1
ÜF-B11	İnformatika	3
ÜF-B12	Fiziki tərbiyə	2
ÜF-B13	Çağırışaqədərki hazırlıq	2
ÜF-B14	İkinci xarici dil*	2
İT - B01	Praktiki laboratoriya dərsləri / istehsalat təlimi	7
Cəmi:		**35**
Qeydlər:		
Ümumtəhsil fənləri tədris olunduğu halda, həmin fənlərə kreditlər ayrılmır. Tədris müddəti 38 həftə (18/20) davam edir.		

Ümumi orta təhsil bazasından qəbul olunmuş qruplarda peşə təhsilinin dövlət standartında göstərilmiş "Ana dilində ünsiyyət" səriştəsi "Azərbaycan dili", "Xarici dildə ünsiyyət" səriştəsi "Xarici dil", "İnformasiya texnologiyaları" səriştəsi "İnformatika", "Hesablama əməliyyatlarını yerinə yetirmə" səriştəsi isə "Riyaziyyat" fənni proqramına inteqrasiya olunmuş şəkildə, həmçinin ixtisasın tələbləri nəzərə alınmaqla uyğunlaşdırılmış proqram əsasında tədris edilir.

“Xarici dil” və “İnformatika” fənnin tədrisi tələbələrin sayı 15 (on beş) və daha çox olan qruplarda müvafiq maddi-texniki baza və ixtisas müəllimləri olduğu halda 2 (iki) qrupa bölünərək aparılır.

Praktiki laboratoriya dərsləri və ya istehsalat təlimi tədrisi təhsil müəssisəsi tərəfindən laboratoriya və emalatxana şəratinə əsasən tədris edilir.

İxtisasın tələbinə uyğun olaraq ikinci xarici dilin tədrisi aparılmadıqdan onun saatları əsas xarici dilə verilir.

3.1.2 Kadr hazırlığı üçün tələb olunan modul və fənn bölümü:

Modul / Fənn	Təlim nəticəsi	Mənimsənilmə nəticələri			Modullar üzrə kredit-lərin sayı	Kompetensiyaların kodları
		Bilik	Bacarıq	Yanaşma		
Təhsil hissəsi						
HBM – B00	**Humantira və baza modullar bölümü** Bu bölümə daxil olan modulların öyrənilməsi nəticəsində subbakalavr:					
HBM–B01 Azərbaycan tarixi		- Azərbaycan tarixinin əsas mərhələləri və xronologiyası barədə təsəvvürə, müstəqillik yolunda qazandığı nailiyyətlər, tarixi şəxsiyyətlər və əsas tarixi hadisələr haqqında məlumata malik olmalı;	Tarixi inkişaf mərhələlərini müqayisə və təhlil etməyi, tarixin qiymətləndirilməsinə dair öz mövqeyini əsaslandırmağı və fikrini ifadə etməyi.		**5**	**ÜK-1** **ÜK-2** **ÜK-5**
HBM–B02 Azərbaycan dilində işgüzar və akademik kommunikasiya		- Azərbaycan Respublikasının dövlət dilini sərbəst bilməli, nitqin düzgünlüyü, aydınlığı və dəqiqliyi naminə sözləri düzgün tələffüz etməyi;	Azərbaycan dilinin leksikonundan peşə fəaliy-yətində istifadə etməyi, dil qaydalarına uyğun danışmağı və yazmağı, rəsmi və işgüzar üslubda yazmağı və danişmağı;		**4**	**ÜK-7** **ÜK-3** **ÜK-4** **ÜK-11**
HBM-B03 / B04 / B05 İnformasiya texnologiyaları		- İnformasiya texnologiyalarından istifadə etməklə ixtisas aid məlumat, əldə etmək və tətbiqi imkanlarını;	- İnformasiya texnologiyalarından təhlükəsiz şəkildə istifadə etməyi və rəqəmsal məzmun yaratmağı, müvafiq sosial media vasitələrindən istifadə etməyi;	İKT, sosial media və digər proqram təminatlarından peşə fəaliyyətində istifadə etmək vərdişlərinə.	**6**	**ÜK-9** **PK-2** **ÜK-13**

HBM-B06 / B07 / B08 / B09 Xarici dildə işgüzar və akademik kommunikasiya		- Xarici dildə olan ixtisasa aid ədəbiyyatı oxuyub başa düşməyi;	- Xarici dildə olan ixtisasa aid ədəbiyyatı lüğətlə tərcümə etməyi, tərcümeyi-hal və digər rəsmi sənədləri xarici dildə tərtib etməyi, xarici dildə yazılı və şifahi ünsiyyət qurmağı;	Xarici dildə olan material-lardan peşə fəaliyyətində istifa-də etmək vərdişlərinə.	**12**	**ÜK-1 ÜK-8 ÜK-13**
HBM-B10 / B11 Texniki hesab		- Məsələlərin həllində riyazi düşüncə nümayiş etdirməyi, və peşə fəaliyyəti ilə bağlı riyazi düşüncəni tətbiq etməyi;	- İxtisas uyğun müvafiq hesablamalar aparmağı, qrafik və cədvəlləri hazırlamaq və istifadə etməyi, təsviri statistikadan istifadə etməyi;	Riyazi yanaşma və metodlardan peşə fəaliyyətində istifadə etmək vərdişlərinə.	**5**	**ÜK-2 PK-3**
HBM-B12 Şəxsi inkişaf və karyera planlaması		- Fərdi özünü inkişaf və karyera planlaması üzrə yanaşma və tətbiqləri başa düşməyi;	- Karyera məqsədlərini müəyyən etməyi, karyera inkişafında müasir işaxtarma və müraciət üsullarından istifadə etməyi;	Fərdi və karyera inkişafı üçün müasir planlama və tətbiq mexanizmlərindən istifadə etmək vərdişlərinə.	**3**	**ÜK-6 ÜK-10**
HBM-B13 Layihə İdarə edilməsi		- Layihələrin hazırlanması, idarə edilməsi və monitorinqi mərhələlərini izah etməyi və fəaliyyətlərin düzgün planlaması tətbiq etməyi;	- Müxtəlif ölçülü layihələrin idarə edilməsi üçün layihə planlaması və idarə edilməsi üzrə alət və üsullardan istifafə etməyi;	Layihə planlanması və idarə edilməsi üzrə müasir yanaşma və vərdişlərə	**3**	**PK-6**
HBMS–B00	**Seçmə modullar***					
HBMS-B01 Etika və estetika (İşgüzar Etika)		- Peşəkarlıq prinsipləri və iş yerində davranış qaydalarını;	- Peşəkarlıq prinsipləri və komanda ilə səmərəli işləməni, vaxtdan səmərəli istifadə etməyi, iş yerində davranış qaydalarına əməl etməyi;	Peşəkarlıq və səmərli iş prinsiplərini, iş yerində düzgün davranış qaydalarından	**3**	**ÜK-1 ÜK-3 ÜK-4 ÜK-5**

				peşə fəaliyyətində istifadə etmək vərdişlərinə.		
HBMS-B02 Estetika və Mədəni İfadə		- Kreativlik və estetika anlayışlarını, etiket və nəzakət qaydalarını başa düşməyi;	- Kreativlik və estetika anlayışlarını, etiket və nəzakət qaydalarını təhlil edərək onlardan istifadə etməyi;	Peşə fəaliyyətində etiket bə nəzakət qaydalarından istifadə etmək vərdişlərinə.	**3**	**ÜK-1 ÜK-3 ÜK-4 ÜK-5**
HBMS-B03 STEM		- STEAM Mühəndislik və Dizaynın əsasları; - 3D qələm, 3D CAD Modelləşdirməyə girişi; - Mikrobit ilə Robototexnika - proqramlaşdırmaya girişi; - CNC lazer texnologiyasına girişi; - Dron texnologiyasının əsaslarını.	- 3D qələm və 3D CAD modelləşdirmə ilə müxtəlif obyektlərin dizaynını; - Mikrobit ilə robototexnika proqramlaşdırma əsasında müxtəlif layihələrin proqramlaşdırılması; - CNC lazer texnologiyası əsasında müxtəlif obyekt düzəldilməsini; - Dron texnologiyası üzrə müəyyən fəaliyyətləri.	STEAM Mühəndisliyi, CNC lazer və Dron texnologiyası üzrə müxtəlif praktiki vərdişlərə.	**3**	**ÜK-9 ÜK-13 PK-2**
HBMS-B04 Sahibkarlığın əsasları və biznesə giriş		- Sahibkarlıq düşüncəsi və yanaşmalarını və onların peşə fəaliyyətində tətbiqi imkanlarını başa düşməyi;	- Peşə fəaliyyəti üzrə tətbiq edilə bilən sahibkarlıq ideyalarını müəyyən etməyi, biznes planlar hazırlamağı və biznes planları təhlil edərək onları tətbiq etməyi;	Peşə fəaliyyətində sahibkarlıq düşüncəsi və sahibkarlıq istiqamətində planlar hazırlama və tətbiq etmək vərdişlərinə.	**3**	**PK-1 PK-6**
HBMS-B05		- İxtisasına aid istehsalat sahələrinin əsas idarəetmə prinsip və mexanizmlərini başa düşməyi;	- Peşə fəaliyyətindən asılı olaraq istehsalatın planlanması və idarə edilməsi ilə bağlı	İxtisasa aid istehsalatın idarə edilməsinin	**3**	**PK-1 PK-6**

İstehsalatın idarə edilməsi			prinsipləri düzgün formada tətbiq etməyi;	əsas prinsiplərinin peşə fəaliyyətində istifadə etmək vərdişlərinə.		
KS-İM-B00	**İxtisas peşə hazırlığı modulları bölümü** Bu bölümə daxil olan modulların öyrənilməsi nəticəsində subbakalavr:					
KS-İM-B01 Komputer proqramlaşdırması və Əməliyyat sistemləri	Müvafiq aparat, proqram təminatı və müxtəlif əməliyyat sistemlərini bilir. Müvafiq simmetrik çox işləmə və paylaşılan yaddaş bölmələri ilə işləməyi bacarır. Müvafiq şəbəkəyə və virtualizasiyaya əsaslanan proseslərarası ünsiyyət modeli ilə bağlı bilikləri tətbiq etməyi bacarır.	- Sistem zəngləri, əməliyyat sistemi və proseslər arası ünsiyyət həyata keçirilməsi üçün tətbiq edilən müxtəlif arxitekturaları izah etmək; - Əməliyyat sistemləri və İnformasiya Təhlükəsizliyində parametrlərə uyğun olaraq komandaların,məlumatların analizi və onların sistemdə verilməsi qaydalarını bilmək və müəyyən etmək; - Proseslərarası ünsiyyətin bir və ya daha çox prosesdə və ya proqramda birdən çox mövzu arasında məlumat mübadiləsi üçün istifadə olunması prinsiplərini anlamaq.	- Memarlıq ya yerli virtualizasiyadan istifadə etməklə virtuallaşdırma dizayn yollarını təmin etmək; - Komputer göstəriciləri və əməliyyat sistemlərinin optimal komponentlərdən istifadə etməklə davamlılıq, innovativlik və təhlükəsizlik meyarlarının qiymətləndirilməyini təyin etmək; - Vaxt bölgülü əməliyyat sistemlərinin səmərəli istifadəsi üzrə tapşırıqları emal etmək.	Kibertəhlükəsizliyin təşkil olunmasında müxtəlif proqramlardan istifadə edilməsi və fərqli əməliyyat sistemləri mühitində işləməyi bacarmağı təmin etmək yönündə startegiya və metodolgiyaların hazırlanması	**4**	**PK – 1** **PK – 5** **PK – 7**
KS-İM-B08 Python programlaşdırma dili	Python üçün mühit yaratmağı və dilin sadə sintaksisini təyin etməyi bacarır. Hadisələrin axın kontrolunu təşkil etməyi, Obyekt Yönümlü Python proqramı(OOP) təşkil etməyi bacarır.	- Funksiyalar: tərif və istifadə, arqumentlər, blok quruluşu, əhatə dairəsi, rekursiya anlayışlarını başa düşmək və sadə funksiya yarada bilmək; - Python-da olan müxtəlif növ əməliyyatların(Arithmetic, Logical, Comparison və s.) sintaksisini sadə nümunələr vasitəsilə anlamaq;	- Python proqramlaşdırma mühitinin müxtəlif əməliyyat sistemlərində qurulmasını həyata keçirmək və GitHub və git-ə giriş etmək; - Dictionary Metodlardan, Tuplelardan istifadə etməklə əməliyyatlar aparmaq; - Python-da olan müxtəlif funksiyaların və metodların	Python programlaşdırma dili üzrə əldə olunmuş bilik və bacarıqların kibertəhlükəsizlik üzrə məsələlərdə və müxtəlif mühitlərdə	**5**	**PK – 1** **PK – 5** **PK – 7**

	Python-da siniflərin, faylların və setlərin implementasiyasını etməyi bacarır	- İrsiliyi, Polimorfizmi, Abstraktlığı, İnkapsulyasiyanının işləmə prinsipini nümunələr əsasında təyin etmək.	tətbiqini nümunələr üzərində reallaşdırmaq; - Əsas fayl əməliyyatları biliklərini nümayiş etdirərək Python-da ZİP fayl nümunəsi yaratmaq.	tətbiqini təmin edən strategiya və metodologiyaların hazırlanması		
KS-İM-B05 IT Sisteminin və təhlükəsizliyin idarəolunması	Müəyyən müəssisədə sistem idarəçiliyinin informasiya texnologiyaları sistemlərinin yaradılması və nəzarəti mexanizmini bilir. Müəssisədə Windows Server mühitindən, Virtualizasiyadan istifadə etməyi bacarır. Windows mühitində istifadəçilər və səlahiyyət vermə prinsiplərinin qurulmasını bilir. İnformasiya təhlükəsizliyi sistemini anlayır, risklər və zəifliklər yarandıqda müvafiq və təxirəsalınmaz tədbirlər görməyi bacarır. Seçilmiş risk azaldılması metodu əsasında informasiya texnologiyaları (IT) sahələrinin təhlükə və/və ya zəifliyindən asılılığını	- Windows Server və onun komponentlərinin işləmə prinsipini bilmək və nümunələr əsasında təyin etmək; - İstifadəçilərin müəssisə mühitində necə yaradıldığı, qruplaşdırıldığı və idarə edildiyini başa düşmək.(AD); - İnformasiya təhlükəsizliyinin idarə edilməsi (ISM) təşkilatın təhlükələrdən, aktivlərin məxfiliyinin, əlçatanlığının və bütövlüyünün qorunmasını təmin etmək üçün tətbiq edilməli olan nəzarət vasitələrini bilmək	- Resurslardan istifadə etməklə şəxsi test mühitinin qurulması prosesini həyata keçirmək; - Şəxsi və müəssisə hesablanması prinsiplərini anlamaq üçün real nümunələr üzərində işləmək; - Addressing və subnetting biliklərini real nümunələr əsasında nümayiş etdirmək; - VMware üzərindən virtualizasiyaya ümumi baxışla əməliyyatlar aparmaq; - İstifadəçilər və Doğrulama (Authentication) anlayışlarının virtual mühitdə nümunələr əsasında qurulmasını yerinə yetirmək. - İnformasiya təhlükəsizliyinin idarə edilməsi (ISM) təşkilatın təhlükələrdən, aktivlərin məxfiliyinin, əlçatanlığının və bütövlüyünün qorunmasını təmin etmək üçün tətbiq edilməli olan nəzarət vasitələrini müəyyənləşdirmək və idarə etmək.; - İSM-in nüvəsi informasiya risklərinin idarə edilməsi, risklərin qiymətləndirilməsi və onlar barədə məlumatların	-İT sistemlərinin yaradılması, idarə olunması və nəzarətinin həyata keçirilməsinin təmin edilməsinə yönəlmiş metodologiya və strategiyaların yaradılması -İT sistemlərinin təhlükəsizliyinin idarə olunmasını öyrənmək və İT sistemlərində mühitə uyğun təhlükəsizlik tədbirlərini icra etmək yönündə metodologiya və strategiyaların hazırlanması.	**6**	**ÜK - 12** **PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	peşəkarcasına anlayır və təmin etməyi bacarır.		müvafiq maraqlı tərəflər arasında yayılmasını özündə ehtiva edən bir prosesi apara bilmək;			
KS-İM-B06 Şəbəkənin və şəbəkə təhlükəsizliyinin İdarəolunması əməliyyatları	Standart arxitekturaya əsaslanan şəbəkə idarəedilmə konseptini bilir. Paylanmış sistemdə ümumi istifadə olunan şəbəkə protokolları və onların arxitekturasını fərqləndirməyi bacarır. Şəbəkə idarə etməsində əsas və trend texnologiyalardan istifadə etməklə monitroing etməyi bacarır. Şəbəkə avadanlıqlarının təhlüksəzlik arxitekturasının ümumi təşkilini təmin edə bilir. Şəbəkə səviyyələri üzrə müvafiq avadanlıqların təhlükəsizlik inteqrasiyasının təmin etməyi bacarır. Şəbəkə üzrə məlumatların müxtəlif vəziyyətlərində təhlükəsizliyini avtomatik və manual idarəsini bacarır.	- Analitik texnikalardan istifadə etməklə şəbəkə daxili ünsiyyət üçün dizayn konseptlərini anlamaq; - OSİ və TCP/İP modellərinin qatlarında olan İnternet Protokollarının müxtəlifliyini analiz etmək. -Şəbəkə arxitekturasını təhlükəsizlik baxımından təşkilini anlamaq;	- Resurslardan istifadə etməklə şəxsi test mühitinin qurulması prosesini həyata keçirmək; - Müxtəlif şəbəkə topologiyaları və onların ötürülməsi xüsusiyyətlərini real nümunələr üzərində işləmək; - Syslog və SNMP-dən istifadə etməklə fault və performans idarə edilməsini həyata keçirmək; - Müştəri-server, peer-to-peer və şəbəkə zəifliklərini nümunələr əsasında nümayiş etdirmək; - Ümumi istifadə olunan monitoring şəbəkə vasitələri ilə bağlı olan logları analiz etmək. - Kiber müdafiənin təminatı üçün şəbəkədəki məlumat axınlarını qarşılıqlı analiz etmək; - Şəbəkə elementlərində və qoşulmalarında kiber təhlükəsizlik qaydalarına riayət etmək; -İnnovativ təhlükəsizlik alətləri ilə işləmək və şəbəkədə tətbiqini icra etmək; - Kiber təhlükəsizlik alətləri ilə şəbəkənin davamlı nəzarətdə saxlanmasını və alətlərin	- Şəbəkələrin dizaynı, qurulması, idarə edilməsi və monitorinqinin həyata keçirilməsi istiqamətində plan və strategiyaların hazırlanması - Şəbəkə təhlükəsizliyinin təmin edilməsi və bu məqsədlə müxtılif təhlükəsizlik alətləri ilə işləmək metodologiyaları və strategiyalarının hazırlanması	**5**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Artan kiber risklər fonunda şəbələnin davamlı təhlükəsizlik nəzarətində saxlamağı bacarır. İnformasiya və Kiber təhlükəsizlik strateji xəritəsində şəbəkə təhlükəsizliyinin yerini və rolunu ifadə edə bilir.		nəticələrinin doğruluğunu yoxlamaq ; - Şəbəkə avadanlıqları üzərindən müxtəlif qoşulmaların inzibatçılığını icra etmək; - Şəbəkə təhlükəsizliyinin biznes mühitindəki mövqeyini qiymətləndirmək və təqdim etmək;			
KS-İM-B02 Alqoritmlər və analitik düşünmə	Alqoritmik düşünmənin informatikada proqramlaşdırma öyrənməkdən asılı olmayaraq inkişaf etdirməyi bacarır. Müxtəlif növ optimallaşdırma problemlərində istifadə olunan sadə, intuitiv alqoritmlərlə bağlı bilir. Dinamik və Heuristik proqramlaşdırma alqoritmləri ilə bağlı olan problemlərin həll yolu mexanizmini bilir.	- Mürəkkəb problemlərin düzgün vizualiasiyası üçün alqoritmlərlə əlaqəli əsas anlayışları anlamaq; - Brute Force alqoritminin müxtəlif növlərini və plotting qraf nəzəriyyəsinin mahiyyətini anlamaq; - Parçala və birləşdir alqoritmi əsasında alqoritm dizayn paradiqmasını anlamaq; - Greedy yanaşmasının xüsusiyyətləri : lokal olaraq optimal seçim etmək üçün problemi həll etmə evristiyasına uyğun gəlməsi mexanizmini anlamaq; - Backtracking alqoritmi və Dinamik proqramlaşdırma arasındakı oxşarlıqları və fərqləri təyin etmək.	- Recurrence əlaqələri həll etməklə bağlı olan 3 varianti real nümunələr üzərində tətbiq etmək; - Heuristic və Approximate Algorithmlərin müxtəlif növləri ilə problem həll etmək.	Müxtəlif alqoritmlərin, eləcə də analitik düşünmənin kibertəhlükəsizliyin müxtəlif sahələrində tətbiq edilməsini təmin etmək məqsədilə plan, strategiya və metodologiyaların hazırlanması	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İM-B03 C proqramlaşdırma dili	Yüksək Səviyyəli Dillər Proqramlaşdırma Dizayn Metodologiyaları və onlarla bağlı olan sadə anlayışların işləmə prinsipini bilir.	- C dilində sadə proqramları müxtəlif növ operatorlardan istifadə etməklə yazmaq; - İf-else statement-i, Dövrlərin mahiyyətini və tam ədədləri üzən nöqtəyə çevirmək(əksinə) prinsipini anlamaq;	- Bir Ölçülü Matixlər, Funksiyalara Keçən Matrixlər, Çoxölçülü Matrixlər və Sətirlər üzərində işləmlər aparmaq; - Avtomatik və ya yerli, Qlobal, Statik Xarici dəyişənləri və	C proqramlaşdırma dilində əldə olunuş bilik və bacarıqların kibertəhlükəsizlik üzrə	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Matrix, Funksiya, Sətir, Göstərici və Strukturlarla bağlı bilir. Yaddaş bloklarının yenidən bölüşdürülməsi və Fayllarda giriş/çıxış əməliyyatları ilə bağlı metodları təmin və təyin edə bilir.	- Göstəricilərlə Bir Ölçülü Matrixlər arasındakı oxşarlıqları təyin etmək; - Strukturlar haqqında fundamental biliklərin anlaşılması və Funksiya prototipləri və keçid parametrləri haqqında təfəkkürə malik olmaq.	Makros anlayışını optimizasiya etmək; - Yaddaşın malloc ilə bölüşdürülməsi, calloc ilə ayrılması və I/O əməliyyatları zamanı səhvlərin idarə edilməsini hərtərəfli analiz etmək.	məsələlərdə və müxtəlif mühitlərdə tətbiqini təmin edən strategiya və metodologiyaların hazırlanması		
KS-İM-B04 İnformasiya Risklərinin İdarə olunması	Aktivlərin qorunması üçün alınan tədbirlərin iş dəyərləri ilə mütənasib olmasını təmin edilməsi prinsiplərini bilir. Risklərin təhlili ilə mümkün təsadüfən və ya qəsdən itkilərlə məşğul olmaq və minimuma endirmək üçün prosedurların hazırlanmasını və həyata keçirilməsini bacarır. Dinamik və Heuristik proqramlaşdırma alqoritmləri ilə bağlı olan problemlərin həll yolu mexanizmini bilir.	- Risklərin tipləri, Qabaqcıl standartlar üzrə Kiber Təhlükəsizlik Çərçivəsinin prinsiplərini anlamaq; - Təhdid və Təhlükə anlayışı, onların mənbələri, APT-lərə qarşı mübarizə üsulları ilə bağlı biliklərə sahib olmaq; - Risklərin İdarə edilməsi üçün plan ölçülərinin əhatə dairəsi və prosesdə rolların bölünməsi mexanizmini anlamaq; - Biznes təsir analizi prosesini(BİA) və Fəlakətin bərpası ilə biznes davamlılığı arasındakı fərqləri aydınlaşdırmaq.	- Əsas risk göstəriciləri(KRİ) təyin edilməsi və report hazırlanmağı ilə bağlı tələbləri optimizasiya etmək; - Risklərin yumşaldılması məqsədli həyata keçirilən təhlükəsizlik nəzarəti tipləri ilə real nümunələr üzərində işləmək; - Səciyyəvi və bəsit risk qeydiyyata alınması prosesini həyata keçirmək.	Risklərin müəyyən lunması, qiymətləndirilməsi,analizi və aradan qaldırılması, eləcə də kibertəhlükəsizlik standardları və çərçivəsi əsasında risklərin idarə olunması planının və informasiya təhlükəsizliyi strukturunun yaradılmasına yönələn plan, strategiya və metodologiyaların hazırlanması	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İM-B10 Bulud təhlükəsizl	Cari standartlara, protokollara və ən yaxşı təcrübələrə əsaslanan bulud	- Bütün təbəqələrdə hərtərəfli məlumat qorunması, uçtan uca şəxsiyyət və giriş idarəçiliyi, monitorinq və audit prosesləri və	- Hesablama nümunəsini/virtual maşını CSP mühitlərində etibarlı şəkildə yerləşdirmək;	Buludda saxlanılmış məlumatların qorunması,	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4**

ik əməliyyatlarının idarə olunması	hesablama memarlığının əsasları ilə bağlı ilkin məlumatları bilir. Müxtəlif bulud xidmətlərində müəssisə məlumatlarını necə düzgün müəyyənləşdirmək və təsnif etməklə əlaqədar anlayışları bilir. Bulud təhlükəsizliyinin qiymətləndirilməsi və audit hesabatları aparmağı bacarır.	sənaye və tənzimləmə mandatlarına uyğunluq prinsiplərini anlamaq; - Bulud əsaslı infrastrukturlar üçün sənaye təhlükəsizlik standartlarını, audit siyasətləri ilə bağlı olan biliklərə sahib olmaq.	- Təhlükəsizlik konfiqurasiyalarını və əməliyyatları avtomatlaşdırmaq üçün İnfrastrukturu Kod (IaC) istifadə etmək; - Məlumatları mövcud olduğu yerdə və şəbəkələri keçərkən şifrələmə metodlarını aydınlaşdırmaq; - Şəbəkə nəzarət vasitəsi ilə bulud məlumatlarının axını necə idarə edəcəyini optimizasiya etmək; - Təhlükəsizlik çatışmazlıqlarının aşkarlanmasını avtomatlaşdırmaq üçün bulud vendoru tərəfindən təmin edilən IAM analiz vasitələrindən istifadə etmək;	eləcə də bulud əməliyyatlarının idarə olunmasının təhlükəsizliyini təmin etmək məqsədilə əldə olunan bilik və bacarıqların tətbiq edilməsini təmin edən plan, strategiya və metodologiyaların hazırlanması		**PK – 5** **PK – 6** **PK – 7**
KS-İM-B09 Dark Web, Anonimlik və İOT-ların mühafizəsinin təşkili	TOR brauzer, TAİLS sistemi və VPN istifadə etməklə anonimliyin təmin edilməsi prinsiplərini bilir. Anonimliyin saxlanılmasını əsas tutaraq müxtəlif texnikalardan istifadə etməklə anonim onlayn kimliyin yaradılmasını və ünsiyyətə keçməyi bacarır. Müxtəlif şifrləmə mexanizmləri və	- VPN-in işləmə prinsipini anlamaq; - TAİLS haqqında ümumi biliklərə sahib olmaq; - XMPP / Jabber haqqında ümumi biliklər, anonim XMPP hesabının yaradılması və TAILS üzərindəki Pidgin istifadə edərək ona necə daxil olunmağı ilə bağlı anlayışlara sahib olmaq; - Kripto Valyutaların işləmə prinsipini anlamaq.	TOR brauzerin müxtəlif əməliyyat sistemlərində qurulmasını həyata keçirmək; - TAİLS-dən VPN-ə qoşulmaqla bağlı 2 əsas metodu laboratoriya mühitində yerinə yetirmək; - Saxta anonim kimlik yaratmağı, Müvəqqəti E -poçt Hesablarından, Gizlilik Fokuslu E -poçt Təchizatçılarından və DarkNet E -poçt Provayderlərindən istifadə etmək; - Anonimliyin saxlanılması məqsədilə metadatanı	İoT cihazlarının təhlükəsizliyi, müxtəlif əməliyyatlar apararkən anonimliyin qorunması və kriptovalyutalardan istifadə zamanı təhlükəsizliyin təmin edilməsi məqsədilə plan, strategiya və metodologiyaların hazırlanması	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Kripto Valyutalar ilə əməliyyatlar aparmağın yollarını bilir.		təmizləmək və faylları TOR brauzer vasitəsilə paylaşmaq; - Simmetrik və assimmetrik şifrləmə mexanizmini, PGP açar cütlüyünü yaratmağı, verilmiş mətni şifr /deşifr etməyi və elektron imza vasitəsilə imza çəkilməyi real nümunələr üzərində işləmək; - Bitcoin Wallet yaratmaq.			
KS-İM-B07 Linux əməliyyat sistemi	Linux açıq mənbə əməliyyat sistemi yanaşmasının arxasında duran əsas fikirləri bilir. Sistem əməliyyatlarını idarəetmə səviyyəsində manipulyasiya etmək üçün istifadə olunan müxtəlif Linux əmrlərindən istifadə etməyi bacarır. TN3: Linux Proqram Təminatı və X Pəncərə sistemi ilə bağlı olan fundamental bilikləri bilir.	- Linux Əməliyyat Sistemi Layerləri, Linux Shell (müxtəlif növ qabıqlar), Proses: (parent və child prosesləri), Fayl quruluşu, Sistemlə qarşılıqlı əlaqə prinsiplərini anlamaq; - Shell əmrləri, Linux mühitində shell əmrlərinin rolu, ümumi istifadə olunan əmrlər və köməkçi proqramlar haqqında biliklərə sahib olmaq; - Kernel İdarəçiliyi: (Linux kernel mənbələri, kernelin yenidən qurulması, kernelin quraşdırılması), İstifadəçilərin İdarə Edilməsi, Fayl Sistemlərinin İdarə Edilməsi, Linux Fayl İcazələri, Cihazlar və Modullar (cihaz sürücüləri) anlayışları haqda təsəvvürə malik olmaq; - Şifrə faylları və onların konfiqurasiyası, GRUB Şifrəsi və tətbiqi biliklərinə sahib olmaq; - Masaüstü (Masaüstü mühitləri -GNOME, KDE, XFCE) X Pəncərə Sistemi, Xorg, Pəncərə meneceri, Ekran Menecerləri,	- Virtual qutuda LAN yaratmaq və Virtual qutuda müxtəlif testləri həyata keçirmək.	Linux əməliyyat sisteminin, habelə onun layer-lərinin, proqramlarının, fayl sisteminin və s. dərindən mənimsənilməsi və Linux əməliyyat sistemi mühitində müxtəlif əməliyyatların yerinə yetirilməsini təmin edən plan, metodologiya və strategiyaların hazırlanması	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

		Widget Kitabxanaları və ya alət dəstləri (Athena Widgets, Motif alət dəsti, Gtk, Qt, LessTif) anlayışlarının mahiyyətini başa düşmək; - Proqram İdarəçiliyi, Ofis və Databaza Tətbiqləri, Qrafik Alətlər və Multimedya, Poçt və Xəbər Müştəriləri, Veb, FTP və Java Müştəriləri, Təhlükəsizlik: Şifrələmə, Dürüstlük Yoxlamaları və İmzalar, Təhlükəsizliyi Təkmilləşdirilmiş Linux, Kerberos, Firewall haqqında ümumi ilkin biliklərə sahib olmaq.				
KS-İM-B11 Sistem analiz və dizayn, Keyfiyyət Təminatı İdarəetmə (Test İdarəetmə)	İT sistemlər və onlardakı məlumat axını diaqramlarını tərtib edə bilir. Proqram təminatı Həyat Dövrü mərhələlərində kiber təhlükəsizlik faktorlarına riayət etməyi bacarır. Proqram təminatı Həyat Dövrü mərhələlərində işçi heyətin səlahiyyətlərini anlayır və təhlükəsizlik səlahiyyətini icra edə bilir. E-kommers proqam təminatlarının "SLDC" diaqramını hazırlayır	-İT sistemin iş fəaliyyətinə əsasən xarakteristikalarının cari və optimal vəziyyətlərini təyin etmək; - "SDLC" yekun mərhələlərinin iş həcmini anlamaq; - Layihə planını və iş həcminin bəlirlənməsi üçün müvafiq addımlar toplusunu və yanaşmanı bilmək;	- "SDLC" üzrə proqram təminatının planını və işlər ardıcıllığını tərtib etmək; - Verilmiş biznes mühit çərçivəsində müvafiq Proqram təminatı metodologiyasının tətbiqini təmin etmək; -Kiber təhlükəsizlik yoxlanışlarını proqram təminatı hazırlığının vacib hissəsi kimi yerinə yetirmək; - "SDLC" yekun mərhələlərində təhlükəsizlik yoxlanışının hər mərhələ üçün işlərini icra etmək; - E-kommersiya proqram təminatının hazırlanmasında təhlükəsizlik qiymətləndirilməsi komponentlərini yoxlamaq; - Layihə kiber təhlükəsizliyinin idarəolunmasını biznes və	- Məlumat axını diaqramını analiz etmək və müxtəlif sahələrdə tətbiq etmək, eləcə də layihənin təqdimatını hazırlamaq istiqamətində metodologiyaların hazırlanması - Layihə idarəolunması mərhələlərini öyrənilməsi və müxtəlif kibertəhlükəsizlik məsələlərində tətbiqi metodologiyalar	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	və təhlükəsizlik qiymətləndirilməsini icra edə bilir. Layihələrin statusu və yekunlarını strateji aspektdə təqdimatını hazırlaya bilir. Layihə mərhələlərini strukturlaşdıra bilir. Layihə mərhələlərini qabaqcıl standartlar və praktikalar əsasında formalaşdıra bilir. Layihə üzrə işçi heyətin vəzifə və öhdəliklərini təyin edə bilir. İT Sistemlərin Həyat Dövrü (SDLC) üzrə inkişaf xəritəsini hazırlamağı bacarır.		texnoloji amillərlə analizini həyata keçirmək - Layihə İdarəolunmasının effektiv təşkili üçün müvafiq standartlar və praktikalara müraciət etmək və onlardan yararlanmaq; - Layihə həcmindən asılı olaraq icraçılarının təşkilini və vəzifələrinin, öhdəliklərinin effektiv bölgüsünü təmin etmək; - Sistemlərin həyat dövrü mərhələri üzrə işləri məntiqi ardıcıllıqla icra etmək və hər növbəti mərhələyə keçid öncəsi müvafiq nəticələrin səbəb-nəticə analitikasını həyata keçirmək; - Dəyişikliklər, patç, güncəlləmələr və digər növlər üzrə təhlükəsizlik qiymətləndirilməsini icra etmək; - Layihə İdarəolunmasının tərkib hissəsi olaraq Keyfiyyət təminatını və biznes əsasını formalaşdırmaq;	ının hazırlanması		
KS-İM-B12 Kiber Hücumlar və Müdafiə, Kriptoqrafi	Kiber təhükəsizlik layihələrində keyfiyyət təminatı yoxlanışını icra etməyi bacarır.	- Mitre Hücum bilik bazası haqqında məlumata sahib olmaq və kiber texnikalarını müvafiq taktikalar üzrə təsnifatlaşdırmaq; - Mitre Hücum taktikalarındakı texnikalara bələd olmaq;	- Mitre Hücum taktikalarındakı texnikalardan təyinatı üzrə istifadə etmək; - Baş vermiş kiber hücumun Mitre Hücum cədvəli üzərindən diaqramını və ardıcıllığını çəkmək;	- Kiberhücum texnikaları və taktikaları arasında strukturlu əlaqələndirməni təmin edir.	**5**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

ya və Həşləmə	Mitre Hücum taktikalarındakı texnikalardan istifadə və bəhrələnməyi bacarır. Mitre Hücum texnikaları üzərindən tam kiber hücum dövrünün analizini apara ilir. Kiber Hücumların biznesə təsirini Mitre Hücum üzərindən təqdim edə bilir Kriptoqrafiya haqqında ümumi məlumatları anlayır, həşləmə ilə əlaqəsini birləşdirməyi bacarır. Kriptoqrafiyanın növlərini fərqləndirməklə kodlaşdırma və həşləmə arasındakı fərqləri seçmək və kod-dekod prosesində hansı metoddan və variantdan necə istifadə etməyi bacarır. Açıq açar infrastrukturunun(PKİ) əslində Kriptoqrafiyanın bir sahəsi olub, rəqəmsal	- Kiber Müdafiə və Hücum ssenarilərində analitikasında biznes effektivliyin artırılması üçün Mitre Hücum cədvəlindən faydalanmaq. -Həşləmə və kriptoqrafiyanı, eyni zamanda onlar arasındakı əlaqə və fərqləri anlamaq; - Kriptoqrafiya müxtəlif növlərini ayırd və ilkin rəftar etmək; -Gizli açarlı kriptoqrafiya, aşkar açar kriptoqrafiyası, kriptoqrafiyada rəqəmsal sertifikat və ya şəxsiyyət sertifikatı kimi tanınan açıq açar sertifikatı, sertifikat zəncirinin yoxlanılması kimi anlayışları başa düşmək və izah etmək;	- Həşləmə, hash funksiyasını tətbiq edərək, normal mətni və ya açarı hash dəyərinə dəyişdirmək və orijinal sadə mətn əldə etmək üçün həş dəyərinin oxunması prosesini icra etmək. - Mesajın daxil olması (MD5) Təhlükəsiz Həşinq alqoritmi(SHA) Tiger Alqoritmi Mesajın daxil olması alqoritmi(MD4) RİPMEND Burulğan alqoritmi(W-T) kimi həşləmə növləri ilə kod və dekod işlərini ilkin icra etmək;	- Kriptoqrafiya və həşləmənin kibertəhlükəsizlik təyinatlı tapşırıqlarda tətbiqi metodologiyasının tərtib edilməsi		

	sertifikatlar və ona uyğun prosedurlardan ibarət olduğunu bilir.					
KS-İMS-B02 Blokçeyn Texnologiyası	Blokçeyn üçün digər texnologiya sistemlərindən əsas fərqləndiriciləri ifadə edə bilir. Nümunələri, təklifləri, vəziyyət araşdırmalarını və ilkin blockchain sistemi dizayn müzakirələrini təhlil etmək üçün müxtəlif blockchain anlayışlarını tətbiq etməyi bacarır. Müvafiq hüquqi, etik və məxfilik məsələlərini və təşkilatların və ya fərdlərin siyasətinə və hərəkətlərinə necə təsir edə biləcəyini bilir.	-Əsas Blockchain anlayışlarını, üstünlüklərini və blockchain texnologiyalarının məhdudiyyətlərini anlamq və ifadə etmək; - Algorand: Kriptovalyutalar üçün Bizans razılaşmalarının miqyası ilə bağlı anlayışlara sahib olmaq; - Kripto Valyutaların işləmə prinsipini başa düşmək.	- Bitcoin Wallet yaratmaq; - Konsensus əsaslarını, Asenkron Şəbəkələrdə Blockchain Protokolunun təhlil etmək; -VDF konstruksiyaları və Artan Doğrulanabilir Hesablamadan VDF -lər etmək; - Ethereum ağ, sarı kağız real nümunələr üzərində işləməyi bacarmaq.	Blokçeyn texnologiyasını və blokçeyn arxitektura dizatnını dərindən mənimsənməsi və tətbiqini təmin edən metodologiyaların hazırlanması	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İM-B13 Müdaxilələrin Aşkarlanması və Qarşısının alınması	İDS/İPS arxitekturasını anlayır və şəbkədə tətbiqini peşakarcasına təmin etməyi bacarır.	-"İDS/İPS" iş mexanizmini anlamaq; - Anomaliyaların detekt olunması qaydalarını bilmək; - İDS\İPS təhlükəsizlik alətlərinin strateji hədəflərə qatqılarını anlamaq və izah etmək.	- Şəbəkədə "İDS/İPS" yerini optimal təyin etmək; - "İDS/İPS" üzərindən məlumat axınını və inteqrasiyasını təmin etmək; - Şəbəkədə kiber hücumların detekt olunması üçün	Kiberhücumların və müdaxilələrin aşkarlanması və qarşısının alınmasını öyrənmək, eləcə də	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Kiber hücumların analizi və qarşı tədbirlərin tətbiqini İDS\İPS üzərdindən işləməyi bacarır. İDS/İPS alətlərinin işinin təkmilləşdirilməsi qaydalarını tətbiq edə bilir. İDS/İPS növlərindən asılı olmayaraq onlarla işləməyi bacarır. Müdaxilələrin Aşkarlanması və qarşısının alınması strateji yol xəritəsində statusunu və inkişaf amillərini təyin etməyi bacarır.		peşəkarcasına tənzimləmə işləri aparmaq; -İDS/İPS alətlərinin işindən maksimal fayda əldə etmək; - Anomaliyaların detekt olunması qaydalarını tətbiq etmək və təkmilləşdirmək; - İDS/İPS alətləri növləri ilə işləmək; - İDS/İPS alətləri loqlarının ümumi şəbəkə loqları və məlumatları fonunda qarşılaşdırmaq və analiz etmək.	"İDS/İPS" iş prinsipini anlamaq və tətbiq etmək metologiya və strategiyasının hazırlanması;		
KS-İM-B17 Təhlükəsizlik insidentlərinin və hadisələrinin idarə olunması (SİEM) - I və II	SİEM həllərinin tətbiqini və ilkin sazlanmasını bacarır. SİEM həllərinin digər alətlərlə inteqrasiyasının təmin edə bilirüzərdindən işləməyi bacarır.	-Təhlükəsizlik mərkəzinin təyinatı və iş fəaliyyətini anlamaq; - SİEM həllinə daxil və xaric olacaq məlumatların struktur formasını təyin etmək;	- SİEM həlli hazırlığı və inteqrasiyalarının təmin olunmasını icra etmək; -SİEM həllinin defolt göstəricilərini analiz etmək; - Təhlükəsizlik insidentlərini parametrlərini müqayisəli analiz etmək; - Təhlükəsizlik insidentlərini parametrlərini yekun bir nəticə əsasında analiz etmək;	- Təhlükəsizlik insidentlərinin analitikası və hesabatının hazırlanması, həmçinin SİEM həllərinin müxtəlif mühitlərdə tətbiqi, işlənməsi və sazlanması	**7**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Təhlükəsizlik insidentlərini analitikasını bacarır. Təhlükəsizlik insidentlərinin eskalasiya məqamlarını təyin edə bilir. Təhlükəsizlik insidentlərinin hesabatını tərtib etməyi bacarır. Təhlükəsizlik insidentlərinin idarəolunması proqramını müvafiq mühitə uyğun tərtib edə bilir. Təhlükəsizlik insidentlərinin idarəolunması alətlərində qaydaları təkmilləşdirə bilir. TİER-1 səviyyəsində təhlükəsizlik insidentlərini idarə edə bilir. TİER-2 səviyyəsində təhlükəsizlik insidentlərini araşdırılmasını bacarır. TİER-3 səviyyəsində təhlükəsizlik insidentlərini idarə		- Bildiriş və insidentlərin idarəolunması üzrə "Əsas Fəaliyyət Göstəriciləri"ni tərtib etmək və hesablamaq; - Təhlükəsizlik insidentlərinin hesabat formasında tərtibatını icra etmək; - Təhlükəsizlik insidentlərinin idarəolunması proqramını və komponentlərini hazırlamaq; - Təhlükəsizlik insidentlərinin aşkarlanması qaydalarını optimizasiya etmək ; - İnsidentlərin aşkar edilməsi və məlumatlandırmasını icra etmək; - Aşkar edilmiş insidentlər üzərində müvafiq mənbələrdə ilkin araşdırma işlərini icra etmək ; - İnsidentlərin "preventiv" və "detektiv" qarşısının alınması yanaşmasını anlayır və ilkin tətbiqini icra etmək; - İnsidentlərin baş vermə (və ya ehtimal) səbəb və nəticələrini hərtərəfli araşdırmaq; - "Dərindən müdafiə" əsasında insidentin "yol"unun və təsir dairəsini minimallaşdırmaq. - Təhlükəsizlik insidentlərinin statistik göstəriciləri üzrə strateji hədəflərə uyğunluğunu analiz etmək	nı təmin olunması istiqamətində metodologiyaların hazırlanması - SİEM həllərinin tətbiqi nəticəsində aşkarlanmış insidentlərinarəşdırılması və onlara qarşı önləyici tədbirlərin görülməsini təmin edən metodologiya və strategiyaların hazırlanması.		

	edilməsi istiqamətlərini bəlirləməyi bacarır.					
	Təhlükəsizlik insidentlərinin qarşılıqlı və hərtərəfli analizini bacarır.					
	Təhlükəsizlik insidentlərinin göstəricilər üzrə staretji analizini icra etməyi bacarır.					
KS-İM-B14 Zəiflik Qiymətləndirmələri və Nüfuzetmə Testi - İnfrastruktur üzrə	Məlumatları tapmağı öyrənir.	-Nüfuzetmə testi icrasına öncəsi məlumat araşdırma metodlarını bilmək və müəyyən etmək; - Avtomatik və manual nüfuzetmə alətlərinin nəticələrini anlamaq və müqayisə etmək; - Nüfuzetmə testi nəticələrinin biznes mühitə təsiri və qabaqcıl təcrübələr əsasında məntiqi sonluğunu anlamaq və izah etmək;	- İnfrastruktur Nüfuz etmə testi avtomatik və manaul qaydada icra etmək; - İnfrastruktura girişi etik nüfuzetmə qaydaları çərçivəsində təmin etmək; -Nüfuzetmə və zəiflik araşdırmalarını lazım olan məlumat alındıqdan sonra dayandırmağı icra etmək;	İnfrastruktur üzrə zəifliklərin qiymətləndirilməsi və nüfuzetmə testinin icra olunması metodologiyalarının və strategiyalarının hazırlanması;	**5**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
	Müvafiq alətlərlə məlumatları toplamağı və araşdırmağı bacarır.					
	Aşkarlanmış məlumatları analiz etməyi bacarır.					
	Nüfuzetmə testi çərçivəsində infrastruktura giriş əldə etməyi və girişinin iş icrası müddətinə qorumağı bacarır məqamlarını təyin edə bilir.					
	Nüfuzetmə testini əks təsirsiz yekunlamağı və hesabat formasına təşkilini hazırlamağı bacarır.					

KS-İM-B16 Mobil avadanlıqların təhlükəsizliyi	Mobil Avadanlıqlar üzrə təhlükəsizlik qaydalarını bilir. Oğurlanmış avadanlıqlar üzrə ilkin Kiber təhlükəsizlik müdaxiləsi icrasını bacarır. Mobil Avadanlıqların nüfüzetmə testini icra edə bilir. Mobil avadanlıqlar üzərində Zəiflik araşdırmasını icra edə bilir. Mobil avadanlıq "CTF" yarışlarına hazırlaşmağı bacarır. Mobil avadanlıqların təhlükəsizliyi üzrə eskalyasiya əsaslı kommunikasiya və hesabatlılığı bacarır	- Mobil Avadanlıqların zəifliklərini anlamaq və müqayisə etmək;	- Mobil Avadanlıqların arxitekturasını hazırlamaq; - Oğurlanmış avadanlıqların təhlükəsizlik analitikasını və əks tədbirləri icra etmək; -Statik applikasiya analitikasını avtomatik qaydada icra etmək; - Dinamik applikasiya analitikasını avtomatik qaydada icra etmək; - Mobil Avadanlıqların nüfuzetmə testini icra etmək; - Mobil Avadanlıqların "CTF" tədbirlərinə hazırlıq və yanaşma hazırlığına yiyələnmək; - Mobil Avadanlıqların təhlükəsizliyi çatışmazlıqlarının hesabatını tərtib etmək;	Mobil avadanlıqlar üzrə təhlükəsizlik qaydalarının və tədbirlərinin öyrənilməsi və tətbiqi metodologiyaları və strategiyalarının tərtibi.	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İM-B15 Təhlükəsizlik Auditi və Qiymətləndirmə ("SCADA" təhlükəsizliyi)	Audit növləri arasında fərqi anlayır və hədəfə yönəlik seçim edə bilir. Təhlükəsizlik auditi planlamasını tərtib etməyi bacarır. Təhlükəsizlik auditi üzrə nəzarət mexanizmlərinin qiymətləndirməyi bacarır.	- Müxtəlif audit növlərinin bilmək və onlar arasındakı fərqləri anlamaq; -Biznes sorğuya əsasən təyinatı üçün müvafiq audit növünün icrasını ayırd etmək;	- Təhlükəsizlik auditi üçün biznes riskləri araşdırmaq; - Risklər üzrə nəzarət mexanizmləri cədvəlini tərtib etmək və qarşılıqlı analiz etmək; -Risklər üzrə nəzarət mexanizmlərinin qiymətləndirilməsini icra etmək;	Təhlükəsizlik auditi və qiymətləndirilməsi proseslərinin öyrənilməsi və tətbiqi metodologiyalarının hazırlanması;	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	1. SCADA təhlükəsizliyinin ilkin qiymətləndirilməsini bacarır. Təhlükəsizlik auditi nəticələrini və sübutlarını hesabatda tərtib etməyi bacarır.		- SCADA təhlükəsizliyinin mühit və qabaqcıl standartlara əsasən effektivlik analizini icra etmək; - Audit nəticələrinin yekun hesabat və eskalasiyasını təmin etmək;			
KS-İMS-B01 Biznesin davamlılığı və bərpa əməliyyatlarının idarə olunması	BTA icrasını bacarır. Ehtiyat nüsxələmə metodunu təyin və təmin edə bilir. Biznesin davamlılığını planını və komponentlərini hazırlaya bilir. TN 4: Bərpa planı və komponentlərini hazırlaya bilir. TN 5: Biznesin davamlılığı və bərpa vəziyyətlərinin taktik planını tərtib etməyi bacarır.	- BTA – Biznes Təsir Analitikasını anlamaq; -Ehtiyat nüsxələmə prosesini anlamaq.	- BTA strukturu və planını tərtib etmək; - Sistemin dayanıqlılığını qiymətləndirmək; -Ehtiyat nüsxələmə prosesini icra etmək; - Biznesin davamlılığını planını və komponentlərini hazırlamaq; - Fövqəladə hallar üzrə Bərpa planı və komponentlərini hazırlamaq; - Təhlükəsizlik testləri zamanı biznesin davamlılığı və bərpa vəziyyətlərinin statusunu qiymətləndirmək.	Biznesin davamlılığı və bərpa əməliyyatlarının öyrənilməsi və müxtəlif mühitlərdə icra edilməsi metodologiyaları və strategiyaları	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İM-B18 Zəiflik Qiymətləndirmələri və Nüfuzetmə Testi - Veb üzrə	Məlumatları tapmağı öyrənir. Müvafiq alətlərlə məlumatları toplamağı və araşdırmağı bacarır. Aşkarlanmış məlumatları analiz etməyi bacarır.	-Nüfuzetmə testi icrasına öncəsi məlumat araşdırma metodlarını anlamaq və müəyyən etmək; - Avtomatik və manual nüfuzetmə alətlərinin nəticələrini anlamaq və müqayisə etmək; - Nüfuzetmə testi nəticələrinin biznes mühitə təsiri və qabaqcıl təcrübələr əsasında məntiqi	- İnfrastruktur Nüfuz etmə testi avtomatik və manaul qaydada icra etmək; -Kiber hücumun peşəkarcasına təşkili və alətlərlə işləmək; - İnfrastruktura girişi etik nüfuzetmə qaydaları çərçivəsində təmin etmək;	Veb üzrə zəifliklərin qiymətləndirilməsi və nüfuzetmə testinin icra olunması metodologiyalarının və	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Nüfuzetmə testi çərçivəsində infrastruktura giriş əldə etməyi və girişinin iş icrası müddətinə qorumağı bacarır. Nüfuzetmə testini əks təsirsiz yekunlamağı və hesabat formasına təşkilini hazırlamağı bacarır.	sonluğunu anlamaq və izah etmək.	- Nüfuzetmə və zəiflik araşdırmalarını lazım olan məlumat alındıqdan sonra dayandırmağı icra etmək.	strategiyalarının hazırlanması;		
KS-İM-B19 Zərərli proqramların və virusların analizi (Malvar analizi)	Zərərli proqramları peşəkarcasına təyin edə bilir. Zərəli proqamlara qarşı müdafiənin texniki təşkilini təmin etməyi bacarır. Malvar virusuna qarşı mübarizə metodikasını bəlirləyə və icra edə bilir. "Bayrağı ələ keçirmək" yarışlarında malvar testlərinə qarşı hazırlıq yanaşmasını bilir. Biznes mühitində zərərli proqramların təsirlərini təsvir və təqdim etməyi bacarır.	-Zərərli proqramları və xarakteristikalarını bilmək və təyin etmək;	- Zərərli proqramlara qarşı mübarizəyə hazırlığını təmin etmək; - Malvar virusuna qarşı ilkin kiber müayinə və əks tədbirlərin icrasını həyata keçirmək; - Mühit amillərinin nəzərə alınaraq zərərli proqramlara qarşı müdafiənin təşkilini icra etmək ; - Zərərli proqramlara qarşı innovativ həllər və onların strateji tətbiqini təmin etmək ; - Zərərli proqramların texniki təsirini qiymətləndirə bilir.	Zərərli proqramların və virusların təyin edilməsi və onlara qarşı kibermüdafiənin təmin olunması metodologiyaları və strategiyalarının hazırlanması.	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İM-B20 Təhlükəsiz	Təhlükəsizlik protokollarını peşəkarcasına təyin edə bilir.	- Təhlükəsizlik protokolu növü - "Publik key" təyin etmək;	- Təhlükəsizlik protokolu növü - "Publik key" tətbiq etmək; - SSL/ TLS sertifikatları ilə işləmək;	Təhlükəsizlik protokollarının təyin olunması, işləmə	**3**	**PK – 1** **PK – 2** **PK – 3** **PK – 4**

protokolların və sistemlərin dizaynı, təhlili və məlumat təminatı	Sistemlərin dizaynında təhlükəsizlik protokollarını tətbiq etməyi bacarır. Şifrələmə növlərini mühitə uyğun tətbiq edə bilir. Kiber müdafiə təşkilində təhlükəsizlik protokollarının formlaşadırılmasını təmin etməyi bacarır.		- İP təhlükəsizliyini və təşkilinin təhlükəsizlik qiymətləndirməsini yerinə yetirmək; - Təhlükəsizlik protokollarının tətbiqinin yetkinlik dərəcəsini qiymətləndirmək; - Simmetrik və asimmetrik şifrələmənin arxitekturasını təşkil etmək; - Şifrələmənin kiber müdafiə proqramında ilkin təhlükəsizlik qiymətləndirilməsi icra etmək; - Sistem dizaynı və təhlilində təhlükəsizlik protokollarının analitik nəticələrinin təqdimatını hazırlamaq;	mexanizmi, dizaynı və tətbiqi metodologiyalarının hazırlanması.		**PK – 5** **PK – 6** **PK – 7**
KS-İM-B21 Kiber Təhdidlərin araşdırılması və ovlanması	Kiber təhdid risklərini ayırd edə və təsnifat cədvəlini formalaşdıra bilir. Açıq və korporativ məlumat mənbələrində kiber təhdidləri ilkin araşdıra bilir. Kiber təhdid və ovlama alətləri ilə peşəkarcasına işləməyi bacarır.	- Kiber təhdid riskləri anlamaq və təsnifatlaşdırmaq;	- Kiber təhdid alətləri ilə işləmək ; - Kiber ovlama alətləri ilə işləmək ; - Kiber təhlükəsizlik zəncirində kiber təhdidlərin yerini bəlirləyir və ilkin önləmə işlərini icra etmək; - Kiber Strategiya çərçivəsində Kiber Təhdidlərin idarəolunması proqramının strukturunu formalaşdırmaq ; - Məlumat mənbələrinə müvafiq kiber təhdidlər əsasında müraciət etmək; - Məlumat mənbələrindəki kiber təhdidlərlə bağlı müxtəlif məlumatları qarşılaşdırmaq	Kibertəhdidlərin mənimsənilməsi, araşdırılması, analizi və ovlanması və bu əməliyyatlar üçün müxtəlif alətlərin istifadəsi metodologiyalarının hazırlanması	**4**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**

	Kiber təhdidlərin hesabatını və biznesə təsirini ikin qiymətləndirərək tərtib edə bilir.					
KS-İM-B22 Layihə təcrübəsi	Seçilmiş layihənin icra mexanizmini planlaşdırır və icra edir Layihənin nəticələrinin testini edir və təhvil verir	- Tədris edilmiş modullar (ən azı 5 modul üzrə 12 kompetensiyada) üzrə praktiki bacarıqlar üzrə icra ediləcək layihələrin seçimi; - Layihələrin icra mexanizminin planlaşdırılması və icrası; - Layihələrin icra nəticələrinin testi və təhvil verilməsi;	- Layihənin məhdud zaman çərçivəsində planlaşdırmaq və tamamlamaq; - Layihə üzrə praktiki həllərin tapılması və icrası;	-Seçdiyi layihələr üzrə həllərin planlaşdırılması, icrası və test edilməsi əməliyyatların icrası üzrə vərdişlərə.	**9**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
KS-İT-B00	**Təcrübələr** Bu bölümə aid olanların öyrənilməsi nəticəsində təhsil alan subbakalavr:					
KS-İT-B01 / B02 / B03 İstehsalat təcrübəsi-1 / 2 / 3		-qazanılmış nəzəri biliklərin təcrübələr keçirilən müəssisələrdə tətbiqinin mütərəqqi üsul və metodlarını.	-konkret ixtisas sahəsinin təşkili və idarə olunması metodlarını, qaydalarını, prinsiplərini və onların praktiki aprobasiyasını.	-nəzəri sahədə əldə etdikləri bilikləri praktikaya tətbiq etməyi, onların nəticələrini ümumiləşdirməyi və sistemləş-dirmək vərdişlərinə	**35**	**PK – 1** **PK – 2** **PK – 3** **PK – 4** **PK – 5** **PK – 6** **PK – 7**
	KS-İT-B01 / B02 İstehsalat təcrübəsi 1 və 2 təhsil müəssisəsinin laboratoriya şəraiti nəzərə alınmaqla praktiki laboratoriya dərsləri ilə əvəz edilə bilər.					
Kreditlərin ümumi cəmi:					**180**	

3.2. “**Kiber təhlükəsizlik”** ixtisasının təhsil proqramını mənimsəmək üçün ayrılan ümumi həftələr -143-dür,
o cümlədən:
- nəzəri təlim üçün 80;
- imtahan sessiyaları üçün 14;
- təcrübələr üçün 24;
- tətillər üçün 23;
- yekun dövlət attestasiyası üçün 2;

3.3. “**Kiber təhlükəsizlik”** ixtisası üzrə təhsil proqramı aşağıdakı tədris-metodiki sənədlər əsasında həyata keçirilməlidir:
- nümunəvi tədris planı;
- işçi tədris planı;
- istehsalat təcrübələrinin keçirilməsinə, tələbələrin yekun dövlət attestasiyasına dair metodik göstərişlər;
- modul və fənn proqramları;
- modul və fənlər üzrə işçi-tədris proqramları;
- modul və fənlər üzrə tapşırıqların yerinə yetirilməsinin cədvəli;
- dərsliklər, əyani vasitələr, təklif olunan ədəbiyyatın siyahısı;
- nəzəri və praktiki məşğələlərin planı;
- modul və fənnin öyrənilməsi ilə bağlı tövsiyələr;
- laborator və qrafik işlərin yerinə yetirilməsinə, istehsalat təcrübələrinin yekunları barədə hesabatların hazırlanmasına dair metodiki tövsiyələr.

3.4. Subbakalavr “**Kiber təhlükəsizlik”** dərəcəsi verən yüksək peşə təhsili pilləsi üzrə təhsil proqramını həyata keçirən peşə təhsili müəssisələri aşağıdakı hüquqlara malikdirlər:
- tələbə üçün proqramda nəzərdə tutulmuş illik orta dərs yükü həddini və təlimin, minimum məzmununu saxlamaqla təhsil materialının mənimsənilməsinə ayrılmış saatların həcmini modul bölümləri arasında 5%, modul bölümləri daxilində isə 20%-ə qədər dəyişmək;
- seçmə modulların siyahısını, onların tədris ardıcıllığını, dərs növləri üzrə saatların miqdarını müəyyən etmək;
- peşə təhsili müəssisələri seçmə modulları müxtəlif bloklar şəklində təklif edə bilər. Bu bloklara daxil olan modullar mümkün qədər müvafiq ixtisaslar üzrə subbakalavr proqramlarına istiqamətləndirilməlidir;
- hər semestrdə nəzəri təlim müddəti (sonuncu semestr istisna olmaqla) 15 həftədir;
- təhsil dövründə tələbənin məcburi auditoriya dərsləri bir qayda olaraq həftədə 35 saata qədər müəyyənləşdirilir.

4. 030219 – “Kiber təhlükəsizlik” ixtisası üzrə təhsil prosesinin planı

Sıra sayı	Modulların (fənlərin) şifri	Modulların (fənlərin) adı	Kreditin sayı	Ümumi saatlar	Auditoriyadan kənar saatlar	Auditoriya saatları	O cümlədən		Prerekvizit modul/ fənlərin şifri	Tədrisi nəzərdə tutulan semestr	Həftəlik dərs yükü
							Nəzəri dərslər	Praktiki məşğələ			
I	**BM-B00**	**Humanitar və baza modulları bölümü**	**44**	**1320**	**660**	**660**	**300**	**360**			**44**
1	HBM-B01	Azərbaycan tarixi	5	150	90	60	30	30		P1	4
2	HBM-B02	Azərbaycan dilində işgüzar və akademik kommunikasiya	4	120	60	60	30	30		P1	4
3	HBM-B03	İnformasiya texnologiyaları I	2	60	30	30	15	15		P1	2
4	HBM-B04	İnformasiya texnologiyaları II	2	60	30	30	15	15	HBM-B03	Y1	2
5	HBM-B05	İnformasiya texnologiyaları III	2	60	30	30	15	15	HBM-B04	P2	2
6	HBM-B06	Xarici dildə işgüzar və akademik kommunikasiya I	3	90	45	45	15	30		P1	3
7	HBM-B07	Xarici dildə işgüzar və akademik kommunikasiya II	3	90	45	45	15	30	HBM-B06	Y1	3
8	HBM-B08	Xarici dildə işgüzar və akademik kommunikasiya III	3	90	45	45	15	30	HBM-B07	P2	3
9	HBM-B09	Xarici dildə işgüzar və akademik kommunikasiya IV	3	90	45	45	15	30	HBM-B08	Y2	3
10	HBM-B10	Texniki hesab I	2	60	30	30	15	15		P1	2
11	HBM-B11	Texniki Hesab II	3	90	45	45	15	30	HBM-B10	Y1	3
12	HBM-B12	Şəxsi inkişaf və karyera planlaması	3	90	30	60	30	30		Y2	4
13	HBM-B13	Layihə idarə edilməsi	3	90	45	45	15	30		P3	3
	HBMS-B00	*Humanitar və baza modulları bölümü üzrə seçmə modulları*	***6***	***180***	***90***	***90***	***60***	***30***			***6***

15	HBMS-B01 HBMS-B02 HBMS-B03	1. Etika və estetika (İşgüzar Etika) 2. Estetika və Mədəni İfadə 3. STEM	3	90	45	45	30	15		P2	3
16	HBMS-B04 HBMS-B05	1. Sahibkarlığın əsasları və biznesə giriş 2. İstehsalatın idarə edilməsi	3	90	45	45	30	15		Y2	3
II	**KS-İM-B00**	**İxtisasın peşə hazırlığı modulları bölümü**	**101**	**3030**	**1070**	**1960**	**705**	**1255**			**154**
1	KS-İM-B01	Komputer proqramlaşdırması və Əməliyyat sistemləri	4	120	30	90	45	45		P1	6
2	KS-İM-B02	Alqoritmlər və analitik düşünmə	3	90	30	60	30	30		P1	4
3	KS-İM-B03	C proqramlaşdırma dili	4	120	30	90	45	45		P1	6
4	KS-İM-B04	Informasiya Risklərinin İdarə olunması	3	90	30	60	30	30		P1	4
5	KS-İM-B05	IT Sisteminin və təhlükəsizliyin idarəolunması	6	180	60	120	45	75		Y1	8
6	KS-İM-B06	Şəbəkənin və şəbəkə təhlükəsizliyinin İdarəolunması əməliyyatları	5	150	30	120	45	75		Y1	8
7	KS-İM-B07	Linux əməliyyat sistemi	4	120	30	90	30	60		Y1	6
8	KS-İM-B08	Python proqramlaşdırma dili	5	150	60	90	30	60		P2	6
9	KS-İM-B09	Dark Web, Anonimlik və İOT-ların mühafizəsinin təşkili	5	150	60	90	30	60		P2	6
10	KS-İM-B10	Bulud təhlükəsizlik əməliyyatlarının idarəolunması	4	120	60	60	30	30		P2	4
11	KS-İM-B11	Sistem analiz və dizayn, Keyfiyyət Təminatı İdarəetmə (Test İdarəetmə)	5	150	90	60	30	30		P2	4
12	KS-İM-B12	Kiber Hücumlar və Müdafiə, Kriptoqrafiya və Həşləmə	5	150	30	120	30	90		Y2	8

13	KS-İM-B13	Müdaxilələrin Aşkarlanması və Qarşısının alınması	4	120	30	90	30	60		Y2	6
14	KS-İM-B14	Zəiflik Qiymətləndirmələri və Nüfuzetmə Testi - İnfrastruktur üzrə	5	150	30	120	30	90		Y2	8
15	KS-İM-B15	Təhlükəsizlik Auditi və Qiymətləndirmə ("SCADA" təhlükəsizliyi)	3	90	30	60	30	30		P3	4
16	KS-İM-B16	Mobil avadanlıqların təhlükəsizliyi	3	90	30	60	15	45		P3	4
17	KS-İM-B17	Təhlükəsizlik insidentlərinin və hadisələrinin idarə olunması (SİEM) - I və II	7	210	90	120	45	75		P3	8
18	KS-İM-B18	Zəiflik Qiymətləndirmələri və Nüfuzetmə Testi - Veb üzrə	4	120	60	60	30	30		P3	4
19	KS-İM-B19	Zərərli proqramların və virusların analizi (Malvar analizi)	3	90	30	60	30	30		P3	4
20	KS-İM-B20	Təhlükəsiz protokolların və sistemlərin dizaynı, təhlili və məlumat təminatı	3	90	30	60	30	30		P3	4
21	KS-İM-B21	Kiber Təhdidlərin araşdırılması və ovlanması	4	120	60	60	30	30		P3	4
22	KS-İM-B22	Layihə təcrübəsi	9	270	95	175	0	175		Y3	35
III	*KS-İMS-B00*	**İxtisasın peşə hazırlığı üzrə seçmə fənlər**	**3**	**90**	**45**	**45**	**15**	**30**			**3**
1	KS-İMS-B01	Biznesin davamlılığı və bərpa əməliyyatlarının idarəolunması	3	90	45	45	15	30		P2	3
2	KS-İMS-B02	Blokçeyn Texnologiyası	3	90	45	45	15	30		P2	3
III	**KS-İT-B00**	**İstehsalat təcrübə bölümü**	**35**	**1050**	**90**	**960**					**120**
1	KS-İT-B01	İstehsalat təcrübəsi-1	7	210	10	200				Y1	40
2	KS-İT-B02	İstehsalat təcrübəsi-2	7	210	10	200				Y2	40
3	KS-İT-B03	İstehsalat təcrübəsi-3	21	630	70	560				Y3	40

Vaxt Bölgüsü

Tədris ili	Nəzəri təlim		İmtahan sessiyası		Təcrübə		Yekun dövlət attestasiyası	Tətil	
	payız semestri	yaz semestri	Qış	yay	tədris	istehsalat		qış	Yay
I	15.09-30.12 15 həftə	31.01-20.05 15 həftə	05.01-23.01 2.5 həftə	25.06-12.07 2.5 həftə	-	20.05-24.06 5 həftə		24.01-30.01 1 həftə	12.07-14.09 10 həftə
II	15.09-30.12 15 həftə	31.01-20.05 15 həftə	05.01-23.01 2.5 həftə	25.06-12.07 2.5 həftə	-	20.05-24.06 5 həftə		24.01-30.01 1 həftə	12.07-14.09 10 həftə
III	15.09-30.12 15 həftə	31.01-05.03 5 həftə	05.01-23.01 2.5 həftə	06.03-15.03 1.5 həftə		18.03-24.06 14 həftə	25.06 – 08.07	24.01-30.01 1 həftə	-
Cəmi	80 həftə		14 həftə		24 həftə		2 həftə	23 həftə	

5. 030219 – “Kiber təhlükəsizlik” ixtisası üzrə subbakalavr hazırlığını həyata keçirən peşə təhsili müəssisəsinin maddi-texniki bazası və kadr potensialı

5.1. Maddi-texniki baza:

- təhsil proqramını həyata keçirən peşə təhsili müəssisəsi subbakalavr hazırlığını təmin edən maddi-texniki bazaya (emalatxanalar, kabinetlər, laboratoriyalar, sinif otaqları, idman zalları, kitabxana və oxu zalları və s.) malik olmalıdır. Maddi-texniki baza qüvvədə olan inşaat normalarına, sanitar və gigiyenik qaydalarına uyğun olmalıdır.

Sinif otaqları və kabinetlər:
Laboratoriyalar:
Kitabxana, internet şəbəkəsinə çıxışı olan oxucu zalı
İdman kompleksi
İKT laboratoriyası
Akt zalı

5.2. Kadr potensialı:

Peşə təhsili müəssisəsi müvafiq ixtisas üzrə ali və orta ixtisas təhsili olan kadrlarla və ya 5 ildən çox peşəkar əmək təcrübəsinə malik orta təhsilli kadrlarla təmin olunmalıdır.
Peşə təhsili müəssisələrində təhsilverənlərin keyfiyyət göstəricilərinə aşağıdakılar daxildir:

- öz fəaliyyətlərində innovativ təlim, informasiya-kommunikasiya, müasir texnika, yeni istehsal və pedaqoji texnologiyalardan istifadə etməli;
- təhsilverənlər ali və ya orta ixtisas təhsilli olmaqla yanaşı müəyyən istehsalat və pedaqoji təcrübəyə malik olmalı;
- mütəmadi olaraq öz bilik və bacarıqlarını artırmaq üçün müəyyən olunmuş müddətdə və qaydada ixtisasartırmadan keçməlidirlər.

6. Tədris prosesinin forma və metodları

6.1 Tədris formal təhsil formasında həyata keçirilir. Təhsilalma forması əyanidir. 030219 – “Kiber təhlükəsizlik” ixtisas üzrə tələbələrin təhsili kredit sisteminə uyğunlaşdırılmış tədris plan və proqramları əsasında həyata keçirilir.

6.2. Tədris prosesində müxtəlif tədris-təlim metodlarından istifadə olunur (nəzəri, praktiki, laborator məşğələləri və s.). Bununla yanaşı təhsil alanların yaradıcı fəaliyyətinə imkan verən, tədqiqatçılıq bacarıqlarını stimullaşdıran yanaşmalara geniş yer ayrılmalıdır. Yeni pedaqoji texnologiyaları və müasir interaktiv təlim metodlarını əks etdirən dərs-ekskursiya, dərs-yarış, dərs-müzakirə, dərs-disput kimi qeyri-standart tədris yanaşmalarından istifadəyə üstünlük verilməli, təlim prosesinin çevikliyini təmin edən müxtəlif iş formalarından (kollektiv iş, qruplarla iş, cütlərlə iş, fərdi iş) istifadə olunmalıdır. Təlim prosesində dialoqa, məntiqi və tənqidi təfəkkürü inkişaf etdirən, yaradıcı fəaliyyətə əsaslanan fəal və interaktiv metodlardan istifadə edilməlidir. Tədris prosesində həmçinin SƏT (Sərištə Əsaslı Tədris) və layihə metodlarından da aktiv istifadə edilməlidir.

SƏT (Sərištə Əsaslı Tədris) Metodu:

(1) Müəllim təkcə təhsilverən olaraq deyil həm də fasilitator rolunu, tələbələr isə sərbəst şəkildə öyrənən təhsilalan rolunu yerinə yetirir. Nəzəri dərslər üçün optimal sinf ölçüsü 20 tələbə, təcrübə dərsi üçün 10 tələbə və kompetensiya təcrübəsi üçün kiçik qrup (2 ~ 5 tələbə) təşkil edir.

(2) Nəzəri dərslər üçün təhsilverən mühazirə, sual-cavab, proyektorundan istifadə etməklə təqdimat, müzakirə metodu və digər üsullardan istifadə edərək tələbələrə dərsi tədris edə bilər.

(3) Müəllimlər tələbələrə dərsi tədris etdikləri zaman, yarımil ərzində bir sərištəyə və ya alt-sərištəyə aid mövzuların tədrisində "blok sistemi"ni tətbiq edə bilərlər. Tələbələr sərištə üzrə mövzusuları bitirdikdən sonra npvbəti "blok" sisteminə keçə bilərlər. Bu sistem tələbələrə nisbətən böyük bir sərištələri səmərəli şəkildə və uğurla əldə etməsinə imkan verir.

Layihə Metodu

(1) Sinifdə tələbələr 2 ~ 5 tələbədən ibarət kiçik qruplara bölünür və yerinə yetirilməsi üçün tapşırıqlar müəyyən edilir. Proses, rol təyinatı və cədvəl də daxil olmaqla layihə planını hazırlanır. Lazımi materialları hazırlanır.

(2) Proses zamanı müəllimin nəzarəti altında peşə təhsili müəssisəsinin avadanlıqları, alətləri və vasitələrindən istifadə edilir. Tələbələr layihənin nəticəsinə dair təqdimatı digər tələbələrə təqdim edir. Qiymətləndirmə meyarlarına görə layihənin nəticəsini müəllim qiymətləndirir. Layihəyə aid müəyyən işləri və nəticələri təhsil müəssisəsinin məhsul sərgisində nümayiş etdirilir.

7. Yekun dövlət attestasiyasına qoyulan tələblər və qiymətləndirmə

7.1. Tələbələrin qiymətləndirilməsi Azərbaycan Respublikasının Təhsil Nazirliyinin KQ-06 nömrəli qərarı ilə təsdiq olunmuş “Peşə təhsili pilləsində təhsilalanların attestasiyasının aparılması Qaydası” sənədində qeyd olunmuş formada həyata keçirilir. Subbakalavriat səviyyəsində ixtisaslar üzrə təhsil proqramları təhsilalanların dövlət attestasiyası ilə yekunlaşır.

7.2. Tədris planının bütün şərtlərini yerinə yetirmiş, o cümlədən nəzərdə tutulmuş attestasiyalardan müvəffəq qiymət almış tələbə üçün təhsil müddətində əldə etdiyi nəticələrə uyğun olaraq ümumi orta müvəffəqiyyət göstəricisi (ÜOMG) hesablanır. ÜOMG tələbənin təhsil proqramını mənimsəmə səviyyəsinin göstəricisidir və diploma əlavəyə daxil edilir. ÜOMG modul/fənlər üzrə toplanan balların həmin modul/fənnə görə qazanılan kreditlərə hasilləri cəmlərinin tədris planında nəzərdə tutulan müvafiq kreditlərin cəminə olan nisbəti kimi müəyyənləşdirilir:

$$\text{ÜOMG}\ \frac{b1+k1^*+b2k2^*+b3k3^*+\ldots+bnkn^*}{k1+k2+k3+\ldots+kn}$$

b1,b2,…,bn - tələbənin modullar (fənn) üzrə yığdığı ballar
k1,k2,…,kn - modullara tədris planında nəzərdə tutulan müvafiq kreditlər
k1*, k2*,..., k3* - modullar üzrə qazanılmış kreditlər (əgər tələbə imtahandan müvəffəq qiymət almazsa o, krediti qazanmamış hesab edilir və bu əmsal «0» sıfr olur)

7.3. Subbakalavriat səviyyəsində tələbələrin topladığı kreditlərin sayı 180 olmalıdır. İxtisaslar üzrə təhsil proqramlarında nəzərdə tutulmuş kreditləri toplayan tələbə həmin proqramı mənimsəmiş hesab edilir. Peşə təhsili müəssisələrində subbakalavriat səviyyəsinə uyğun yüksək peşə təhsili proqramı üzrə tədris planını tam yerinə yetirmiş şəxslərə yekun Dövlət Attestasiya Komissiyasının qərarı əsasında “subbakalavr” peşə-ixtisas dərəcəsi verilir.