AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

Azərbaycan Respublikasının
Elm və Təhsil Nazirliyinin
3-29/3 -2 -548F/2025/1 nömrəli
08.09.2025-ci il tarixli əmri
ilə təsdiq edilmişdir.

MAGİSTRATURA SƏVİYYƏSİNİN İXTİSAS ÜZRƏ

T Ə H S İ L P R O Q R A M I

İxtisasın şifri və adı: 7006017 - İnformasiya təhlükəsizliyi

BAKI – 2025

AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN UNİVERSİTETİ

Azərbaycan Universiteti Elmi şurasının
12.09.2025-ci il tarixli,
01 saylı protokolu ilə təsdiq edilmişdir.

Rektor S.N. Əliyeva

MAGİSTRATURA SƏVİYYƏSİNİN İXTİSAS ÜZRƏ
T Ə H S İ L P R O Q R A M I

İxtisasın şifri və adı: 7006017 - İnformasiya təhlükəsizliyi

İxtisaslaşma adı: Kibertəhlükəsizlik

BAKI – 2025

MAGİSTRATURA SƏVİYYƏSİNİN İXTİSAS ÜZRƏ TƏHSİL PROQRAMININ ÇƏRÇİVƏ SƏNƏDİ

1. Ümumi müddəalar

1.1. Magistratura səviyyəsinin **7006017 – İnformasiya təhlükəsizliyi** ixtisası üzrə təhsil proqramı (bundan sonra – təhsil proqramı) "Təhsil haqqında" Azərbaycan Respublikasının Qanununa, Azərbaycan Respublikasının Nazirlər Kabinetinin müvafiq qərarlarına, eləcə də "Ali təhsilin magistratura səviyyəsi üzrə ixtisasların Təsnifatı"na, qabaqcıl beynəlxalq təcrübə və əmək bazarının tələblərinə uyğun olaraq hazırlanmışdır.

1.2. Təhsil proqramının məqsədləri aşağıdakılardır:

- ixtisas üzrə məzunun səriştələrini, ixtisasın çərçivəsini, fənlər üzrə tədris və təlim metodlarını, qiymətləndirmə üsullarını, təlim nəticələrini, kadr hazırlığı aparmaq üçün infrastruktur və kadr potensialına olan tələbləri, təhsilalanın təcrübə keçmə, işə düzəlmə və təhsilini davam etdirmə imkanlarını müəyyənləşdirmək;
- təhsilalanları və işəgötürənləri məzunların əldə etdiyi bilik, bacarıq və təlim nəticələri ilə tanış etmək;
- təhsil proqramı üzrə kadr hazırlığının bu proqrama uyğunluğunun qiymətləndirilməsi zamanı prosesə cəlb olunan tərəfdaşları məlumatlandırmaq.

1.3. Təhsil proqramı, tabeliyindən, mülkiyyət növündən və təşkilati-hüquqi formasından asılı olmayaraq, Azərbaycan Respublikasında fəaliyyət göstərən və həmin ixtisas üzrə magistr hazırlığını həyata keçirən bütün ali təhsil müəssisələri üçün məcburidir.

1.4. Təhsilalanın 5 (beş) günlük iş rejimində həftəlik auditoriya və auditoriyadankənar ümumi yükünün həcmi 45 akademik saatdır (xüsusi təyinatlı ali təhsil müəssisələri istisna olmaqla). Bu zaman auditoriya saatlarının həcmi 12-16 akademik saat təşkil edir. Peşəkar məqsədlər üçün dərindən öyrənilən ixtisaslaşmalar üzrə həftəlik dərs yükünün həcmi dəyişdirilə bilər.

1.5. Ali təhsil müəssisəsi tərəfindən ixtisasın həmin müəssisədə kadr hazırlığı aparılan hər bir ixtisaslaşması üzrə ayrıca təhsil proqramı hazırlanmalıdır. Hər bir ixtisaslaşma üzrə təhsil proqramı müvafiq ixtisasın təhsil proqramındakı bölmələrlə yanaşı, həmin ixtisaslaşma üzrə tədris və təlim metodları, təlim nəticələrinin qiymətləndirilməsi üsulları, təcrübələrin təşkili və qiymətləndirilməsi və s. bölmələri də əks etdirməlidir.

2. Məzunun səriştələri

2.1. Təhsil proqramının sonunda məzun aşağıdakı ***ümumi səriştələrə*** yiyələnməlidir:

- peşəkar fəaliyyəti çərçivəsində gözlənilməz və mürəkkəb məsələləri müstəqil şəkildə həll edə bilmək;
- müvafiq fəaliyyət və metodları təklif etmək, planlaşdırmaq, onların cari və perspektiv nəticələrini təhlil etmək;
- fəaliyyət və ya təhsil sahəsi ilə bağlı problemlərin səbəblərini araşdırmaq, konkret vaxt çərçivəsində və məhdud informasiya şəraitində onları həll edə bilmək;

- fəaliyyət və ya təhsil sahəsi ilə bağlı problemlərin həlli zamanı müvafiq texnologiya və metodları seçmək və onlardan istifadə edə bilmək, həmçinin gözlənilən nəticələri müəyyənləşdirmək, dəyərləndirmək və qiymətləndirmək;
  fəaliyyət və ya təhsil sahəsi ilə bağlı problemlərin həlli zamanı öz fəaliyyətini tənqidi şəkildə dəyərləndirmək;
- fəaliyyət və ya təhsil sahəsi ilə bağlı problemləri Azərbaycan dilində və bir xarici dildə şifahi və yazılı olaraq təqdim etmək, əsaslandırmaq, həmçinin mütəxəssis və qeyrimütəxəssislərlə birgə müvafiq müzakirələrdə iştirak etmək;
- müxtəlif üsullarla öz bilik və səriştələrini başqalarına ötürə bilmək;
- istənilən şəraitdə etik davranış qaydalarına uyğun şəkildə fəaliyyət göstərmək, şəxsi davranışlarının etik aspekt və imkanlarını, məhdudiyyətlərini və sosial rolunu anlamaq;
- davamlı öyrənmə və peşəkar inkişafla bağlı özünün və digərlərinin ehtiyaclarını qiymətləndirə bilmək, həmçinin müstəqil öyrənmə üçün zəruri olan səmərəli metodlardan istifadə edə bilmək;
- zəruri metod və alətlərdən, süni intellekt və maşın öyrənməsi üsullarından istifadə etməklə yeni təhlükəsizlik modellərinin və qorunma vasitələrinin işlənməsi istiqamətində elmi tədqiqatlar aparmaq, elmi məqalə, texniki hesabat və təqdimatlar hazırlamaq və alınmış nəticələri tətbiq etmək

2.2. İxtisaslaşmalar üzrə məzun aşağıdakı **peşə səriştələrinə** yiyələnməlidir.

Kibertəhlükəsizlik ixtisaslaşması üzrə:

- kriptoqrafiya, autentifikasiya, identifikasiya, məlumatların gizliliyi, bütövlüyü və əlçatanlığı (CIA modeli) ilə bağlı zəruri bililklərə malik olmaq, kriptoqrafik qoruma üsullarını, şifrələmə alqoritmlərini, elektron imza, açarların idarə edilməsi sistemlərini (PKI), SSL/TLS protokollarını reallaşdırmaq və tətbiq edə bilmək;
- kibertəhlükəsizlik strategiyasını hazırlamaq, təşkilatın təhlükəsizlik siyasətlərini formalaşdırmaq və tətbiq etmək;
- kibertəhlükəsizlik risklərini təhlil etmək, qiymətləndirmək, uyğun müdafiə tədbirlərinin planlaşdırılması, idarə edilməsi strategiyalarını hazırlamaq və icra etmək;
- zəif yerlərin aşkarlanması skanerlərini, penetrasiya testlərini və etik hakerliyi həyata keçirmək;
- kiberinsidentlərin aşkarlanması, təhlili və cavablandırılması, loq analizləri, forensik analiz və sübutların toplanması, qorunması, hüquqi prosedurlarla, SIEM (Splunk, Qradar və s.) sistemləri ilə işləmək;
- zərərli proqram təminatlarını (malware, phishing, DoS/DDoS, ransomware və s.) analiz etmək və qarşısını almaq;
- firewall, IDS/IPS, VPN, şəbəkə monitorinqi kimi texnologiyaları konfiqurasiya və idarə etmək;
- kibertəhlükəsizlik sahəsində yaranan problemlərin həllində süni intellekt və maşın öyrənməsi texnologiyalarını tətbiq etmək;
- ISO/IEC 27001, COBIT, NIST SP 800 seriyasından olan standartları öz fəaliyyətində rəhbər tutmaq, tətbiq etmək və onların tələblərinə riayət etmək.

3. Təhsil proqramının strukturu

3.1. Təhsil proqramının mənimsənilməsinin normativ müddəti və məzunlara verilən ali elmi-ixtisas dərəcəsi:

İxtisaslaşmaların adları	Verilən dərəcə	Əyani forma üzrə təhsil müddəti	Kreditlərin sayı
Kİbertəhlükəsizlik	Magistr ali elmi-ixtisas	2 il	120

3.2. Təhsil proqramı 120 (2 il) AKTS kreditindən ibarət olmalıdır. Hər semestrdə 5 fəndən çox olmamaq şərti ilə 30 kredit nəzərdə tutulmuşdur. Kreditlər aşağıdakı şəkildə bölüşdürülür

Sıra sayı	Fənnin adı	AKTS krediti
1	**Tədqiqat metodları** *Bu fənn kəmiyyət və keyfiyyət tədqiqat metodlarının, ölçmə, tədqiqat dizaynı və təhlilin qarşılıqlı asılılığına diqqət yetirir. Fənn çərçivəsində tədqiqat səriştələri, kitabxana və internet resurslarından məlumat qaynağı kimi istifadə edilməsi, verilənlərin araşdırılması, təhlil edilərək təqdim edilməsi kimi keyfiyyətin aşılanmasını nəzərdə tutur.*	6
2	**Akademik yazı və etika** *Bu fənnin məqsədi akademik yazı, danışıq və dürüstlüyün əsaslarını öyrətmək, magistrantların elmi məqalə, dissertasiya, esse və digər akademik sənədləri peşəkar şəkildə yazmaq, konfrans, simpozium, seminar və elmi diskussiyalarda peşəkar şəkildə danışmaq, nəşr etikası bacarıqlarını inkişaf etdirməkdir. Fənn təhsilalanlara akademik üslub, mənbələrdən düzgün istifadə, istinad qaydaları və etik normalar haqqında bilik və səriştələr verəcəkdir.*	6

3	**Tədqiqat analitikası** *Bu fənnin tədrisi məlumat təhlili prosesi, məlumat növləri, məlumatların toplanma mənbələri, məlumat təhlili üzrə strategiyanın qurulması, məlumatların təhlil üçün hazırlanması və təmizlənməsi, təhlil üçün məlumatların sistemləşdirilməsi, məlumatların vizuallaşdırılması, sahəyə uyğun olaraq təhlillərdə istifadə olunacaq proqram təminatları ilə tanışlıq ("Excel", "SPSS", "Stata", "R", "MAXQDA", "Matlab", "Python" və s. kimi), ixtisas sahəsində tədqiqatlarda istifadə olunan təhlil metodları ilə təhlillərin aparılması (statistik testlər və təhlillər, kəmiyyət və keyfiyyət təhlilləri, eksperimental təhlillər, anket və sorğu təhlilləri və s. kimi) və təhlillərin əsasında müvafiq rəylərin hazırlanmasını nəzərdə tutur.*	6
4	**Ali təhsil müəssisəsi tərəfindən müəyyən edilən məcburi fənlər[1]** *ixtisaslaşmadan asılı olaraq buraya daxil edilən fənlər hər bir ali təhsil müəssisəsi tərəfindən fərdi qaydada müəyyən edilir və həmin ixtisaslaşmanın təhsil proqramında öz əksini tapır.*	72
...	**Ali təhsil müəssisəsi tərəfindən müəyyən edilən seçmə fənlər[2]** *Müvafiq fənlər hər bir ali təhsil müəssisəsi tərəfindən fərdi qaydada ixtisaslaşmadan asılı olaraq müəyyən edilir və həmin ixtisaslaşmanın təhsil proqramında əksini tapır.*	
Təcrübə		
...	**Elmi-pedaqoji təcrübə**	6
...	**Elmi tədqiqat təcrübəsi**	6
Dissertasiya işi		
...	**Magistrlik dissertasiyası**	18
CƏMİ		**120**

[1] Burada "fənlər" dedikdə fənlərlə yanaşı, layihələr (eləcə də "Capstone" layihəsi), yaradıcılıq işi, laboratoriya işləri və digər aidiyyəti tədris fəaliyyətləri (olduğu təqdirdə) başa düşülür. Bu fənlər akademik heyətin təcrübəsi, tədqiqat infrastrukturu, yerli və beynəlxalq iş imkanları nəzərə alınaraq ali təhsil müəssisəsi tərəfindən müəyyən edilir və müvafiq ixtisaslaşma üzrə qəbul olan təhsilalan üçün məcburi xarakter daşıyır. Bu bölmədə minimum 4 fənn olmalıdır.

[2] Burada "fənlər" dedikdə fənlərlə yanaşı, layihələr (eləcə də "Capstone" layihəsi), yaradıcılıq işi, laboratoriya işləri və digər aidiyyəti tədris fəaliyyətləri (olduğu təqdirdə) başa düşülür. Bu fənlər akademik heyətin təcrübəsi, tədqiqat infrastrukturu, yerli və beynəlxalq iş imkanları nəzərə alınaraq ali təhsil müəssisəsi tərəfindən təklif edilir. Sözügedən fənlər müəyyən edilən zaman əmək bazarının təklifləri də nəzərə alınır və bu məqsədlə ali təhsil müəssisələri və əmək bazarı nümayəndələrindən ibarət işçi qrupunun yaradılması tövsiyə olunur. Ali təhsil müəssisəsi tərəfindən müəyyən edilən fənlər təhsilalanlar üçün seçmə xarakter daşımalı, eləcə də təhsilalanların xarici mübadilə proqramlarında iştirakına şərait yaratmalıdır. Bu bölmədə minimum 3 fənn olmalıdır.

4. Proqramın və hər bir fənnin təlim nəticələri

4.1. Bu təhsil proqramı üzrə məzunlar təhsil və ya fəaliyyət sahəsi ilə bağlı əsas anlayışlar, nəzəri prinsip və tədqiqat metodları haqqında sistemli, ümumi təsəvvürə və geniş biliyə malik olmalı, konkret (ixtisaslaşmış) təhsil və ya fəaliyyət sahəsində dərin biliklərə yiyələnməlidirlər.

4.2. İxtisaslaşmanın təhsil proqramının hər bir fənn üzrə təlim nəticələrinin müəyyənləşdirilməsi və hər bir fənnin sillabusunun hazırlanması ali təhsil müəssisəsinin/akademik heyətin səlahiyyətindədir.

4.3. İxtisaslaşma üzrə proqramın təlim nəticələri Əlavə 1-də müəyyən olunur. Fənlər üzrə təlim nəticələri isə hər bir ali təhsil müəssisəsi tərəfindən müəyyənləşdirilir. Təlim nəticələri matrisində (Əlavə 2) fənlərlə təhsil proqramının təlim nəticələri arasındakı əlaqə əks olunmalıdır.

4.4. Təhsil proqramının cəmiyyətin və əmək bazarının dəyişən ehtiyaclarına cavab verən elmi və praktiki məzmunu təmin etməsi məqsədilə fənlərin sillabusları müntəzəm şəkildə yenilənməlidir.

5. İnfrastruktur və kadr potensialı

5.1. Ali təhsil müəssisəsi tədris, təlim və qiymətləndirmə fəaliyyətlərinin yüksək səviyyədə təşkil olunması üçün informasiya-kommunikasiya texnologiyaları ilə təchiz edilmiş müasir auditoriyalara malik olmalı, tələbələrə lokal şəbəkə və internetə, elektron kitabxanalara və onlayn arxiv resurslarına fasiləsiz çıxış imkanı yaratmalıdır. Eyni zamanda, tələbələrin ixtisaslaşma üzrə dərin biliklərə yiyələnməsi və elmi-tədqiqat işlərinin aparılmasını dəstəkləmək məqsədilə müasir elmi jurnallara, elmi məlumat bazalarına və virtual laboratoriya mühitlərinə, akademik etik mühitə inteqrasiya üçün antiplagiat sistemlərinə çıxışı təmin edilməlidir.

5.2. Ali təhsil müəssisələrinin tədrisə cəlb olunan akademik heyəti, bir qayda olaraq, elmi dərəcəyə malik olur. Elmi dərəcəsi olmayan, lakin müvafiq sahədə ən az 5 il iş təcrübəsi olan mütəxəssislər də tədrisə cəlb oluna bilərlər.

5.3. Magistrlik dissertasiyalarına elmi rəhbərlik, bir qayda olaraq, elmi ada və ya elmi dərəcəyə sahib olan şəxslər tərəfindən həyata keçirilir.

6. Karyera imkanları və ömürboyu təhsil

6.1. "İnformasiya təhlükəsizliyi" ixtisası üzrə magistr proqramını uğurla başa vuran məzunlar aşağıdakı sahələrdə və vəzifələrdə fəaliyyət göstərə bilərlər:

Məşğulluq sahələri:

- Milli təhlükəsizlik və kiberhücumlarla mübarizə mərkəzləri;
- Dövlət informasiya sistemləri və təhlükəsizlik xidmətləri;
- Hərbi və müdafiə qurumları (kiberhücumlara qarşı mübarizə üçün);
- Hüquq-mühafizə orqanları;
- Kriminalistik təhqiqat müəssisələri;
- Səhiyyə təşkilatları (xəstəxanalar, klinikalar, tibb mərkəzləri və s.);
- Maliyyə, bank, kredit, vergi, gömrük və digər hökumət təşkilatları;

- Sığorta şirkətləri;
- Telekommunikasiya və rabitə təşkilatları;
- İnternet provayderləri;
- Mobil operatorlar;
- Bulud xidməti təminatı şirkətləri;
- İnformasiya texnologiyaları sahəsində fəaliyyət göstərən şirkərlər;
- Təhlükəsizlik məhsulları və proqram təminatları istehsal edən şirkətlər;
- Kibertəhlükəsizlik və bulud təhlükəsizliyi üzrə məsləhət və xidmət təminatı təşkilatları;
- Penetrasiya testləri və şəbəkə təhlükəsizliyi auditləri aparan şirkətlər;
- Ticarət və kommersiya şirkətləri;
- Elektron ticarət və rəqəmsal xidmət platformaları;
- Universitetlər, elmi tədqiqat institutları;
- Kütləvi informasiya vasitələri (televiziya, radio, xəbər portalları).

Peşələr və vəzifələr:

- İnformasiya təhlükəsizliyi mütəxəssisi;
- Kibertəhlükəsizlik mütəxəssisi;
- Sistem təhlükəsizliyi inzibatçısı;
- Şəbəkə təhlükəsizliyi mütəxəssisi;
- Verilənlər bazası təhlükəsizliyi mütəxəssisi;
- Kibertəhlükəsizlik analitiki;
- Risk meneceri;
- Audit mütəxəssisi;
- Rəqəmsal kriminalistika və ekspertiza mütəxəssisi;
- Forensika analitiki;
- Penetrasiya testi üzrə mütəxəssis;
- Etik haker;
- DevSecOps mühəndisi;
- Universitetlərdə müəllim;
- Elmi-tədqiqat institutlarında elmi-tədqiqatçı.

6.2. Ali təhsil müəssisəsi təhsil proqramının məzunlarının məşğulluğuna dair müntəzəm sorğular keçirməli, eləcə də vakant iş yerlərinə dair məlumatları öz veb-səhifələrində yerləşdirməlidir.

6.3. Ali təhsil pilləsinin magistratura səviyyəsini bitirən (magistrlik dissertasiyasını müdafiə edən), yaxud təhsili ona bərabər tutulan şəxslər (tibbi təhsildə həkim-mütəxəssis) fəlsəfə doktoru proqramı üzrə doktoranturaya qəbul oluna bilərlər.

6.4. Təhsil müddətində əldə olunan bilik, bacarıq və yanaşmalar məzunların müstəqil şəkildə ömür boyu təhsil almaları üçün ilkin şərtlərdəndir.

7. Təcrübə

7.1. Təcrübə tələbənin nəzəri biliklərinin praktikada tətbiqi, eləcə də peşə bacarıqlarının gücləndirilməsi baxımından önəmlidir. İxtisasın xüsusiyyətlərindən asılı olaraq təcrübənin təşkili qayadaları ali təhsil müəssisəsi tərəfindən müəyyən oluna bilər.

7.2. Təcrübə özəl şirkətdə, dövlət müəssisəsində, tədqiqat laboratoriyasında (eləcə də universitet, AMEA, yerli, yaxud beynəlxalq özəl təşkilat və şirkətlərdə və s.) təşkil oluna bilər.

7.3. Təcrübə prosesindən maksimal fayda əldə etmək məqsədilə tələbələr ilkin hazırlıq prosesinə cəlb edilməli (karyera palanlanması) və onların müvafiq bacarıqları (yumşaq və sərt bacarıqlar) fromalaşdırılmalıdır.

7.4. Təcrübənin təşkili ali təhsil müəssisəsinin vəzifəsidir. Təcrübədən öncə ali təhsil müəssisəsi və təcrübə təşkil olunacaq qurum arasında müqavilə imzalanmalıdır. Müqavilədə təcrübənin keçirilmə şərtləri, tələbələrin hüquq və vəzifələri və digər zəruri təfərrüatlar əks olunur. Təcrübəni təşkili iki formada təklif olunacaqdır. İmzalanmış müqaviləyə uyğun olaraq, tələbələr müvafiq şirkət və qurumlarda təcrübə imkanlarını araşdıracaq və müsbət dəyərləndirilən tələbələr qarşı tərəfin razılıq sənədlərini universitetə təqdim edəcəkdir. Eyni zamanda, tələbənin fərdi müraciəti əsasında onun ixtisasına uyğun digər qurumlarda, o cümlədən xaricdə təcrübə keçməsinə icazə verilir.

7.5. Təcrübənin təşkilinin ikinci forması isə, tələbələrin iş dünyasından daxil olan sifariş layihələrinin icra olunmasıdır. Belə ki, müxtəlif Özəl və dövlət qurumlarında ehtiyac duyulan araşdırmalar, təkmilləşmə imkanları, problemlərə həll yolları tələbə və mentor müəllimlərin birgə fəaliyyəti ilə təhlil və tədqiq ediləcək və layihə şəklində sifarişçilərə təqdim ediləcəkdir.

7.6. Təcrübənin qiymətləndirilməsi təqdim olunmuş layihənin dəyərləndirilməsindən sonra iş dünyası nümayəndələri tərəfindən həyata keçiriləcəkir.

7.7. Təcrübənin qiymətləndirilməsi: tələbə təcrübə müddətində istehsalat müəssisəsi və ya şirkətdə aparılan təcrübə layihəsinin nəticələrinə dair hesabatın yazmalı və ali məktəbin akademik heyəti və təcrübə yerinin nümayəndələrindən ibarət komissiya qarşısında müdafiə etməlidir. Təcrübə proqramının yerinə yetirilməsi üzrə nəticələr təhsil müəssisəsi tərəfindən müəyyənləşdirilmiş formada qiymətləndirilir.

Əlavə 1

Təhsil proqramı və tədris fəaliyyəti üzrə təlim nəticələri

Proqramın təlim nəticələri (PTN)
PTN 1. Elmi etika prinsiplərinə əsaslanaraq sahə üzrə probelmləri müəyyənləşdirməyi, həlli istiaqamətində tədqiqat suallarını formalaşdırmağı, uyğun tədqiqat metodlarını seçib tətbiq etməyi, verilənləri analitik üsullarla təhlil etməyi və əldə olunan nəticələri akademik yazı standartlarına uyğun şəkildə təqdim etməyi bacaracaq.
PTN 2. İnformasiya təhlükəsizliyi probleminin mahiyyətini, konsepsiyasını, əsas prinsiplərini, CIA modelini (konfidensiallıq, bütövlük, mövcudluq), rəqəmsal sistemlər, şəbəkələr, əməliyyat sistemləri və proqram təminatının təhlükəsizlik aspektləri, kompüter və telekommunikasiya şəbəkələrinin qorunması üsul və vasitələrini bilir.
PTN 3. Klassik və müasir kriptoqrafik üsulları (simmetrik/asimmetrik şifrələmə, rəqəmsal imza, açar mübadiləsi), kriptoqrafiyanın real sistemlərdə tətbiqi protokollarını (VPN, SSL/TLS, PKI və s.), elektron sertifikatları, rəqəmsal identifikasiya və autentifikasiya texnologiyaları (biometrik sistemlər, çoxmərhələli autentifikasiya (MFA), SSO və s.) ilə işləyir, Firewall, IDS/IPS, WAF, NAT, DMZ, VLAN və digər qoruma texnologiyalarını bilir və tətbiq edir, infrastruktur və bulud sistemlərinin təhlükəsiz arxitekturasını layihələndirməyi bacarır
PTN 4. Təhlükəsizlik risklərinin identifikasiyası, qiymətləndirilməsi və qarşısının alınması üsulları bilir və tətbiq edir, müəssisələrdə təhlükəsizlik strategiyasını, təhlükəsizlik siyasətlərini və prosedurlarını hazırlayır və həyata keçirir, informasiya təhlükəsizliyi idarəetmə sistemlərini (ISMS) qurur.
PTN 5. Penetrasiya testləri keçirir, etik hacking texnikalarını tətbiq edir, təhlükəsizlik insidentlərinin aşkarlanması, cavablandırılması və təhlili, rəqəmsal forensika və sübutların toplanması üsul və vasitələri ilə işləyir
PTN 6. İnformasiya təhlükəsizliyi üzrə yerli və beynəlxalq normativ hüquqi sənədləri, standart və protokollarl (ISO/IEC 27001, NIST, COBIT, GDPR və s.) bilir və fəaliyyətində rəhbər tutur, uyğunluq (compliance) və audit proseslərinin təşkil edir.
PTN 7.İnformasiya təhlükəsizliyi sahəsində, informasiya təhlükəsizliyi üsul və vasitələrinin, yeni texnologiyaların (süni intellekt, blokçeyn, post-kvant kriptoqrafiya və s.) işlənməsi, təhlükəsizlik aspektlərinin qiymətləndirilməsi istiqamətlərində elmi-tədqiqat işləri aparır, tədris və metodoloji fəaliyyət üçün elmi əsaslar hazırlayır.

Kibertəhlükəsizlik ixtisaslaşması üzrə:

Proqramın təlim nəticələri (PTN)
PTN 1. Elmi etika prinsiplərinə əsaslanaraq sahə üzrə probelmləri müəyyənləşdirməyi, həlli istiaqamətində tədqiqat suallarını formalaşdırmağı, uyğun tədqiqat metodlarını seçib tətbiq etməyi, verilənləri analitik üsullarla təhlil etməyi və əldə olunan nəticələri akademik yazı standartlarına uyğun şəkildə təqdim etməyi bacaracaq.
PTN 2. Kriptoqrafiya, autentifikasiya, identifikasiya, məlumatların gizliliyi, bütövlüyü və əlçatanlığı (CIA modeli) ilə bağlı zəruri bililklərə malik olur, kriptoqrafik qoruma üsullarını, şifrələmə alqoritmlərini, elektron imza, açarların idarə edilməsi sistemlərini (PKI), SSL/TLS protokollarını reallaşdırır və tətbiq edir.
PTN 3. Kibertəhlükəsizlik strategiyasını hazırlayır, təşkilatın təhlükəsizlik siyasətlərini formalaşdırırı və tətbiq edir

PTN 4. Risklərin təhlili, qiymətləndirilməsi, uyğun müdafiə tədbirlərinin planlaşdırılması, idarə edilməsi strategiyalarını bilir və tətbiq edir, zəif yerlərin aşkarlanması skanerləri, penetrasiya testləri və etik hakerliyi həyata keçirir, zərərli proqram təminatlarının (malware, phishing, DoS/DDoS, ransomware və s.) analizini edir və qarşısını alır.
PTN 5. Kiberinsidentlərin aşkarlanması, təhlili və cavablandırılması, loq analizləri, forensik analiz və sübutların toplanması, qorunması, hüquqi prosedurlarla, SIEM (Splunk, Qradar və s.) sistemləri ilə işləyir, firewall, IDS/IPS, VPN, şəbəkə monitorinqi kimi texnologiyaları konfiqurasiya və idarə edir.
PTN 6. Kiberbertəhlükəsizlik sahəsində yaranan problemlərin həllində süni intellekt və maşın öyrənməsi texnologiyalarını tətbiq edə bilir.
PTN 7.ISO/IEC 27001, COBIT, NIST SP 800 seriyasından olan standartları bilir, öz fəaliyyətində rəhbər tuturvə onların tələblərinə riayət edir.

Fənn Təlim Nəticələri
“Kibertəhlükəsizlik” ixtisaslaşması üzrə

1. Kibertəhlükəsizliyin əsasları

FTN 1. Kibertəhlükəsizlik sahəsində əsas konsepsiyaları, hüquqi və etik prinsipləri sistemli şəkildə təhlil edir və onların təşkilati idarəetmədə rolunu qiymətləndirir.

FTN 2. Müxtəlif kiberhücum modellərini (APT, ransomware, sosial mühəndislik, zərərli proqram təminatı və s.) analiz edir və onların qarşısının alınması üçün qabaqlayıcı strategiyalar hazırlayır.

FTN 3. Məlumat təhlükəsizliyinin təminində istifadə olunan texnologiyaları (kriptosistemlər, şəbəkə müdafiə sistemləri, təhlükəsizlik protokolları və s.) elmi əsaslarla qiymətləndirir və tətbiq edir.

FTN 4. Kibertəhlükəsizlik üzrə risklərin idarə edilməsi, insidentlərin aşkarlanması və cavab mexanizmlərinin planlaşdırılması üzrə kompleks yanaşma formalaşdırır.

FTN 5. Milli və beynəlxalq kibertəhlükəsizlik siyasətləri, standartları və normativ aktlar kontekstində təşkilatın təhlükəsizlik arxitekturasını qiymətləndirir və təkmilləşdirmə təklifləri irəli sürür.

2. Kriptoqrafiyanın əsasları

FTN 1. Kriptoqrafiyanın nəzəri əsaslarını, onun tarixi inkişafını, formal modellərini və müasir tətbiq sahələrini sistemli şəkildə təhlil edir.

FTN 2. Simmetrik və assimmetrik şifrələmə alqoritmlərinin (AES, RSA, ECC və s.) riyazi əsaslarını və işləmə mexanizmlərini elmi səviyyədə izah edir və müqayisə edir.

FTN 3. Kriptoqrafik açarların idarəedilməsi, açar mübadiləsi protokolları (Diffie–Hellman, PKI və s.) və rəqəmsal imza texnologiyalarını tətbiq və analiz edir.

FTN 4. Kriptoqrafik sistemlərin dayanıqlığını, hücuma qarşı müqavimətini və performans göstəricilərini qiymətləndirir, zəiflikləri müəyyən edir və təkmilləşdirmə təklifləri hazırlayır.

FTN 5. Real informasiya sistemlərində kriptoqrafik müdafiə strategiyalarını layihələndirir, hüquqi və etik çərçivələr kontekstində təhlükəsizlik siyasətləri formalaşdırır.

3. Kibertəhlükəsizliyin menecmenti sistemləri

FTN 1. Kibertəhlükəsizliyin idarəetmə sistemlərinin konseptual əsaslarını, standartlarını (ISO/IEC 27001, NIST, COBIT və s.) və onların təşkilati tətbiq mexanizmlərini sistemli şəkildə təhlil edir.

FTN 2. Kiberrisklərin identifikasiyası, qiymətləndirilməsi və prioritetləşdirilməsi proseslərini elmi əsaslarla həyata keçirir və risk idarəetmə planı hazırlayır.

FTN 3. Təşkilat daxilində kibertəhlükəsizlik siyasətlərinin, prosedurlarının və nəzarət mexanizmlərinin hazırlanması və tətbiqi üzrə kompleks yanaşma formalaşdırır.

FTN 4. Kibertəhlükəsizlik insidentlərinin idarə olunması, bərpa planlarının (Business Continuity, Disaster Recovery) və monitorinq mexanizmlərinin layihələndirilməsində iştirak edir.

FTN 5. Kibertəhlükəsizliyin menecmenti sistemlərinin effektivliyini audit, uyğunluq və performans göstəriciləri əsasında qiymətləndirir və təkmilləşdirmə strategiyaları irəli sürür.

4. Kompüter şəbəkələrinin təhlükəsizliyi

FTN 1. Kompüter şəbəkələrinin arxitekturasını, təhlükəsizlik təhdidlərini və müdafiə mexanizmlərini sistemli şəkildə analiz edir, təhlükəsizlik prinsiplərini (məlumatın məxfiliyi, bütövlüyü, əlçatanlığı) tətbiq edir.

FTN 2. Şəbəkə təhlükəsizliyinin texnoloji komponentlərini — firewall, VPN, IDS/IPS, proxy-serverlər, VLAN və s. — elmi əsaslarla qiymətləndirir və layihələndirir.

FTN 3. Şifrələmə protokollarını (SSL/TLS, IPsec, SSH və s.), autentifikasiya və identifikasiya mexanizmlərini tətbiq və optimallaşdırır.

FTN 4. Şəbəkə hücum növlərini (DoS/DDoS, spoofing, sniffing, man-in-the-middle və s.) təhlil edir, aşkarlama və qarşısını alma üsullarını modelləşdirir.

FTN 5. Təşkilat səviyyəsində şəbəkə təhlükəsizliyinin idarə olunması, monitorinqi və insidentlərə cavab mexanizmləri üzrə strategiyalar hazırlayır və qiymətləndirir.

5. İnformasiya təhlükəsizliyi və etik hakinq

FTN 1. İnformasiya təhlükəsizliyinin nəzəri və hüquqi əsaslarını, etik hakinq anlayışını və onun kibertəhlükəsizlik ekosistemində rolunu sistemli şəkildə izah edir.

FTN 2. Etik və qeyri-etik haker fəaliyyətləri arasında fərqləri təhlil edir, beynəlxalq standartlar (ISO 27001, NIST, EC-Council Code of Ethics və s.) çərçivəsində etik davranış prinsiplərini tətbiq edir.

FTN 3. Müxtəlif hücum metodlarını (penetration testing, social engineering, web application testing, wireless security testing və s.) planlaşdırır, həyata keçirir və nəticələrini analiz edir.

FTN 4. Sistem və şəbəkə zəifliklərini müəyyən etmək üçün istifadə olunan alətləri (Nmap, Metasploit, Wireshark, Burp Suite və s.) elmi əsaslarla qiymətləndirir və praktik sınaqlarda tətbiq edir.

FTN 5. Aşkar edilən zəifliklər üzrə risk qiymətləndirməsi aparır, hesabat hazırlayır və etik qaydada bərpa strategiyaları təklif edir, təşkilat üçün təhlükəsizlik siyasətləri formalaşdırır.

6. Maşın öyrənməsi

FTN 1. Maşın öyrənməsinin nəzəri əsaslarını, alqoritmik yanaşmalarını (nəzarətli, nəzarətsiz, dərin öyrənmə və s.) və onların tətbiq sahələrini sistemli şəkildə izah edir və təhlil edir.

FTN 2. Məlumatların hazırlanması, təmizlənməsi və xüsusiyyətlərin (features) seçilməsi proseslərini həyata keçirir, modellərin keyfiyyətinə təsirini qiymətləndirir.

FTN 3. Ənənəvi və müasir maşın öyrənmə alqoritmlərini (Linear/Logistic Regression, SVM, Decision Trees, Neural Networks və s.) proqramlaşdırma vasitəsilə (Python, R və s.) tətbiq və müqayisə edir.

FTN 4. Model performansını qiymətləndirmək üçün statistik və hesablama metodlarından (cross-validation, confusion matrix, ROC-AUC və s.) istifadə edir və nəticələri elmi əsaslarla şərh edir.

FTN 5. Real problemlər üçün maşın öyrənmə əsaslı həllər layihələndirir, etik, hüquqi və sosial aspektləri nəzərə alaraq nəticələrin interpretasiyasını aparır və tövsiyələr irəli sürür.

7. Tədqiqat metodları

FTN 1. Tədqiqat problemini və suallarını formalaşdırır, hipotez(ləri) qurur və əsaslandırır.

FTN 2. Kəmiyyət, keyfiyyət və qarışıq dizaynları müqayisə edir, məqsədə uyğun dizaynı seçir və planlaşdırır.

FTN 3. Nümunə götürmə strategiyasını və ölçmə alətlərini hazırlayır, keçərlilik və etibarlılığı qiymətləndirir.

FTN 4. Məlumat toplama prosedurlarını (sorğu, müsahibə, müşahidə) tətbiq edir və protokollaşdırır.

FTN 5. Etik tələbləri (razılıq, məxfilik, risklərin azaldılması) şərh edir və tədqiqat planına inteqrasiya edir.

8. Akademik yazı və etika

FTN 1. Tədqiqat mövzusu üzrə ədəbiyyatı axtarır, seçir və tənqidi icmal edir.

FTN 2. IMRaD strukturu üzrə akademik mətn (giriş–metod–nəticə–müzakirə) yazır və redaktə edir.

FTN 3. Sitat və istinad qaydalarını (məs., APA/MLA) düzgün tətbiq edir; istinad siyahısını formatlaşdırır.

FTN 4. Plagiat risklərini aşkarlayır və qarşısını alır (sitat, parafraz, istinad tətbiq edir).

FTN 5. Akademik və peşə etikası dilemmlərini təhlil edir, əsaslandırılmış mövqe və etik qərar formalaşdırır.

9. Tədqiqat analitikası

FTN 1. Məlumatları toplayır, təmizləyir və strukturlaşdırır; meta-məlumatı sənədləşdirir.

FTN 2. Təsviri statistikanı və ilkin araşdırma analizini (EDA) icra edir; cədvəl və qrafiklərlə vizuallaşdırır.

FTN 3. Hipotez testlərini (məs., t-test, χ^2), korrelyasiya və sadə reqressiyanı seçir, tətbiq edir və şərh edir.

FTN 4. Analiz nəticələrini təfsir edir, etibar intervalı və təsir ölçüsü ilə qiymətləndirir, məhdudiyyətləri göstərir.

FTN 5. Tapıntıları auditoriyaya uyğun hesabat və təqdimat şəklində hazırlayır, analitik prosesin təkrarlanmasını təmin edir.

Əlavə 2

Təhsil proqramı və tədris fəaliyyətlərinin təlim nəticələrinin matrisi

Ali təhsil müəssisəsi aşağıdakı cədvəldən istifadə edərək ixtisaslaşmanın təhsil proqramının təlim nəticələrinin əldə olunmasına necə dəstək verdiyini müəyyənləşdirməlidir.

Kibertəhlükəsizlik

Tədris fəaliyyətinin (fənnin) adı	Proqramın təlim nəticələri						
	PTN 1	PTN 2	PTN 3	PTN 4	PTN 5	PTN 6	PTN 7
Tədqiqat metodları	X						
Akademik yazı və etika	X						
Tədqiqat analitikası	X						
Kibertəhlükəsizliyin əsaslar		X					
Kriptoqrafiyanın əsasları			X				
Kibertəhlükəsizliyin menecmenti sistemləri				X			X
Kompüter şəbəkələrinin təhlükəsizliyi						X	
İnformasiya təhlükəsizliyi və etik hakinq					X		
Maşın öyrənməsi							X

Elmi-pedaqoji təcrübə							**X**
Elmi tədqiqat təcrübəsi	**X**						**X**
Magistrlik dissertasiyası	**X**						**X**

Razılaşdırıldı:

Tədris şöbəsinin müdiri

_____f-r.ü.f.d. .A.Ağamalıyeva

Beynalxalq Magistratura və Doktrantura mərkəzinin direktoru

_____t.ü.f.d.,dos N.Y. Quliyeva

Riyaziyyat və İnformatika kafedrasının müdiri

_____ r.ü.f.d., dos. R.O. Məstəliyev