AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ

Azərbaycan Respublikasının
Təhsil Nazirliyinin
F-963 nömrəli 25.07.22 -ci il
tarixli qərarı ilə təsdiq edilmişdir.

ƏSLİNDƏN DÜZDÜR

# BAKALAVRİAT SƏVİYYƏSİNİN (ƏSAS (BAZA) ALİ TİBB TƏHSİLİNİN) İXTİSAS ÜZRƏ

# TƏHSİL PROQRAMI

İxtisasın (proqramın) şifri və adı: 050615 - "İnformasiya təhlükəsizliyi"

BAKI – 2022

## 1. Ümumi müddəalar

1.1. Bakalavriat səviyyəsinin **050615 - "İnformasiya təhlükəsizliyi"** ixtisası üzrə Təhsil Proqramı (bundan sonra ixtisas üzrə Təhsil Proqramı) "Təhsil haqqında" Azərbaycan Respublikasının Qanununa, Azərbaycan Respublikasının Nazirlər Kabinetinin müvafiq qərarlarına, eləcə də "Ali təhsilin bakalavriat (əsas (baza ali) tibb təhsili) səviyyəsi üzrə ixtisasların (proqramların) Təsnifatı"na uyğun hazırlanmışdır.

1.2. Təhsil Proqramının məqsədləri aşağıdakılardır:

- İxtisas üzrə məzunun kompetensiyalarını, ixtisasın çərçivəsini, fənlər üzrə təlim və öyrənmə metodlarını, qiymətləndirmə üsullarını, təlim nəticələrini, kadr hazırlığı aparmaq üçün infrastruktura və kadr potensialına olan tələbləri, tələbənin təcrübə keçmə, işə düzəlmə və təhsilini artırma imkanlarını müəyyənləşdirmək;
- Tələbələri və işəgötürənləri məzunların əldə etdiyi bilik və bacarıqlar, eləcə də təlim nəticələri barədə məlumatlandırmaq;
- Təhsil Proqramı üzrə kadr hazırlığının bu proqrama uyğunluğunun qiymətləndirilməsi zamanı bu prosesə cəlb olunan ekspertləri məlumatlandırmaq.

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

1.4. Tələbənin 5 (beş) günlük iş rejimində həftəlik auditoriya və auditoriyadankənar ümumi yükünün həcmi 45 saatdır (xüsusi təyinatlı ali təhsil müəssisələri istisna olmaqla). Həftəlik auditoriya saatlarının həcmi ümumi həftəlik yükün 50%-dən çox olmamalıdır. İxtisasın xüsusiyyətindən asılı olaraq həftəlik yükün həcmi dəyişdirilə bilər.

## 2. Məzunun kompetensiyaları

2.1. Təhsil Proqramının sonunda məzun aşağıdakı ümumi kompetensiyalara yiyələnməlidir:

- İxtisası üzrə Azərbaycan dilində şifahi və yazılı kommunikasiya bacarıqlarına;
- İxtisası üzrə ən azı bir xarici dildə kommunikasiya bacarıqlarına;
- Azərbaycan dövlətçiliyinin tarixi, hüquqi, siyasi, mədəni, ideoloji əsasları və müasir dünyadakı yeri və roluna dair sistemli və hərtərəfli biliklərə, milli dövlətimizin perspektiv inkişafını proqnozlaşdırma qabiliyyətlərinə;
- Dövlətin qarşılaşdığı təhdidləri və çağırışları müəyyən etmə bacarıqlarına;
- Kibergigiyena vərdişlərinə;
- Problemlərin həllinə yaradıcı yanaşma və müstəqil araşdırma bacarıqlarına;
- Məsələlərin həlli üçün əlavə məlumat resurslarını müəyyən etmək və seçə bilmək qabiliyyətinə;
- Peşəkar məqsədlər üçün müvafiq məlumatı təhlil etmək, ümumiləşdirmək və tətbiq etmək bacarıqlarına;
- Kritik və analitik düşünmə, müstəqil öyrənmə və qərar qəbuletmə bacarığına;
- Komandada iş, problemin həllinə ortaq yanaşmaya nail olmaq qabiliyyətinə;
- Yeni şəraitə uyğunlaşmaq, təşəbbüs irəli sürmək qabiliyyətinə və uğur qazanmaq iradəsinə;
- Peşəkar fəaliyyətini planlaşdırmaq və təşkil etmək, gələcək təhsilini və mövcud bacarıqlarını təkmilləşdirilmək, vaxtı idarə etmək və tapşırıqları vaxtında tamamlamaq qabiliyyətinə;
- Fəaliyyətində sosial və ekoloji məsuliyyətə, eləcə də vətəndaş şüuru və etik yanaşmaya, həmçinin keyfiyyətə üstünlük vermək bacarığına;

- Bilik və bacarıqlarını inkişaf etdirmək məqsədilə vəziyyəti və özünü yenidən qiymətləndirmək və özünütənqid bacarığına;

2.2. Təhsil Proqramının sonunda məzun aşağıdakı peşə kompetensiyalarına yiyələnməlidir:

2.2.1. *Kompetensiya modulu A:* ***İnformasiya sistemlərinin preventiv mühafizəsi***

| Bacarıqlar | Biliklər |
|---|---|
| Kibertəhdidlərin və kibertəhdidlərlə bağlı yeniliklərin fasiləsiz monitorinqi | Risk kataloqları, istehsalçıların, forumların, texniki komitələrin və s. təhlükəsizlik hesabatları kimi məlumat mənbələri |
| Kibertəhdidlərin analizi və hesabatların hazırlanması | Strateji, taktiki, əməliyyat və texniki konsepsiya, həmçinin Kibertəhdid Kəşfiyyatı (ing. CTI) səviyyələri |
| İnformasiya təhlükəsizliyinə təhdidlərin obyekti hesab olunan aktivlərin – mühafizə predmetlərinin, onlara tələblərin müəyyən edilməsi | İnformasiya təhlükəsizliyinə təhdidlərin obyekti hesab olunan aktivlər – mühafizə predmetləri;<br>İnformasiya təhlükəsizliyinə bu aktivlərlə əlaqədar tələblər;<br>İnformasiya təhlükəsizliyinin göstəriciləri, "KPİ" və məqbul hədd anlayışları. |
| Təhlükəsizlik boşluqlarının/zəifliklərin müəyyən edilməsi | Audit və audit növləri (risklərin qiymətləndirilməsi, zəifliklərin qiymətləndirilməsi, nüfuzetmə sınaqları və uyğunluq auditləri).<br>Nüfuzetmə (müdaxilə) sınaqları (testləri), boşluqların/zəifliklərin aşkarlanması və uyğunluqların yoxlanılması üçün prosedurlar və alətlər;<br>Müdaxilə göstəriciləri (IOC)/hücum göstəriciləri (IOA).<br>Proaktiv təhdid axtarışı.<br>Kibercinayətlər barədə ümumi hüquqi müddəalar. |
| Boşluqların/zəifliklərin aradan qaldırılması | İnformasiya təhlükəsizliyi siyasətinə əsaslanan normalar;<br>Verilənlərin mühafizəsi üçün sistemə xas olan texniki və təşkilati tədbirlər, eləcə də təhlükəsizlik həlləri və qabaqcıl təcrübələr;<br>Sistemlərin mühafizəsinin gücləndirilməsi üsulları və vasitələri (nüfuzetmə sınaqları, informasiya təhlükəsizliyi auditi);<br>Proqram təminatlarının təhlükəsizlik sınaqlarının keçirilməsi üsulları və vasitələri. |
| Taktiki metodların tətbiqi | Kiberhücumlar və kibercinayətlərlə mübarizə üçün taktiki üsullar və alətlər (məsələn, aşkaredici və qabaqlayıcı üsul və vasitələr). |
| İnformasiya təhlükəsizliyinin ölçülməsi | İnformasiya təhlükəsizliyini ölçmələr, ölçmə metrikaları, mühafizə səmərəliliyini dəyərləndirmə. |
| Maraqlı tərəflərin texniki məsləhətlərlə təmin edilməsi | Sistemli həllə yönəlmiş məsləhət prinsipləri;<br>Kommunikasiya modelləri və qaydaları. |

| | |
|---|---|
| Maraqlı tərəflərə təlimlərin keçirilməsi | Metodoloji-didaktik prinsiplər;<br>Təlimlərin planlaşdırılması və həyata keçirilməsi. |

2.2.2. *Kompetensiya modulu B:* ***İnformasiya təhlükəsizliyi insidentlərinin aşkarlanması***

| Bacarıqlar | Biliklər |
|---|---|
| Sistemlərin monitorinqi | Şəbəkələrin, proqramların server xidmətlərinin, saxlanc həllərinin, cihazların və periferiya qurğularının monitorinqi üçün prosedurlar və alətlər;<br>Hücumların aşkarlanması üçün şəbəkə ekranları (təhlükəsizlik divarı (səddi)) (həmçinin Yeni Nəsil Təhlükəsizlik Divarı (səddi)), müdaxilə aşkarlama sistemləri (IDS), müdaxilə qabaqlama sistemləri (IPS) və ya veb tətbiqlər üçün təhlükəsizlik divarı (səddi) kimi texniki həllər və qurğular;<br>Təhlükəsizlik məlumatları və hadisələrinin idarə edilməsi (SIEM) sistemi. |
| Verilənlərin təhlili və şərhi | Loqların müxtəlif üsullarla təhlili;<br>Yanlış pozitivlərin (false positive) aşkarlanması;<br>Verilənlərin təhlili üçün "skript" dillərindən (Bash, Python, Awk, Perl və s.) istifadə;<br>Verilənlərin təhlili metodları;<br>İnformasiyanın icmalının təqdimat üsulları. |
| Təhlükəsizlik insidentlərinin prioritetləşdirilməsi | Daxili təlimatlar və proseslər.<br>İnsidentlərin təsnifatı və prioritetləşdirilməsi;<br>İnsidentlərin araşdırmaya yönləndirilməsi. |
| Təhlükəsizlik insidentlərinin sənədləşdirilməsi | İnsidentlərin həyat dövrü ərzində idarə edilməsi üçün tapşırıqların izlənilməsi sistemləri;<br>İnsident və ya sorğulara aid informasiyanın tərkib elementləri. |
| Təhlükəsizlik insidentlərinin idarə edilməsinə nəzarət | Əməliyyat Səviyyəsi Müqaviləsi və ya Xidmət Səviyyəsi Müqaviləsinə (ƏSM, XSM) uyğun olaraq insidentlərin idarə edilməsi;<br>ƏSM və XSM-ə uyğun olaraq eskalasiya səviyyələri. |

2.2.3. *Kompetensiya modulu C:* ***İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi***

| Bacarıqlar | Biliklər |
|---|---|
| Təcili (operativ) tədbirlərin görülməsi | İnsidentə cavab planında göstərilən tələblər;<br>Sistemlərin və ya xidmətlərin təcrid olunması, deaktiv edilməsi və ya söndürülməsi/dayandırılması kimi təcili texniki tədbirlər. |
| Sübutların identifikasiyası, toplanılması, sənədləşdirilməsi, saxlanılması, istifadə | Rəqəmsal kriminalistika siyasəti və prinsipləri;<br>Hüquqi aktlara və tənzimedici sənədlərə uyğunluq;<br>Sübutların identifikasiyası, toplanılması, sənədləşdirilməsi, saxlanılması, istifadə olunması, mühafizəsi və təqdim olunması üsulları. |

| | |
|---|---|
| olunması, mühafizəsi və təqdim olunması | |
| Səbəb və nəticələrin təhlili | Hücumların və insidentlərin təhlili;<br>Zərərli proqramların statik və dinamik təhlili;<br>Sistem, şəbəkə və yaddaşın ekspertizası;<br>Səbəblərin köklü, sistemli və strukturlaşdırılmış təhlili üçün istifadə olunan metod və üsullar. |
| Mühafizə tədbirlərinin təşkil olunması | Texniki və təşkilati tədbirlər;<br>Maraqlı tərəflərlə effektiv ünsiyyət bacarıqları və üsulları. |
| Sistemin bərpasının dəstəklənməsi | Fəaliyyət davamlılığının idarə edilməsi;<br>Fövqəladə hallarda bərpa tədbirləri |

2.2.4. *Kompetensiya modulu D:* ***İnformasiya təhlükəsizliyi*** **həllərinin planlaşdırılması və tətbiqi**

| Bacarıqlar | Biliklər |
|---|---|
| Sistem sərhədlərinin təyin edilməsi və tələblərin müəyyənləşdirilməsi | Sistemlərin, altsistemlərin və sistem sərhədlərinin modelləşdirilməsi;<br>İnterfeyslərin təsviri;<br>"S.M.A.R.T." (ing. Specific, Measurable, Achievable, Relevant, and Time-Bound) hədəflərin müəyyən olunması |
| Mümkünlüyün və effektivliyin yoxlanılması | Mümkünlüyün qiymətləndirilməsi üsulları (məsələn: konsepsiyanın isbatı, mümkünlüyün əsaslandırılması, modelləşdirmə, pilot layihələr). |
| İş yükünün və xərclərin qiymətləndirilməsi | Xərclərin qiymətləndirilməsi üsulları;<br>Xərclər planı və xərclərin hesablanması;<br>Maliyyə nəzarəti və hesabatlılığın təmini |
| Dəyərləndirmələrin həyata keçirilməsi | Dəyərləndirmə/qiymətləndirmə meyarlarının hazırlanması;<br>Tələblər və performans göstəriciləri/xüsusiyyətləri;<br>Həll variantlarının müqayisə olunması;<br>Effektiv danışıqların aparılması və satınalma proseslərinə dəstək. |
| Alt-layihələrin həyata keçirilməsi | Layihələrin və alt-layihələrin planlaşdırılması;<br>Risklərin idarə edilməsi və kommunikasiyav<br>Keyfiyyətə nəzarət;<br>Layihənin idarə edilməsi və hesabatlılıq. |
| Komandanın idarə edilməsi | Xüsusi kontekstlərə və vəziyyətlərə uyğunlaşdırılmış liderlik davranışı;<br>Kommunikasiya modelləri və qaydaları;<br>Komanda quruculuğu və motivasiya;<br>Komandada münaqişələrin idarə edilməsi |

## 3. Təhsil Proqramının strukturu

3.1. Təhsil Proqramı 240 (4 il) AKTS kreditindən ibarət olmalıdır.

| Fənlərin sayı | Fənnin adı | AKTS krediti |
|---|---|---|
| | **Ümumi fənlər** | |
| 1 | **Azərbaycan tarixi**<br>*Bu fənn Azərbaycanın müasir dövlətçilik ənənələrinin yaranması, formalaşması və inkişafını sistemli şəkildə, xronoloji ardıcıllıqla öyrənir, müasir Azərbaycan dövlətçiliyinin formalaşmasında siyasi, ideoloji, iqtisadi, mədəni amillərin rolunu təhlil və tədqiq edilir. Müasir dünyada Azərbaycan dövlətinin yeri və rolu sistemli təhlil edilir.* | 5 |
| 2 | **Azərbaycan dilində işgüzar və akademik kommunikasiya**<br>*Bu fənn cərçivəsində tələbələrə Azərbaycan dilində təqdimat etmək, natiqlik, akademik və işgüzar yazı, eləcə də tədqiqat bacarıqlarının aşılanmasına xüsusi diqqət yetirilməlidir.* | 4 |
| 3 | **Xarici dildə işgüzar və akademik kommunikasiya**<br>*Bu fənn çərçivəsində tələbələrə ixtisası üzrə xarici dillərdən birində təqdimat etmək, natiqlik, akademik və işgüzar yazı, şifahi və yazılı kommunikasiya, eləcə də akademik araşdırma bacarıqlarının aşılanmasına xüsusi diqqət yetirilməlidir.* | 15 |
| 4 | **Seçmə fənlər** *(Seçmə fənlər ali təhsil müəssisəsi tərəfindən müəyyən edilir. İxtisasın spesifikasından asılı olaraq seçmə fənlərə əlavələr edilə bilər. Tələbə hər biri 3 kredit olmaqla iki fənn seçməlidir.)* | 6 |
| | Psixologiya | 3 |
| | Sosiologiya | |
| | Hüququn əsasları | |
| | Mühəndis etikası | |
| | Kritik düşünmə | |
| | Sahibkarlığın əsasları və biznesə giriş | |
| | Təhsil və karyera planlaması | |
| | **Cəmi** | **30** |

| İxtisas fənləri | | |
|---|---|---|
| 5 | **İnformasiya təhlükəsizliyinin əsasları** *(Basics of information security)*<br>*Bu fənn ilk növbədə tələbəni informasiya təhlükəsizliyi ixtisası ilə tanış edir. Kursda informasiya təhlükəsizliyinin predmeti, əhatə sahəsi, əsas prinsipləri və anlayışları, məqsədləri öyrədilir. İnformasiya təhlükəsizliyi mütəxəssisinin bilməli olduğu bilik və bacarıqlar, digər fənlər və ixtisaslarla əlaqələri öyrədilir. Mühazirələr tələbələr üçün informasiya təhlükəsizliyinin əhatə etdiyi sahələri aydın təsvir etməyə, təcrübə məşğələləri isə əldə olunmuş biliklərin əmək fəaliyyətində istifadə imkanlarını göstərərək informasiya təhlükəsizliyi mütəxəssisinə xas olan düşüncəni formalaşdırır.* | 6 |
| 6 | **Proqramlaşdırmanın əsasları** *(Basics of programming)*<br>*Bu fənn çərçivəsində tələbələr hər hansı bir proqramlaşdırma dilində sərbəst şəkildə proqramların tərtib olunması, data strukturları və onlara aid məşhur alqoritmlərin yerinə yetirilməsi, alqoritmlərin çalışma müddəti və istifadə etdiyi yaddaşın analizi öyrədilir. Həmçinin kodların versiyalarının idarəedilməsi, müasir proqramlaşdırma mühitlərindən biri (məsələn, IntelliJ, Visual Studio və s.), onun köməyi ilə proqramdakı xətaların tapılması, kodun test olunması üçün vərdişlər formalaşdırılır. Proqramların test olunması üçün müvafiq test ssenarilərinin yazılması da bu fənnin mövzularındandır. Yekunda əldə olunan biliklərdən müxtəlif quruluşlu məlumatlar üzərində təhlillər aparmaq, müəyyən tapşırıqların avtomatlaşdırılması kimi praktiki biliklərə yiyələnirlər.* | 6 |
| 7 | **Riyazi analiz** *(Calculus)*<br>*Riyazi analiz fənninin əsasını bir və çoxdəyişənli funksiyaların diferensial və inteqral hesabı və sıralar nəzəriyyəsi təşkil edir. Tələbələr bu fənni mənimsəyərkən ədədi ardıcıllıqlar haqqında zəruri biliyə malik olmalı, bir və çoxdəyişənli funksiyaların limit, kəsilməzlik və müntəzəm kəsilməzlik anlayışlarına, diferensial və inteqral hesabına, ədədi və funksional sıralara, habelə tətbiqi riyaziyyat, informatika və kriptologiya məsələlərində onların tətbiq olunmasının öyrənilməsinə diqqət yetirməlidir.* | 6 |
| 8 | **Kibertəhlükəsizliyin əsasları** *(Basics of cybersecurity)*<br>*Bu fənn çərçivəsində kibertəhlükəsizliyin konseptual modeli, rolu və əhəmiyyəti, eləcə də onun informasiya təhlükəsizliyindən fərqi, həmçinin qarşılıqlı əlaqələri öyrədilir. Müxtəlif kiberhücum vektorları və subyektləri, kibertəhlükəsizlik sahəsində yayılmış zəifliklər, təhdidlər və risklər, kiberhücum zəncirinin hər bir mərhələsinin xüsusiyyətləri və onlara qarşı zəruri tədbirlərin görülməsi yolları, kibertəhlükəsizliyin təmin olunması sahəsində texniki və təşkilati tədbirlərin rolu və xüsusiyyətləri tədris olunur.* | 6 |
| 9 | **Şəbəkələrin əsasları** *(Basics of networks)*<br>*Bu fənndə tələbələrə kompüter şəbəkələrin dizaynı və praktik tətbiqi öyrədilir. Kursda qabaqcıl şəbəkə avadanlıqları barədə məlumat verilir. Şəbəkənin OSI modeli və IP ünvanlaması, IPv4, IPv6 barədə əsas məlumatlar öyrədilir, LAN, WLAN, MAN və digər növ şəbəkə modelləri barədə ümumi məlumatlar verilir.* | 6 |

| | | |
|---|---|---|
| | *Həmçinin peyk əsaslı şəbəkələr də daxil olmaqla simsiz (radiodalğa əsaslı) şəbəkələr barədə təməl məlumatlar verilir.* | |
| 10 | **Xətti cəbr** *(Linear Algebra)*<br>*Bu fənn çərçivəsində matrislər və xətti cəbri tənliklər sisteminin ümumi nəzəriyyəsi, həmçinin xətti çevirmə, kvadratik forma və bu kimi vacib mövzular tədris olunur. Tələbə matrislər üzərində əməllər, determinantın hesablanması və xassələri, cəbri tənliklər sisteminin müxtəlif həll üsullarının öyrənilməsi, kvadratik formanın kanonik şəklə gətirilməsi və tətbiq sahəsini öyrənməklə bu fənn üzrə qarşıya qoyulan məqsədə çatmış hesab olunur.* | 6 |
| 11 | **Əməliyyat sistemləri** *(Operating systems)*<br>*Bu fənn əməliyyat sisteminin dizaynı və tətbiqi ilə bağlı mühüm problemləri araşdırır. Tədris dövründə müasir əməliyyat sistemlərinin təkamülünün qısa tarixinə nəzər salınaraq onların əsas komponentlərinin iş prinsipləri əhatə edilir. Fəndə əməliyyat sistemi resurslarının (disk, şəbəkə və prosessorlar) paylaşdırılması, proqramlar üçün lazım olan ümumi xidmətlərin təmin edilməsi və qorunması üçün işlənmiş prinsiplər icmal edilir. Fənn ƏS-də proses və yaddaşın idarə edilməsi, fayl sisteminin iş prinsipi və paylanmış sistemlərdəki iş prinsiplərini əhatə edir.* | 5 |
| 12 | **Şəbəkələrin təhlükəsizliyi** *(Network Security)*<br>*Bu fənn çərçivəsində şəbəkələrin təhlükəsizlik məsələləri anlaşılsın deyə şəbəkələr barədə daha dərin biliklər öyrədilir. Tələbələr burada RADİUS, TACACS+, Kerberos, SSO, LDAP və s. kimi anlayışları bilməli və fərqli şəbəkə avadanlıqları (IDS, IPS) barədə biliklər əldə etməlidir. Şəbəkələrin auditini və loqlaşdırmasını öyrənir. Şəbəkələrdə sniffinq mexanizmlərini, şəbəkələrdə təhlükəsizliyin təmin olunması üçün lazım olan sazlamalar barədə öyrənir. Şəbəkədə mövcud təhlükəsizlik protokollarının anlayır və istifadə edir. Yeni nəsil təhlükəsizlik divarları, eləcə də, SIEM, SOAR, UEBA barədə məlumatları öyrənir.* | 5 |
| 13 | **Diskret riyaziyyat** *(Discrete Mathematics)*<br>*Diskret riyaziyyat fənni riyazi və predikatlar məntiqinin, qraflar nəzəriyyəsinin, bul cəbrinin, kombinatorikanın elementlərini, obyektlər arası münasibətləri tədqiq edir, tələbələr xüsusilə düzgün riyazi anlayışların öyrənilməsinə, müxtəlif üsullarla isbatların tətbiqinə və diskret riyaziyyatın üsullarından istifadə etməklə optimal proqramların hazırlanmasına diqqət yetirməlidirlər. Qraflar nəzəriyyəsinin kiberkriminalistikada, şəbəkə təhlükəsizliyində tətbiqi praktik məşğələlərdə nəzərə alınmalıdır.* | 5 |
| 14 | **Veb təhlükəsizlik** *(Web security)*<br>*Bu fənn çərçivəsində tələbələr veb tətbiqlərin çalışması prinsiplərini, onların brauzer proqramları tərəfindən vizuallaşdırılması məntiqini, serverlə əlaqə prinsiplərini öyrənirlər. Daha sonra veb tətbiqlər və veb xidmətlərdəki* | 5 |

| | | |
|---|---|---|
| | *təhlükəsizlik boşluqlarının necə və haradan qaynaqalandığını, həmçinin o boşluqların/zəifliklərin necə aradan qaldırılmasına dair praktiki biliklərə yiyələnirlər. Bununla yanaşı, veb tətbiqlərdə təhlükəsizliyin təmin olunmasına dair qabaqcıl təcrübələr, geniş yayılmış boşluqlar/zəifliklər, həmçinin boşluqların/zəifliklərin istismarına dair üsul və vasitələr öyrədilir.* | |
| 15 | **Ehtimal nəzəriyyəsi** *(Probability Theory)*<br>*Ehtimal nəzəriyyəsi fənni kütləvi bircins hadisələrin ehtimal qanunauyğunluqlarının öyrənilməsini, elmi və praktik nəticələr almaq üçün statistik verilənlərin toplanması və emalı üsullarının yaradılmasını tədqiq edir, tələbələr xüsusilə ehtimalın təriflərinin tətbiqlərinə, təsadüfi kəmiyyətlərin ədədi xarakteristikalarının hesablanmasına, müxtəlif teoremlərin tətbiqilə məsələ həllinə diqqət yetirməlidirlər.* | 5 |
| 16 | **İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri**<br>*(Legal aspects of information security and cybersecurity)*<br>*Bu fənn çərçivəsində informasiya təhlükəsizliyi və kibertəhlükəsizlik sahəsində yaranan ictimai münasibətləri tənzimləyən hüquq normalarının tədrisi həyata keçirilir. Fənnin tədrisi zamanı informasiya hüququnun əsasları, informasiya təhlükəsizliyi və kibertəhlükəsizliklə bağlı normativ-hüquqi baza, informasiya sahəsində əsas insan hüquq və azadlıqlarının mühafizəsi mexanizmləri, eləcə də, fərdi məlumatların, habelə dövlət sirri təşkil edən və konfidensial informasiyanın mühafizəsinin hüquqi aspektləri, kibercinayətkarlığa qarşı mübarizənin hüquqi mexanizmləri, həmçinin informasiya müharibəsi/kibermüharibənin hüquqi aspektlərinin tədrisinə xüsusi diqqət yetirilməlidir.* | 5 |
| 17 | **İnformasiya təhlükəsizliyinin idarəedilməsi sistemləri** *(Information Security Management Systems)*<br>*Kurs çərçivəsində tələbələr İnformasiya Təhlükəsizliyinin İdarəedilməsi Sistemlərinin (İTİS) aktuallığı, əsasları, planlaşdırılması və təşkil edilməsi üçün zəruri bilikləri əldə edəcəklər. Bir təşkilatda fərqli idarəetmə sistemləri ilə İTİS-nin vəhdətini yaratmağa dair bacarıqlara yiyələnirlər. Bununla yanaşı, tələbə İTİS üzrə əsasən ISO 27001, eləcə də fəaliyyət sahələrinin xüsusiyyətinə uyğun olaraq digər beynəlxalq standartların (ITIL, COBIT) təşkilatda tətbiq olunmasının aktuallığını, rolunu, prinsiplərini və üsullarını öyrənəcəklər.* | 5 |
| 18 | **Verilənlər bazalarının təhlükəsizliyi** *(Database security)*<br>*Bu fənn çərçivəsində verilənlər bazalarına (VB) dair ilkin zəruri biliklərin verilməsi, daha sonra VB-nın layihələndirilməsi, qurulması və istismarı zamanı informasiya təhlükəsizliyinin təmin olunmasının əsas prinsipləri tədris olunur. Həmçinin VB-də mümkün təhlükəsizlik boşluqları/zəifliklərinin aşkarlanması, qarşısının alınması üsul və vasitələri tədris olunmaqla müvafiq kiberhücumlara qarşı mübarizə tədbirləri, VB-də təhlükəsizlik auditinin üsul* | 5 |

| | | |
|---|---|---|
| | *və vasitələri öyrədilir. Bununla yanaşı, bulud əsaslı və NoSQL tipli VB-lər barədə əsas məlumatlar və anlayışlar tədris olunur.* | |
| 19 | **Bulud təhlükəsizliyi** *(Cloud security)*<br>*Bu fənndə bulud texnologiyalarının nə olduğu, onların faydaları, ənənəvi xidmətlərdən fərqləri öyrədilir. Tələbələr bulud xidmətlərində təhlükəsizlik modelləri, riskləri araşdırmağı, onların qarşısının alınmasını, təhlükəsizliyə fərqli bucaqlardan yanaşmanı, təhlükəsizlik strategiyasının qurulması üçün lazımi bilik və bacarıqlara yiyələnirlər.* | 5 |
| 20 | **Kriptoqrafiyanın əsasları** *(Basics of cryptography)*<br>*Bu kurs çərçivəsində tələbələr ənənəvi kritoqrafiyanın yaranması və inkişafına dair qısa tarixi, aktuallığını, tətbiq sahələrini və mövcud problemlərini, həmçinin müasir kriptosistemlər və şifrləmə üsulları ilə birlikdə kriptoqrafiyanın informasiya təhlükəsizliyinin hansı prinsiplərini necə təmin etdiyini öyrənirlər. Kursda blok, axın və açıq açarlı şifrləmə alqoritmaları ilə yanaşı qabaqcıl kriptoqrafik alqoritmlər icmal edilir, bu alqoritmlərin praktiki tətbiqləri ilə əlaqəli məlumatlar verilir.* | 5 |
| 21 | **Nüfuzetmə sınaqlarının əsasları** *(Penetration testing)*<br>*Bu fənn tələbələrə nüfuzetmə sınaqlarının üsul və vasitələrini, onun planlaşdırılması, hazırlanması və icra mərhələlərini öyrədir. Tələbələr laboratoriya şəraitində sistemlərdə boşluqların/zəifliklərin aşkar edilməsi məqsədilə şərti kiberhücumlar yerinə yetirməyi, sistemlərə fərqli yanaşmalarla baxmağı öyrənirlər. Tələbələrə informasiya sistemlərindən aktiv və (və ya) passiv məlumat toplamaq üsulları öyrədilir, həmçinin tapılan boşluqlardan/zəifliklərdən istifadə edərək səlahiyyətləri yüksəltmək, təşkilata vurula biləcək mümkün ziyanın dərəcəsini ölçmək və əsas ələcə risk faktorlarını müəyyən etmək, onların qarşısının alınması, habelə nüfuzetmə sınağının nəticələri barədə hesabatların hazırlamağı öyrənirlər.* | 8 |
| 22 | **Elektronikanın əsasları və IoT təhlükəsizliyi** *(Basic of Electronics and IoT security)*<br>*Bu fənn elektronika, mikrokontrollerlər və onların köməyi ilə yaradılmış cihazlara, xüsusilə IoT (əşyaların interneti) və onların istifadə etdiyi fərqli simli və simsiz şəbəkələr, həmin şəbəkələrin təhlükəsizliyi mövzularında biliklər öyrədilir. IoT qurğuların istifadə etdiyi fiziki protokollar və əlaqə üsulları, həmçinin xəbərləşmə protokolları, onların güclü və zəif cəhətləri izah olunur. Bundan əlavə IoT qurğulara yönəlmiş informasiya təhlükəsizliyi məsələləri, onlara qarşı mümkün kiberhücumlar və kibermüdafiə üsullarına aydınlıq gətirilir.* | 5 |

| | | |
|---|---|---|
| 23 | **Təhlükəsiz proqramlaşdırma** *(Secure programming)*<br>*Bu fənn proqram təminatının ilkin kodlarından qaynaqlanan təhlükəsizlik boşluqları, onların təbiətini izah edir, bu boşluqların aradan qaldırılması üçün lazım olan bilikləri öyrədir. Kurs çərçivəsində tələbələrə proqram təminatının yardılmasından etibarən istismarınadək olan dövrdə kodların təhlükəsizlik tələblərinə uyğunlaşdırılması üsul və vasitələri öyrədiləcək. Tələbələr kurs zamanı zəruri laboratoriya mühitinin qurulmasının əsaslarını və bu mühitdə statik (SAST) və dinamik (DAST) kod analizinin necə aparılacağına dair təcrübələri öyrənəcəklər.* | 5 |
| 24 | **Rəqəmsal Kriminalistikanın əsasları** *(Digital Forensics fundamentals)*<br>*Bu fənn çərçivəsində təhlükəsizlik insidentlərinin araşdırılması, eləcə də, rəqəmsal kriminalistikanın həyata keçirilməsi, rəqəmsal sübutların identifikasiyası, toplanılması, sənədləşdirilməsi, saxlanılması, istifadə olunması, mühafizəsi və təqdim olunması sahəsində zəruri mövzuların tədrisi həyata keçirilir. Məhkəmə kompüter-texniki ekspertizasının/rəqəmsal kriminalistikanın anlayışı, növləri və prinsipləri, kriminalistik diaqnostika və tədqiqat prosesi, rəqəmsal kriminalistik taktika və texnika, rəqəmsal sübutların əldə olunması və təhlili üçün zəruri resurslar, eləcə də, rəqəmsal kriminalistikanın bəzi problemləri barədə biliklərin əldə edilməsi diqqətdə saxlanılmalıdır. Bununla yanaşı tələbələr təcrübədə açıq kodlu həllərin və eləcə də qabaqcıl istehsalçıların həllərini öyrənəcəklər.* | 8 |
| 25 | **Sənaye idarəetmə sistemlərinin təhlükəsizliyi** *(Security of industrial management systems)*<br>*Bu fənndə tələbələr kritik infrastrukturlar və onların əhəmiyyətini öyrənərək kritik infrastrukturlarda kibertəhlükəsizlik mövzuları ilə tanış olacaq. IT mühitində olmayan protokolları (modbus, DNP3, ICCP və s), texnologiyaları (SCADA, PLC, DCS, və s) və OT (Sənaye idarəetmə sistemlərinin) mühitinin təhlükəsizliyinin təmin olunması üsul və vasitələrini öyrənəcəklər.* | 5 |
| 26 | **Mülki müdafiə**<br>*Bu fənn çərçivəsində mülki müdafiənin əsasları, qüvvə və vasitələri, fövqəladə hallar və onların xarakteristikaları, fövqəladə hallarda əhalinin mühafizəsi, əhalinin mülki müdafiə üzrə maarifləndirilməsi, fövqəladə halların nəticələrinin aradan qaldırılması yolları haqqında məlumat verilməli, fərdi və kollektiv mühafizə vasitələrindən istifadə etmək, fövqəladə hallarda sənaye obyektlərinin işinin dayanıqlığının əsasları və qiymətləndirilməsinə dair məlumat verilməlidir.* | 3 |
| | Cəmi | 120 |
| **Ali təhsil müəssisəsi tərəfindən müəyyən edilən seçmə fənlər** | | |
| | Cəmi | 60 |
| **Təcrübə** | | |

| | |
|---|---|
| **Təcrübə** | 30 |
| **Cəmi** | 30 |
| **Kreditlərin yekun sayı** | **240** |

***Qeyd:*** *İxtisas fənlərinin ardıcıllıq sırası* ***Əlavə 1****-də tövsiyə edilmişdir. Ali təhsil müəssisəsi tərəfindən müəyyən ediləcək seçmə fənlərə dair tövsiyyələr* ***Əlavə 2****-də öz əksini tapmışdır.*

## 4. Tədris və öyrənmə

4.1. Tədris və öyrənmə mühiti elə təşkil olunmalıdır ki, tələbələr təhsil proqramında nəzərdə tutulan təlim nəticələrini əldə edə bilsinlər.

4.2. Tədris və öyrənmə metodları müvafiq sənədlərdə (məsələn, müəllimin sillabusunda və s.) təsvir edilməli və ictimaiyyətə (məsələn, universitetin veb səhifəsində, proqramın broşurlarında və s.) açıq olmalıdır.

4.3. Tədris və öyrənmə metodları innovativ təhsil təcrübələri nəzərə alınaraq davamlı şəkildə nəzərdən keçirilməli və təkmilləşdirilməlidir. Tədris və öyrənmə metodlarının müntəzəm şəkildə təkmilləşdirilməsi universitetin keyfiyyət təminatı sisteminin bir hissəsi olmalıdır.

4.4. Təlim prosesində fərqli tədris metodlarından istifadə edilməlidir. Bu metodlar tələbəyönümlü yanaşmanı və tələbələrin təlim prosesindəki fəal rol oynamasını təşviq etməlidir. İstifadə edilə biləcək tədris və öyrənmə üsullarına aşağıdakıları nümunə olaraq göstərmək olar:

- mühazirələr, seminarlar, təcrübi tapşırıqlar;
- təqdimatlar və müzakirələr, debatlar;
- müstəqil iş/araşdırma (məsələn, təcrübi nümunələrlə iş, təcrübi layihələrdə birbaşa iştirak);
- layihələr;
- problemlərə əsaslanan tədris;
- sahə işləri;
- rol oyunları;
- hesabatlar;
- qrup qiymətləndirməsi;
- ekspert metodu;
- video və audio konfrans texnologiyaları;
- video və audio mühazirələr;
- distant təhsil;
- simulyasiyalar;
- və s.

***Qeyd:*** *sadalanan metodlar ixtisasın xüsusiyyətindən asılı olaraq seçilə və (və ya) dəyişdirilə bilər.*

4.5. Təhsildə nəzəriyyə və praktiki təlim arasında tarazlıq gözlənilməlidir. Əsas diqqət əmək bazarının dəyişən ehtiyaclarına uyğun olaraq praktiki bacarıqların gücləndirilməsinə yetirilməlidir.

4.6. Təhsil proqramı tələbələrin müstəqilliyini dəstəkləməli və ömürboyu təlim konsepsiyasını inkişaf etdirməlidir. Təhsil prosesinin sonunda tələbə hər hansı istiqamətdə müstəqil işləyə bilməli və təhsilini ömürboyu davam etdirməyi bacarmalıdır.

## 5. Qiymətləndirmə

5.1. Qiymətləndirmə elə təşkil olunmalıdır ki, tələbələrin gözlənilən təlim nəticələrini, bacarıqları əldə etmələri səmərəli şəkildə ölçülə bilinsin. Bu, əldə olunan irəliləyişi monitorinq etməyə, təhsil proqramlarının nəticələrinə hansı dərəcədə nail olunduğunu qiymətləndirməyə, eləcə də tələbələrlə fikir mübadiləsinə şərait yaratmağa və təhsil proqramlarının təkmilləşdirilməsi üçün ilkin şərtlərin formalaşdırılmasına yardım etməlidir.

5.2. Qiymətləndirmə üsulları müvafiq sənədlərdə (məsələn, fənn proqramında, sillabusda və s.) təsvir edilməli və hamı üçün açıq olmalıdır (məsələn, universitetin veb səhifəsində, proqramın broşurlarında və s.). Fənni tədris edən müəllim fənn üzrə qiymətləndirmə üsullarını müəyyən etməlidir. Bunun üçün **Əlavə 3**-dəki cədvəldən istifadə edilməlidir.

5.3. Qiymətləndirmə üsulları innovativ tədris təcrübələri nəzərə alınaraq davamlı şəkildə nəzərdən keçirilməli və təkmilləşdirilməlidir. Qiymətləndirmə üsullarının müntəzəm şəkildə yenilənməsi ali təhsil müəssisəsinin keyfiyyət təminatı sisteminin bir hissəsi olmalıdır.

5.4. Tədris prosesində fərqli qiymətləndirmə üsullarından istifadə edilməlidir. Bu üsullar tələbəyönümlü yanaşmanı və tələbələrin təlim prosesindəki fəal rol oynamasını təşviq etməlidir. İstifadə edilə biləcək qiymətləndirmə üsullarına nümunələr:

- yazılı tapşırıqlar;
- bilik və bacarıqlara dair testlər, kompüter əsaslı testlər;
- şifahi təqdimatlar;
- sorğular;
- açıq müzakirələr;
- təcrübə hesabatları, sahə işləri hesabatları;
- təcrübədə, laboratoriyada müşahidələrə əsasən bacarıqların qiymətləndirilməsi;
- layihə işlərinə dair hesabatlar;
- portfolionun qiymətləndirilməsi;
- frontal sorğu;
- qrup şəklində və özünü qiymətləndirmə;
- və s.

***Qeyd:*** *sadalanan üsullar fənnin xüsusiyyətindən asılı olaraq seçilə və (və ya) dəyişdirilə bilər.*

5.5. Təlim nailiyyətlərinin qiymətləndirilməsində istifadə olunan üsullar aydın müəyyənləşdirilmiş meyarlara əsaslanmalıdır və təhsil müddətində tələbənin əldə etdiyi bilik, bacarıq və qabiliyyət səviyyəsini düzgün və etibarlı şəkildə müəyyən etməyə imkan verməlidir. Təlim nəticələrinin qiymətləndirilməsi zamanı müəllimlər şəffaflıq, qərəzsizlik, qarşılıqlı hörmət və humanistlik prinsiplərini rəhbər tutmalıdırlar.

5.6. Tələbələrə müəllimlərlə/qiymətləndiricilərlə təhsillərinin bütün aspektlərini, o cümlədən qiymətləndirmə prosesini müzakirə etmək imkanı verilməlidir. Ali təhsil müəssisəsi müvafiq qaydalara uyğun olaraq qiymətləndirmə prosesi, yaxud qiymətlə bağlı apelyasiya prosedurlarını müəyyən etməlidir.

5.7. Akademik etika təhsil prosesində önəmli yer tutur. Tələbələrə akademik dürüstlüyə riayət etmək, plagiatlıq problemini anlamaq öyrədilir. Onlar intellektual əməyin əqli mülkiyyət hüquqları barəsində məlumatlandırılmalıdırlar.

## 6. Proqramın və hər bir fənnin təlim nəticələri

6.1. Təhsil proqramının təlim nəticələri, eləcə də hər bir fənnin təlim nəticələrinin müəyyənləşdirilməsi və hər bir fənnin sillabusunun hazırlanması ali təhsil müəssisəsinin/akademik heyətin səlahiyyətindədir.

6.2. Təhsil proqramının Təlim nəticələri və fənlərin təlim nəticələri **Əlavə 4**-də əks olunmuşdur. Seçmə fənlərin təlim nəticələri ali məktəb tərəfindən müəyyənləşdirilir. Təlim nəticələri matrisində (**Əlavə 5**) fənlərlə təlim nəticələri arasındakı əlaqə əks olunmuşdur.

6.3. Təhsil Proqramının cəmiyyətin və əmək bazarının dəyişən ehtiyaclarına cavab verən nəzəri və praktiki məzmunu təmin etməsi məqsədilə cari təhsil proqramı və fənlərin sillabusları müntəzəm şəkildə yenilənməlidir.

## 7. İnfrastruktur və kadr potensialı

7.1. Təhsil Proqramının tədris, öyrənmə və qiymətləndirmə prosesi ali təhsil müəssisəsinin aşağıdakı infrastruktura malik olmasını zəruri edir:

- tədris planında nəzərdə tutulan fənlər üzrə dərslərin aparılması, praktiki və laboratoriya dərslərinin keçirilməsi üçün müvafiq proqram təminatı və internetə çıxışla təmin edilmiş kabinetlər, laboratoriyalar, kompüter sinifləri;
- müvafiq layihə və elmi-tədqiqat işlərinin yerinə yetirilməsi üçün tələbə və müəllimlərin müasir fiziki avadanlıqla və ya simulyatorlarla təchiz olunmuş maddi-texniki bazaya, o cümlədən müstəqil tədqiqat apara bilmələri üçün fərdi qurğularının ali təhsil müəssisəsinin lokal şəbəkəsinə, internetə, aidiyyəti informasiya bazalarına, elektron kitabxanalara, axtarış sistemlərinə çıxışı təmin edilməlidir.

7.2. Ali təhsil müəssisələrinin professor-müəllim heyəti, bir qayda olaraq, elmi dərəcəyə malik olur. O cümlədən dövlət, özəl müəssisələrdən və digər təşkilatlardan müvafiq təcrübəsi olan mütəxəssislər tədrisə cəlb oluna bilərlər.

## 8. Təcrübə

8.1. Təcrübə tələbənin nəzəri biliklərinin praktikada tətbiqi, eləcə də peşə bacarıqlarının gücləndirilməsi baxımından önəmlidir.

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

8.3. Təcrübədən öncə ali təhsil müəssisəsi və təcrübə təşkil olunacaq şirkət/müəssisə/laboratoriya arasında müqavilə imzalanmalıdır. Eyni zamanda, tələbənin fərdi müraciəti əsasında onun ixtisasına uyğun digər şirkət/müəssisə/laboratoriyada, o cümlədən xaricdə təcrübə keçməsinə icazə verilir. Müqavilədə şərtlər, tələbələrin hüquq və öhdəlikləri və digər zəruri təfərrüatlar əks olunur.

8.4. Təcrübə tələbənin təcrübə keçdiyi təşkilatda hazırladığı hesabat əsasında ali təhsil müəssisəsi tərəfindən qiymətləndirilir.

## 9. Kurs layihələri

9.1. Tələbələr hər il ali təhsil müəssisəsi tərəfindən müəyyən olunmuş bir fənn üzrə kurs layihəsi yerinə yetirirlər.

9.2. Bu kurs layihələri fərdi və ya qrup şəklində hazırlana bilər.

9.3. Kurs layihələri "İnformasiya Təhlükəsizliyi" sahəsinə aid praktiki əhəmiyyət kəsb edən mövzulara dair olmalıdır.

## 10. Məşğulluq və ömürboyu təhsil

10.1. "İnformasiya təhlükəsizliyi" ixtisası üzrə təhsil alan məzunlar dövlət və özəl sektorda informasiya təhlükəsizliyinin təmin olunması istiqamətində bir sıra peşələr üzrə çalışa bilərlər. **Əlavə 6**-də bu peşələrin və rolların bir qisminin adları nümunə (tövsiyə) kimi qeyd edilmişdir.

10.2. Ali təhsil müəssisəsi Təhsil Proqramının məzunlarının məşğulluğuna dair müntəzəm sorğular keçirməli, vakant iş yerlərinə dair məlumatları öz veb səhifəsində yerləşdirməli və əmək yarmarkaları təşkil etməlidir.

10.3. Ali təhsil müəssisəsi tələbələrin məşğulluq səviyyəsini artırmaq məqsədilə ustad dərsləri və/və ya seminarları keçmək üçün əmək bazarının nümayəndələrini dəvət edə bilər.

10.4. Bu Təhsil Proqramının məzunları təhsillərini aşağıdakı ixtisaslar üzrə magistratura səviyyəsində davam etdirə bilərlər:

- 060509 - Kompüter elmləri
- 060631 - Kompüter mühəndisliyi
- 060632 - İnformasiya texnologiyaları və sistemləri mühəndisliyi
- və digər müvafiq ixtisaslar üzrə

10.5. Təhsil müddətində əldə olunan bilik, bacarıq və yanaşmalar məzunların müstəqil şəkildə ömürboyu təhsil almaları üçün ilkin şərtlərdəndir.

Əlavə 1

## İxtisas fənlərinin tədrisi ardıcıllığı

| Fənlərin adı | Kreditlərin sayı |
|---|---|
| **1 tədris ili 1-ci semestr** | |
| Riyazi analiz | 6 |
| İnformasiya təhlükəsizliyinin əsasları | 6 |
| Proqramlaşdırmanın əsasları | 6 |
| **1-ci tədris ili 2-ci semestr** | |
| Xətti cəbr | 6 |
| Şəbəkələrin əsasları | 6 |
| Kibertəhlükəsizliyin əsasları | 6 |
| **2-ci tədris ili 1-ci semestr** | |
| Diskret riyaziyyat | 5 |
| Əməliyyat sistemləri | 5 |
| Şəbəkələrin təhlükəsizliyi | 5 |
| **2-ci tədris ili 2-ci semestr** | |
| Web təhlükəsizlik | 5 |
| İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi əsasları | 5 |
| Ehtimal nəzəriyyəsi | 5 |
| **3-cü tədris ili 1-ci semestr** | |
| İnformasiya təhlükəsizliyinin idarəedilməsi sistemləri | 5 |
| Verilənlər Bazalarının təhlükəsizliyi | 5 |
| Bulud təhlükəsizliyi | 5 |
| Mülki müdafiə | 3 |
| **3-cü tədris ili 2-ci semestr** | |
| Kriptoqrafiyanın əsasları | 5 |
| Nüfuzetmə sınaqlarının əsasları | 8 |
| Elektronika və IoT cihazların təhlükəsizliyi | 5 |
| **4-cü tədris ili 1-ci semestr** | |
| Təhlükəsiz proqramlaşdırma | 5 |
| Rəqəmsal kriminalistikanın əsasları | 8 |
| Sənaye idarəetmə sistemlərinin təhlükəsizliyi | 5 |

Əlavə 2

## Tövsiyə olunan seçmə fənlər

1. Təhlükəsizlik avadanlıqları
2. Data-mərkəzi əməliyyatlarının əsasları
3. Korporativ şəbəkə (informasiya) sistemlərinin təhlükəsizliyi
4. Zərərverici proqram vasitələrinin təhlili (Malware analysis)
5. Maşın öyrənməsi
6. Rəqəmsal təsvir və video emalın əsasları (Fundamentals of digital image and video processing)
7. Tətbiqi statistika və data analitikası
8. Paralel və paylanmış hesablamalar
9. Qraflar nəzəriyyəsi
10. Mobil və simsiz avadanlıqların təhlükəsizliyi
11. VoIP sistemlərinin təhlükəsizliyi
12. Blokçeyn texnologiyaları
13. Ədədi üsullar
14. Rəqəmsal transformasiya
15. Sistem proqramlaşdırması
16. Data mədənçiliyi
17. Sistem dizaynı
18. Proqram təminatı üzrə layihə menecmenti
19. Proqram mühəndisliyi
20. C proqramlaşdırma dili
21. Mobil qurğular üçün proqramlaşdırma
22. Veb proqramlaşdırma
23. Mobil qurğularda təhqiqatlar
24. Alqoritmlərin qurulması və analizi
25. Bulud texnologiyaları
26. Sosial şəbəkə analizi
27. Sosial mühəndislik

Əlavə 3

Fənnin təlim nəticələrinə nail olmaq məqsədilə istifadə olunan
təlim və öyrənmə metodları və qiymətləndirmə üsulları

| Fənnin adı | Təlim nəticələri | Hər bir təlim nəticəsi üçün istifadə olunan təlim və öyrənmə metodları | Hər bir təlim nəticəsi üçün istifadə olunan qiymətləndirmə üsulları |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Əlavə 4

## Təhsil Proqramı və fənlər üzrə təlim nəticələri

Ali təhsil müəssisəsi Təhsil Proqramı və hər fənn üzrə gözlənilən təlim nəticələrini müəyyən etməlidir.

| Təhsil Proqramının təlim nəticələri (PTN) |
| --- |
| PTN 1 - Azərbaycanın müasir dövlətçilik ənənələrinin yaranması, formalaşması və inkişafını bilməlidir, müasir Azərbaycan dövlətçiliyinin formalaşmasında siyasi və ideoloji, iqtisadi və texnoloji, elmi və mədəni amillərin rolunu təhlil və tədqiq etməyi bacarmalıdır. Müasir dünyada Azərbaycan dövlətinin yeri və rolunu sistemli təhlil etməyi bacarmalıdır<br><br>Azərbaycanın kibernetika, tətbiqi riyaziyyat, informasiya və kommunikasiya texnologiyaları sahələrində inkişaf tarixinə, bu sahələrdə elm, təhsil və sənaye ənənələrinə və potensialına, dünya səviyyəli mütəxəssislərinin peşə fəaliyyətinə aid məlumatlı olmalıdır.<br><br>Azərbaycan dilində təqdimat etmək, natiqlik, akademik və işgüzar yazı bacarıqlarına yiyələnməlidir.<br><br>Xarici dillərdən birində təqdimat etmək, natiqlik, akademik və işgüzar yazı, şifahi və yazılı ünsiyyət bacarıqlarına malik olmalıdır.<br><br>"İnformasiya təhlükəsizliyi" ixtisasının məqsədi və vəzifələrini, digər ixtisas sahələri ilə qarşılıqlı əlaqəsini, dövlət və özəl sektordakı tələbatın vacibliyini, gələcək perspektivlərini bilməlidir.<br><br>Mühəndislik etikasının vacibliyi, bu ixtisasla əlaqədar öyrənilən biliklərin yalnız qanunvericilik və etik normalar çərçivəsində, peşə səlahiyyətlərinə uyğun tətbiq olunmasının vacibliyini bilmlidir. |
| PTN 2 - Ədədi və yığılan ardıcıllıqlar, funksiyanın limiti və kəsilməzliyi, funksiyanın törəməsi, birdəyişənli funksiyanın ekstremumları, qeyri-müəyyən inteqral, müəyyən inteqral, ədədi və qüvvət sıraları, çoxdəyişənli funksiyanın limiti, xüsusi törəmələri və diferensialı haqqında biliklərə malik olmalıdır.<br><br>Matris anlayışı, matrislər üzərində əməllər və matrisin transponirə edilməsi, iki və üçtərtibli determinantların hesablanması, iki matrisin hasilinin determinantı. Tərs matris və onun varlığı, n-ölçülü vektorlar fəzası, vektorların xətti asılılığı, matrisin rankı, xətti cəbri tənliklər sistemi, çoxhədlilər və onlar üzərində əməllər, Çoxhədlinin kökü, Hörner sxemi, kvadratik formalar haqqında biliklərə malik olmalıdır.<br><br>Məntiq cəbrinin elementar funksiyaları, onların xassələri, onlar üzərində əməliyyatlar, ikili funksiya, ikilik prinsipi, qraf anlayışı, qrafın həndəsi ifadəsi, əlaqəli, alt, tam, izomorf və homomorf qraflar, istiqamətlənmiş, istiqamətlənməmiş və qarışıq qraf, hamar və bircins qraf, kodlaşdırma, dekodlaşdırma, qarşılıqlı birqiymətli dekodlaşdırma, əlifba və müntəzəm kodlaşdırması, kodun seçilməsi, maneələr mənbəyi, birqiymətli dekodlaşdırma meyarı haqqında biliklərə malik olmalıdır.<br><br>Ehtimal nəzəriyyəsinin predmeti, klassik ehtimal. Kombinatorikanın elementləri, Kolmoqorov aksiomları. Ehtimalın xassələri. Həndəsi ehtimal, entropiya və informasiya miqdarı. Bernulli sxemi, ehtimal paylanması, diskret paylanma, təsadüfi kəmiyyətin ədədi xarakteristikaları, riyazi gözləmə, |

dispersiya, Markov və Çebışev bərabərsizliyi, asimmetriya əmsalı, kovariyasiya və korrelyasiya əmsalı, böyük ədədlər qanunu haqqında biliklərə malik olmalıdır.

PTN 3 - İnformasiya sistemlərinin preventiv mühafizəsi, informasiya təhlükəsizliyi risklərini minimallaşdırma, təhdidlərin və zəifliklərin aşkarlanması, fəsadların qabaqlanması üçün bilik və bacarıqlara yiyələnməlidir.

İnformasiya təhlükəsizliyinin əhatə sahəsini (*"scope"*) müəyyən etmə, informasiya aktivlərinin və informasiya proseslərində istifadə olunan aktivlərin, onlara aid funksionallığın uçotunu aparmağı, İnformasiya təhlükəsizliyinin idarəetmə siyasətini və riskləri, insidentləri, İKT-xidmətləri və İKT-layihələri idarəetmə alt-siyasətlərini müəyyən etməyi bacarmalıdır.

Mühafizə olunan, o cümlədən mühafizə aləti olan aktivlərə informasiya təhlükəsizliyi üzrə tələbləri, informasiya təhlükəsizliyini ölçmə göstəricilərini (metrikaları) müəyyənetmə bacarıqlarına yiyələnməlidir.

Təhdidlərdən törənə bilən insidentləri (informasiya təhlükəsizliyinə) və fəsadları (fəaliyyət davamlılığına), onların ciddilik dərəcələrini müəyyənetməyi bilməlidir.

Kiber kəşfiyyat (*"cyber-intelligence"*), o cümlədən təhdidləri, onlara aid cəhdləri və hazırlıqları və onlara aid qabaqlayıcı əks-tətbirləri müəyyənetmə bacarıqlarına yiyələnməlidir.

Kriptoqrafiya xidmətləri göstərmə (tövsiyə xarakterli), informasiya təhlükəsizliyini idarəetmənin auditi və dəyərləndirmə, İnformasiya təhlükəsizliyini idarəetmə siyasətinə uyğun local (korporativ) normativ hüquqi aktların layihələrini, təlimatları, praktiki icra kitabçalarını (*"playbook"*ları) hazırlamağa bacarmalıdır.

PTN 4 - İnformasiya təhlükəsizliyi insidentlərinin aşkarlanması üçün insident menecmentin, o cümlədən fasiləsiz monitorinqlərin, mütəmadi auditlərin, ekspertizaların və digər nəzarət mexanizmlərinin təşkili üçün bilik və bacarıqlara yiyələnməlidir.

İnformasiya təhlükəsizliyi üzrə struktur vahidinə – Təhlükəsizliyin monitorinq əməliyyatları mərkəzinə (*"SOC, Security Operation Centre"*) aid proseslərin icrasını təmin etməyi bacarmalıdır.

Mühafizə olunan aktivlərdə informasiya təhlükəsizliyi hadisələrini müəyyənetmə və qiymətləndirməni, informasiya təhlükəsizliyi insidentini aşkaretmə, insidentlərin ciddilik dərəcələrini, fəsadların növlərini və dərəcələrini müəyyənetmə üsullarını bilməlidir.

Kiber-tədqiqat/kriminalistika və sübutları/dəlilləri toplama (*"cyber-forensics"* & *"collection of evidence/findings"*), onların təhlükəsizliyi tələblərini təminetmə barədə məlumatlı olmalıdır.

| |
|---|
| PTN 5 - İnformasiya təhlükəsizliyi insidentlərinə cavabvermə məqsədilə zəifliklərin aradan qaldırılması üçün mühafizə olunan aktivlərdə konfiqurasiyaların və dəyişikliklərin idarə olunmasına aid bilik və bacarıqlara yiyələnməlidir.<br><br>İnformasiya təhlükəsizliyi insidentlərinə əks-cavab üçün uyğun olan variantı (bloklama, bərpaetmə, dəyişiklik aparma, yeniləmə, təkmilləşdirmə, ehtiyat varianta keçmə, əvvəlki vəziyyətə geri qaytarma) seçmə və müvafiq *"playbook"*ları formalaşdırma, tətbiqetmə və ya böhran halarında kənardan dəstək üçün müraciət etmə üsullarını bilməlidir.<br><br>İnformasiyanı mühafizə vasitələri olan proqram-texniki servislərinə (*"control"larına*) inzibatçılıq etmə barədə məlumatlı olmaldır. |
| PTN 6 - İnformasiya təhlükəsizliyi həllərinin planlaşdırılmasına və tətbiq edilməsinə, bu həllərin İKT vasitələrinin təməlindən təyin olunmuş mükəmməllik və etimadlılıq səviyyələrinə uyğun layihələndirilməsinə, inkişafına, işlənib hazırlanmasına və tətbiq edilməsinə, bu sahədə layihə menecmentinə aid bilik və bacarıqlara yiyələnməlidir.<br><br>İnformasiya təhlükəsizliyinin əhatə sahəsində mühafizə olunan, o cümlədən mühafizə aləti olan İKT məhsuluna (o cümlədən proqram təminat vasitələrinə, elektronika, elektrotexnika, telekommunikasiya və digər texniki təminat vasitələrinə) tələbatı (*"request for proposal, RFP"*) müəyyəetmə və sənədləşdirməni bacaramalıdır.<br><br>İKT məhsulunun təyinat yerinin texniki tələblər toplusuna, aidiyyəti standartlara uyğunluğunun analizini (məsələn *"GAP analisis"* metodu ilə) apara bılməlidir.<br><br>İKT məhsulunun yaradılmasına yanaşma (*"Waterfall"* – kaskadlı yanaşma / *"Agile"* – iterativ yanaşma və s.) metodlarından xəbərdar olmalıdır, müvafiq yanaşma üçünuyğun metodologiyanı (*"Scrum"*, *"Lean"*, *"XP"*) seçmək üçün lazımi biliklərə yiyələnməlidir.<br><br>İKT məhsuluna texniki tələbləri (*"statement of requirements, SOR"*) və texniki tapşırıqları/ şərtləri (*"terms of reference, TOR"*) müəyyəetmə və sənədləşdirmə, İKT məhsulunun verifikasiya testlərini təminetmə, o cümlədən texniki tələblərin və texniki tapşırıların/ şərtlərin həyata keçirildiyini yoxlama və sənədləşdirmə mexanizmlərini bilməlidir. |

| **"Azərbaycan tarixi" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - Azərbaycanın müasir dövlətçilik ənənələrinin yaranması, formalaşması və inkişafını bilir. |
| FTN 2 - Azərbaycan dövlətçiliyi qədim və orta əsrlər dövründə və XV-XVIII əsrlərdə Azərbaycan xalqı tərəfindən Şərqdə böyük imperiyaların yaradılması haqqında bilikləri nümayiş etdirir. |
| FTN 3 - Müasir Azərbaycan dövlətçiliyinin formalaşmasında siyasi, ideoloji, iqtisadi, mədəni amillərin rolunu təhlil və tədqiq etməyi bacarır. |
| FTN 4 - XIX əsrin ilk onilliklərində Azərbaycan dövlətçiliyinin itirilməsi və onun siyasi, iqtisadi, sosial nəticələri, Azərbaycanda milli dövlətçilik uğrunda mübarizə, Azərbaycan xalq cümhuriyyətinin yaradılması-birinci respublika dövrü, ikinci Respublika, Azərbaycan dövlətçiliyi Sovet imperiyası dövründə, XX əsrin 80-ci illərin ikinci yarısında müstəqillik uğrunda mübarizənin başlanması və müstəqil dövlətçiliyin bərpasına dair biliklərə yiyələnib |
| FTN 5 - Müasir dünyada Azərbaycan dövlətinin yeri və rolunu sistemli təhlil etməyi bacarır. |

| |
|---|
| FTN 6 - Müasir dövlətçiliyin qorunması üçün təhlükəsiz beynəlxalq şəraitin yaradılması, dövlətimizin ərazi bütövlüyünün bərpası uğrunda mübarizə, Azərbaycanın Qafqazda lider dövlətə çevrilməsi haqqında biliklərə yiyələnib. |

| **"Azərbaycan dilində işgüzar və akademik kommunikasiya" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - Azərbaycan dilinin tarixi, onun inkişafı və zənginləşdirilməsi yollarını bilir. |
| FTN 2 - Tarixin müəyyən dövrlərində dilimizin düşmən qüvvələrinin təzyiqinə, təcavüzünə məruz qalmasını, lakin xalqımızın milli birliyi, milli qüruru sayəsində onun qorunmasına müvəffəq olmasını və bu işdə görkəmli sərkərdələrin, dövlət xadimlərinin xidmətlərini bilir. |
| FTN 3 - Azərbaycan dilində ixtisas üzrə elmi məlumatları təhlil edir, şifahi və yazılı təqdimatlar hazırlayır. |
| FTN 4 - Azərbaycan dilində akademik və işgüzar natiqlik bacarığını nümayiş etdirir. |
| FTN 5 - Azərbaycan dilinin özünəməxsusluğunu qorumağı, tərcümə vasitəsilə başqa xalqların mədəni irsi ilə tanış olmağı, onlarla ünsiyyət qurmağı bacarır. |
| FTN 6 - Azərbaycan dilinin təmizliyi uğrunda mübarizə aparmağı, dili yad ünsürlərdən qorumağı, onu yaşatmağı bacarır. |

| **"Xarici dildə işgüzar və akademik kommunikasiya" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - İxtisası üzrə xarici dillərdən birində oxuduğu elmi məqaləni təhlil edir, onların xülasəsini hazırlaya bilir. |
| FTN 2 - Xarici dilin qrammatik, leksik, semantik strukturlarını analiz etməyi bacarır. |
| FTN 3 - Beynəlxalq arenaya çıxaraq öz xalqının milli-mənəvi dəyərlərini, qazandığı nailiyyətləri başqalarına çatdırmağı bacarır. |
| FTN 4 - Xarici dildə fikir və təcrübə mübadiləsini aparır, işgüzar kommunikasiya yaradır. |
| FTN 5 - Xarici dildə texniki ədəbiyyatdan yararlana bilir, xarici həmkarlar üçün texniki sənədləşmələri, təqdimatları hazırlaya bilir. |
| FTN 6 - Xarici dil bacarığına malik olmaqla, komandada işləmək, şəxslərarası ünsiyyət səriştəliyini formalaşdırır. |

| **"Psixologiya" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - Psixologiyanın predmeti və metodları, psixologiyanın elmlər sistemində yeri və onun əsas sahələri, psixoloji fikrin əsas inkişaf istiqamətləri haqqında biliklər əldə etmək. |
| FTN 2 - İnsan psixikasının quru-luşu, davranışın tənzimində şüurun və şüursuzluğun rolu, davranış və fəaliyyətin motivasiyası və psixi tənzimi haqqında təsəvvürə malik olmaq. |
| FTN 3 - Psixologiya elminin əsas kateqoriya və anlayışları, psixi olanın idraki, emosional-iradi, motivasyon sahələri, şəxsiyyət, şəx-siy-yətin inkişafı və formalaşması xüsusiyyətləri, təfəkkür, ünsiyyət və fəaliyyət, temperament, xarakter və qabiliyyətlər, təhsil və özünüinkişaf problemi haqında biliklərə malik olmaq. |
| FTN 4 - Peşəkar və problemli təlim situasiyalarının təhlilini aparmağı, profes-sio-nal ünsiyyəti və qarşılıqlı təsiri, fərdi və birgə qərar qəbulunu, refleksiyanı təşkil etməyi bacarmaq. |
| FTN 5 - İnsanların şəxsi və fərdi-psixoloji xüsusiy-yət-lə-rinin, eləcə də onların idraki və professional fəaliyyət üslubunun diaqnos-tika-sını aparmağı bacar-maq. |
| FTN 6 - Əldə edilmiş bilikləri istər təhsildə pedaqoji sahədə, sənaye və ticarət sahəsində, istərsə də hüquqazidd davranışla mübarizə və s. sahələrdə müxtəlif psixoloji xarakterli praktik problemlərin həllində və qərarların qəbul edilməsində tətbiq etmək. |

| "Sosiologiya" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Sosial və peşə problemlərinin həllində sosial, humanitar və iqtisadi elmlərin əsas prinsip və metodlarından istifadə etməyi bacarmaq. Sosial sahənin və idarəetmənin inkişafında qlobal, milli və regional xüsusiyyətləri və müasir şəraiti nəzərə almaq. |
| FTN 2 - Sosial həyatdakı problemlərə münasibətdə müstəqil düşünmə və tənqidi təhlil bacarıqlarını formalaşdırmaq. |
| FTN 3 - Cəmiyyətin istənilən sferasında yaranan problemlərin üzə çıxarılması və onların daha adekvat həlli yollarının axtarılması səriştəsinə yiyələnmək. |
| FTN 4 - Sosioloji tədqiqatların həyata keçirilməsi və nəticələrinin təhlil edilməsi texnikasına yiyələnmək. |
| FTN 5 - Müxtəlif sosial qrupların sosial həyatı, rifahı və sosial sahədə davranış xüsusiyyətlərini bilmək. Milli-mədəni məkanın xüsusiyyətlərini və müxtəlif milli, cins, yaş qruplarının və sosial qurumların fəaliyyətlərini sosial layihə obyekti kimi tətbiq etməyi bacarmaq. |
| FTN 6 - Sosioloji biliklərin əsaslarını peşə və peşə fəaliyyətlərində və müxtəlif sosial hadisələrin təhlilində yaradıcı şəkildə tətbiq etmək. |

| "Hüququn əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Hüququn anlayışı, mahiyyəti, funksiyaları, əlamətləri, mənbələri, eləcə də hüquq sisteminin konstitusiya əsasları barədə ümumi biliklər əldə etməlidir. |
| FTN 2 - Hüququn fəaliyyətinin əsas qanunauyğunluqlarının, onun dövlətlə və digər sosial institutlarla qarşılıqlı əlaqələrinin, həmçinin suveren Azərbaycan Respublikasında əsas inkişaf tendensiyalarının dərki vərdişlərini inkişaf etdirməlidir. |
| FTN 3 - Azərbaycan Respublikasının konstitusiya quruluşu, insan və vətəndaşın konstitusion hüquqi statusu, əsas hüquqları, azadlıqları və vəzifələrini öyrənməlidir. |
| FTN 4 - Hüququn ictimai münasibətlərin effektiv huquqi nizam-layı-cısı kimi sosial dəyərinin dərkinə, hüquq pozuntuları ilə müba-ri-zə-yə, ölkə vətəndaşlarının hüquq və azadlıqlarının mühafizəsinə yönə-lik hüquq düşüncəsini formalaşdırılmalı,tələbələrin Qanunun aliliyinin ciddi şəkildə gözlənilməsi əsasında professional vəzifələrinin icrasına yönləndirilməsi. |
| FTN 5 - Hüquq normasının və normativ-hüquqi aktların anlayışı və əlamətlərini bilməli, Azərbaycan Respublikası qanunvericiliyinin timsalında hüquq normalarının təsnifatı və növlərini öyrənməli, Azərbaycan Respublikası Konstitusiyasına görə normativ hüquqi aktların sistemi barədə biliklər əldə etməlidir. |
| FTN 6 - Hüquqauyğun davranışın, hüquq pozuntusunun və hüquq məsuliyyətinin anlayışı və əsas cəhətlərini bilməli, hüquq məsuliyyətinin növləri, hüquq məsuliyyətinə cəlb etmə, habelə hüquq məsuliyyətindən azad etmə əsasları barədə zəruri biliklərə yiyələnməlidir. |

| "Mühəndis etikası" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Etik və qeyri-etik vəziyyətləri ayırd edə bilmək və dilemma şəraitində əxlaqi mühakimə irəli sürməyi bacarır. |
| FTN 2 - İctimaiyyətin təhlükəsizliyini, sağlamlığını və rifahını hər şeydən üstün tutmağı anlayır. |
| FTN 3 - Yalnız öz səlahiyyətləri üzrə xidmətlər göstərməyin vacibliyini bilir. |
| FTN 4 - İşəgötürən və ya müştəri üçün sadiq nümayəndə kimi davranmağı başa düşür. |
| FTN 5 - Peşənin şərəfini, nüfuzunu və faydalılığını artırmaq üçün özlərini şərəfli, məsuliyyətli, etik və qanuni şəkildə aparmağı bilir. Peşə xidməti zamanı yalnız qanuni və etibarlı mənbələrdən istifadə etməli olduğunu bilir. |

| |
|---|
| FTN 6 - Sosial təcrübələrdə və məlumat toplanması zamanı etika və şərəf kodeksini rəhbər tutmağın vacibliyini bilir. |

| "Kritik düşünmə" fənn üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Mümkün olan seçimlərdən ən optimalını seçmə bacarığı əldə edilir. |
| FTN 2 - Problemin həllinə sistemli və davamlı yanaşmağı öyrədir. |
| FTN 3 - Digərlərinin fikirlərinə dözümlü olmağı və onlara öz fikrini bildirməyə imkan verməyi öyrədir. |
| FTN 4 - Düşünceli, vaxtında və məlumatlı mühakimə yürütməyə çalışmaq vərdişi qazandırır. |
| FTN 5 - Fakta söyklənəcək düşüncə ilə əldə edilən nəticələrə etibar etməyi və nəticələri proqnozlaşdırmaq məqsədi ilə problemlərə yanaşma bacarığını formalaşdırır. |
| FTN 6 - Məsələnin və ya problemin təhlilindən məntiqi nəticə çıxarmaq bacarıq və üsullarını öyrədir. |

| "Sahibkarlığın əsasları və biznesə giriş" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Sahibkarlığın əsas iqtisadi–hüquqi institutlarını, biznes–planlaşdırmanın əsas aspektlərini və sahibkarlıq niyyətinin işlənilməsini, sosial-iqtisadi alətlərin sahibkarlıqda fəal surətdə istifadə olunmasını bilmək. |
| FTN 2 - Biznes planın hazırlanması, müəssisənin qurulması, biznesdə tərəfdaşlıq əlaqələrinin qurulması, optimal təşkilatı strukturunun və biznesin xüsusiyyətlərinə uyğun infranstrukturun müəyyənləşdirilməsini bacarmaq. Biznesin effektiv idarəedilməsi üçün zəruri olan əsas anlayışlar və alətləri bilmək. |
| FTN 3 - Müəssisənin strukturunda yer alan əsas və köməkçi funksiyaların iş prinsipləri ilə bağlı məsələləri bilmək. İdarəetmə metod və növlərini öyrənmək və onun funksiyalarının effektiv icrasını həyata keçirə bilmək. |
| FTN 4 - İstehsal, istehsal prosesi, istehsal sistemləri, müasir istehsalın xüsusiyyətləri və idarə edilməsinə bələd olmaq, biznesin subyektlərinin fasiləsiz işləmələri üçün zəruri xammal-material və yarımfabrikatların planlaşdırılmasını bacarmaq. |
| FTN 5 - Mühit amillərinin müəssisənin fəaliyyəti üzərindəki təsirlərini müəyyənləşdirə bilmək və bu təsirlərə adekvat cavab verə bilmək. |
| FTN 6 - Biznes proseslərini analiz etmək, qiymətləndirmək və idarə etmək. |

| "Təhsil və karyera planlaması" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Karyera inkişafı prosesini təsvir edə bilmək və hazıda olduğu mərhələni anlamağa kömək edir. |
| FTN 2 - Demoqrafik, iqtisadi və təşkilati dəyişikliklərin iş dünyasına və onların şəxsi karyera inkişafı qərarlarına təsirini izah edir. |
| FTN 3 - Müxtəlif müasir qiymətləndirmə vasitələrindən və əks etdirmə fəaliyyətlərindən istifadə edərək, öz şəxsi prioritetlərini, bacarıqlarını, maraqlarını, güclü tərəflərini və dəyərlərini müəyyən etməyi öyrədir. |
| FTN 4 - Təşkilatlar, peşələr və sənayelər haqqında məlumat almış olur. |
| FTN 5 - Özünü əmək bazarına doğru və dürüst qaydada təqdim edə biləcək CV, təqdimat və xasiyyətnamə məktubu yazma bacarığını öyrədir. |
| FTN 6 - Perspektivli təcrübə və iş yerləri üçün müsahibələrə hazırlayır. |

| "İnformasiya təhlükəsizliyinin əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - İnformasiya təhlükəsizliyi sahəsində vacib anlayışları, həmçinin sənədlərdə və ya işgüzar müzakirələr zamanı istifadə olunan terminologiyanı bilməlidir. İnformasiya təhlükəsizliyi sahəsində ümumi və xüsusi tələblərin əsaslarını, həmçinin onların formalaşma xüsusiyyətlərini bilməlidir. |
| FTN 2 - İnformasiya təhlükəsizliyinin konseptual modelini bilməli, informasiya təhlükəsizliyinin təmin olunması məqsədilə müvafiq tələblərin formalaşdırılması üçün sadə düşüncəyə sahib olmalıdır. |
| FTN 3 - İnformasiya təhlükəsizliyi sahəsində rəhbər hüquqi aktları, onun tələblərini və tətbiqi qaydalarını bilməli, həmçinin belə aktların inkişafını izləməyi bacarmalıdır. İnformasiya təhlükəsizliyi sahəsində qlobal, regional və milli normaları, standartları və qabaqcıl təcrübələri bilməli, onların inkişafını izləməyi bacarmalı və tətbiqinə dair fikirlərə sahib olmalıdır. |
| FTN 4 - İnformasiya təhlükəsizliyinin təmin olunmasında təşkilati forma və metodları bilməlidir. İnformasiya təhlükəsizliyinin təmin olunması üçün əsas prinsipləri bilməli, həmçinin texniki üsul və vasitələri öyrənməlidir. |
| FTN 5 - İnformasiya təhlükəsizliyi sahəsində riskləri, onların xüsusiyyətlərini, həmçinin idarə olunmasına dair ümumi biliklərə sahib olmalıdır. İnformasiya təhlükəsizliyi siyasətinin aktuallığı, formalaşma xüsusiyyətləri və tətbiqinə dair ümumi biliklərə sahib olmalı, həmçinin təmin olunması üsullarını bilməlidir. İnformasiya təhlükəsizliyi üzrə auditin əsasları, xüsusiyyətləri, aktuallığı, həmçinin prosedur qaydalarına dair ümumi biliklərə sahib olmalıdır. |
| FTN 6 - İnformasiyanı mühafizə vasitələrinin hüquqi, təşkilati və texniki əsasları, tətbiq sahələri, həmçinin bu vasitələrin yaradılması və qaydalara uyğun şəkildə sertifikatlaşdırılmasına dair ümumi biliklərə sahib olmalıdır. İnformasiyanı mühafizə vasitələrinə verilmiş xarici sertifikatların tanınması qaydalarını bilməlidir. |

| "Proqramlaşdırmanın əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Hər hansı bir proqramlaşdırma dilində sərbəst olaraq proqram yazmağı bacarır, proqramlaşdırmada şərt, dövr, funksiya, obyekt, sinif anlayışlarını bilir. Verilənlərin tiplərini, onların yaddaşda necə yerləşdiyini anlayır. Kompilyasiya prosesi, baytkod, maşın kodunun nə olduğunu anlayır. |
| FTN 2 - Massiv, Əlaqəli siyahılar (LinkedList), stek, növbə, qraf, ağac kimi data strukturlarını, həmin data strukturları üzərində klassik alqoritmləri bilir, sadalanan data strukturları və alqoritmləri hər hansı bir proqramlaşdırma dilində yerinə yetirməyi bacarır. |
| FTN 3 - Alqoritmlərin çalışma müddətini və istifadə etdiyi yaddaşı analiz edə bilir. Sistemin imkanları və məhdudiyyətlərini nəzərə alaraq hansı alqoritmin tətbiq edilməsinə dair doğru qərarları verməyi bacarır. |
| FTN 4 - Proqramların peşəkar şəkildə yazılması üçün istifadə olunan mühitlərdən biri ilə tanışdır, o mühitdə proqramın kompilyasiya olunması, "debug" prosesi, proqram kodlarının versiyalarının idarəolunmasını (məsələn, "git" sistemi ilə) bacarır. |
| FTN 5 - Proqram modullarının test olunması üsullarını bilir, test ssenarilərinin yazılmasını bacarır. Proqramların oxunaqlığı və keyfiyyət meyarları barədə məlumatlı olmalıdır. |
| FTN 6 - Öyrənilən biliklərdən istifadə edərək, fərqli fayl formatları arasında çeviricilər, müxtəlif parserlər, loqların təhlili üçün proqramların tərtib edilməsini, fərqli sistemlərin interfeyslərini istifadə etməklə məlumatların hasilatini bacarmalıdır. |

| "Riyazi Analiz" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Ardıcıllığın limitinin tərifini,yığılan və dağılan ardıcıllıqlar anlayışlarını, limitin bəzi xassələrini bilməlidir. |
| FTN 2 - Funksiyanın limiti, nöqtədə kəsilməz funksiyanın tərifi, əsas xassələri, kəsilmə nöqtələri haqqında biliklərə malik olmalıdır. |
| FTN 3 - Funksiyanın törəməsinin tərifi, əsas xassələri, nöqtədə differensialın tərifi və onunla bağlı hökmlər haqqında biliklərə malik olmalıdır. Funksiyanın maksimum və minimum nöqtələrinin tərifi, ekstremum üçün zəruri şərt, birinci və ikinci kafi şərtlər haqqında biliklərə yiyələnməlidir. |
| FTN 4 - Parçanın bölgüsü, onun xassələri, müəyyən inteqralın tərifi, inteqrallanan funksiyalar sinifləri haqqında məlumata malik olmalıdır. |
| FTN 5 - Ədədi sıranın tərifini, zəruri şərt və yığılan sıranın xassələrini bilməlidir. Qüvvət sıralarının yığılma radiusu və yığılma intervalı, Koşi-Adamar düsturu, Teylor sırası haqqında məlumatlara yiyələnməlidir. |
| FTN 6 - Çoxdəyişənli funksiyanın xüsusi törəmələri və diferensialı haqqında biliklərə yiyələnməlidir. |

| "Kibertəhlükəsizliyin əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Kibertəhlükəsizlik üzrə əsas konsepsiya və anlayışları bilməlidir. |
| FTN 2 - Kibertəhlükəsizliyi idarə etməyin əhəmiyyətini başa düşülməlidir. Kibertəhlükəsizliyin təmin olunmasında təşkilati forma və metodları bilməlidir. |
| FTN 3 - Kibertəhlükəsizliyinin təmin olunması üçün əsas prinsipləri bilməli, həmçinin texniki üsul və vasitələri öyrənməlidir. Habelə zəifliklər, boşluqlar, təhdidlər və risklər barədə bilməli, onların xüsusiyyətlərini, həmçinin idarə olunmasına dair ümumi biliklərə sahib olmalıdır. |
| FTN 4 - Müdafiə və hücumyönümlü kibertəhlükəsizlik sahəsində zəruri vasitələrin funksiyalarını bilməlidir. |
| FTN 5 - Təhlükəsizliyi idarə etmə alətlərini ("control"ları, üsul və vasitələri) tətbiq etməklə təhlükəsizlik siyasətlərini həyata keçirməyi bacarmalıdır. Kibertəhlükəsizlik siyasətinin aktuallığı, formalaşma xüsusiyyətləri və tətbiqinə dair ümumi biliklərə sahib olmalı, həmçinin təmin olunması üsullarını bilməlidir. |
| FTN 6 - Kibertəhlükəsizlik sahəsində qlobal, regional və milli normaları, standartları və qabaqcıl təcrübələri bilməli, onların inkişafını izləməyi bacarmalıdır. |

| "Şəbəkələrin əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Kompüter şəbəkələri haqqında ilkin anlayışları bilməlidir. |
| FTN 2 - Şəbəkə ötürücüləri, onların xüsusiyyətləri, məhdudiyyətlərini, əsas şəbəkə avadanlıqlarını, onların funksiyalarını bilməlidir. |
| FTN 3 - Şəbəkə topologiyalarını tanımalıdır, şəbəkə arxitekturalarını, dizayn və protokollarını başa düşməlidir. |
| FTN 4 - OSİ səviyyələrini tanımalıdır, IP ünvanalamanın iş prinsipini, alt-şəbəkələrin necə çalışdığını, IP ünvanların paylanmasını və siniflərini bilməlidir. |
| FTN 5 - Şəbəkədə marşurutlaşmanı və fərqli OSİ səviyyələri üçün müvafiq şəbəkə avadanlıqlarını quraşdırmağı, sazlamanı yerinə yetirməyi bacarmalıdır. |
| FTN 6 - Şəbəkədə təhlükəsizliyin və etibarlılığın təmin olunması ilə bağlı anlayışları bilməlidir. |

| "Xətti Cəbr" fənni üzrə təlim nəticələri (FTN) |
|---|

| |
|---|
| FTN 1 - Matrisin ümumi tərifini, müxtəlif növlərini, matrislər üzərində bütün əməlləri, bu əməllərin əsas xassələrini və matrisin transponirə edilməsini bilməlidir. İki və üçtərtibli determinatların hesablanması üsullarına yiyələnməlidir. |
| FTN 2 - Minor və cəbri tamamlayıcı anlayışı, determinantın sətir və ya sütun üzrə ayrılış düsturu, yüksək tərtib determinantın induktiv tərifi və həmçinin hesablanması üsulları kimi biliklərə malik olmalıdır. İki matrisin hasilinin determinantının hesablanmasını və kvadratik matrisin tərsinin hesablanmasını bacarmalıdır. Ortoqonal matrislər və blok matrislər üzərində əməlləri yerinə yetirməyi bacarmalıdır. |
| FTN 3 - n-ölçülü vektor anlayışını, vektorlar sisteminin xətti asılılığının tərifini, xətti asılılığın zəruri və kafi şərtini və matrisin ranqının hesablanması üsullarını bilməlidir. Xətti fəzanın tərifi, bazisi, ölçüsü, xətti çevirmə, xətti çevirmənin matrisi və xətti çevirmələr üzərində əməllər haqqında biliklərə malik olmalıdır. Matrisin məxsusi ədəd və vektoru anlayışlarına, məxsusi ədəd və uyğun məxsusi vektorların tapılması alqoritminə yiyələnməlidir. |
| FTN 4 - Xətti cəbri tənliklər sistemi, bircins və qeyri-bircins xətti cəbri tənliklər sistemi, uyuşan və uyuşmayan xətti cəbri tənliklər sistemi haqqında biliklərə malik olmalıdır. Xətti cəbri tənliklər sistemini Kramer və Qauss üsulu ilə həll etməyi və bircins xətti cəbri tənliklər sistemini həll etməyi bilməlidir. |
| FTN 5 - Çoxhədli, onlar üzərində hesab əməlləri, çoxhədlilərin qalıqlı bölünməsi alqoritmi, Bezu teoremi və Hörner sxeminin alqoritmi haqqında biliklərə malik olmalıdır. Çoxhədlinin həqiqi köklərinin sərhədlərinin tapılması üçün Laqranj, Nyuton üsullarını bilməlidir. |
| FTN 6 - Kvadratik formanı, kvadratik formanın matris şəklində yazılışını və kanonik şəkildə olan kvadratik formanı bilməlidir. Kvadratik formanın kanonik şəkilə gətirmək üçün Laqranj və Yakobi üsulları ilə işləməyi bacarmalıdır. |

| **"Əməliyyat sistemləri" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - Fərqli əməliyyat sistemləri, onların fərqlərini və tətbiq sahələrini fərqləndirməyi bacarır. |
| FTN 2 - Əməliyyat sistemlərinin əsas funksiyaları, prosesləri, avadanlıqlarla əlaqəni izah edə bilir. |
| FTN 3 - Proseslər arasında məlumat mübadiləsi mexanizmlərini, proseslərin paralel emalının prinsiplərini bilir. |
| FTN 4 - Əməliyyat sisteminin yaddaşı necə idarə etdiyini, yaddaşdakı məlumata əsasən araşdırma aparma üsul və alətlərindən istifadəni bacarır. |
| FTN 5 - Fərqli əməliyyat sistemlərində fayl sistemi və giriş/çıxış mexanizmlərinin arxitekturasını bilir, proqramlaşdırma interfeysləri vasitəsilə onlardan yararlanmağın qaydalarını bilir. |
| FTN 6 - Əməliyyat sistemlərində əsas təhlükəsizlik mexanizmləri və səlahiyyət bölgülərininin prinsiplərini bilir. |

| **"Şəbəkələrin təhlükəsizliyi" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - Şəbəkədə autentifikasiya, identifikasiya və qaydalara uyğun girişi təşkil etməyi bacarmalıdır. |
| FTN 2 - Şəbəkənin auditini və loqlaşdırma işlərini həyata keçirməyi bacarmalıdır. |
| FTN 3 - Şəbəkələrin təhlükəsizliyi ilə bağlı olan protokol və qoşulma növlərini, IoT avadanlıqlarının internet və ya digər şəbəkələrə qoşulması üsullarını bilməlidir. |
| FTN 4 - Şəbəkələrin digər şəbəkələrlə inteqrasiya və ya qoşulması zamanı DMZ zonaların qurulması və sazlanmasını həyata keçirə bilməlidir. |
| FTN 5 - Yeni nəsil təhlükəsizlik divarları ilə bağlı əsaslı biliklərə malik olmalıdır. |

| |
|---|
| FTN 6 - Şəbəkələrə qarşı həyata keçirilə biləcək məlum hücümlar barədə məlumatlı olmalıdırvə onların qarşısının alınması və ya vurulan nəticələrin qısa müddətdə aradan qaldırılması üsullarını bilməlidir. |

| "Diskret riyaziyyat" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Məntiq cəbrinin elementar funksiyaları və onların xassələri haqqında biliklərə malik olmalıdır. Düsturlar, funksiyaların düsturlarla ifadəsi, eyni quruluşlu düsturlarla işləməyi bacarmalıdır. Tavtalogiya və eyniliklə yalan düsturlar, düsturların ekvivalentliyi haqqında biliklərə malik olmalıdır. |
| FTN 2 - İkili funksiya, ikilik prinsipi haqqında biliklərə malik olmalıdır. Məntiq cəbri funksiyalarının dəyişənlər üzrə ayrılışını, mükəmməl dizyunktiv formaları və mükəmməl normal formaları qura bilməlidir. |
| FTN 3 - Bul funksiyalarının və onların rəqəmsal sxemlərin və kriptoqrafik primitivlərin modelləşdirilməsində sadə tətbiqlərini bilməlidir. |
| FTN 4 - Ədədlər nəzəriyyəsinin açıq açarlı kriptoqrafiyada istifadə edilən zəruri elementlərini və onların müvafiq kriptoqrafik alqoritmlərdə tətbiqlərini bilməlidir. |
| FTN 5 - Sonlu meydanların əsas elementlərini bilməli və onların kriptoqrafik alqoritmlərdə tətbiqi nümunələrindən məlumatlı olmalıdır. |
| FTN 6 - Qrafların təsviri üsullarını və çəkili qraflarda ən qısa yolların tapılması alqoritmlərini bilməli və onları şəbəkə modelləşdirməsində tətbiq etməyi bacarmalıdır (OSPF). |

| "Veb təhlükəsizlik" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Veb brauzerlərin iş prinsiplərini, veb tətbiqlərin layihələndirilməsi, yaradılması və istismarı qaydalarını bilməlidir. |
| FTN 2 - Müasir texnologiyalardan istifadə edərək təhlükəsiz veb səhifələr hazırlamağı bacarır. HTML, CSS, JavaScript kimi texnologiyaları bilməlidir. |
| FTN 3 - HTTP protokolunun necə çalışdığını bilir. SSL sertifikatlarının necə çalışdığını və veb səhifələrin təhlükəsizliyini necə qoruduğunu bilir. |
| FTN 4 - Veb saytlarda hücumların təbiəti haqqında məlumatlıdır. |
| FTN 5 - REST və GraphQL kimi veb xidmətlərin necə çalışdığını bilir. |
| FTN 6 - OWASP Top 10 - təhlükəsizlik zəiflikləri ilə tanışdır. o siyahıları müəyyənləşdirməyi, onların qarşısının alınması mexanizmlərini bacarır. |

| "Ehtimal nəzəriyyəsi" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Stoxastik eksperiment və hadisə anlayışlarını bilmədir. Hadisələr üzərində əməllər aparmağı bacarmalıdır. Klassik ehtimal anlayışını bilməli, kombinatorikanın elementləri haqqında biliklərə malik olmalıdır. |
| FTN 2 - Şərti ehtimal və hadisələrin asılı olmazlığı anlayışlarını bilməlidir. Tam ehtimal və Bayes düsturlarına yiyələnməlidir. Entropiya və informasiya miqdarı anlayışlarını bilməli, onların informasiyanın kodlaşdırılmasında tətbiqi ilə bağlı məsələlərə tətbiq etməyi bacarmalıdır. |
| FTN 3 - Bayes düsturu, təsadüfi kəmiyyət və paylanma funksiyası, bəzi məşhur diskret və kəsilməz paylanmalar, Puasson təsadüfi prosesi, Markov zəncirləri, kütləvi xidmət sistemlərinə aid sadə modelləri bilir. |
| FTN 4 - Əsas diskret paylanmaları (Bernulli, binomial, Puasson və həndəsi paylanmaları) bilməlidir. Əsas mütləq kəsilməz paylanmaları (müntəzəm, üstlü, normal, Koşi |

| |
|---|
| paylanmalarını) bilməlidir. |
| FTN 5 - Asılı olmayan təsadüfi kəmiyyətlərin cəminin paylanmasını və təsadüfi kəmiyyətdən asılı funksiyaların paylanmasını tapmağı bacarmalıdır. Təsadüfi kəmiyyətin ədədi xarakteristikalarını bilməlidir. |
| FTN 6 - Yüksək tərtib momentlər, kovariyasiya və korrelyasiya əmsalı anlayışlarını bilməlidir. |

| **"İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - İnformasiya hüququnun əsasları, mənbələri, hüquq münasibətlərinin elementləri, hüquq normalarının subyektləri barədə biliklər qazanmalı, habelə informasiya sahəsində əsas insan hüquq və azadlıqlarını öyrənməlidir. |
| FTN 2 - Azərbaycan Respublikasında informasiya sahəsində dövlət siyasətinin əsas istiqamətləri, müvafiq strategiya və dövlət proqramları barədə biliklər əldə etməli, eləcə də ölkənin informasiya sahəsində milli təhlükəsizlik maraqları və informasiya təhlükəsizliyi siyasəti ilə bağlı biliklərə yiyələnməlidir. |
| FTN 3 - İnformasiya təhlükəsizliyi və kibertəhlükəsizliklə bağlı rəhbər normativ hüquqi aktlarla tanış olmalı və onların tələblərini bilməlidir. |
| FTN 4 - Kritik informasiya infrastrukturunun təhlükəsizliyinin təmin olunması sahəsində hüquqi və təşkilati məsələlər, eləcə də, infrastruktur obyektlərinin təsnifatlaşdırılması, minimal təhlükəsizlik tələbləri, nəzarət mexanizmləri barədə ümumi biliklərə yiyələnməlidir. |
| FTN 5 - Fərdi məlumatların, eləcə də dövlət sirri təşkil edən və konfidensial informasiyanın, habelə peşə, kommersiya, istintaq və məhkəmə sirrinin mühafizəsi sahəsində müvafiq qanunvericiliyin tələblərini bilməli, eləcə də mövcud qanunverciliyinin tələblərinin pozulmasına görə nəzərdə tutulan məsuliyyət tədbirlərini öyrənməlidir. |
| FTN 6 - Kibercinayətlərin anlayışı, təsnifatı, və kibercinayətkarlığa qarşı mübarizənin hüquqi əsasları, habelə informasiya müharibəsi və kibermüharibə anlayışları və onların xüsusiyyətləri, müasir çağırışlar və hibrid müharibələrin hüquqi aspektləri barədə ümumi biliklər əldə etməlidir. |

| **"İnformasiya təhlükəsizliyinin idarəedilməsi sistemləri" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - İnformasiya təhlükəsizliyi menecmentinin nə olduğunu və onun əsas prinsiplərini bilir. |
| FTN 2 - İnformasiya təhlükəsizliyinin idarəedilməsinin təşkilatların üçün vacibliyini və faydalarını başa düşür. |
| FTN 3 - İnformasiya təhlükəsizliyinin idarəedilməsi üzrə yerli və beynəlxalq standartlar ilə tanışdır. |
| FTN 4 - ISO/IEC 27000 standartlar ailəsi barədə məlumatlıdır. |
| FTN 5 - ISO/IEC 27001:2013 standartının əsas konsepsiya və prinsipləri, orada istifadə olunan əsas anlayışları bilir. |
| FTN 6 - ISO/IEC 27001:2013 standartının əsas tələblərini bilir. |

| **"Verilənlər bazalarının əsasları və təhlükəsizliyi" fənni üzrə təlim nəticələri (FTN)** |
|---|
| FTN 1 - Verilənlər bazalarının idarəetmə sistemlərinin əsas funksiyalarını bilir. Müasir zamanda istifadə olunan VBİS-lərdən bir neçəsi ilə işləməyi bacarır. Relyasiyalı VBİS-lərin sistem kataloqlarının necə çalışdığını, orada hansı məlumatların yerləşdiyini bilir. Təhlükəsizlik və etibarlılıq üçün verilənlər bazası auditini və loqlamanı aparmağı bacarır. |
| FTN 2 - VBİSlərdə istifadəçi profilləri, parol siyasətləri, icazə(hüquq/haqq) və rolların idarə edilməsilə VBİSdə ilkin təhlükəsizlik tədbirlərinin görülməsini bacarır. |

| |
|---|
| FTN 3 - Verilənlər bazalarının əlçatanlıq problemlərinin səbəblərini bilir, ehtiyat nüsxələr, onlar arasında sinxronlaşdırma, yüklərin balanslaşdırılması üsullarını bilir. |
| FTN 4 - Verilənlər bazalarında tamlığın qorunması üçün üsulları bilir. Verilənlər bazalarında fərqli səviyyələrdə (fayl sistemi, cədvəl, sütun və s.) müxtəlif şifrləmə üsullarını və həllərini yerinə yetirməyi bacarır. |
| FTN 5 - Tətbiqi proqramlardan gələn təhlükələr barədə xəbərdardır. SQL inyeksiyası və bu zəmindən olan təhlükələr, onların qarşısının alınması yollarını bilir. |
| FTN 6 - NoSQL tipli verilənlər bazaları, onların iş prinsipləri, praktiki əhəmiyyətləri, ənənəvi VBİSlərdən üstün və mənfi cəhətlərini bilir. |

| "Bulud təhlükəsizliyi" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Bulud xidmətinin prinsipləri, təqdim edilən əsas xidmət barədə ümumi məlumat təqdim edir və onun ənənəvi xidmətlərdən fərqini, üstün və mənfi cəhətlərini anlayır. |
| FTN 2 - Buluddan istifadə edərək sadə həllər yaratmaq və ona müvafiq təhlükəsizlik tədbirlərini yerinə yetirmək üçün nəzəri və praktik həllər verməyi bacarır. |
| FTN 3 - Serversiz hesablamalar, onların xüsusiyyətləri və fərqli cəhətləri, bu xidmətlərdə təhlükəsizlik məsələlərinə aid məsuliyyət öhdəliklərini izah etməyi bacarır. |
| FTN 4 - Buludda olan risk və boşluqların çərçivəsini ölçmə üsul və meyarlarını bilir. |
| FTN 5 - Buludda şəbəkə təhlükəsizliyi vasitələrindən istifadə etməyi bacarır. |
| FTN 6 - Buludda məlumat sızmasının simptomlarını bilmək, onu izləmək, səbəblərini tapmaq və qarşısını almaq bacarır. |

| "Kriptoqrafiyanın əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Klassik ve müasir kriptoqrafiya arasındakı fərqləri bilməli, klassik şifrlərin kriptoanalizi metodları ilə tanış olmalıdır. Simmetrik ve asimmetrik şifrləmə sistemlərinin fərqlərini bilməlidir. |
| FTN 2 - İnformasiya təhlükəsizliyi prinsiplərindən konfidensiallıq və tamlığın, o cümlədən autentikasiya və inkar edilməmə prinsiplərinin kriptoqrafik üsullarla necə təmin olunduğunu bilməlidir. |
| FTN 3 - Blok şifrlər və axın şifrlər arasındakı fərqləri, onlara uyğun alqoritmlər və bu alqoritmlərin tətbiq sahələrini bilməlidir. |
| FTN 4 - Açıq açarlı şifrlərlə əlaqəli alqoritmləri, onlarin tətbiqlərini bilməlidir. Açıq açar infrastrukturu haqda məlumatlı olmalıdır. |
| FTN 5 - Heş funksiyalarının xususiyyətlərini bilməli onlardan istifadə edilərək tamlığın necə təmin edildiyini və rəqəmsal imzalardakı mahiyyətini bilməlidir. |
| FTN 6 - Qabaqcıl kriptoqrafik protokolları və onların tətbiqlərini bilməlidir. |

| "Nüfuzetmə sınaqlarının əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Nüfuzetmə sınaqlarının prinsip və texnikaları ilə tanış olacaqsınız. |
| FTN 2 - Nüfuzetmə sınağının mərhələlərini öyrənəcəksiniz. |
| FTN 3 - Aktiv və passiv məlumat toplama metodlarıyla tanış olacaqsınız. |
| FTN 4 - Verilmiş hədəf üçün təhlükəsizlik boşluqlarını aşkarlama, istismar etmə, riskini ölçmə və qarşısını alma yollarını təklif etməyi öyrənəcəksiniz. |
| FTN 5 - Nüfuzetmə testi zamanı istifadə olunan alətlərlə tanış olacaqsınız. |
| FTN 6 - Nüfuzetmə testinin nəticələri əsasında professional hesabat hazırlamaqla bağlı biliklər əldə edəcəksiniz. |

| "Elektronika və IoT cihazların təhlükəsizliyi" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Əsas elektronika komponentlərini – məntiqi sxemləri, çeviriciləri, rezistor, kondensator, tranzistor, induktiv sarğılar, diodları tanıyır, onlardan istifadə edərək dövrələr qurnağı bacarır. |
| FTN 2 - Elektronika dövrələrində müşahidə və sınaqlar etmək üçün simulyasiya proqramından istifadə etməyi bacarır.. |
| FTN 3 - Elektrik dövrələrinin əsas kəmiyyətlərini ölçmək üçün ölçmə alətlərindən istifadə edə bilərsiniz. |
| FTN 4 - Qurğular arasında məlumat mübadiləsi üçün fərqli protokollarla tanış olmalıdır. |
| FTN 5 - Qurğular arasında simsiz rabitə üçün fərqli texnologiyalar barədə məlumatlı olmalıdır. |
| FTN 6 - IoT qurğularla bağlı informasiya təhlükəsizliyi məsələlərini öyrənməli, onlara qarşı mümkün kiber-hücumları və hücumlardan müdafiə üsullarını bilməlidir. |

| "Təhlükəsiz proqramlaşdırma" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Proqram təminatı təhlükəsizliyinin nə olduğunu, hansı səbəblərdən baş verdiyini anlayır. |
| FTN 2 - Kompüterin yaddaşının quruluşunu, yaddaşın dolubdaşması, bu səbəbdən baş verən eksploitlərin necə çalışdığını anlayır. |
| FTN 3 - Proqram təminatının arxitekturasının qurulması zamanı təhlükəsizlik aspektlərini nəzərə almağı, onların qarşısının alınması prinsiplərini bilir. |
| FTN 4 - Proqram təminatı üzrə kod auditi, avtomatlaşdırılmış dinamik və statik kod sınaqları üçün vasitələrdən istifadə etməyi bacarır. |
| FTN 5 - Proqram təminatının qurulmasının bütün həyat dövrü ərzində təhlükəsizlik məsələlərinin vacibliyini, onun izlənilməsi prinsiplərini bilir. |
| FTN 6 - Təhlükəsiz kod auditini yerinə yetirməyi bacarır. Dünyada ən çox rastgəlinən proqram təhlükəsizlik boşluqlarından məlumatlıdır. |

| "Rəqəmsal kriminalistikanın əsasları" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Məhkəmə kompüter-texniki ekspertizasının/Rəqəmsal kriminalistikanın rolunu və əhəmiyyətini dərk etməli, növlərini bilməli, tədqiqat metodlarını anlamalı və tətbiq edə bilməlidir. |
| FTN 2 - Sübuti əhəmiyyətə malik olan rəqəmsal dəlilləri ayırd edə bilməli, onların növlərini və əhəmiyyətini dərk etməlidir. |
| FTN 3 - Rəqəmsal sübutların identifikasiyası, toplanılması, sənədləşdirilməsi, saxlanılması, istifadə olunması, mühafizəsi və təqdim olunmasının prosessual əsaslarını öyrənməlidir. |
| FTN 4 - Rəqəmsal sübutların identifikasiyası, toplanılması, sənədləşdirilməsi, saxlanılması, istifadə olunması, mühafizəsi və təqdim olunması üçün zəruri resurs və avadanlıqlardan istifadə üzrə bilik və bacarıqlara yiyələnməli, eləcə də açıq kodlu və qabaqcıl həlləri tətbiq etməyi bacarmalıdır. |
| FTN 5 - Rəqəmsal sübutların kriminalistik diaqnostikasını aparmalı, əldə edilmiş nəticələri qiymətləndirməli və nəticələri formulə edə bilməlidir. |
| FTN 6 - Sübutların mümkünlüyünün təmin olunması üçün zəruri hüquqi prosedurları və tələbləri bilməlidir. |

| "Sənaye idarəetmə sistemlərinin təhlükəsizliyi" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - IT ve OT mühitləri arasindaki fərqləri, OT sistemlərinə aid olan protokolları və işləyişini bilməlidir. |

| |
|---|
| FTN 2 - Kritik infrastrukturlarda sistemlərə aid boşluqları/zəiflikləri müəyyən edə bilməli və onları aradan qaldırmağın üsullarına yiyələnməlidir. |
| FTN 3 - Kritik infrastrukturlarda PLC, DCS, RTU, HMI, AVR kimi sistemlər ilə tanış olmalıdır. |
| FTN 4 - Kritik infrastrukturlarda potensiyal kiber təhdidləri müəyyən edə bilməli və risk analizi edə bilməlidir. |
| FTN 5 - IT mühitində tətbiq edilən uyğun kiber təhlükəsizlik addımlarının OT mühitinə tətbiqini bilməlidir. |
| FTN 6 - Kritik infrastrukturlara aid baş vermiş hadisələri analiz edə bilməli, əsas səbəbin tapılması üçün müvafiq addımların tətbiqlərini bilməlidir. |

| "Mülki müdafiə" fənni üzrə təlim nəticələri (FTN) |
|---|
| FTN 1 - Mülki müdafiənin əsasları, qüvvə və vasitələrini bilməlidir. |
| FTN 2 - Fövqəladə hallar və onların xarakteristikalarını bilməlidir. |
| FTN 3 - Fövqəladə hallarda əhalinin mühafizəsi, əhalinin mülki müdafiə üzrə maarifləndirilməsi haqqında biliklərə yiyələnməlidir. |
| FTN 4 - Fərdi və kollektiv mühafizə vasitələrindən istifadə etməyi bacarmalıdır. |
| FTN 5 - Fövqəladə hallarda sənaye obyektlərinin işinin dayanıqlığının əsaslarını və qiymətləndirilməsini bilməlidir. |
| FTN 6 - Fövqəladə halların nəticələrinin aradan qaldırılması yollarının təşkili və həyata keçirilməsi haqqında biliyə malik olmalıdır. |

Əlavə 5

## Fənlərin və Təhsil Proqramının təlim nəticələrinin matrisi

Ali təhsil müəssisəsi aşağıdakı cədvəldən istifadə edərək ixtisasın Təhsil Proqramının təlim nəticələrinin əldə olunmasına necə dəstək verdiyini müəyyən etməlidir.

| Blokun adı | Fənlərin adı | Proqramın təlim nəticələri | | | | | |
|---|---|---|---|---|---|---|---|
| | | PT N 1 | PT N 2 | PT N 3 | PT N 4 | PT N 5 | PT N 6 |
| Ümumi fənlər | Azərbaycan tarixi | X | | | | | |
| | Azərbaycan dilində işgüzar və akademik kommunikasiya | X | | | | | |
| | Azərbaycan dövlətçiliyi və ideologiya | X | | | | | |
| | Xarici dildə işgüzar və akademik kommunikasiya | X | | | | | |
| İxtisas fənləri | İnformasiya təhlükəsizliyinin əsasları | X | | X | | | X |
| | Proqramlaşdırmanın əsasları | | X | | X | | |
| | Riyazi analiz | | X | | X | | |
| | Kibertəhlükəsizliyin əsasları | X | | X | | | X |
| | Şəbəkələrin əsasları | | | X | | | |
| | Xətti cəbr | | X | | | | |
| | Əməliyyat sistemləri | | | | | X | |
| | Şəbəkələrin təhlükəsizliyi | | | | | X | |
| | Diskret riyaziyyat | | X | X | | | |
| | Veb təhlükəsizlik | | | X | | | |
| | Ehtimal nəzəriyyəsi və riyazi statistika | | X | | X | | |
| | İnformasiya təhlükəsizliyi və kibertəhlükəsizliyin hüquqi aspektləri | | X | X | | | |
| | İnformasiya təhlükəsizliyinin idarəedilməsi sistemləri | | | X | X | X | X |
| | Verilənlər Bazalarının təhlükəsizliyi | | | X | | X | |
| | Bulud təhlükəsizliyi | | | X | | X | |
| | Kriptoqrafiyanın əsasları | | | | X | | |
| | Nüfuzetmə sınaqlarının əsasları | | | X | | | |
| | Elektronikanın əsasları və IoT təhlükəsizliyi | | | | | X | |
| | Təhlükəsiz proqramlaşdırma | | | X | | | X |
| | Rəqəmsal Kriminalistikanın əsasları | | | | X | | |
| | Sənaye idarəetmə sistemlərinin təhlükəsizliyi | X | | | | | X |

Əlavə 6

**Təhsil Proqramı məzunlarının işləyə biləcəyi rollara nümunə**

- informasiya təhlükəsizliyi inzibatçısı
- informasiya təhlükəsizliyi auditoru
- informasiya təhlükəsizliyi üzrə insident menecer
- informasiya təhlükəsizliyi üzrə analitik
- informasiya təhlükəsizliyi sistemləri üzrə mütəxəssis
- informasiya təhlükəsizliyi üzrə tədqiqatçı-mütəxəssis
    - proqram təminatının mənbə (ilkin) kodu üzrə tədqiqatçı-mütəxəssis
    - veb proqram təminatı üzrə tədqiqatçı-mütəxəssis
    - texniki təminat üzrə tədqiqatçı-mütəxəssis
    - mobil cihaz üzrə tədqiqatçı-mütəxəssis
- proqram təminatı üzrə təhlükəsizlik arxitektoru
- proqram təminatı üzrə təhlükəsizlik əməliyyatları mühəndisi (DevSecOps)
- nüfuzetmə sınaqçısı
- kiber tədqiqatçı*(investigator)*
- kripto-analitik
- kriptoqraf
- bulud texnologiyaları üzrə tədqiqatçı-mütəxəssis
- kiberinsidentlərin və kibercinayətlərin araşdırılması üzrə mütəxəssis
- İKT xidmət meneceri (təhlükəsizlik üzrə)
- İKT üzrə davranış analitiki (psixoanalitik)
- İKT layihə meneceri
- İKT arxitektor, layihəçi
- informasiya xidmətləri meneceri
- informasiya təminatı üzrə analitik (data analitik)
- biometrik identifikasiya xidməti meneceri
- bulud təhlükəsizliyi üzrə inzibatçı
- şəbəkə təhlükəsizliyi administratoru
- kibertəhlükəsizlik üzrə məsləhətçi
- 1-ci səviyyəli SOC təhlilçisi (SOC Tier-1 analyst)
- kibertəhlükəsizlik üzrə risk təhlilçisi