**AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ**

**BAKI BİZNES UNİVERSİTETİ**

İnformasiya təhlükəsizliyinin əsasları

(Fənnin adı)

**“İnformasiya texnologiyları”** kafedrası

**Hüseynli Cavad Rəşad oğlu tərəfindən hazırlanmış**

**Sillabus**

**Bakı – 2025**

**Təsdiq edirəm\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(kafedra müdiri)

**İmza: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Tarix: “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025-ci il**

1. **Ali təhsil pilləsi – bakalavr**

**Tədris forması - əyani/qiyabi**

1. **Fənn haqqında məlumat**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fənnin kodu, adı** | **Kafedra** | **Tədris ili, semestr** | **Kredit sayı** | **Tədris yükü** | |
| **Müh/saat** | **Məş/saat** |
|  |  | 2025-2026-cı il  I semestr | 6 | 45 | 30 |

1. **Müəllim haqqında məlumat:**\_ Hüseynli Cavad Rəşad .

(Soyadı, adı, atasının adı,)

E-mail ünvanı: cava5284@gmail.com

1. **Fənnin təsviri:** (Fənn haqqında qısa məlumat, fənnin digər fənlərlə qarşılıqlı əlaqəsi)

“İnformasiya təhlükəsizliyinin əsasları” fənni tələbələrə informasiya resurslarının qorunması, təhlükə və risklərin müəyyənləşdirilməsi, kriptoqrafiya, identifikasiya və autentifikasiya üsulları, həmçinin şəbəkə və sistemlərin müdafiəsi üzrə baza bilik və bacarıqlar qazandırır. Fənn “Kompüter şəbəkələri”, “Məlumat bazaları”, “Proqramlaşdırma dilləri” və digər baza fənlərlə sıx qarşılıqlı əlaqədədir və tələbələrə gələcəkdə “Şəbəkə təhlükəsizliyi”, “Kiberhücumların analizi və müdafiə üsulları”, “Etik hakerlik” kimi ixtisaslaşmış fənlərin mənimsənilməsi üçün nəzəri-praktiki zəmin yaradır.

1. **Fənnin sonunda tələbənin yiyələnəcəyi kompetensi­ya (kompetensiyalar):**

**Fənnin sonunda tələbə informasiya təhlükəsizliyi üzrə baza biliklərinə, risklərin təhlili və mühafizə mexanizmlərinin tətbiqi kompetensiyasına yiyələnəcəkdir.**

1. **Fənnin məqsədi**

|  |  |
| --- | --- |
| **№** | **Fənnin məqsədi** |
| M1 | Tələbələrə informasiya təhlükəsizliyinin nəzəri əsaslarını mənimsətmək. |
| M2 | İnformasiya resurslarının qorunması və təhlükəsizlik siyasətlərinin tətbiq bacarıqlarını inkişaf etdirmək. |
| M3 | Təhlükə və risklərin növlərini təhlil etmək və qiymətləndirmək bacarığını təmin etmək. |
| M4 | Kriptoqrafiya və məlumat şifrələmə üsullarını nəzəri və praktiki şəkildə tətbiq etmək. |
| M5 | İdentifikasiya və autentifikasiya mexanizmlərini anlamaq və praktikada tətbiq etmək. |
| M6 | Şəbəkə və sistemlərin müdafiəsi metodlarını mənimsəmək və tətbiq etmək bacarığını formalaşdırmaq. |
| M7 | Müasir kibertəhdidlərə qarşı effektiv müdafiə strategiyalarını öyrətmək. |

### **Fənnin təlim nəticələri (öyrənmə nəticələri)**

|  |  |  |
| --- | --- | --- |
| **№** | **Təlim nəticələri** | **Məqsədlərlə əlaqəsi** |
| TN1 | İnformasiya təhlükəsizliyinin əsas anlayışlarını və prinsiplərini izah edə biləcəklər. | M1 |
| TN2 | İnformasiya resurslarını qoruma və təhlükəsizlik siyasətlərini tətbiq edə biləcəklər. | M2 |
| TN3 | Təhlükə və risklərin növlərini təhlil edib qiymətləndirə biləcəklər. | M3 |
| TN4 | Kriptoqrafiya və məlumat şifrələmə üsullarını nəzəri və praktik şəkildə tətbiq edə biləcəklər. | M4 |
| TN5 | İdentifikasiya və autentifikasiya mexanizmlərini anlamaq və praktikada tətbiq edə biləcəklər. | M5 |
| TN6 | Şəbəkə və sistemlərin müdafiəsi metodlarını mənimsəyərək tətbiq edə biləcəklər. | M6 |
| TN7 | Müasir kibertəhdidlərə qarşı effektiv müdafiə strategiyalarını seçib tətbiq edə biləcəklər. | M7 |

1. **Öyrətmə və öyrənmə metodları ( Təlim metodları)**

**TM1.** Mühazirələrin təqdimat şəklində aparılması.

**TM2.** Mühazirə dərslərində yeni informasiya texnologiyalarında qazanılmış biliklərin tətbiqi ilə iqtisadi məzmunlu məsələlərin müxtəlif tətbiqi proqramlarda həll edilməsi.

**TM3.** Tələbəyönümlü təhsil prinsiplərinə uyğun olaraq mühazirə dərslərində yeri gəldikcə diskussiyalar təşkil edilərək, tələbə aktivliyinin təmin edilməsi.

**TM4.** Sadə məsələlərin kodlaşdırılması üsullarından istifadə etməklə praktiki məsələlərin nümayişi.

1. **Qiymətləndirmə üsulları**

**QM1.** Şifahi təqdimatlar;

**QM2.** Sorğular;

**QM3.** Açıq müzakirələr;

**QM4.** Seminar (məşğələ) dərslərində mühazirədə tələbənin qazandığı biliklərin təhlili və tətbiqi nəticəsində bacarıqlarının qiymətləndirilməsi;

**QM5.** Frontal sorğu;

**QM6.** Qrup şəklində və özünü qiymətləndirm

**Qiymətləndirmə sistemi**

|  |  |  |
| --- | --- | --- |
| **№** | **Fəaliyyətlər** | **Bal** |
|  | Auditoriya və auditoriyadankənar fəaliyyətin qiymətləndirilməsi   * + - 1. Mühazirə dərslərində fəal iştirakına və tematik tapşırıqların yerinə yetirilməsi bacarıqlarına, mühazirə müddətində cari mövzunun mənimsənilməsinə görə       2. Seminar (məşğələ) dərslərində nəzəri biliklərin mənimsənilməsi səviyyəsinə görə 0-5 bal, interaktiv metodlardan istifadə və frontal sorğularda fəal iştiraka, debatlardan və digər üsullardan istifadəyə görə 0-5 bal       3. Kollokviumların seminar dərslərində mövzuların 1/3-ni tam əhatə etməklə, 2-yazılı 1-şifahi kollokvium 3-5 sualdan ibarət tərtib edilərək keçirilir və nəticə qiymətləndirilir       4. Layihə-referatın tərtibi və təqdimatı. 0-5 bal referat işlərinin qiymətləndirilməsi, 0-10 bal təqdimat bacarıqları üçün nəzərdə tutulmuşdur | 50  10  10  15  15 |
|  | Aralıq imtahan (final) | 50 |

**Təhsil alanların biliyinin balın yekun miqdarına görə qiymətləndirilməsi:**

|  |  |  |
| --- | --- | --- |
| * 51 bala qədər | “qeyri-kafi” | * F |
| * 51-60 bal | “qənaətbəxş” | * E |
| * 61-70 bal | “kafi” | * D |
| * 71-80 bal | “yaxşı” | * C |
| * 81-90 bal | “çox yaxşı” | * B |
| * 91-100 bal | “əla” | * A |

1. **Təklif olunan ədəbiyyatlar**

- əsas ədəbiyyat

* + - 1. *İnformasiya təhlükəsizliyinin əsasları*. Dərslik. Bakı: MTN Maddi-texniki Təminat Baş İdarəsinin Nəşriyyat-Poliqrafiya Mərkəzi, 2009. 340 s.
      2. **Stallings,W.** *Kriptoqrafiya və Şəbəkə Təhlükəsizliyi: Prinsiplər və Təcrübə*, 8-ci nəşr, Pearson, 2019.

1. **Fənn üzrə təqvim-tematik plan**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S/N** | **Mövzunun adı və planı** | **Təlim metodları** | **Qiymətləndirmə metodları** | **Mövzunun FTN ilə əlaqəsi** | **Müh** | **Məş** |
| 1 | **Mühazirə 1. Giriş və İnformasiya Təhlükəsizliyinə Giriş** 1. İnformasiya təhlükəsizliyinin əsas anlayışları 2. Təhlükəsizlik prinsipləri və qaydaları 3. İnformasiya təhlükəsizliyinin əhəmiyyəti və tətbiq sahələri **Mövzunun məqsədi:** Tələbələrə informasiya təhlükəsizliyinin nəzəri əsaslarını mənimsətmək, təhlükəsizlik prinsiplərini başa salmaq və praktiki sahələrdə tətbiqini anlamaq bacarığını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN1 | 2 | 2 |
| 2 | **Mühazirə 2. İnformasiya Resurslarının Qorunması** 1. Resursların kateqoriyalara ayrılması və idarə edilməsi 2. Təhlükəsizlik siyasətləri və standartları 3. Qoruma strategiyalarının praktik tətbiqi **Mövzunun məqsədi:** Tələbələrə informasiya resurslarını qoruma və təhlükəsizlik siyasətlərini tətbiq bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN1 | 2 | 2 |
| 3 | **Mühazirə 3. Təhlükə və Risklərin Analizi** 1. Təhlükə və risk növlərinin müəyyən edilməsi 2. Risk qiymətləndirmə metodları 3. Risklərin idarə olunması və azaldılması strategiyaları **Mövzunun məqsədi:** Tələbələrə təhlükə və riskləri təhlil etmək, qiymətləndirmək və uyğun həll yollarını müəyyən etmək bacarığını təmin etmək. | TM1, TM2 | QM1, QM2 | TN1 | 2 | 2 |
| 4 | **Mühazirə 4. Kriptoqrafiya və Məlumat Şifrələmə Üsulları** 1. Kriptoqrafiyanın əsas anlayışları 2. Simmetrik və assimmetrik şifrələmə üsulları 3. Praktik tətbiq nümunələri **Mövzunun məqsədi:** Tələbələrə kriptoqrafiya və məlumat şifrələmə üsullarını nəzəri və praktik şəkildə tətbiq etmə bacarığını öyrətmək. | TM1, TM2 | QM1, QM2 | TN1 | 2 | 2 |
| 5 | **Mühazirə 5. İdentifikasiya və Autentifikasiya Mexanizmləri** 1. İdentifikasiya və autentifikasiya anlayışları 2. Şifrə, token və biometrik metodlar 3. Praktik tətbiq nümunələri **Mövzunun məqsədi:** Tələbələrə identifikasiya və autentifikasiya mexanizmlərini başa salmaq və praktik tətbiq bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN2 | 2 | 2 |
| 6 | **Mühazirə 6. Şəbəkə və Sistemlərin Müdafiəsi** 1. Şəbəkə təhlükəsizliyinin əsas prinsipləri 2. Firewall, IDS/IPS, VPN kimi müdafiə texnologiyaları 3. Təhlükəsizlik siyasətləri və praktik tətbiq nümunələri **Mövzunun məqsədi:** Tələbələrə şəbəkə və sistemlərin müdafiəsi metodlarını öyrətmək və tətbiq bacarıqlarını formalaşdırmaq. | TM1, TM2 | QM1, QM2 | TN2 | 2 | 2 |
| 7 | **Mühazirə 7. Müasir Kibertəhdidlər və Hücum Növləri** 1. Malware, phishing, DoS/DDoS hücumları 2. Hücumların analizi və təsirləri 3. Təhlükəsizlik strategiyalarının seçimi və tətbiqi **Mövzunun məqsədi:** Tələbələrə müasir kibertəhdidlərə qarşı effektiv müdafiə strategiyalarını öyrətmək. | TM1, TM2 | QM1, QM2 | TN2 | 2 | 2 |
| 8 | **Mühazirə 8. İnformasiya Təhlükəsizliyi Problemlərinin Analizi və Qərar Qəbuletmə** 1. Təhlükəsizlik problemlərinin identifikasiyası 2. Risk qiymətləndirmə və qərar qəbuletmə metodları 3. Praktik həll yollarının tətbiqi **Mövzunun məqsədi:** Tələbələrə informasiya təhlükəsizliyi problemlərini analiz etmək, qərar qəbul etmək və uyğun həll yollarını tətbiq etmək bacarığını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN2 | 2 | 2 |
| 9 | **Mühazirə 9. Təhlükəsizlik Hüquqi və Normativ Tənzimləmələr** 1. Hüquqi tələblər və standartlar 2. ISO/IEC standartları və yerli qanunvericilik 3. Praktik tətbiq nümunələri **Mövzunun məqsədi:** Tələbələrə təhlükəsizlik hüquqi və normativ tələbləri öyrətmək. | TM1, TM2 | QM1, QM2 | TN3 | 2 | 2 |
| 10 | **Mühazirə 10. Şəbəkə Hücumlarının Analizi və Müdafiəsi** 1. Şəbəkə hücum növləri (DoS, DDoS, MITM) 2. Hücumların aşkarlanması və analizi 3. Müdafiə texnologiyalarının praktik tətbiqi **Mövzunun məqsədi:** Tələbələrə şəbəkə hücumlarını təhlil etmək və müdafiə üsullarını tətbiq etmək bacarığını öyrətmək. | TM1, TM2 | QM1, QM2 | TN3 | 2 | 2 |
| 11 | **Mühazirə 11. Kriptoqrafiya Təhlükəsizlik və Şifrləmə Analizi** 1. Kriptoqrafiya hücumları və zəifliklər 2. Şifrləmə metodlarının analiz edilməsi 3. Təhlükəsizlik strategiyalarının tətbiqi **Mövzunun məqsədi:** Tələbələrə kriptoqrafiya zəifliklərini tanıtmaq və analiz bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN3 | 2 | 2 |
| 12 | **Mühazirə 12. Məlumatların Qorunması və Backup Strategiyaları** 1. Məlumatların qorunma prinsipləri 2. Backup və Recovery metodları 3. Praktik tətbiq nümunələri **Mövzunun məqsədi:** Tələbələrə məlumatların qorunması və backup strategiyalarını öyrətmək. | TM1, TM2 | QM1, QM2 | TN3 | 2 | 2 |
| 13 | **Mühazirə 13. Müasir Kibertəhlükələr və Risklərin İdarə Edilməsi** 1. Müasir kibertəhdid növləri 2. Risklərin idarə edilməsi metodları 3. Praktik nümunələr və strategiyalar **Mövzunun məqsədi:** Tələbələrə kibertəhlükələr və risklərin idarə edilməsi bacarığını öyrətmək. | TM1, TM2 | QM1, QM2 | TN3 | 2 | 2 |
| 14 | **Mühazirə 14. Layihə İnkişafı və Testlər** 1. Layihə planlaşdırılması və icra 2. Kod inkişafı və versiya idarəetməsi 3. Test strategiyaları və səhv düzəlişləri **Mövzunun məqsədi:** Tələbələrə layihə inkişafı və test bacarıqlarını öyrətmək. | TM1, TM2 | QM1, QM2 | TN4 | 2 | 2 |
| 15 | **Mühazirə 15. Təhlükəsizlik Monitorinqi və Audit** 1. Təhlükəsizlik monitorinqi prinsipləri 2. Audit prosesləri və standartları 3. Praktik nümunələr və analiz **Mövzunun məqsədi:** Tələbələrə təhlükəsizlik monitorinqi və audit bacarıqlarını öyrətmək. | TM1, TM2 | QM1, QM2 | TN4 | 2 | 2 |
| 16 | **Mühazirə 16. Qabaqcıl Müdafiə Strategiyaları və Praktik Təlimlər** 1. Müasir müdafiə texnologiyaları 2. Təhlükəsizlik planlarının hazırlanması və tətbiqi 3. Praktik təlim və nümunələr **Mövzunun məqsədi:** Tələbələrə qabaqcıl müdafiə strategiyalarını mənimsətmək və praktiki bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN4 | 2 |  |
| 17 | **Mühazirə 17. İdentifikasiya və Autentifikasiya Texnologiyaları** 1. Şifrə və token əsaslı autentifikasiya 2. Biometrik identifikasiya üsulları 3. Praktik nümunələr və tətbiq **Mövzunun məqsədi:** Tələbələrə identifikasiya və autentifikasiya mexanizmlərini başa salmaq və praktik tətbiq bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN5 | 2 |  |
| 18 | **Mühazirə 18. İdentifikasiya və Autentifikasiya ilə Təhlükəsizlik Strategiyaları** 1. Multi-faktor autentifikasiya 2. Tətbiq və şəbəkə səviyyəsində təhlükəsizlik 3. Praktik nümunələr və analiz **Mövzunun məqsədi:** Tələbələrə effektiv identifikasiya və autentifikasiya strategiyalarını tətbiq etmə bacarığını öyrətmək. | TM1, TM2 | QM1, QM2 | TN5 | 2 |  |
| 19 | **Mühazirə 19. Şəbəkə və Sistem Müdafiəsi Prinsipləri** 1. Firewall, IDS/IPS, VPN texnologiyaları 2. Təhlükəsizlik siyasətləri və tətbiqi 3. Praktik nümunələr və analiz **Mövzunun məqsədi:** Tələbələrə şəbəkə və sistem müdafiəsi prinsiplərini mənimsətmək və tətbiq bacarıqlarını formalaşdırmaq. | TM1, TM2 | QM1, QM2 | TN6 | 2 |  |
| 20 | **Mühazirə 20. Qabaqcıl Şəbəkə Müdafiə Strategiyaları** 1. Şəbəkə təhlükəsizliyində qabaqcıl texnologiyalar 2. Təhlükəsizlik siyasətlərinin təkmilləşdirilməsi 3. Praktik nümunələr və analiz **Mövzunun məqsədi:** Tələbələrə qabaqcıl şəbəkə müdafiə strategiyalarını öyrətmək və bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN6 | 2 |  |
| 21 | **Mühazirə 21. Müasir Kibertəhdidlər** 1. Malware və ransomware növləri 2. Phishing və sosial mühəndislik hücumları 3. Praktik nümunələr və müdafiə strategiyaları **Mövzunun məqsədi:** Tələbələrə müasir kibertəhdidləri öyrətmək və onların təsirini analiz etmək bacarığını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN7 | 2 |  |
| 22 | **Mühazirə 22. Hücum Analizi və Təhlükəsizlik Taktikaları** 1. Hücumların təhlili və qiymətləndirilməsi 2. Müdafiə planlarının hazırlanması 3. Praktik nümunələr **Mövzunun məqsədi:** Tələbələrə hücumları analiz etmək və effektiv müdafiə taktikalarını tətbiq etmək bacarığını öyrətmək. | TM1, TM2 | QM1, QM2 | TN7 | 2 |  |
| 23 | **Mühazirə 23. Qoruma və Müdafiə Praktik Təlimləri** 1. Hücumların praktiki təhlili 2. Təhlükəsizlik strategiyalarının sınağı və tətbiqi 3. Praktik nümunələr və analiz **Mövzunun məqsədi:** Tələbələrə real ssenarilər üzərində müdafiə bacarıqlarını inkişaf etdirmək. | TM1, TM2 | QM1, QM2 | TN7 | 1 |  |

**X. Referat Mövzuları**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Mövzular** | **Tələbənin soyadı və adı** | **Qrup** | **İmza** |
| 1 | İnformasiya təhlükəsizliyinin əsas anlayışları və prinsipləri |  |  |  |
| 2 | Təhlükəsizlik siyasətləri və qaydalarının tətbiqi |  |  |  |
| 3 | İnformasiya təhlükəsizliyinin əhəmiyyəti və tətbiq sahələri |  |  |  |
| 4 | Kriptoqrafiya və məlumat şifrələmə üsullarının tarixi və inkişafı |  |  |  |
| 5 | Simmetrik və assimmetrik şifrələmə üsullarının müqayisəsi |  |  |  |
| 6 | İdentifikasiya və autentifikasiya üsulları: şifrə, token və biometrik texnologiyalar |  |  |  |
| 7 | Multi-faktor autentifikasiya texnologiyaları və praktik tətbiqləri |  |  |  |
| 8 | Şəbəkə və sistem müdafiəsinin əsas prinsipləri |  |  |  |
| 9 | Müasir kibertəhdidlərin təhlili və qoruma strategiyaları |  |  |  |
| 10 | İnformasiya təhlükəsizliyi problemlərinin analizi və qərar qəbuletmə mexanizmləri |  |  |  |
| 11 | Hüquqi tənzimləmələr və ISO/IEC standartları ilə informasiya təhlükəsizliyi |  |  |  |
| 12 | Şəbəkə hücumlarının növləri və müdafiə üsulları |  |  |  |
| 13 | Kriptoqrafiya zəiflikləri və hücumların analizi |  |  |  |
| 14 | Məlumatların qorunması və backup strategiyaları |  |  |  |
| 15 | Kibertəhlükələr və risklərin idarə olunması metodları |  |  |  |
| 16 | Layihə inkişafı və təhlükəsizlik testləri |  |  |  |
| 17 | Təhlükəsizlik monitorinqi və auditin tətbiqi |  |  |  |
| 18 | Qabaqcıl müdafiə strategiyaları və real ssenarilər üzrə praktiki təlimlər |  |  |  |
| 19 | İdentifikasiya və autentifikasiya mexanizmlərinin effektivliyi |  |  |  |
| 20 | Biometrik və token əsaslı autentifikasiya texnologiyalarının müqayisəsi |  |  |  |
| 21 | Şəbəkə və sistem müdafiəsi texnologiyaları: firewall, IDS/IPS, VPN |  |  |  |
| 22 | Qabaqcıl şəbəkə təhlükəsizliyi strategiyaları və tətbiqi |  |  |  |
| 23 | Müasir kibertəhdidlər: malware, ransomware, phishing |  |  |  |
| 24 | Hücum analizi və təhlükəsizlik taktikalərinin inkişaf etdirilməsi |  |  |  |
| 25 | Real ssenarilər üzrə qoruma və müdafiə praktiki təlimləri |  |  |  |

**İnformasiya texnologiyası**

**kafedrası :** **C.R.Hüseynli**