**İXTİSAS: Telekommunikasiya və kompüter sistemlərinin informasiya təhlükəsizliyi III kurs**

**FƏNN: İnformasiyanın qorunmasının texniki vasitələri və üsulları**

|  |  |
| --- | --- |
|  | İnformasiya təhlükəsizliyinin təmin edilməsi üsullarının təsnifatı |
|  | İnformasiya təhlükəsizliyinin təmin edilməsi vasitələrinin təsnifatı |
|  | İnformasiyanın qorunmasının qeyri-texniki vasitələri |
|  | Təşkilati qoruma tədbirləri |
|  | Hüquqi qoruma vasitələri |
|  | Mənəvi etik tədbirlər |
|  | İnformasiyanın qorunmasının mühəndis-texniki üsulları və vasitələri |
|  | Funksional təyinatına görə mühəndis-texniki vasitələrin növləri |
|  | Fiziki qoruma vasitələri |
|  | Funksional təyinatına görə fiziki qoruma vasitələrinin kateqoriyaları |
|  | İnformasiyanın qorunmasının aparat [vasitələri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark488) |
|  | Funksional təyinatına görə informasiyanın qorunmasının aparat [vasitələri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark488)nin təsnifatı |
|  | Texniki imkanlarına görə informasiyanın qorunmasının aparat [vasitələri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark488)nin qrupları |
|  | İnformasiyanın qorunmasının aparat vasitələrinin inkişafına təsir edən amilllər |
|  | İnformasiyanın qorunmasının proqram [vasitələri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark517) |
|  | İnformasiyanın qorunmasının proqram [vasitələri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark517)nin növləri |
|  | Kabel sistemlərinin qorunması |
|  | Ehtiyyat enerji təminatı ( elektrik qidalanma ) sistemləri |
|  | İnformasiyanın arxivləşdirilməsi və ehtiyat surətlərininyaradılması sistemləri |
|  | [İnformasiyanın kompüter viruslarından qorun­ması](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark563)  |
|  | Funksional təyinatına görə antivirus proqramlarının kateqoriyaları |
|  | Müasir antivirus proqramlarının funksiyaları |
|  | Şəbəkə təhlükəsizliyində əsas anlayışlar |
|  | Şəbəkə təhlükəsizliyinin təmin edilməsi probleminə “fraqmentlərlə” yanaşma |
|  | Şəbəkə təhlükəsizliyinin təmin edilməsi probleminə “kompleks” yanaşma |
|  | Təhlükə anlayışı  |
|  | Təsir məqsədlərinə görə təhlükələrin növləri |
|  | Digər əlamətlərinə görə təhlükələrin təsnifatı |
|  | Lokal şəbəkələrdə təhlükələr |
|  | Kriptologiya nədir  |
|  | Kriptoanaliz nədir |
|  | Kritoqrafik sistemlərin inkişaf tarixi |
|  | Kriptoqrafiyanın inkişaf tarixinin mərhələləri |
|  | Sadə kriptoqrafiya |
|  | Formal kriptoqrafiya |
|  | Elmi kriptoqrafiya |
|  | Kompüter kriptoqrafiyası |
|  | Kriptoqrafik sistəmlər və onlara qoyulan tələblər |
|  | Kriptoqrafik sistemin modeli |
|  | Kriptoqrafik şifrləmə üsulları |
|  | Kriptoqrafik sistemlərin davamlılığı |
|  | Nəzəri davamlılıq |
|  | Praktiki davamlılıq |
|  | Mükəmməl davamlılıq |
|  | Kriptoqrafik üsulların təsnifatı |
|  | Kodlaşdırma və ya gizli yazı |
|  | Simvol kodlaşdırması |
|  | Məna kodlaşdırması |
|  | Statistik sıxma üsulları |
|  | Adaptiv sıxma üsulları |
|  | Parçalama və dağıtma üsulları |
|  | Kriptoqrafik şifrləmə |
|  | Kriptoqrafik şifrləmə üsullarının (alqoritmlərinin) əlamətlərə görə təsnifatı |
|  | Kriptoqrafiya siyasətinin əsasistiqamətləri |
|  | Simmetrik (biraçarlı) şifrləmə üsulları |
|  | [Asimmetrik (ikiaçarlı) şifrləmə üsulları](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark657) |
|  | Asimmetrik şifrləməmdə əvəzləmə üsulları |
|  | Sadə şifrləmə üsullarının nümunələri  |
|  | Dolama-çubuq şifrələmə üsulu |
|  | Qoşa disk şifrələmə üsulu |
|  | Bibliya kodu şifrələmə üsulu |
|  | Polibiy kvadratı |
|  | Nömrələnmiş kvadrat |
|  | “Atbaş” şifrləməsi |
|  | Sezar şifri |
|  | Sadə əvəzetmə şifri |
|  | Qronefeld şifri |
|  | Kardanonun sehrli kvadratı |
|  | Elektron sənəd dövriyyəsi və autentifikasiya problemi |
|  | [Elektron imza texnologiyası](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark865) |
|  | Elektron imzanın açıq açarı |
|  | Elektron imzanın gizli açarı |
|  | Elektron imzanın yaradılması funksiyası |
|  | Elektron imzanın yoxlanması funksiyası |
|  | Biristiqamətli heş funksiyalar və onların qurulması [prinsipləri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark879) |
|  76. | Heş funksiya |
| 77. | Heş funksiyaya qoyulan tələblər |
| 78. | Biristiqamətli heş funksiyalarının qurulması [prinsipləri](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark879) |
| 79. | Açarların idarə olunması  |
| 80. | Açarların generasiyası |
| 81. | Açarların saxlanması |
| 82. | Açarların paylanması |
| 83. | Açıq açar infra­strukturu |
| 84. | Açıq açar infrastrukturunun informasiya təhlükəsizliyi sistemində həll etdiyi məsələlər  |
| 85. | Effektiv açıq açar infrastrukturunun yaradılması [metodikası](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark920) |
| 86. | Effektiv açıq açar infrastrukturunun yaradılması [metodikası](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C4%B0MTAHAN_SUALLARI.docx#bookmark920)nın mərhələləri |
| 87. | Steqanoqrafiya nədir |
| 88. | Steqanoqrafiyanın kateqoriyaları |
| 89. | Kompüter steqanoqrafiyası  |
| 90. | Kompüter steqanoqrafiyasının əsas prin­sipləri |
| 91. | Kompüter steqanoqrafiyasının geniş istifadə edilən üsulları |
| 92. | Kompüter steqanoqrafiyasının geniş istifadə edilən proqramları |
| 93. | Kompüterlərdə istifadə olunan formatların xüsusi xassələrinin istifadəsinə əsaslanan üsullar |
| 94. | Rəqəmli fotoşəkildə, rəqəmli səsdə və rəqəmli video­da izafiliyin istifadə edilməsinə əsaslanan üsulları |
| 95. | Müasir kompüter steqanoqrafiyasının əsas müddəaları |
| 96. | Klassik steqanoqrafiya  |
| 97. | Klassik steqanoqrafiyanın inkişaf tarixi |
| 98. | Klassik steqanoqrafik üsullar |
| 99. | Praktikada daha çox istifadə olunan klassiksteqanoqrafik üsullar |
| 100. | Tətbiq olunan mexanizm və vasitələrə görə steqanoqrafik üsulların kateqoriyaları |