**AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ**

**NAXÇIVAN DÖVLƏT UNİVERSİTETİ**

**Elektronika və informasiya texnologiyaları kafedrası**

**İxtisas qrupu:** Texnika elmləri

**İxtisas:** İnformasiyanın mühafizəsi üsulları və sistemləri, informasiya təhlükəsizliyi

**İxtisas şifrəsi**: 3339.01

**İxtisaslaşma:** İnformasiyanın mühafizəsi üsulları və sistemləri

**DOKTORANTURAYA QƏBUL ÜÇÜN İXTİSAS FƏNNİNDƏN**

**İMTAHAN SUALLARI**

1. İnformasiya təhlükəsizliyi anlayışı. İnformasiya təhlükəsizliyinin üç aspekti.
2. İnformasiya təhlükəsizliyi təhdidləri və onların təsnifatı.
3. Konfidensial informasiya və onun növləri. Dövlət sirri. Xidməti sirr və kommersiya sirri.
4. İnformasiya təhlükəsizliyi üzrə qanunvericilik tədbirləri. İnformasiya təhlükəsizliyi üzrə standartlar.
5. İnformasiya təhlükəsizliyi siyasəti. İnformasiya təhlükəsizliyi siyasətinin əsas növləri
6. Zərərli proqramların təsnifatı və yayılma üsulları. Antivirusların iş prinsipləri.
7. Elektron imza. Gücləndirilmiş elektron imza. Sertifikat və sertifikat xidmətləri mərkəzləri.
8. İdentifikasiya və autentifikasiya vasitələri. Biometrik texnologiyaların növləri
9. Girişə nəzarət modelləri. Rollar əsasında girişə nəzarət.
10. Protokollaşdırma və audit. Aktiv audit.
11. Şəbəkələrarası ekranların funksiyaları və iş prinsipləri. Şəbəkələrarası ekranların təsnifatı.
12. "Açıq sistem" anlayışı. OSI modeli. OSI modelinin səviyyələri.
13. Kompüter şəbəkələri. Şəbəkə topologiyaları və protokolları.
14. Ethernet texnologiyası. CSMA/CD texnologiyasının mahiyyəti. Ethernet kadrlarının formatları.
15. Lokal və qlobal şəbəkələr və onların proqram təminatı.
16. İnternet şəbəkəsi: arxitekturası, xidmətləri, şəbəkə protokolları, ünvanlaşdırma.
17. TCP/IP protokollar steki. TCP və UDP protokolları.
18. IP-protokolu. IP-protokolunun ünvan sxemi.
19. İnformasiya sisteminin arxitekturası. Lokal və paylanmış sistemlər.
20. Şəbəkədə məlumatların marşrutlaşdırılması. OSPF protokolunun iş prinsipi
21. Korporativ kompüter şəbəkələrinin ümumi xarakteristikası, tipik strukturu və yaradılması üçün zəruri komponentlər (İntranet).
22. Alqoritm və onun əsas xassələri. Alqoritmin təsviri üsulları. Verilənlərin strukturu.
23. Əməliyyat sistemlərinin (ƏS) ümumi xarakteristikaları. ƏS-nin nüvəsinin funksiyaları. Şəbəkə əməliyyat sistemləri.
24. Əməliyyat sistemlərində informasiya təhlükəsizliyinin əsas mexanizmləri
25. Aşağı və yüksək səviyyəli proqramlaşdırma dilləri. Kompilyatorlar və interpretatorlar. Obyektyönlü proqramlaşdırma texnologiyası.
26. Müasir proqramlaşdırma texnologiyaları. Struktur proqramlaşdırma. Funksional və məntiqi proqramlaşdırma.
27. Proqram təminatının təhlükəsizliyi. Proqram təminatının təhlükəsizliyinin təmin edilməsinin əsas prinsipləri
28. Verilənlər bazasının yaradılmasının ümumi prinsipləri: relyasion, iyerarxik və şəbəkə modelləri. Kompüter şəbəkələrində paylanmış verilənlər bazaları. Verilənlər bazasının idarəetmə sistemi (VBİS).
29. Verilənlər bazasının təhlükəsizliyinin təmin olunması vasitələri: VB-nin ehtiyat surətlərin yaradılması və bərpası vasitələri, VB sistemlərinə uzaqdan müraciət texnologiyaları, paylanmış VB sistemlərində nüsxələmə və sinxronlaşdırma.
30. Veb-texnologiyaları. Veb-proqramlaşdırma. Veb-xidmətlər.
31. İnformasiyanın texniki mühafizəsinin əsas məsələləri. İnformasiyanın texniki mühafizəsinin baza prinsipləri
32. Kriptoqrafiyanın əsas anlayışları: simmetrik şifrləmə, asimmetrik şifrləmə, rəqəmsal imza, heş funksiya, kriptoqrafik açar. Açıq açar və gizli açar.
33. Virtual xüsusi şəbəkələr
34. İnformasiya nəzəriyyəsi. İnformasiya anlayışı. Entropiya. Şərti entropiya. Qarşılıqlı informasiya və onun xassələri.
35. Xətti kodlar. Dövri kodlar. Xemminq kodu. Əlaqə kanalının riyazi modeli. Düz və əks kodlaşdırma teoremləri.
36. Qraflar nəzəriyyəsinin elementləri: qrafın tərifi, qrafın əlaqəlilik və insidentlik matrisləri.
37. Qraflarda marşrutlar, yollar, zəncirlər, tsikllər, konturlar. Əlaqəli və güclü əlaqəli qraflar.
38. Qraf üzərində ekstremal məsələlər: Deykstra alqoritmi.
39. Sonlu avtomatlar. Avtomatın keçid qrafı.
40. Kombinatorikanın əsas anlayışları (permutasiya, aranjeman, kombinezon). Cəmləmə və vurma qaydaları. Daxiletmə və çıxarma üsulu.
41. Ehtimalın klassik tərifi. Ehtimal fəzası. Şərti ehtimal. Ehtimalların vurulması teoremi. Ehtimalların toplanması teoremi. Bayes düsturu.
42. Təsadüfi kəmiyyətlər və onların paylanma funksiyaları. Normal paylanma.
43. Böyük ədədlər qanunu. Mərkəzi limit teoremi.
44. Markov zəncirləri.
45. Riyazi statistikanın əsas məsələləri. Variasiya sırası və onun statistik parametrləri (ədədi orta və dispersiya). Ən kiçik kvadratlar üsulu.
46. Statistik hipotezlərin yoxlanması.
47. Kütləvi xidmət nəzəriyyəsi: M/M/1 modeli.
48. Riyazi proqramlaşdırma məsələlərinin qoyuluşu. Məqsəd funksiyaları. Riyazi proqramlaşdırma məsələlərinin təsnifatı.
49. Şərtsiz optimallaşdırma məsələsinin qoyuluşu. Nyuton üsulu. Koordinat enişi üsulu. Ən tez eniş üsulu.
50. Şərti ekstremum məsələləri və Laqranj vuruqları üsulu. Lokal və qlobal ekstremum.
51. Xətti proqramlaşdırma məsələsinin qoyuluşu və həndəsi mənası. Xətti proqramlaşdırmanın düz və qoşma məsələləri. Simpleks-metodu.
52. Diskret proqramlaşdırma məsələsinin qoyuluşu. Tamqiymətli xətti proqramlaşdırma məsələləri. Budaqlar və sərhədlər üsulu.
53. İnformasiya təhlükəsizliyi anlayışı. İnformasiya təhlükəsizliyinin əsas aspektləri
54. Konfidensial informasiya və onun növləri. Dövlət sirri.
55. İnformasiya təhlükəsizliyi üzrə qanunvericilik tədbirləri. İnformasiya təhlükəsizliyi siyasəti.
56. Zərərli proqramların təsnifatı və yayılma üsulları. Antivirusların iş prinsipləri.
57. Elektron imza
58. Elektron dövlət konsepsiyası.
59. Kompüter şəbəkələri. Şəbəkə topologiyaları və protokolları.
60. Lokal və qlobal şəbəkələr və onların proqram təminatı.
61. İnternet şəbəkəsi: arxitekturası, xidmətləri, şəbəkə protokolları, ünvanlaşdırma. İnternetdə informasiya axtarışı.
62. İnformasiya texnologiyalarının və sistemlərinin təsnifatı.
63. İnformasiya anlayışı, onun formaları, təsvir üsulları
64. İnformasiya anlayışının xassələri, informasiyanın kəmiyyət ölçüsü
65. EHM-lərin yaranma tarixi və nəsilləri
66. Fərdi kompüterin quruluşu, əsas qurğuları və onların təyinatı
67. Fərdi kompüterin periferik (əlavə) qurğuları və onların təyinatı
68. Əməliyyat sistemlərinin növləri, funksiyaları
69. Əməliyyat sistemlərinin müxtəlif parametrlərə görə təsnifat
70. Windows əməliyyat sisteminin təyinatı və xüsusiyyətləri
71. Kriptoqrafiya anlayışı haqqında məlumat, şifrələmə metodu
72. Arxiv proqramlarının təyinatı və təsnifatı. Faylların arxivləşdirilməsi
73. Virusların növləri və antivirus proqramlarının təyinatı və təsnifatı
74. WinRar və WinZip proqramları haqqında ümumi məlumat
75. Təhlükəsizlik modelinin təyinatı və anlayışı
76. Kriptoqrafiyanın əsas anlayışları
77. İnformasiya təhlükəsizliyində standartların rolu
78. Təhlükə,hücum, pozma
79. İnformasiya mühafizəsinin metodları və vasitələri
80. Antivirus proqramları
81. Şifrələmə ilə kodlaşdırma
82. Kompüter virusları
83. Aparat və proqram mühafizəsi
84. Nitqin özəlliklərinə görə identifikasiya
85. Konfidensiallıq
86. İdentifikasiya və audentifikasiya
87. İnformasiya cəmiyyətinin əsas komponentləri
88. Elektron imza
89. Biometrik informasiya və identifikasiya
90. Simmetrik və assimetrik şifrələnmə
91. Kriptoqrafik metodlar
92. Kriptoqrafiya
93. İnformasiyanın kanallar vasitəsilə sızması
94. İnformasiya mühafizəsinin metodları və vasitələri
95. Təhlükəsizliyin pozulmasının nəticələri
96. Azərbaycan Respublikasında informasiya cəmiyyəti
97. İnformasiya təhlükəsizliyinə yönəlmiş təhlükələr
98. İnformasiya təhlükəsizliyində informasiyanın xüsusiyyətləri(konfidensiallıq,tamlıq,əlçatanlıq
99. Parolun təhlükəsizliyinin təmini
100. Biometrik mühafizə vasitələri, barmaq izinə görə identifikasiya

**Ədəbiyyat:**

1. Kərimov S.Q., Həbibullayev S.B., İbrahimzadə T.İ.  İnformatika*.*Ali məktəblər üçün dərslik. Bakı, 2009. 436 səh.
2. Kərimov S., Sərdarov Y. Kompyuter elminin nəzəri əsasları, Bakı, 2009, 290 səh.
3. Kərimov S.Q. İdarəetmənin informasiya texnologiyaları və korporativ informasiya sistemləri, Bakı, 2010, 426 səh.
4. Əliyev A.Y. İnformatika və proqramlaşdırma. Bakı, Mütərcim, 2008.
5. Hüseynov Ə. Ə. Diskret riyaziyyat. Dərs vəsaiti. Bakı: Çaşıoğlu, 2010. – 408 səh.
6. Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: İnformasiya texnologiyaları. 2006. 698 s.
7. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentləri. Bakı: “İnformasiya Texnologiyaları” nəşriyyatı, 2012, 219 səh.
8. Таненбаум Э.С. Компьютерные сети. 4-е изд. 2004, СПб, Издательский дом "Питер", 992 стр.
9. Stallings W., Cryptography and Network Security: Principles and Practice. Pearson; 6th edition, 2013, 752 p.

**Kafedra müdiri: tex.f.d. H.Ə.Qasımov**