AZƏRBAYCAN RESPUBLİKASI
ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ
YÜKSƏK TƏHSİL İNSTİTUTU

3339.01 - "İnformasiyanın mühafizəsi üsulları və sistemləri, informasiya təhlükəsizliyi (texnika sahəsi)" ixtisası üzrə fəlsəfə doktoru hazırlığının imtahan sualları

1. İnformasiya təhlükəsizliyi anlayışı. İnformasiya təhlükəsizliyinin üç aspekti
2. İnformasiya təhlükəsizliyi təhdidi anlayışı. Təhdidlərin əsas xarakteristikaları. Təhdidlərinin təsnifatı
3. Konfidensial informasiya və onun növləri. Dövlət sirri. Xidməti sirr və kommersiya sirri
4. Ziyanverici proqramlar. Kompüter virusları və şəbəkə soxulcanlarının müxtəlif sinifləri. Troyanlar və onların təsnifatı
5. Ziyanverici proqramların statik və dinamik analizi. Antivirus proqramlarının iş prinsipləri
6. Kiberhücumların təsnifatı. Hədəfyönlü hücumlar. "Cyber kill chain" modeli
7. Botnetlər və onların arxitekturası. DoS hücumların növləri. TCP SYN flooding hücumu DDoS hücum üçün üçsəviyyəli arxitektura. DDoS-hücumlardan müdafiə mexanizmləri
8. Paylanmış sistemlərdə informasiya təhlükəsizliyi funksiyaları. İdentifikasiya və autentifikasiya. Girişə nəzarət. Girişə nəzarət siyahıları. Rollar əsasında girişə nəzarət
9. İnformasiya təhlükəsizliyi risklərinin idarə edilməsi. Risklərin kəmiyyət və keyfiyyət qiymətləndirilməsi. Risklərin emalına yanaşmalar
10. İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi. İnsidentlərin emalı prosesinin mərhələləri. CERT-komandaları və onların funksiyaları
11. İnformasiya təhlükəsizliyi üzrə qanunvericilik. Azərbaycan Respublikasında kritik informasiya infrastrukturunun təhlükəsizliyinin təmin edilməsi sahəsində qanunvericilik
12. İnformasiya təhlükəsizliyi üzrə standartlar. ISO/IEC 27001 standartı. PDCA modeli
13. İnformasiya təhlükəsizliyinin auditi və onun mərhələləri. Standarta uyğunluğun auditi. Nüfuzetmə testləri anlayışı
14. İnformasiya təhlükəsizliyinin təşkilati təminatı. İnformasiya təhlükəsizliyi siyasəti. İnformasiya təhlükəsizliyi siyasətinin əsas növləri
15. Şəbəkələrarası ekranların funksiyaları və iş prinsipləri. Şəbəkələrarası ekranların təsnifatı
16. Kriptoqrafiyanın əsas anlayışları. Klassik şifrlər: sadə əvəzetmə və yerdəyişmə şifrləri. Vijener şifri. Vernam şifri
17. Simmetrik blok şifrləri. Şifrlərin qurulması üçün Şennon prinsipləri. Feystel şəbəkəsi. DES (Data Encryption Standard) standartı
18. AES (Advanced Encryption Standard) şifrləmə standartı. AES alqoritminin strukturu.
19. Blok şifrlərin iş rejimləri: ECB, CBC, CFB, OFB və CTR
20. Açıq açarlı kriptoqrafiyanın əsas anlayışları. RSA kriptosistemi: açarların generasiyası, şifrləmə və deşifrləmə alqoritmləri
21. Diskret loqarifm məsələsi və ona əsaslanan kriptosistemlər. Diffi-Hellman açar mübadiləsi sxemi
22. Rəqəmsal imza sxemi və onun növləri. ElGamal imza sxemində imzalama və imzanı yoxlama alqoritmləri
23. Kriptoqrafik heş funksiyaların tərifi, xassələri və qurulmasının əsas prinsipləri. "Ad günü" hücumu

24. SHA-1 heş funksiyası. Məlumatı autentifikasiya kodları. Açarlı heş funksiyalar (HMAC)
25. Elektron imzanın tərifi və funksiyaları. Açıq açarlar infrastrukturunun komponentləri. Açıq açarlar infrastrukturunun modelləri
26. Şəbəkə təhlükəsizliyinin kriptoqrafik protokolları. IPSec protokolu. SSL protokolu
27. Virtual xüsusi şəbəkələr. Virtual xüsusi şəbəkə protokolları
28. Əməliyyat sistemlərinin (ƏS-nin) ümumi xarakteristikaları. ƏS-nin nüvəsinin funksiyaları. ƏS-nin təsnifatı. Şəbəkə əməliyyat sistemləri
29. Əməliyyat sistemlərində informasiya təhlükəsizliyinin əsas mexanizmləri
30. Proqram təminatının təhlükəsizliyi. Boşluqların idarə edilməsinin həyat dövrü. Boşluqların qiymətləndirilməsinə yanaşamlar (CVSS metodikası)
31. Kompüter şəbəkələri. Şəbəkə topologiyaları. Lokal və qlobal şəbəkələr. Ethernet texnologiyası
32. OSI modeli. OSI modelinin səviyyələri
33. TCP/IP protokollar steki. TCP və UDP protokolları
34. IP-protokolu. IP-protokolunun ünvan sxemi. DNS xidməti
35. Veb təhlükəsizlik təhdidləri (OWASP 2021 üzrə). SQL inyeksiyanın növləri. SQL inyeksiya alətləri və əks-tədbirlər
36. Müasir proqramlaşdırma texnologiyaları. Obyektyönlü proqramlaşdırmanın əsas konsepsiyaları
37. İnformasiya anlayışı. İnformasiyanın miqdarı. Entropiya. Şərti entropiya
38. Verilənlər bazalarının relyasiya, iyerarxik və şəbəkə modelləri. Verilənlər bazasını idarəetmə sistemləri (VBİS). NoSQL bazaları
39. VBİS-lərdə istifadəçi profilləri, parol siyasətləri, icazə (hüqüq) və rolların idarə edilməsi.
40. Paylanmış VBİS-lərdə ehtiyat nüsxələmə, sinxronlaşdırma və yükün balanslaşdırılması üsulları
41. Müdaxilələrin aşkarlanması sistemləri və onların komponentləri. Müdaxilələrin aşkarlanmasının host və şəbəkə sistemləri. Honeypot sistemləri
42. Qraflar nəzəriyyəsinin elementləri: qrafın tərifi, qrafların növləri. Qrafın əlaqəlilik və insidentlik matrisləri. Deykstra alqoritmi
43. Matrislər üzərində əməllər. Minor və cəbri tamamlayıcı anlayışı. Determinant və onun xassələri. Tərs matris və onun varlığı
44. Ehtimalın klassik tərifi. Şərti ehtimal. Bayes düsturu
45. Təsadüfi kəmiyyətlər. Paylanma funksiyası. Bəzi paylanma qanunları (binomial, Puasson). Normal paylanma
46. Riyazi statistikanın əsas məsələləri. Variasiya sırası və onun statistik parametrləri (ədədi orta və dispersiya)
47. Paylanma parametrlərinin statistik qiymətləndirilməsi. Nöqtəvi qiymətləndirmə. İnam intervalının qurulması. Statistik hipotezlərin yoxlanması. Pirson kriteriyası
48. Korrelyasiya analzinin əsas elementləri. Reqressiya analizi. Ən kiçik kvadratlar üsulu
49. Riyazi proqramlaşdırma məsələsinin komponentləri. Riyazi proqramlaşdırma məsələlərinin təsnifatı
50. Xətti proqramlaşdırma (XP) məsələsinin qoyuluşu və yazılış formaları. XP məsələsinin həndəsi mənası. XP haqqında teoremlər (isbatsız)

ƏDƏBİYYAT

1. Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentləri. Bakı: İnformasiya texnologiyaları, 2012, 212 s.
2. Əliyev F.N., Mikayılov C.İ., Əliyev Y.N. Statistika. Dərslik. Bakı, 2015, 240 s.
3. Hüseynov Ə.Ə. Diskret riyaziyyat. Dərs vəsaiti. Bakı: Çaşıoğlu, 2010. 408 s.

4. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: MTN-in nəşriyyat-poliqrafiya mərkəzi. 2009, 340 s.
5. Hoffman A. Web application security: Exploitation and countermeasures for modern web applications. O'Reilly Media, 2020, 330 p.
6. Sinha S.M. Mathematical programming: Theory and methods. 2006, 572 p.
7. Stallings W. Cryptography and network security: Principles and practice (6th edition). Wiley, 2013, 752 p.
8. Tanenbaum A.S., Computer networks, 5th edition. Prentice Hall, 2010, 960 p.