Predmet: Zaštita IS i podataka

-pitanja za ispit-

PRVI DEO

Poglavlje 2.

1. Pojam i ciljevi zaštite

Poglavlje 3.

2. Jedinstvene osnove zaštite
3. Zaštita privatnosti
4. Zaštita intelektualne svojine
5. Sankcionisanje računarskog kriminala

Poglavlje 4.

6. Upravljanje zaštitom
7. Analiza rizika
8. Objekti koje treba štititi
9. Moguće pretnje-opasnosti
10. Moguće posledice
11. Mere zaštite.

Poglavlje 5.

12. Zloupotreba informacionih tehnologija
13. Vrste zloupotrebe informacionih tehnologija
14. Krađe, Pronevere, Prevare, Falsifikovanje, Iznude i ucene, Narušavanje privatnosti u IT okruženju.
15. Tehnike realizacije zloupotrebe informacionih tehnologija
16. Unošenje i priprema ulaznih podataka za obradu
17. Manipulacija izlaznim podacima
18. Programiranje kao način zloupotrebe IT
19. Tehnika "seckane salame" ("Salami swindle")
20. Lovac, Hvatač ("Sniffer" programi)
21. Pismo-bomba ("Letter bomb", "E-mail bomb")
22. Nadmudrivanje ("Spoofing)
23. Trojanski konj ("Trojan horse")
24. Prikriveni ulaz ("Trap Door")
25. Logička ili vremenska bomba ("Logic or time bomb")
26. Prikupljanje "otpadaka" ("Scavenging")
27. Virusi i crvi ("Viruses and worms")
28. Zloupotrebe IT u prenosu/komunikacijama
29. Ometanje servisa ("Denial of services")
30. Amateri u kiber kriminalu
31. Profesionalci u kiber kriminalu
32. Hakeri

DRUGI DEO

Poglavlje 6.

33. Fizičko-tehnički segmenti zaštite.
34. Zaštita magnetnih nosilaca podataka (klase podataka).
35. Elektronsko obezbeđenje (kompletno poglavlje 6.2)

Poglavlje 9.

36. Identifikacija i verifikacija.
37. Lozinke (kompromitacija, nadzor i zaštita).
38. Autorizacija – objašnjenje pojma i specifikacija (bez 9.3.2).

Poglavlje 10.

39. Kriptografija (klasične kriptografske metode, kodiranje, šifriranje (cezarova šifra))
40. Moderne kriptografske tehnike (10.1.2.3, i 10.1.2.4)
41. Digitalni potpis i digitalni sertifikat.
42. Zaštita od računarskih virusa