

ZÁRÓVIZSGA KÉRDÉSEK

RENDSZERBIZTONSÁG

1. Az IT-rendszer fenyegetettsége, az IT-biztonság értelmezése, elemei.
2. A vállalat IT-biztonsági rendszerének kialakítása, biztonságpolitika szerepe, dokumentumai.
3. Az IT-rendszer biztonságának tanúsítása. A belső- és a külső audit megvalósítása, szabványok.
4. Kockázatok elemzése és kezelése, kockázatmenedzsment.
5. Az információ védelme. Biztonsági mechanizmusok. A kriptológia fogalma, összetevői. A kriptomodell, a kriptográfia módszerei.
6. A kriptográfia biztonsága. Támadás és védekezés az üzenet feltörési kísérletei ellen. Feltételes és feltétel nélküli biztonság.
7. A negyedik generációs rejtjelezési eljárások jellemzői. Shanon javaslata.
8. A DES és DES-alapú eljárások.
9. Nyilvános kulcsú titkosítás - RSA.
10. Ismertesse az SSH szabványcsalád szerepét és felépítését!
11. A Kriptoprotokollok szerepe az IT-biztonság területén.
12. A PKI-technológia. Alapok, szerepe, PKI-szolgáltatások.
13. Az IT-biztonság követelményeinek érvényesítése a rendszer tervezésekor.