ПЕРЕЛІК ЗАПИТАНЬ
до диференційованого заліку
з дисципліни «Безпека інформаційно-комунікаційних систем»

1. Поясніть різницю між термінами «автоматизована система», «інформаційно-комунікаційна система».
2. Основні особливості процесів ідентифікації та автентифікації.
3. На порушення яких властивостей інформації та системи спрямована загроза прослуховування трафіку?
4. Назвіть загрози, які розглядаються в моделі STRIDE.
5. Які з наявних способів реалізації загрози розглядаються в моделі загроз?
6. Модель порушника: особливості побудови.
7. Назвіть типові рівні інформаційно-комунікаційної системи.
8. Дайте визначення функціонального сервісу безпеки.
9. Які механізми захисту впроваджують на рівні захисту від НСД до ресурсів системи?
10. Які механізми захисту впроваджують на рівні захисту від несанкціонованого використання ресурсів системи?
11. Які механізми захисту впроваджують на рівні захисту від некоректного використання ресурсів системи?
12. Які механізми захисту впроваджують на рівні внесення інформаційної та функціональної надлишковості?
13. Який рівень захисту забезпечує захист конфіденційності інформації?
14. Назвіть типові підсистеми КЗЗ.
15. Яке завдання виконує підсистема ідентифікації та автентифікації?
16. Назвіть основні причини появи вразливостей у сучасних інформаційно-комунікаційних системах.
17. На яких етапах життєвого циклу ІКС можуть виникати вади захисту? Охарактеризуйте типові вади для кожного з етапів.
18. За якими головними ознаками доцільно класифікувати шкідливе програмне забезпечення?
19. Які класи шкідливого програмного забезпечення можна виділити за механізмами їх розповсюдження?
20. Що таке програмні закладки? Наведіть класифікацію програмних закладок.
21. Яким чином може здійснюватися керування ботнетом?
22. Які головні ознаки мають комп'ютерні віруси?
23. Наведіть класифікацію комп'ютерних вірусів.
24. У чому полягає особлива небезпека завантажувальних (бутових) вірусів?
25. Назвіть основні технології виявлення комп'ютерних вірусів. Які переваги й недоліки має кожна з цих технологій?
26. Які головні ознаки мережних хробаків, що вирізняють їх з-поміж інших шкідливих програм?
27. За якими ознаками класифікують мережних хробаків?
28. Назвіть стратегії проникнення на віддалені комп'ютери, які реалізовував хробак Морріса.
29. Які програмні засоби дістали назву «троянські коні»? Наведіть їх класифікацію.
30. Які програми можуть належати до спеціальних хакерських утиліт?
31. Що таке відкриті системи і які вони мають переваги?
32. Назвіть відомі Вам стеки мережних протоколів, і розкажіть про їх призначення.
33. Які проблеми безпеки можуть виникнути через протокол FTP?

34. Які засоби контролю і захисту сесії впроваджено у протоколі TCP?
35. Як реалізовано передбачення номерів TCP-послідовності, і для чого це використовують?
36. У чому полягає атака IP spoofing і як їй можна запобігти?
37. Які помилки оброблення фрагментованих пакетів можна було зустріти в мережних ОС і до яких наслідків призводило використання цих помилок?
38. Сформулюйте вимоги до архітектури захищених мереж.
39. Які топології мереж сприяють побудові захищених мереж, а які - ні?
40. У який спосіб створюють віртуальні локальні мережі?
41. На яких рівнях мережної взаємодії можна реалізовувати міжмережні екрани?
42. Які переваги мають пакетні фільтри?
43. Наведіть приклад шлюзу мережного рівня.
44. Які переваги мають шлюзи прикладного рівня?
45. Назвіть основні способи обходу мережних екранів.
46. Мережні екрани якого рівня дають змогу застосовувати трансляцію мережних адрес?
47. Назвіть три складові технології виявлення атак.
48. Які основні методи аналізу даних для пошуку атак?
49. Що таке сканер безпеки? Які принципи його роботи?
50. Дайте визначення VPN. Які завдання захисту вирішує VPN?
51. Де можуть бути розміщені кінцеві точки захищених тунелів? Назвіть переваги й недоліки всіх варіантів.
52. На яких рівнях моделі OSI можна реалізувати VPN? Назвіть переваги й недоліки всіх варіантів.
53. У яких випадках найчастіше використовують протокол SSL/TLS?
54. Які функції виконує протокол SOCKS?
55. Назвіть рівні, визначені в архітектурі IPsec.
56. Поясніть різницю між протоколами AH і ESP.
57. Чим режим тунелювання відрізняється від транспортного режиму?
58. Які функції виконує протокол IKE?
59. Які протоколи забезпечують утворення VPN на канальному рівні?