**Питання і завдання до іспиту з дисципліни «Інформаційна безпека» - 2018в**

1. Основні поняття інформаційної безпеки

2. Способи і засоби захисту інформації

3. Методи дослідження ІБ підприємства. Перерахуйте і охарактеризуйте компоненти архітектури безпеки

4. Основні законодавчі акти (українські, британські, російські та міжнародні стандарти в області ІБ, помаранчева книга). Структура, зміст, призначення

5. Уразливості інформаційних систем. Поняття, особливості, класифікація

6. Загрози інформаційної безпеки. Види загроз. Основні загрози цілісності. Основні загрози доступності.

7. Поняття і сутність зовнішніх і внутрішніх загроз. Розкрити суть поняття та навести приклади

8. Поняття «ризик інформаційної безпеки». Класифікація ризиків.

9. Механізми оцінювання ризиків інформаційної безпеки.

10. Методики оцінки ризиків ІБ. Способи кількісної оцінки величини ризику.

11. Етапи управління ризиками. Управління ризиками та життєвий цикл інформаційної системи.

12. Коротка характеристика сучасних пакетів управління ризиками та їх особливості (СRAMM, RiskWatch, Digital Security Office 2006

13. Назвіть і охарактеризуйте предмет і основні поняття криптології. Етапи розвитку криптографії. Особливості сучасного етапу розвитку криптографії.

14. Симетричне шифрування. Визначення опис найбільш відомих симетричних алгоритмів. Класифікація. (AES, Blowfish, ГОСТ 28147-89, CAST, DES Калина).

15. Асиметричні алгоритми шифрування. Особливості асиметричних алгоритмів. Класифікація. Приклади. (RSA, DSA, Elgamal або Diffie-Hellman).

16. Основні відмінності, переваги та недоліки принципів симетричного і асиметричного шифрування.

17. Поняття «Політики інформаційної безпеки». Сфери дії політик інформаційної безпеки. Рівні політик безпеки і їх цілі. Порядок побудови політики ІБ організації

18. Склад та основні частини систем ідентифікації й аутентифікації. Поняття стійкості систем аутентифікації. Параметри визначення стійкості та основні вимоги до вибору пароля.

19. Дискреційна політика безпеки. Матриця доступу та операції над нею при зміні прав доступу. Опишіть та поясніть сутність, наведіть приклади

20.Особливості і загальний опис алгоритму шифрування «Калина».

21. Поняття «ризики інформаційної безпеки». Класифікація ризиків.

22. Складові інформаційної безпеки. Поняття доступності, цілісності і конфіденційності інформації.

23. Адміністративний рівень забезпечення інформаційної безпеки. Цілі, задачі і зміст адміністративного рівня. Принципи розробки політик інформаційної безпеки

24. Класифікація погроз інформаційної безпеки. Класи погроз. Канали несанкціонованого доступу до інформації.

25. Визначення понять "ідентифікація" та "аутентифікація". Механізм ідентифікації і аутентифікації користувачів

26. Класифікація систем шифрування даних. Симетричні і асиметричні методи шифрування. Переваги та недоліки.

27.Визначення і зміст аудиту безпеки інформаційних систем. Етапи і методи проведення аудиту інформаційної системи

28. Методи аналізу програмних реалізацій й їх особливості

29. Методи розмежування доступу. Мандатне і дискретне управління доступом