## Технологии защиты в государственных информационных системах

**Вопросы для проведения промежуточной аттестации (зачет)**

1. Информация. Основные свойства информации с точки зрения ее защиты.
2. Понятие информационной системы. Системы связи и обмена информацией.
3. Классификации информационных систем.
4. Государственные информационные системы.
5. Угрозы защищаемой информации и каналы утечки.
6. Определение уровня значимости информации.
7. Определение класса защищенности информационной системы.
8. Оценка угроз безопасности информации.
9. Выбор мер защиты информации для государственной информационной системы.
10. Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе.
11. Определение базового набора мер защиты информации.
12. Адаптация базового набора мер защиты информации.
13. Уточнение адаптированного базового набора мер защиты информации.
14. Дополнение уточненного адаптированного базового набора мер защиты информации.
15. Применение компенсирующих мер защиты информации
16. Основные положения стратегии национальной безопасности Российской Федерации.
17. Основные положения доктрины информационной безопасности Российской Федерации..
18. Нормативное обеспечение информационной безопасности США.
19. Нормативное обеспечение информационной безопасности Франции.
20. Нормативное обеспечение информационной безопасности Китая.
21. Нормативное обеспечение информационной безопасности в странах постсоветского пространства.
22. Обзор отечественных нормативных правовых актов, регламентирующих обеспечение безопасности информационных систем.
23. Политика безопасности: разработка и использование
24. Оценка эффективности политики безопасности.
25. Разделение прав доступа: идентификация и аутентификация.
26. Определение качества защиты информационной системы.
27. Парольная защита. Правила составления паролей.
28. Установка парольной защиты на документы.
29. Дискреционная политика доступа.
30. Различие физиологических и поведенческих параметров биометрических систем контроля доступа.
31. Видов пластиковых карт доступа.
32. Оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа.
33. Защита информации при авариях и иных экстремальных ситуациях.
34. Вредоносное программное обеспечение: классификация и защита.
35. Шифрование. Виды шифрования: симметричное и асимметричное.
36. Алгоритмы шифрования.
37. Кодирование информации.
38. Архивирование информации. Создание резервных копий.
39. Работа с электронной подписью.
40. Электронная подпись. Сертификат электронной подписи.
41. Алгоритм получения цифровой подписи.
42. Законодательные требования к удостоверяющим центрам.
43. Защита структур (файлов и папок), сохраняемых на носителях.
44. Контейнерная защита.
45. Особенности записи информации на внешние носители. Коды Рида-Соломона.