2018 Вопросы к экзамену по защите информации

1. Необходимость защиты информации. Понятия «информационная безопасность», «защита информации».
2. Составляющие информационной безопасности. Понятия «уязвимость», «риск» и «окно опасности».
3. Основные угрозы доступности.
4. Основные угрозы целостности.
5. Основные угрозы конфиденциальности.
6. Политика безопасности как административный документ.
7. Управление рисками.
8. Управление персоналом и информационная безопасность.
9. «Оранжевая книга». Основные определения.
10. «Оранжевая книга». Классы безопасности.
11. Архитектурная безопасность информационных систем.
12. Классификация удаленных атак.
13. Российская классификация информационных систем.
14. Классификация СУиК ЯМ Госкорпорации «Росатом».
15. Сертификация и аттестация СУиК ЯМ. Органы сертификации.
16. Сертификационные требования 3 класса СУиК ЯМ.
17. Аттестационные требования 3 класса СУиК ЯМ.
18. Идентификация, аутентификация, авторизация. Парольная аутентификация.
19. Аутентификация с помощью биометрических данных.
20. Управление доступом. Матрица доступа.
21. Дискреционное и мандатное управление доступом. Списки доступа.
22. Ролевое управление доступом.
23. Протоколирование и аудит.
24. Активный аудит.
25. Симметричное шифрование как сервис безопасности.
26. Асимметричное шифрование как сервис безопасности.
27. Контроль целостности с помощью шифрования. ЭЦП.
28. Экранирование как сервис безопасности.
29. Межсетевой экран как сервис безопасности.
30. Основные понятия криптографии: открытый текст, шифртекст, зашифрование, расшифрование, ключ, криптосистема, дешифрование, криптоанализ.
31. Основные понятия криптографии: гамма шифра, гаммирование, абсолютно стойкий шифр, диффузия, конфузия.
32. Схема одного раунда алгоритма шифрования DES.
33. Схема функции шифрования алгоритма шифрования DES.
34. Преобразования ключа в раунде алгоритма шифрования DES.
35. Алгоритм асимметричного шифрования RSA.
36. Типовая удаленная атака: отказ в обслуживании.