

## 2019 Вопросы билетов к экзамену по защите информации

12 билетов по 3 вопроса в каждом.

Вопросы билетов:

1. Понятие информационной безопасности и защиты информации. Составляющие информационной безопасности.
2. Угрозы информационной безопасности. Уязвимость, риск, окно опасности.
3. Классификация угроз. Основные угрозы доступности.
4. Классификация угроз. Основные угрозы целостности.
5. Классификация угроз. Основные угрозы конфиденциальности.
6. Уровни обеспечения информационной безопасности.
7. Административный уровень. Политика безопасности и программа безопасности.
8. Административный уровень. Управление рисками.
9. Процедурный уровень. Управление персоналом.
10. Процедурный уровень. Физическая защита.
11. Процедурный уровень. Поддержание работоспособности.
12. «Оранжевая книга». Доверенная вычислительная база. Механизмы безопасности. Классы безопасности.
13. Российская классификация автоматизированных систем.
14. Требования к АС. Подсистема управления доступом.
15. Требования к АС. Подсистема регистрации и учета.
16. Требования к АС. Подсистема Криптографическая подсистема.
17. Требования к АС. Подсистема обеспечения целостности.
18. Классификация СУиК ЯМ Госкорпорации «Росатом».
19. Сертификационные требования 3 класса СУиК ЯМ.
20. Аттестационные требования 3 класса СУиК ЯМ.
21. Идентификация, аутентификация, авторизация. Парольная аутентификация.
22. Одноразовые пароли.
23. Аутентификация с помощью биометрических данных.
24. Управление доступом. Матрица доступа.
25. Дискреционное и мандатное управление доступом. Списки доступа.
26. Ролевое управление доступом.
27. Протоколирование и аудит. Активный аудит.
28. Симметричные и асимметричные алгоритмы шифрования.
29. Контроль целостности. ЭЦП. Цифровые сертификаты.
30. Экранирование как сервис безопасности.
31. Защита локальных сетей при помощи межсетевых экранов.
32. Основные понятия криптографии: открытый текст, шифртекст, шифрование, расшифрование, ключ, криптосистема, дешифрование, криптоанализ, гамма шифра, гаммирование, абсолютно стойкий шифр, диффузия, конфузия.
33. Схема одного раунда алгоритма шифрования DES.
34. Схема функции шифрования алгоритма шифрования DES.
35. Преобразования ключа в раунде алгоритма шифрования DES.
36. Режимы шифрования.