# Перечень вопросов к экзамену по дисциплине «Информационная безопасность»

1. Система правового обеспечения защиты информации РФ. Виды тайн.
2. ФЗ №152 «О персональных данных»: область действия закона, основные понятия и термины, используемые в законе, механизмы защиты персональных данных.
3. ФЗ № 98 «О коммерческой тайне»: область применения, понятие коммерческая тайна и механизмы ее защиты.
4. Понятие «информационная безопасность» и механизмы ее обеспечения.
5. Основные механизмы защиты информации.
6. Конфиденциальность информации и механизмы ее обеспечения.
7. Целостность информации и механизмы ее обеспечения.
8. Доступность информации и механизмы ее обеспечения.
9. В каких случаях используются механизмы достоверности, неотказуемости и неизменяемости информации?
10. Какие направления включает в себя комплекс мер по защите информации ?
11. Понятие «угрозы информационной безопасности». Статистика и примеры угроз. Проблемы моделирования угроз.
12. Понятие «уязвимость информационной системы». Примеры уязвимостей.
13. Методы идентификации и аутентификации пользователя в информационных системах.
14. Как хранить и передавать пароли?
15. Методы разграничения доступа к информационным активам организации.
16. Что такое криптографическая хэш-функция и какими свойствами она обладает ?
17. Какие задачи решают с использованием смарт-карт и какие проблемы при этом могут возникать ?
18. Методы биометрии, используемые при реализации механизма конфиденциальности информации. Краткая характеристика, достоинства и недостатки.
19. Симметричные криптографические алгоритмы и принципы их работы. Примеры реализации симметричных криптографических алгоритмов.
20. Проблемы использования симметричных криптосистем.
21. Асимметричные криптографические алгоритмы и принципы их работы. Примеры реализации.
22. Проблемы использования асимметричных криптосистем.
23. Методы защиты внешнего периметра информационных систем и их краткая характеристика.
24. Криптографические методы обеспечения целостности информации: цифровые подписи, криптографические хэш-функции, коды проверки подлинности. Краткая характеристика методов.
25. Цифровые сертификаты и технологии их использования в электронной цифровой подписи.
26. Механизм обеспечения достоверности информации с использованием электронной цифровой подписи.
27. Механизмы построения системы защиты от угроз нарушения доступности.
28. Механизмы построения системы защиты от угроз нарушения неизменяемости информации и неотказуемости действий персонала с информацией.
29. Формы проявления компьютерных угроз.
30. Понятие «вредоносная программа». Классификация вредоносных программ.
31. Краткая характеристика вредоносных программ: эксплойтов, кейлоггеров и бэкдоров.
32. Краткая характеристика вредоносных программ: руткитов, троянов и бот-сетей.
33. Механизмы заражения вирусами.
34. Основные функции классических компьютерных вирусов.
35. Сетевые черви: механизм заражения и основные функции.
36. DDOS –атаки: механизмы и последствия.
37. Бот-сети: механизм создания и управления сетью. Возможные последствия.
38. Рекомендации по защите от вредоносного кода.
39. Методы борьбы со спамом.
40. Как осуществляется расследование инцидентов информационной безопасности ?
41. Чем отличается защита персональных данных от коммерческой тайны ?
42. Электронная подпись и механизмы ее реализации.
43. Защита персональных данных.
44. Что мы понимаем по термином «персональные данные» ?
45. Банковская тайна - технологии и организация ее защиты.
46. Какие стратегии анализа рисков используются при моделировании рисков и принятии решения на создания системы информационной безопасности ?
47. Рекомендации по защите от вредоносного кода.
48. Методы борьбы со спамом.
49. Безопасность работы в социальных сетях: угрозы, механизмы защиты.
50. Как обеспечивается непрерывность бизнеса в системах защиты информации.