**Вопросы по ИБ экзамен**

1. Роль и место гуманитарных наук в системе глубинно-сущностного объяснения мира.
2. Исторические аспекты развития концепции информационных войн.
3. Поведенческая война, как новый этап информационного противоборства.
4. Первая мировая война.
5. Период между первой и второй мировыми войнами
6. Вторая мировая война.
7. Почему СССР победил во второй мировой войне
8. Период между второй и третьей мировыми войнами
9. Третья мировая война.
10. Интерес к сектам и оккультным псевдооздоровительным практикам.
11. Профиль пользователя Интернета.
12. Секты в Интернете.
13. Методы работы вербовщиков ДАИШ.
14. Реализация технологий формирования и управления поведением
15. Сущность социальной инженерии и ее место в социальном проектировании.
16. Основная схема воздействия в социальной инженерии
17. Основные отличия социальной инженерии от социального программирования
18. Об истории социальной инженерии
19. Основные области применения социальной инженерии
20. Возможность образования технических каналов утечки информации в системах, средствах информатизации и связи
21. Модель технического канала утечки
22. Определение размеров контролируемой зоны
23. Побочные излучения технических средств обработки информации
24. ПКУИ по цепям заземления
25. Канал утечки по цепям электропитания
26. Виброакустический канал утечки информации
27. Высокочастотное облучение
28. Высокочастотное навязывание
29. Меры защиты от ПКУИ
30. Основные понятия криптографии
31. Алгебраические модели шифров.
32. Вероятностные модели шифров.
33. Математические модели открытых сообщений.
34. Теоретико-информационный подход к оценке криптостойкости шифров.
35. Практическая стойкость шифров.
36. Имитостойкость шифров. Имитация и подмена сообщения.
37. Способы обеспечения имитостойкости.
38. Помехостойкость шифров.
39. Практические вопросы повышения надежности.
40. Виды симметричных шифров. Особенности программной и аппаратной реализации.
41. Принципы построения блочных шифров.
42. Современные блочные криптоалгоритмы.
43. Принципы построения поточных шифров
44. Современные поточные криптоалгоритмы.
45. Режимы использования шифров.
46. Математические основы асимметричной криптографии.
47. Криптосистема RSA.
48. Взаимосвязь компонентов RSA.
49. Криптосистема Эль-Гамаля.
50. Криптосистема Рабина.