Перечень вопросов для вступительного испытания.

1. Место информационной безопасности в системе национальной безопасности.
2. Современная концепция информационной безопасности.
3. Цели и концептуальные основы защиты информации.
4. Критерии, условия и принципы отнесения информации к защищаемой.
5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
6. Понятие и структура угроз защищаемой информации.
7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
8. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
9. Виды уязвимости информации и формы ее проявления.
10. Каналы и методы несанкционированного доступа к конфиденциальной информации.
11. Методологические подходы к защите информации и принципы организации.
12. Системы защиты информации.
13. Основные подходы к защите данных от несанкционированного доступа.
14. Методы и средства ограничения доступа к компонентам ЭВМ.
15. Законодательства, регулирующие правоотношения в сфере коммерческой, служебной тайн.
16. Модель нарушителя ИБ.
17. Дерево угроз.
18. Формальная теория защиты информации: основные определения.
19. Методы обеспечения целостности информации. Примеры.
20. Классификация методов аутентификации.
21. Особенности парольных методов и угрозы их безопасности.
22. Структура системы защиты от угроз нарушения целостности.
23. Структура системы защиты от угроз нарушения доступности.
24. Резервирование ресурсов ИТ инфраструктуры.
25. Классификация стандартов в области ИБ.
26. Оранжевая книга.
27. Руководящие документы Гостехкомиссии России.
28. Недостатки стандартов ИБ первого поколения.
29. Общие критерии (ОК).
30. Категории пользователей и среда безопасности в ОК.