Примерный перечень вопросы для подготовки к государственному экзамену 10.03.01 (2026 г.)

1. Сущность и содержание информационной безопасности в системе национальной безопасности Российской Федерации. Доктрина информационной безопасности РФ. (Утверждена Указом Президента РФ от 05.12.2016 г. № 646.)
2. Основные положения государственной информационной политики Российской Федерации.
3. Национальные интересы в информационной сфере. Обеспечение интересов личности в области информационной безопасности. Стратегия национальной безопасности РФ. (Утверждена Указом Президента РФ № 400 от 02.07.2021 г.)
4. Сущность и содержание статей Конституции Российской Федерации по вопросам информационной безопасности.
5. Цель, задачи и содержание Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".
6. Цель, задачи и содержание Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".
7. Сформулируйте основные требования, предъявляемые к системе стандартизации в области защиты информации. Назовите известные вам системы стандартов в этой области, принятые в России и за рубежом.
8. Механизмы, виды и способы защиты информации
9. Силы и средства обеспечения информационной безопасности.
10. Способы и средства защиты информации
11. Назовите основные принципы защиты информации от несанкционированного доступа? В чем заключается суть каждого из них?
12. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
13. Раскрыть принципы процессного подхода в управлении ИБ.
14. К каким процессам организации может быть применена циклическая модель PDCA? Приведите пример
15. Приведите отличительные черты стандартов серии ISO/IEC 27000.
16. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ? Кратко охарактеризуйте этот стандарт.
17. В каком стандарте серии ISO/IEC 27000 описана инфраструктура руководства ИБ? Кратко охарактеризуйте этот стандарт.
18. Преимущества использования (учета) требований российских и международных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ
19. Преимущества одновременного учета требований стандартов, предъявляемых как к СУИБ в целом, так и к отдельным процессам, разрабатываемым в рамках СУИБ.

20. Содержание стандартов серии СТО БР ИББС в рамках развития стандартизации управления ИБ в России.
21. Понятия политики обеспечения ИБ и политики ИБ организации
22. Иерархия документов в области УИБ для организации БС РФ.
23. Сущность и содержание политики информационной безопасности организации.
24. Какова роль государственной политики в области обеспечения информационной безопасности? Какие государственные органы отвечают за защиту информации, перечислите их функции и полномочия в вопросах информационной безопасности.
25. Понятие «правовая защита информации», основные составляющие общественных отношений в области обеспечения ИБ. Принципы правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации.
26. Источники, субъекты и объекты права в сфере информации, информационных технологий и защиты информации. Состав правонарушения, формы правоприменительной деятельности в области обеспечения ИБ.
27. Что включает в себя организация обеспечения информационной безопасности на уровне государства и на предприятии? Опишите содержание организационной составляющей в комплексной системе защиты информации.
28. Классификация правонарушений в сфере информации, информационных технологий и защиты информации. Понятие преступления и виды наказаний, применяемых за их совершение.
29. Понятие юридической ответственности за правонарушения в сфере информации, информационных технологий и защиты информации, цели ее применения. Виды и функции юридической ответственности.
30. Понятие информации ограниченного доступа. Защита информации ограниченного доступа. Содержание правового режима работы и с информацией ограниченного доступа. Юридическая ответственность за нарушение порядка ограничения доступа к информации.
31. Понятие «персональные данные» и их категории. Предмет и цели правового регулирования персональных данных, а также особые режимы их обработки. НПА в сфере организации обращения и защиты персональных данных в Российской Федерации.
32. Субъект персональных данных и его основные права. Права и обязанности оператора персональных данных. Виды обработки персональных данных. Ответственность за нарушение требований законодательства по защите персональных данных.
33. Разновидности информационных систем, обрабатывающих персональные данные. Типы актуальных угроз для ИС. Уровни защищенности информационных систем персональных данных.
34. Понятие банковской тайны, ее объекты и субъекты. Операции, проводимые кредитными организациями, в ходе которых возможна утечка банковской тайны. Какие органы имеют право получать банковскую тайну,

особенности обращения с ней. Виды ответственности за нарушение правового режима банковской тайны.

35. Понятие объектов интеллектуальной собственности и их характеристика. Интеллектуальные права на разработки в сфере IT и их защита. Юридическая ответственность за правонарушения в сфере интеллектуальных прав. Международная деятельность по защите интеллектуальной собственности.

36. Правовая основа защиты тайны связи. Субъекты, обеспечивающие тайну связи. Государственное регулирование деятельности в области связи. Защита прав пользователей услуг связи и меры ответственности за разглашение сведений ограниченного доступа при осуществлении деятельности в области связи. Сферы деятельности Минкомсвязи России. Полномочия Роскомнадзора России.

37. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Принципы обеспечения безопасности критической информационной инфраструктуры. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

38. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Категорирование объектов критической информационной инфраструктуры. Права и обязанности субъектов критической информационной инфраструктуры.

39. Оценка безопасности критической информационной инфраструктуры. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Ответственность за нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов.

40. Опишите алгоритм, реализующий схему открытого распространения ключей Диффи–Хеллмана. Приведите пример расчета. Секретные ключи выберите самостоятельно.

41. Опишите алгоритм, реализующий алгоритм шифрования Шамира. Приведите пример расчета. Параметры шифрования выбрать самостоятельно.

42. Опишите алгоритм, реализующий процедуру шифрования Эль-Гамаля. Приведите пример расчета. Секретные ключи и другие параметры выбрать самостоятельно

43. Опишите алгоритм шифрования RSA для передачи секретных сообщений в адрес абонентов A или B. Приведите пример расчета. Рекомендуемые значения параметров выбрать самостоятельно.

44. Генерация криптографических ключей. Схема генерации случайного ключа в соответствии со стандартом ANSI X9.17.

45. ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», основные положения.

46. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.

47. Однонаправленные функции. Хеш-функции, коллизии. Хеш-функции на основе СБШ. Анализ хеш-функций. Парадокс дней рождения.

48. Методы и методики проверки соответствия требованиям на основе критериев аудита ИБ для банковской сферы. Основные нормативно-правовые акты.

49. Организация системы обеспечения информационной безопасности в кредитно-финансовой компании, которая анализируются при проведении аудита информационной безопасности.

50. Документы, определяющие функционирование системы обеспечения информационной безопасности в кредитно-финансовой организации, и которые анализируются при проведении аудита информационной безопасности.

51. Аудит подсистемы аутентификации в защищённой информационно-технологической системе кредитно-финансовой организации.

52. удит подсистемы управления доступом в защищённой информационно-технологической системе кредитно-финансовой организации.

53. Аудит подсистемы обеспечения конфиденциальности в защищённой информационно-технологической системе кредитно-финансовой организации.

54. Аудит подсистемы обеспечения целостности в защищённой информационно-технологической системе кредитно-финансовой организации.

55. Аудит подсистемы оповещения о нарушениях безопасности в защищённой информационно-технологической системе кредитно-финансовой организации.

56. Аудит подсистемы обеспечения криптографическими ключами в защищённой информационно-технологической системе кредитно-финансовой организации.

57. Аудит внутренней инфраструктуры открытых ключей в защищённой информационно-технологической системе кредитно-финансовой организации.

58. Аудит применения асимметричных криптографических систем (электронной подписи) в финансово-экономической сфере.

59. Внешний аудит ИБ. Данные, необходимые для обеспечения и проведения аудита информационной безопасности. Контроль за деятельностью аудиторов информационной безопасности. Понятие «компетентность аудитора».

60. Внутренний аудит ИБ. Цели и задачи внутренних аудитов ИБ. Организационные принципы внутреннего аудита ИБ.

61. Аудит политики обеспечения информационной безопасности.

62. Доверенная третья сторона в системах аутентификации и обеспечения неотказуемости (определение и функции). Аудит привлекаемой доверенной третьей стороны.

63. Виды проверок СУИБ. Принципы обеспечения эффективности внутреннего аудита ИБ.

64. Перечислите требования законодательства при использовании электронных денежных средств. Опишите распространенные виды мошенничества в сфере электронных денежных средств и методы противодействия.

65. Опишите схемы (не менее 2х схем) отмывания денежных средств через электронные средства платежа и перечислите методы противодействия для каждой схемы.

66. Определите перечень и содержание процедуры расследования инцидентов в системах электронного банкинга, данные для проведения расследований с указанием источников, средства форензики для расследований инцидентов в системах электронного банкинга. Укажите средства контр-форензики, которые могут быть использованы для защиты данных в процессе обслуживания через электронный банкинг.

67. Определите порядок и особенности расследования заражения вредоносным кодом: перечень и содержание процедур, данные, используемые для расследований.

68. Определите порядок и особенности расследования утечки информации: перечень и содержание процедур, данные, используемые для расследований.

69. Опишите систему защиты данных держателей карт в приложениях на базе стандарта PCI DSS: определите основные требования стандарта и методы реализации каждого требования. Перечислите и обоснуйте угрозы, снижаемые в рамках реализации требований стандарта.

70. Приведите требования для кредитных организаций к обеспечению защиты информации при осуществлении удаленной банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, укажите нормативные документы, определяющие требования.

71. Опишите актуальные схемы мошенничества в рамках операций с банкоматами и терминалами. Определите способы обеспечения безопасности операций в банкоматах или терминалах.

72. Определите систему организации противодействия методам социальной инженерии (технические средства) в отношении клиентов кредитной организации и опишите порядок использования компонент системы.

73. Дайте графическое представление аналогового и дискретного сигналов. Обоснуйте их отличие.

Практико-ориентированные задания

1. Составьте схему канала утечки информации по побочным электромагнитным излучениям и наводкам (ПЭМИН) и обоснуйте ее структурные элементы.

2. Составьте схему для оценки защищенности информации от утечки по акустическому каналу из защищаемого помещения.

3. Составьте схему для оценки защищенности информации от утечки по вибрационному каналу из защищаемого помещения.

4. Исходя из приведенной схемы разместите основные и вспомогательные технические средства и системы в защищаемом помещении. Обоснуйте свои предложения. (См. схему)

Схема защищаемого помещения

5. Приведите примеры технических средств, которые могут быть источниками опасных сигналов ПЭМИН. Укажите опасные режимы обработки информации при оценке защищенности от утечки за счет ПЭМИН.

6. Составьте общую схему модели технического канала утечки информации и обоснуйте ее структурные элементы. Составьте схему канала перехвата информации за счет применения лазерной акустической системы разведки (ЛАСР).

7. Составьте схему объекта информатизации финансовой организации для обработки конфиденциальной информации.

8. Разработайте схему заземления технических средств, обрабатывающих конфиденциальную информацию. Укажите на схеме возможные места установки средств защиты информации от утечки по цепям заземления.

9. Составьте и обоснуйте схему прямого акустического канала утечки речевой информации. Составьте схему канала перехвата речевой информации с использованием направленного микрофона.

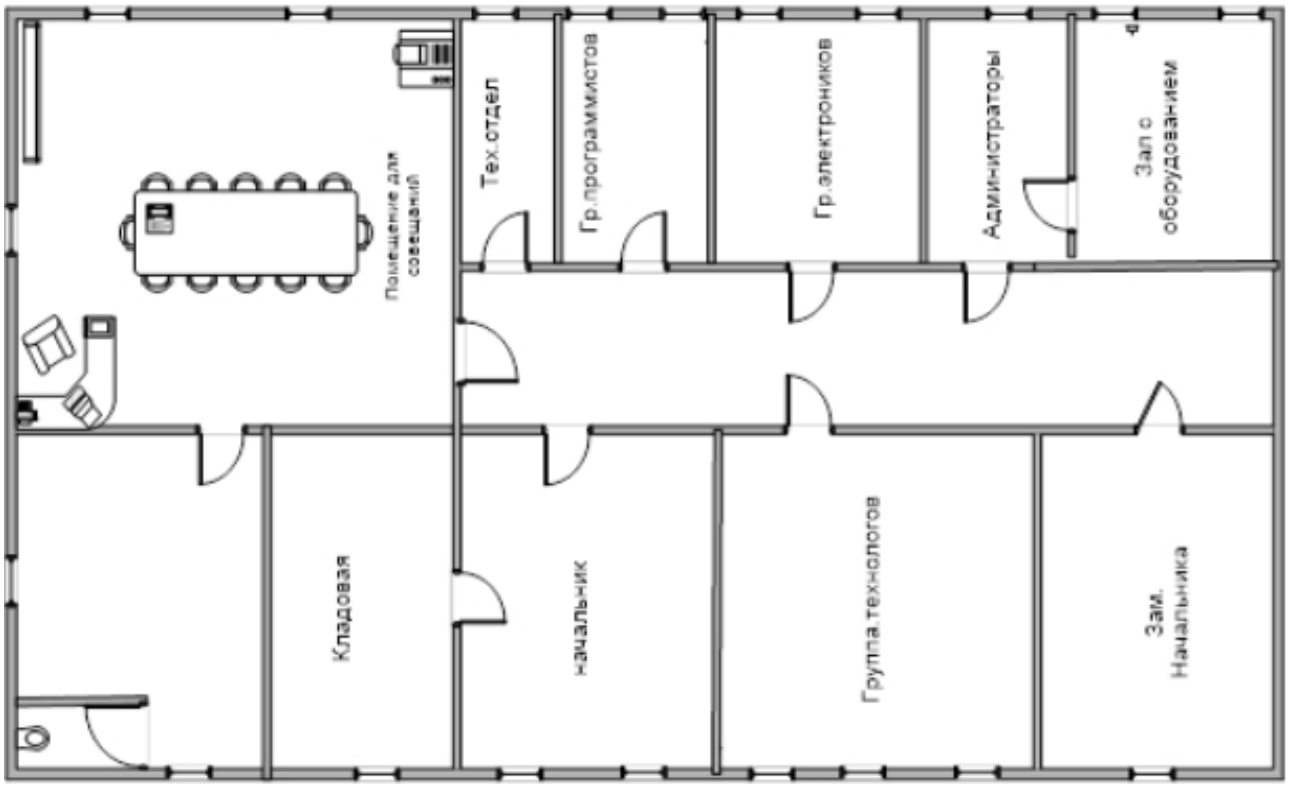
10. Составьте и обоснуйте структурную схему системы виброакустического зашумления (СВАЗ).

11. Составьте и обоснуйте алгоритм лицензирования объектов информатизации.

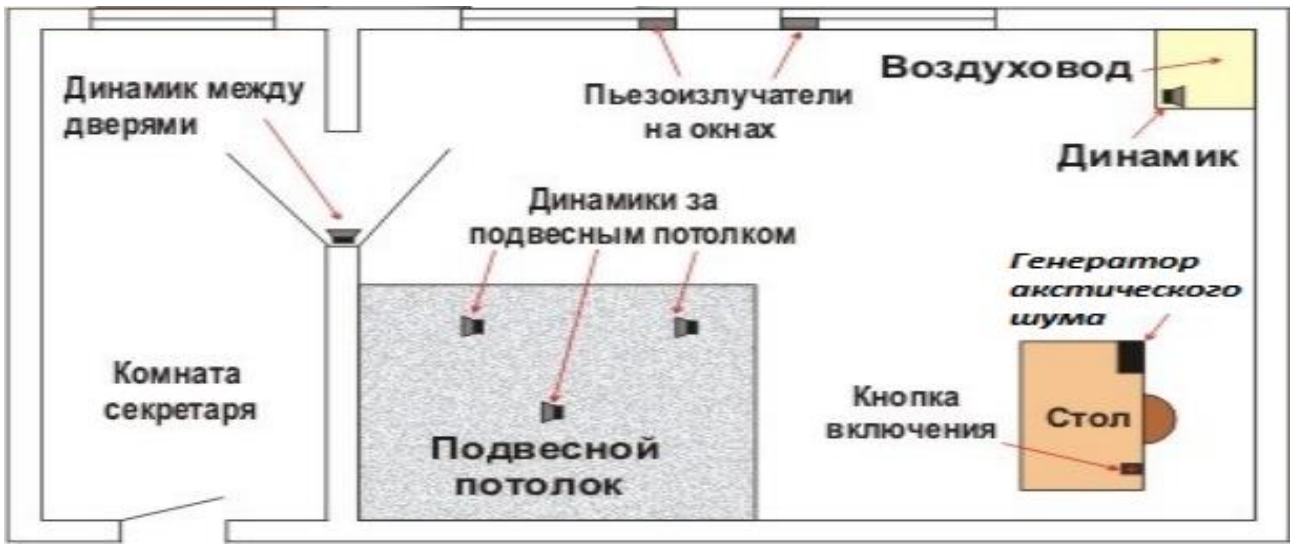
12. Составьте и обоснуйте алгоритм аттестации объектов информатизации.

13. Составьте и обоснуйте алгоритм сертификации средств защиты информации.

14. Для объекта защиты, представленного на рисунке, составьте список потенциальных угроз безопасности. Составьте перечень потенциальных каналов утечки информации и перечень мер по закрытию каналов.



15. На рисунке представлен план защиты объекта. Поясните, от каких угроз безопасности информации защищают представленные на плане технические средства. Какими инженерно-техническими средствами можно дополнить защиту и почему.



16. BRUTE FORCE: Основные определения. Классы брутфорса. Предложите алгоритм взлома WiFi.

17. Поиск следов атак в сетевом трафике: Проблемная составляющая. Связка из техник. Предложите алгоритм поиска следов атак в сетевом траффике.

18. Составьте схему модели технического канала утечки речевой информации за счет высокочастотного навязывания сигналов на ВТСС и обоснуйте ее структурные элементы.

19. Составьте схему модели технического канала утечки речевой информации за счет высокочастотного облучения ВТСС и обоснуйте ее структурные элементы.

20. Составьте схему модели технического канала утечки речевой информации по слаботочным линиям за счет акустоэлектрического преобразования сигналов в ВТСС и обоснуйте ее структурные элементы.

21. Составьте схему модели технического канала утечки речевой информации по линиям электропитания за счет акустоэлектрического преобразования сигналов в ВТСС и обоснуйте ее структурные элементы.

22. Составьте схему модели технического канала утечки речевой информации с использованием закладочных устройств с передачей информации по электросети 220 В и обоснуйте ее структурные элементы.

23. Составьте схему модели технического канала утечки речевой информации с помощью закладочных устройств типа «телефонного уха» с передачей информации по телефонной линии на низкой частоте и обоснуйте ее структурные элементы.

24. Составьте схему модели технического канала утечки речевой информации с использованием закладочных устройств с передачей информации по телефонной линии на высокой частоте и обоснуйте ее структурные элементы.

25. Составьте схему модели технического канала утечки речевой информации с использованием радиостетоскопов и обоснуйте ее структурные элементы.

26. Составьте схему модели технического канала утечки речевой информации с использованием электронных стетоскопов и обоснуйте ее структурные элементы.

27. Составьте схему модели технического канала утечки речевой информации от ВТСС, имеющих в своем составе генераторы, и обоснуйте ее структурные элементы.

28. Перечислите основные задачи защиты информации и предложите конкретные криптографические методы, направленные на решение указанных задач.

29. Перечислите базовые режимы работы блочных шифров по ГОСТ 34.13-2018 и укажите области практического применения для каждого из режимов.

30. Сформулируйте основные этапы криптографических протоколов TLS и IPsec. Укажите области применения указанных протоколов.

31. Составьте схемы алгоритмов шифрования по ГОСТ 34.12-2018. Укажите параметры данных блочных шифров (размер блока, размер ключа, число раундов, размер раундового ключа).

32. Перечислите криптографические методы проверки целостности данных. Составьте схему функции хэширования по ГОСТ 34.11-2018 и схему режима выработки имитовставки по ГОСТ 34.13-2018.

33. Перечислите, в каких задачах криптографии важно использовать простые числа. Укажите известные способы генерации простых чисел и тесты для проверки простоты числа. С помощью теста Ферма исследуйте на простоту число n =277.

34. Перечислите основные виды криптографических генераторов. Сформулируйте принципы построения модуля генерации псевдослучайных чисел в СКЗИ.

35. Составьте схему электронной подписи RSA. При модуле RSA n=323 выберите открытый ключ e, вычислите закрытый ключ d. Запишите формулу для вычисления подписи сообщения «2025».