Экзаменационное задание (Вариант № 6)

по дисциплине «Основы информационной безопасности»

На заданные вопросы следует давать однозначные ответы, т.е. на один вопрос необходим один правильный ответ. Если существует два и более непротиворечивых ответа, то один из них является наиболее полным, он и является правильным ответом.

1. Основные уровни антивирусной защиты? 1. Поиск и уничтожение неизвестных вирусов 2. Блокировка проявления вирусов; 3. Поиск и уничтожение известных вирусов 4. 1, 2 5. 1, 3 6. 2, 3 7. 1, 2, 3	**2. К методам защиты информации средствами инженерно-технического обеспечения СИБ относится?** 1. Защита информации от преднамеренного воздействия 2. Защита информации от появившихся угроз 3. Предотвращение нарушения целостности информации 4. Скрытие достоверной информации, посредством информационного и энергетического срытия 5. Предотвращение доступности информации 6. Защита информации от воздействия угроз
3. Выводы аудита не включают? 1. Выводы (наблюдения), превосходящие границы обычной практики, или возможности для улучшения 2. Размер представительной выборки 3. Распределение выводов аудита по категориям (если они имеются) 4. Требования заказчика аудита 5. Задачи на следующий период аудита 6. Меры, предпринятые по результатам предыдущих записей и заключений аудита	**4. Одной из целей организационно-правового обеспечения защиты информации является?** 1. Узакониваются меры ответственности за нарушения правил защиты информации 2. Обеспечиваются концептуальные разработки политики ИБ 3. Формируются практические ограничительные меры по обеспечению ИБ 4. Определяются режимные мероприятия по обеспечению ИБ 5. Обеспечивается ликвидация последствий воздействия угроз 6. Формируются меры защиты территорий и помещений
5. Что не относится к способам гарантированного уничтожения информации? 1. Размагничивание носителя 2. Шифрование данных 3. Захоронение носителя установленным порядком 4. Химическое уничтожение носителя 5. Перезапись данных по специальному алгоритму 6. Механическое уничтожение носителя 7. Термическое уничтожение носителя	**6. Не относится к типам межсетевых экранов?** 1. Помехоподавляющие фильтры 2. Шлюзы прикладного уровня 3. Гибридные межсетевые экраны 4. Шлюзы уровня соединения; 5. Фильтры с контекстной проверкой 6. Пакетные фильтры
7. К объектам критической информационной инфраструктуры относится? 1. Информационные системы 2. Информационно-телекоммуникационные сети 3. Автоматизированные системы управления 4. Системы контроля и управления доступом 5. 1, 2, 3 6. 2,3,4 7. 1, 3, 4	**8. Организационные принципы построения защищенной сети?** 1. Система должна быть распределенной 2. Система должна быть избыточна за счет применения компонентов разных изготовителей 3. Система защиты должна строиться комплексно 4. Система должна быть замкнутого цикла 5. 1, 2, 3 6. 2, 3, 4 7. 1, 2, 4
9. Какие особенности работы с персоналом, допущенным к работе с конфиденциальной информацией должны учитываться руководством предприятия (организации)? 1. Процесс обучения должен проходить непрерывно 2. Противоправные действия могут совершаться только по некоторому умыслу 3. Сотрудники, имеющие доступ к конфиденциальной информации, должны получать достойную зарплату 4. Обязательное дополнительное материальное стимулирование работников 5. 1, 3 6. 1, 2, 4	**10. К средствам поиска каналов утечки информации за счет ПЭМИН не относятся?** 1. Обнаружители диктофонов 2. Анализаторы спектра 3. Генераторы шума 4. Селективные микровольтметры 5. Специальные измерительные комплексы для проведения измерений уровней ЭМИ

11. Типы учетных записей являются? 1. Учетная запись «Администраторы» 2. Учетная запись «Пользователи» 3. Учетная запись «Гости» 4. 1, 2 5. 1, 3 6. 2, 3 7. 1, 2, 3	**12. К силам ИБ относятся?** 1. Совокупность органов и исполнителей работ, связанных с защитой информации 2. Совокупность органов и исполнителей работ, связанных с законодательной базой ИБ 3. Совокупность органов и исполнителей работ, определяющих ответственность за нарушения защиты информации 4. Совокупность органов и исполнителей работ, обеспечивающих техническую и физическую защиту информации 5. Совокупность органов и исполнителей работ, связанных с защитой активов организации
13. К средствам защиты телефонных аппаратов и двухпроводных линий не относятся? 1. Средства блокирования радиозакладок 2. Средства ограничения, фильтрации и отключения источников опасных сигналов в оконечном оборудовании слаботочных линий 3. Средства подавления акустических закладок 4. Средства криптографической защиты телефонных линий 5. Средства линейного зашумления телефонных аппаратов 6. Средства зашумления и уничтожения радиозакладок	**14. К способам защиты телефонных линий не относится?** 1. Подача в линию импульсов напряжением до 1500 В для выжигания электронных устройств и блоков их питания 2. Подача в линию высокочастотных электромагнитных импульсов 3. Генерация в линию с последующей компенсацией на определенном участке телефонной линии сигнала речевого диапазона с известным спектром 4 Подача в линию маскирующего низкочастотного сигнала при положенной трубке 5. Подача в линию во время разговора маскирующих низкочастотных сигналов звукового диапазона, или ультразвуковых колебаний 6. Поднятие напряжения в линии во время разговора
15. Виды экранирования? 1. Магнитостатическое 2. Электромагнитное 3. Электростатическое 4. 1, 2 5. 2, 3 6. 1, 2, 3	**16. Типы доступа в операционной системе Windows?** 1. Стандартные 2. Родовые права 3. Специальные 4. 1, 2 5. 1, 3 6. 2, 3 7. 1, 2, 3
17. Не относится к задачам организационно-правового обеспечения СИБ? 1. Обеспечение контроля функционирования организации 2. Формирование и проведение политики информационной безопасности организации (предприятия) 3. Разработка нормативно-правовых актов, регламентирующих отношения в информационной сфере 4. Организация мероприятий обеспечения СИБ 5. 1, 2, 3 6. 2, 3, 4	**18. К средствам защиты от утечки информации по материально-вещественному каналу относятся?** 1. Средства защиты и экстренного уничтожения информации в отходах деятельности организации 2. Средства защиты и экстренного уничтожения информации на машинных носителях 3. Средства защиты и экстренного уничтожения информации на бумажных носителях 4. 1, 2 5. 1, 3 6. 2, 4
19. Не относятся к типам сканеров уязвимостей? 1. Сканеры, исследующие уязвимости сетевых сервисов 2. Сканеры доступа 3. CGI-сканеры 4. Сканеры, исследующие топологию компьютерной сети 5. Сканер портов	**20. Безопасность информации – состояние защищенности информации, при котором обеспечены ее?** 1. Оперативность 2. Целостность 3. Достоверность 4. Доступность 5. Конфиденциальность 6. 2, 4, 5 7. 1, 3, 5
21. Средствами организационного обеспечения являются? 1. Концепции ИБ 2. Политики ИБ 3. Анализ угроз ИБ 4. Устав организации 5. 1, 2, 4 6. 1, 2, 3	**22. Анализаторы спектра средств поиска каналов утечки информации за счет ПЭМИН предназначены для?** 1. Опознавания информационных сигналов и измерения их уровней 2. Измерения наводок в сети питания, линиях и коммуникациях 3. Обнаружения электромагнитного излучения 4. Отслеживания изменений панорамы радиосигналов выбранного частотного диапазона, определения времени его появления и основных параметров 5. Идентификации сигналов радиозакладок в выбранном диапазоне

23. Какие из перечисленных источников угроз относятся к внутренним источникам угроз ИБ? 1. Временные пользователи 2. Системы водоснабжения 3. Сервера, рабочие станции 4. 1, 2 5. 2, 3 6. 1, 3	**24. Не относится к методам защиты от спама и фишинга?** 1. Серые списки 2. Анализ приложений 3. Неавтоматическая фильтрация 4. Черные списки 5. Автоматическая фильтрация спама 6. Анализ заголовков 7. Анализ вложений
25. Инженерно-техническое обеспечение СИБ это совокупность? 1. Средств инженерно-технической защиты каналов утечки информации 2. Средств обнаружения и защиты технических каналов утечки информации 3. Средств инженерно-технической защиты компьютерной информации от несанкционированного доступа 4. Средств инженерно-технической защиты территорий и помещений объекта 5. 1, 2 6. 2, 4 7. 3, 4	**26. Функционально подсистема кадрового обеспечения должна?** 1. Базироваться на созданной системе подготовки специалистов в области информационной безопасности 2. Базироваться на специализированных центрах подготовки специалистов ИБ 3. Иметь систему работы с сотрудниками 4. Иметь систему подбора специалистов 5. 1, 2, 3 6. 2, 3, 4 7. 1, 3, 4
27. Что понимают под объектами защиты информации? 1. Объекты организации 2. Информационный процесс 3. Носитель информации 4. 1, 3 5. 2, 3 6. 1, 3	**28. Управление доступом это?** 1. Предоставление программно-аппаратного обеспечения 2. Предотвращение несанкционированного доступа 3. Предотвращение утечки информации 4. Предоставление санкционированного доступа 5. 1, 2 6. 3, 4 7. 2, 4
29. К средствам защиты информации, встроенным в системное программное обеспечение относятся? 1. Средства аутентификации и идентификации 2. Средства авторизации 3. Средства системного аудита 4. 1, 2 5. 1, 3 6. 2, 3 7. 1, 2, 3	**30. К собираемой информации аудита информационной безопасности не относится?** 1. Существующие риски и требования безопасности, предъявляемые к информационной системе 2. Распределение механизмов безопасности по структурным элементам и уровням функционирования информационной системы 3. Элементы информационной системы, относящиеся к активам организации 4. Документация на информационную систему 5. Информация об организационной структуре пользователей информационной системы и обслуживающих подразделений
31. К средствам подготовки кадров не относится? 1. Учебная и методическая литература 2. Учебные программы 3. Программы повышения осведомленности 4. Компетенции специалиста ИБ 5. Процесс обучения специалиста 6. Учебные планы 7. Профессорско-преподавательский состав	**32. Не относится к задачам резервного копирования?** 1. Разграничение доступа к хранимым данным 2. Ограничение, фильтрация и отключение источников опасных сигналов, влияющих на хранение данных 3. Восстановление сохранённых данных 4. Обеспечение устойчивости хранимых данных к изменению и уничтожению 5. Обеспечение контроля системы и процесса резервного копирования 6. Выделение целевых данных
33. Функционально подсистема кадрового обеспечения должна? 1. Базироваться на созданной системе подготовки специалистов в области информационной безопасности 2. Базироваться на специализированных центрах подготовки специалистов ИБ 3. Иметь систему работы с сотрудниками 4. Иметь систему подбора специалистов 5. 1, 2, 3 6. 2, 3, 4 7. 1, 3, 4	**34. К средствам визуального поиска закладных устройств подсистемы обнаружения технических каналов утечки информации относятся?** 1. Электрические фонари 2. Досмотровые зеркала 3. Волоконно-оптические технические приборы (эндоскопы) 4. 1, 2, 3 5. 1, 3 6. 2, 3

35. Цель программно-аппаратного обеспечение СИБ? 1. Обеспечение выполнения физических и технических требований по защите конфиденциальности, доступности и целостности защищаемой информации организации, а также обеспечение безопасности персонала, владеющего этой информацией 2. Обеспечение конфиденциальности, доступности и целостности компьютерной информации при воздействии угроз на информационную систему 3. Оценка текущего уровня защищенности информационных систем 4. Локализация узких мест в системе защиты информационных систем 5. Предупреждение и сдерживание потенциальных нарушителей 6. Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности информационных систем	**36. Какие из перечисленных направлений относятся к системе кадрового обеспечения СОИБ?** 1. Подготовка кадров 2. Регламентация деятельности сотрудников 3. Адаптация сотрудников в коллективе 4. Профессиональная этика специалиста ИБ 5. 1, 4 6. 2, 3
37. Что из перечисленного не относится к задачам СИБ? 1. Предупреждение появления угроз 2. Обнаружение появившихся угроз 3. Обнаружение воздействия угроз 4. Стабилизация обнаруженных угроз 5. Ликвидация последствий воздействия угроз	**38. К средствам методов инструментального (технического) контроля каналов утечки информации подсистемы обнаружения технических каналов утечки информации относятся?** 1. Средства обнаружения неизлучающих закладных устройств 2. Средства поиска каналов утечки информации за счет побочного электромагнитного излучения и наводок 3. Средства обнаружения радиоизлучений закладных устройств 4. 1, 2 5. 1, 3 6. 1, 2, 3
39. Перечислите в порядке возрастания уровни зрелости организации? 1. Оптимизируемый 2. Управляемый (измеряемый) 3. Начальный (анархия) 4. Определенный (стандартный) 5. Повторяемый (фольклор)	**40. Не является видом резервного копирования?** 1. Интегрированное резервное копирование 2. **Метод отображающего дублирования диска** 3. **Добавочное резервное копирование** 4. **Дифференциальное резервное копирование** 5. **Пофайловое резервное копирование** 6. **Полное резервное копирование**
41. Что понимается под управлением рисками? 1. Скоординированные действия по руководству и управлению расчета неблагоприятного исхода 2. Процесс определения достоверного знания о благоприятном исходе. 3. Процесс выявления основных классов рисков 4. Скоординированные действия по руководству и управлению идентификации и уменьшения рисков, которые могут воздействовать на информационную систему 5. Процесс измерения вероятности неблагоприятного исхода 6. Скоординированные действия по руководству и управлению организацией в отношении риска информационной безопасности с целью его минимизации	**42. Не относятся к средствам подсистемы обнаружения и защиты технических каналов утечки информации?** 1. Средства защиты от утечки информации по коммутируемым каналам 2. Средства защиты компьютерной информации от несанкционированного доступа 3. Средства обнаружения технических каналов утечки информации 4. Средства защиты от утечки информации по материально-вещественному каналу 5. Средства защиты информации от утечек по техническим каналам
43. Какие существуют категории систем резервного копирования данных? 1. Дифференцированные системы 2. Каталоговые системы 3. Интегрированные системы 4. Целевые системы 5. 1, 2 6. 2, 3 7. 3, 4	**44. Выполнение каких функции должна обеспечивать нормативно-правовая база СИБ?** 1. Определение мер ответственности за нарушения ИБ 2. Создание благоприятных межличностных отношений 3. Определение системы органов и должностных лиц, ответственных за информационную безопасность 4. Создание нормативных документов обеспечения ИБ 5. Определение величины риска ИБ 6. 1, 3, 4 7. 1, 2, 4, 5

45. Не являются зонами безопасности инженерных средств физической защиты? 1. Помещение 2. Шкаф, сейф, хранилище 3. Коридор или его часть 4. Здание на территории 5. Проходная или контрольно-пропускной пункт 6. Территория, занимаемая организацией и ограничиваемая забором или условной внешней границей	**46. Сведения, составляющие коммерческую тайну?** 1. Сведения любого характера, составляющие активы организации и являются неизвестными для третьих лиц 2. Сведения любого характера, обладающие признаками информационных ресурсов, и являются неизвестными для третьих лиц 3. Сведения любого характера, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам 4. Сведения любого характера, обладающие конфиденциальностью, целостностью, доступностью 5. Сведения любого характера, имеющие финансовую стоимость в силу неизвестности их третьим лицам
47. Какие существуют виды аудита? 1. Комплексный аудит 2. Внутренний аудит 3. Выборочный аудит 4. Внешний аудит 5. 1, 2 6. 1, 3 7. 2, 4 8. 3, 4	**48. Не относится к средствам программно-аппаратной защиты информации?** 1. Средства управления периферийными устройствами 2. Средства криптографической защиты 3. Средства управления сетевого действия 4. Средства методов инструментального контроля каналов утечки информации 5. Программно-аппаратные и аппаратные межсетевые экраны 6. Системы резервного копирования
49. К составляющим затрат на обеспечение СИБ не относится? 1. Структурирование затрат на предупредительные мероприятия 2. Структурирование затрат на Политику СИБ 3. Структурирование затрат на контроль СИБ 4. Структурирование внутренних затрат на компенсацию нарушений политики СИБ 5. Структурирование внешних затрат на компенсацию нарушений политики СИБ	**50. Какая из перечисленных подсистем не относится к СОИБ?** 1. Кадровое обеспечение 2. Инженерно-техническое обеспечение 3. Информационное обеспечение 4. Аудит ИБ 5. Программно-аппаратного обеспечения 6. Организационно-правовое обеспечение
51. Не относится к задачам инженерно-технической защиты территорий и помещений? 1. Осуществление контролируемого доступа в здания и помещения 2. Охрана оборудования, продукции, финансов и информации 3. Осуществление режимных мероприятий по обеспечению ИБ 4. Охрана территории предприятия и наблюдение за ней 5. Охрана зданий, внутренних помещений и контроль за ними	**52. Система распределения ключей-паролей?** 1. Двухуровневая 2. Трехуровневая 3. Четырехуровневая 4. Многоуровневая 5. 1, 2 6. 2, 3 7. 3, 4
53. К мотивам нарушителя относится? 1. Целеустремленность 2. Безответственность 3. Безразличие 4. Самоутверждение 5. Корыстный интерес 6. 1, 3, 4 7. 2, 4, 5	**54. Что не относится к функциям подсистемы организационно-правового обеспечения?** 1. Формирование правового поля для выполнения мероприятий обеспечения ИБ 2. Обеспечение выполнения концептуальных разработок по обеспечению ИБ 3. Формирование практических ограничительных по обеспечению ИБ 4. Определение режимных мероприятий по обеспечению ИБ 5. Определение мер ответственности за нарушения ИБ
55. На каком уровне категорий осуществляется степень детализации управления доступом? 1. Заданная группа пользователей; 2. Владелец информации 3. Все другие авторизованные пользователи 4. 1, 2 5. 1, 3 6. 2, 3 7. 1, 2, 3	**56. К средствам инженерно-технической защиты территорий и помещений относятся?** 1. Инженерно-технические средства подсистемы ликвидации угроз 2. Инженерно-технические средства подсистемы обнаружения угроз 3. Инженерно-технические средства подсистемы предупреждения угроз 4. 1, 2, 3 5. 1, 3 6. 2, 3

57. При каком уровне зрелости организации применяется модель оценки эффективности затрат на ИБ «Планирование непрерывности бизнеса (BCP)»? 1 – начальный 2 – повторяемый 3 – определенный 4 – управляемый 5 – оптимизируемый	**58. Способы защиты информации не включают?** 1. Защиту информации от разведки (иностранной разведки) 2. Защиту информации от санкционированного доступа 3. Защиту информации от непреднамеренного воздействия 4. Защиту информации от утечки 5. Защиту информации от разглашения, защита информации от несанкционированного доступа 6. Защиту информации от преднамеренного воздействия
59. К средствам СКУД не относятся? 1. Устройства контроля состояния преграды; идентификаторы 2. Исполнительный механизм устройства контроля состояния преграды 3. Средства управления устройством запирания с модулем идентификации 4. Информационно-телекоммуникационные сети 5. Средства пропуска персонала или транспорта (преграда)	**60. Комплексная система обеспечения безопасности беспроводных сетей включает?** 1. WPA2 = IEEE 502.1X + CCMP + EAP + MIC 2. WPA2 = IEEE 802.1X +QH + CM + MIC 3. WPA2 = IEEE 802.1X + CCMP + EAP + MIC 4. WPA2 = IEEE 802.1X +CH + QP + EAP 5. WPA2 = IEEE 609.1X + CCMP + EAP + MIC 6. WPA2 = IEEE 802.1X + CCMP + AS + AC