Экзаменационное задание (Вариант № 5)

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. 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	**2. К техническим средствам защиты компьютерной информации от несанкционированного доступа не относятся?** 1. Широкополосные передатчики помех 2. Высокочастотные маскирующие помехи 3. Смарт-карты 4. Биометрические сканеры 5. iButton 6. Экранирование и фильтрация компьютера
3. Не относится к задачам программной защиты информации? 1. Восстановление компьютерных ресурсов и информационной системы 2. Защита конфиденциальной информации от шпионских программ 3. Контроль доступа к компьютерным ресурсам 4. Предотвращение воздействия вредоносных программ на информационные ресурсы 5. Средства защиты и экстренного уничтожения информации на машинных носителях 6. Предупреждение воздействия вредоносных программ на компьютерные ресурсы	**4. Какие угрозы не относятся к природе возникновения?** 1. Непреднамеренные 2. Естественные 3. Искусственные 4. Техногенные угрозы
5. К средствам обнаружения радиоизлучений закладных устройств не относятся? 1. Автоматизированные поисковые комплексы 2. Аппаратура обнаружения элементов закладок 3. Универсальные поисковые приборы 4. Обнаружители поля 5. Радиоприемные устройства	**6. Средства правового обеспечения?** 1. Законодательная база организации 2. Международное право и стандарты 3.Законодательная база государства 4. Внутригосударственное право и стандарты 5. 2, 4 6. 1, 3 7. 1, 4
7. Функцией подсистемы программно-аппаратного обеспечения системы информационной безопасности является? 1. Формирование правового поля для выполнения мероприятий обеспечения информационной безопасности 2. Определение возможных масштабов финансирования деятельности по обеспечению информационной безопасности 4. Обеспечение контроля и проверок качества функционирования всех подсистем и элементов СОИБ 5. Обеспечение выполнения концептуальных разработок, а также практических ограничительных и режимных мероприятий по обеспечению информационной безопасности в интересах организации 6. Обеспечение выполнения функций защиты информации в информационной системе, а также самих элементов информационной системы от различных угроз	**8. К алгоритму проведения оценки рисков информационной безопасности не относится?** 1. Определение допустимого уровня рисков 2. Анализ и оценка рисков затрат на информационную безопасность 3. Определение рисков несоответствия законодательству 4. Процедура количественного определения рисков 5. Идентификация активов 6. Разработка модели угроз
9. К задачам ФЭО СИБ относится: 1. Экономическая защита организации 2. Анализ и оценка эффективности затрат на информационную безопасность 3. Руководство и управление расчетами неблагоприятного исхода рисков 4. Финансовое обеспечение активов организации 5. Защита информации о финансовой деятельности организации 6. Предотвращение разглашения финансовой информации	**10. Активный метод защиты компьютерной информации от утечки по ПЭМИН основан на?** 1. Подавлении радиоизлучающих закладок 2. Зашумлении электросетей, посторонних проводников и соединительных линий 3. Изменения напряженности электромагнитного поля 4. Идентификации сигналов радиозакладок 5. Применении специальных широкополосных передатчиков помех 6. Постановке прицельных помех

11. К контактным извещателям (датчикам) не относятся? 1. Вибрационные 2. Ударноконтактные 3. Электроконтактные 4. Магнитоконтактные 5. Обрывные	**12. Формами предоставления доступа являются?** 1. Интегрированный принцип 2. Разделительный принцип 3. Мандатный принцип 4. Дискреционный принцип 5. 1, 2 6. 3, 4 7. 2, 4
13. Средства защиты информации – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты? 1. Информационной системы организации 2. Информации от непреднамеренного воздействия 3. Информационно-телекоммуникационных сетей 4. Автоматизированной системы управления 5. Информационных ресурсов от внутренних и внешних воздействий 6. Системы контроля и управления доступом	**14. Селективные микровольтметры средств поиска каналов утечки информации за счет ПЭМИН применяются для?** 1. Обнаружения радиоизлучающих закладок 2. Автоматического опознавания информационных сигналов и измерения их уровней 3. Измерения напряженности электромагнитного поля 4. Идентификация сигналов радиозакладок 5. 1, 2 6. 1, 3 7. 2, 4
15. Управление доступом пользователя осуществляется? 1. На уровне файлов 2. На уровне пользователя 3. На уровне каталогов 4. На уровне авторизации 5. 1, 2 6. 1, 3 7. 2, 4	**16. Что позволяет получить показатель ТСО?** 1. Цену совокупной стоимости владения системой ИБ 2. Объем расходной части от вложенных в ИБ средств 3. Оценку возможности возврата вложенных в обеспечение ИБ средств 4. 1, 3 5. 1, 2 6. 2, 3
17. Что не относится к стратегии управления рисками? 1. Принятие риска 2. Уклонение от риска 3. Отражение риска 4. Изменение характера риска 5. Уменьшение риска	**18. Пассивный метод защиты компьютерной информации от утечки по ПЭМИН основан на?** 1. Экранировании помещения 2. Акустической изоляции помещения 3. Экранировании источников излучения компьютера 4. Размещении компьютера в экранированном шкафу 5. 1, 2, 3 6. 2, 3, 4 7. 1, 3, 4
19. К подсистеме обнаружения технических каналов утечки информации системы обнаружения и защиты технических каналов утечки информации относятся? 1. Средства методов поиска утечки информации по побочным электромагнитным излучениям и наводкам 2. Средства методов инструментального (технического) контроля каналов утечки информации 3. Средства методов защиты информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации 4. Средства методов физического поиска каналов утечки информации 5. 1, 2 6. 1, 3 7. 2, 4	**20. Программно-аппаратное обеспечение СИБ это совокупность?** 1. Производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз 2. Средств защиты территорий и помещений объекта, средств обнаружения и защиты технических каналов утечки информации, организованная направленность применения которых состоит в создании системы охраны и защиты информации на объектах и элементах информационной системы организации (предприятия) от угроз ее хищения, модификации или уничтожения 3. Системного, прикладного и специального программного компьютерного обеспечения, а также специальных технических устройств 4. Норм-принципов, закрепляющих и регулирующих производственные отношения, связанные с функционированием СИБ, материальной собственностью объекта, его бюджета и иного финансирования в интересах функционирования объекта 5. Объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности 6. Законов, нормативов и управленческих решений, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание, и функционирование систем защиты информации на конкретных объектах

21. С какого мероприятия необходимо начинать работу по обеспечению функционирования СИБ? 1. Организации кадровой работы 2. Изучения правовых основ обеспечения ИБ 3. Введением комплекса ограничительных мер 4. Определение перечня источников конфиденциальной информации 5. Применения комплекса мер инженерно-технических защиты	**22. К средствам подсистемы обнаружения угроз системы инженерно-технической защиты территорий и помещений относятся?** 1. Средства охранного освещения 2. Средства охранной, охранно-пожарной (пожарной) сигнализации 3. Средства охранного телевидения (видеонаблюдения) 4. 1, 2 5. 1, 3 6. 1, 2, 3
23. Не относится к средствам программной защиты информации? 1. Защита компьютерной информации от утечки по побочным электромагнитным излучениям и наводкам 2. Программные сканеры безопасности 3. Программное обеспечение для защиты от шпионских программ 4. Программное обеспечение для шифрования и кодирования информации 5. Программное обеспечение для защиты от спама 6. Антивирусное программное обеспечение	**24. К сведениям, составляющим государственную тайну, не относятся сведения в области?** 1. Оперативно-розыскной деятельности 2. Контрразведывательной деятельности 3. Антитеррористической деятельности 4. Внешнеполитической деятельности 5. Разведывательной деятельности 6. Экономической деятельности 7. Военной деятельности
25. Не включаются в аудиторский отчет? 1. Состав аудиторской комиссии 2. Рекомендации по устранению существующих недостатков и совершенствованию системы защиты 3. Границы проведения аудита и используемых методов 4. Выводы по аудиту 5. Характеристика обследуемой информационной системы 6. Результаты анализа данных аудита 7. Описание целей проведения аудита	**26. Какие из перечисленных методов оценки экономической эффективности инвестиций не относятся к стандартным?** 1. Метод оценки возврата инвестиций 2. Метод расчета срока окупаемости инвестиций 3. Метод расчета коэффициента эффективности инвестиций 4. Метод расчета чистой текущей стоимости 5. Метод расчета нормы доходности инвестиций
27. Не относится к задачам инженерно-технического обеспечения СИБ? 1. Предотвращение утечки информации по различным техническим каналам 2. Воспрещение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или модификации 3. Защита информации от непреднамеренного воздействия 4. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении 5. 1, 4 6. 2, 4	**28. Не относится к видам идентификации?** 1. Первичная верификация 2. Первичная идентификация 3. Вторичная верификация 4. Вторичная идентификация 5. 1, 3 6. 3, 4 7. 2, 4
29. Что не относится к категориям цели Политики информационной безопасности? 1. Доступность 2. Аутентификация 3. Авторизация 4. Целостность 5. Конфиденциальность 6. Аудит безопасности	**30. Какое отношение характеризует область снижения величины риска ИБ при увеличении затрат на обеспечение ИБ?** 1. $\delta R/\delta S \geq 0$ 2. $\delta R/\delta S = 0$ 3. $\delta R/\delta S > 0$ 4. $\delta R/\delta S < 0$ 5. $\delta R/\delta S \leq 0$
31. Не относится к задачам программно-аппаратного обеспечение СИБ? 1. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении 2. Ликвидация последствий воздействия угроз на информационную систему 3. Обеспечение контроля доступа к информационной системе 4. Обнаружение воздействия угроз на информационную систему и локализация этого воздействия 5. Предупреждение появления угроз в информационной системе	**32. К способам переноса информации по материально-вещественному каналу за пределы контролируемой зоны не относятся?** 1. Жидкой средой 2. Излучениями радиоактивных веществ 3. Лицами, незаконно проникнувшими на территорию объекта 4. Излучениями средств ТСПИ, выходящими за пределы контролируемой зоны 5. Воздушными массами атмосферы 6. Сотрудниками организации

33. Информационная безопасность организации – состояние защищенности интересов организации в условиях? 1. Угроз в информационной сфере 2. Рисков в информационной сфере 3. Уязвимостей информационной безопасности 4. Атак на ресурсы организации 5. Угроз активам организации 6. Атак на защиту информации	**34. В чем заключаются мероприятия, призванные регламентировать на предприятии организационное обеспечение СИБ?** 1. В работе с кадрами 2. В определении режимных мероприятий 3. В контроле за расходами активов 4. В работе с документами 5. 1, 3, 4 6. 2, 3, 4 7. 1, 2, 4
35. Не относятся по классификации к средствам инженерно-технического обеспечения СИБ? 1. Программно-аппаратные средства 2. Аппаратные средства 3. Криптографические средства 4. Физические средства 5. Программные средства	**36. К приемам доказательства аутентичности не относится?** 1. Владение механическим ключом 2. Использование рисунка радужной оболочки глаза 3. Знание пароля 4. Владение смарт-картой 5. Владение электронной картой 6. Знание графического пароля
37. Система информационной безопасности – функциональная подсистема системы комплексной безопасности объекта, функционирующая по правилам, установленным правовыми, организационно-распорядительными и нормативными документами по защите информации и объединяющая: 1. Силы 2. Активы организации 3. Средства 4. Нормативно-правовую базу 5. Объекты защиты информации 6. 1, 3, 5 7. 2, 4, 5	**38. Злоумышленник – это?** 1. Нарушитель, намеренно идущий на нарушение законодательства 2. Нарушитель, намеренно идущий на нарушение из социальных побуждений 3. Нарушитель, намеренно идущий на нарушение из финансовых побуждений 4. Нарушитель, намеренно идущий на нарушение из корыстных побуждений 5. Нарушитель, намеренно идущий на нарушение из преступных побуждений 6. Нарушитель, намеренно идущий на нарушение мер информационной безопасности
39. Не относится к криптографическим методам защиты информации? 1. Шифрование 2. Кодирование графических данных 3. Кодирование звуковой информации 4. Кодирование текстовых данных 5. Кодирование телефонных линий 6. Кодирование целых и действительных чисел 7. Универсальная система кодирования текстовых данных	**40. Не относится к этапам аудита системы информационной безопасности?** 1. Выработка рекомендаций 2. Подготовка аудиторской комиссии 3. Подготовка аудиторского отчета 4. Инициирование процедуры аудита 5. Анализ данных аудита 6. Сбор информации аудита
41. Обеспечение информационной безопасности организации – это деятельность, направленная на? 1. Устранение внутренних угроз ИБ 2. Устранение внешних угроз ИБ 3. Минимизацию ущерба от угроз 4. 1, 2, 3 5. 1, 2 6. 2, 3	**42. Какие из организационных мероприятий кадровой работы таковыми не являются?** 1. Тестирование кандидатов 2. Воспитание сотрудников 3. Принятие на работу по рекомендациям 4. Повышение квалификации сотрудников 5. Повышение правовой грамотности персонала
43. К средствам подсистемы защиты информации от утечек по техническим каналам не относятся? 1. Средства защиты компьютерной информации от утечки по побочным электромагнитным излучениям и наводкам 2. Средства защиты телефонных аппаратов и двух проводных линий 3. Средства криптографической защиты телефонных линий 4. Средства защиты информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации 5. Средства защиты акустической информации в помещении	**44. Какие функции не относятся к средствам защиты презентаций в PowerPoint?** 1. Преобразование слайдов в изображения 2. Преобразование презентации в формат PDF 3. Преобразование презентации в видеоролик 4. Защита на создание документа 5. Защита паролем от редактирования 6. Добавление цифровой подписи 7. Пометить как «Окончательный»

45. К угрозам ИБ по аспекту информационной безопасности относятся? 1. Угрозы целостности, ограниченности, обеспеченности 2. Угрозы конфиденциальности, доступности, уязвимости 3. Угрозы доступности, разрушения, уничтожения 4. Угрозы конфиденциальности, целостности, надежности 5. Угрозы целостности, доступности, уязвимости 6. Угрозы конфиденциальности, целостности, доступности	**46. Что не относится к Кодексу профессиональной этики специалиста в области информационной безопасности?** 1. Обеспечение объективной и качественной работы 2. Обеспечение конфиденциальности информации 3. Развитие собственных компетенций 4. Обеспечение прозрачности своей работы и результатов 5. Обеспечение спортивного образа жизни 6. Повышение осведомленности других специалистов 7. Ориентир на «лучшие этики»
47. Типы управления периферийными устройствами? 1. Дискреционное управление 2. Косвенное управление 3. Прямое управление 4. Мандатное управление 5. 1, 2 6. 2, 3 7. 3, 4	**48. К техническим средствам обнаружения и защиты каналов утечки информации подсистемы обнаружения и защиты технических каналов утечки информации не относятся?** 1. Средства защиты компьютерной информации от несанкционированного доступа 2. Средства защиты от утечки информации по материально-вещественному каналу 3. Средства защиты информации от утечек по техническим каналам 4. Средства защиты от утечек по физическому каналу 5. Средства обнаружения технических каналов утечки информации
49. Какие из принципов не относятся к отражаемым в концепции ИБ? 1. Законность 2. Непрерывность совершенствования системы ИБ 3. Масштабность использования средств защиты ИБ 4. Комплексность использования средств защиты информации 5. 1, 2, 3 6. 1, 2, 4	**50. Одной из задач обучения кадров является?** 1. Определить меры ответственности за нарушения ИБ 2. Создать благоприятные межличностные отношения 3. Защитить информацию от непреднамеренного воздействия 4. Определить должностных лиц, ответственных за информационную безопасность 5. Создать нормативные документы обеспечения ИБ 6. Предотвратить утечку информации по причине небрежности
51. Не относится к направлениям деятельности в области аудита информационной безопасности? 1. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок 2. Проектирование объектов в защищенном исполнении 3. Аттестация объектов информатизации по требованиям безопасности информации 4. Разработка концепции и политик информационной безопасности 5. Контроль защищенности информации ограниченного доступа	**52. 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
53. Каналы утечки информации по способу получения информации? 1. Информационный 2. Электромагнитный 3. Физический 4. Технический 5. 1, 2, 3 6. 2, 3, 4 7. 1, 3, 4	**54. Организация использования технических средств не включает?** 1. Организацию накопления конфиденциальной информации 2. Организацию хранения конфиденциальной информации 3. Организацию передачи конфиденциальной информации 4. Организацию сбора конфиденциальной информации 5. Организацию обработки конфиденциальной информации 6. Организацию уничтожения конфиденциальной информации
55. По виду охраняемой зоны (виду защиты) к извещателям (датчикам) не относятся? 1. Поверхностные средства 2. Контактные средства 3. Объемные средства 4. Линейные средства 5. Точечные средства	**56. К средствам контроля состояния проводных сетей не относятся?** 1. Сетевые анализаторы 2. Кабельные тестеры с расширенным функционалом 3. Простые кабельные тестеры 4. Радиоприемные тестеры 5. Простые кабельные тестеры с дополнительными функциями 6. Сетевые тестеры

57. Подсистема программно-аппаратного обеспечения обеспечивает выполнение функций защиты информации в информационной системе, а также самих элементов информационной системы от различных угроз применением? 1. Физической защиты 2. Технических решений 3. Программных и программно-аппаратных решений 4. Организационно-правового обеспечения 5. Предотвращением несанкционированного допуска	**58. Организация использования технических средств не включает?** 1. Организацию накопления конфиденциальной информации 2. Организацию хранения конфиденциальной информации 3. Организацию передачи конфиденциальной информации 4. Организацию сбора конфиденциальной информации 5. Организацию обработки конфиденциальной информации 6. Организацию уничтожения конфиденциальной информации
59. Не относится к функциональным возможностям VPN? 1. Защита соединений с мобильными клиентами 2. Создание периметра безопасности 3. Регистрация событий, мониторинг и управление межсетевыми потоками 4. Управление ключевой системой 5. Кодирование межсетевых потоков 6. Выборочное кодирование трафика 7. Защита соединений блокированием трафика	**60. К подсистеме предупреждения угроз инженерно-технической защиты территорий и помещений относятся?** 1. Средства методов физического поиска каналов утечки информации 2. Средства контроля и управления доступом 3. Средства обнаружения радиоизлучений закладных устройств 4. Инженерные средства физической защиты 5. 1, 3 6. 1, 4 7. 2, 4