МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

_____ М.О. Таныгин
(подпись)

«31» 08 2021 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине

Порядок проведения аттестации объектов информатизации
(наименование дисциплины)

10.05.02 Информационная безопасность телекоммуникационных систем, профиль

«Управление безопасностью телекоммуникационных сетей и систем»
(код и наименование ОПОП ВО)

Курск – 2021

Юго-Западный государственный университет

Кафедра информационной безопасности

Вопросы для собеседования

по дисциплине «Порядок проведения аттестации объектов информатизации»

Тема 1. Основные понятия в области технической защиты информации

1. Информация и её характеристики.
2. Угрозы безопасности информации.
3. Меры защиты информации.
4. Системный подход к защите информации.
5. Правовая защита информации.
6. Объекты технической защиты информации.
7. Основные принципы с позиции системного подхода к защите информации.

Тема 2. Концептуальные основы защиты информации. Система документов по технической защите информации

1. Основные положения концепции защиты информации.
2. Характеристики состояния национальной безопасности.
3. Стратегия национальной безопасности РФ.
4. Доктрина информационной безопасности.
5. Принципы правового обеспечения информационной безопасности Российской Федерации.
6. Законодательные и иные правовые акты в области технической защиты информации.
7. Нормативные и методические документы по технической защите информации.

Тема 3. Органы по технической защите информации в РФ.

1. Государственные органы в области защиты информации.
2. Ключевые государственные органы в области технической защиты информации.
3. Основные задачи ФСТЭК России.
4. Полномочия ФСТЭК.
5. Государственные органы защиты государственной тайны.
6. Государственное управление в области обеспечения безопасности Российской Федерации

Тема 4. Лицензирование деятельности в области ТЗИ.

1. Государственная система лицензирования деятельности в области технической защиты информации.
2. Виды деятельности, относящиеся к защите информации, на осуществление которых требуется получение лицензии.
3. Порядок получения лицензии.
4. Документы необходимые для получения лицензии.
5. Причины возможного отказа в получении лицензии.
6. Пункты, содержащиеся в решение о предоставлении лицензии и в документе, подтверждающем наличие лицензии.
7. Случаи прекращения деятельности лицензии.
8.Требования для получения лицензии деятельности по технической защите конфиденциальной информации.
9. Способы контроля за соблюдением лицензионных требований и условий.
10. Плановые и внеплановые проверки лицензиата.

Тема 5. Объект информатизации. Классификация объектов защиты.

1. Объекты защиты информации и их классификация.
2. Степени секретности такой информации.
3. Общедоступная информация.
4. Сведений конфиденциального характера.
5. Классификация автоматизированных систем.
6. Классы защищённости автоматизированных систем от НСД.
7. Классификация средств вычислительной техники.
8. Классы защищённости средств вычислительной техники от НСД.
9. Принципы разграничения доступа к информации.

Тема 6. Общий порядок сертификации средств защиты информации

1. Средства защиты информации.
2. Участники сертификации.
3. Функции федерального органа по сертификации.
4. Функции центрального органа системы сертификации.
5. Органы по сертификации средств защиты информации.
6. Процедура сертификации.
7. Основные схемы проведения сертификации средств защиты информации.
8. Основные органы сертификации в области технической защиты информации.

Тема 7. Порядок сертификации во ФСТЭК России.

1. Перечень действий по сертификации во ФСТЭК России.

2. Содержание решения ФСТЭК на проведение сертификационных испытаний.
3. Обязанности заявителя.
4. Этапы проведения сертификационных испытаний.
5. Заключение договоров с испытательной лабораторией и органом сертификации.
6. Оформление результатов испытаний.
7. Результаты проверки, решение о выдаче сертификата ФСТЭК.

Тема 8. Аттестация объекта информатизации по требованиям безопасности информации.

1. Аттестация объектов информатизации.
2. Случаи, при которых аттестация является обязательной.
3. Требования, проверяемые аттестацией.
4. Перечень работ органа по аттестации.
5. Требования к органу, проводящему аттестацию.
6. Деятельность, осуществляемая органами по аттестации.
7. Перечень работ и обязанности заявителя.
8. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.
9. Содержание протокола аттестационных испытаний.
10. Требования к содержанию аттестата соответствия.

Тема 9. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

1. Основные аспекты документа "Специальные требования и рекомендации по технической защите конфиденциальной информации".
2. Рекомендованные основные меры по защите информации.
3. Стадии создания средств защиты информации в автоматизированных системах.
4. Порядок обеспечения защиты информации в АС.
5. Защита информации в локальных вычислительных сетях и при межсетевом взаимодействии.
6. Защита информации при работе с системами управления базами данных.
7. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
8. Рекомендации при создании абонентского пункта.
9. Основные требования при разработке и эксплуатации АС предполагающих использование информации, составляющей служебную тайну, а также персональных данных.

10. Организационно-технические мероприятия, рекомендуемые к выполнению при разработке и эксплуатации АС, предполагающих использование сведений, составляющих коммерческую тайну.

Критерии оценки:

– 0 баллов выставляется обучающемуся, если студент не может ответить на поставленные вопросы.

– 2 баллов выставляется обучающемуся, если доля правильных ответов от 50% до 90%.

– 4 балла выставляется обучающемуся, если доля правильных ответов более 90%.

Составитель М.А. Ефремов

«31» 08 2021 г.

Юго-Западный государственный университет

Кафедра информационной безопасности

Контрольные вопросы для защиты

практических работ

по дисциплине «Порядок проведения аттестации»

(наименование дисциплины)

Контрольные вопросы для защиты практической работы №1.

1. Какие части документа относятся к вопросам защиты информации?
2. Что показывают комментарии к данному документу?
3. Как менялся текст нормативного акта с момента его создания по настоящее время?

Контрольные вопросы для защиты практической работы №2.

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

Контрольные вопросы для защиты практической работы №3.

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?

6. Какова структура организационно-правовой основы защиты информации?

7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

Критерии оценки:

- 0 баллов выставляется обучающемуся, если студент не выполнил работу.

- 8 балла выставляется обучающемуся, если студент выполнил работу и доля правильных ответов от 50% до 90%.

- 12 балла выставляется обучающемуся, если студент выполнил работу и доля правильных ответов более 90%.

Составитель  М.А. Ефремов

«31» 08 2021 г.

Юго-Западный государственный университет

Кафедра информационной безопасности

Контрольные вопросы для защиты

практических работ

по дисциплине «Порядок проведения аттестации объектов информатизации»

(наименование дисциплины)

1) Выберите виды организационных мер по защите информации?

1) Установление пространственных ограничений

2) Временные ограничения на условия использования и режимы работы объекта информатизации

3) Установка сертифицированного средства защиты информации от несанкционированного доступа

4) Пространственное зашумление путем установки генератора шума

2) На какое количество подсистем условно делится система защиты информации от несанкционированного доступа?

1) 7

2) 4

3) 6

4) 5

3) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты информации от несанкционированного доступа посредством использования механизмов шифрования пользовательских данных?

1) Регистрации и учета

2) Криптографической защиты

3) Обеспечения целостности

4) Управления доступом

4) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты от несанкционированных изменений программной и аппаратной среды ПЭВМ?

1) Регистрации и учета

2) Криптографической защиты

3) Обеспечения целостности

4) Управления доступом

5) В каких случаях необходимо применять активные технические меры по защите информации?

1) В случае использования на ОИ несертифицированных средств вычислительной техники

2) В случае недостаточности использованных организационных и пассивных технических мер защиты информации

3) В случае большой границы контролируемой зоны

4) В случае обработки информации, содержащей сведения, составляющие государственную тайну

6) Меры по защите информации, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации – это:

1) Пассивные технические меры

2) Криптографические меры

3) Организационные меры

4) Активные технические меры

7) Подлежат ли реализации меры защиты информации - обнаружение (предотвращение) вторжений при защите государственных информационных систем?

1) Да

2) Нет

8) Какой документ должны иметь средства защиты информации для подтверждения их соответствия установленным требованиям по защите информации?

1) Аттестат соответствия

2) Лицензию

3) Аттестат аккредитации

4) Сертификат соответствия

9) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для фиксации системных событий в специальном журнале?

1) Регистрации и учета

2) Криптографической защиты

3) Обеспечения целостности

4) Управления доступом

10) Какие виды средств используются при реализации технических мер защиты информации?

1) Инструментальные

2) Технические

3) Программно-технические

4) Контрольные

11) Подсистема управления доступом предназначена для:

1) Защиты объекта информатизации от сторонних пользователей, не имеющих прав доступа к ОИ и пытающихся осуществить несанкционированный доступ к информации

2) Защиты ПЭВМ от внедрения программных закладок, вирусов и прочих специальных математических воздействий на систему

3) Защиты информации от несанкционированного доступа посредством использования механизмов шифрования пользовательских данных

4) Управления доступом уполномоченных пользователей к объекту информатизации в соответствии с правилами разграничения доступа

12) К какому виду мер относится мера: размещение дисплеев и других средств отображения информации таким образом, чтобы исключить несанкционированный или непреднамеренный просмотр защищаемой информации?

1) Организационная

2) Техническая

13) Применение каких мер защиты может исключить утечку информации по акустическому каналу?

1) Проведение специальной проверки технических средств, установленных в помещении

2) Увеличение границы контролируемой зоны на время проведения «закрытых» совещаний

3) Использование аналоговых телефонных аппаратов

4) Использование специальных материалов для облицовки стен, для пола и потолка, повышающих звукоизоляцию защищаемого помещения

5) Использование системы активной защиты речевой информации

6) Использование специальных звукоизолирующих экранов на элементах систем отопления и вентиляции

14) Какая подсистема системы защиты информации от несанкционированного доступа предназначена для защиты ОИ от сторонних пользователей, не имеющих прав доступа к ОИ и пытающихся осуществить несанкционированный доступ к информации?

1) Регистрации и учета

2) Криптографической защиты

3) Обеспечения целостности

4) Управления доступом

15) Что лежит в основе формирования перечня достаточных мер защиты информации?

1) Результаты обследования объекта информатизации

2) Сформулированные требования по защите информации

3) Перечень установленных на объекте информатизации средств защиты информации

4) Результаты аттестации объекта информатизации

16) При каком принципе управления доступом уполномоченный пользователь получает доступ к документам заданного уровня конфиденциальности?

1) Дискреционный

2) Мандатный

17) К какому виду мер относится мера: использование специальных звукоизолирующих экранов на элементах систем отопления и вентиляции?

1) Организационная

2) Техническая

18) Выберите верный номер сертификата соответствия на фильтр сетевой помехоподавляющий ФСП-1Ф-7А

1) 2533/1 до 09.11.2021

2) 633/1 до 15.06.2020

3) 148/2 до 01.04.2019

4) 3552 до 14.04.2019

19) Каким документом определены состав и содержание, а также форма программ и методик аттестационных испытаний?

1) ГОСТ РО 0043-004-2013 «Защита информации. …»

2) «Положение по аттестации объектов информатизации по требованиям безопасности информации», утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.

3) ГОСТ Р 51624-2000 «Защита информации. …».

4) ГОСТ Р 51583-201

5) «Защита информации. …»

20) На какой стадии аттестации объекта информатизации разрабатывается «Программа и методики аттестационных испытаний»?

1) В ходе аттестационных испытаний

2) После проведения аттестационных испытаний

3) До начала проведения аттестационных испытаний

4) Вместе с «Аттестатом соответствия…»

21) Кто разрабатывает и согласовывает «Программу и методики аттестационных испытаний»?

1) Разрабатывает заявитель и согласовывает с органом по аттестации

2) Разрабатывает орган по аттестациии согласовывает с заявителем

3) Разрабатывает заявитель и согласовывает со ФСТЭК России

22) Указывается ли в программе и методиках аттестационных испытаний перечень средств защиты информации, планируемый к установке на аттестуемом объекте информатизации?

1) Да

2) Нет

23) Что определяют «Программа и методики аттестационных испытаний»?

1) Порядок проведения опытной эксплуатации аттестованного объекта информатизации

2) Порядок создания, подготовки и аттестации объекта информатизации

3) Методы проведения аттестационных испытаний

4) Перечень работ в рамках проведения аттестационных испытаний

24) Кто подписывает программу и методики аттестационных испытаний?

1) Руководитель органа по аттестации

2) Сотрудник заявителя, ответственный за объект информатизации

3) Члены аттестационной комиссии

4) Руководитель аттестационной комиссии

25) Необходимо ли разрабатывать «Программу и методики аттестационных испытаний» для защищаемого помещения?

1) Да

2) Нет

26) Раздел «Программа аттестационных испытаний» содержит:

1) Перечень работ по аттестации объекта информатизации

2) Перечень средств защиты информации, планируемых к установке на объекте информатизации

3) Перечень контрольно-измерительной аппаратуры

4) Порядок проведения аттестационных испытаний объекта информатизации

27) Можно ли разработать «Программу и методики аттестационных испытаний» после проведения работ по аттестации, указав какие методы были использованы?

1) Да

2) Нет

28) Раздел «Условия и порядок проведения аттестационных испытаний» включает в себя?

1) Перечень средств защиты информации, планируемых к установке на объекте информатизации

2) Перечень работ по аттестации объекта информатизации

3) Перечень документов, которые должны быть представлены заявителем органу по аттестации

4) Перечень контрольно-измерительной аппаратуры

29) Кто разрабатывает «Программу и методики аттестационных испытаний»?

1) Заявитель

2) Орган по аттестации

3) Федеральный орган по сертификации и аттестации

30) Указывается ли в программе и методиках аттестационных испытаний перечень контрольно-измерительной аппаратуры, планируемой к использованию при проведении аттестационных испытаний?

1) Да

2) Нет

31) Раздел «Подготовка отчетной документации» включает в себя:

1) Наименование (перечень) документов, выдаваемых по результатам аттестационных испытаний

2) Краткое содержание документов, выдаваемых по результатам аттестационных испытаний

3) Полное содержание документов, выдаваемых по результатам аттестационных испытаний

4) Образцы документов, выдаваемых по результатам аттестационных испытаний

32) Является ли документ «Программа и методики аттестационных испытаний» обязательным при проведении работ по аттестации автоматизированной системы?

1) Нет, данный документ носит необязательный характер

2) Нет, данный документ разрабатывается только для защищаемых помещений

3) Да, если такое требование выставит заявитель

4) Да, это предусмотрено руководящими документами по защите информации

33) В каком разделе «Программы и методик аттестационных испытаний» указывается перечень методов проверок и испытаний (экспертно-документальный, инструментальный, инструментально-расчетный)?

1) Общие положения

2) Программа аттестационных испытаний

3) Условия и порядок проведения аттестационных испытаний

4) Методики аттестационных испытаний

34) Указывается ли в программе и методиках аттестационных испытаний схема размещения ОТСС относительно границ контролируемой зоны?

1) Да

2) Нет

35) С кем согласовывается «Программа и методики аттестационных испытаний»?

1) С заявителем

2) С органом по аттестации

3) С федеральным органом по сертификации и аттестации

36) Укажите данные, описываемые в разделе «Общие положения» программы и методик аттестационных испытаний автоматизированной системы?

1) Цели и задачи проведения аттестации объекта информатизации

2) Требования и периодичность проведения периодического контроля за состоянием защищенности аттестованного объекта информатизации

3) Порядок проведения аттестационных испытаний объекта информатизации

4) Наименование (перечень) документов, выдаваемых по результатам аттестационных испытаний (протоколы, заключение, аттестат соответствия)

37)На какие две категории можно разделить информацию при классификации ее по категории доступа:

1) Открытая и закрытая

2) Общедоступная и конфиденциальная

3) Общедоступная и ограниченного доступа

4) Секретная и несекретная

38)Можно ли относить нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина к информации ограниченного доступа:

1) Да

2) Нет

39)Какая информация отнесена к сведениям конфиденциального характера:

1) Персональные данные

2) Служебная тайна

3) Государственная тайна

4) Общедоступная информация

5) Сведения, связанные с профессиональной деятельностью

6) Информация ограниченного доступа

40)Укажите федеральные органы исполнительной власти, уполномоченные в области безопасности информации:

1) Служба внешней разведки РФ

2) Федеральная служба по техническому и экспортному контролю РФ

(3) Федеральная служба охраны РФ

(4) Федеральная служба безопасности РФ

41)Определите процедуру, которая должна быть проведена с целью оценки соответствия требованиям по безопасности информации принятых на объекте мер по защите информации:

1) Сертификация

2) Аттестация

3) Аккредитация

4) Лицензирование

42) Имеет ли право владелец Интернет-ресурса единолично принимать решение об общедоступности информации, размещаемой пользователем на ресурсе:

1) Да

2) Нет

43) Выберите виды информации при классификации ее по категориям доступа:

1) Открытая информация

2) Общедоступная информация

3) Информация ограниченного доступа

4) Секретная информация

5) Информация свободного доступа

6) Конфиденциальная информация

7) Свободно распространяемая информация

44) Информация какого вида, в соответствие с федеральными законами, не может быть отнесена к информации ограниченного доступа:

1) Государственная тайна

2) Информация о состоянии окружающей среды

3) Информация о частной жизни гражданина

4) Тайна голосования

5) Нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина

6) Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

45) Какая информация не относится к сведениям конфиденциального характера, исходя из «Перечня сведений конфиденциального характера», утвержденным Указом Президента РФ от 6 марта 1997 г. N 188:

1) Персональные данные

2) Государственная тайна

3) Тайна следствия и судопроизводства

4) Общедоступная информация

5) Служебная тайна

6) Информация ограниченного доступа

46) ФСТЭК России - это:

1) Федеральная служба по техническому и экспортному контролю, осуществляющая защиту безопасности личности, общества и государства от внешних угроз

2) Федеральная служба по техническому и экспертному контролю, осуществляющая организацию деятельности государственной системы технической защиты информации

3) Федеральная служба по техническому и экспортному контролю, осуществляющая организацию деятельности государственной системы противодействия техническим разведкам и технической защиты информации

4) Федеральная служба по техническому и экспертному контролю, осуществляющая защиту безопасности личности, общества и государства от внешних угроз

47) Оценка соответствия объекта информатизации требованиям безопасности информации осуществляется в ходе:

1) Лицензирования

2) Сертификации

3) Аккредитации

4) Аттестации

48) Паспортные данные (ФИО, прописка, место и дата рождения, семейное положение, серия и номер паспорта) клиентов компании, оказывающей услуги связи это:

1) Информация ограниченного доступа

2) Общедоступная информация

3) Служебная тайна

4) Персональные данные

49) Аттестация объектов информатизации по требованиям безопасности информации это:

1) Обеспечение защиты информации на объекте информатизации

2) Соответствие комплекса мероприятий по защите информации, проведенного на объекте информатизации, требованиям по безопасности информации

3) Мероприятия по обеспечению безопасности при обработке информации на объекте информатизации

4) Процедура подтверждения правильности выбора объекта информатизации

50) К какой государственной системе относится аттестация:

1) Лицензирования

2) Обеспечения государственной безопасности

3) Сертификации средств защиты информации

4) Защиты информации

51) Станут ли персональные данные общедоступной информацией при размещении ее в социальных сетях?

1) Нет

2) Да

52) Кто может выступать обладателем информации?

1) Индивидуальный предприниматель

2) Российская Федерация

3) Физическое лицо

4) Субъект Российской Федерации

52) Включена ли государственная тайна в «Перечень сведений конфиденциального характера», утвержденный Указом Президента РФ от 6 марта 1997 г. N 188?

1) Да

2) Нет

53) Выберите из ниже предложенного пассивные технические мероприятия (возможно несколько вариантов):

1) Назначение ответственного за защиту информации в организации

2) Улучшение звукоизолирующих свойств помещения посредством облицовки стен панелями

3) Экранирование технических средств обработки информации

4) Использование системы защиты информации от несанкционированного доступа

54) Выберите объект испытаний при проведении процедуры аттестации:

1) Индивидуальный предприниматель

2) Средство контроля эффективности защиты информации

3) Помещение для проведения конфиденциальных переговоров

4) Юридическое лицо

55) Государственная система защиты информации включает в себя:

1) Подсистему сертификации СЗИ и подсистему лицензирования в области ЗИ

2) Подсистему сертификации СЗИ и подсистему аттестации ОИ

3) Подсистему лицензирования в области ЗИ и подсистему аттестации ОИ

55) Выберите из ниже предложенного объекты информатизации, подлежащие защите:

1) Автоматизированные системы

2) Средство защиты информации

3) Система размножения документов

4) Средство контроля эффективности защиты информации

56) Выберите объект испытаний при проведении процедуры лицензирования:

1) Объект информатизации

2) Средство защиты информации

3) Автоматизированная система

4) Юридическое лицо

57) Выберите из ниже предложенного организационные мероприятия (возможно несколько вариантов):

1) Классификация автоматизированных систем

2) Установка шумоизолирующих прокладок на дверь

3) Составление перечня информации, подлежащей защите

4) Установка сертифицированной по требованиям безопасности информации операционной системы

58) Выберите объект испытаний при проведении процедуры сертификации:

1) Объект информатизации

2) Изделие

3) Помещение для ведения конфиденциальных переговоров

4) Индивидуальный предприниматель

59) К какому типу мер по защите информации относится установка уплотнителей в дверном проеме защищаемого помещения?

1) Организационная

2) Активная техническая

3) Строительная

4) Пассивная техническая

60) В какой процедуре участвует третья сторона – испытательная лаборатория?

1) Аттестация

2) Аккредитация

3) Лицензирование

4) Сертификация

61) Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности это:

1) Аттестат аккредитации

2) Сертификат соответствия

3) Лицензия

4) Аттестат соответствия

5) Заключение

6) Предписание

62) Выберите виды мероприятий по защите информации:

1) Технические пассивные

2) Активные

3) Организационные пассивные

4) Технические активные

5) Организационные активные

6) Пассивные

63) Какой орган государственной власти является правопреемником Гостехкомиссии России?

1) ФАПСИ

2) ФСО

3) ФСТЭК

4) ФСБ

64) По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается:

1) Аттестат соответствия

2) Аттестат аккредитации

3) Сертификат соответствия

4) Лицензия

5) Заключение

6) Предписание

65) Какие меры защиты информации предусматривают использование конструктивных решений и технологических особенностей обработки информации ограниченного доступа на объектах информатизации?

1) Активные

2) Пассивные

3) Организационные пассивные

4) Организационные активные

5) Технические пассивные

6) Технические активные

66) При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура:

1) Аттестации

2) Лицензирования

3) Сертификации

4) Аккредитации

67) Можно ли в качестве активной технической меры выбрать установку сертифицированной антивирусной программы?

1) Да

2) Нет

68) Выберите стороны, участвующие в процессе лицензирования:

1) Юридическое лицо и ФСТЭК России

2) Орган по аттестации и испытательная лаборатория

3) Заявитель и орган по аттестации

4) Заявитель и юридическое лицо

5) Физическое лицо и орган по сертификации

69) Какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну?

1) На проведение работ, связанных с созданием средств защиты информации

2) На осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну

3) На деятельность по технической защите конфиденциальной информации

4) На деятельность по разработке и производству средств защиты конфиденциальной информации

70) Является ли лицензиат, имеющий лицензию на деятельность по ТЗКИ, органом по аттестации объектов информатизации, предназначенных для обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну?

1) Да

2) Нет

71) Какой документ необходим органу по аттестации для проведения работ по аттестации ОИ по требованиям безопасности информации при обработке информации, не содержащей сведения, составляющие государственную тайну:

1) Сертификат соответствия

2) Лицензия на разработку и производство СЗКИ

3) Аттестат аккредитации

4) Аттестат соответствия

5) Лицензия на осуществление деятельности по ТЗКИ

72)Какая организация из нижеперечисленных при наличии соответствующего разрешительного документа может проводить сертификационные испытания средств защиты информации:

1) Испытательная лаборатория

2) Орган по аттестации

3) Лицензиат, имеющий лицензию на ТЗКИ

4) Заявитель

73)Выберите из ниже предложенного функции органа по аттестации:

1) Учет аттестованных ОИ

2) Приостановка действия «Аттестата соответствия…»

3) Проведение периодического контроля за состоянием защищенности информации на аттестованных ОИ

4) Выдача предписания на приостановление работ на объектах информатизации

74) Кому испытательная лаборатория имеет право направить протокол о проведенных испытаниях средств защиты информации:

1) Органу по аттестации

2) Федеральному органу по сертификации средств защиты информации

3) Никому, оставляет их у себя

4) Производителю средства защиты информации, подавшему заявку на сертификацию

5) Направляет в любую организацию по запросу

75) Выберите из нижеперечисленного задачи, стоящие перед заявителем на аттестацию ОИ для обработки информации ограниченного доступа:

1) Получение лицензии на деятельность по разработке и производству СЗКИ

2) Проведение аттестационных испытаний ОИ

3) Подготовка необходимых документов и технических средств для проведения аттестации

4) Установка и настройка сертифицированных СЗИ

5) Извещение органа по аттестации об изменениях, возникающих на ОИ и способных повлечь за собой снижение заданного уровня защищенности

76) Необходим ли органу по аттестации аттестат аккредитации для проведения работ по аттестации ОИ по требованиям безопасности информации при обработке информации, не содержащей сведения, составляющие государственную тайну:

1) Да

2) Нет

77) Кто выдает предписания на приостановление работ на аттестованном объекте информатизации?

1) ФСТЭК России

2) Орган по аттестации

3) Лицензиат, имеющий лицензию на ТЗКИ

4) Заявитель

78) Может ли испытательная лаборатория, получившая Лицензию на деятельность по ТЗКИ, проводить работы по аттестации объектов информатизации заявителя?

1) Да

2) Нет

79) Выберите функции, возложенные на ФСТЭК России по вопросам аттестации ОИ (возможно несколько вариантов):

1) Осуществляет периодический контроль за состоянием защищенности информации на аттестованных объектах информатизации заявителя.

2) Выдает лицензии на осуществление деятельности по ТЗКИ.

3) Осуществляет работы по аттестации ОИ по заявкам от заявителей.

4) Выдает предписания на приостановление работ на ОИ.

5) Рассматривает апелляции по вопросам аттестации ОИ по требованиям безопасности информации.

6) Осуществляет подготовку объекта информатизации заявителя к проведению работ по аттестации.

80) Имеет ли право заявитель обратиться к органу по аттестации за помощью по подготовке объекта информатизации к аттестации:

1) Нет, заявитель должен самостоятельно готовить объект информатизации к аттестации

2) Да, при условии получения разрешения от ФСТЭК России

3) Да, оплатив дополнительный объем работ органу по аттестации

4) Нет, это не предусмотрено законодательством Российской Федерации в области защиты информации

81) Может ли испытательная лаборатория, получившая Лицензию на деятельность по ТЗКИ, проводить работы по аттестации объектов информатизации заявителя?

1) Да

2) Нет

82) Выберите функции испытательной лаборатории:

1) Осуществляет установку средств защиты информации на объектах информатизации.

2) Проводит оценку эффективности средств защиты информации, установленных на объектах информатизации.

3) Проводит сертификацию средств защиты информации.

4) Выдает протоколы испытаний с заключением о соответствии или несоответствии средств защиты информации установленным требованиям.

5) Осуществляет настройку средств защиты информации в соответствии с требованиями, предъявляемыми к системе защиты информации.

83) Какую лицензию должен получить орган по аттестации для проведения работ по аттестации объектов информатизации?

1) На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации)

2) На деятельность по технической защите конфиденциальной информации.

3) На проведение работ, связанных с созданием средств защиты информации.

4) На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны

84) Выберите верный перечень органов и организаций, входящих в организационную структуру системы аттестации объектов информатизации:

1) ФСТЭК России, лицензиаты в области ТЗКИ, заявители

2) Федеральный орган по сертификации средств защиты информации, испытательные лаборатории.

3) ФСТЭК России, органы по аттестации, испытательные лаборатории, заявители

4) Федеральный орган по аттестации ОИ по требованиям безопасности информации, органы по аттестации, заявители.

85) Чем определены сроки и последовательность прохождения процедур для получения лицензии на деятельность по разработке и производству средств защиты конфиденциальной информации?

1) Федеральным законом

2) Постановлением Правительства

3) Руководящим документом

4) Административным регламентом

5) Нормативным документом

6) Положением

7) ГОСТом

8) Рекомендациями по стандартизации

86) Какого вида деятельности нет в лицензии на деятельность по технической защите конфиденциальной информации?

1) Услуги по мониторингу информационной безопасности средств и систем информатизации.

2) Услуги по проектированию в защищенном исполнении средств и систем информатизации.

3) Услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

4) Услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации защищаемых помещений.

5) Услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации

6) Услуги по проведению спец. исследований на побочные электромагнитные излучения и наводки технических средств обработки информации

87) Какие разделы включает в себя инструкция по организации антивирусной защиты в автоматизированной системе объекта информатизации?

1) Порядок применения средств антивирусной защиты

2) Перечень действий с антивирусными средствами, которые пользователю запрещается осуществлять.

3) Порядок действий при необходимости отключения средств антивирусной защиты

4) Порядок действий пользователя по замене антивирусного средства

88) Необходимо ли оформлять Акт классификации для защищаемого помещения?

1) Да

2) Нет

3) По желанию заявителя

89) Какие разделы включает в себя технический паспорт на автоматизированную систему?

1) Структура, топология и размещение основных технических средств и систем относительно границ контролируемой зоны

2) Данные о классификации объекта информатизации

3) Перечень каналов утечки информации объекта информатизации

4) Сведения о методах проведения проверок объекта информатизации

90) К защищаемым помещениям относятся:

1) Помещения для ведения секретных переговоров

2) Помещения для проведения переговоров с обсуждением конфиденциальной информации

3) Помещения для хранения документов, содержащих информацию ограниченного доступа

4) Помещения для проведения совещания с доведением информации, содержащей коммерческую тайну

91) Выберите мероприятия, которые должен провести Заявитель в рамках подготовки к аттестации ОИ:

1) Провести классификацию объекта информатизации

2) Установить и настроить средства защиты информации

3) Определить вид информации, планируемой к обработке на объекте информатизации

4) Ввести объект информатизации в эксплуатацию

5) Разработать организационно-распорядительные документы по защите информации на объекте информатизации

92) Какое количество перечней сведений конфиденциального характера необходимо разработать в организации, если ведется обработка коммерческой тайны и персональных данных?

1) 0

2) 1

3) 2

93) Контролируемая зона – это

1) Пространство вокруг объекта информатизации, в котором запрещено обрабатывать информацию ограниченного доступа

2) Пространство вокруг объекта информатизации, в котором исключена возможность несанкционированного доступа к информации

3) Пространство вокруг объекта информатизации, в котором исключено неконтролируемое пребывание посторонних лиц, а также движение транспортных средств

94) Определите верный порядок действий при проведении работ по аттестации объекта информатизации:

1) Проведение аттестационных испытаний; разработка программы и методик аттестационных испытаний; оценка эффективности принятых мер по защите информации

2) Оценка эффективности принятых мер по защите информации; проведение аттестационных испытаний; разработка программы и методик аттестационных испытаний

3) Разработка программы и методик аттестационных испытаний; проведение аттестационных испытаний; оценка эффективности принятых мер по защите информации

4) Разработка программы и методик аттестационных испытаний; оценка эффективности принятых мер по защите информации; проведение аттестационных испытаний

95) Кто выбирает схему проведения работ по аттестации объекта информатизации заявителя?

1) Орган по аттестации

2) Заявитель

3) Заявитель, по согласованию со ФСТЭК России

4) ФСТЭК России, исходя из поданных органом по аттестации данных об объекте информатизации

96) В какой инструкции определяется порядок действий ответственного лица, которые необходимо осуществить до и после проведения закрытых совещаний и переговоров?

1) Инструкция по эксплуатации средств защиты информации на объекте информатизации - защищаемом помещении

2) Инструкция по обеспечению защиты информации, обсуждаемой в защищаемом помещении

3) Инструкция пользователю

4) Инструкция администратору безопасности

97) Содержит ли технический паспорт на автоматизированную систему данные об аттестации объекта информатизации?

1) Да

2) Нет

98) Какие документы разрабатываются в ходе аттестации объекта информатизации – автоматизированной системы?

1) Инструкция о порядке установки, настройки и эксплуатации средств защиты информации

2) Протокол оценки уровня подготовки кадров

3) Протокол оценки эффективности принятых мер по защите информации

4) Модель угроз безопасности информации

99) Какое право предоставляет «Аттестат соответствия» заявителю?

1) Проводить аттестацию собственных объектов информатизации

2) Обрабатывать информацию ограниченного доступа на любом автоматизированном рабочем месте заявителя

3) Осуществлять обработку информации на аттестованном объекте информатизации

4) Устанавливать на объекте информатизации средства защиты информации по желанию заявителя

100) На какой стадии жизненного цикла объекта информатизации проводится его аттестация по требованиям безопасности информации

1) На этапе ввода в эксплуатацию

2) До ввода в эксплуатацию

3) На любом этапе жизненного цикла

4) После ввода в эксплуатацию

101) Выберите верное определение аттестации в соответствии с "Положением по аттестации объектов информатизации по требованиям безопасности информации", утвержденным председателем Гостехкомиссии России 25 ноября 1994 г.:

1) Комплекс мероприятий по приведению объекта информатизации в соответствие с требованиями документов по защите информации

2) Комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России

3) Комплекс мер, направленных на исключение утечки информации, обрабатываемой на объекте информатизации

102) Если по результатам аттестационных испытаний были выявлены несоответствия защищаемого объекта информатизации установленным требованиям, то:

1) Проводятся мероприятия по уничтожению объекта информатизации.

2) Объект информатизации создается заново.

3) Проводятся дополнительные мероприятия с целью устранения выявленных недостатков и нарушений.

4) Выдается аттестат соответствия независимо от полученных результатов.

103) Допускается ли проведение аттестации объекта информатизации после ввода его в эксплуатацию

1) Да

2) Нет

104) Какова основная цель аттестации объекта информатизации для владельца коммерческих секретов?

1) Выполнение установленных законодательством требований по защите коммерческой тайны

2) С целью получения лицензии на деятельность по защите информации.

3) С целью реализации функций, возложенных на собственников бизнеса.

4) С целью защиты коммерческих секретов от утечки, разглашения или несанкционированного доступа.

105) Можно ли получить (приобрести) у органа по аттестации уже аттестованный объект информатизации?

1) Да, если он имеет Аттестат соответствия.

2) Нет.

3) Нет, если он не имеет сертификата соответствия.

4) Да.

106) Какой документ устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации?

1) Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации».

2) ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении…»

3) «Положение по аттестации объектов информатизации по требованиям безопасности информации».

4) ГОСТ РО 0043-003-2012 «Аттестация объектов информатизации…»

107) Укажите период времени, в течение которого может эксплуатироваться аттестованный объект информатизации:

1) В течение срока, определенного заявителем.

2) В течение срока, установленного в Федеральным законом

3) Пока в нем существует потребность.

4) В течение срока, установленного аттестатом соответствия.

108) Целью аттестации объекта информатизации является

1) Подтверждение правильности установки и настройки средств защиты информации.

2) Подтверждения правильности классификации автоматизированной системы.

3) Подтверждение правильности размещения объекта информатизации относительно границ контролируемой зоны.

4) Подтверждение соответствия системы защиты информации объекта информатизации установленным требованиям.

109) Когда заявитель может начать обработку информации ограниченного доступа на объекте информатизации?

1) После установки и размещения технических средств объекта информатизации.

2) После проведения классификации автоматизированной системы.

3) После получения Аттестата соответствия на объект информатизации.

4) После проведения проверки на отсутствие вирусов в автоматизированной системе.

Задания в открытой форме

1. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

2. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная).

3. Участники аттестации и их полномочия (компетенции).

4. Критически важные объекты инфраструктуры Российской Федерации: классификация и категории.

5. Задачи, функции, права и обязанности органов по аттестации. Деятельность аттестационных комиссий.

6. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.

7. Основные мероприятия по проведению аттестации объектов информатизации критически важных объектов на соответствие требованиям безопасности информации.

8. Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации критически важных объектов.

9. Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации критически важных объектов.

10. Экспертно-документальный метод проверки, применяемый при проведении аттестационных испытаний.

11. Инструментальный метод проверки, применяемый при проведении аттестационных испытаний с использованием контрольно-измерительной аппаратуры.

12. Этапы аттестации объектов информатизации критически важных объектов.

13. Подача заявки на рассмотрение и проведение аттестации. Анализ исходных данных по аттестуемому объекту информатизации.

14. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

15. Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации

16. Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний.

17. Заключение договоров на аттестацию. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

18. Проведение аттестационных испытаний объекта информатизации.

19. Оформление, регистрация и выдача «Аттестата соответствия». Порядок рассмотрения апелляций.

20. Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации критически важных объектов.

21. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации критически важных объектов.

22. Заключение аттестационной проверки: структура, содержание.

23. Протокол аттестационного испытания: структура, содержание.

24. Аттестат соответствия объектов информатизации критически важных объектов требованиям безопасности.

Задание на установление правильной последовательности

1) Укажите правильный порядок действий органа по аттестации при исполнении своих функций:

a. Разработка программы и методики аттестационных испытаний

b. Проведение анализа исходных данных по аттестуемому объекту

c. Проведение аттестации объектов информатизации

2) Выберите верный порядок действий:

a. Выбор СЗИ

b. Проведение классификации АС

c. Проверка эффективности СЗИ

d. Установка и настройка СЗИ

3) Определите верный порядок действий при проведении работ по аттестации объекта информатизации:

a. проведение аттестационных испытаний

b. оценка эффективности принятых мер по защите информации

c. разработка программы и методик аттестационных испытаний

d. оценка эффективности принятых мер по защите информации

4) Укажите правильный порядок степеней секретности:

a. Особо важный

b. Совершенно секретный

c. Секретный

5) В соответствии с документом, классификация АС включает следующие этапы:

a. Сравнение выявленных признаков АС с классифицируемыми.

b. Присвоение АС соответствующего класса защиты информации от НСД.

c. Выявление основных признаков АС, необходимых для классификации.

d. Разработка и анализ исходных данных.

6) Порядок сертификации во ФСТЭК России

1. Экспертиза результатов сертификационных испытаний

2. Заключение договора с испытательной лабораторией

3. Решение на проведение сертификационных испытаний

4.Заключение договора с органом по сертификации

5. Подача заявки на сертификацию во ФСТЭК России.

6. Сертификационные испытания.

7.Решение о выдаче сертификата.

8. Оформление результатов испытаний

9. Подготовка исходных данных.

7) Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

1.испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);

2.проведение аттестационных испытаний объекта информатизации;

3.оформление, регистрация и выдача "Аттестата соответствия";

4. подачу и рассмотрение заявки на аттестацию;

5. разработка программы и методики аттестационных испытаний;

6.осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;

7. предварительное ознакомление с аттестуемым объектом;

8. рассмотрение апелляций.

9.заключение договоров на аттестацию;

8) На этапе аттестационных испытаний объекта информатизации:

1. определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

2.оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных

нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

3.проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

4. проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

5. осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

6.проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

9) Общий порядок сертификации

1. Заключение Договора на проведение сертификационных испытаний

2. Подготовка исходных данных

3. Оформление Заявки на сертификацию

4. Экспертиза результатов сертификационных испытаний

5. Оформление Решения на проведение сертификации

6. Заключение Договора о проведении экспертизы результатов сертификационных испытаний в Органе по сертификации

7. Проведение сертификационных испытаний

8. Оформление Сертификата

9. Оформление Протоколов сертификационных испытаний и Технических заключений

10) порядок получения лицензии

a. оформить заявление

b. оплатить госпошлину

c. собрать все документы, необходимые для получения лицензии

Задание на установление соответствия

1) Соотнесите название закона с его номером

1."О безопасности".	a.№128.
2. "О *государственной тайне*".	b. № 2446-1
3. "О *лицензировании* отдельных видов деятельности"	c.№ 5485-1

2) Соотнесите название федеральных закона с его номером

1. "О техническом регулировании"	a.№149
2."Об информации, информационных технологиях и о защите информации"	b. № 152
3. "О *персональных данных*"	c.№184

3) Соотнесите органы по тех.защите информации с их названиями.

1 Комитет Государственной думы по безопасности	А основной орган внешней разведки Российской Федерации.
2 Совет безопасности России	В структура в Государственной Думе Федерального собрания России, в ведении которой находятся рассмотрение и подготовка законопроектов по вопросам безопасности государства и граждан.
3 Служба внешней разведки Российской Федерации (СВР России)	С совещательный орган, осуществляющий подготовку решений Президента Российской Федерации по вопросам обеспечения защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики по обеспечению национальной безопасности.

4) Соотнесите органы по тех.защите информации с их названиями.

1 Министерство обороны Российской Федерации (Минобороны России)	А федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки *персональных данных* требованиям законодательства Российской Федерации в области *персональных данных*, а также функции по организации деятельности радиочастотной службы.
2 Министерство внутренних дел Российской Федерации (МВД России)	В федеральный орган исполнительной власти (федеральное министерство), проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по вопросам обороны.
3 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)	С федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также по выработке государственной политики в сфере миграции.

5) Соотнесите свойства информации:

1 конфиденциальность информации	А состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
2 целостность информации	В состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
3 доступность информации	С состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

6) Соотнесите понятие и определение:

1 национальная безопасность	А прямая или косвенная возможность нанесения ущерба конституционным

	правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства;
2 национальные интересы Российской Федерации	В состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;
3 угроза национальной безопасности	С совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства;

7) Соотнесите понятие и определение:

1 стратегические национальные приоритеты	А Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации;
2 система обеспечения национальной безопасности	В важнейшие направления обеспечения национальной безопасности, по которым реализуются конституционные права и свободы граждан Российской Федерации, осуществляются устойчивое социально-экономическое развитие и охрана суверенитета страны, ее независимости и территориальной целостности;
3 силы обеспечения национальной безопасности	С силы и средства обеспечения национальной безопасности;

8) Установите соответствие класса защищённости АС и группы:

1 I группа	А классы 3Б и 3А.
2 II группа	В классы 1Д, 1Г, 1В, 1Б и 1А.
3 III группа	С классы 2Б и 2А.

9) Установите соответствие класса защищённости СВТ и группы:

1 I группа	А 4, 3 и 2 классы
2 II группа	В 7 класс

3 III группа	C 1 класс
4 IV группа	D 6 и 5 классы

10) Соотнесите стадию и ее этапы

1 Техническое (частное техническое) задание на разработку СЗИ	A разработка задания и проекта; разработка раздела технического проекта на объект информатизации в части защиты информации;
2 стадия проектирования и создания объекта информатизации	B приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком; аттестация объекта информатизации по требованиям безопасности информации.
3 стадия ввода в действие объекта информатизации	C обоснование разработки; класс защищенности АС; ссылку на нормативные документы;

Компетентностно-ориентированные задачи

1) Установить и настроить антивирус

2) Установить и настроить Dallas Lock

3) Установить и настроить Secret Net

4) Установить и настроить аппаратно-программный модуль доверенной загрузки «Соболь»

5) Установить и настроить Zemana AntiLogger

6) Установить и настроить KeyScrambler

7) Установить и настроить NextGen AntiKeylogger

8) Настройка прав пользователей

9) Настройка брандмауэра для защиты компьютеров в сети.

10) Установить и настроить Comodo Internet Security Suite.

Критерии оценки:

— задание в закрытой форме — 2 балла,
— задание в открытой форме — 2 балла,
— задание на установление правильной последовательности — 2 балла,
— задание на установление соответствия — 2 балла,
— решение компетентностно-ориентированной задачи — 3 балла.

Составитель  М.А. Ефремов

«31» 08 2021 г.