МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

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

Порядок проведения аттестации объектов информатизации
(наименование учебной дисциплины)

10.05.02 Информационная безопасность телекоммуникационных систем, направленность (профиль) «Управление безопасностью телекоммуникационных систем и сетей»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ

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:

3 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ К ЛАБОРАТОРНЫМ РАБОТАМ

Контрольные вопросы к лабораторной работе №1

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?
5. Перечислите отличия сертифицированных версий от версий общего пользования.

6. Можно ли устанавливать на сертифицированную операционную систему несертифицированные продукты?

Контрольные вопросы к лабораторной работе №2

1. Какие части документа относятся к вопросам защиты информации?
2. Что показывают комментарии к данному документу?
3. Дайте характеристику Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. О чем Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»?
5. Как менялся текст нормативного акта с момента его создания по настоящее время?
6. В чем заключаются основные принципы проектирования защищённых систем?

Контрольные вопросы к лабораторной работе №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 органы отвечают за обеспечение ИБ в стране?
6. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
7. Какова структура организационно-правовой основы защиты информации?
8. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

Критерии оценки:

6-7 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

4-5 баллов (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

2-3 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0-1 балл (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. 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

2. 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

3. 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.

4. Выберите из предложенного ниже списка возможные цели проведения аттестации объекта информатизации:

1) С целью защиты общедоступной информации, обрабатываемой на объекте информатизации.

2) С целью дальнейшего получения лицензии органом по аттестации.

3) С целью подтверждения соответствия реализованной на объекте информатизации системы защиты информации уровню безопасности информации, заданному владельцем объекта информатизации, исходя из требований по защите информации, установленных законодательством Российской Федерации.

4) С целью защиты коммерческой тайны, обрабатываемой на объекте информатизации.

5) С целью подтверждения отсутствия в автоматизированной системе компьютерных вирусов

5. Допускается ли проведение аттестации объекта информатизации после ввода его в эксплуатацию

1) Да

2) Нет

6. 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.

7. 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.

8. 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…»

9. 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.

10. Выполнения каких требований по защите информации необходимо добиться в ходе проведения аттестации объекта информатизации?

1) Требования по защите информации от несанкционированного доступа.

2) Требования по защите от непреднамеренных воздействий.

3) Требования по защите от преднамеренных воздействий.

4) Требования по защите информации от наводок.

11. 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.

12. 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.

13. В течение какого периода разрешается эксплуатировать аттестованный объект информатизации?

1) В течение срока, установленного в аттестате соответствия.

2) В течение срока, установленного ФСТЭК России.

3) В течение срока, определенного заявителем.

4) В течение срока, указанного в сертификате средства вычислительной техники ,входящие в состав объекта информатизации.

14. Какова основная цель аттестации объектов информатизации органов власти, обрабатывающих служебную информацию?

1) С целью реализации требований по наличию лицензий для участия в тендерах
2) Для получения лицензии на деятельность по ТЗКИ
3) Выполнение требований законодательства в области защиты информации в рамках реализации возложенных на них функций
4) Защита ноу-хау

15. Аттестация объекта информатизации проводится:

1) В реальных условиях эксплуатации
2) В специальной лаборатории органа по аттестации
3) В экранированной камере
4) На территории заявителя, в помещении площадью не менее 20 кв.м.

16. Выберите основные цели аттестации объектов информатизации для органа по аттестации?

1) Для получения лицензии на деятельность по ТЗКИ.
2) Выполнение требований по защите информации в рамках реализации возложенных на него функций.
3) С целью разработки документов ограниченного доступа для заявителей
4) Для защиты ноу-хау.

17. Выявление несоответствия объекта информатизации установленным требованиям влечет за собой?

1) Служебное разбирательство.

2) Выбор и аттестацию другого объекта информатизации.

3) Устранение недостатков и повторную аттестацию

4) Лишение органа по аттестации лицензии по ТЗКИ.

18. 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

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

1) Да

2) Нет

20. 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

21. 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

22. 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

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

1) Да

2) Нет

24. 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

25. Информация какого вида,в соответствие с федеральными законами, не может бытьотнесена 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

26. 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

27. 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

28. Оценка соответствия объекта информатизации требованиям безопасности информации осуществляется в ходе:

1) Лицензирования

2) Сертификации

3) Аккредитации

4) Аттестации

29. 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

30. 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

31. К какой государственной системе относится аттестация:

1) Лицензирования
2) Обеспечения государственной безопасности
3) Сертификации средств защиты информации
4) Защиты информации

32. Станут ли персональные данные общедоступной информацией при размещении ее в социальных сетях?

1) Нет
2) Да

33. Кто может выступать обладателем информации?

1) Индивидуальный предприниматель
2) Российская Федерация
3) Физическое лицо
4) Субъект Российской Федерации

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

1) Да
2) Нет

35. 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

36. 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

37. 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

38. Выберите объект испытаний при проведении процедуры лицензирования:

1) Объект информатизации
2) Средство защиты информации
3) Автоматизированная система
4) Юридическое лицо

39. 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

40. Выберите объект испытаний при проведении процедуры сертификации:

1) Объект информатизации
2) Изделие
3) Помещение для ведения конфиденциальных переговоров
4) Индивидуальный предприниматель

41. 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

42. В какой процедуре участвует третья сторона – испытательная лаборатория?

1) Аттестация

2) Аккредитация

3) Лицензирование

4) Сертификация

43. 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

44. Выберите виды мероприятий по защите информации:

1) Технические пассивные
2) Активные
3) Организационные пассивные
4) Технические активные
5) Организационные активные
6) Пассивные

45. Какой орган государственной власти является правопреемником Гостехкомиссии России?

1) ФАПСИ
2) ФСО
3) ФСТЭК
4) ФСБ

46. 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

47. 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

48. При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура:

1) Аттестации

2) Лицензирования

3) Сертификации

4) Аккредитации

49. Можно ли в качестве активной технической меры выбрать установку сертифицированной антивирусной программы?

1) Да

2) Нет

50. Оценка возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями проводится при:

1) Сертификации

2) Аттестации

3) Лицензировании

51. 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

52. 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

53. 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

54. 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

55. 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

56. 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

57. 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

58. 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

59. 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

60. 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

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

1) Да

2) Нет

62. 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 безопасностиинформации.

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

63. 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

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

1) Да

2) Нет

65. 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.

66. 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

67. Выберите верный перечень органов и организаций, входящих в организационную структуру системы аттестации объектовинформатизации:

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 безопасностиинформации, органы по аттестации, заявители.

68. 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

69. 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 специсследований на побочные электромагнитные излучения и наводки технических средств обработки информации

70. Если на объекте информатизации планируется обработка информации, составляющей коммерческую тайну, то заявителем в этом случае будет являться:

1) Юридическое лицо

2) Индивидуальный предприниматель

3) Государственный орган

4) Оператор персональных данных

71. Имеет ли право заявитель самостоятельно провести работы по подготовке и проведению аттестации своих объектов информатизации:

1) Да

2) Нет

3) Да, при условии наличия у него лицензии на соответствующий вид деятельности

4) Нет, запрещается аттестовывать собственные объекты информатизации

72. Выберите сводные перечни, ведение которых осуществляет ФСТЭК России в рамках системы сертификации средств защиты информации:

1) Перечень нарушений правил безопасности на аттестованных объектах информатизации

2) Перечень органов по аттестации объектов информатизации

3) Перечень сертифицированных средств защиты информации

4) Перечень аннулированных аттестатов соответствия

5) Перечень средств защиты информации, на которые аннулированы сертификаты соответствия

73. Участниками аттестации объектов информатизации по требованиям безопасности информации являются:

1) Органы по аттестации, Заявители, Федеральный орган по сертификации и аттестации

2) Лицензиаты, Заявители, Органы по аттестации

3) Испытательная лаборатория, Заявители, Федеральный орган по сертификации и аттестации

74. Если на объекте информатизации планируется обработка служебной информации, то заявителем в этом случае будет являться:

1) Юридическое лицо
2) Государственный орган
3) Индивидуальный предприниматель
4) Учреждение, подведомственное государственному органу

75. Может ли выступать заявителем орган государственной власти?

1) Да
2) Нет

76. В соответствии с Федеральным законом Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, обладатель информации обязан:

1) Ограничивать доступ к информации, если такая обязанность установлена федеральными законами
2) Принимать меры по защите информации
3) Предоставлять ее третьим лицам по первому требованию
4) Проводить аттестацию объектов информатизации независимо от вида обрабатываемой в нем информации

77. Какие перечни (реестры) ведет ФСТЭК России в рамках своих полномочий?

1) Сертифицированных средств защиты информации

2) Органов по аттестации

3) Проверяемых органов по аттестации

4) Лицензий на деятельность по ТЗКИ

5) Апелляций от заявителей

6) Перечень заявителей

78. Какие мероприятия осуществляет заявитель в процессе подготовки объекта информатизации к аттестации?

1) Классификация объекта информатизации

2) Закупка средств защиты информации

3) Определение вида обрабатываемой на объекте информации

4) Разработка приказа о вводе объекта в эксплуатацию

79. В каком документе определяется полный перечень изменений на объекте информатизации, о которых необходимо извещать орган по аттестации:

1) Приказ о вводе объекта информатизации в эксплуатацию

2) Технический паспорт на объект информатизации

3) Аттестат соответствия

4) Формуляр на объект информатизации

80. Если заявителем будет выступать юридическое лицо или индивидуальный предприниматель, какой вид информации они могут обрабатывать на объекте информатизации?

1) Государственная тайна

2) Служебная тайна

3) Персональные данные

4) Коммерческая тайна

81. Имеет ли право заявитель подать апелляцию во ФСТЭК России, в случае неудовлетворительного качества проведенных органом по аттестации работ?

1) Да

2) Нет

82. Если заявителем будет выступать государственный орган или подведомственное ему учреждение, какой вид информации они могут обрабатывать на объекте информатизации?

1) Коммерческая тайна

2) Государственная тайна

3) Служебная тайна

4) Персональные данные

83. Какую лицензию ФСТЭК России 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. Каким образом можно проверить наличие и действие лицензии органа по аттестации, имеющего право аттестовывать объекты информатизации, обрабатывающие информацию, не содержащую государственную тайну?

1) Посмотреть реестр органов по аттестации

2) Посмотреть реестр лицензий на деятельность по технической защите конфиденциальной информации

3) Посмотреть реестр системы сертификации

4) Посмотреть реестр аннулированных лицензий органов по аттестации

85. Кто обязан исполнять нормативные правовые акты и методические документы, изданные по вопросам деятельности ФСТЭК России?

1) Аппаратами органов государственной власти субъектов Российской Федерации

2) Организации и предприятия

3) Физические лица

4) Органы местного самоуправления

86. Кто может являться оператором персональных данных?

1) Орган власти
2) Юридическое лицо
3) Индивидуальный предприниматель
4) Физическое лицо

87. Имеет ли право ФСТЭК России выдавать предписания на приостановление работ на объектах информатизации?

1) Да
2) Нет

88. Какую форму оценки соответствия необходимо выбрать для аттестации объекта информатизации, обрабатывающего информацию служебного характера?

1) Оценка эффективности принятых мер по защите информации
2) Сертификационные испытания
3) Обязательная аттестация по требованиям безопасности информации
4) Добровольная аттестация по требованиям безопасности информации

89. Какой документ вводит понятия добровольной и обязательной аттестации объектов информатизации?

1) «Положением по аттестации объектов информатизации…», утвержденным председателем Гостехкомиссии России 25 ноября 1994 г.

2) «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденные приказом Гостехкомиссии России от 30 августа 2002г. № 282

3) Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

4) Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации …» от 17.03.2008 № 351

90. Какую форму оценки соответствия может выбрать оператор ИСПДн, не являющейся ГИС и не обрабатывающей ГТ:

1) Оператор вправе не проводить оценку соответствия

2) Добровольная аттестация по требованиям безопасности информации

3) Оценка эффективности реализованных в рамках системы защиты мер по обеспечению безопасности информации

4) Обязательная аттестация по требованиям безопасности информации

91. В том случае, если заявителем является государственный орган, информацию какого вида могут обрабатывать его объекты информатизации:

1) Служебная тайна

2) Персональные данные

3) Коммерческая тайна

4) Государственная тайна

92. Выберите из нижеприведенного списка виды объектов информатизации, подлежащие обязательной аттестации:

1) Объекты информатизации, обрабатывающие служебную тайну
2) Объекты информатизации, обрабатывающие государственную тайну
3) Информационные системы персональных данных
4) Объекты информатизации, обрабатывающие коммерческую тайну

93. Какую процедуру необходимо провести для помещения, предназначенного для ведения конфиденциальных переговоров?

1) Сертификационные испытания
2) Оценку эффективности принятых мер по защите информации
3) Обязательную аттестацию по требованиям безопасности информации
4) Добровольную аттестацию по требованиям безопасности информации

94. Проводится ли обязательная аттестации объекта информатизации, обрабатывающего информацию служебного характера:

1) Да
2) Нет
3) По желанию заявителя

95. Выберите из нижеприведенного списка виды объектов информатизации, не подлежащие обязательной аттестации:

1) Информационные системы персональных данных

2) Объекты информатизации, обрабатывающие служебную тайну

3) Объекты информатизации, обрабатывающие государственную тайну

4) Объекты информатизации, обрабатывающие коммерческую тайну

96. Какую форму оценки соответствия необходимо выбрать для информационной системы персональных данных, являющейся ГИС?:

1) Обязательную аттестацию по требованиям безопасности информации

2) Оценку достаточности мер по защите информации

3) Оценку эффективности принятых мер по защите информации

4) Добровольную аттестацию по требованиям безопасности информации

97. Если заявителем является коммерческая организация, информацию какого вида могут обрабатывать ее объекты информатизации:

1) Персональные данные

2) Служебная тайна

3) Государственная тайна

4) Коммерческая тайна

98. Какие виды аттестации установлены "Положением по аттестации объектов информатизации по требованиям безопасности информации", утвержденным председателем Гостехкомиссии России 25 ноября 1994 г.:

1) Обязательная и необязательная

2) Добровольная и принудительная

3) Добровольная и обязательная

4) Необязательная и принудительная

99. К объектам информатизации, подлежащим аттестации по требованиям безопасности информации относятся:

1) Средства защиты информации

2) Защищаемые помещения

3) Операционные системы и прикладные программы

4) Автоматизированные системы

100. Государственные информационные системы – это:

1) Системы, создаваемые государством для собственных нужд

2) Системы, создаваемые с целью реализации полномочий государственных органов

3) Системы, доступ к которым имеют только государственные органы

4) Системы, созданные для обеспечения обмена информацией между государственными органами

101. Является ли наличие на объекте информатизации государственной тайны обязательным условием для аттестации такого объекта?

1) Да

2) Нет

102. Допускается ли проведение аттестации ИСПДн, не являющейся ГИС и не обрабатывающей информацию, содержащую сведения, составляющие государственную тайну?

1) Да, если заявитель докажет такую необходимость органу по аттестации
2) Нет, поскольку ИСПДн не является ГИС
3) Да, по желанию заявителя
4) Нет
5) Нет, поскольку ИСПДн не обрабатывает государственную тайну

Задания в открытой форме

1) Реестр сертифицированных средств защиты информации ведет ….
2) … – осуществляет оплату работы членов аттестационной комиссии
3) … формирует аттестационную комиссию.
4) … осуществляет государственный контроль и надзор за соблюдением порядка аттестации объектов информатизации.
5) … – отвечает за нарушение правил эксплуатации аттестованного объекта информатизации.
6) … ФСТЭК России имеет право передать некоторые из своих функций государственного контроля и надзора по аттестации и за эксплуатацией аттестованных объектов информатизации.
7) … оплачиваются расходы ФСТЭК России по осуществлению контроля и надзора за соблюдением порядка аттестации и эксплуатацией аттестованных объектов.
8) В соответствии с Указом Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 № 188, к информации конфиденциального характера относятся ...

9) …. (Количество) перечней сведений конфиденциального характера необходимо разработать в организации, если ведется обработка коммерческой тайны и персональных данных?.

10) … – пространство вокруг объекта информатизации, в котором исключено неконтролируемое пребывание посторонних лиц, а также движение транспортных средств.

11) … — это защита от несанкционированного доступа к информации.

12) … – действие, которое потенциально может привести к нарушению безопасности.

13) … – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

14) … аспект. Означает, что нужно тщательно контролировать работу с данными, чтобы устранить возможность их утечки, а также предотвратить несанкционированный доступ к ним со стороны неизвестных людей.

15) … - помещение, в котором планируется в ходе закрытых совещаний обсуждать информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну.

16) … - в соответствии с этим документом проводится аттестация объектов информатизации.

17) ... - выбирает схему проведения работ по аттестации объекта информатизации заявителя.

18) При объединении двух автоматизированных систем разных классов посредством межсетевого экрана каждая система …

19) … - этим документом определены состав и содержание, а также форма программ и методик аттестационных испытаний.

20) С … согласовывается «Программа и методики аттестационных испытаний».

Задание на установление соответствия

1. Установить соответствие:

1) III группа – классы 3Б и 3А.	a) Это вероятный ущерб, который зависит от защищенности системы.
2) II группа – классы 2Б и 2А.	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3) I группа – классы 1Д, 1Г, 1В, 1Б и 1А.	c) В этих автоматизированных системах одновременно обрабатывается или хранится информация разных уровней конфиденциальности. Не все пользователи имеют доступ ко всей информации в АС.

2. Установить соответствие:

1) Служебная тайна	a) защищаемые ... сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб государству.
2) Государственная тайна	b) сведения, которые не относятся к .. тайне, доступ к которым ограничен органами … власти и федеральными органами исполнительной власти в соответствии с законодательством.
3) Информация ограниченного доступа	c) информация, доступ к которой ограничен в интересах обеспечения национальной безопасности в соответствии с законодательством о государственных секретах и иными нормативно-правовыми актами, регулирующими отношения в области защиты государственных секретов

3. Установить соответствие:

1) Персональные данные	a) общеизвестные сведения и иная информация, доступ к которой не ограничен
2) Общедоступная информация	b) любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу
3) Сведения, связанные с	c) сведения, связанные с …, доступ к которым ограничен в соответствии с

профессиональной деятельностью	Конституцией РФ и федеральными законами.

4. Установить соответствие:

1) Угроза безопасности	a) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	b) Это угроза раскрытия информации.
3) Атака	c) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
4) Угроза конфиденциальности	d) Это действие по использованию уязвимости; реализация угрозы.

5. Установить соответствие:

1) Угроза целостности	a) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3) Ущерб	c) Это угроза нарушения работоспособности системы при доступе к информации.
4) Риск	d) Это угроза изменения информации.

6. Установить соответствие:

1) Сертификация	a) подтверждение квалификации, уровня знаний и умений человека — отзыв, характеристика.
2) Аттестация	b) это форма подтверждения соответствия объектов установленным требованиям, осуществляемая органом.
3) Аккредитация	c) разрешение на право, либо право на выполнение некоторых действий, которое может удостоверяться одноимённым документом.

4) Лицензирование	d) процедура официального подтверждения соответствия объекта установленным критериям и показателям.

7. Установить соответствие:

1) Правовая защита информации	a) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
2) Техническая защита информации	b) защита информации с помощью ее криптографического преобразования.
3) Криптографическая защита информации	c) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
4) Физическая защита информации	d) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

8. Установить соответствие:

1) Обладатель информации	a) гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
2) Информационная система	b) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
3) Оператор информационной системы	c) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или

	ограничивать доступ к информации, определяемой по каким-либо признакам;.

9. Установить соответствие:

1) Канал связи	a) совокупность средств связи и канала связи, посредством которых осуществляется передача информации от источника к приемнику.
2) Линия связи	b) совокупность технических устройств, обеспечивающих передачу сигнала от источника к получателю.
3) Криптографическая защита информации	c) это защита информации с помощью ее криптографического преобразования.

10. Установить соответствие:

1) конфиденциальность информации	a) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.
2) целостность информации	b) состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
3) доступность информации	c) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

11. Установить соответствие:

1) Морально-этические меры	a) защита информации … методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением
2) Правовая защита	b) устоявшиеся в обществе нормы поведения.

3) Организационные меры защиты	c) меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой.

12. Установить соответствие:

1) угрозы конституционным правам и свободам человека	a) Сюда относится нарушение работы государственных СМИ, монополизация информационного рынка России.
2) угрозы информационному обеспечению государственной политики России.	b) Примером данного вида угроз может быть незаконное ограничение доступа к информации, намеренное дезинформирование или прослушивание телефона.
3) угрозы безопасности информационных и телекоммуникационных средств и систем	c) Сюда относятся противоправные сбор и обработка информации, хищение, утечка по техническим каналам и несанкционированный доступ к информации.

13. Установить соответствие:

1) Соблюдение принципа законности	a) предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.
2) Соблюдение принципа баланса интересов граждан, общества и государства в информационной сфере	b) включает в себя мероприятия по *информатизации* правовой сферы в целом.
3) Соблюдение принципа разработки механизмов правового	c) требует от федеральных органов государственной власти и органов государственной власти субъектов

обеспечения информационной безопасности Российской Федерации	Российской Федерации при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

14. Установить соответствие:

1) Закон Российской Федерации от 05.03.1992 № 2446-1	a) "О *государственной тайне*".
2) Закон Российской Федерации от 22.06.1993 № 5485-1	b) "О безопасности".
3) Федеральный закон №128 от 08.08.2001	c) "О *лицензировании* отдельных видов деятельности"

15. Установить соответствие:

1) Федеральный Закон №184 от 27.12.2002	a) "Об информации, информационных технологиях и о защите информации"
2) Федеральный Закон №149 от 27.07.2006	b) "О техническом регулировании"
3) Федеральный закон №152 от 27.07.2006	c) "О *персональных данных*"

16. Установить соответствие:

1) МВД России	a) 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.

2) Минобороны России	b) 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.
3) СВР России	c) основной орган внешней разведки Российской Федерации.
4) Роскомнадзор	d) 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.

17. Установить соответствие:

1) *Коммерческая тайна*	a) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);
2) Профессиональная тайна	b) сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
3) *Служебная тайна*	c) сведения, составляющие тайну следствия и судопроизводства, а также сведения о

	защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ и другими нормативными правовыми актами Российской Федерации;.
4) Тайна следствия и судопроизводства	d) - сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

18. Установить соответствие:

1) III группа	a) – классы 2Б и 2А.
2) II группа	b) – классы 3Б и 3А.
3) I группа	c) – классы 1Д, 1Г, 1В, 1Б и 1А.

19. Установить соответствие:

1) 7 класс защищённости СВТ от НСД	a) – верифицированная защита.
2) 6 и 5 классы	b) – мандатная защита.
3) 4, 3 и 2 классы	c) – дискреционная защита.
4) 1 класс	d) – СВТ, которые были представлены к оценке, однако не удовлетворяют требованиям более высоких классов.

20. Установить соответствие:

1) Федеральный орган по сертификации	a) организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации;

2) Центральный орган системы сертификации	b) осуществляет выбор способа подтверждения соответствия средств защиты информации требованиям нормативных документов;
3) Изготовители	c) маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации;

Задание на установление правильной последовательности

1. Установите верный порядок действий:
1) Выбор СЗИ, установка и настройка СЗИ.
2) Проверка эффективности СЗИ.
3) Проведение классификации АС.

2. Установите верный порядок действий при проведении работ по аттестации объекта информатизации:
1) Разработка программы и методик аттестационных испытаний;
2) Проведение аттестационных испытаний;
3) Оценка эффективности принятых мер по защите информации

3. Установите верный порядок действий работ по аттестации объекта информатизации:
1) Определение угроз безопасности информации
2) Разработка и реализация разрешительной системы доступа
3) Настройка сертифицированных средств защиты информации
4) Обучение сотрудников заявителя вопросам защиты информации с выдачей документа, подтверждающего прохождение обучения

4. Установите порядок сертификации:
1) Заключение Договора на проведение сертификационных испытаний
2) Подготовка исходных данных
3) Оформление Сертификата
4) Проведение сертификационных испытаний
5) Оформление Заявки на сертификацию
6) Оформление Решения на проведение сертификации
7) Оформление Протоколов сертификационных испытаний и Технических заключений
8) Заключение Договора о проведении экспертизы результатов сертификационных испытаний в Органе по сертификации
9) Экспертиза результатов сертификационных испытаний

5. Установите этапы классификация АС:

1) Сравнение выявленных признаков АС с классифицируемыми.

2) Присвоение АС соответствующего класса защиты информации от НСД.

3) Разработка и анализ исходных данных.

4) Выявление основных признаков АС, необходимых для классификации.

6. Установите этапы сертификации во ФСТЭК России:

1) Подача заявки на сертификацию во ФСТЭК России

2) Подготовка исходных данных

3) Сертификационные испытания

4) Решение на проведение сертификационных испытаний

5) Заключение договора с испытательной лабораторией

7. Установите этапы сертификации во ФСТЭК России:

1) Оформление результатов испытаний

2) Экспертиза результатов сертификационных испытаний

3) Решение о выдаче сертификата

4) Заключение договора с органом по сертификации

8. Установите порядок проведения аттестации объектов информатизации по требованиям безопасности информации:

1) Испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

2) Разработка программы и методики аттестационных испытаний.

3) Заключение договоров на аттестацию.

4) Проведение аттестационных испытаний объекта информатизации.

5) Подача и рассмотрение заявки на аттестацию

6) Предварительное ознакомление с аттестуемым объектом

9. Установите порядок сертификации:

1) Проведение сертификационных испытаний

2) Оформление Протоколов сертификационных испытаний и Технических заключений

3) Заключение Договора о проведении экспертизы результатов сертификационных испытаний в Органе по сертификации

4) Экспертиза результатов сертификационных испытаний

10. Установите порядок сертификации:

1) Оформление Сертификата

2) Оформление Заявки на сертификацию
3) Оформление Решения на проведение сертификации
4) Заключение Договора на проведение сертификационных испытаний
5) Подготовка исходных данных

11. Установите порядок обеспечения защиты информации в АС:
1) Стадия проектирования
2) Предпроектная стадия
3) Производится классификация ас
4) Стадии ввода в действие объекта информатизации

12. Установить этапы разработки программной документации:
1) Разработка технического проекта.
2) Комплексное внедрение программной документации.
3) Подготовка технического специального задания.
4) Составление подробного эскизного варианта проекта.
5) Оформление рабочего документа.

13. Установите этапы сертификации:
1) Оформление результатов испытаний
2) Экспертиза результатов сертификационных испытаний
3) Решение о выдаче сертификата
4) Заключение договора с органом по сертификации
5) Подача заявки на сертификацию во ФСТЭК России
6) Подготовка исходных данных
7) Сертификационные испытания
8) Решение на проведение сертификационных испытаний
9) Заключение договора с испытательной лабораторией

14. Установите порядок классов защищенности по возрастанию:
1) классы 3Б и 3А.
2) классы 2Б и 2А.
3) классы 1Д, 1Г, 1В, 1Б и 1А.

15. Установите верный порядок действий органа по аттестации при исполнении своих функций?
1) Проведение анализа исходных данных по аттестуемому объекту,
2) Разработка программы и методики аттестационных испытаний,
3) Проведение аттестации объектов информатизации

16. Установите порядок этапа «Технический проект»:
1) Разработка проектных решений по системе в целом и ее частям
2) Разработка заданий на проектирование в смежных частях проекта объекта автоматизации

3) Разработка документации на АСЗИ и ее части

4) Разработка и оформление документации на поставку изделий для комплектования АСЗИ

17. Установите порядок этапа «Ввод в действие»:

1) Подготовка АСЗИ к вводу в действие

2) Подготовка персонала

3) Комплектация АС поставляемыми изделиями (ПС и ТС)

4) Строительно-монтажные работы

5) Пуско-наладочные работы

18. Установите порядок этапа «Формирование требований к АС»:

1) Обследование объекта и обоснование необходимости создания АСЗИ

2) Оформление отчета о выполняемой работе и заявки на разработку АСЗИ

3) Формирование требований пользователя к АСЗИ

19. Установите верный порядок действий:

1) Проведение классификации ас,

2) Установка и настройка сзи,

3) Проверка эффективности сзи

4) Выбор сзи,

20. Установите порядок этапа «Разработка концепции АС»:

1) Изучение объекта

2) Проведение необходимых НИР

3) Разработка вариантов концепции АС и выбор варианта концепции АС

4) Оформление отчета о выполненной работе

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Какой класс может быть присвоен автоматизированной системе, если в ней работает один пользователь, допущенный ко всей информации автоматизированной системы, размещенной на носителях одного уровня конфиденциальности?
2. Если в результате объединения двух автоматизированных систем (АС 1 и АС 2) различных классов была сформирована новая автоматизированная система (АС3), какой класс должен быть ей присвоен?
3. Реализуйте управлением атрибутами файлов и катологов в Linux
   каталог – почтовый ящик
4. Выполните сохранение результатов скремблирования в файл с применением HEX-редактора.
5. Проконтролируйте обратимость преобразования при ассиметричном шифровании.
6. Подберите несколько вариантов закрытого ключа на основе открытого ключа в алгоритме RSA.
7. Реализуйте управлением атрибутами файлов и катологов в Linux
   возможность просмотра и перлюстрации общего файла для обмена информацией между пользователями
8. Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 32 бит.
9. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 120 узлов.
10. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 50 узлов.

11. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 80 узлов.

12. Определить максимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 32 бит.

13. Определить максимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 16 бит.

14. Сеть может передавать данные в двух режимах: с помощью дейтаграмм и по виртуальным каналам. Какие соображения вы бы приняли во внимание при выборе того или иного режима для передачи ваших данных, если главным критерием выбора для вас является скорость и надежность доставки?

15. В сети, поддерживающей технику виртуальных каналов, между узлами A и B существует три потока и три альтернативных маршрута. Можно ли направить каждый поток по отдельному маршруту?

16. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 9 Мбит/с и состоит из 50 узлов.

17. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 180 узлов.

18. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 180 узлов.

19. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 7 Мбит/с и состоит из 30 узлов.

20. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 110 узлов.

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по

результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.