


СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области


А.Н. Калугин
« 08. 2022 » г.

УТВЕРЖДАЮ
Зам. директора по УР
Иванешко И.В.
« 31 » 08 2022 г.

Комплект оценочных материалов для промежуточной аттестации
(другая форма аттестации - 8 семестр, дифференцированный зачет – 9 семестр)
по МДК.03.02 Применение комплексной системы защиты информации в
инфокоммуникационных системах и сетях связи
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем
связи
по специальности 11.02.15. Инфокоммуникационные сети и системы связи

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи.

Результатом освоения программы МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи является овладение студентами профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.

Результатом освоения программы МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи являются освоенные умения и усвоенные знания.

В результате освоения МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи студент должен уметь:

У1 - классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

- У2 - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;
- У3 - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;
- У4 - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
- У5 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
- У6 - выполнять тестирование систем с целью определения уровня защищенности;
- У7 - определять оптимальные способы обеспечения информационной безопасности;
- У8 - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;
- У9 - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;
- У10 - разрабатывать политику безопасности сетевых элементов и логических сетей;
- У11 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
- У12 - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;
- У13 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- У14 - защищать базы данных при помощи специализированных программных продуктов;
- У15 - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами;
- У16 - проводить мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
- У19 - производить выбор необходимых средств криптографической защиты информации;
- У20 - применять программные средства, реализующие основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;
- У21 - вырабатывать рекомендации для принятия решения о модернизации системы защиты информации;
- У22 - осуществлять мероприятия по защите персональных данных;
- знать:
- 31 - принципы построения информационно-коммуникационных сетей;
- 32 - международные стандарты информационной безопасности для проводных и беспроводных сетей;
- 33 - нормативно - правовые и законодательные акты в области информационной безопасности;
- 34 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;
- 35 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
- 36 - способы и методы обнаружения средств съёма информации в радиоканале;
- 37 - классификацию угроз сетевой безопасности;
- 38 - характерные особенности сетевых атак;
- 39 - возможные способы несанкционированного доступа к системам связи;
- 310 - правила проведения возможных проверок согласно нормативных документов ФСТЭК;
- 311 - этапы определения конфиденциальности документов объекта защиты;
- 312 - назначение, классификацию и принципы работы специализированного оборудования;
- 313 - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;

- 314 - методы и средства защиты информации в телекоммуникациях от вредоносных программ;
- 315 - технологии применения программных продуктов;
- 316 - возможные способы, места установки и настройки программных продуктов;
- 317 - методы и способы защиты информации, передаваемой по кабельным направляющим системам;
- 318 - конфигурации защищаемых сетей;
- 319 - алгоритмы работы тестовых программ;
- 320 - средства защиты различных операционных систем и среды передачи информации;
- 321 - способы и методы шифрования (кодирование и декодирование) информации;
- 322 - концепцию инженерно-технической защиты информации;
- 323 - методы оценки угрозы инженерно-технического добывания информации;
- 324 - основные принципы организации и методы реализации технической защиты информации;
- 325 - методы аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем передачи, хранения и обработки информации;
- 326 - методы инженерного расчета размеров контролируемой зоны;
- 327 - основные требования к системам криптографической защиты.

Другая форма аттестации и дифференцированный зачёт являются промежуточными формами контроля, подводят итог освоения программы МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи.

Другая форма аттестации проводится в форме тестирования, дифференцированный зачёт по МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи проводится в форме тестирования. На промежуточную аттестацию выделяется по 2 часа (последнее занятие в семестре) из общего количества часов на МДК.03.02.

Тест содержит два блока: блок 1 для 8 семестра (в 1 блоке 75 тестовых позиций и 75 теоретических вопросов с кратким ответом, блок 2 для 9 семестра (85 тестовых позиций и 80 теоретических вопросов с кратким ответом).

Тест для 8 семестра содержит 30 вопросов (суммарно 20 тестовых позиций и 10 теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока заданий.

Время тестирования – 90 минут (по 1,5 минуты на каждый вопрос тестовых позиций и по 2 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 40 минут.

Тест для 9 семестра содержит 30 вопросов (суммарно 20 тестовых позиций и 10 теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока заданий.

Время тестирования – 90 минут (по 1,5 минуты на каждый вопрос тестовых позиций и по 2 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 40 минут.

Результаты другой формы аттестации и дифференцированного зачета определяются на основании итогового ответа с оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», вносятся в учебный журнал группы и объявляются в тот же день.

Критерии оценивания:

5 баллов - получают студенты, справившиеся с работой 90-100%;

4 балла - ставится в том случае, если верные ответы составляют 75%-89% от общего количества;

3 балла - соответствует работа, содержащая 55-74% правильных ответов;

2 балла - соответствует работа, содержащая менее 55% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла
«удовлетворительно»	Студент набрал 3 балла
«неудовлетворительно»	Студент набрал 0-2 балла

Тестовое задание для другой формы аттестации
по МДК.03.02 Применение комплексной системы защиты информации в
инфокоммуникационных системах и сетях связи

Блок 1 (8 семестр)

1.	Информационная безопасность – это?	1.Состояние защищённости информационной среды. 2.Сохранность информационных ресурсов. 3.Защита конфиденциальности, целостности и доступности информации. 4.Все ответы не верны.
2.	Какие решения направлены на обеспечение информационной безопасности?	1.Высокопроизводительные системы защиты каналов. 2.Автоматизированные системы в защищенном исполнении. 3.Защита периметра информационной системы. 4.Все ответы верны.
3.	Что входит в комплексную систему защиты информации?	1. Средства управления учетными записями. 2. Средства управления событиями. 3. Средства защищенного доступа. 4. Средства контроля защищенности. 5. Средства разделения физической сети на несколько логических сетей.
4.	Что не относится к государственным органам РФ, контролирующим деятельность в области защиты информации?	1.Комитет Государственной думы по безопасности. 2.Совет безопасности России. 3.Федеральная служба по техническому и экспортному контролю. 4.Служба экономической безопасности.
5.	Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?	1.Доступность 2.Целостность 3.Конфиденциальность 4.Управляемость 5.Надежность
6.	Что такое доступность информации?	1.Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия. 2.Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов. 3.Свойство системы, обеспечивать закрытый доступ к информации любых субъектов. 4.Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)
7.	Что такое целостность информации?	1.Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). 2.Свойство информации, заключающееся в возможности ее изменения любым субъектом 3.Свойство информации, заключающееся в возможности изменения только единственным пользователем 4.Свойство информации, заключающееся в ее

		существовании в виде единого набора файлов.
8.	Что такое конфиденциальность информации?	<ol style="list-style-type: none"> 1.Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней. 2.Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). 3.Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора. 4.Свойство информации, заключающееся в ее шифровании. 5.Свойство информации, заключающееся в ее принадлежности к определенному набору.
9.	Какие документы относятся к актам федерального законодательства?	<ol style="list-style-type: none"> 1.Международные стандарты. 2.Международные договоры РФ. 3.Приказы ФСБ. 4.Указы президента РФ.
10.	Что относится к угрозам информационной безопасности?	<ol style="list-style-type: none"> 1.Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию. 2.Классификация информации. 3.Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.). 4.Сбои и отказы оборудования (технических средств) АС. 5.Ошибки эксплуатации. (пользователей, операторов и другого персонала). 6.Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов). 7.Последствия ошибок проектирования и разработки компонентов АС. (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.). 8.Иерархическое расположение данных.
11.	Какие угрозы безопасности информации являются преднамеренными?	<ol style="list-style-type: none"> 1.Взрыв в результате теракта. 2.Поджог. 3.Забастовка. 4.Ошибки персонала. 5.Неумышленное повреждение каналов связи. 6.Некомпетентное использование средств защиты. 7.Утрата паролей, ключей, пропусков. 8.Хищение носителей информации. 9.Незаконное получение паролей.
12.	Какие угрозы безопасности информации являются непреднамеренными?	<ol style="list-style-type: none"> 1.Взрыв в результате теракта. 2.Поджог. 3.Забастовка. 4.Ошибки персонала. 5.Неумышленное повреждение каналов связи. 6.Некомпетентное использование средств защиты. 7.Утрата паролей, ключей, пропусков. 8.Хищение носителей информации.

13.	Что относится к правовым мерам защиты информации?	<ol style="list-style-type: none"> 1. Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения. 2. Действия правоохранительных органов для защиты информационных ресурсов. 3. Организационно-административные меры для защиты информационных ресурсов. 4. Действия администраторов сети защиты информационных ресурсов.
14.	Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности?	<ol style="list-style-type: none"> 1. Уголовная 2. Административно-правовая. 3. Гражданско-правовая. 4. Дисциплинарная. 5. Материальная. 6. Условная. 7. Договорная.
15.	Что такое государственная тайна?	<ol style="list-style-type: none"> 1. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. 2. Сведения о состоянии окружающей среды. 3. Все сведения, которые хранятся в государственных базах данных. 4. Сведения о состоянии здоровья президента РФ. 5. Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне.
16.	Какие правовые документы решают вопросы информационной безопасности?	<ol style="list-style-type: none"> 1. Уголовный кодекс РФ. 2. Конституция РФ. 3. Закон "Об информации, информатизации и защите информации". 4. Закон РФ "О государственной тайне". 5. Закон РФ "О коммерческой тайне". 6. Закон РФ "О лицензировании отдельных видов деятельности". 7. Закон РФ "Об образовании". 8. Закон РФ "Об электронной цифровой подписи".
17.	Что относят к физическим средствам защиты?	<ol style="list-style-type: none"> 1. Стены. 2. Заграждения. 3. Решетки. 4. Межсетевые экраны 5. Ударо- и взрывостойкое остекление. 6. Устройства хранения. 7. Замки (механические, электрические, электромеханические, гидравлические)
18.	Какую информацию запрещено относить к информации ограниченного доступа?	<ol style="list-style-type: none"> 1. Информацию о чрезвычайных ситуациях. 2. Информацию о деятельности органов государственной власти. 3. Документы открытых архивов и библиотек. 4. Все, перечисленное в остальных пунктах.
19.	Какой из перечисленных законодательных актов обладает наибольшей юридической силой в вопросах информационного права?	<ol style="list-style-type: none"> 1. Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне". 2. ГК РФ. 3. Закон "Об информации, информатизации и защите информации". 4. Конституция РФ.

20.	Что понимается под средствами физического управления доступом?	<ol style="list-style-type: none"> 1. Механические, электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации. 2. Силовые действия охраны организации против потенциальных нарушителей. 3. Указания в инструкциях на мероприятия по поддержанию физической формы сотрудников 4. Программные меры защиты, предназначенные для создания препятствий потенциальным нарушителям. 5. Информационное обеспечение секретных задач.
21.	Какие задачи решает система физической защиты?	<ol style="list-style-type: none"> 1. Предупреждение несанкционированного доступа, нерегламентированных воздействий. 2. Задержка нарушителей, их выявления на объекте. 3. Реагирование сотрудников службы безопасности. 4. Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 5. Обеспечение целостности программно-аппаратной среды
22.	Какие компоненты входят в комплекс защиты охраняемых объектов?	<ol style="list-style-type: none"> 1. Сигнализация 2. Охрана 3. Датчики 4. Телевизионная система 5. Устройства несанкционированного доступа, нерегламентированных воздействий. 6. Устройства обеспечения целостности программно-аппаратной среды.
23.	Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	<ol style="list-style-type: none"> 1. Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 2. Обеспечение функций регистрации и учета событий безопасности. 3. Обеспечение неизменности (целостности) программно-аппаратной среды применяемых программных и программно-технических средств. 4. Задержка нарушителей, их выявление на объекте. 5. Реагирование сотрудников службы безопасности.
24.	Какие существуют виды угроз информационной безопасности (внешние и внутренние)?	<ol style="list-style-type: none"> 1. Несанкционированный доступ 2. Угроза утечки информации 3. Мошенничество 4. Кибервойны и кибертерроризм 5. Угроза аутентификации пользователей. 6. Верификация.
25.	Какие из перечисленных средств относятся к средствам обнаружения угроз?	<ol style="list-style-type: none"> 1. Охранная сигнализация. 2. Охранное телевидение. 3. Ударо- и взрывостойкое остекление. 4. Устройства хранения. 5. Электромеханические и гидравлические замки.
26.	Что из перечисленного является угрозами конфиденциальности информации:	<ol style="list-style-type: none"> 1. Маскарад. 2. Карнавал. 3. Переадресовка. 4. Перехват данных. 5. Блокирование. 6. Злоупотребления полномочиями.
27.	Что из перечисленного относится к инженерным средствам защиты?	<ol style="list-style-type: none"> 1. Аутентификация. 2. Средства удаленного администрирования автоматизированных рабочих мест и серверов.

		<p>3. Ограждение периметра ПС и внутренних зон ограниченного доступа.</p> <p>4. Контрольно-пропускные пункты (КПП) с соответствующим досмотровым оборудованием.</p> <p>5. Въездные ворота, калитки, шлагбаумы.</p>
28.	Какие существуют технические каналы утечки информации?	<p>1. Визуально-оптические каналы утечки информации.</p> <p>2. Акустические каналы утечки информации.</p> <p>3. Электромагнитные каналы утечки информации (или каналы утечки информации по ПЭМИН).</p> <p>4. Материально-вещественные каналы утечки информации.</p> <p>5. Визуально-вещественные каналы утечки информации.</p> <p>6. Все ответы верны.</p>
29.	Что такое процедура?	<p>1. Правила использования программного и аппаратного обеспечения в компании.</p> <p>2. Пошаговая инструкция по выполнению задачи.</p> <p>3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах.</p> <p>4. Обязательные действия.</p>
30.	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?	<p>1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски.</p> <p>2. Когда риски не могут быть приняты во внимание по политическим соображениям.</p> <p>3. Когда необходимые защитные меры слишком сложны.</p> <p>4. Когда стоимость контрмер превышает ценность актива и потенциальные потери.</p>
31.	Как классифицируются технические каналы акустической (речевой) утечки информации в зависимости от физической природы возникновения информационных сигналов, среды их распространения?	<p>1. Прямые акустические (воздушные).</p> <p>2. Акустиковибрационные.</p> <p>3. Акустооптические (лазерные).</p> <p>4. Акустоэлектрические.</p> <p>5. Акустовизуальные.</p> <p>6. Все ответы верны.</p>
32.	Что из перечисленного является косвенными каналами утечки информации?	<p>1. Пропажа, кража или потеря информационного накопителя, исследование удаленной корзины.</p> <p>2. Прослушивание, дистанционные снимки.</p> <p>3. Перехват электромагнитных устройств.</p> <p>4. Утечка данных из-за несоблюдения режима коммерческой тайны.</p> <p>5. Непосредственное копирование данных.</p>
33.	Что такое анализ защищенности ИТ-инфраструктуры?	<p>1. Анализ защищенности – это неконтролируемое техническое воздействие, направленное на выявление минимального количества уязвимостей в исследуемой ИТ-инфраструктуре.</p> <p>2. Анализ защищенности – это контролируемое техническое воздействие, направленное на выявление максимального количества уязвимостей и недостатков в исследуемой ИТ-инфраструктуре или информационной системе.</p> <p>3. Анализ защищенности – это организационное воздействие, направленное на выявление потерь от угрозы информационной безопасности в исследуемой ИТ-инфраструктуре или информационной системе.</p>
34.	Какие задачи решаются при проведении анализа защищенности?	<p>1. Выполнение требований регуляторов.</p> <p>2. Получение представления о текущем уровне защищенности системы.</p> <p>3. Оценка защищенности ИТ-инфраструктуры и эффективности используемых механизмов защиты.</p> <p>4. Получение подробной картины уязвимостей и недостатков исследуемой системы.</p>

		5.Все, перечисленное в остальных пунктах.
35.	Когда рекомендуется проводить работы по анализу защищенности?	1.При первичной установке информационной системы. 2.При публикации новой версии используемой ИС. 3.При внесении существенных изменений в систему или инфраструктуру. 4.По прошествии длительного периода времени с последней проверки. 5.Все, перечисленное в остальных пунктах.
36.	Какая угроза возникает всякий раз, когда в результате преднамеренных действий умышленно блокируется доступ к некоторому ресурсу информационной системы?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
37.	Какая угроза заключается в том, что информация становится известна неавторизованному пользователю?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
38.	Какая угроза включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую?	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
39.	Сколько классов защищенности автоматизированных систем от несанкционированного доступа к информации выделено в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации», часть 1?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
40.	На сколько групп разделены классы автоматизированных систем согласно специфическим особенностям обработки информации в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации»?	1. 4 группы. 2. 7 групп. 3. 3 группы. 4. 2 группы. 5. 5 групп.
41.	К какой группе относятся АСОД, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
42.	К какой группе относятся АСОД, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности?	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
43.	К какой группе относятся многопользовательские АСОД, в которых одновременно обрабатывается и/или	1.Третья группа. 2.Вторая группа. 3.Первая группа.

	хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации?	4. Четвертая группа.
44.	На сколько групп классы защищенности СВТ подразделяются в зависимости от реализованных моделей защиты и надежности их проверки?	1. Две группы. 2. Три группы. 3. Четыре группы. 4. Шесть групп.
45.	Какая группа классов защищенности СВТ включает только один седьмой класс - минимальная защищенность?	1. Первая группа. 2. Вторая группа. 3. Третья группа. 4. Четвертая группа.
46.	Какая группа классов защищенности СВТ характеризуется избирательной защитой, которая предусматривает контроль доступа поименованных субъектов к поименованным объектам, и включает шестой и пятый классы?	1. Первая группа. 2. Вторая группа. 3. Третья группа. 4. Четвертая группа.
47.	Что из перечисленного является прямыми каналами утечки информации?	1. Прослушивание, дистанционные снимки. 2. Перехват электромагнитных устройств. 3. Человеческий фактор. 4. Утечка данных из-за несоблюдения режима коммерческой тайны. 5. Непосредственное копирование данных.
48.	Какая группа классов защищенности СВТ характеризуется верифицированной защитой и содержит только первый класс?	1. Первая группа. 2. Вторая группа. 3. Третья группа. 4. Четвертая группа.
49.	Сколько классов защищенности СВТ установлено в Руководящем документе ГТК?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
50.	При каких режимах обработки информации средствами вычислительной техники возникают побочные электромагнитные излучения?	1. Вывод информации на экран монитора. 2. Ввод данных с клавиатуры. 3. Запись информации на накопители. 4. Чтение информации с накопителей. 5. Передача данных в каналы связи. 6. Вывод данных на периферийные печатные устройства - принтеры, плоттеры. 7. Запись данных от сканера на магнитный носитель. 8. Все ответы верны.
51.	Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	1. Перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ. 2. Перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС. 3. Перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ. 4. Съём информационных сигналов с линий электропитания ТСПИ. 5. Съём информационных сигналов с цепей заземления ТСПИ и ВТСС.
52.	Что из перечисленного относится к электрическим каналам утечки информации (КУИ)?	1. Съём наводок ПЭМИ ТСПИ с соединительных линий ВТСС и посторонних проводников. 2. Съём информационных сигналов с линий электропитания ТСПИ. 3. Съём информационных сигналов с цепей заземления ТСПИ и ВТСС. 4. Съём информации путем установки в ТСПИ

		<p>электронных устройств перехвата информации.</p> <p>5. Перехват побочных электромагнитных излучений (ПЭМИ) элементов ТСПИ.</p> <p>6. Перехват ПЭМИ на частотах работы высокочастотных (ВЧ) генераторов в ТСПИ и ВТСС.</p>
53.	Что из перечисленного является целями и задачами технической защиты информации?	<p>1. Предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения.</p> <p>2. Защита носителей информации от уничтожения в результате различных природных и техногенных воздействий.</p> <p>3. Предотвращение утечки информации по различным техническим каналам.</p> <p>4. Использование лицензионного ПО, или прошедших аттестацию программ по защите клиентов и личных данных.</p> <p>5. Систематическое обновление программного обеспечения.</p>
54.	Какие объекты относятся к критической информационной инфраструктуре (КИИ)?	<p>1. Информационные системы.</p> <p>2. Телекоммуникационные сети.</p> <p>3. Автоматизированные системы управления технологическими процессами.</p> <p>4. Все, перечисленное в остальных пунктах.</p>
55.	Как называют единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках?	<p>1. Критическая информационная инфраструктура (КИИ).</p> <p>2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).</p> <p>3. Межгосударственная нормативно-методическая комиссия (МНМК).</p> <p>4. Система оперативно-розыскных мероприятий (СОРМ).</p>
56.	Как называют документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей?	<p>1. Нормативно-методический документ.</p> <p>2. Стандарт.</p> <p>3. Руководящий документ.</p> <p>4. Нормативно правовой акт.</p>
57.	Какие из перечисленных функций являются основными функциями ФСТЭК?	<p>1. Проведение единой технической политики и координация работ по защите информации</p> <p>2. Организация и контроль над проведением работ по защите информации в организациях и учреждениях от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения.</p> <p>3. Поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.</p> <p>4. Все, перечисленное в остальных пунктах.</p>
58.	Что такое техническая защита информации?	<p>1. Защита информации с помощью ее криптографического преобразования.</p> <p>2. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств.</p> <p>3. Защита информации путем применения</p>

		организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
59.	Что такое физическая защита информации?	1. Защита информации с помощью ее криптографического преобразования. 2. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств 3. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
60.	Что такое криптографическая защита информации?	1. Защита информации с помощью ее криптографического преобразования. 2. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств 3. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.
61.	Какие угрозы называют естественными угрозами?	1. Угрозы ИБ АС, вызванные деятельностью человека. 2. Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 3. Угрозы, вызванные воздействиями на АС и ее компоненты физических процессов, зависящими от человека.
62.	Какие угрозы называют искусственными угрозами?	1. Угрозы ИБ АС, вызванные деятельностью человека. 2. Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 3. Угрозы, вызванные воздействиями на АС и ее компоненты физических процессов, независящими от человека.
63.	Что такое модель угроз информационной безопасности?	1. Угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека. 2. Описание существующих угроз ИБ, их актуальности, возможности реализации и последствий. 3. Угрозы ИБ АС, вызванные деятельностью человека.
64.	Операционные системы какого типа устанавливаются на средства вычислительной техники общего назначения, такие как АРМ, серверы, смартфоны, планшеты, телефоны?	1. Операционные системы типа «А». 2. Операционные системы типа «Б». 3. Операционные системы типа «В».
65.	Операционные системы какого типа устанавливаются в специализированные технические средства, решающие заранее определенные наборы задач?	1. Операционные системы типа «А». 2. Операционные системы типа «Б». 3. Операционные системы типа «В».
66.	Операционные системы какого типа предназначены для обеспечения реагирования на события в рамках заданных временных ограничений при	1. Операционные системы типа «А». 2. Операционные системы типа «Б». 3. Операционные системы типа «В».

	заданном уровне функциональности?	
67.	Какие виды средств защиты информации должны содержаться в информационных системах общего пользования?	<ol style="list-style-type: none"> 1.СЗИ от неправомерных действий (в том числе средства криптографической защиты информации). 2.Средства обнаружения вредоносных программ (в том числе антивирусные средства). 3.Средства контроля доступа к информации (в том числе средства обнаружения компьютерных атак). 4.Средства фильтрации и блокирования сетевого трафика (в том числе средства межсетевого экранирования). 5. Все, перечисленное в остальных пунктах.
68.	Как условно разделяются ценные активы организации в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»?	<ol style="list-style-type: none"> 1. Временные и финансовые. 2.Основные и вспомогательные. 3.Неопределенные и определенные.
69.	Что из перечисленного относится к основным активам организации?	<ol style="list-style-type: none"> 1. Место функционирования организации - пределы контролируемой зоны, в которой функционирует информационная система. 2. Бизнес-процессы - совокупность различных видов деятельности, в результате которой создается продукт или услуга, представляющие интерес для потребителя. 3. Информация - сведения, являющиеся предметом собственности, подлежащие защите от нарушения конфиденциальности, целостности и доступности, в соответствии с требованиями правовых документов и требованиями владельца информации, вне зависимости от формы представления. 4.Сведения, компрометация которых никаким образом не повлияет на деятельность организации.
70.	Какие важные задачи решаются при создании системы физической защиты (СФЗ) объекта?	<ol style="list-style-type: none"> 1.Установку режимов доступа, прием и обработка информации со считывателей. 2.Предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения активов организации. 3.Защита объекта от воздействия стихийных сил и прежде всего, пожара и воды.
71.	Какие мероприятия по управлению ИБ реализуют при размещении оборудования?	<ol style="list-style-type: none"> 1.Оборудование необходимо размещать так, чтобы свести до минимума излишний доступ в места его расположения. 2.Средства обработки и хранения важной информации следует размещать так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием. 3.Должны быть сведены к минимуму риски потенциальных угроз ИБ, включая: воровство; пожар; взрыв; задымление; затопление; пыль; вибрацию; химические эффекты; помехи в электроснабжении; электромагнитное излучение. 4.Важно проводить мониторинг состояния окружающей среды для выявления условий, которые могли бы неблагоприятно повлиять на функционирование СОИ. 5.Необходимо разработать меры по ликвидации последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание

		<p>воды через крышу, взрыв на улице.</p> <p>6. Все, перечисленное в остальных пунктах.</p>
72.	<p>Каким образом обеспечивают подачу электропитания при перебоях в подаче электроэнергии и других сбоях, связанных с электричеством?</p>	<p>1.Наличие нескольких источников электропитания.</p> <p>2.Применение устройств бесперебойного электропитания (UPS).</p> <p>3.Использование резервного генератора, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника.</p> <p>4. Все, перечисленное в остальных пунктах.</p>
73.	<p>Какие мероприятия проводят для силовых и телекоммуникационных кабельных сетей, по которым передаются данные или предоставляются другие ИТ-сервисы, для защиты от перехвата информации или повреждения?</p>	<p>1.Силовые и телекоммуникационные линии, связывающие СООИ, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой.</p> <p>2.Сетевой кабель должен быть защищен от несанкционированных подключений или повреждения, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков.</p> <p>3.Применение устройств бесперебойного электропитания (UPS).</p> <p>4.Силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи.</p> <p>5.Использование бронированных кожухов, закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках, дублирующих маршрутов прокладки кабеля или альтернативных способов передачи, оптоволоконных линий связи, а также проверки на подключение несанкционированных устройств к кабельной сети.</p>
74.	<p>Для обеспечения непрерывной работоспособности и целостности в организации постоянно проводится надлежащее техническое обслуживание (ТО) оборудования. Какие меры следует применять для этих целей?</p>	<p>1.Оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком.</p> <p>2.Необходимо, чтобы ТО и ремонт оборудования проводились только санкционированными лицами (персоналом).</p> <p>3.Следует хранить записи обо всех случаях, предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного ТО.</p> <p>4.Необходимо принимать соответствующие меры безопасности при отправке оборудования для ТО за пределы организации.</p> <p>5. Все, перечисленное в остальных пунктах.</p>
75.	<p>Служебная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования. Какие мероприятия по управлению ИБ следует применять в этом случае?</p>	<p>1.Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать защищенным образом.</p> <p>2.Использовать стандартные функции удаления.</p> <p>3.Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного ПО.</p> <p>4.Проводить оценку рисков в отношении носителей данных, содержащих важную информацию, с целью определения целесообразности их разрушения, восстановления или выбраковки.</p>

Вопросы задания открытого типа для другой формы аттестации
по МДК.03.02 Применение комплексной системы защиты информации в
инфокоммуникационных системах и сетях связи

Блок 1 (8 семестр)

1. Какие компоненты входят в комплекс защиты охраняемых объектов?
2. Как определить класс защищенности системы?
3. Какие существуют виды инженерно-технических средств безопасности?
4. Какие существуют возможные способы организации утечки информации?
5. Что такое технические каналы утечки информации (ТКУИ)?
6. Каким образом классифицируются каналы утечки информации?
7. Что входит в структуру канала утечки информации?
8. Что такое конфиденциальность информации?
9. Что такое целостность информации?
10. Что такое доступность информации?
11. В чем заключается угроза раскрытия информации?
12. В чем заключается угроза целостности?
13. Когда возникает угроза отказа служб?
14. Что понимают под контролируемой зоной?
15. Что такое злонамеренные радиоэлектронные средства (ЗРЭС)?
16. Что называется каналом радиосвязи?
17. Какие бывают каналы связи?
18. Для каких целей предназначены системы радиосвязи?
19. Что понимают под термином «средство негласной активации сотового телефона»?
20. Что такое инфракрасный микрофон?
21. Как называют техническое средство, перехватывающее не акустическую, а вибрационную информацию (звуковые колебания, распространяющиеся по элементам конструкции здания)?
22. Как работает лазерный стетоскоп?
23. Какая деятельность называется защитой информации?
24. Как называется защита информации, заключающаяся в обеспечении безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств?
25. Как называется защита информации, применяющая организационные мероприятия и средства, создающие препятствия для проникновения неуполномоченных физических лиц к объекту защиты?
26. Что называют естественными угрозами безопасности информации?
27. Что называют искусственными угрозами безопасности информации?
28. Что понимают под моделью угроз информационной безопасности?
29. При построении модели угроз безопасности часто используют банк данных угроз безопасности информации ФСТЭК России. Где находится эта электронная база?
30. Какая структура определяет порядок и координирует действия обеспечения некриптографическими методами ИБ?
31. Какая структура определяет порядок и координирует действия обеспечения криптографическими методами ИБ?
32. Как называется совокупность требований в части защиты СВТ и АС?
33. Какие технические средства применяют для выявления радиозакладных устройств (РЗУ)?
34. Сколько определено ФСТЭК классов защищенности автоматизированных систем?
35. Как работает скремблер?
36. Что такое закладные устройства?
37. Что понимают под политикой информационной безопасности оператора связи?
38. Какой вид передачи информации называют радиосвязью?
39. Что понимают под радиовещанием?
40. Как называют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?

41. Какую информацию о человеке можно отнести к персональным данным?
42. Что такое модель нарушителя информационной безопасности?
43. С какой целью проводится анализ защищенности?
44. Какой способ защиты информации заключается в создании на пути распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры?
45. Какой способ защиты информации предполагает преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется?
46. К каким способам защиты информации относятся криптографические методы преобразования информации, скрывание объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы?
47. К какому способу защиты информации относится разработка таких правил обращения с конфиденциальной информацией, которые позволили бы максимально затруднить получение этой информации злоумышленником?
48. Как называется способ защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности?
49. Что такое система виброакустической защиты?
50. Какие средства защиты информации относятся к формальным средствам?
51. Какие средства защиты информации относятся к неформальным средствам?
52. К каким средствам защиты относятся механические, электрические, электромеханические устройства и системы, создающие препятствия на пути дестабилизирующих факторов?
53. К каким средствам защиты относятся различные электронные и электронно-механические устройства, встраиваемые в аппаратуру системы обработки данных, для решения задач защиты информации?
54. Какие средства защиты объединены в класс технических средств защиты информации?
55. К каким средствам защиты относятся специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем, с целью решения задач защиты информации?
56. К каким средствам защиты относятся организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей?
57. Для каких целей применяют индикатор поля?
58. Для каких целей применяют детектор радиоизлучающих устройств?
59. Для каких целей используют блокиратор сотовых телефонов?
60. Для каких целей используют индикатор электрических сигналов?
61. Какие средства защиты используются для проведения анализа защищенности?
62. Какова основная цель проведения анализа защищенности?
63. Зачем нужно проводить тестирование на проникновение (пентест) в рамках инструментального анализа защищенности?
64. По каким сценариям проводят тестирование на проникновение?
65. Что содержит реестр идентификации оборудования EIR?
66. Какие списки формирует реестр идентификации оборудования EIR?
67. Где производится аутентификация абонента, а точнее - SIM?
68. На какие группы подразделяются категории обрабатываемых персональных данных?
69. Как называют совокупность средств контроля и управления физическим доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью?
70. Что такое периметр безопасности?
71. Какой регулятор ИБ осуществляет организацию и контроль над проведением работ по защите информации от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами?
72. Какой регулятор ИБ осуществляет поддержание и развитие сегмента международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации?

73. Как называется единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках?

74. Что входит в состав объектов критической информационной инфраструктуры?

75. Как называют сотрудников, которым доступна конфиденциальная информация организации, где они работают и которые могут использовать секреты в корыстных целях, провоцируя умышленные утечки информации?

Тестовое задание закрытого типа для дифференцированного зачета
по МДК.03.02 Применение комплексной системы защиты информации в
инфокоммуникационных системах и сетях связи
Блок 2 (9 семестр)

1.	Какие компоненты из перечисленных входят в комплексную систему защиты информации?	1. Средства управления учетными записями. 2. Средства управления событиями. 3. Средства разделения физической сети на несколько логических сетей. 4. Средства инвентаризации активов.
2.	Какие компоненты из перечисленных входят в комплексную систему защиты информации?	1. Средства разделения физической сети на несколько логических сетей. 2. Средства контроля подключения к сетевым устройствам. 3. Средства защищенного доступа. 4. Средства контроля защищенности.
3.	Что из перечисленного относится к способам несанкционированного доступа к защищаемой информации?	1. Инициативное сотрудничество. 2. Опосредованный контакт. 3. Выведывание 4. Подделка.
4.	Что из перечисленного относится к способам несанкционированного доступа к защищаемой информации?	1. Уничтожение. 2. Наблюдение 3. Склонение к сотрудничеству. 4. Неофициальная беседа на публичном мероприятии.
5.	Что из перечисленного относится к физическим средствам защиты информации?	1. Стены. 2. Средства защищенного доступа. 3. Заграждения. 4. Аппаратные межсетевые экраны.
6.	Что из перечисленного относится к физическим средствам защиты информации?	1. Аппаратные межсетевые экраны. 2. Системы обнаружения вторжений. 3. Устройства хранения. 4. Электромеханические замки.
7.	Какие задачи решает система физической защиты информации?	1. Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 2. Предупреждение несанкционированного доступа, нерегламентированных воздействий. 3. Реагирование сотрудников службы безопасности. 4. Обеспечение целостности программно-аппаратной среды.
8.	Какие задачи решает система физической защиты информации?	1. Обеспечение целостности программно-аппаратной среды. 2. Задержка нарушителей, их выявления на объекте. 3. Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 4. Предупреждение несанкционированного доступа, нерегламентированных воздействий.
9.	Какие объекты из перечисленных являются объектами защиты при	1. Устройства хранения данных. 2. Информация.

	обеспечении информационной безопасности?	3. Ресурсные объекты. 4. Физические объекты. 5. Устройства передачи данных.
10.	Какие компоненты входят в комплекс защиты охраняемых объектов?	1. Датчики 2. Телевизионная система 3. Устройства несанкционированного доступа, нерегламентированных воздействий. 4. Устройства обеспечения доступности программно-аппаратной среды.
11.	Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	1. Задержка нарушителей, их выявление на объекте. 2. Разграничение доступа к ресурсам АРМ и серверов информационной системы. 3. Обеспечение функций регистрации и учета событий безопасности. 4. Реагирование сотрудников службы безопасности.
12.	Какие компоненты из перечисленных входят в состав системы защиты от несанкционированного доступа?	1. Встроенные в системное программное обеспечение средства идентификации, аутентификации, авторизации, мониторинга событий и контроля целостности. 2. Средства удаленного администрирования автоматизированных рабочих мест и серверов, входящих в состав информационной системы. 3. Средства контроля подключения к сетевым устройствам, средства изменений конфигураций. 4. Средства резервного копирования и восстановления конфигураций и других параметров настроек применяемых средств защиты.
13.	Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	1. Измерение различных информационных полей и каналов утечки защищаемой информации. 2. Обеспечение функций регистрации и учета событий безопасности. 3. Обеспечение неизменности программно-аппаратной среды применяемых программно-технических средств. 4. Реагирование сотрудников службы безопасности.
14.	Что из перечисленного входит в состав системы защиты от несанкционированного доступа?	1. Встроенные в системное программное обеспечение инструменты, используемые в работе ИТ-администраторов. 2. Средства удаленного администрирования автоматизированных рабочих мест и серверов, входящих в состав информационной системы. 3. Средства контроля подключения к сетевым устройствам, средства изменений конфигураций.
15.	Какие существуют виды угроз информационной безопасности (внешние и внутренние)?	1. Угроза ограничения полномочий пользователей. 2. Несанкционированный доступ. 3. Мошенничество. 4. Кибервойны и кибертерроризм. 5. Верификация.
16.	Какие меры из перечисленных включает в себя система защиты персональных данных?	1. Установление ограничений по доступу персонала. 2. Выбор ответственного лица. 3. Составление и утверждение локальных документов. 4. Задержка нарушителей, их выявление на объекте защиты. 5. Все ответы верны.
17.	Какие методы используются для обеспечения защиты данных, хранящихся и передающихся техническими средствами?	1. Выбор ответственного за безопасность лица. 2. Шифрующая система файлов. 3. Ключи. 4. Безопасные соединения. 5. Использование средств антивирусной защиты.
18.	Какие методы используются для	1. Выбор ответственного за безопасность лица.

	обеспечения защиты данных, хранящихся и передающихся техническими средствами?	2. Аутентификация. 3. Регламентирование доступа к объектам. 4. Использование средств антивирусной защиты.
19.	Какими механизмы из перечисленных можно использовать для защиты корпоративной информации?	1. Использовать удаленное администрирование автоматизированных рабочих мест и серверов, входящих в состав корпоративной системы. 2. Установить четкие правила и регламенты работы с информацией, назначить наказания за их нарушение. 3. Закрыть информацию от несанкционированного доступа с помощью аппаратуры или специального программного обеспечения.
20.	Какие существуют технические каналы утечки информации?	1. Визуально-оптические каналы утечки информации. 2. Электромагнитные каналы утечки информации. 3. Визуально-вещественные каналы утечки информации. 4. Все ответы верны.
21.	Какие механизмы безопасности из перечисленных используются для защиты данных в информационных системах?	1. Персонализация. 2. Авторизация. 3. Верификация. 4. Регламентация. 5. Превентизация.
22.	Как классифицируются технические каналы акустической утечки информации в зависимости от физической природы возникновения информационных сигналов, среды их распространения?	1. Прямые акустические. 2. Обратные акустические. 3. Акустовибрационные. 4. Акустоэлектромагнитные.
23.	Какие существуют технические каналы утечки информации?	1. Визуально-вещественные каналы утечки информации. 2. Акустические каналы утечки информации. 3. Материально-вещественные каналы утечки информации. 6. Все ответы верны.
24.	Как классифицируются технические каналы акустической утечки информации в зависимости от физической природы возникновения информационных сигналов, среды их распространения?	1. Косвенные акустические. 2. Акустооптические. 3. Акустоэлектрические. 4. Акустоэлектромагнитные. 5. Все ответы верны.
25.	При каких режимах обработки информации средствами вычислительной техники возникают побочные электромагнитные излучения?	1. Вывод информации на экран монитора. 2. Ввод данных с электронной почты. 3. Запись информации на накопители. 4. Запись данных, полученных от СУБД.
26.	Что из перечисленного является косвенными каналами утечки информации?	1. Утечка данных из-за несоблюдения режима коммерческой тайны. 2. Пропажа, кража или потеря информационного накопителя, исследование неудаленной корзины. 3. Прослушивание, дистанционные снимки. 4. Перехват электромагнитных устройств. 5. Непосредственное копирование данных.
27.	Что из перечисленного является прямыми каналами утечки информации?	1. Утечка данных из-за несоблюдения режима коммерческой тайны. 2. Перехват электромагнитных устройств. 3. Человеческий фактор. 4. Прослушивание, дистанционные снимки. 5. Непосредственное копирование данных.
28.	При каких режимах обработки информации средствами вычислительной техники возникают	1. Запись данных от СУБД. 2. Чтение информации с накопителей. 3. Ввод данных с электронной почты.

	побочные электромагнитные излучения?	4. Запись данных от сканера на магнитный носитель.
29.	Где могут возникать наводки информативных сигналов?	<ol style="list-style-type: none"> 1. В линиях электропитания ТСОИ. 2. В линиях электропитания и соединительных линиях ВТСС. 3. В посторонних проводниках (неметаллических трубах, пластмассовых конструкциях). 4. В цепях заземления ТСОИ и ВТСС. 5. Все ответы верны.
30.	Каким образом создаются возможные каналы утечки информации?	<ol style="list-style-type: none"> 1. Во время влияния на ТСПИ и ВТСС электрических, магнитных и акустических полей. 2. При возникновении паразитной нагрузки. 3. При прохождении информативных сигналов в цепи электропитания. 4. При взаимном влиянии коммутаций.
31.	Как создаются возможные каналы утечки информации?	<ol style="list-style-type: none"> 1. Низкочастотными электромагнитными полями, которые возникают во время работ ТСПИ и ВТСС. 2. При возникновении паразитной высокочастотной генерации. 3. При взаимном влиянии цепей. 4. Вследствие ошибочных коммутаций и несанкционированных действий. 5. Все ответы верны.
32.	Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	<ol style="list-style-type: none"> 1. Перехват информационных сигналов с линий электропитания ТСПИ. 2. Перехват побочных электромагнитных излучений элементов ТСПИ. 3. Перехват ПЭМИ на частотах работы высокочастотных генераторов в ТСПИ и ВТСС. 4. Перехват ПЭМИ путем установки в ТСПИ электронных устройств перехвата информации. 5. Перехват информационных сигналов с цепей заземления ТСПИ и ВТСС.
33.	Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	<ol style="list-style-type: none"> 1. Перехват информационных сигналов с линий электропитания ТСПИ. 2. Перехват ПЭМИ на частотах работы высокочастотных генераторов в ТСПИ и ВТСС. 3. Перехват ПЭМИ на частотах самовозбуждения усилителей низкой частоты ТСПИ. 5. Перехват информационных сигналов с цепей заземления ТСПИ и ВТСС.
34.	Что из перечисленного относится к электрическим каналам утечки информации (КУИ)?	<ol style="list-style-type: none"> 1. Съём информационных сигналов с линий электропитания ТСПИ. 2. Съём информационных сигналов с цепей заземления ТСПИ и ВТСС. 3. Съём информации путем установки в ТСПИ электронных устройств перехвата информации. 4. Перехват информационных сигналов на частотах самовозбуждения усилителей низкой частоты ТСПИ. 5. Съём информации на частотах работы высокочастотных генераторов в ТСПИ и ВТСС.
35.	Что из перечисленного относится к вспомогательным техническим средствам и системам (ВТСС)?	<ol style="list-style-type: none"> 1. Системы охранной и пожарной сигнализации. 2. Системы оперативно-командной связи. 3. Средства оповещения и сигнализации. 4. Системы видеозаписи и видеовоспроизведения. 5. Системы кондиционирования.
36.	Что из перечисленного относится к ТСПИ и ВТСС?	<ol style="list-style-type: none"> 1. Задающие генераторы. 2. Генераторы тактовой частоты. 3. Генераторы стирания и подмагничивания

		<p>магнитофонов.</p> <p>4. Гетеродины радиоприемных и телевизионных устройств.</p> <p>5. Все ответы верны.</p>
37.	Что из перечисленного относится к основным техническим средствам и системам (ОТСС)?	<p>1. Системы охранной и пожарной сигнализации.</p> <p>2. Системы оперативно-командной связи.</p> <p>3. Средства оповещения и сигнализации.</p> <p>4. Системы видеозаписи и видеовоспроизведения.</p> <p>5. Аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода.</p>
38.	Что из перечисленного является примером прямого канала утечки данных?	<p>1. Пропажа, кража информационного накопителя.</p> <p>2. Прослушивание, дистанционные снимки.</p> <p>3. Перехват электромагнитных устройств.</p> <p>4. Работа инсайдеров.</p>
39.	Какими способами рекомендуется бороться с утечкой персональных данных?	<p>1. Использовать надежные пароли и настроить многофакторную аутентификацию.</p> <p>2. Своевременно обновлять программное обеспечение.</p> <p>3. Регулярно создавать резервные копии данных.</p> <p>4. Обновить адресную книгу электронной почты.</p> <p>5. Все ответы верны.</p>
40.	Какими способами обеспечивается защита информации от утечки по электромагнитным каналам?	<p>1. Фильтрация ПЭМИ на частотах работы высокочастотных генераторов в ТСПИ и ВТСС.</p> <p>2. Фильтрация в цепях заземления и питания.</p> <p>3. Ослабление связей между элементами.</p> <p>4. Экранирование элементов и узлов оборудования.</p>
41.	Что из перечисленного относят к пассивным техническим способам защиты?	<p>1. Установка комплексных систем защиты от несанкционированного доступа на ТСПИ и кабельные линии связи.</p> <p>2. Установка систем гарантированного уничтожения информации.</p> <p>3. Контроль радиоспектра и побочных электромагнитных излучений ТСПИ.</p> <p>4. Звуко- и виброизоляция ВП и механических узлов ТСПИ.</p>
42.	Какие каналы утечки информации выявляются в процессе поисковых мероприятий?	<p>1. Каналы, обрабатываемые ТСПИ.</p> <p>2. Каналы речевой информации.</p> <p>3. Каналы визуально-графической информации.</p> <p>4. Каналы видовой информации.</p> <p>5. Каналы цифровой информации.</p>
43.	Какими способами в ходе специальной проверки осуществляется выявление закладных устройств?	<p>1. Контроль радиоспектра и побочных электромагнитных излучений ТСПИ.</p> <p>2. Выявление с помощью индикаторов электромагнитного поля, интерсепторов, частотомеров, сканеров негласно установленных подслушивающих приборов.</p> <p>3. Специальная проверка с использованием нелинейных локаторов и мобильных рентгеновских установок.</p> <p>4. Все ответы верны.</p>
44.	Что из перечисленного относят к пассивным техническим способам защиты информации?	<p>1. Фильтрация ПЭМИ на частотах работы высокочастотных генераторов в ТСПИ и ВТСС.</p> <p>2. Экранирование ВП, ТСПИ и отходящих от них соединительных линий.</p> <p>3. Заземление ТСПИ и экранов соединительных линий приборов.</p> <p>4. Установка систем гарантированного уничтожения информации.</p>
45.	Что из перечисленного относят к пассивным техническим способам защиты?	<p>1. Встраивание в ВТСС, обладающих "микрофонным" эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров.</p>

		<p>2.Акустическое и вибрационное зашумление строительных конструкций.</p> <p>3.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения).</p> <p>4.Монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров.</p>
46.	Что из перечисленного относят к пассивным техническим способам защиты?	<p>1.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения).</p> <p>2.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор.</p> <p>3.Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ.</p> <p>4.Акустическое и вибрационное зашумление строительных конструкций.</p>
47.	Какими методами из перечисленных осуществляется активное воздействие на каналы утечки информации?	<p>1.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения).</p> <p>2.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров.</p> <p>3.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор.</p> <p>4.Зашумление каналов передачи данных.</p>
48.	Какими методами осуществляется активное воздействие на каналы утечки информации?	<p>1.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров.</p> <p>2.Пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ.</p> <p>3.Акустическое и вибрационное зашумление строительных конструкций.</p> <p>4. Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ.</p>
49.	Какими способами осуществляется активное воздействие на каналы утечки информации?	<p>1.Зашумления силовой сети и цепей заземления.</p> <p>2.Установка систем гарантированного уничтожения информации.</p> <p>3.Шифрование информации, передаваемой по каналам связи.</p> <p>4.Монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров.</p>
50.	Какие методы защиты информации могут быть использованы для предотвращения несанкционированного доступа?	<p>1.Пароли для авторизации во время работы.</p> <p>2.Модули доверенной загрузки.</p> <p>3.Криптографические средства шифрования информации для ее передачи и хранения.</p> <p>4.Средства предотвращения сетевых атак (межсетевой экран, антивирус, прокси-сервер).</p> <p>5.Все ответы верны.</p>
51.	Какие компоненты включает в себя комплекс радиолокационной системы?	<p>1. Модули доверенной загрузки.</p> <p>2.Система периметрального наблюдения, состоящая из камер и тепловизоров.</p> <p>3.Инфракрасные и вибрационные извещатели.</p> <p>4.Радиолокатор.</p> <p>5.Рабочее операторское место.</p>
52.	Какие виды средств защиты информации должны содержаться в информационных системах общего	<p>1.СЗИ от неправомерных действий (в том числе средства криптографической защиты информации).</p> <p>2.Средства обнаружения вредоносных программ (в том</p>

	пользования?	<p>числе антивирусные средства).</p> <p>3. Средства контроля доступа к информации (в том числе средства обнаружения компьютерных атак).</p> <p>4. Средства фильтрации и блокирования сетевого трафика (в том числе средства межсетевого экранирования).</p> <p>5. Все, перечисленное в остальных пунктах.</p>
53.	Что из перечисленного является основными закономерностями распространения радиоволн, которые позволяют обнаруживать объекты и измерять координаты и параметры их движения?	<p>1. Постоянство скорости и прямолинейность распространения радиоволн в однородной среде.</p> <p>2. Способность радиоволн отражаться от различных областей пространства, электрические или магнитные параметры которых отличаются от аналогичных параметров среды распространения.</p> <p>3. Изменение скорости принимаемого сигнала.</p> <p>4. Изменение частоты принимаемого сигнала по отношению к частоте излученного сигнала при относительном движении источника излучения и приемника радиолокационного сигнала.</p>
54.	Что из перечисленного относится к организационно-режимным мероприятиям по защите информации на объекте?	<p>1. Определение границ контролируемой зоны (КЗ) вокруг объекта и обеспечение режимного ограничения доступа на объекты размещения ТСПИ и в выделенные помещения (ВП).</p> <p>2. Контроль радиоспектра и побочных электромагнитных излучений ТСПИ.</p> <p>3. Введение частотных, энергетических, временных и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации (ТСПИ).</p> <p>4. Специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием мобильных рентгеновских установок.</p> <p>5. Отключение на период проведения закрытых совещаний вспомогательных технических средств и систем (ВТСС), обладающих качествами электроакустических преобразователей от соединительных линий.</p>
55.	Что из перечисленного относится к организационно-режимным мероприятиям по защите информации на объекте?	<p>1. Использование только сертифицированных ТСПИ и ВТСС.</p> <p>2. Специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок.</p> <p>3. Привлечение к строительству выделенных (защищенных) помещений, монтажу аппаратуры ТСПИ, а также к работам по ЗИ организаций, лицензированных соответствующими службами на деятельность в данной области.</p> <p>4. Контроль радиоспектра и побочных электромагнитных излучений ТСПИ.</p> <p>5. Категорирование и аттестование объектов информатизации и выделенных помещений на соответствие требованиям обеспечения ЗИ при проведении работ со сведениями различной степени секретности.</p>
56.	На какие виды можно разделить методы и способы защиты информации от утечки по ТКУИ в зависимости от целей, порядка проведения и применяемого оборудования?	<p>1. Организационно-режимные.</p> <p>2. Правовые.</p> <p>3. Поисковые (выявление возможных ТКУИ).</p> <p>4. Программные.</p> <p>3. Технические.</p>

57.	Какие каналы утечки информации выявляются в процессе поисковых мероприятий?	<ol style="list-style-type: none"> 1. Каналы утечки, обрабатываемые ТСПИ. 2. Каналы утечки речевой информации. 3. Каналы утечки шумовой информации. 4. Каналы утечки при передаче информации по каналам связи. 5. Каналы утечки видовой информации.
58.	Какие мероприятия из перечисленных выполняются в ходе специальной проверки?	<ol style="list-style-type: none"> 1. Контроль радиоспектра и побочных электромагнитных излучений ТСПИ. 2. Категорирование и аттестование объектов информатизации и выделенных помещений на соответствие требованиям обеспечения ЗИ при проведении работ со сведениями различной степени секретности. 3. Выявление с помощью индикаторов электромагнитного поля, интерсепторов, частотомеров, сканеров или программно-аппаратных комплексов негласно установленных подслушивающих приборов. 4. Введение частотных, энергетических, временных и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации. 5. Специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок.
59.	Какие из перечисленных защитных приемов и средств относятся к пассивным техническим способам защиты?	<ol style="list-style-type: none"> 1. Акустическое и вибрационное зашумление строительных конструкций. 2. Установка комплексных систем защиты от несанкционированного доступа (НСД) на ТСПИ и кабельные линии связи. 3. Шифрование информации, передаваемой по каналам связи. 4. Экранирование ВП, ТСПИ и отходящих от них соединительных линий. 5. Зашумления силовой сети и цепей заземления.
60.	Какие из перечисленных защитных приемов и средств относятся к пассивным техническим способам защиты?	<ol style="list-style-type: none"> 1. Заземление ТСПИ и экранов соединительных линий приборов. 2. Пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ. 3. Звуко- и виброизоляция ВП и механических узлов ТСПИ. 4. Зашумление каналов передачи данных; 5. Встраивание в ВТСС, обладающие "микрофонным" эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров.
61.	Какие из перечисленных защитных приемов и средств относятся к пассивным техническим способам защиты?	<ol style="list-style-type: none"> 1. Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор. 2. Разрушающее воздействие на средства съема сигналами большой мощности (тепловое разрушение электронных устройств). 3. Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ. 4. Установка систем гарантированного уничтожения информации. 5. Монтаж в цепях электропитания ТСПИ, а также в электросетях выделенных помещений, помехоподавляющих фильтров.
62.	Какие из перечисленных защитных приемов и средств относят к	<ol style="list-style-type: none"> 1. Пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ.

	активному воздействию на каналы утечки информации?	2.Акустическое и вибрационное зашумление строительных конструкций. 3.Экранирование ВП, ТСПИ и отходящих от них соединительных линий. 4.Заземление ТСПИ и экранов соединительных линий приборов. 5.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения).
63.	Какие из перечисленных защитных приемов и средств относят к активному воздействию на каналы утечки информации?	1.Зашумление каналов передачи данных; 2.Звуко- и виброизоляция ВП и механических узлов ТСПИ. 3.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 4.Зашумления силовой сети и цепей заземления. 5.Разрушающее воздействие на средства съема сигналами большой мощности (тепловое разрушение электронных устройств).
64.	Какие из перечисленных защитных приемов и средств относят к активному воздействию на каналы утечки информации?	1.Установка комплексных систем защиты от несанкционированного доступа на ТСПИ и кабельные линии связи. 2.Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ. 3.Установка систем гарантированного уничтожения информации. 4.Шифрование информации, передаваемой по каналам связи.
65.	Какие средства криптографической защиты обеспечивают создание ЭЦП с использованием закрытого ключа и подтверждение с использованием открытого ключа подлинности ЭЦП?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
66.	Какие средства криптографической защиты информации обеспечивают возможность разграничения доступа к ней?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
67.	Какие СЗИ обеспечивают защиту от навязывания ложной информации и возможность обнаружения изменений информации?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты 5.Средства шифрования.
68.	В каких средствах шифрования часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств для выполнения таких операций?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
69.	Как называют электронные документы, содержащие ключевую информацию, необходимую для выполнения криптографических преобразований с помощью средств шифрования?	1.Шифрованные документы. 2.Кодовые документы. 3.Ключевые документы. 4.Подлинные документы.
70.	Сколько классов криптографических средств защиты информации определено ФСБ России?	1.Шесть классов. 2.Пять классов. 3.Семь классов.

		4. Четыре класса.
71.	К какому классу криптографических средств защиты информации относятся средства, защищающие от атак, проводимых из-за пределов контролируемой зоны?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
72.	К какому классу криптографических средств защиты информации относятся средства, защищающие от атак, блокируемых средствами класса КС1, а также от атак, проводимых в пределах контролируемой зоны?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
73.	К какому классу криптографических средств защиты информации относятся средства, защищающие от атак при наличии физического доступа к СВТ с установленными криптографическими СЗИ?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
74.	К какому классу криптографических СЗИ относятся средства, защищающие от атак, при реализации которых участвовали специалисты в области разработки и анализа криптографических СЗИ?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
75.	К какому классу криптографических СЗИ относятся средства, защищающие от атак, при реализации которых привлекались специалисты в области использования НДВ системного программного обеспечения?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
76.	Какие бывают наземные РЛС?	1. Статические. 2. Надгоризонтные. 3. Загоризонтные. 4. Подповерхностные. 5. Надповерхностные
77.	Какой метод использует для своей работы индикатор поля?	1. Метод широкополосного прямого детектирования. 2. Метод узкополосного прямого детектирования. 3. Метод широкополосного обратного детектирования. 4. Метод узкополосного обратного детектирования.
78.	Что из перечисленного относится к средствам защиты акустической речевой информации?	1. Системы голосовой защиты. 2. Средства защиты слаботочных линий. 3. Средства защиты от несанкционированного применения сотовых телефонов, диктофонов и радиопередатчиков. 4. Электромагнитные подавители сотовых телефонов.
79.	Что из перечисленного является основными организационными мероприятиями по защите речевой (акустической) информации, составляющей коммерческую тайну?	1. Использование в защищаемых помещениях электромагнитных подавителей сотовых телефонов. 2. Выбор помещений для ведения конфиденциальных переговоров (защищаемых помещений). 3. Категорирование защищаемых помещений. 4. Использование в защищаемых помещениях сертифицированных ВТСС. 5. Все ответы верны.
80.	Что из перечисленного является основными организационными мероприятиями по защите речевой (акустической) информации, составляющей коммерческую тайну?	1. Установление контролируемой зоны вокруг защищаемых помещений. 2. Демонтаж в защищаемых помещениях незадействованных ВТСС, их соединительных линий и посторонних проводников. 3. Встраивание в ВТСС, обладающие "микрофонным"

		<p>эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров.</p> <p>4. Организация режима и контроля доступа в защищаемые помещения.</p> <p>5. Все ответы верны.</p>
81.	В чем разница между информационной безопасностью и кибербезопасностью?	<p>1. Информационная безопасность направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) и места хранения.</p> <p>2. Кибербезопасность направлена на защиту цифровых данных от компрометации или атак.</p> <p>3. Кибербезопасность направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) от компрометации или атак.</p> <p>4. Информационная безопасность направлена на защиту цифровых данных от компрометации или атак.</p>
82.	Что представляют собой угрозы типа АРТ (advanced persistent threat)?	<p>1. Программы-вымогатели, которые получают доступ к файлам или системам и блокируют их для получения выкупа.</p> <p>2. Многоступенчатые атаки, в ходе которых хакеры проникают в сеть незамеченными и остаются в ней в течение длительного времени, чтобы получить доступ к конфиденциальным данным или нарушить работу критически важных служб.</p> <p>3. Практика манипулирования людьми с целью заставить их раскрыть чувствительную конфиденциальную информацию для получения денежной выгоды или доступа к данным.</p>
83.	Какие бывают типы угроз кибербезопасности?	<p>1. Атаки на основе социальной инженерии.</p> <p>2. Атаки при помощи вредоносного ПО.</p> <p>3. Атаки на Интернет вещей (IoT).</p> <p>4. Атаки типа «отказ в обслуживании» (DoS).</p> <p>5. Все ответы верны.</p>
84.	Что из перечисленного является организационными методами защиты информации?	<p>1. Разработка и внедрение регламентов по обработке сведений внутри организации.</p> <p>2. Регулярное создание бэкапов наиболее важных и ценных информационных массивов.</p> <p>3. Проведение инструктажа персонала по основам кибербезопасности и правилам работы с информацией.</p> <p>4. Выполнение резервирования, дублирования вспомогательных компонентов информационной системы, которые связаны с хранением информации.</p>
85.	Что из перечисленного является организационными методами защиты информации?	<p>1. Создание защиты информационных ресурсов от ЧС.</p> <p>2. Использование ПО, отвечающего за управление доступом к информации, ведение мониторинга, предотвращение утечек информации.</p> <p>3. Установление зон ответственности. Руководитель назначает конкретных персон, ответственных за исполнение правил и норм информационной безопасности.</p> <p>4. Разработка плана по восстановлению информации при чрезвычайных ситуациях.</p>

Вопросы задания открытого типа для дифференцированного зачета
по МДК.03.02 Применение комплексной системы защиты информации в
инфокоммуникационных системах и сетях связи

1. Что является объектом защиты информации?
2. Как называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, и помещений, в которых они установлены?
3. Что понимается под защищаемыми помещениями (ЗП)?
4. Что такое автоматизированная система (АС)?
5. Что такое контролируемая зона (КЗ)?
6. Что такое специальные исследования (СИ)?
7. Что такое специальная проверка (СП)?
8. Как называют комплекс мер в области защиты информации в части проведения работ по выявлению электронных устройств негласного получения сведений в помещениях, где циркулирует информация ограниченного пользования?
9. Что такое аттестация объекта защиты?
10. Как называют неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации?
11. Как называются технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации?
12. Что относится к основным техническим средствам и системам (ОТСС)?
13. Как называются технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в защищаемых помещениях?
14. Как называют электрические сигналы, акустические, электромагнитные поля, по параметрам которых может быть раскрыта защищаемая информация, передаваемая, хранимая или обрабатываемая в ОТСС, или обсуждаемая в защищаемых помещениях?
15. Что понимают под техническим каналом утечки информации?
16. Что такое тестовый сигнал?
17. Как называют установление нормативными документами численных значений показателей защищенности информации?
18. Что является целью аттестации объекта информатизации?
19. Какой криптографический протокол обеспечивает защищённую передачу данных между узлами в сети Интернет?
20. Каковы основные функции протокола TLS?
21. Какие программные или программно-аппаратные средства обеспечивают охрану данных от возможной утечки внутри компании?
22. Какие программные или программно-аппаратные средства, позволяют осуществлять запуск операционной системы исключительно с доверенных носителей информации (например, жестких дисков)?
23. Какие СЗИ предназначены для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении?
24. Какие средства безопасности предназначены для анализа защищенности информации в корпоративных сетях и могут выполнять проверку установленных patch'ей системы безопасности ОС?
25. Как называют сетевые шлюзы безопасности, состоящие из шлюзового антивируса; механизма блокировки сайтов по их содержимому, категории или конкретному адресу; VPN; IPS/IDS и др.?
26. Какая система безопасности защищает от воздействия внешних злоумышленников на компьютерную сеть, а именно от DoS-атак, сетевого сканирования, работы ботнетов и спам-сетей?

27. Какую технологию используют для объединения компьютерных сетей организации, географически удаленных друг от друга?

28. К какому виду способов и средств обеспечения информационной безопасности относят средства авторизации; мандатное и избирательное управление доступом; управление доступом на основе ролей; журналирование?

29. К какому виду программно-технических средств обеспечения ИБ относят системы обнаружения и предотвращения вторжений (IDS/IPS) и системы предотвращения утечек конфиденциальной информации (DLP-системы)?

30. К какому виду программно-технических средств обеспечения информационной безопасности относят шифрование и цифровую подпись?

31. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят пароль; ключ доступа; сертификат; биометрию?

32. К какому виду программно-технических способов и средств обеспечения информационной безопасности относят источники бесперебойного питания; резервирование нагрузки; генераторы напряжения.

33. Какие СЗИ собирают исходящий, входящий и внутрикорпоративный трафик организации, действия пользователей с помощью модулей-перехватчиков, и перехваченную информацию обрабатывают с помощью политик фильтрации, контентного и контекстного анализа?

34. Как называется технология идентификации, основанная на использовании радиочастотного электромагнитного излучения?

35. Как называют технологию беспроводной высокочастотной связи малого радиуса действия, позволяющую осуществлять бесконтактный обмен данными между устройствами, расположенными на небольших расстояниях?

36. Как называют двумерный штрихкод, в котором кодируется информация, состоящая из символов (включая кириллицу, цифры и спецсимволы)?

37. Какие существуют виды инженерно-технических средств безопасности?

38. Какие методы биометрической идентификации основываются на уникальной физиологической характеристике человека, данной ему от рождения и неотъемлемой от него?

39. Какой метод биометрической идентификации построен на геометрии кисти руки: строится трехмерный образ кисти руки, по которому формируется свертка и распознается человек?

40. При каком методе биометрической идентификации с помощью инфракрасной камеры считывается рисунок вен на лицевой стороне ладони или кисти руки, и по схеме расположения вен формируется цифровая свертка.

41. В основе какого метода биометрической идентификации лежит уникальность распределения на лице артерий, снабжающих кровью кожу, и используются специальные камеры инфракрасного диапазона?

42. Какие методы биометрической идентификации основываются на поведенческой характеристике человека, построены на особенностях, характерных для подсознательных движений?

43. При каком методе биометрической идентификации основной характеристикой, по которой строится свертка для идентификации, является динамика набора кодового слова?

44. Как называют пластиковые карты, содержащие микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти?

45. Какое USB-устройство, предназначено для безопасной аутентификации пользователей, защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов?

46. Какое средство аутентификации и защищенного хранения данных, аппаратно поддерживает работу с цифровыми сертификатами и электронной цифровой подписью, исполняется в виде USB-ключей, смарт-карт, генераторов одноразовых паролей?

47. Какие системы автоматизируют процесс управления учетными записями, например, управляют процессом по созданию, изменению и блокированию учетных записей?

48. Какая модель доступа базируется на явно заданных для каждого субъекта (пользователя) правах доступа к объектам / сегментам информации?
49. В какой модели доступа субъект имеет право на чтение только тех объектов, уровень конфиденциальности которых не выше его уровня?
50. Какой криптографический сетевой протокол служит для безопасного управления сетевыми службами в незащищенной сети?
51. Что является причиной возникновения акустического и виброакустического каналов утечки информации?
52. Что такое комплексная система защиты информации?
53. Что такое физическая защита информации?
54. Что такое техническая защита информации?
55. Какие компоненты входят в комплекс защиты охраняемых объектов?
56. Как определить класс защищенности информационной системы?
57. Какие существуют способы организации утечки информации?
58. Что такое технические каналы утечки информации (ТКУИ)?
59. Как называют паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники?
60. Каким образом классифицируются каналы утечки информации?
61. Что входит в структуру канала утечки информации?
62. Каковы основные причины утечки данных?
63. Что такое защита информации от утечки?
64. Какие проблемы решает DLP-система?
65. Что называют каналом утечки речевой информации?
66. Как классифицируются акустические каналы утечки информации?
67. Какие существуют средства защиты акустической речевой информации от утечки по техническим каналам?
68. Что такое закладные устройства?
69. Какие технические средства применяют для выявления радиозакладных устройств (РЗУ)?
70. Какие каналы утечки информации различают в зависимости от среды распространения?
71. Какова дальность передачи информации при перехвате с использованием устройства типа «телефонное ухо» по радиоканалу при использовании сотового телефона в качестве закладного устройства?
72. Что является носителем информации в электромагнитных каналах утечки информации?
73. Что называют побочным электромагнитным излучением (ПЭМИ)?
74. Как называются сигналы, представляющие собой высокочастотную несущую, модулированную информацией, обрабатываемой на СВТ (например, изображением, выводимым на экран монитора)?
75. Как называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ?
76. Какими способами можно перехватить речевую информацию по прямому акустическому каналу утечки?
77. Какими способами можно перехватить речевую информацию по виброакустическому каналу утечки?
78. Какими способами можно перехватить речевую информацию по прямому акустоэлектромагнитному каналу утечки?
79. Какими способами можно перехватить речевую информацию по акустоэлектрическому каналу утечки?
80. Какими способами можно перехватить речевую информацию по акустооптическому (лазерному) каналу утечки?

Составил:

Преподаватель Е.М. Грубник