СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
_____ А.Н. Калугин
«31» 08 2020 г.

РАССМОТРЕНО
на заседании методической
комиссии дисциплин
средств подвижной связи
Председатель _____ Е.Н. Кожекина
Протокол №1 31.08 2020 г.

УТВЕРЖДАЮ
Заместитель директора по
учебной работе
_____ И. В. Иванешко
«31» 08 2020 г.

Контрольно-оценочные средства для промежуточной аттестации
МДК.02.01 Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи
ПМ.02 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи
по специальности 11.02.11 Сети связи и системы коммутации

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК 02.01.

В результате освоения МДК 02.01 студент должен освоить следующие профессиональные компетенции:

Код	Наименование профессиональных компетенций
ПК 2.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
ПК 2.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
ПК 2.3	Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.

А также общие компетенции:

Код	Наименование общих компетенций
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Иметь практический опыт:

ПО 1 – выявления каналов утечки информации;

ПО 2 – определения необходимых средств защиты;

ПО 4 - разработки политики безопасности для объекта защиты;

ПО 6 - выявления возможных атак на автоматизированные системы;

ПО 9 - проверки защищенности автоматизированных систем и информационно-коммуникационных сетей;

ПО 13 – использования систем и решений для борьбы с мошенничеством в сети;

ПО16 - установки, настройки специализированного программного обеспечения (свободно распространяемого программного обеспечения) по защите информации в информационно-коммуникационных сетях.

Уметь:

У1 – классифицировать угрозы информационной безопасности;

У2 – проводить выбор средств защиты в соответствии с выявленными угрозами;

У3 - определять возможные виды атак;

У5 - разрабатывать политику безопасности объекта;

У6 - использовать программные продукты, выявляющие недостатки систем защиты;

У9 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

У13 – использовать общую схему подключения системы фродконтроля;

У15 – использовать программно-аппаратные комплексы с применением технологий IPS (IDS);

У16 – использовать стандарты и рекомендации в области защиты виртуальных сред.

Знать:

З1 – каналы утечки информации;

З3 - принципы построения информационно-коммуникационных сетей;

З4 - возможные способы несанкционированного доступа;

З5 - законодательные и нормативные правовые акты в области информационной безопасности;

З6 - правила проведения возможных проверок;

З7 - этапы определения конфиденциальности документов объекта защиты;

З10 - конфигурации защищаемых сетей;

З11 - алгоритмы работы тестовых программ;

З14 – виды мошенничества в телекоммуникациях;

З15 – принципы детектирования предфродового состояния;

З17 - угрозы информационной безопасности, актуальные для виртуальных сред.

Дифференцированный зачет по МДК 02.01 проводится в форме тестирования. Тест содержит 20 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока (первый блок 150 вопросов, второй блок 150 вопросов) заданий по 10 вопросов.

Время тестирования – 90 минут (по 3 минуты на каждый вопрос тестовых позиций и по 4 минуты на краткие ответы теоретических вопросов). Время на подготовку и проверку тестирования – 20 минут

Критерии оценивания:

- оценка «отлично» выставляется обучающемуся, если процент результативности (в % выполнения) составляет 90-100%;

- оценка «хорошо» «4» - ставится в том случае, если верные ответы составляют 71 -89% от общего количества;

- оценке «удовлетворительно» соответствует работа, содержащая 51-70% правильных ответов;

- оценке «неудовлетворительно» соответствует работа, содержащая менее 50% правильных ответов.

Блок заданий закрытого типа Формируемые ПК 2.1		
1.	Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …	1.С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды. 2.С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации. 3.Способна противостоять только информационным угрозам, как внешним так и внутренним. 4.Способна противостоять только внешним информационным угрозам.
2.	Информационная безопасность – это…	1.Состояние защищённости информационной среды. 2.Сохранность информационных ресурсов. 3.Защита конфиденциальности, целостности и доступности информации. 4.Все ответы не верны.
3.	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.
4.	В качестве стандартной модели безопасности часто приводят модель из трёх категорий, каких?	1.Конфиденциальность. 2.Целостность. 3.Доступность. 4.Надежность.
5.	Какие существуют основные уровни обеспечения защиты информации?	1.Законодательный. 2.Организационно-административный. 3.Программно-технический (аппаратный). 4.Физический. 5.Вероятностный. 6.Распределительный.
6.	Методические документы государственных органов России?	1.Руководящие документы ФСТЭК. 2.Приказы ФСБ. 3.Конституция РФ; 4.Указы президента.
7.	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.
8.	Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности?	1.Уголовная 2.Административно-правовая. 3.Гражданско-правовая. 4.Дисциплинарная. 5.Материальная. 6.Условная. 7.Договорная.
9.	Какие документы относятся к актам федерального законодательства?	1.Международные стандарты. 2.Международные договоры РФ. 3.Приказы ФСБ. 4.Указы президента РФ.
10.	Какие основные свойства информации	1.Доступность

	и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?	2.Целостность 3.Конфиденциальность 4.Управляемость 5.Надежность
11.	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)
12.	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.
13.	Основные угрозы доступности информации:	1.Непреднамеренные ошибки пользователей. 2.Злонамеренное изменение данных 3.Хакерская атака. 4.Отказ программного и аппаратного обеспечения. 5.Разрушение или повреждение помещений. 6.Перехват данных.
14.	Что такое конфиденциальность информации?	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.
15.	Что относится к угрозам информационной безопасности?	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.
16.	Какие угрозы безопасности информации являются преднамеренными?	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.
17.	Какие угрозы безопасности информации являются непреднамеренными?	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.
18.	Что относится к правовым мерам защиты информации?	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.
19.	Что такое государственная тайна?	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.
20.	Какие правовые документы решают вопросы информационной безопасности?	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 ".
21.	Что такое коммерческая тайна?	1.Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее

		неизвестности третьим лицам. 2.Информация, к которой нет доступа на законном основании. 3.Информации, обладатель которой принимает меры к охране ее конфиденциальности. 4.Информация, содержащая в учредительных документах. 5.Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов.
22.	По доступности информация классифицируется на …	1.Открытую информацию и государственную тайну. 2.Конфиденциальную информацию и информацию свободного доступа. 3.Информацию с ограниченным доступом и общедоступную информацию. 4.Виды информации, указанные в остальных пунктах.
23.	Запрещено относить к информации ограниченного доступа	1.Информацию о чрезвычайных ситуациях. 2.Информацию о деятельности органов государственной власти. 3.Документы открытых архивов и библиотек. 4.Все, перечисленное в остальных пунктах.
24.	Вопросы информационного обмена регулируются (...) правом?	1.Гражданским. 2.Информационным. 3.Конституционным. 4.Уголовным.
25.	Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется?	1.Достоверной. 2.Конфиденциальной. 3.Документированной. 4.Коммерческой тайной.
26.	Из перечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает	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.
27.	К коммерческой тайне могут быть отнесены?	1.Сведения, не являющиеся государственными секретами. 2.Сведения, связанные с производством и технологической информацией. 3.Сведения, связанные с управлением и финансами. 4.Сведения, перечисленные в остальных пунктах.
28.	Гриф "ДСП" используется …	1.Для секретных документов. 2.Для документов, содержащих коммерческую тайну. 3.Как промежуточный для несекретных документов. 4.В учебных целях.
29.	Срок засекречивания сведений, составляющих государственную тайну?	1.Составляет 10 лет. 2.Составляет 50 лет. 3.Ограничен 30 годами. 4.Ограничен 20 годами.
30.	Что понимается под средством физического управления доступом?	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

		подержанию физической формы сотрудников 4.Программные меры защиты, предназначенные для создания препятствий потенциальным нарушителям. 5.Информационное обеспечение секретных задач.
31.	Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется?	1.Профилем защиты. 2.Профилем безопасности. 3.Стандартом безопасности. 4.Системой защиты.
32.	Недостатком модели политики безопасности на основе анализа угроз системе является?	1.Изначальное допущение вскрываемости системы. 2.Необходимость дополнительного обучения персонала. 3.Сложный механизм реализации. 4.Статичность.
33.	Основным положением модели системы безопасности с полным перекрытием является наличие на каждом пути проникновения в систему …	1.Хотя бы одного средства безопасности. 2.Аудита. 3.Пароля. 4.Всех средств безопасности.
34.	Недостатком модели конечных состояний политики безопасности является?	1.Сложность реализации. 2.Изменение линий связи. 3.Статичность. 4.Низкая степень надежности.
35.	При качественном подходе риск измеряется в терминах …	1.Заданных с помощью шкалы или ранжирования. 2.Денежных потерь. 3.Объема информации. 4.Оценок экспертов.
36.	Что является наилучшим описанием количественного анализа рисков?	1.Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности. 2.Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков. 3.Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков. 4.Метод, основанный на суждениях и интуиции.
37.	Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?	1.Чтобы убедиться, что проводится справедливая оценка. 2.Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ. 3.Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа. 4.Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.
38.	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?	1.Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования. 2.Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации 3.Улучшить контроль за безопасностью этой информации. 4.Снизить уровень классификации этой информации.
39.	Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?	1.Только военные имеют настоящую безопасность. 2.Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности. 3.Военным требуется больший уровень безопасности,

		т.к. их риски существенно выше. 4.Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности.
40.	Задачей анализа модели политики безопасности на основе анализа угроз системе является …	1.Минимизация вероятности преодоления системы защиты. 2.Максимизация затрат для взлома. 3.Максимизация ресурса для взлома. 4.Максимизация времени взлома.
41.	Выделение пользователям и администраторам только тех прав доступа, которые им необходимы это?	1.Принцип минимизации привилегий. 2.Принцип простоты и управляемости ИС. 3.Принцип многоуровневой защиты. 4.Принцип максимизации привилегий.
42.	Достоинством дискретных моделей политики безопасности является …	1.Простой механизм реализации. 2.Числовая вероятностная оценка надежности. 3.Высокая степень надежности. 4.Динамичность.
43.	Достоинством модели политики безопасности на основе анализа угроз системе является …	1.Числовая вероятностная оценка надежности. 2.Высокая степень надежности. 3.Динамичность. 4.Простой механизм реализации.
44.	Процесс анализа рисков при разработке СЗ ИС включает:	1.Анализ потенциального злоумышленника. 2.Оценка возможных затрат. 3.Оценка возможных потерь. 4.Анализ потенциальных угроз.
45.	Подсистема управления доступом системы защиты информации должна обеспечивать:	1.Оповещение о попытках нарушения защиты. 2.Идентификация. 3.Аутентификация. 4.Учет носителей информации. 5.Управление потоками информации.
46.	Основные угрозы конфиденциальности информации:	1.Маскарад. 2.Карнавал. 3.Переадресовка. 4.Перехват данных. 5.Блокирование. 6.Злоупотребления полномочиями.
47.	Политика безопасности строится на основе:	1.Общих представлений об ИС организации. 2.Изучения политик родственных организаций. 3.Анализа рисков.
48.	В число целей программы безопасности верхнего уровня входит:	1.Управление рисками. 2.Определение ответственных за информационные сервисы. 3.Определение мер наказания за нарушения политики безопасности.
49.	В рамках программы безопасности нижнего уровня осуществляются:	1.Стратегическое планирование. 2.Повседневное администрирование. 3.Отслеживание слабых мест защиты.
50.	Что из перечисленного НЕ является задачей руководства в процессе внедрения и сопровождения безопасности?	1.Поддержка. 2.Выполнение анализа рисков. 3.Определение цели и границ. 4.Делегирование полномочий.
Блок заданий закрытого типа Формируемые ПК 2.2		
1.	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?	1.Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования. 2.Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации. 3.Улучшить контроль за безопасностью этой

		информации. 4.Снизить уровень классификации этой информации.
2.	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	1.Сотрудники. 2.Хакеры. 3.Атакующие. 4.Контрагенты (лица, работающие по договору).
3.	Что подразумевает принцип «разделение обязанностей»?	1.Для выполнения критических или необратимых операций требуется участие нескольких независимых пользователей. 2.Данный принцип требует создания механизма подотчётности пользователей, позволяющего отследить моменты нарушения целостности информации. 3.Порядок передачи привилегий должен полностью соответствовать организационной структуре предприятия.
4.	Что такое процедура?	1.Правила использования программного и аппаратного обеспечения в компании. 2.Пошаговая инструкция по выполнению задачи. 3.Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах. 4.Обязательные действия.
5.	Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?	1.Поддержка высшего руководства. 2.Эффективные защитные меры и методы их внедрение. 3.Актуальные и адекватные политики и процедуры безопасности. 4.Проведение тренингов по безопасности для всех сотрудников.
6.	Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?	1.Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски. 2.Когда риски не могут быть приняты во внимание по политическим соображениям. 3.Когда необходимые защитные меры слишком сложны. 4.Когда стоимость контрмер превышает ценность актива и потенциальные потери.
7.	Какая из приведенных техник является самой важной при выборе конкретных защитных мер?	1.Анализ рисков. 2.Анализ затрат / выгоды. 3.Результаты ALE. 4.Выявление уязвимостей и угроз, являющихся причиной риска.
8.	Что является определением воздействия (exposure) на безопасность?	1.Нечто, приводящее к ущербу от угрозы. 2.Любая потенциальная опасность для информации или систем. 3.Любой недостаток или отсутствие информационной безопасности. 4.Потенциальные потери от угрозы.
9.	Эффективная программа безопасности требует сбалансированного применения:	1.Технических и нетехнических методов. 2.Контрмер и защитных механизмов. 3.Физической безопасности и технических средств защиты. 4.Процедур безопасности и шифрования.
10.	Что из перечисленного не является целью проведения анализа рисков?	1.Делегирование полномочий. 2.Количественная оценка воздействия потенциальных угроз. 3.Выявление рисков. 4.Определение баланса между воздействием риска и стоимостью необходимых контрмер.
11.	Что такое CobiT и как он относится к разработке систем информационной безопасности и программ	1.Список стандартов, процедур и политик для разработки программы безопасности. 2.Текущая версия ISO 17799.

	безопасности?	3.Структура, которая была разработана для снижения внутреннего мошенничества в компаниях. 4.Открытый стандарт, определяющий цели контроля.
12.	Защита информации от утечки - это деятельность по предотвращению:	1.Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. 2.Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. 3.Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений. 4.Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа. 5.Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
13.	Что такое анализ защищенности ИТ-инфраструктуры?	1.Анализ защищенности – это неконтролируемое техническое воздействие, направленное на выявление минимального количества уязвимостей в исследуемой ИТ-инфраструктуре. 2.Анализ защищенности – это контролируемое техническое воздействие, направленное на выявление максимального количества уязвимостей и недостатков в исследуемой ИТ-инфраструктуре или информационной системе. 3.Анализ защищенности – это организационное воздействие, направленное на выявление потерь от угрозы информационной безопасности в исследуемой ИТ-инфраструктуре или информационной системе.
14.	Какие задачи решаются при проведении анализа защищенности?	1.Выполнение требований регуляторов. 2.Получение представления о текущем уровне защищенности системы. 3.Оценка защищенности ИТ-инфраструктуры и эффективности используемых механизмов защиты. 4.Получение подробной картины уязвимостей и недостатков исследуемой системы. 5.Все, перечисленное в остальных пунктах.
15.	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.
16.	Мониторинг и аудит сети – это?	1.Функции, не обязательные для сетевого администратора. 2.Обязательные составные части работы сетевого администратора. 3.Функции, реализуемые только операционными системами. 4.Дополнительные функции сетевого администратора.
17.	Угроза (…) возникает всякий раз,	1.Целостности.

	когда в результате преднамеренных действий умышленно блокируется доступ к некоторому ресурсу вычислительной системы. Вставьте пропущенное слово.	2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
18.	Угроза (…) заключается в том, что информация становится известна неавторизованному пользователю. Она возникает всякий раз, когда получен несанкционированный доступ к секретной информации, хранящейся в вычислительной системе, или передаваемой от одной системы к другой. Вставьте пропущенное слово.	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
19.	Иногда в связи с угрозой (…) информации используется термин «утечка информации». Вставьте пропущенное слово.	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
20.	Угроза (…) включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Вставьте пропущенное слово.	1.Целостности. 2.Конфиденциальности. 3.Доступности. 4.Управляемости. 5.Итеративности. 6.Дезинформации. 7.Шпионажа.
21.	Для определения требуемого класса защищенности в Российской Федерации существует конкретный подход. Данный подход реализован в руководящем документе Государственной технической комиссией при Президенте РФ …	1.«Классификация автоматизированных систем и требований по защите информации» Часть 1. 2.«Классификация автоматизированных систем и требований по защите информации» Часть 2. 3.Федеральный закон от 26 июля 2017 г. №187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации».
22.	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.
23.	В Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации», часть 1 классы систем согласно специфическим особенностям обработки информации разделены на (…) групп(ы)?	1. 4 группы. 2. 7 групп. 3. 3 группы. 4. 2 группы. 5. 5 групп.
24.	Системы АСОД, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности, относятся к (…) группе.	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
25.	Системы АСОД, в которых работает несколько пользователей, которые	1.Третья группа. 2.Вторая группа.

	имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности, относятся к (…) группе.	3.Первая группа. 4.Четвертая группа.
26.	Многопользовательские системы АСОД, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации относятся к (…) группе.	1.Третья группа. 2.Вторая группа. 3.Первая группа. 4.Четвертая группа.
27.	В зависимости от реализованных моделей защиты и надежности их проверки классы защищенности СВТ подразделяются на (…) группы	1.Две группы. 2.Три группы. 3.Четыре группы. 4. Шесть групп.
28.	Какая группа классов защищенности СВТ включает только один седьмой класс - минимальная защищенность?	1.Первая группа. 2.Вторая группа. 3.Третья группа. 4. Четвертая группа.
29.	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.
30.	Какая группа классов защищенности СВТ характеризуется полномочной защитой, которая предусматривает присвоение каждому субъекту и объекту системы классификационных меток, указывающих место субъекта объекта в соответствующей иерархии, и включает четвертый, третий и второй классы?	1.Первая группа. 2.Вторая группа. 3.Третья группа. 4. Четвертая группа.
31.	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.
32.	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.
33.	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию, называется?	1. Нормативно-методические документы. 2.Электроннаяподпись 3. Критическая информационная инфраструктура. 4.Хэш-фунция.
34.	Выделяются два вида электронной подписи, какие?	1.Простая и усиленная 2.Усиленная и сертифицированная. 3.Простая и квалифицированная.
35.	Какая электронная подпись (ЭП)	1.Усиленая неквалифицированная ЭП.

	однозначно подтверждает, что данное электронное сообщение отправлено конкретным лицом?	2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.
36.	Какая электронная подпись (ЭП) позволяет не только однозначно идентифицировать отправителя, но и подтвердить, что с момента подписания документа его никто не изменял?	1.Усиленая неквалифицированная ЭП. 2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.
37.	Какая электронная подпись (ЭП) дополнительно подтверждается сертификатом, выданным аккредитованным удостоверяющим центром?	1.Усиленая неквалифицированная ЭП. 2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.
38.	Какие объекты относятся к критической информационной инфраструктуре (КИИ)?	1. Информационные системы. 2. Телекоммуникационные сети. 3.Автоматизированные системы управления технологическими процессами. 4. Все, перечисленное в остальных пунктах.
39.	Единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках называется?	1.Критическая информационная инфраструктура (КИИ). 2.Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). 3.Межгосударственная нормативно-методическая комиссия (МНМК). 4.Система оперативно-розыскных мероприятий (СОРМ).
40.	Документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей называется?	1. Нормативно-методический документ. 2.Стандарт. 3.Руководящий документ. 4. Нормативно правовой акт.
41.	В России ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является?	1. Федеральная служба безопасности. 2. Федеральная служба по техническому и экспортному контролю (ФСТЭК). 3. Служба внешней разведки. 4. Федеральная служба охраны.
42.	Основными функциями ФСТЭК являются?	1.Проведение единой технической политики и координация работ по защите информации 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. 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. 4. Все, перечисленное в остальных пунктах.
43.	Техническая защита информации – это?	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.
44.	Физическая защита информации – это?	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.
45.	Криптографическая защита информации – это?	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.
46.	Какие наиболее характерные и часто реализуемые угрозы ИБ АС?	1.Несанкционированное копирование с носителей информации. 2.Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной. 3.Игнорирование установленных правил при определении ранга системы. 4. Все, перечисленное в остальных пунктах.
47.	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.
48.	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.
49.	Модель угроз информационной безопасности – это	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.

50.	Совокупность требований в части защиты СВТ и АС образуют?	1.Окно защиты. 2.Класс защищенности. 3.Окно угрозы. 4. Уровень контроля отсутствия недекларированных возможностей.
Блок заданий закрытого типа Формируемые ПК 2.3		
1.	Межсетевые экраны какого типа устанавливают на физическом периметре информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
2.	Межсетевые экраны какого типа устанавливаются на логической границе информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
3.	Межсетевые экраны какого типа предназначены для размещения на мобильных или стационарных узлах информационных систем?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
4.	Межсетевые экраны какого типа осуществляют разбор http(s)-трафика между веб-сервером и клиентом?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
5.	Межсетевые экраны какого типа работают с промышленными протоколами передачи данных?	1.Межсетевые экраны типа «А» 2.Межсетевые экраны типа «Б» 3.Межсетевые экраны типа «В» 4.Межсетевые экраны типа «Г» 5.Межсетевые экраны типа «Д»
6.	Сколько существует классов систем обнаружения вторжений?	1.Четырехуровненевая классификация систем обнаружения вторжений. 2.Шестиуровневая классификация систем обнаружения вторжений. 3.Трехуровневая классификация систем обнаружения вторжений.
7.	Замкнутая программная среда – это?	1.Ограничение подключений к системе и информационных потоков извне. 2. Ограничение программной среды. 3. Только разрешённые информационные потоки внутри системы. 4. Все, перечисленное в остальных пунктах.
8.	В спецификации профилей защиты выделяют системы обнаружения вторжений каких уровней?	1.Сегмента и хоста. 2.Сети и узла. 3.Шлюза и хоста.
9.	Какая система обнаружения вторжений подключается к коммуникационному оборудованию и контролирует сетевой трафик, наблюдая за несколькими сетевыми узлами?	1.Система уровня приложений. 2.Система уровня сети. 3.Система уровня узла. 4.Система уровня системных вызовов.
10.	Какая система обнаружения вторжений устанавливается на узел и проводит анализ системных вызовов, журналов работы приложений?	1.Система уровня приложений. 2.Система уровня сети. 3.Система уровня узла. 4.Система уровня системных вызовов.
11.	Сколько существует классов защищенности средств антивирусной	1.Четырехуровненевая классификация средств антивирусной защиты.

	защиты информации?	2.Шестиуровневая классификация средств антивирусной защиты. 3.Трехуровневая классификация средств антивирусной защиты.
12.	Какие существуют типы средств антивирусной защиты?	1.Средства антивирусной защиты, предназначенные для централизованного администрирования средств антивирусной защиты, установленных на компонентах информационных систем (тип «А»). 2.Средства антивирусной защиты, предназначенные для применения на серверах (тип «Б»). 3.Средства антивирусной защиты, предназначенные для применения на автоматизированных рабочих местах (тип «В»). 4.Средства антивирусной защиты, предназначенные для применения на автономных автоматизированных рабочих местах (тип «Г»). 5. Все, перечисленное в остальных пунктах.
13.	Сколько существует классов защиты средств доверенной загрузки?	1.Четырехуровненевая классификация средств доверенной загрузки. 2.Шестиуровневая классификация средств доверенной загрузки. 3.Трехуровневая классификация средств доверенной загрузки. 4.Пятиуровневая классификация средств доверенной загрузки.
14.	Какие выделяют типы средств доверенной загрузки?	1.Средства доверенной загрузки уровня базовой системы ввода-вывода. 2.Средства доверенной загрузки уровня платы расширения. 3.Средства доверенной загрузки уровня загрузочной записи. 4. Все, перечисленное в остальных пунктах.
15.	Сколько существует классов защиты средств контроля съемных машинных носителей?	1.Четырехуровненевая классификация контроля съемных машинных носителей. 2.Шестиуровневая классификация средств контроля съемных машинных носителей. 3.Трехуровневая классификация средств контроля съемных машинных носителей. 4.Пятиуровневая классификация средств контроля съемных машинных носителей.
16.	Какие различают типы средств контроля съемных машинных носителей информации?	1.Средства контроля подключения съемных носителей информации. 2.Средства контроля отчуждения (переноса) информации со съемных машинных носителей. 3.Средства контроля загрузки съемных носителей информации. 4.Средства контроля взаимодействия съемных носителей информации.
17.	Сколько введено классов операционных систем, используемых для обеспечения защиты информации?	1.Четырехуровненевая классификация операционных систем. 2.Шестиуровневая классификация операционных систем. 3.Трехуровневая классификация операционных систем. 4.Пятиуровневая классификация операционных систем.
18.	Какие различают типы операционных систем, используемых в целях обеспечения защиты информации?	1.Операционные системы общего назначения (тип «А»). 2.Встраиваемые операционные системы (тип «Б»). 3.Операционные системы реального времени (тип «В»). 4. Все, перечисленное в остальных пунктах.
19.	Операционные системы какого типа	1.Операционные системы типа «А».

	устанавливаются на средства вычислительной техники общего назначения, такие как АРМ, серверы, смартфоны, планшеты, телефоны?	2.Операционные системы типа «Б». 3.Операционные системы типа «В».
20.	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».
21.	Операционные системы какого типа предназначены для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности?	1.Операционные системы типа «А». 2.Операционные системы типа «Б». 3.Операционные системы типа «В».
22.	Какие виды средств защиты информации должны содержаться в информационных системах общего пользования?	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.
23.	Какие различают виды средств криптографической защиты информации (по ГОСТ Р 50922-2006)?	1.Средства шифрования. 2.Средства имитозащиты. 3.Средства электронной подписи. 4.Средства кодирования. 5.Средства изготовления ключевых документов. 6.Ключевые документы. 7.Аппаратные шифровальные (криптографические) средства. 8.Программные шифровальные (криптографические) средства. 9.Программно-аппаратные шифровальные (криптографические) средства. 10. Все, перечисленное в остальных пунктах.
24.	Является ли лицензируемым видом деятельности разработка, изготовление и распространение средств защиты информации, реализующих алгоритмы криптографического преобразования информации?	1.Да, является. 2.Нет, не является.
25.	Какие средства криптографической защиты обеспечивают создание электронной цифровой подписи с использованием закрытого ключа, подтверждение с использованием открытого ключа подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
26.	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.
27.	Какие средства шифрования	1.Средства электронной подписи.

	обеспечивают создание ключевых документов?	2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
28.	Какие СЗИ обеспечивают защиту от навязывания ложной информации, возможность обнаружения изменений информации с помощью реализованных в СЗИ криптографических механизмов?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты 5.Средства шифрования.
29.	Средства шифрования, в которых часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств, предназначенных для выполнения таких операций, - это?	1.Средства электронной подписи. 2.Средства кодирования. 3.Средства изготовления ключевых документов. 4. Средства имитозащиты. 5.Средства шифрования.
30.	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.
31.	Сколько классов криптографических средств защиты информации определено ФСБ России?	1.Шесть классов. 2.Пять классов. 3.Семь классов. 4.Четыре класса.
32.	К основным особенностям СЗИ этого класса относится их возможность противостоять атакам, проводимым из-за пределов контролируемой зоны?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
33.	Если криптографическое СЗИ может противостоять атакам, блокируемым средствами класса КС1, а также проводимым в пределах контролируемой зоны, то такое СЗИ соответствует какому классу?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
34.	В случае возможности противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными криптографическими СЗИ говорят о соответствии таких средств какому классу?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
35.	Если криптографическое СЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то речь идет о соответствии какому классу?	1. КС1. 2. КС2. 3. КС3. 4. КВ. 5. КА.
36.	Если к разработке способов атак привлекались специалисты в области использования НДВ системного программного обеспечения, была	1. КС1. 2. КС2. 3. КС3. 4. КВ.

	доступна соответствующая конструкторская документация и был доступ к любым аппаратным компонентам криптографических СЗИ, то защиту от таких атак могут обеспечивать средства какого класса?	5. КА.
37.	В соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» ценные активы организации условно можно разделить на какие активы?	1. Временные и финансовые. 2.Основные и вспомогательные. 3.Неопределенные и определенные.
38.	Что из перечисленного относится к основным активам организации?	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.
39.	Что из перечисленного относится к вспомогательным активам организации?	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.Сведения, компрометация которых никаким образом не повлияет на деятельность организации. 4.Аппаратно-программный комплекс – совокупность технических и программных средств, предназначенных для выполнения взаимосвязанных эксплуатационных функций по обработке информации ограниченного распространения, включающая в себя активную аппаратуру обработки данных, стационарную аппаратуру, периферийные обрабатывающие устройства, операционные системы и прикладное программное обеспечение. 5.Носители данных - носитель для хранения данных, включая электронный носитель и аналоговый. 6. Сеть - совокупность телекоммуникационных устройств, используемых для соединения нескольких физически удаленных сегментов информационной системы. 7. Персонал - все субъекты, имеющие легитимный доступ в пределах контролируемой зоны и являющиеся потенциальными внутренними нарушителями.
40.	Какой процесс понимается под идентификацией риска?	1. Процесс оценки и обработки рисков. 2.Процесс нахождения и определения рисков ИБ. 3. Коммуникация риска.
41.	Какой процесс понимается под оценкой риска?	1. Присвоение числовых значений последствиям реализации риска, а также вероятности его реализации.

		2.Процесс нахождения и определения рисков ИБ. 3. Коммуникация риска.
42.	В пакете организационно-распорядительной документации по информационной безопасности значительную роль играют документы второго уровня иерархии, определяющие порядок и методы выполнения того или иного вида деятельности по защите от угроз ИБ. Какие документы наиболее часто используются?	1.Типовой сценарий. 2.Регламент. 3. Описание требований и методов работы. 4.Инструкция.
43.	Регламент представляет собой свод правил принятия решений исполнителями в определенных ситуациях. Каких типов могут быть регламенты?	1.Регламенты верхнего уровня – описывают общие принципы, цели и границы принятия решений. 2.Регламенты среднего уровня - синхронизация действий и взаимная увязка подпроцессов ИБ. 3.Регламенты нижнего уровня - устанавливают варианты готовых решений (совокупности определенных действий).
44.	Какой документ определяет порядок выполнения отдельных или взаимосвязанных действий, совершаемых конкретным подразделением или работником организации в рамках определенных процессов ИБ?	1.Типовой сценарий. 2.Регламент. 3. Описание требований и методов работы. 4.Инструкция.
45.	Какие важные задачи решаются при создании системы физической защиты (СФЗ) объекта?	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.
46.	Какие мероприятия по управлению ИБ реализуют при размещении оборудования?	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 воды через крышу, взрыв на улице. 6. Все, перечисленное в остальных пунктах.
47.	Каким образом обеспечивают подачу электропитания при перебоях в подаче электроэнергии и других сбоях, связанных с электричеством?	1.Наличие нескольких источников электропитания. 2.Применение устройств бесперебойного электропитания (UPS). 3.Использование резервного генератора, если необходимо обеспечить функционирование

		оборудования в случае длительного отказа подачи электроэнергии от общего источника. 4. Все, перечисленное в остальных пунктах.
48.	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?	1.Силовые и телекоммуникационные линии, связывающие СОИ, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой. 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. 3.Применение устройств бесперебойного электропитания (UPS). 4.Силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи. 5.Использование бронированных кожухов, закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках, дублирующих маршрутов прокладки кабеля или альтернативных способов передачи, оптико-волоконных линий связи, а также проверки на подключение несанкционированных устройств к кабельной сети.
49.	Для обеспечения непрерывной работоспособности и целостности в организации постоянно проводится надлежащее техническое обслуживание (ТО) оборудования. Какие меры следует применять для этих целей?	1.Оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком. 2.Необходимо, чтобы ТО и ремонт оборудования проводились только санкционированными лицами (персоналом). 3.Следует хранить записи обо всех случаях, предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного ТО. 4.Необходимо принимать соответствующие меры безопасности при отправке оборудования для ТО за пределы организации. 5. Все, перечисленное в остальных пунктах.
50.	Служебная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования. Какие мероприятия по управлению ИБ следует применять в этом случае?	1.Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать защищенным образом. 2.Использовать стандартные функции удаления. 3.Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного ПО. 4.Проводить оценку риской в отношении носителей данных, содержащих важную информацию, с целью определения целесообразности их разрушения, восстановления или выбраковки.

Блок заданий открытого типа

Формируемые ПК 2.1.

1.Преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты, когда нарушитель с самого начала не планирует платить за услуги или же в какой-то момент времени отказывается от их отплаты называется?

2. Проникновение в компьютерную систему безопасности для удаления механизмов защиты или переконфигурирования системы с целью несанкционированного использования сети называется?

3. Неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карточек с фальшивыми идентификаторами абонентов, номеров и платежных отметок называется?

4.Неправомочное вмешательство в бизнес-процедуры (например, биллинг) с целью уменьшения оплаты услуг связи называется?
5. Для идентификации мошенничества важно определить его источники, от которых исходит угроза. Перечислите основные виды мошенничества?
6. Определите вид мошенничества: клонирование SIM-карт, телефонных трубок, позволяющее мошенникам совершать бесплатные вызовы в любых направлениях, так как счет за предоставленные услуги связи придет законному владельцу SIM-карты?
7. В этом виде мошенничества недобросовестный оператор конфигурирует свой коммутатор для осуществления международных вызовов через не подозревающего об этом оператора. "Благодаря" недостаткам в конфигурации коммутационного оборудования пострадавшая сторона даже не будет подозревать о том, что вызовы являются международными. В результате недобросовестный оператор выставляет клиенту счет за международное соединение, однако сам платит только за междугородный или местный вызов. С другой стороны, пострадавшему оператору приходится платить по международным тарифам, получая заметно меньшую плату от оператора-мошенника.
Определите вид мошенничества?
8. В этом виде мошенничества недобросовестный оператор направляет полученный вызов обратно оператору, из сети которого он исходит, но через сеть третьего оператора. В результате звонок возвращается недобросовестному оператору, который опять отправляет его по этой цепочке еще раз, таким образом, вызов "зацикливается", то есть многократно проходит через сеть одного и того же оператора - "жертвы", а недобросовестный оператор «положит» в свой карман приличную сумму. Определите вид мошенничества?
9. В этом виде мошенничества недобросовестный оператор доставляет свой клиентский трафик в сеть "жертвы" через сети VoIP. Для этого в сети оператора устанавливается шлюз IP-телефонии. Выигрыш, получаемый от реализации такого рода мошенничества, базируется на варьировании стоимости входящего и исходящего трафиков. В результате недобросовестный оператор существенно экономит свои денежные ресурсы. Определите вид мошенничества?
10. В этом виде мошенничества два недобросовестных оператора, один из которых не имеет лицензии на предоставление заявленных им услуг связи, заключают между собой соглашение с целью получения дополнительной прибыли. В соглашении оговаривается, что оператор, не имеющий лицензии, будет использовать сеть связи партнера-оператора в качестве транзитной для пропуска своего трафика и вливания его на сеть третьего оператора-"жертвы". В итоге через сеть ничего не подозревающего третьего оператора будет проходить трафик от двух операторов, а оплачиваться будет только часть трафика, пропускаемого согласно межоператорскому договору - налицо факт упущенной выгоды. Определите вид мошенничества?
11.Поясните понятие «внутреннее мошенничество»?
12. В этом виде внутреннего мошенничества сотрудник предприятия связи настраивает коммутационное оборудование таким образом, что для части маршрутов информация о предоставленных услугах не будет регистрироваться либо станет выводиться на незадействованный порт ввода/вывода, что чрезвычайно сложно обнаруживать, даже при анализе данных биллинговой системы, так как первичная информация о соединениях в нее не поступает. Определите вид мошенничества?
13. В этом виде внутреннего мошенничества биллинговые системы подвергаются действиям злоумышленника с целью прекращения регистрации или тарификации определенного объема записей о предоставленных услугах, которые создаются коммутационным оборудованием. Определите вид мошенничества?
14. Информационная безопасность – это?
15. Информационная безопасность согласно ГОСТ Р ИСО/МЭК 17799-2005, ст.2.1 – это?

Ответ. Защита конфиденциальности, целостности и доступности информации.

16. Дайте понятие угрозы информационной безопасности?
17. Конфиденциальность информации – это?
18. Целостность информации – это?
19. Доступность информации – это?
20. В чем заключается угроза раскрытия информации?
21. В чем заключается угроза целостности?
22. Когда возникает угроза отказа служб?
23. Дайте понятие контролируемой зоны?
24. Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или АС, преднамеренное обращение субъекта к компьютерной информации, доступ к которой ему не разрешен, независимо от цели обращения – это?
25. Какая информация относится к коммерческой тайне?
26. Политика безопасности – это?
27. В чем заключается режим разграничения доступа?
28. Защита информации – это?
29. Разработка законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением, называется?
30. Защита информации с помощью ее криптографического преобразования – это?
31. Обеспечение безопасности информации некриптографическими методами, с применением технических, программных и программно-технических средств, называется?
32. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты – это?
33. Что обычно понимают под угрозой?
34. Как называется попытка реализации угрозы и тот, кто предпринимает такую попытку?
35. Возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления называется?
36. Перечислите наиболее характерные и часто реализуемые угрозы ИБ АС?
37.Что такое естественные угрозы?
38.Что такое искусственные угрозы?
39.Модель угроз информационной безопасности – это?
40. При построении модели угроз безопасности часто возникают сложности с выявлением и указанием факторов риска, которые могут быть реализованы в ИС. Упростить работу возможно используя банк данных угроз безопасности информации ФСТЭК России. Где находится эта электронная база?
41.Какая структура определяет порядок и координирует действия обеспечения некриптографическими методами ИБ?
42. Какая структура определяет порядок и координирует действия обеспечения криптографическими методами ИБ?
43. Как называется документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей?
44. Как называется совокупность требований в части защиты СВТ и АС?
45.Так как любое СЗИ содержит некий программный код, то можно предположить, что он обладает функциональностью, способствующей организации успешных атак в отношении защищаемых объектов. Как называются такие возможности, не указанные в документации или описанные с искажением, использование которых может привести к нарушению ИБ?

46. Сколько уровней контроля на отсутствие недекларированных возможностей?
47.Сколько определено ФСТЭК классов защищенности средств вычислительной техники?
48.Сколько определено ФСТЭК классов защищенности автоматизированных систем?
49.Что такое СОРМ?
50.Совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами в области защиты информации называется?

Блок заданий открытого типа
Формируемые ПК 2.2.

1.Перечислите основные уровни обеспечения защиты информации?
2.Режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду называется?
3.Защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах государственного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости называется?
4.Обязанность не разглашать того, что стало известно лицу в силу его профессиональной деятельности; сюда принадлежит тайна исповеди, врачебная, адвокатская, нотариальная, служебная (канцелярская), тайна совещаний присяжных заседателей называется?
5.Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации называется?
6. В РФ устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений, перечислите их?
7.Любые сведения о физическом лице, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, называются?
8.Что такое модель нарушителя информационной безопасности?
9. Что понимается под идентификацией риска?
10.Присвоение числовых значений последствиям реализации риска, а также вероятности его реализации называется?
11.Процесс проверки инфраструктуры организации на наличие возможных уязвимостей сетевого периметра, виртуальной инфраструктуры, вызванных в том числе ошибками конфигурации, а также программного обеспечения и исходного кода приложений называется?
12.С какой целью проводится анализ защищенности?
13.Какой способ защиты информации заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры?
14.К каким способам защиты информации относятся блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств?
15.Какой способ защиты информации предполагает такие преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется, а также комплекс мероприятий по уменьшению степени распознавания самого объекта?

16.К каким способам защиты информации относятся криптографические методы преобразования информации, скрытие объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы?
17.Какой способ защиты информации заключается в разработке и реализации в процессе функционирования объекта комплекса мероприятий, создающих такие условия, при которых существенно затрудняются проявление и воздействие угроз?
18.К какому способу защиты информации относится разработка таких правил обращения с конфиденциальной информацией и средствами ее обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником?
19.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?
20.Как называется способ защиты информации, при котором пользователи и персонал объекта внутренне (т.е. материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации?
21.Какие средства защиты информации относятся к формальным средствам?
22.Какие средства защиты информации относятся к неформальным средствам?
23.К каким средствам защиты относятся механические, электрические, электромеханические и т.п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов?
24.К каким средствам защиты относятся различные электронные и электронно-механические и т.п. устройства, схемно- встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?
25.Какие средства защиты объединены в класс технических средств защиты информации?
26.К каким средствам защиты относятся специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решении задач защиты информации?
27.К каким средствам защиты относятся специально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач защиты информации, осуществляемые в виде целенаправленной деятельности людей?
28.К каким средствам защиты относятся существующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации?
29.К каким средствам защиты относятся сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе?
30.Какие средства чаще всего используются для проведения анализа защищенности?
31.Механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход политики разграничения доступа называется?
32.Разделение информации, циркулирующей в информационной системе, на части, элементы, компоненты, объекты и т.д. и организация системы работы с информацией, предполагающей доступ пользователей к той части (к тем компонентам) информации, которая им необходима для выполнения функциональных обязанностей называется?
33.Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками, называется?
34.Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации, называется?

35.Деятельность, направленная на предотвращение воздействия на защищаемую информацию от ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.
36.Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации, называется?
37. Как называется документ, определяющий порядок взаимодействия подразделений и работников организации в рамках определенного процесса ИБ?
38.Как называется документ, определяющий порядок выполнения отдельных или взаимосвязанных действий конкретным работником организации в рамках определенных процессов ИБ?
39.Какой документ определяет унифицированные правила и методы выполнения действий (функций), независимые от исполнителей?
40.На какие группы подразделяются категории обрабатываемых персональных данных?
41.К какой группе ПДн относится информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информация о здоровье и интимной жизни субъект?
42.К какой группе ПДн относятся данные, характеризующие биологические или физиологические особенности субъекта, например, фотография или отпечатки пальцев?
43.К какой группе ПДн относятся сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом?
44.Какие персональные данные относят к 4 группе – иные категории ПДн?
45. Сколько уровней защищенности персональных данных устанавливается в ИС при обработке персональных данных?
46. Что такое модель нарушителя ИБ?
47.Какие рекомендации по составлению модели нарушителя дают ФСТЭК и ФСБ?
48.Какая категория нарушителей вносит закладки в программно-техническое обеспечение системы, применяет особые средства проникновения в систему и проводит специальные исследования и выделена под иностранные спецслужбы?
49.Какая категория нарушителей может проводить анализ кода прикладного ПО, сопоставлять данные, находить уязвимости и использовать их. В эту категорию попадают конкуренты, системные администраторы и разработчики программного обеспечения, криминальные и террористические группы?
50.Какая категория нарушителей использует для осуществления атак только доступные источники. К ним причисляются рядовые сотрудники организации, пользователи системы и люди, не имеющие отношение к компании?

Блок заданий открытого типа
Формируемые ПК 2.3.

1.Для каких целей используется физическая защита информации?
2. Какие задачи решаются при создании системы физической защиты?
3. Что такое периметр безопасности?
4. Какие средства, реализующие контроль за информацией, направленной в АС или исходящей из нее, выполняющие фильтрацию информации по заданным критериям, рассматриваются ФСТЭК в качестве СЗИ?
5.Какие средства автоматизируют процесс контроля событий в сети с проведением анализа этих событий с целью поисках признаков инцидента ИБ?

6.Какие СЗИ выявляют и соответствующим образом реагируют на средства несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации СЗИ?
7.Какие СЗИ обеспечивают меры по защите машинных носителей информации в части обеспечения контроля за их использованием?
8.Сколько классов защищенности межсетевых экранов по уровням контроля межсетевых информационных потоков определено ФСТЭК?
9. Сколько уровней защиты содержит классификация межсетевых экранов по классам защиты?
10.Какие типы межсетевых экранов определены ФСТЭК России?
11. Где устанавливаются межсетевые экраны типа «А»?
12. Где устанавливаются межсетевые экраны типа «Б»?
13. Где устанавливаются межсетевые экраны типа «В»?
14. Какого типа межсетевые экраны осуществляют разбор http(s)-трафика между веб-сервером и клиентом, и где они устанавливаются?
15. Какого типа межсетевые экраны работают с промышленными протоколами передачи данных?
16.Сколько уровней защиты содержит классификация средств защиты систем обнаружения вторжений?
17.Какие типы систем обнаружения вторжений Вы знаете?
18.Где подключается система обнаружения вторжений уровня сети и что она контролирует?
19.Где устанавливается система обнаружения вторжений уровня узла и что она анализирует?
20.Сколько уровней защиты содержит классификация защищенности средств антивирусной защиты информации?
21. Какие типы средств антивирусной защиты Вы знаете?
22.Сколько установлено классов защиты средств доверенной загрузки?
23. Какие типы средств доверенной загрузки выделено ФСТЭК?
24. Сколько установлено классов защиты средств контроля съемных машинных носителей?
25.Какие выделяются типы средств контроля съемных машинных носителей информации?
26. Сколько установлено классов операционных систем для обеспечения защиты информации?
27. Какие различают типы операционных систем, используемых в целях обеспечения защиты информации?
28. Где устанавливаются операционные системы типа «А»?
29. Где устанавливаются операционные системы типа «Б»?
30. Для каких целей предназначены операционные системы типа «В»?
31.Средства защиты информации, реализующее алгоритмы криптографического преобразования информации называются?
32. Является ли разработка, изготовление и распространение криптографических средств защиты информации лицензируемым видом деятельности?
33.Какие криптографические СЗИ, обеспечивают возможность разграничения доступа к информации?
34.Средства шифрования, в которых часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств, предназначенных для выполнения таких операций, называют?
35. Электронные документы, содержащие ключевую информацию, необходимую для выполнения криптографических преобразований с помощью средств шифрования, называют?
36.Средства шифрования, обеспечивающие создание ключевых документов, называют?
37.Защиту от навязывания ложной информации, возможность обнаружения изменений информации с помощью реализованных в СЗИ криптографических механизмов, обеспечивают?
38.Какие классы криптографических СЗИ определены ФСБ России?
39. Если криптографическое СЗИ может противостоять атакам, проводимым из-за пределов контролируемой зоны, при этом подразумевается, что создание способов атак, их подготовка и проведение осуществляется без участия специалистов в области разработки и анализа криптографических СЗИ, предполагается, что информация о системе, в которой применяются

указанные СЗИ, может быть получена из открытых источников, то такое СЗИ соответствует классу?
40. Если криптографическое СЗИ может противостоять атакам, блокируемым средствами класса КС1, а также проводимым в пределах контролируемой зоны, то такое СЗИ соответствует классу?
41. Если криптографическое СЗИ может противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными криптографическими СЗИ, то такое СЗИ соответствует классу?
42. Если криптографическое СЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то такое СЗИ соответствует классу?
43.Если к разработке способов атак привлекались специалисты в области использования НДВ системного программного обеспечения, была доступна соответствующая конструкторская документация и был доступ к любым аппаратным компонентам криптографических СЗИ, то такое СЗИ соответствует классу?
44. Какой регулятор ИБ осуществляет организацию и контроль над проведением работ по защите информации в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения?
45. Какой регулятор ИБ осуществляет поддержание и развитие сегмента международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации», а также за безопасность системы межведомственного электронного документооборота?
46. Как называется единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках?
47. Что подразумевается под критической информационной инфраструктурой?
48. Что входит в состав объектов критической информационной инфраструктуры?
49.Как называют информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию?
50. Что подтверждает простая ЭП?

Составил: преподаватель Грубник Е.М.