СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
_____ А.Н. Калугин
«28». 06.2024 г.

УТВЕРЖДАЮ
Зам. директора по УР
_____ Иванешко И.В.
«28» 06 2024 г.

Комплект оценочных материалов для промежуточной аттестации
(другая форма аттестации - 7 семестр, дифференцированный зачет – 8 семестр)
по МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания
ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания
специальность 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания

Дифференцированный зачет является промежуточной формой контроля, подводит итог освоения МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания.

Результатом освоения программы МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания является овладение студентами профессиональных (ПК) и общих (ОК) 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 системах радиосвязи, мобильной связи и телерадиовещания.
ПК 3.3.	Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Результатом освоения программы МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания являются освоенные умения и усвоенные знания.

В результате освоения МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания студент должен уметь:

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

У2 – определять оптимальные способы обеспечения информационной безопасности;

У3 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;

У4 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;

У5 - защищать базы данных при помощи специализированных программных продуктов;

знать:

З1 – принципы построения систем радиосвязи, мобильной связи и телерадиовещания;

З2 - международные стандарты информационной безопасности;

З3 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;

З4 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

З5 - классификацию угроз сетевой безопасности;

З6 - методы и способы защиты информации, передаваемой по проводным и беспроводным направляющим системам;

З7 - правила проведения возможных проверок согласно нормативным документам ФСТЭК;

З8 - средства защиты различных операционных систем и среды передачи информации;

Другая форма аттестации и дифференцированный зачёт являются промежуточными формами контроля, подводят итог освоения программы МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания

Другая форма аттестации проводится в форме тестирования, дифференцированный зачёт по МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания проводится в форме тестирования. На промежуточную аттестацию выделяется по 2 часа (последнее занятие в 7 семестре) из общего количества часов на МДК.03.01.

Тест содержит два блока: блок 1 для 7 семестра (в 1 блоке 75 тестовых позиций и 75 теоретических вопросов с кратким ответом, блок 2 для 8 семестра (80 тестовых позиций и 80 теоретических вопросов с кратким ответом).

Тест для 7 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 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.

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 100-90%;

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.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания
Блок заданий 1 (7 семестр) закрытого типа

Проверяемые результаты обучения – ПК 3.1		
1.	Прочитайте текст и выберите несколько правильных ответов. Какие службы из перечисленных организуют защиту информации на уровне предприятия?	1.Служба экономической безопасности. 2.Служба безопасности персонала (режимный отдел). 3.Кадровая служба. 4.Служба юридической безопасности.
2.	Прочитайте текст и выберите несколько правильных ответов. На какие категории разделяются кризисные ситуации, не предотвращенные СЗИ, по степени серьезности и размерам наносимого ущерба?	1.Угрожающая. 2.Умышленная. 3.Серьезная. 4.Случайная.
3.	Прочитайте текст и выберите несколько правильных ответов. Какими мерами из перечисленных достигается непрерывность процесса функционирования АС и своевременность восстановления ее работоспособности?	1. Постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты. 2.Проведением специальных регламентных мероприятий и оперативной заменой оборудования. 3.Применением различных способов резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов системы.
4.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к угрожающим кризисным ситуациям, не предотвращенным средствами защиты информации?	1.Выход из строя рабочей станции (с потерей информации). 2.Нарушение подачи электроэнергии в здании. 3.Выход из строя файлового сервера (с потерей информации). 4.Выход из строя файлового сервера (без потери информации).
5.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к угрожающим кризисным ситуациям, не предотвращенные средствами защиты информации?	1.Частичная потеря информации на сервере без потери его работоспособности. 2.Частичная потеря информации на рабочей станции без потери ее работоспособности. 3.Выход из строя рабочей станции (без потери информации). 4.Выход из строя локальной сети (физической среды передачи данных).
6.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к серьезным кризисным ситуациям, не предотвращенным средствами защиты информации?	1.Выход из строя рабочей станции (с потерей информации). 2.Выход из строя рабочей станции (без потери информации). 3. Частичная потеря информации на сервере без потери его работоспособности. 4.Частичная потеря информации на рабочей станции без потери ее работоспособности.
7.	Прочитайте текст и выберите один правильный ответ. Что из перечисленного относится к ситуациям, не предотвращенным средствами защиты информации, требующим внимания?	1. Частичная потеря информации на сервере без потери его работоспособности. 2.Частичная потеря информации на рабочей станции без потери ее работоспособности. 3.Несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

8.	Прочитайте текст и выберите несколько правильных ответов. Какие объекты информатизации подлежат обязательной аттестации по требованиям безопасности информации?	1. Объекты, предназначенные для обработки конфиденциальной информации 2.Объекты, предназначенные для обработки информации, составляющей государственную тайну. 3. Объекты, предназначенные для управления экологически опасными объектами. 4. Объекты, предназначенные для ведения секретных переговоров.
9.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного обеспечивает механизм полномочного управления доступом?	1.Разграничение доступа пользователей к информации, которой назначена категория конфиденциальности. 2. Обнаружение и регистрация попыток несанкционированного доступа. 3.Контроль потоков конфиденциальной информации в системе. 4.Контроль работоспособности используемых систем защиты информации.
10.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного обеспечивает механизм полномочного управления доступом?	1.Контроль подключения и использования устройств с назначенными категориями конфиденциальности. 2.Контроль допуска к информации для пользователей разных уровней. 3. Контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей. 4. Контроль печати конфиденциальных документов.
11.	Прочитайте текст и выберите один правильный ответ. Для каких видов устройств поддерживается теневое копирование?	1.Подключаемые сменные диски. 2.Дисководы оптических дисков с функцией записи. 3.Принтеры. 4.Все ответы верны.
12.	Прочитайте текст и выберите несколько правильных ответов. Какие функции выполняет средство защиты информации от НСД?	1.Идентификация и аутентификация пользователей и устройств. 2.Регистрация запуска (завершения) программ и процессов. 3.Управление информационными потоками между устройствами. 4.Контроль работоспособности используемых систем защиты информации.
13	Прочитайте текст и выберите один правильный ответ. Как называют сервис, который гарантирует, что информация получена из законного источника и получателем является тот, кто нужно?	1.Аутентификация. 2.Авторизация. 3.Идентификация.
14.	Прочитайте текст и выберите один правильный ответ. Какую возможность вычислительной системе дает идентификация пользователя?	1.Отличать одного пользователя от другого. 2.Гарантировать, что пользователь является тем, за кого он себя выдает. 3.Обеспечить корректное управление доступом. 4.Гарантировать отсутствие несанкционированного доступа.
15.	Прочитайте текст и выберите один правильный ответ. В чем заключается суть процедуры управления доступом или авторизации?	1.Гарантирование того, что пользователь является тем, за кого он себя выдает. 2.Гарантирование того, что пользователь обращается к требуемому ресурсу (серверу). 3.Определение прав и разрешений пользователей по доступу к ресурсам. 4.Невозможность несанкционированного просмотра и изменения данных.

16.	Прочитайте текст и выберите один правильный ответ. Какую аутентификацию рекомендуется использовать при удаленном доступе?	1.Однофакторную. 2.Двухфакторную. 3.Трехфакторную.
17.	Прочитайте текст и выберите несколько правильных ответов. Какие записи должны вестись при аудите информационной безопасности?	1.Вход/выход пользователей. 2.Неудачные попытки входа. 3.Все системные события 4.Записи зависят от уровня аудита.
18.	Прочитайте текст и выберите один правильный ответ. В чем заключается суть многофакторной аутентификации?	1.Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия. 2.Аутентификация не может выполняться с помощью пароля. 3.Аутентификация должна выполняться третьей доверенной стороной. 4.Аутентификация должна выполняться с использованием смарт-карты.
19	Прочитайте текст и выберите один правильный ответ. Для чего нужна система контроля доступа?	1.Предотвратить проникновение на частную территорию посторонних лиц. 2.Организовать учет рабочего времени, фиксацию времени въезда и выезда транспортных средств. 3.Защитить материальные ценности, включая оборудование, от повреждений и кражи. 4.Все ответы верны.
20.	Прочитайте текст и выберите один правильный ответ. Как называется уникальная информация, позволяющая различать пользователей друг от друга?	1.Идентификатор (логин). 2.Пароль. 3.Учетная запись. 4.Ключ.
21.	Прочитайте текст и выберите один правильный ответ. Как называют совокупность идентификатора и пароля пользователя?	1.Логин пользователя. 2.Учетная запись пользователя. 3.Ключ пользователя.
22.	Прочитайте текст и выберите один правильный ответ. Какое средство аутентификации рекомендуется использовать в VPN?	1.Смарт-карту и пароль. 2.Только смарт-карту. 3.Только пароль. 4.Биометрическую идентификацию.
23.	Прочитайте текст и выберите один правильный ответ. Как называют процедуру проверки принадлежности пользователю предъявленного им идентификатора?	1.Идентификацией пользователя. 2.Аутентификацией пользователя. 3.Регистрацией пользователя. 4.Созданием учетной записи пользователя.
24.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных мер используют для повышения общего уровня защищенности сетевого периметра?	1.Постоянный контроль сетевого периметра компании с целью обнаружения сервисов, расположенных на периметре и доступных из сети Интернет. 2.Автоматизированный поиск уязвимостей в сервисах, расположенных на периметре. 3.Использование фрагментарного подхода к ИБ сервисов, расположенных на периметре.
25.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных мер используют для повышения общего уровня защищенности сетевого	1.Устранение лишних сервисов, размещение которых на периметре не обусловлено необходимостью. 2.Автоматизированный поиск уязвимостей в сервисах, расположенных на серверах компании. 3.Внедрение политики патч-менеджмента, уделение

	периметра?	внимания системам с уязвимостями, для которых существуют эксплойты в открытом доступе, а также наиболее уязвимым системам.
Проверяемые результаты обучения – ПК 3.2		
26.	Прочитайте текст и выберите несколько правильных ответов. Решение каких задач обеспечивает система защиты информации от угроз несанкционированного доступа?	1. Задержка нарушителей, их выявление на объекте. 2.Разграничение доступа к ресурсам автоматизированных рабочих мест и серверов информационной системы. 3.Обеспечение функций регистрации и учета событий безопасности. 4.Обеспечение целостности программно-аппаратной среды применяемых программных и программно-технических средств. 5. Реагирование сотрудников службы безопасности.
27.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного входит в состав системы защиты от несанкционированного доступа?	1.Средства централизованного управления средствами защиты от несанкционированного доступа. 2.Сертифицированные средства защиты от несанкционированного доступа. 3. Средства предупреждения несанкционированного доступа, нерегламентированных воздействий. 4.Средства удаленного администрирования АРМ и серверов, входящих в состав информационной системы.
28.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного входит в состав системы защиты от несанкционированного доступа?	1.Встроенные в системное программное обеспечение средства идентификации, аутентификации, авторизации, мониторинга событий и контроля целостности. 2. Средства предупреждения несанкционированного доступа, нерегламентированных воздействий. 3.Средства резервного копирования и восстановления конфигураций средств защиты от несанкционированного доступа. 4.Средства реагирования сотрудников службы безопасности.
29.	Прочитайте текст и выберите несколько правильных ответов. Какие методы защиты информации могут быть использованы для предотвращения несанкционированного доступа?	1.Пароли для авторизации во время работы. 2.Регулярное создание бэкапов наиболее важных и ценных информационных массивов. 3.Криптографические средства шифрования информации для ее передачи и хранения. 4.Все ответы верны.
30.	Прочитайте текст и выберите несколько правильных ответов. Какие методы защиты информации могут быть использованы для предотвращения несанкционированного доступа?	1.Модули доверенной загрузки. 2.Средства предотвращения сетевых атак (межсетевой экран, антивирус, прокси-сервер). 3.Выполнение резервирования, дублирования компонентов информационной системы, которые связаны с хранением информации. 4.Все ответы верны.
31.	Прочитайте текст и выберите несколько правильных ответов. Какие существуют методы контроля аппаратной конфигурации компьютера?	1.Статический контроль конфигурации. 2.Стандартный контроль конфигурации. 3.Динамический контроль конфигурации. 4.Индивидуальный контроль конфигурации.
32.	Прочитайте текст и выберите несколько правильных ответов. Каковы преимущества пользовательских VPN?	1.Сотрудники, находящиеся в командировке могут подключаться к сети компании. 2.Удаленные сайты могут осуществлять обмен информацией незамедлительно. 3.Сотрудники могут работать из дома, необязательно присутствие на работе. 4.Преимуществ нет.

33.	Прочитайте текст и выберите несколько правильных ответов. Какие политики безопасности из перечисленных являются для межсетевого экрана «политиками по умолчанию»?	1.Запретить весь входящий трафик, который явно не разрешен. 2.Разрешить весь входящий трафик, который явно не запрещен. 3.Разрешить весь исходящий трафик, который явно не запрещен. 4.Запретить весь исходящий трафик, который явно не разрешен.
34.	Прочитайте текст и выберите один правильный ответ. Когда рекомендуется проводить работы по анализу защищенности ИТ-инфраструктуры?	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.
35.	Прочитайте текст и выберите один правильный ответ. Сколько классов защищенности АС от несанкционированного доступа к информации выделено в Руководящем документе ГТК «Классификация автоматизированных систем и требований по защите информации»?	1. 6 классов защищенности. 2. 7 классов защищенности. 3. 9 классов защищенности. 4. 5 классов защищенности. 5. 8 классов защищенности.
36.	Прочитайте текст и выберите несколько правильных ответов. Какие шаги следует предпринимать при обнаружении подозрительного трафика в сети?	1.Записывать в журнал сведения о дополнительном трафике между источником и пунктом назначения. 2.Заблокировать удаленную систему. 3.Записывать в журнал весь трафик, исходящий из источника. 4.Записывать в журнал содержимое пакетов из источника.
37.	Прочитайте текст и выберите один правильный ответ. Где лучше размещать VPN сервер?	1.В отдельной DMZ. 2.В DMZ интернета, вместе с остальными серверами. 3.Во внутренней сети компании.
38.	Прочитайте текст и выберите один правильный ответ. Какой должна быть система аутентификации, используемая в VPN?	1.Однофакторной. 2.Двухфакторной. 3.Трехфакторной. 4.Четырехфакторной.
39.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного могут определять атаки сканирования сети?	1.Топологию целевой сети. 2.Типы сетевого трафика, пропускаемые межсетевым экраном. 3. Оценку общего состояния безопасности системы 4.Операционные системы, которые выполняются на хостах.
40	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного могут определять атаки сканирования сети?	1.Программное обеспечение сервера, которое выполняется на хостах. 2.Номера версий для всего обнаруженного программного обеспечения. 3.Аутентификационные данные пользователей. 6.Все ответы верны.
41.	Прочитайте текст и выберите один правильный ответ. Наличие какого элемента характерно для всех архитектур DMZ?	1.Почтовый сервер. 2.DNS. 3.NTP. 4.Межсетевой экран.
42.	Прочитайте текст и выберите несколько правильных ответов.	1.Информация сохраняется в секрете. 2.Удаленные сайты могут осуществлять обмен

	Каковы преимущества виртуальных частных сетей?	информацией незамедлительно. 3.Удаленные пользователи не ощущают себя изолированными от системы, к которой они осуществляют доступ. 4.Низкая стоимость.
43.	Прочитайте текст и выберите один правильный ответ. Что такое пользовательские VPN?	1.Построены между отдельной пользовательской системой и узлом или сетью организации. 2.Используются частными пользователями для связи друг с другом. 3.Одно из названий VPN.
44.	Прочитайте текст и выберите один правильный ответ. Каким образом осуществляется доступ к внутренней сети пользователем, подключенным через VPN?	1.Нужно просто знать адрес сервера VPN. 2.Необходимо пройти процедуру аутентификации на сервере. 3.Доступ к внутренней сети не может быть получен ни каким образом.
45.	Прочитайте текст и выберите один правильный ответ. Каковы преимущества использования системы унифицированного управления угрозами?	1.Увеличивается пропускная способность сети. 2.Уменьшается сложность управления. 3.Увеличивается безопасность сетевого периметра. 4.Уменьшается количество попыток несанкционированного доступа.
46.	Прочитайте текст и выберите один правильный ответ. Что должно располагаться в сети демилитаризованной зоны (DMZ)?	1.Рабочие станции пользователей. 2.Серверы, которые должны быть доступны только внутренним пользователям. 3.Серверы, которые должны быть доступны из внешних сетей. 4.Серверы, содержащие наиболее чувствительные данные.
47.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных веб-серверов следует расположить во внешней DMZ?	1.Веб-сервер, на котором осуществляется on-line'овый заказ услуг. 2.Веб-сервер, на котором публикуются распоряжения руководства организации. 3.Веб-сервер, на котором могут находиться личные данных сотрудников. 4.Веб-сервер, на котором опубликованы общедоступные телефоны и координаты организации.
48.	Прочитайте текст и выберите один правильный ответ. Как называется атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения путем создания огромного количества фальшивых запросов на доступ к ресурсам системы?	1. Отказ от обслуживания 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Сниффинг (Sniffing). 5.Спуфинг. 6.Сканирование портов.
49.	Прочитайте текст и выберите один правильный ответ. Как называется атака, целью которой является трафик локальной сети?	1. Отказ от обслуживания. 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Сниффинг (Sniffing). 5.Спуфинг. 6.Сканирование портов.
50.	Прочитайте текст и выберите один правильный ответ. Как называется атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой?	1.«Отказ от обслуживания» (Denial of Service - DoS). 2.Срыв стека. 3.Внедрение на компьютер деструктивных программ. 4.Сниффинг (Sniffing). 5.Спуфинг. 6.Сканирование портов.

Проверяемые результаты обучения – ПК 3.3		
51.	Прочитайте текст и выберите несколько правильных ответов. Каковы преимущества использования IDS?	1.Возможность иметь реакцию на атаку. 2.Возможность блокирования атаки. 3.Выполнение документирования существующих угроз для сети и систем. 4.Нет необходимости в межсетевых экранах.
52.	Прочитайте текст и выберите один правильный ответ. Что анализируется при определении злоупотреблений?	1.Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак». 2.Анализируются события для обнаружения неожиданного поведения. 3.Анализируются подписи в сертификатах открытого ключа. 4.Анализируется частота возникновения некоторого события.
53.	Прочитайте текст и выберите один правильный ответ. Что анализируется при определении аномалий?	1.Анализируется частота возникновения некоторого события. 2.Анализируются различные статистические и эвристические метрики. 3.Анализируются события на соответствие некоторым образцам, называемым «сигнатурами атак». 4.Анализируется исключительно интенсивность трафика.
54.	Прочитайте текст и выберите несколько правильных ответов. Какие устройства могут выполнять функции NAT?	1.Маршрутизаторы. 2.Межсетевые экраны. 3.Почтовые сервера. 4.DNS сервера.
55.	Прочитайте текст и выберите один правильный ответ. Что из перечисленного понимают под унифицированным управлением угрозами (UTM)?	1.Создание базы данных потенциальных угроз. 2.Создание базы данных точек входа в сеть. 3.Централизованное управление несколькими сетевыми устройствами. 4.Централизованное управление всеми межсетевыми экранами.
56.	Прочитайте текст и выберите несколько правильных ответов. Что включает в себя типовая система унифицированного управления угрозами?	1.Межсетевой экран с возможностями определения и удаления вредоносного ПО на находящихся под его управлением хостах. 2.Рабочие станции специалистов по информационной безопасности. 3.Межсетевой экран с возможностями блокирования нежелательного трафика. 4.Сервера, предоставляющие сервисы удаленным пользователям.
57	Прочитайте текст и выберите несколько правильных ответов. Какие функции из перечисленных выполняют DLP-системы?	1.Контроль каналов коммуникаций, мест хранения информации, действий пользователей на рабочих станциях. 2.Управление доступом к данным и ресурсам. 3.Анализ поведения пользователей. 4.Анализ событий информационной безопасности. 5.Проведение расследований.
58.	Прочитайте текст и выберите один правильный ответ. 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»
59.	Прочитайте текст и выберите один правильный ответ. Где устанавливают межсетевые экраны для веб-приложений?	1.После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану). 2.Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.

		3.Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу). 4.Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен.
60.	Прочитайте текст и выберите один правильный ответ. Почему существует необходимость в межсетевых экранах для виртуальных инфраструктур?	1.Сетевой трафик, который передается между гостевыми ОС внутри хоста, передается в зашифрованном виде. 2.Сетевой трафик, который передается между гостевыми ОС внутри хоста, использует протоколы, отличные от TCP/IP. 3.Сетевой трафик, который передается между гостевыми ОС внутри хоста, не может просматриваться внешним межсетевым экраном. 4.В сетевом трафике, который передается между гостевыми ОС внутри хоста, указаны другие номера портов, чем в обычном сетевом трафике.
61.	Прочитайте текст и выберите один правильный ответ. 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»
62.	Прочитайте текст и выберите один правильный ответ. 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»
63.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите несколько правильных ответов. Какие механизмы защиты информации должны обязательно использоваться в криптошлюзах согласно требований руководящих документов?	1.Аутентификации взаимодействующих сторон. 2.Криптографическая защита передаваемых данных. 3. Подтверждение подлинности и целостности доставленной информации. 4. Анализ и перехват трафика для выявления конфиденциальной информации. 5.Защите от повтора, задержки и удаления сообщений.
65.	Прочитайте текст и выберите несколько правильных ответов. Какие механизмы защиты должен включать сервис для проведения видеоконференций?	1.Защиту передачи аудио и видео по технологии WebRTC. 2.Шифрование данных с помощью протоколов TLS, DTLS, AES-128, AES-256. 3. Защиту передачи аудио и видео по технологии WebPPC. 4.Дополнительное шифрование контента протоколом SRTP. 5.Защиту от DDoS-атак.
66.	Прочитайте текст и выберите несколько правильных ответов. Какие мероприятия из перечисленных необходимо проводить для решения проблемы несанкционированного доступа к видеоконференцсвязи?	1.Использовать пароль для подключения к конференции и сообщать его участникам по защищённым каналам связи. 2.Размещать ссылку и пароль вместе. 3.Если нет защиты доступа паролем, то следует постоянно менять ссылку приглашения. 4.Использовать функцию зала ожидания.
67.	Прочитайте текст и выберите один правильный ответ.	1.Шифрование данных, передаваемых между узлами сети.

	Какие функции из перечисленных выполняют криптошлюзы?	2.Обнаружение и предотвращение компьютерных атак. 3.Управление доступом к данным и ресурсам. 4. Все ответы верны.
68.	Прочитайте текст и выберите один правильный ответ. Что такое криптостойкость?	1.Способность системы радиосвязи противостоять введению в нее неверной информации, а также навязыванию ложных рабочих режимов. 2.Способность системы радиосвязи противодействовать раскрытию злоумышленником смысла передаваемой информации. 3.Передача ложной информации, специально разработанной для введения злоумышленника в заблуждение, по каналам радиосвязи.
69.	Прочитайте текст и выберите несколько правильных ответов. Какие функции из перечисленных выполняет SIEM система?	1.Сбор событий ИБ. 2.Контроль каналов коммуникаций, мест хранения информации, действий пользователей на рабочих станциях. 3.Анализ поведения пользователей в сети. 4.Предоставление пользователю данных об активах, событиях и инцидентах. 5.Анализ событий ИБ.
70.	Прочитайте текст и выберите несколько правильных ответов. Какие функции из перечисленных выполняет SIEM система?	1.Управление доступом к данным и ресурсам. 2.Обработка (корреляция) событий ИБ. 3.Создание и управление записями об инцидентах ИБ. 4.Отчетность. 5.Анализ и перехват трафика компании для выявления конфиденциальной информации.
71.	Прочитайте текст и выберите один правильный ответ. Какая электронная подпись (ЭП) однозначно подтверждает, что данное электронное сообщение отправлено конкретным лицом?	1.Усиленая неквалифицированная ЭП. 2. Усиленная квалифицированная ЭП. 3. Простая ЭП. 4.Сложная ЭП.
72.	Прочитайте текст и выберите несколько правильных ответов. Какие функции из перечисленных выполняют DLP-системы?	1.Контроль рабочего времени сотрудников. 2.Обработка (корреляция) событий информационной безопасности. 3.Построение отчетов по событиям и инцидентам. 4.Работа в территориально распределенной сети.
73	Прочитайте текст и выберите несколько правильных ответов. Какие требования предъявляются к хранению ключевых носителей содержащих электронную подпись?	1.Личные ключевые носители пользователей рекомендуется хранить в электронном виде. 2. Личные ключевые носители пользователей рекомендуется хранить в запираемом хранилище. 3. Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией.
74.	Прочитайте текст и выберите несколько правильных ответов. Какими мерами обеспечивается безопасность резервных копий?	1.Хранение резервных копий в шифрованном виде. 2.Соблюдение мер физической защиты резервных копий. 3.Строгая регламентация порядка использования резервных копий.
75.	Прочитайте текст и выберите один правильный ответ. 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.

Вопросы задания открытого типа для другой формы аттестации
по МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания
Блок заданий 1 (7 семестр)
Проверяемые результаты обучения – ПК 3.1

1. Прочитайте текст и напишите ответ.

Как называется процедура распознавания субъекта в процессе регистрации в системе?

2. Прочитайте текст и напишите ответ.

Как называется процедура проверки подлинности заявленного пользователя, процесса или устройства?

3. Прочитайте текст и напишите ответ.

Как называется процедура предоставления субъекту определенных прав доступа к ресурсам системы?

4. Прочитайте текст и напишите ответ.

Какие СЗИ выявляют и соответствующим образом реагируют на средства несанкционированного уничтожения, блокирования, модификации, или нейтрализации СЗИ?

5. Прочитайте текст и напишите ответ.

Сколько классов защищенности межсетевых экранов по уровням контроля межсетевых информационных потоков определено ФСТЭК?

6. Прочитайте текст и напишите ответ.

Сколько уровней защиты содержит классификация межсетевых экранов по классам защиты?

7. Прочитайте текст и напишите ответ.

Какие типы межсетевых экранов определены ФСТЭК России?

8. Прочитайте текст и напишите ответ.

Где устанавливаются межсетевые экраны типа «А»?

9. Прочитайте текст и напишите ответ.

Где устанавливаются межсетевые экраны типа «Б»?

10. Прочитайте текст и напишите ответ.

Где устанавливаются межсетевые экраны типа «В»?

11. Прочитайте текст и напишите ответ.

Какого типа межсетевые экраны осуществляют разбор http(s)-трафика между веб-сервером и клиентом, и где они устанавливаются?

12. Прочитайте текст и напишите ответ.

Где подключается система обнаружения вторжений уровня сети и что она контролирует?

13. Прочитайте текст и напишите ответ.

Где устанавливается система обнаружения вторжений уровня узла и что она анализирует?

14. Прочитайте текст и напишите ответ.

Какие типы средств антивирусной защиты выделено ФСТЭК?

15. Прочитайте текст и напишите ответ.

Какие типы средств доверенной загрузки выделено ФСТЭК?

16. Прочитайте текст и напишите ответ.

Когда возникает ситуация, требующая несколько уровней межсетевых экранов?

17. Прочитайте текст и напишите ответ.

При каком методе идентификации пользователя первый рубеж - это логин и пароль, второй - специальный код, приходящий по электронной почте?

18. Прочитайте текст и напишите ответ.

Какие типы средств контроля съемных машинных носителей информации выделяются ФСТЭК?

19. Прочитайте текст и напишите ответ.

Какие различают типы операционных систем, используемых в целях обеспечения защиты информации?

20. Прочитайте текст и напишите ответ.

На какие средства вычислительной техники устанавливаются операционные системы типа «А»?

21. Прочитайте текст и напишите ответ.

На какие средства вычислительной техник устанавливаются операционные системы типа «Б»?

22. Прочитайте текст и напишите ответ.

Для каких целей предназначены операционные системы типа «В»?

23. Прочитайте текст и напишите ответ.

Как называют совокупность технических средств, направленных на контроль входа и выхода в помещение с целью обеспечения безопасности и регулирования посещений объекта?

24. Прочитайте текст и напишите ответ.

При использовании какой модели разграничения доступа указываются полномочия субъекта относительно каждого объекта или сегмента информации?

25. Прочитайте текст и напишите ответ.

При использовании какой модели разграничения доступа субъект имеет право на чтение только тех объектов, уровень конфиденциальности которых не выше его уровня?

Проверяемые результаты обучения – ПК 3.2

26. Прочитайте текст и напишите ответ.

Какой стандарт системы аутентификации предоставляет пользователю возможность создания единой учётной записи для аутентификации на множестве интернет-ресурсов, используя услуги третьих лиц?

27. Прочитайте текст и напишите ответ.

Какой пароль действителен только для одного сеанса аутентификации, действие этого пароля может быть ограничено определённым промежутком времени?

28. Прочитайте текст и напишите ответ.

Как называют технологию однократного ввода учетных данных для доступа к нескольким системам/приложениям?

29. Прочитайте текст и напишите ответ.

Какая технология позволяет не только проверять устройства и пользователей на подступах к ресурсам корпоративной сети, но и предотвращать доступ устройств, не соответствующих политике безопасности?

30. Прочитайте текст и напишите ответ.

Какое средство унифицированного управления угрозами обеспечивает комплексную защиту от сетевых угроз и объединяет в себе множество функций, связанных с обеспечением сетевой безопасности?

31. Прочитайте текст и напишите ответ.

Как называется процесс оценки подозрительных действий в защищаемой сети, который реализуется либо с помощью анализа журналов регистрации ОС и приложений, либо с помощью анализа сетевого трафика?

32. Прочитайте текст и напишите ответ.

Какие программные или аппаратные системы сетевой и компьютерной безопасности обнаруживают вторжения или нарушения безопасности и автоматически защищают от них?

33. Прочитайте текст и напишите ответ.

Какие основные группы задач решает шлюз web-безопасности класса SWG?

34. Прочитайте текст и напишите ответ.

Какова главная задача криптошлюза в сети передачи данных?

35. Прочитайте текст и напишите ответ.

Какие архитектурные способы установки криптошлюзов в сети являются основными?

36. Прочитайте текст и напишите ответ.

К каким средствам защиты информации относится криптошлюз?

37. Прочитайте текст и напишите ответ.

На каких объектах необходимо использовать криптошлюзы по требованиям регуляторов?

38. Прочитайте текст и напишите ответ.

Какие функции помимо шифрования передаваемого трафика между узлами выполняет криптошлюз?

39. Прочитайте текст и напишите ответ.

Для каких целей предназначена система мониторинга событий ИБ?

40. Прочитайте текст и напишите ответ.

Из каких источников данных собирает информацию система мониторинга событий ИБ?

41. Прочитайте текст и напишите ответ.

Как называют процесс проверки всех событий безопасности, получаемых от антивирусных систем, журналов ОС, сканеров анализа защищенности инфраструктуры, сетевого оборудования?

42. Прочитайте текст и напишите ответ.

Какие шпионские программы передают злоумышленнику данные о местоположении устройства, открываемых веб-сайтах, документах, списках контактов, маршруте передвижения, наиболее часто посещаемых местах?

43. Прочитайте текст и напишите ответ.

Как называют устройство или программное обеспечение для перехвата данных, вводимых с клавиатуры?

44. Прочитайте текст и напишите ответ.

Какие программы используются для удаленного управления рабочими станциями, выполнения почти любых действий с удаленной системой: передача файлов, наблюдение за действиями пользователя, настройка системы?

45. Прочитайте текст и напишите ответ.

Какие СЗИ работают внутри периметра безопасности, анализируют учётные записи, права, файлы, их содержимое, доступы и перемещения, выявляют нарушения и исправляют проблемы с хранением данных в компании?

46. Прочитайте текст и напишите ответ.

Сотрудники компании, неискушенные в теме информационной безопасности, зачастую могут путать DoS-атаки и DDoS-атаки. Объясните, в чем отличия этих атак?

47. Прочитайте текст и напишите ответ.

Какие программные и аппаратные средства используются для обнаружения неавторизованного входа в систему, а также несанкционированных попыток по управлению защищаемой сетью?

48. Прочитайте текст и напишите ответ.

Как называют единицу информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа?

49. Прочитайте текст и напишите ответ.

Какая учетная запись имеет больше прав, чем стандартная учетная запись и объем прав таких записей различается в зависимости от организации, должностных обязанностей и используемых технологий?

50. Прочитайте текст и напишите ответ.

Какая модель описывает потенциального нарушителя безопасности и подходы по определению актуальности угроз и вероятности их наступления с учетом возможностей потенциального нарушителя?

Проверяемые результаты обучения – ПК 3.3

51. Прочитайте текст и напишите ответ.

Какая целевая продолжительная высокоуровневая атака проводится группировкой профессиональных киберпреступников, зачастую действующих в интересах какого-либо государства?

52. Прочитайте текст и напишите ответ.

Какой сетевой протокол прикладного уровня служит для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия?

53. Прочитайте текст и напишите ответ.

Как называют файлы с записями о событиях в хронологическом порядке?

54. Прочитайте текст и напишите ответ.

Как называют технологию поиска, аккумулирования и анализа данных, собранных из доступных источников в интернете?

55. Прочитайте текст и напишите ответ.

Какие средства защиты устанавливают между общедоступной сетью (такой, как Internet) и внутренней?

56. Прочитайте текст и напишите ответ.

Какую функцию выполняет межсетевой экран?

57. Прочитайте текст и напишите ответ.

Для чего нужно контролировать и регулировать доступ пользователей внутренней сети к ресурсам общедоступной сети?

58. Прочитайте текст и напишите ответ.

На какие группы можно разделить все межсетевые экраны по способу их реализации?

59. Прочитайте текст и напишите ответ.

Какая VPN защищает данные, передаваемые между узлами корпоративной сети (но не сетями) и обычно реализуется для узлов, находящихся в одном сетевом сегменте?

60. Прочитайте текст и напишите ответ.

Что такое Next-generation firewall (NGFW)?

61. Прочитайте текст и напишите ответ.

Для каких целей используются прокси-серверы?

62. Прочитайте текст и напишите ответ.

Для каких целей используются средства или модули доверенной загрузки (СДЗ или МДЗ)?

63. Прочитайте текст и напишите ответ.

Для чего используют сканеры уязвимостей?

64. Прочитайте текст и напишите ответ.

Для чего используют системы защиты от утечек информации (DLP)?

65. Прочитайте текст и напишите ответ.

Что такое SIEM системы?

66. Прочитайте текст и напишите ответ.

Кто является оператором персональных данных (ПДн)?

67. Прочитайте текст и напишите ответ.

Кто является субъектом персональных данных (ПДн)?

68. Прочитайте текст и напишите ответ.

На какие категории делятся персональные данные?

69. Прочитайте текст и напишите ответ.

Какие данные относятся к биометрическим персональным данным?

70. Прочитайте текст и напишите ответ.

Какие данные относятся к специальным персональным данным?

71. Прочитайте текст и напишите ответ.

Какие данные относятся к общедоступным персональным данным?

72. Прочитайте текст и напишите ответ.

Какие данные относятся к иным персональным данным?

73. Прочитайте текст и напишите ответ.

Какие типы актуальных угроз учитываются при работе с ИСПДн?

74. Прочитайте текст и напишите ответ.

Для чего проводят аудит информационной безопасности?

75. Прочитайте текст и напишите ответ.

Являются ли равнозначными понятиями служебная и профессиональная тайна?

Тестовое задание закрытого типа для дифференцированного зачета
по МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания

Блок заданий 2 (8 семестр) закрытого типа

Проверяемые результаты обучения – ПК 3.1		
1.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к способам несанкционированного доступа к защищаемой информации?	1.Инициативное сотрудничество. 2.Опосредованный контакт. 3.Выведывание 4.Подделка.
4.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к физическим средствам защиты информации?	1.Стены. 2. Средства защищенного доступа. 3. Заграждения. 4. Аппаратные межсетевые экраны.
6.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к физическим средствам защиты информации?	1. Аппаратные межсетевые экраны. 2. Системы обнаружения вторжений. 3. Устройства хранения. 4. Электромеханические замки.
7.	Прочитайте текст и выберите несколько правильных ответов. 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 целостости программно-аппаратной среды.
8.	Прочитайте текст и выберите несколько правильных ответов. Какие задачи решает система физической защиты информации?	1. Обеспечение целостости 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.	Прочитайте текст и выберите несколько правильных ответов. Какие объекты из перечисленных являются объектами защиты при обеспечении информационной безопасности?	1. Устройства хранения данных. 2. Информация. 3. Ресурсные объекты. 4. Физические объекты. 5. Устройства передачи данных.

10.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Какие методы используются для	1.Выбор ответственного за безопасность лица. 2.Аутентификация. 3.Регламентирование доступа к объектам.

	обеспечения защиты данных, хранящихся и передающихся техническими средствами?	4.Использование средств антивирусной защиты.
19.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Какие механизмы безопасности из перечисленных используются для защиты данных в информационных системах?	1.Персонализация. 2.Авторизация. 3.Верификация. 4.Регламентация. 5.Превентизация.
22.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного является косвенными каналами утечки информации?	1. Утечка данных из-за несоблюдения режима коммерческой тайны. 2.Пропажа, кража или утеря информационного накопителя, исследование неудаленной корзины. 3.Прослушивание, дистанционные снимки. 4.Перехват электромагнитных устройств. 5.Непосредственное копирование данных.

27.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. При каких режимах обработки информации средствами вычислительной техники возникают побочные электромагнитные излучения?	1. Запись данных от СУБД. 2. Чтение информации с накопителей. 3. Ввод данных с электронной почты. 4. Запись данных от сканера на магнитный носитель.
29.	Прочитайте текст и выберите несколько правильных ответов. Где могут возникать наводки информативных сигналов?	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.
Проверяемые результаты обучения – ПК 3.2		
30.	Прочитайте текст и выберите несколько правильных ответов. Каким образом создаются возможные каналы утечки информации?	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.	Прочитайте текст и выберите один правильный ответ. Как создаются возможные каналы утечки информации?	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.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	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.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к электромагнитным каналам утечки информации (КУИ)?	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.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к электрическим каналам утечки информации (КУИ)?	1. Съем информационных сигналов с линий электропитания ТСПИ. 2. Съем информационных сигналов с цепей заземления ТСПИ и ВТСС. 3. Съем информации путем установки в ТСПИ электронных устройств перехвата информации.

		4. Перехват информационных сигналов на частотах самовозбуждения усилителей низкой частоты ТСПИ. 5. Съем информации на частотах работы высокочастотных генераторов в ТСПИ и ВТСС.
35.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к вспомогательным техническим средствам и системам (ВТСС)?	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.	Прочитайте текст и выберите один правильный ответ. Что из перечисленного относится к ТСПИ и ВТСС?	1. Задающие генераторы. 2. Генераторы тактовой частоты. 3. Генераторы стирания и подмагничивания магнитофонов. 4. Гетеродины радиоприемных и телевизионных устройств. 5. Все ответы верны.
37.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к основным техническим средствам и системам (ОТСС)?	1.Системы охранной и пожарной сигнализации. 2. Системы оперативно-командной связи. 3.Средства оповещения и сигнализации. 4.Системы видеозаписи и видеовоспроизведения. 5. Аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода.
38.	Прочитайте текст и выберите один правильный ответ. Что из перечисленного является примером прямого канала утечки данных?	1. Пропажа, кража информационного накопителя. 2. Прослушивание, дистанционные снимки. 3. Перехват электромагнитных устройств. 4. Работа инсайдеров.
39.	Прочитайте текст и выберите один правильный ответ. Какими способами рекомендуется бороться с утечкой персональных данных?	1. Использовать надежные пароли и настроить многофакторную аутентификацию. 2. Своевременно обновлять программное обеспечение. 3. Регулярно создавать резервные копии данных. 4. Обновить адресную книгу электронной почты. 5.Все ответы верны.
40.	Прочитайте текст и выберите несколько правильных ответов. Какими способами обеспечивается защита информации от утечки по электромагнитным каналам?	1. Фильтрация ПЭМИ на частотах работы высокочастотных генераторов в ТСПИ и ВТСС. 2.Фильтрация в цепях заземления и питания. 3.Ослабление связей между элементами. 4. Экранирование элементов и узлов оборудования.
41.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относят к пассивным техническим способам защиты?	1.Установка комплексных систем защиты от несанкционированнного доступа на ТСПИ и кабельные линии связи. 2. Установка систем гарантированного уничтожения информации. 3. Контроль радиоспектра и побочных электромагнитных излучений ТСПИ. 4.Звуко- и виброизоляция ВП и механических узлов ТСПИ.
42.	Прочитайте текст и выберите несколько правильных ответов. Какие каналы утечки информации выявляются в процессе поисковых мероприятий?	1.Каналы, обрабатываемые ТСПИ. 2.Каналы речевой информации. 3.Каналы визуально-графической информации. 4.Каналы видовой информации. 5.Каналы цифровой информации.
43.	Прочитайте текст и выберите один правильный ответ. Какими способами в ходе специальной проверки осуществляется выявление закладных устройств?	1.Контроль радиоспектра и побочных электромагнитных излучений ТСПИ. 2.Выявление с помощью индикаторов электромагнитного поля, интерсепторов, частотомеров, сканеров негласно установленных подслушивающих приборов. 3.Специальная проверка с использованием нелинейных

		локаторов и мобильных рентгеновских установок. 4.Все ответы верны.
44.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относят к пассивным техническим способам защиты информации?	1. Фильтрация ПЭМИ на частотах работы высокочастотных генераторов в ТСПИ и ВТСС. 2.Экранирование ВП, ТСПИ и отходящих от них соединительных линий. 3.Заземление ТСПИ и экранов соединительных линий приборов. 4.Установка систем гарантированного уничтожения информации.
45.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относят к пассивным техническим способам защиты?	1.Встраивание в ВТСС, обладающих “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 2.Акустическое и вибрационное зашумление строительных конструкций. 3.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения). 4.Монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров.
46.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относят к пассивным техническим способам защиты?	1.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения). 2.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор. 3.Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ. 4.Акустическое и вибрационное зашумление строительных конструкций.
47.	Прочитайте текст и выберите несколько правильных ответов. Какими методами из перечисленных осуществляется активное воздействие на каналы утечки информации?	1.СВЧ - воздействие на микрофонные цепи (подавления диктофонов устройствами направленного высокочастотного радиоизлучения). 2.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 3.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор. 4.Зашумление каналов передачи данных.
48.	Прочитайте текст и выберите несколько правильных ответов. Какими методами осуществляется активное воздействие на каналы утечки информации?	1.Встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 2.Пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ. 3.Акустическое и вибрационное зашумление строительных конструкций. 4. Установка автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ.
49.	Прочитайте текст и выберите несколько правильных ответов. Какими способами осуществляется активное воздействие на каналы утечки информации?	1.Зашумления силовой сети и цепей заземления. 2.Установка систем гарантированного уничтожения информации. 3.Шифрование информации, передаваемой по каналам связи. 4.Монтаж в цепях электропитания ТСПИ, а также в электросетях ВП помехоподавляющих фильтров.
50.	Прочитайте текст и выберите один правильный ответ. Какие методы защиты информации	1.Пароли для авторизации во время работы. 2.Модули доверенной загрузки. 3.Криптографические средства шифрования

	могут быть использованы для предотвращения несанкционированного доступа?	информации для ее передачи и хранения. 4.Средства предотвращения сетевых атак (межсетевой экран, антивирус, прокси-сервер). 5.Все ответы верны.
51.	Прочитайте текст и выберите несколько правильных ответов. Какие компоненты включает в себя комплекс радиолокационной системы?	1. Модули доверенной загрузки. 2.Система периметрального наблюдения, состоящая из камер и тепловизоров. 3.Инфракрасные и вибрационные извещатели. 4.Радиолокатор. 5.Рабочее операторское место.
52.	Прочитайте текст и выберите один правильный ответ. 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.
53.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного является основными закономерностями распространения радиоволн, которые позволяют обнаруживать объекты и измерять координаты и параметры их движения?	1.Постоянство скорости и прямолинейность распространения радиоволн в однородной среде. 2.Способность радиоволн отражаться от различных областей пространства, электрические или магнитные параметры которых отличаются от аналогичных параметров среды распространения. 3. Изменение скорости принимаемого сигнала. 4. Изменение частоты принимаемого сигнала по отношению к частоте излученного сигнала при относительном движении источника излучения и приемника радиолокационного сигнала.
54.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к организационно-режимным мероприятиям по защите информации на объекте?	1.Определение границ контролируемой зоны (КЗ) вокруг объекта и обеспечение режимного ограничения доступа на объекты размещения ТСПИ и в выделенные помещения (ВП). 2.Контроль радиоспектра и побочных электромагнитных излучений ТСПИ. 3.Введение частотных, энергетических, временных и пространственных ограничений в режимы работы технических средств приема, обработки, хранения и передачи информации (ТСПИ). 4.Специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием мобильных рентгеновских установок. 5.Отключение на период проведения закрытых совещаний вспомогательных технических средств и систем (ВТСС), обладающих качествами электроакустических преобразователей от соединительных линий.
55.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного относится к организационно-режимным мероприятиям по защите информации на объекте?	1.Использование только сертифицированных ТСПИ и ВТСС. 2.Специальная проверка выделенных помещений, ТСПИ и ВТСС с использованием нелинейных локаторов и мобильных рентгеновских установок. 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.

		4.Контроль радиоспектра и побочных электромагнитных излучений ТСПИ. 5.Категорирование и аттестование объектов информатизации и выделенных помещений на соответствие требованиям обеспечения ЗИ при проведении работ со сведениями различной степени секретности.
56.	Прочитайте текст и выберите несколько правильных ответов. На какие виды можно разделить методы и способы защиты информации от утечки по ТКУИ в зависимости от целей, порядка проведения и применяемого оборудования?	1.Организационно-режимные. 2.Правовые. 3.Поисковые (выявление возможных ТКУИ). 4.Программные. 3. Технические.
57.	Прочитайте текст и выберите несколько правильных ответов. Какие каналы утечки информации выявляются в процессе поисковых мероприятий?	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.	Прочитайте текст и выберите несколько правильных ответов. Какие мероприятия из перечисленных выполняются в ходе специальной проверки?	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.
Проверяемые результаты обучения – ПК 3.3		
59.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных защитных приемов и средств относятся к пассивным техническим способам защиты?	1.Акустическое и вибрационное зашумление строительных конструкций. 2.Установка комплексных систем защиты от несанкционированнного 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.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных защитных приемов и средств относятся к пассивным техническим способам защиты?	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.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных защитных приемов и средств относятся к пассивным техническим способам защиты?	1.Использование специальных конструкций оконных блоков, специальных пленок, жалюзи и штор. 2. 6.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.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных защитных приемов и средств относят к активному воздействию на каналы утечки информации?	1.Пространственное электромагнитное зашумление ЗУ и ПЭМИН ТСПИ. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. Какие из перечисленных защитных приемов и средств относят к активному воздействию на каналы утечки информации?	1.Установка комплексных систем защиты от несанкционированнного 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. Сколько классов криптографических средств защиты информации определено ФСБ России?	1.Шесть классов. 2.Пять классов. 3.Семь классов. 4.Четыре класса.
71.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите один правильный ответ.	1. КС1. 2. КС2.

	К какому классу криптографических СЗИ относятся средства, защищающие от атак, при реализации которых привлекались специалисты в области использования НДВ системного программного обеспечения?	3. КС3. 4. КВ. 5. КА.
76.	Прочитайте текст и выберите несколько правильных ответов. Какие бывают наземные РЛС?	1.Статические. 2.Надгоризонтные. 3.Загоризонтные. 4.Подповерхностные. 5.Надповерхностные
77.	Прочитайте текст и выберите один правильный ответ. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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.	Прочитайте текст и выберите несколько правильных ответов. 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” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров. 4. Организация режима и контроля доступа в защищаемые помещения. 5. Все ответы верны.
81.	Прочитайте текст и выберите несколько правильных ответов. В чем разница между информационной безопасностью и кибербезопасностью?	1.Информационная безопасность направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) и места хранения. 2.Кибербезопасность направлена на защиту цифровых данных от компрометации или атак. 3.Кибербезопасность направлена на защиту всех данных организации независимо от их типа (цифровые или аналоговые) от компрометации или атак. 4.Информационная безопасность направлена на защиту цифровых данных от компрометации или атак.
82.	Прочитайте текст и выберите один правильный ответ. Что представляют собой угрозы типа APT (advanced persistent threat)?	1.Программы-вымогатели, которые получают доступ к файлам или системам и блокируют их для получения выкупа. 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. 3.Практика манипулирования людьми с целью заставить

		их раскрыть чувствительную конфиденциальную информацию для получения денежной выгоды или доступа к данным.
83.	Прочитайте текст и выберите один правильный ответ. Какие бывают типы угроз кибербезопасности?	1.Атаки на основе социальной инженерии. 2.Атаки при помощи вредоносного ПО. 3.Атаки на Интернет вещей (IoT). 4.Атаки типа «отказ в обслуживании» (DoS). 5.Все ответы верны.
84.	Прочитайте текст и выберите несколько правильных ответов. Что из перечисленного является организационными методами защиты информации?	1.Разработка и внедрение регламентов по обработке сведений внутри организации. 2.Регулярное создание бэкапов наиболее важных и ценных информационных массивов. 3.Проведение инструктажа персонала по основам кибербезопасности и правилам работы с информацией. 4.Выполнение резервирования, дублирования вспомогательных компонентов информационной системы, которые связаны с хранением информации.
85.	Прочитайте текст и выберите один правильный ответ. Какие преимущества позволяет получить проведение аудита информационной безопасности?	1.Выявление уязвимостей и возможных угроз безопасности, что позволяет принять меры по обеспечению безопасности информационных систем. 2.Оценка эффективности системы защиты информации и выявление ее недостатков. 3.Проверка соответствия системы защиты информации законодательству и стандартам безопасности. 4.Улучшение имиджа компании. 5.Все ответы верны.

Вопросы задания открытого типа для дифференцированного зачета
по МДК.03.01 Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания
Блок заданий 2 (8 семестр)
Проверяемые результаты обучения – ПК 3.1

1. Прочитайте текст и напишите ответ.

Что является объектом защиты информации?

2. Прочитайте текст и напишите ответ.

Как называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, и помещений, в которых они установлены?

3. Прочитайте текст и напишите ответ.

Что понимается под защищаемыми помещениями (ЗП)?

4. Прочитайте текст и напишите ответ.

Что такое автоматизированная система (АС)?

5. Прочитайте текст и напишите ответ.

Что такое контролируемая зона (КЗ)?

6. Прочитайте текст и напишите ответ.

Что такое специальные исследования (СИ)?

7. Прочитайте текст и напишите ответ.

Что такое специальная проверка (СП)?

8. Прочитайте текст и напишите ответ.

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. Прочитайте текст и напишите ответ.

Что такое аттестация объекта защиты?

10. Прочитайте текст и напишите ответ.

Как называют неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации?

11. Прочитайте текст и напишите ответ.

Как называются технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации?

12. Прочитайте текст и напишите ответ.

Что относится к основным техническим средствам и системам (ОТСС)?

13. Прочитайте текст и напишите ответ.

Как называются технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с ОТСС или в защищаемых помещениях?

14. Прочитайте текст и напишите ответ.

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. Прочитайте текст и напишите ответ.

Что понимают под техническим каналом утечки информации?

16. Прочитайте текст и напишите ответ.

Что такое тестовый сигнал?

17. Прочитайте текст и напишите ответ.

Как называют установление нормативными документами численных значений показателей защищенности информации?

18. Прочитайте текст и напишите ответ.

Что является целью аттестации объекта информатизации?

19. Прочитайте текст и напишите ответ.

Какой криптографический протокол обеспечивает защищённую передачу данных между узлами в сети Интернет?

20. Прочитайте текст и напишите ответ.

Каковы основные функции протокола TLS?

21. Прочитайте текст и напишите ответ.

Какие программные или программно-аппаратные средства обеспечивают охрану данных от возможной утечки внутри компании?

22. Прочитайте текст и напишите ответ.

Какие программные или программно-аппаратные средства, позволяют осуществлять запуск операционной системы исключительно с доверенных носителей информации (например, жестких дисков)?

23. Прочитайте текст и напишите ответ.

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. Прочитайте текст и напишите ответ.

Какие средства безопасности предназначены для анализа защищенности информации в корпоративных сетях и могут выполнять проверку установленных patch'ей системы безопасности ОС?

25. Прочитайте текст и напишите ответ.

Как называют сетевые шлюзы безопасности, состоящие из шлюзового антивируса; механизма блокировки сайтов по их содержимому, категории или конкретному адресу; VPN; IPS/IDS и др.?

Проверяемые результаты обучения – ПК 3.2

26. Прочитайте текст и напишите ответ.

Какая система безопасности защищает от воздействия внешних злоумышленников на компьютерную сеть, а именно от DoS-атак, сетевого сканирования, работы ботнетов и спам-сетей?

27. Прочитайте текст и напишите ответ.

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

28. Прочитайте текст и напишите ответ.

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

29. Прочитайте текст и напишите ответ.

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. Прочитайте текст и напишите ответ.

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

31. Прочитайте текст и напишите ответ.

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

32. Прочитайте текст и напишите ответ.

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

33. Прочитайте текст и напишите ответ.

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. Прочитайте текст и напишите ответ.

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

35. Прочитайте текст и напишите ответ.

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

36. Прочитайте текст и напишите ответ.

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

37. Прочитайте текст и напишите ответ.

Какие существуют виды инженерно технических средств безопасности?

38. Прочитайте текст и напишите ответ.

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

39. Прочитайте текст и напишите ответ.

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

40. Прочитайте текст и напишите ответ.

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. Прочитайте текст и напишите ответ.

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

42. Прочитайте текст и напишите ответ.

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

43. Прочитайте текст и напишите ответ.

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

44. Прочитайте текст и напишите ответ.

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

45. Прочитайте текст и напишите ответ.

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

46. Прочитайте текст и напишите ответ.

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

47. Прочитайте текст и напишите ответ.

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

48. Прочитайте текст и напишите ответ.

Какая модель доступа базируется на явно заданных для каждого субъекта (пользователя) правах доступа к объектам / сегментам информации?

49. Прочитайте текст и напишите ответ.

В какой модели доступа субъект имеет право на чтение только тех объектов, уровень конфиденциальности которых не выше его уровня?

50. Прочитайте текст и напишите ответ.

Какой криптографический сетевой протокол служит для безопасного управления сетевыми службами в незащищенной сети?

51. Прочитайте текст и напишите ответ.

Что является причиной возникновения акустического и виброакустического каналов утечки информации?

52. Прочитайте текст и напишите ответ.

Что такое комплексная система защиты информации?

53. Прочитайте текст и напишите ответ.

Что такое физическая защита информации?

54. Прочитайте текст и напишите ответ.

Что такое техническая защита информации?

55. Прочитайте текст и напишите ответ.

Какие компоненты входят в комплекс защиты охраняемых объектов?

56. Прочитайте текст и напишите ответ.

Как определить класс защищенности информационной системы?

Проверяемые результаты обучения – ПК 3.3

57. Прочитайте текст и напишите ответ.

Какие существуют способы организации утечки информации?

58. Прочитайте текст и напишите ответ.

Что такое технические каналы утечки информации (ТКУИ)?

59. Прочитайте текст и напишите ответ.

Как называют паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники?

60. Прочитайте текст и напишите ответ.

Каким образом классифицируются каналы утечки информации?

61. Прочитайте текст и напишите ответ.

Что входит в структуру канала утечки информации?

62. Прочитайте текст и напишите ответ.

Каковы основные причины утечки данных?

63. Прочитайте текст и напишите ответ.

Что такое защита информации от утечки?

64. Прочитайте текст и напишите ответ.

Какие проблемы решает DLP-система?

65. Прочитайте текст и напишите ответ.

Что называют каналом утечки речевой информации?

66. Прочитайте текст и напишите ответ.

Как классифицируются акустические каналы утечки информации?

67. Прочитайте текст и напишите ответ.

Какие существуют средства защиты акустической речевой информации от утечки по техническим каналам?

68. Прочитайте текст и напишите ответ.

Что такое закладные устройства?

69. Прочитайте текст и напишите ответ.

Какие технические средства применяют для выявления радиозакладных устройств (РЗУ)?

70. Прочитайте текст и напишите ответ.

Какие каналы утечки информации различают в зависимости от среды распространения?

71. Прочитайте текст и напишите ответ.

Какова дальность передачи информации при перехвате с использованием устройства типа «телефонное ухо» по радиоканалу при использовании сотового телефона в качестве закладного устройства?

72. Прочитайте текст и напишите ответ.

Что является носителем информации в электромагнитных каналах утечки информации?

73. Прочитайте текст и напишите ответ.

Что называют побочным электромагнитным излучением (ПЭМИ)?

74. Прочитайте текст и напишите ответ.

Как называются сигналы, представляющие собой высокочастотную несущую, модулированную информацией, обрабатываемой на СВТ (например, изображением, выводимым на экран монитора)?

75. Прочитайте текст и напишите ответ.

Как называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ?

76. Прочитайте текст и напишите ответ.

Какими способами можно перехватить речевую информацию по прямому акустическому каналу утечки?

77. Прочитайте текст и напишите ответ.

Какими способами можно перехватить речевую информацию по вибракустическому каналу утечки?

78. Прочитайте текст и напишите ответ.

Какими способами можно перехватить речевую информацию по прямому акустоэлетромагнитному каналу утечки?

79. Прочитайте текст и напишите ответ.

Какими способами можно перехватить речевую информацию по акустоэлектрическому каналу утечки?

80. Прочитайте текст и напишите ответ.

Какими способами можно перехватить речевую информацию по акустооптическому (лазерному) каналу утечки?

Составил преподаватель Е.М. Грубник