Министерство образования и науки Республики Дагестан
Государственное бюджетное профессиональное образовательное учреждение
Республики Дагестан
«Кизлярский профессионально-педагогический колледж»

СОГЛАСОВАНА С РАБОТОДАТЕЛЯМИ:
ООО «Оптимасеть»
наименование предприятия
директор
должность
Гусейнов С.А.
подпись (инициалы, фамилия)

УТВЕРЖДАЮ
заместитель директора по учебной работе
_____ Н.Шелкова
_____ 2022 г.

Комплект контрольно-оценочных средств

по профессиональному модулю

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

образовательной программы (ОП)

по специальности/

10.02.05 Обеспечение информационной безопасности автоматизированных систем

код, наименование

Рассмотрен и одобрен предметной (цикловой) комиссией профессиональных дисциплин технических специальностей
наименование по приказу

Председатель предметной (цикловой) комиссии

_____ / Раджабова А.Н.
подпись *расшифровка подписи*

29. 08 2022 г.

Кизляр, 2022 г.

Комплект контрольно-оценочных средств разработан на основе: Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем входящей в состав УГПС 10.00.00 Информационная безопасность рабочей программы ПМ 03. Защита информации техническими средствами.

Разработчик(и):

Искандырова Ажар Асадулаева
ФИО, должность, место работы

Раджабова Альбина Ниязовна
ФИО, должность, место работы

Рекомендована методическим советом ГБПОУ РД «Кизлярский профессионально-педагогический колледж» для применения в учебном процессе.

Заключение методического совета № 1 от 29 08 2022 г.

СОДЕРЖАНИЕ

Общие положения

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Защита информации техническими средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения основной образовательной программы в целом. Формой аттестации по профессиональному (квалификационный). Итогом экзамена является профессиональной деятельности освоен/не освоен». модулю является экзамен однозначное решение: Экзамен (квалификационный) проводится в форме выполнения практико-ориентированных заданий.

1. Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	**Форма контроля и оценивания**		
	Промежуточная аттестация	**Рубежный контроль**	**Текущий контроль**
МДК.03.01. Техническая защита информации	Дифференцированный зачет (6,7 семестр) Экзамен (8 семестр)	Тестирование Контрольная работа	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Тестирование; Контроль выполнения самостоятельной работы;
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	Дифференцированный зачет (6,7 семестр) Экзамен (8 семестр)	Тестирование	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Контроль выполнения самостоятельной работы;
УП. 03	Дифференцированный зачет (7 семестры)	------	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП 03	Дифференцированный зачет (8 семестр)	------	Оценка выполнения работ и оформления отчетной документации на производственной практике
Профессиональный модуль ПМ.03	Экзамен (квалификационный)		

2. Результаты освоения модуля, подлежащие проверке на экзамене (квалификационном)

В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Профессиональные и общие компетенции	Показатели оценки результата
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	распознает задачу и/или проблему в профессиональном контексте; анализирует задачу и/или проблему и выделяет её составные части; определяет этапы решения задачи; выявляет и осуществляет поиск информации, необходимой для

	решения задачи и/или проблемы; составляет план действия; определяет необходимые ресурсы; владеет актуальными методами работы в профессиональной и смежных сферах; реализует составленный план; оценивает результат и последствия своих действий, выделяет в нём сильные и слабые стороны
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	определяет задачи поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует получаемую информацию в соответствии с параметрами поиска; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; интерпретирует полученную информацию в контексте профессиональной деятельности; оформляет результаты поиска
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	использует актуальную нормативно-правовую документацию по специальности; применяет современную научно профессиональную терминологию; определяет актуальность нормативно-правовой документации в профессиональной деятельности; выстраивает траектории профессионального и личностного развития; участвует в конкурсах профессионального мастерства; участвует в мероприятиях профессиональной направленности (вебинары, семинары, конференции, круглые столы, форумы и т.д.)
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	участвует в деловом общении для эффективного решения деловых задач; планирует профессиональную деятельность; организует работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами;

	при групповом обсуждении задает вопросы для понимания идей других; при групповом обсуждении: убеждается, что коллеги по группе поняли предложенную идею; участвует в деятельности по выявлению ресурсов команды; анализирует работу членов группы; анализирует результаты выполненного задания; презентует результаты работы группы; защищает полученные командой результаты
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	грамотно (устно и письменно) излагает свои мысли по профессиональной тематике на государственном языке; проявляет толерантность в рабочем коллективе; извлекает из устной речи (монолог, диалог, дискуссия) нужную информацию и логические связи, организующие эту информацию; грамотно оформляет документы на государственном языке; корректно общается с преподавателями и одногруппниками; соблюдает заданный жанр высказывания (служебный доклад, выступление на совещании / собрании, презентация товара / услуг); корректно отвечает на вопросы, направленные на выяснение мнения (позиции); задает четко сформулированные вопросы, направленные на получение необходимой информации.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; понимать значимость своей специальности; демонстрирует поведение на основе общечеловеческих ценностей
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик участие в спортивных мероприятиях и/или мероприятиях направленных на формирование здорового образа жизни
ОК 09. Использовать информационные технологии в профессиональной деятельности	ориентируется в информационно-коммуникационных технологиях, применяемых в профессиональной деятельности; применяет средства информатизации и информационных технологий для реализации профессиональной деятельности; в профессиональной деятельности использует современное программное обеспечение; представляет информацию в различных формах с использованием разнообразного программного обеспечения; способен адаптироваться в новых программных продуктах.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); понимает тексты на базовые профессиональные темы; применяет в профессиональной деятельности инструкции на государственном и иностранном языке; строит простые высказывания о себе и о своей профессиональной деятельности; пишет простые связные сообщения на знакомые или интересующие профессиональные темы

2.1. Общие/профессиональные компетенции, проверяемые дополнительно:

ОК	Основные показатели результата	Дополнительные формы контроля		
		Портфо-лио	Курсовое проектирование	Промежуточная аттестация по практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к	выбранный способ решения задачи аргументирован; доказана оптимальность	-	+	-
различным контекстам	выбранного способа решения применительно к контексту тематики курсового проекта			
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	наличие дипломов, грамот и сертификатов участия в мероприятиях по специальности; наличие дипломов, грамот и сертификатов участия в мероприятиях по формированию SoftSkills; положительный отзыв руководителя производственной практики.	+	-	+
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	пояснительная записка оформлена грамотно на государственном языке; выдержан научный стиль изложения материала;	-	+	-
ОК 09. Использовать информационные технологии в профессиональной деятельности	в процессе подготовки пояснительной записки эффективно использовались различные офисные приложения для обработки текстовой, числовой информации; защита курсового проекта осуществлялась с использованием презентационной графики.	-	+	-

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	~ список литературы содержит источники как на русском, так и на иностранных языках.	-	+	-

2.2. Требования к портфолио

Тип портфолио: смешанный.
Состав портфолио:
- ~ дипломы, грамоты и сертификаты участия в мероприятиях профессиональной направленности;
- ~ дипломы, грамоты и сертификаты участия в мероприятиях по формированию SoftSkills;
- ~ отзывы, характеристики с производственных практик;
- ~ разработанные проекты.

3. Оценка освоения профессионального модуля

3.1. Типовые задания для текущего контроля по **МДК.03.01. Техническая защита информации**

1)Вопросы для устного опроса по темам

Критерии оценки

«Отлично» ставится, если:
- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«Хорошо» ставится, если:
- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; -
изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«Удовлетворительно» ставится, если:
- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют некоторые нарушения;
- допущены несущественные ошибки в изложении теоретического материала и употреблении терминов;
- знания показаны слабо, речь неграмотная.

«Неудовлетворительно» ставится, если:
- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах); -

знания отсутствуют, речь неграмотная

Тема 1.1 Предмет и задачи технической защиты информации

1. Предмет и задачи технической защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности.
3. Системный подход при решении задач инженерно-технической защиты информации. 4. Основные параметры системы защиты информации.

Тема 1.2 Общие положения защиты информации техническими средствами

1. Задачи и требования к способам и средствам защиты информации техническими средствами.
2. Принципы системного анализа проблем инженерно-технической защиты информации. 3. Классификация способов и средств защиты информации.

Тема 2.1 Информация как предмет защиты
1. Особенности информации как предмета защиты. Свойства информации. 2. Виды, источники и носители защищаемой информации.
3. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
4. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.
5. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке

Тема 2.2 Технические каналы утечки информации 1. Понятие и особенности утечки информации.
2. Структура канала утечки информации.
3. Классификация существующих физических полей и технических каналов утечки информации.
4. Характеристика каналов утечки информации.
5. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.

Тема 2.3 Методы и средства технической разведки 1. Классификация технических средств разведки. 2. Методы и средства технической разведки.
3. Средства несанкционированного доступа к информации. 4. Средства и возможности оптической разведки.
5. Средства дистанционного съема информации.

Тема 3.1 Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок
1. Физические основы побочных электромагнитных излучений и наводок. 2. Акустоэлектрические преобразования.
3. Паразитная генерация радиоэлектронных средств. 4. Виды паразитных связей и наводок.
5. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
6. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей

Тема 3.2 Физические процессы при подавлении опасных сигналов 1. Скрытие речевой информации в каналах связи.

2. Подавление опасных сигналов акустоэлектрических преобразований. 3.
Экранирование.
4. Зашумление

Тема 4.1 Системы защиты от утечки информации по акустическому каналу 1.
Технические средства акустической разведки.
2. Непосредственное подслушивание звуковой информации.
3. Прослушивание информации направленными микрофонами. 4.
Система защиты от утечки по акустическому каналу.

5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу

Тема 4.2 Системы защиты от утечки информации по проводному каналу 1.
Принцип работы микрофона и телефона.
2. Использование коммуникаций в качестве соединительных проводов. 3.
Негласная запись информации на диктофоны.
4. Системы защиты от диктофонов.
5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.

Тема 4.3 Системы защиты от утечки информации по вибрационному каналу 1.
Электронные стетоскопы.
2. Лазерные системы подслушивания. 3.
Гидроакустические преобразователи.
4. Системы защиты информации от утечки по вибрационному каналу.
5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу

Тема 4.4 Системы защиты от утечки информации по электромагнитному каналу 1.
Прослушивание информации от радиотелефонов.
2. Прослушивание информации от работающей аппаратуры. 3.
Прослушивание информации от радиозакладок.
4. Приемники информации с радиозакладок.
5. Прослушивание информации о пассивных закладок.
6. Системы защиты от утечки по электромагнитному каналу.
7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу

Тема 4.5 Системы защиты от утечки информации по телефонному каналу 1.
Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
2. Использование микрофона телефонного аппарата при положенной телефонной трубке.
3. Утечка информации по сотовым цепям связи.
4. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.

Тема 4.6 Системы защиты от утечки информации по электросетевому каналу 1.
Низкочастотное устройство съема информации.
2. Высокочастотное устройство съема информации.
3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу

Тема 4.7 Системы защиты от утечки информации по оптическому каналу 1.

Телевизионные системы наблюдения.
2. Приборы ночного видения.
3. Системы защиты информации по оптическому каналу

Тема 5.1 Применение технических средств защиты информации
1. Технические средства для уничтожения информации и носителей информации, порядок применения.

2. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.
3. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.
4. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

Тема 5.2 Эксплуатация технических средств защиты информации 1.
Этапы эксплуатации технических средств защиты информации.
2. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.
3. Установка и настройка технических средств защиты информации.
4. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
5. Организация ремонта технических средств защиты информации. 6.
Проведение аттестации объектов информатизации

3.2. Типовые задания для рубежного контроля по **МДК.03.01. Техническая защита информации**

1)Типовая контрольная работа. Тема «Технические каналы утечки информации»

Задание. Ответить письменно на поставленные вопросы

Вариант 1
1. Задачи и требования к способам и средствам защиты информации техническими средствами.
2. Структура канала утечки информации.
3. Методы и средства технической разведки.

Вариант 2
1. Принципы системного анализа проблем инженерно-технической защиты информации. 2.
Характеристика каналов утечки информации.
3. Средства дистанционного съема информации.

Критерии оценки
Отметкой «отлично» оцениваются ответы, которые показывают прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, давать аргументированные ответы, приводить примеры. *Отметкой «хорошо»* оцениваются ответы, обнаруживающие прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение

терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, приводить примеры. Однако допускаются две-три неточности в ответах. *Отметкой «удовлетворительно»* оцениваются ответы, свидетельствующие в основном о знании материалов, их свойств, технологий, но отличающиеся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа тем изучаемой дисциплины, недостаточным умением давать аргументированные ответы и приводить примеры. Допускается несколько ошибок в содержании ответа.

Отметкой «неудовлетворительно» оцениваются ответы, обнаруживающие незнание материалов, их свойств, технологий изучаемой предметной области, отличающиеся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа тем изучаемой дисциплины; неумением давать аргументированные ответы. Допускаются серьезные ошибки в содержании ответов.

3.3. Типовые задания для промежуточного контроля по **МДК.03.01. Техническая защита информации**

1)Вопросы для подготовки к экзамену

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства 4.

Аппаратные средства 5.

Программные средства

6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля. 8.

Генераторы шума.

9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.
18. . Концепции инженерно-технической защиты информации. 19.

Системный подход к защите информации.

20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.
22. Направления инженерно-технической защиты информации.

23. Показатели эффективности инженерно-технической защиты информации. 24. Теоретические основы инженерно-технической защиты информации.
25. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений. 27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта. 31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок. 34. Распространение сигналов в технических каналах утечки информации. 35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты. 37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам. 40. Организационные основы инженерно-технической защиты информации. 41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.
44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации по оценке эффективности защиты информации.

3.5. Тестовое задание
по дисциплине МДК. 03.01 «Техническая защита информации»
I-аттестация

Вариант № 1

1. Какой вид разведки основан на использовании звуковых волн?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

2. В рамках какого процесса техническая разведка может проводиться?
a) сбор, обработка и анализ информации
b) разработка технических устройств для разведки
c) обучение разведывательных агентов
d) разработка программного обеспечения для разведки

3. Какую роль играет техническая разведка в современном мире?
a) обеспечение безопасности государства
b) развитие науки и технологий
c) повышение эффективности военных операций
d) все вышеперечисленное

4. Какой вид разведки использует методы дистанционного зондирования Земли?

a) радиоэлектронная разведка
b) оптическая разведка
c) акустическая разведка
d) радиационная разведка

5. Что такое техническая разведка?
a) процесс поиска и сбора информации о технических объектах и системах
b) метод получения конкурентной информации о компаниях
c) сфера деятельности специальных разведывательных служб
d) форма кибератак на информационные системы

6. Какие факторы могут повысить эффективность технической разведки?
a) использование специализированных технических средств
b) высококвалифицированный персонал
c) доступ к информационным системам и базам данных
d) все вышеперечисленное

7. Какие типы информации могут быть получены с помощью технической разведки?
a) информация о структуре и состоянии оборудования
b) информация о технологиях производства
c) информация о конкурентах и их активностях
d) все вышеперечисленное

8. Какие методы могут быть использованы при сборе информации с помощью технической разведки?
a) анализ открытых источников информации
b) применение технических средств наблюдения и подслушивания
c) использование социальной инженерии
d) все вышеперечисленное

9. Какова роль технической разведки в бизнесе?
a) обеспечение конкурентного преимущества
b) предотвращение утечек коммерческой информации
c) определение потенциальных уязвимостей в ИТ-инфраструктуре
d) все вышеперечисленное

10. Каковы основания классификации технической разведки по техническим характеристикам носителей информации?
a) Аппаратные основания
b) Программные основания
c) Сетевые основания
d) Коммуникационные основания

11. По какой физической природе носителей информации может быть классифицирована техническая разведка?
a) Электромеханическая техническая разведка
b) Электронная техническая разведка
c) Акустическая техническая разведка
d) Радиоволновая техническая разведка

12. Какие источники разведывательной информации могут использоваться при классификации технической разведки?
a) Внутренние источники
b) Внешние источники
c) Общедоступные источники
d) Скрытые источники

13. Какой уровень секретности может быть использован при классификации технической разведки?
a) Официальный уровень секретности
b) Особый уровень секретности
c) Секретный уровень секретности
d) Особо секретный уровень секретности

14. Какие меры безопасности могут быть применены для защиты от технической разведки?
a) Физическая защита помещений и оборудования
b) Контроль доступа к информационным ресурсам
c) Шифрование данных
d) Системы обнаружения вторжений

15. Какие последствия может иметь утечка конфиденциальной информации в результате технической разведки?
a) Потеря коммерческого преимущества
b) Репутационные и финансовые потери
c) Повреждение бизнес-партнерств
d) Потеря доверия клиентов

16. Какие методы сбора информации использует техническая разведка?
a) Пассивные методы сбора информации
b) Активные методы сбора информации
c) Сочетание пассивных и активных методов сбора информации
d) Методы социальной инженерии

17. Как осуществляется оценка уровня угрозы технической разведки?
a) Оценка степени вероятности исхода угрозы
b) Оценка потенциального вреда угрозы
c) Оценка возможности предотвращения угрозы
d) Совокупная оценка вероятности, вреда и возможности предотвращения угрозы

18. Какие факторы могут влиять на эффективность технической разведки?
a) Уровень квалификации персонала
b) Компетентность в области информационной безопасности
c) Использование современных технологий и методик
d) Реактивные меры безопасности

19. Какие организации занимаются противодействием технической разведке?
a) Службы безопасности государственных организаций

b) Компании по информационной безопасности
c) Разведывательные службы
d) Специализированные аналитические центры

20. Какие методы и средства относятся к технической разведке?
a) Физические основы утечки информации
b) Физические процессы при подавлении опасных сигналов
c) Методы и средства технической разведки
d) Наводки электромагнитных излучений

Вариант № 2

1. Какие методы сбора информации использует техническая разведка?
a. Пассивные методы сбора информации
b. Активные методы сбора информации
c. Сочетание пассивных и активных методов сбора информации
d. Методы социальной инженерии

2. Как осуществляется оценка уровня угрозы технической разведки?
a. Оценка степени вероятности исхода угрозы
b. Оценка потенциального вреда угрозы
c. Оценка возможности предотвращения угрозы
d. Совокупная оценка вероятности, вреда и возможности предотвращения угрозы

3. Какие факторы могут влиять на эффективность технической разведки?
a. Уровень квалификации персонала
b. Компетентность в области информационной безопасности
c. Использование современных технологий и методик
d. Реактивные меры безопасности

4. Какие организации занимаются противодействием технической разведке?
a. Службы безопасности государственных организаций
b. Компании по информационной безопасности
c. Разведывательные службы
d. Специализированные аналитические центры

5. Какие методы и средства относятся к технической разведке?
a. Физические основы утечки информации
b. Физические процессы при подавлении опасных сигналов
c. Методы и средства технической разведки
d. Наводки электромагнитных излучений

6. По какой физической природе носителей информации может быть классифицирована техническая разведка?
a. Электромеханическая техническая разведка
b. Электронная техническая разведка
c. Акустическая техническая разведка
d. Радиоволновая техническая разведка

7. Какие источники разведывательной информации могут использоваться при классификации технической разведки?
a. Внутренние источники
b. Внешние источники
c. Общедоступные источники
d. Скрытые источники

8. Какой уровень секретности может быть использован при классификации технической разведки?
a. Официальный уровень секретности
b. Особый уровень секретности
c. Секретный уровень секретности
d. Особо секретный уровень секретности

9. Какие меры безопасности могут быть применены для защиты от технической разведки?
a. Физическая защита помещений и оборудования
b. Контроль доступа к информационным ресурсам
c. Шифрование данных
d. Системы обнаружения вторжений

10. Какие последствия может иметь утечка конфиденциальной информации в результате технической разведки?
a. Потеря коммерческого преимущества
b. Репутационные и финансовые потери
c. Повреждение бизнес-партнерств
d. Потеря доверия клиентов

11. Какие факторы могут повысить эффективность технической разведки?
a. использование специализированных технических средств
b. высококвалифицированный персонал
c. доступ к информационным системам и базам данных
d. все вышеперечисленное

12. Какие типы информации могут быть получены с помощью технической разведки?
a. информация о структуре и состоянии оборудования
b. информация о технологиях производства
c. информация о конкурентах и их активностях
d. все вышеперечисленное

13. Какие методы могут быть использованы при сборе информации с помощью технической разведки?
a. анализ открытых источников информации
b. применение технических средств наблюдения и подслушивания
c. использование социальной инженерии
d. все вышеперечисленное

14. Какова роль технической разведки в бизнесе?

a. обеспечение конкурентного преимущества
b. предотвращение утечек коммерческой информации
c. определение потенциальных уязвимостей в ИТ-инфраструктуре
d. все вышеперечисленное
15. Каковы основания классификации технической разведки по техническим характеристикам носителей информации?
a. Аппаратные основания
b. Программные основания
c. Сетевые основания
d. Коммуникационные основания

16. Какой вид разведки основан на использовании звуковых волн?
a. оптическая разведка
b. радиоэлектронная разведка
c. акустическая разведка
d. химическая разведка

17. В рамках какого процесса техническая разведка может проводиться?
a. сбор, обработка и анализ информации
b. разработка технических устройств для разведки
c. обучение разведывательных агентов
d. разработка программного обеспечения для разведки

18. Какую роль играет техническая разведка в современном мире?
a. обеспечение безопасности государства
b. развитие науки и технологий
c. повышение эффективности военных операций
d. все вышеперечисленное

19. Какой вид разведки использует методы дистанционного зондирования Земли?
a. радиоэлектронная разведка
b. оптическая разведка
c. акустическая разведка
d. радиационная разведка

20. Что такое техническая разведка?
a. процесс поиска и сбора информации о технических объектах и системах
b. метод получения конкурентной информации о компаниях
c. сфера деятельности специальных разведывательных служб
d. форма кибератак на информационные системы

Вариант № 3

1. По какой физической природе носителей информации может быть классифицирована техническая разведка?
a. Электромеханическая техническая разведка
b. Электронная техническая разведка
c. Акустическая техническая разведка
d. Радиоволновая техническая разведка

2. Какие источники разведывательной информации могут использоваться при классификации технической разведки?
a. Внутренние источники
b. Внешние источники
c. Общедоступные источники
d. Скрытые источники

3. Какой уровень секретности может быть использован при классификации технической разведки?
a. Официальный уровень секретности
b. Особый уровень секретности
c. Секретный уровень секретности
d. Особо секретный уровень секретности

4. Какие меры безопасности могут быть применены для защиты от технической разведки?
a. Физическая защита помещений и оборудования
b. Контроль доступа к информационным ресурсам
c. Шифрование данных
d. Системы обнаружения вторжений

5. Какие последствия может иметь утечка конфиденциальной информации в результате технической разведки?
a. Потеря коммерческого преимущества
b. Репутационные и финансовые потери
c. Повреждение бизнес-партнерств
d. Потеря доверия клиентов

6. Какие методы сбора информации использует техническая разведка?
a. Пассивные методы сбора информации
b. Активные методы сбора информации
c. Сочетание пассивных и активных методов сбора информации
d. Методы социальной инженерии

7. Как осуществляется оценка уровня угрозы технической разведки?
a. Оценка степени вероятности исхода угрозы
b. Оценка потенциального вреда угрозы
c. Оценка возможности предотвращения угрозы
d. Совокупная оценка вероятности, вреда и возможности предотвращения угрозы

8. Какие факторы могут влиять на эффективность технической разведки?
a. Уровень квалификации персонала
b. Компетентность в области информационной безопасности
c. Использование современных технологий и методик
d. Реактивные меры безопасности

9. Какие организации занимаются противодействием технической разведке?
a. Службы безопасности государственных организаций
b. Компании по информационной безопасности

c. Разведывательные службы
d. Специализированные аналитические центры

10. Какие методы и средства относятся к технической разведке?
a. Физические основы утечки информации
b. Физические процессы при подавлении опасных сигналов
c. Методы и средства технической разведки
d. Наводки электромагнитных излучений

11. Какой вид разведки основан на использовании звуковых волн?
a. оптическая разведка
b. радиоэлектронная разведка
c. акустическая разведка
d. химическая разведка

12. В рамках какого процесса техническая разведка может проводиться?
a. сбор, обработка и анализ информации
b. разработка технических устройств для разведки
c. обучение разведывательных агентов
d. разработка программного обеспечения для разведки

13. Какую роль играет техническая разведка в современном мире?
a. обеспечение безопасности государства
b. развитие науки и технологий
c. повышение эффективности военных операций
d. все вышеперечисленное

14. Какой вид разведки использует методы дистанционного зондирования Земли?
a. радиоэлектронная разведка
b. оптическая разведка
c. акустическая разведка
d. радиационная разведка

15. Что такое техническая разведка?
a. процесс поиска и сбора информации о технических объектах и системах
b. метод получения конкурентной информации о компаниях
c. сфера деятельности специальных разведывательных служб
d. форма кибератак на информационные системы

16. Какие факторы могут повысить эффективность технической разведки?
a. использование специализированных технических средств
b. высококвалифицированный персонал
c. доступ к информационным системам и базам данных
d. все вышеперечисленное

17. Какие типы информации могут быть получены с помощью технической разведки?
a. информация о структуре и состоянии оборудования
b. информация о технологиях производства

c. информация о конкурентах и их активностях
d. все вышеперечисленное

18. Какие методы могут быть использованы при сборе информации с помощью технической разведки?
a. анализ открытых источников информации
b. применение технических средств наблюдения и подслушивания
c. использование социальной инженерии
d. все вышеперечисленное

19. Какова роль технической разведки в бизнесе?
a. обеспечение конкурентного преимущества
b. предотвращение утечек коммерческой информации
c. определение потенциальных уязвимостей в ИТ-инфраструктуре
d. все вышеперечисленное

20. Каковы основания классификации технической разведки по техническим характеристикам носителей информации?
a. Аппаратные основания
b. Программные основания
c. Сетевые основания
d. Коммуникационные основания

Вариант № 4

1. Какой вид разведки основан на использовании звуковых волн?
a. оптическая разведка
b. радиоэлектронная разведка
c. акустическая разведка
d. химическая разведка

2. В рамках какого процесса техническая разведка может проводиться?
a. сбор, обработка и анализ информации
b. разработка технических устройств для разведки
c. обучение разведывательных агентов
d. разработка программного обеспечения для разведки

3. Какую роль играет техническая разведка в современном мире?
a. обеспечение безопасности государства
b. развитие науки и технологий
c. повышение эффективности военных операций
d. все вышеперечисленное

4. Какой вид разведки использует методы дистанционного зондирования Земли?
a. радиоэлектронная разведка
b. оптическая разведка
c. акустическая разведка
d. радиационная разведка

5. Что такое техническая разведка?
a. процесс поиска и сбора информации о технических объектах и системах
b. метод получения конкурентной информации о компаниях
c. сфера деятельности специальных разведывательных служб
d. форма кибератак на информационные системы

6. По какой физической природе носителей информации может быть классифицирована техническая разведка?
a. Электромеханическая техническая разведка
b. Электронная техническая разведка
c. Акустическая техническая разведка
d. Радиоволновая техническая разведка

7. Какие источники разведывательной информации могут использоваться при классификации технической разведки?
a. Внутренние источники
b. Внешние источники
c. Общедоступные источники
d. Скрытые источники

8. Какой уровень секретности может быть использован при классификации технической разведки?
a. Официальный уровень секретности
b. Особый уровень секретности
c. Секретный уровень секретности
d. Особо секретный уровень секретности

9. Какие меры безопасности могут быть применены для защиты от технической разведки?
a. Физическая защита помещений и оборудования
b. Контроль доступа к информационным ресурсам
c. Шифрование данных
d. Системы обнаружения вторжений

10. Какие последствия может иметь утечка конфиденциальной информации в результате технической разведки?
a. Потеря коммерческого преимущества
b. Репутационные и финансовые потери
c. Повреждение бизнес-партнерств
d. Потеря доверия клиентов

11. Какие факторы могут повысить эффективность технической разведки?
a. использование специализированных технических средств
b. высококвалифицированный персонал
c. доступ к информационным системам и базам данных
d. все вышеперечисленное

12. Какие типы информации могут быть получены с помощью технической разведки?
a. информация о структуре и состоянии оборудования

b. информация о технологиях производства
c. информация о конкурентах и их активностях
d. все вышеперечисленное

13. Какие методы могут быть использованы при сборе информации с помощью технической разведки?
a. анализ открытых источников информации
b. применение технических средств наблюдения и подслушивания
c. использование социальной инженерии
d. все вышеперечисленное

14. Какова роль технической разведки в бизнесе?
a. обеспечение конкурентного преимущества
b. предотвращение утечек коммерческой информации
c. определение потенциальных уязвимостей в ИТ-инфраструктуре
d. все вышеперечисленное

15. Каковы основания классификации технической разведки по техническим характеристикам носителей информации?
a. Аппаратные основания
b. Программные основания
c. Сетевые основания
d. Коммуникационные основания

16. Какие методы сбора информации использует техническая разведка?
a. Пассивные методы сбора информации
b. Активные методы сбора информации
c. Сочетание пассивных и активных методов сбора информации
d. Методы социальной инженерии

17. Как осуществляется оценка уровня угрозы технической разведки?
a. Оценка степени вероятности исхода угрозы
b. Оценка потенциального вреда угрозы
c. Оценка возможности предотвращения угрозы
d. Совокупная оценка вероятности, вреда и возможности предотвращения угрозы

18. Какие факторы могут влиять на эффективность технической разведки?
a. Уровень квалификации персонала
b. Компетентность в области информационной безопасности
c. Использование современных технологий и методик
d. Реактивные меры безопасности

19. Какие организации занимаются противодействием технической разведке?
a. Службы безопасности государственных организаций
b. Компании по информационной безопасности
c. Разведывательные службы
d. Специализированные аналитические центры

20. Какие методы и средства относятся к технической разведке?

a. Физические основы утечки информации
b. Физические процессы при подавлении опасных сигналов
c. Методы и средства технической разведки
d. Наводки электромагнитных излучений

Ключи к тесту

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	d	d	a	a
2	b	b	a	d
3	a	a	c	a
4	a	a	b	c
5	d	d	d	b
6	a	a, b	d	a, b
7	a	a	d	a
8	b	a, c	d	a, c
9	d	b	a, c, d	b
10	a	a	a	a
11	d	a	a	a
12	d	a	a	d
13	d	b	b	d
14	b	a	a	d
15	d	d	d	b
16	d	a	d	d
17	d	d	b	b
18	a, c, d	a	a	a
19	a	c	a	a
20	d	b	d	d

Тестовое задание
по дисциплине МДК. 03.01 «Техническая защита информации»
II-аттестация

Вариант №1

1. Что такое техническая разведка?
a) Исследование физических закономерностей
b) Методы сбора и анализа информации
c) Управление вычислительными сетями
d) Обработка геофизических данных

2. Какие виды технической разведки относятся к оптической разведке?
a) Радиоэлектронная, акустическая
b) Оптическая, радиоэлектронная
c) Химическая, радиационная
d) Сейсмическая, магнитометрическая

3. Какой носитель информации используется в радиоэлектронной разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

4. Какое значение приобретают силы и средства, связанные с вычислительной техникой?
a) Бурное развитие радиоволновых технологий
b) Использование радиоактивных веществ в разведке
c) Подключение к вычислительным сетям для добычи информации
d) Улучшение качества акустической разведки

5. Какие классификационные признаки важны при анализе сил и средств, добывающих информацию из компьютеров и вычислительных сетей?
a) Физическая природа носителей информации
b) Виды носителей технических средств добывания
c) Магнитные характеристики носителей информации
d) Размер и форма технических устройств

6. Что становится самостоятельным значением в связи с развитием вычислительной техники?
a) Спутниковая связь
b) Силы и средства для добычи информации из компьютеров и сетей
c) Исследование подземных ресурсов
d) Изучение акустических особенностей воды

7. Какие виды носителей информации используются в химической разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

8. Какой носитель информации используется в радиационной разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Магнитное поле

9. Какой носитель информации используется в сейсмической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

10. Какой носитель информации используется в магнитометрической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

11. Какую информацию можно получить с помощью акустической разведки?
a) Радиоэлектронные сигналы
b) Звуковые волны

c) Оптический спектр
d) Магнитное поле

12. Какие методы используются для анализа электромагнитной разведки?
a) Радиолокация, тепловизионное наблюдение
b) Спектральный анализ, анализ формы и динамики сигналов
c) Инфракрасная тепловая разведка
d) Оптический спектральный анализ

13. Какие виды разведки относятся к тактической разведке?
a) Акустическая, радиоэлектронная, оптическая
b) Техническая, оперативная, стратегическая
c) Космическая, гидрографическая, оптическая
d) Наблюдение на местности, изучение карт черного рынка

14. Какие особенности имеет индустриальная разведка?
a) Исследование промышленного производства и технологий
b) Анализ политической обстановки
c) Географическое изучение районов
d) Наблюдение за поведением граждан

15. Какие виды технической разведки существуют, если классифицировать их по физической природе носителей информации?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) все вышеперечисленные

16. Какой вид разведки использует электромагнитное поле в видимом и инфракрасном диапазонах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

17. Какой вид разведки использует акустическую волну в газообразной, жидкой и твердых средах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

18. Какой вид разведки использует излучения радиоактивных веществ в качестве носителя информации?
a) радиоэлектронная разведка
b) радиационная разведка
c) магнитометрическая разведка
d) сейсмическая разведка

19. Какие основания классификации технической разведки наиболее широко применяются?
a) по техническим характеристикам носителей информации
b) по физической природе носителей информации
c) по источнику разведывательной информации
d) по уровню секретности информации

20. Какой вид технической разведки использует различные электромагнитные системы и устройства?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

Вариант № 2

1. Какой вид разведки использует электромагнитное поле в видимом и инфракрасном диапазонах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

2. Какой вид разведки использует акустическую волну в газообразной, жидкой и твердых средах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

3. Какой вид разведки использует излучения радиоактивных веществ в качестве носителя информации?
a) радиоэлектронная разведка
b) радиационная разведка
c) магнитометрическая разведка
d) сейсмическая разведка

4. Какие основания классификации технической разведки наиболее широко применяются?
a) по техническим характеристикам носителей информации
b) по физической природе носителей информации
c) по источнику разведывательной информации
d) по уровню секретности информации

5. Какой вид технической разведки использует различные электромагнитные системы и устройства?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка

d) химическая разведка

6. Какую информацию можно получить с помощью акустической разведки?
a) Радиоэлектронные сигналы
b) Звуковые волны
c) Оптический спектр
d) Магнитное поле

7. Какие методы используются для анализа электромагнитной разведки?
a) Радиолокация, тепловизионное наблюдение
b) Спектральный анализ, анализ формы и динамики сигналов
c) Инфракрасная тепловая разведка
d) Оптический спектральный анализ

8. Какие виды разведки относятся к тактической разведке?
a) Акустическая, радиоэлектронная, оптическая
b) Техническая, оперативная, стратегическая
c) Космическая, гидрографическая, оптическая
d) Наблюдение на местности, изучение карт черного рынка

9. Какие особенности имеет индустриальная разведка?
a) Исследование промышленного производства и технологий
b) Анализ политической обстановки
c) Географическое изучение районов
d) Наблюдение за поведением граждан

10. Какие виды технической разведки существуют, если классифицировать их по физической природе носителей информации?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) все вышеперечисленные

11. Что становится самостоятельным значением в связи с развитием вычислительной техники?
a) Спутниковая связь
b) Силы и средства для добычи информации из компьютеров и сетей
c) Исследование подземных ресурсов
d) Изучение акустических особенностей воды

12. Какие виды носителей информации используются в химической разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

13. Какой носитель информации используется в радиационной разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток

c) Акустическая волна в газообразной, жидкой и твердых средах
d) Магнитное поле

14. Какой носитель информации используется в сейсмической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

15. Какой носитель информации используется в магнитометрической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

16. Что такое техническая разведка?
a) Исследование физических закономерностей
b) Методы сбора и анализа информации
c) Управление вычислительными сетями
d) Обработка геофизических данных

17. Какие виды технической разведки относятся к оптической разведке?
a) Радиоэлектронная, акустическая
b) Оптическая, радиоэлектронная
c) Химическая, радиационная
d) Сейсмическая, магнитометрическая

18. Какой носитель информации используется в радиоэлектронной разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

19. Какое значение приобретают силы и средства, связанные с вычислительной техникой?
a) Бурное развитие радиоволновых технологий
b) Использование радиоактивных веществ в разведке
c) Подключение к вычислительным сетям для добычи информации
d) Улучшение качества акустической разведки

20. Какие классификационные признаки важны при анализе сил и средств, добывающих информацию из компьютеров и вычислительных сетей?
a) Физическая природа носителей информации
b) Виды носителей технических средств добывания
c) Магнитные характеристики носителей информации
d) Размер и форма технических устройств

Вариант № 3

1. Что становится самостоятельным значением в связи с развитием вычислительной техники?
a) Спутниковая связь
b) Силы и средства для добычи информации из компьютеров и сетей
c) Исследование подземных ресурсов
d) Изучение акустических особенностей воды

2. Какие виды носителей информации используются в химической разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

3. Какой носитель информации используется в радиационной разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Магнитное поле

4. Какой носитель информации используется в сейсмической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

5. Какой носитель информации используется в магнитометрической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

6. Какую информацию можно получить с помощью акустической разведки?
a) Радиоэлектронные сигналы
b) Звуковые волны
c) Оптический спектр
d) Магнитное поле

7. Какие методы используются для анализа электромагнитной разведки?
a) Радиолокация, тепловизионное наблюдение
b) Спектральный анализ, анализ формы и динамики сигналов
c) Инфракрасная тепловая разведка
d) Оптический спектральный анализ

8. Какие виды разведки относятся к тактической разведке?
a) Акустическая, радиоэлектронная, оптическая
b) Техническая, оперативная, стратегическая
c) Космическая, гидрографическая, оптическая
d) Наблюдение на местности, изучение карт черного рынка

9. Какие особенности имеет индустриальная разведка?
a) Исследование промышленного производства и технологий
b) Анализ политической обстановки
c) Географическое изучение районов
d) Наблюдение за поведением граждан

10. Какие виды технической разведки существуют, если классифицировать их по физической природе носителей информации?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) все вышеперечисленные

11. Какой вид разведки использует электромагнитное поле в видимом и инфракрасном диапазонах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

12. Какой вид разведки использует акустическую волну в газообразной, жидкой и твердых средах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

13. Какой вид разведки использует излучения радиоактивных веществ в качестве носителя информации?
a) радиоэлектронная разведка
b) радиационная разведка
c) магнитометрическая разведка
d) сейсмическая разведка

14. Какие основания классификации технической разведки наиболее широко применяются?
a) по техническим характеристикам носителей информации
b) по физической природе носителей информации
c) по источнику разведывательной информации
d) по уровню секретности информации
15. Какой вид технической разведки использует различные электромагнитные системы и устройства?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

16. Что такое техническая разведка?

a) Исследование физических закономерностей
b) Методы сбора и анализа информации
c) Управление вычислительными сетями
d) Обработка геофизических данных

17. Какие виды технической разведки относятся к оптической разведке?
a) Радиоэлектронная, акустическая
b) Оптическая, радиоэлектронная
c) Химическая, радиационная
d) Сейсмическая, магнитометрическая

18. Какой носитель информации используется в радиоэлектронной разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

19. Какое значение приобретают силы и средства, связанные с вычислительной техникой?
a) Бурное развитие радиоволновых технологий
b) Использование радиоактивных веществ в разведке
c) Подключение к вычислительным сетям для добычи информации
d) Улучшение качества акустической разведки

20. Какие классификационные признаки важны при анализе сил и средств, добывающих информацию из компьютеров и вычислительных сетей?
a) Физическая природа носителей информации
b) Виды носителей технических средств добывания
c) Магнитные характеристики носителей информации
d) Размер и форма технических устройств

Вариант № 4

1. Какой вид разведки использует электромагнитное поле в видимом и инфракрасном диапазонах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

2. Какой вид разведки использует акустическую волну в газообразной, жидкой и твердых средах?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

3. Какой вид разведки использует излучения радиоактивных веществ в качестве носителя информации?

a) радиоэлектронная разведка
b) радиационная разведка
c) магнитометрическая разведка
d) сейсмическая разведка

4. Какие основания классификации технической разведки наиболее широко применяются?
a) по техническим характеристикам носителей информации
b) по физической природе носителей информации
c) по источнику разведывательной информации
d) по уровню секретности информации

5. Какой вид технической разведки использует различные электромагнитные системы и устройства?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) химическая разведка

6. Что становится самостоятельным значением в связи с развитием вычислительной техники?
a) Спутниковая связь
b) Силы и средства для добычи информации из компьютеров и сетей
c) Исследование подземных ресурсов
d) Изучение акустических особенностей воды

7. Какие виды носителей информации используются в химической разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

8. Какой носитель информации используется в радиационной разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Магнитное поле

9. Какой носитель информации используется в сейсмической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

10. Какой носитель информации используется в магнитометрической разведке?
a) Излучения радиоактивных веществ
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в земной поверхности
d) Магнитное поле

11. Какую информацию можно получить с помощью акустической разведки?
a) Радиоэлектронные сигналы
b) Звуковые волны
c) Оптический спектр
d) Магнитное поле

12. Какие методы используются для анализа электромагнитной разведки?
a) Радиолокация, тепловизионное наблюдение
b) Спектральный анализ, анализ формы и динамики сигналов
c) Инфракрасная тепловая разведка
d) Оптический спектральный анализ

13. Какие виды разведки относятся к тактической разведке?
a) Акустическая, радиоэлектронная, оптическая
b) Техническая, оперативная, стратегическая
c) Космическая, гидрографическая, оптическая
d) Наблюдение на местности, изучение карт черного рынка

14. Какие особенности имеет индустриальная разведка?
a) Исследование промышленного производства и технологий
b) Анализ политической обстановки
c) Географическое изучение районов
d) Наблюдение за поведением граждан

15. Какие виды технической разведки существуют, если классифицировать их по физической природе носителей информации?
a) оптическая разведка
b) радиоэлектронная разведка
c) акустическая разведка
d) все вышеперечисленные

16. Что такое техническая разведка?
a) Исследование физических закономерностей
b) Методы сбора и анализа информации
c) Управление вычислительными сетями
d) Обработка геофизических данных

17. Какие виды технической разведки относятся к оптической разведке?
a) Радиоэлектронная, акустическая
b) Оптическая, радиоэлектронная
c) Химическая, радиационная
d) Сейсмическая, магнитометрическая

18. Какой носитель информации используется в радиоэлектронной разведке?
a) Электромагнитное поле в видимом и инфракрасном диапазонах
b) Электромагнитное поле в радиодиапазоне или электрический ток
c) Акустическая волна в газообразной, жидкой и твердых средах
d) Частицы вещества

19. Какое значение приобретают силы и средства, связанные с вычислительной техникой?
a) Бурное развитие радиоволновых технологий
b) Использование радиоактивных веществ в разведке
c) Подключение к вычислительным сетям для добычи информации
d) Улучшение качества акустической разведки

20. Какие классификационные признаки важны при анализе сил и средств, добывающих информацию из компьютеров и вычислительных сетей?
a) Физическая природа носителей информации
b) Виды носителей технических средств добывания
c) Магнитные характеристики носителей информации
d) Размер и форма технических устройств

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	b	a	b	a
2	b	c	d	c
3	b	b	a	b
4	c	b	c	b
5	b	b	d	b
6	b	b	b	b
7	d	b	b	d
8	a	a	a	a
9	c	a	a	c
10	d	d	d	d
11	b	b	a	b
12	b	d	c	b
13	a	a	b	a
14	a	c	b	a
15	d	d	b	d
16	a	b	b	b
17	c	b	b	b
18	b	b	b	b
19	b	c	c	c
20	b	b	b	b

3.6. Типовые задания для текущего контроля по **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации**:

1) Практические работы, представленные в методических указаниях по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

2)Вопросы для устного опроса по темам

«Отлично» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«Хорошо» ставится, если:
- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; -
изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«Удовлетворительно» ставится, если:
- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют некоторые нарушения;
- допущены несущественные ошибки в изложении теоретического материала и употреблении терминов;
- знания показаны слабо, речь неграмотная.

«Неудовлетворительно» ставится, если:
- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах); -
знания отсутствуют, речь неграмотная

Тема 1.1 Цели и задачи физической защиты объектов информатизации 1.
Характеристики потенциально опасных объектов.
2. Содержание и задачи физической защиты объектов информатизации.
3. Основные понятия инженерно-технических средств физической защиты. 4.
Категорирование объектов информатизации.
5. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.
6. Особенности задач охраны различных типов объектов.

Тема 1.2 Общие сведения о комплексах инженерно-технических средств физической защиты
1. Общие принципы обеспечения безопасности объектов. 2.
Жизненный цикл системы физической защиты.
3. Принципы построения интегрированных систем охраны. 4. Классификация и состав интегрированных систем охраны.
5. Требования к инженерным средствам физической защиты.
6. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты
1. Информационные основы построения системы охранной сигнализации. 2.
Назначение, классификация технических средств обнаружения.
3. Построение систем обеспечения безопасности объекта.
4. Периметровые средства обнаружения: назначение, устройство, принцип действия. 5.
Объектовые средства обнаружения: назначение, устройство, принцип действия.

Тема 2.2 Система контроля и управления доступом
1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.
2. Особенности построения и размещения СКУД. 3.

Структура и состав СКУД.
4. Периферийное оборудование и носители информации в СКУД.
5. Основы построения и принципы функционирования СКУД.
6. Классификация средств управления доступом.
7. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.
8. Обнаружение металлических предметов и радиоактивных веществ.

Тема 2.3 Система телевизионного наблюдения
1. Аналоговые и цифровые системы видеонаблюдения. 2.
Назначение системы телевизионного наблюдения.
3. Состав системы телевизионного наблюдения.
4. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.

Тема 2.4 Система сбора, обработки, отображения и документирования информации 1.
Классификация системы сбора и обработки информации.
2. Схема функционирования системы сбора и обработки информации.
3. Варианты структур построения системы сбора и обработки информации. 4.
Устройства отображения и документирования информации.

Тема 2.5 Система воздействия
1. Назначение и классификация технических средств воздействия. 2.
Основные показатели технических средств воздействия.

Тема 3.1 Применение инженерно-технических средств физической защиты 1.
Периметровые и объектовые средства обнаружения, порядок применения.
2. Работа с периферийным оборудованием системы контроля и управления доступом. 3.
Особенности организации пропускного режима на КПП.
4. Управление системой телевизионного наблюдения с автоматизированного рабочего места.
5. Порядок применения устройств отображения и документирования информации. 6.
Управление системой воздействия.

Тема 3.2 Эксплуатация инженерно-технических средств физической защиты
1. Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.
2. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.
3. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.
4. Организация ремонта технических средств физической защиты.

3.6. Задания по разделам дисциплины МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты.

ОК-01, ОК-02, ОК-09, ОК-10

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Что такое процедура? а. Правила использования программного и аппаратного обеспечения в компании б. Пошаговая инструкция по выполнению задачи в. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах г. Обязательные действия	б
Задание 2. *Прочитайте текст, выберите один правильный ответ* Что такое IDS? а. Система обнаружения вторжений б. Система межсетевого экранирования в. Система тактического планирования г. Система протоколирования и аудита	а
Задание 3. *Прочитайте текст, выберите один правильный ответ* Достоинством дискретных моделей политики безопасности является а. простой механизм реализации б. числовая вероятностная оценка надежности а.высокая степень надежности г. динамичность	а
Задание 4. *Прочитайте текст, выберите один правильный ответ* Для решения проблемы правильности выбора и надежности функционирования средств защиты в «Европейских критериях»вводится понятие а.адекватности средств защиты б.унификации средств защиты в.надежности защиты информации г.оптимизации средств защиты	а
Задания открытого типа	
Задание 5. *Прочитайте текст и ответьте на вопрос* Наукой, изучающей математические методы защиты информациипутем ее преобразования, является?	Криптология

Задание 6. *Прочитайте текст и ответьте на вопрос* Основу политики безопасности составляет?	Способ управления доступом
Задание 7. *Прочитайте текст и ответьте на вопрос* С точки зрения ГТК основной задачей средств безопасностиявляется обеспечение?	Защиты от НСД
Задание 8. *Прочитайте текст и дополните ответ* Класс F-DC согласно «Европейским критериям» характеризуется повышенными требованиями к _____	Конфиденциальности
Задание 9. *Прочитайте текст и ответьте на вопрос* Какая длина исходного ключа у алгоритма шифрования DES(бит)?	56
Задание 10. *Прочитайте текст и дополните ответ* В многоуровневой модели, если субъект доступа формируетзапрос на изменение, то уровень безопасности объекта относительно уровня безопасности субъекта должен _____	Доминировать
Задание 11. *Прочитайте текст и дополните ответ* В многоуровневой модели, если субъект доступа формируетзапрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен _____	Быть равен
Задание 12. *Прочитайте текст и дополните ответ* Оконечное устройство канала связи, через которое процесс может передавать или получать данные, называется _____	Сокет
Задание 13. *Прочитайте текст и дополните ответ* Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется _____	Качеством информации

Раздел 2. Основные компоненты комплекса инженерно- технических средств физической защиты

ОК-01, ОК-02, ОК-09, ОК-10

Типы заданий и диагностические задания	Эталонные ответы
Задания закрытого типа	
Задание 1. *Прочитайте текст, выберите один правильный ответ* Что из перечисленного не является целью проведения анализарисков? а. Делегирование полномочий б. Количественная оценка воздействия потенциальных угроз в. Выявление рисков г. Определение баланса между воздействием риска и стоимостью необходимых контрмер д.	а
Задание 2. *Прочитайте текст, выберите один правильный ответ* Перехват, который основан на фиксации электромагнитныхизлучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: а .активный перехват; б.пассивный перехват; в.аудиоперехват; г.видеоперехват;	б
Задание 3. *Прочитайте текст, выберите один правильный ответ* Под replay-атакой понимается: а. модификация передаваемого сообщения б. повторное использование переданного ранее сообщения в. невозможность получения сервиса законным пользователем	б
Задание 4. *Прочитайте текст, выберите один правильный ответ* Выделения пользователем и администраторам только тех правдоступа, которые им необходимы это а.принцип минимазации привилегий б.принцип простоты и управляемости ИС в.принцип многоуровневой защиты г.принцип максимизации привилегий	а
Задания открытого типа	
Задание 5. *Прочитайте текст и ответьте на вопрос* Достоинствами программной реализации криптографического закрытия данных являются?	Практичность и гибкость
Задание 6. *Прочитайте текст и дополните ответ* Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается _____	Высокой

Задание 7. *Прочитайте текст и дополните ответ* Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно "Европейским критериям" безопасность считается _____	Средней
Задание 8. *Прочитайте текст и дополните ответ* Если средство защиты способно противостоять отдельным атакам, то согласно "Европейским критериям" безопасность считается _____	Базовой
Задание 9. *Прочитайте текст и дополните ответ* Длина исходного ключа в ГОСТ 28147-89 (бит) составляет _____	256
Задание 10. *Прочитайте текст и дополните ответ* По документам ГТК количество классов защищенности АСот НСД _____	9
Задание 11. *Прочитайте текст и дополните ответ* С помощью закрытого ключа информация _____	Расшифровывается
Задание 12. *Прочитайте текст и дополните ответ* Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это _____	Аутентификация
Задание 13. *Прочитайте текст и дополните ответ* При полномочной политике безопасности совокупностьметок с одинаковыми значениями образует _____	Уровень безопасности

Раздел 3. Применение и эксплуатация инженерно- технических средств физической защиты

ОК-01, ОК-02, ОК-03, ОК-04, ОК-09, ОК-10

ПК-3.5

Вопрос	Ответ

Задание 1. *Прочитайте текст, выберите один правильный ответ* Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: а.активный перехват; б.пассивный перехват; в.аудиоперехват; г.видеоперехват; д.просмотр мусора.	в
Задание 2. *Прочитайте текст, выберите один правильный ответ* Если используются автоматизированные инструменты для анализарисков, почему все равно требуется так много времени для проведения анализа? а. Много информации нужно собрать и ввести в программу б. Руководство должно одобрить создание группы в. Анализ рисков не может быть автоматизирован, что связано ссамой природой оценки г. Множество людей должно одобрить данные	а
Задание 3. *Прочитайте текст, выберите один правильный ответ* В модели политики безопасности Лендвера ссылка на сущность,если это идентификатор сущности, называется а. прямой б. простой в. циклической г. косвенной	а
Задание 4. *Прочитайте текст, выберите один правильный ответ* Абстрактное описание системы, без связи с ее реализацией, даетмодель политики безопасности а. С полным перекрытием б. Белла-ЛаПадула в. На основе анализа угроз г.Лендвера	б
Задания открытого типа	
Задание 5. *Прочитайте текст и дополните ответ* Для реализации технологии RAID создается _____	Псевдодрайвер
Задание 6. *Прочитайте текст и дополните ответ* Единственный ключ используется в криптосистемах называется _____	Симметричный

Задание 7. *Прочитайте текст и дополните ответ* Запись определенных событий в журнал безопасностисервера называется _____	Аудитом
Задание 8. *Прочитайте текст и дополните ответ* Главным параметром криптосистемы является показатель _____	Криптостойкости
Задание 9. *Прочитайте текст и ответьте на вопрос*	Руководство
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?	
Задание 10. *Прочитайте текст и дополните ответ* Недостатком дискретных моделей политики безопасности является _____	Статичность
Задание 11. *Прочитайте текст и дополните ответ* Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется_____	Профилем защиты
Задание 12. *Прочитайте текст и дополните ответ* Математические методы нарушения конфиденциальности иаутентичности информации без знания ключей объединяет _____	Криптоанализ
Задание 13. *Прочитайте текст и ответьте на вопрос* Какое количество уровней адекватности, которое определяют «Европейские критерии»?	7

Типовые задания для рубежного контроля по **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации**:

Тестовое задание

К первой рубежной аттестации

Вариант №1

1. Что представляет собой информация в информатизации?

а) Смесь цветов
б) Случайные символы
в) Организованные данные смыслового содержания
г) Звуковая волна

2. Какие объекты могут подвергаться информатизации?

а) Только природные явления
б) Различные объекты, включая данные, процессы и системы
в) Исключительно химические соединения
г) Только материальные объекты

3. Что представляет собой информационный сигнал в контексте передачи данных?

а) Световая волна
б) Звуковая волна
в) Передающее сообщение в виде электрического сигнала
г) Цветовой спектр

4. Какие физические свойства могут быть характерны для аналоговых сигналов?

а) Дискретность значений
б) Бесконечное количество значений в диапазоне
в) Ограниченный диапазон частот
г) Цифровое кодирование

5. Какой документ регулирует вопросы информационной безопасности в Российской Федерации?

а) Конституция Российской Федерации
б) Закон о защите от вредоносных программ
в) Федеральный закон "Об информации, информационных технологиях и о защите информации"
г) Декларация прав человека и гражданина

6. Что определяют нормативные акты в области защиты информации?

а) Лишь рекомендации и советы
б) Методы взлома информационных систем
в) Обязательные требования и правила по обеспечению безопасности информации
г) Программы для шифрования данных

7. Что включает в себя физическая защита объектов информатизации?

а) Только программное обеспечение
б) Организационные и технические меры, направленные на предотвращение несанкционированного доступа
в) Электронные пароли
г) Защита от вирусов

8. Какое значение имеет правовое обеспечение физической защиты объектов информатизации?

а) Только документирование процедур
б) Установление норм и правил обеспечения безопасности, а также ответственности за их нарушение
в) Инвентаризация оборудования

г) Обучение персонала

9. Что определяет объект как потенциально опасный?
а) Только наличие огнестрельного оружия
б) Возможность причинения вреда здоровью людей и окружающей среде
в) Только размер объекта
г) Отдаленное расположение от населенных пунктов

10. Какие критерии могут указывать на потенциальную опасность объекта в информатизированном обществе?
а) Наличие ценной информации, влияющей на функционирование общества и государства
б) Лишь количество сотрудников компании
в) Только финансовые показатели
г) Уровень образования сотрудников

11. Что включает в себя физическая защита объектов информатизации?
а) Охрана со стороны сотрудников
б) Организационные, технические и меры контроля доступа
в) Установка антивирусного программного обеспечения
г) Электронные пароли

12. Какие задачи решает физическая защита в области информатизации?
а) Защита от вирусов
б) Предотвращение несанкционированного доступа, обеспечение целостности и конфиденциальности информации, обеспечение работоспособности системы
в) Контроль за содержанием информации
г) Оптимизация работы компьютеров

13. Что представляют собой инженерно-технические средства физической защиты?
а) Только электрические приборы
б) Совокупность средств и систем, предназначенных для обеспечения безопасности объектов
в) Только строительные конструкции
г) Автомобильные дороги

14. Какие задачи решают инженерно-технические средства физической защиты?
а) Только охрана от пожаров
б) Предотвращение несанкционированного проникновения, обнаружение и реагирование на инциденты безопасности
в) Только декоративное украшение объекта
г) Улучшение климата в помещении

15. Какие этапы включает в себя жизненный цикл системы инженерно-технических средств физической защиты?
а) Только проектирование
б) Проектирование, внедрение, эксплуатация, вывод из эксплуатации
в) Только обслуживание
г) Разработка технической документации

16. На каком этапе жизненного цикла происходит разработка технических требований к системе физической защиты?
а) На этапе проектирования б)
Только на этапе внедрения
в) Только на этапе эксплуатации
г) На этапе вывода из эксплуатации

17. Какие методы могут быть использованы при внедрении инженерно-технических средств на объекты информатизации?
а) Только метод проб и ошибок
б) Метод пилотного проекта, этапного внедрения, стратегии "большого взрыва" в) Только принуждение сотрудников
г) Метод случайного выбора

18. Какой метод предпочтителен при внедрении инженерно-технических средств с минимальными рисками?
а) Метод "большого взрыва"
б) Метод пилотного проекта
в) Метод этапного внедрения
г) Метод случайного выбора

19. Какие требования предъявляются к системам видеонаблюдения с точки зрения информационной безопасности?
а) Только высокая разрешающая способность
б) Шифрование передаваемых видеопотоков, защита от несанкционированного доступа
в) Только цветовое воспроизведение
г) Простота использования

20. Каким образом системы контроля доступа должны обеспечивать информационную безопасность предприятия?
а) Ограничение и регулирование доступа, регистрация действий сотрудников
б) Только обнаружение движения на территории
в) Легкость обхода системы
г) Только визуализацию рабочего времени

Вариант №2

1. Что характеризует информацию в контексте информатизации?
а) Безупречная форма
б) Значимость и организованность данных
в) Непредсказуемость
г) Случайность и случайность

2. Какова цель информатизации объектов?
а) Сокрытие информации
б) Уменьшение доступности данных
в) Эффективное управление информацией и повышение производительности
г) Случайная трансформация данных

3. Какое из перечисленных является примером цифрового сигнала?
а) Синусоидальная волна
б) Битовая последовательность 01010101
в) Амплитудная модуляция
г) Аналоговый ток

4. Что определяет частоту информационного сигнала?
а) Временной интервал между битами
б) Скорость передачи данных
в) Диапазон изменения амплитуды
г) Количество колебаний в секунду

5. Какой орган в России отвечает за контроль и надзор в области защиты информации?

а) Министерство здравоохранения
б) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
в) Министерство образования и науки
г) Федеральная служба безопасности (ФСБ)

6. Какие данные относятся к категории ограниченного доступа согласно законодательству России?
а) Информация о погоде
б) Сведения о подготовке к военным действиям и действиям в чрезвычайных ситуациях
в) Новости о спорте
г) Объявления о продаже недвижимости

7. Какие органы ответственны за контроль за соблюдением правил физической защиты?
а) Только местные органы самоуправления
б) Федеральные органы исполнительной власти и органы местного самоуправления, уполномоченные в сфере информационной безопасности
в) Только представители бизнес-структур
г) Акционеры компании

8. Какое документальное оформление необходимо для обеспечения физической защиты?
а) Только устные инструкции от руководства
б) Письменные объявления на дверях помещений
в) Только устные инструкции от сотрудников
г) Разработка и утверждение положений о физической защите, планов мероприятий по безопасности

9. Что подразумевается под термином "критерии оценки потенциальной опасности"?
а) Только цвет стен здания
б) Определенные параметры и характеристики, позволяющие оценить степень возможного воздействия объекта на окружающую среду
в) Только наличие забора вокруг объекта
г) Лишь местоположение объекта

10. Какие объекты могут быть отнесены к потенциально опасным в информационной сфере?
а) Только банковские учреждения
б) Информационные системы, обрабатывающие данные государственной важности
в) Только склады материалов
г) Культурные учреждения

11. Каким образом реализуется организационная часть физической защиты объектов информатизации?
а) Установка сигнализации
б) Разработкой и внедрением правил и процедур безопасности, обучением персонала
в) Использование биометрической идентификации
г) Регулярной сменой паролей

12. Какие технические средства могут быть задействованы в физической защите?
а) Огнетушители
б) Системы видеонаблюдения, датчики движения, системы контроля доступа
в) Оборудование для автоматического восстановления данных
г) Программы антивирусной защиты

13. Какие функции могут выполнять системы видеонаблюдения в инженерно-технических средствах физической защиты?
а) Определение и фиксация движения, визуальное наблюдение за объектом, детекция нарушений безопасности
б) Только запись звука
в) Только подсветка территории
г) Предупреждение об авариях

14. Каким образом датчики движения могут использоваться в инженерно-технических средствах физической защиты?
а) Только для замера температуры
б) Определение влажности воздуха
в) Только для измерения уровня освещенности
г) Обнаружение движения и сигнализация о наличии посторонних объектов на охраняемой территории

15. Что включает в себя этап внедрения в жизненном цикле системы физической защиты?
а) Только тестирование оборудования
б) Установка и настройка системы, обучение персонала, внедрение в реальные условия
в) Только разработка технической документации
г) Обслуживание оборудования

16. На каком этапе происходит активное использование системы физической защиты?
а) Только на этапе проектирования
б) На этапе вывода из эксплуатации
в) Только на этапе внедрения
г) На этапе эксплуатации

17. Как осуществляется внедрение по методу "большого взрыва"?
а) Только поэтапно
б) Одновременно на всем объекте
в) Только по одному элементу в день
г) Случайным образом

18. Что представляет собой метод этапного внедрения?
а) Внедрение на случайно выбранных этапах
б) Постепенное внедрение на различных этапах с последующей проверкой и корректировкой
в) Только внедрение на последних этапах
г) Одновременное внедрение на всех этапах

19. Какие требования к датчикам движения необходимы для обеспечения информационной безопасности?
а) Надежность обнаружения, защита от ложных срабатываний
б) Только высокая чувствительность
в) Только совместимость с другими устройствами
г) Простота монтажа

20. Какую роль выполняют системы сигнализации в обеспечении информационной безопасности?
а) Только визуальное оповещение
б) Своевременное обнаружение и сигнализация о возможных инцидентах безопасности в) Только запись видеоматериалов
г) Поддержание микроклимата в помещении

Вариант № 3

1. Что является основой для объектов информатизации?
а) Только человеческий фактор
б) Данные и информационные технологии
в) Эмоциональные состояния
г) Несистематизированные хаос и беспорядок

2. Какой процесс непосредственно связан с информатизацией объектов?
а) Случайное изменение данных
б) Отделение от информационных технологий
в) Внедрение современных технологий для управления информацией
г) Изоляция данных от доступа

3. Какова роль шума в передаче данных?
а) Увеличение скорости передачи
б) Искажение и исключение полезной информации
в) Снижение частоты сигнала
г) Увеличение амплитуды сигнала

4. Что характеризует амплитуду информационного сигнала?
а) Временной интервал между битами
б) Частоту передачи данных
в) Максимальное отклонение сигнала от нулевого уровня
г) Длительность сигнала

5. Какие меры обеспечения безопасности информации предписаны законодательством?
а) Только шифрование данных
б) Только установка антивирусного программного обеспечения
в) Комплекс мер, включая шифрование, антивирусную защиту, контроль доступа и т.д.
г) Регулярное копирование данных

6. Какой документ содержит основные положения о защите информации в информационных системах?
а) ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации"
б) Техническое задание на создание сайта
в) Рецепт приготовления кофе
г) Справочник по программированию на языке Python

7. Какова роль технических средств в физической защите объектов информатизации?
а) Обеспечение физической безопасности при помощи видеонаблюдения, контроля доступа и т.д.
б) Исключительно оформление бумажных документов
в) Только защита от вирусов
г) Сокрытие компьютеров от посторонних глаз

8. Какие основные нормативно-правовые акты регулируют физическую защиту объектов информатизации в России?
а) Законы о земле и воде
б) Федеральный закон "Об информации, информационных технологиях и о защите информации"
в) Налоговый кодекс
г) Конституция Российской Федерации

9. Какие характеристики могут быть важны для оценки потенциальной опасности в информатизированных системах?
а) Только год создания компании
б) Уровень заработной платы сотрудников
в) Значимость обрабатываемой информации, уровень защиты данных
г) Цвет фасада здания

10. Какое значение имеет оценка вероятности возникновения опасных ситуаций на объекте?
а) Только для страховых компаний
б) Позволяет определить необходимость и эффективность мер по физической защите
в) Лишь для геологов
г) Применяется только в промышленности

11. Какое значение имеет контроль доступа в физической защите объектов информатизации?
а) Ограничение доступа к печатающим устройствам
б) Предотвращение несанкционированного проникновения, контроль за перемещением людей в помещении
в) Защита от перегрева оборудования
г) Увеличение скорости передачи данных

12. Какие принципы лежат в основе технической части физической защиты информатизированных объектов?
а) Принцип энергосбережения
б) Принципы целесообразности, неотвратимости, комплексности и сочетания с организационными мерами
в) Принцип экономии бумаги
г) Принцип самообслуживания

13. Какую роль могут выполнять системы контроля доступа в инженерно-технических средствах физической защиты?
а) Только регистрация рабочего времени
б) Определение температуры в помещении
в) Только контроль за исправностью оборудования
г) Ограничение и регулирование доступа сотрудников и посетителей на объект

14. Какие преимущества обеспечивает использование биометрической идентификации в системах физической защиты?
а) Только низкая стоимость оборудования
б) Высокий уровень точности идентификации, исключение возможности передачи аутентификационных данных
в) Только дополнительный эффект декоративности
г) Улучшение качества интернет-соединения

15. Какие меры могут быть предприняты на этапе эксплуатации системы физической защиты?

а) Только заключение контрактов с поставщиками оборудования
б) Проведение регулярных технических обслуживаний, мониторинг работы системы, обучение персонала
в) Только разработка новых технических требований
г) Обновление программного обеспечения

16. Какие этапы включают в себя мероприятия по выводу системы физической защиты из эксплуатации?
а) Только разработка технической документации
б) Подготовка к выводу, анализ эффективности, разработка отчетов
в) Только демонтаж оборудования
г) Подписание нового контракта

17. Какова основная идея метода пилотного проекта?
а) Провести внедрение только в одном отделе
б) Внедрение только на критических объектах
в) Только обучение персонала на отдельных образцах
г) Выбрать небольшую часть объекта для тестирования и корректировки перед полным внедрением

18. Какие преимущества предоставляет метод проб и ошибок при внедрении инженерно-технических средств?
а) Постепенное выявление недостатков и корректировка, минимизация рисков б) Только сокращение сроков внедрения
в) Только снижение бюджетных затрат
г) Ускорение процесса внедрения на всех объектах

19. Каким образом технические барьеры должны способствовать обеспечению информационной безопасности предприятия?
а) Только как декоративные элементы
б) Ограничение доступа посетителей, создание зон контролируемого доступа в) Только для обозначения территории
г) Снижение энергопотребления

20. Какие требования предъявляются к системам биометрической идентификации для обеспечения информационной безопасности?
а) Высокий уровень точности идентификации, исключение возможности передачи аутентификационных данных
б) Только низкая стоимость оборудования
в) Только дополнительный эффект декоративности г) Улучшение качества интернет-соединения

Вариант № 4

1. Как изменяется природа информации при информатизации объектов?
а) Становится менее структурированной
б) Теряет свою значимость
в) Становится более организованной и целенаправленной
г) Превращается в случайный набор данных

2. Какое влияние оказывает информатизация на эффективность управления информацией?
а) Снижает эффективность
б) Не влияет на эффективность
в) Делает управление беспорядочным
г) Повышает эффективность

3. Как влияет демпфирование на информационный сигнал?
а) Уменьшение амплитуды сигнала по мере распространения
б) Увеличение частоты сигнала
в) Искажение формы сигнала
г) Увеличение длительности сигнала

4. Что определяет скорость передачи данных в канале связи?
а) Амплитуду сигнала
б) Количество бит, передаваемых за единицу времени
в) Частоту сигнала
г) Длительность сигнала

5. Какие субъекты относятся к категории субъектов информационных отношений согласно законодательству России?
а) Только физические лица
б) Только юридические лица
в) Физические и юридические лица, осуществляющие обработку информации
г) Информационные технологии

6. Какова ответственность за нарушение законодательства о защите информации в России?
а) Только предупреждение
б) Административная, гражданская и уголовная ответственность
в) Штраф в размере 5000 рублей
г) Ограничение доступа к интернету

7. Что подразумевается под термином "организационные меры" в физической защите?
а) Только установление технических средств защиты
б) Только охрана со стороны правоохранительных органов
в) Система правил и процедур, направленных на обеспечение безопасности г) Только пожарная безопасность

8. Какие документы могут определять порядок физической защиты?
а) Только техническая документация
б) Положения о физической защите и планы мероприятий по обеспечению безопасности
в) Только устав предприятия
г) Протоколы собраний акционеров

9. Какие виды угроз могут быть связаны с потенциально опасными объектами в информационной сфере?
а) Только стихийные бедствия
б) Кибератаки, утечка конфиденциальной информации, нарушение целостности данных
в) Только человеческий фактор
г) Загрязнение окружающей среды

10. Что подразумевается под термином "возможные последствия потенциально опасных объектов"?
а) Только возможные финансовые потери
б) Потенциальные угрозы для здоровья людей, окружающей среды и общества в целом
в) Только временные проблемы с работой объекта
г) Возможность создания новых рабочих мест

11. Какие методы обучения персонала используются в организациях для обеспечения физической безопасности?
а) Чтение статей в интернете
б) Проведение тренингов, семинаров, тестирование сотрудников
в) Самостоятельное изучение литературы по теме
г) Принуждение к выполнению правил

12. Как обеспечивается физическая защита в условиях удаленной работы сотрудников?
а) Применение VPN-соединений
б) Комбинацией технологий, включая шифрование данных, использование защищенных каналов связи и контроль дистанционного доступа
в) Проведение ежегодных тренингов по физической защите
г) Запрет на удаленную работу

13. Каким образом технические барьеры могут применяться в инженерно-технических средствах физической защиты?
а) Только как декоративные элементы
б) Ограничение доступа посетителей, создание зон контролируемого доступа
в) Только для обозначения территории
г) Снижение энергопотребления

14. Какую роль могут играть системы сигнализации в инженерно-технических средствах физической защиты?
а) Своевременное обнаружение и сигнализация о возможных инцидентах безопасности
б) Только визуальное оповещение
в) Только запись видеоматериалов
г) Поддержание микроклимата в помещении

15. На каком этапе возможно проведение модернизации системы физической защиты?
а) Только на этапе проектирования
б) На этапе внедрения
в) Только на этапе эксплуатации
г) На любом этапе жизненного цикла

16. Какие факторы могут повлиять на принятие решения о модернизации системы физической защиты?
а) Техническое устаревание оборудования, изменение уровня угроз, появление новых технологий
б) Только изменение структуры персонала
в) Только финансовые аспекты
г) Рост числа сотрудников

17. Каким образом может быть реализован метод случайного выбора?
а) Только розыгрышем среди сотрудников
б) Выбор случайного объекта для внедрения
в) Только решением руководства
г) Путем проведения конкурса

18. Какие этапы включает в себя стратегия "большого взрыва"?
а) Только этап обучения персонала
б) Подготовка, внедрение, обучение персонала
в) Только этап тестирования
г) Этап выбора метода внедрения

19. Какие требования предъявляются к системам датчиков утечки воды для обеспечения информационной безопасности?

а) Быстрое обнаружение утечки, оповещение персонала б) Только визуальное отображение информации

в) Только совместимость с другими системами безопасности г) Простота использования

20. Что необходимо учитывать при выборе технических средств физической защиты для обеспечения информационной безопасности предприятия?

а) Соответствие современным стандартам, возможность интеграции с другими системами безопасности

б) Только цветовое воспроизведение

в) Наличие красочной инструкции по эксплуатации

г) Простота монтажа

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	в	б	б	б
2	б	в	в	г
3	в	б	б	г
4	б	г	в	б
5	в	б	в	в
6	в	б	а	б
7	б	б	а	в
8	б	г	б	б
9	б	б	в	б
10	а	б	б	б
11	в	в	в	в
12	в	в	в	в
13	б	а	г	б
14	б	г	б	а
15	б	б	б	г
16	а	г	б	а
17	б	б	г	б
18	а	б	а	б
19	б	а	б	а
20	а	б	а	а

Вопросы ко 2-ой рубежной аттестации

1. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.
2. Общие принципы обеспечения безопасности объектов.
3. Жизненный цикл системы физической защиты.
4. Принципы построения интегрированных систем охраны.
5. Классификация и состав интегрированных систем охраны.
6. Требования к инженерным средствам физической защиты.
7. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
8. Информационные основы построения системы охранной сигнализации.
9. Назначение, классификация технических средств обнаружения.
10. Построение систем обеспечения безопасности объекта)
11. Периметровые средства обнаружения: назначение, устройство, принцип действия.
12. Назначение объектовых средств обнаружения.

Тестовые задания по дисциплине МДК. 03. 02 «Инженерно-технические средства физической защиты объектов информатизации»
II-аттестация

Вариант № 1

1. Что представляет собой модель нарушителя?
а) Только описание внешности нарушителя
б) Абстрактное представление о характеристиках потенциального нарушителя и его действиях
в) Только портрет нарушителя
г) Графическое изображение нарушителя
2. Какие основные компоненты включает в себя модель нарушителя?
а) Характеристики нарушителя, его цели, методы и средства проникновения
б) Только визуальное представление нарушителя
в) Только описание его внешности г)
Портрет нарушителя
3. Каким образом принцип регулярного аудита безопасности воздействует на обеспечение защиты объектов?
а) Позволяет выявлять уязвимости и ошибки в системе безопасности, обеспечивает постоянный мониторинг
б) Ограничивает функциональность системы безопасности
в) Только усложняет процесс управления безопасностью
г) Приводит к снижению эффективности системы
4. Как принцип реагирования на инциденты влияет на обеспечение безопасности объектов?
а) Позволяет оперативно реагировать на инциденты, минимизирует ущерб
б) Увеличивает время реакции на инциденты
в) Только усложняет систему безопасности
г) Приводит к снижению эффективности мер по обеспечению безопасности
5. Что включает в себя этап проектирования в жизненном цикле системы физической защиты?
а) Разработка концепции и выбор средств защиты
б) Ограничение только выбором средств защиты
в) Только техническое обслуживание
г) Прототипирование
6. Каким образом этап внедрения влияет на функционирование системы физической защиты?

а) Обеспечивает установку и настройку средств защиты, переход системы в рабочий режим б) Не влияет на функционирование системы
в) Только предоставляет документацию
г) Ограничивает функциональность системы

7. Что представляет собой принцип централизации в интегрированных системах охраны?

а) Разделение ответственности между различными службами
б) Сосредоточение управления и контроля в едином центре
в) Только использование технических средств
г) Разнообразие систем управления

8. Как принцип распределенной архитектуры влияет на гибкость интегрированных систем охраны?

а) Обеспечивает гибкость и надежность системы
б) Снижает гибкость и усложняет управление
в) Только увеличивает стоимость системы
г) Приводит к увеличению энергопотребления

9. Что включает в себя классификация интегрированных систем охраны по области применения?

а) Системы для охраны жилых зон
б) Только системы для охраны промышленных объектов
в) Системы только для автомобилей
г) Ограничение только системами для охраны банков

10. Каким образом происходит классификация интегрированных систем охраны по типу объектов?

а) Только по степени важности объектов
б) По видам объектов: промышленные, коммерческие, государственные, жилые и другие в) Только по географическому положению объектов
г) Ограничение только по размерам объектов

11. Какие требования предъявляются к прочности инженерных средств физической защиты?

а) Только эстетическая прочность б) Только механическая прочность
в) Высокая механическая прочность и устойчивость к воздействию внешних факторов г) Прототипирование

12. Каким образом требования к эргономике влияют на эффективность использования инженерных средств?

а) Уменьшают эффективность
б) Обеспечивают удобство использования и повышают эффективность
в) Только усложняют систему безопасности
г) Приводят к увеличению стоимости системы

13. Как инженерные конструкции могут предотвращать физический доступ к серверным комнатам?

а) Только использование паролей
б) Использование биометрических замков и систем контроля доступа
в) Только видеонаблюдение
г) Все перечисленное

14. Какие инженерные решения могут использоваться для защиты от несанкционированного доступа к кабельным системам?

а) Только шифрование данных
б) Все перечисленное
в) Только использование сетевых экранов
г) Использование кабельных каналов с физической защитой

15. Что является основой информационных систем охранной сигнализации?

а) Только физические барьеры
б) Только звуковые сигнализаторы
в) Использование сенсоров, детекторов и передача информации

г) Все перечисленное

16. Каким образом информационные системы охранной сигнализации реагируют на обнаружение угрозы?

а) Только оповещение охраны б)
Все перечисленное
в) Только активация звуковых сигнализаторов
г) Моментальная передача информации о событии на пульт централизованной охраны

17. Что является основным назначением технических средств обнаружения?

а) Только создание шумового фона
б) Раннее обнаружение и сигнализация о возможной опасности
в) Только создание видимости охранного оборудования
г) Все перечисленное

18. Какие технические средства обнаружения относятся к классу "датчиков движения"?

а) Только микрофоны
б) Инфракрасные датчики движения и ультразвуковые датчики движения
в) Только видеокамеры
г) Все перечисленное

19. Какие компоненты включает в себя система обеспечения безопасности объекта?

а) Только физическая охрана
б) Инженерно-технические средства, персонал охраны и системы обнаружения
в) Только системы видеонаблюдения
г) Все перечисленное

20. Каким образом инженерно-технические средства влияют на эффективность системы безопасности?

а) Путем раннего обнаружения и сигнализации о возможных угрозах
б) Только созданием видимости оборудования
в) Только путем предупреждения охранного персонала г)
Все перечисленное

Вариант № 2

1. Какие цели может преследовать нарушитель согласно модели?

а) Только попытка нанесения физического вреда
б) Несанкционированный доступ к информации, уничтожение данных, прерывание работы систем
в) Только изменение цвета объекта
г) Попытка уклонения от ответственности

2. Как характеристики нарушителя используются при анализе модели?

а) Они помогают предсказать возможные действия нарушителя и его методы проникновения
б) Не имеют значения при анализе модели
в) Только они формируют внешность нарушителя
г) Они не учитываются в анализе

3. Какие меры могут быть приняты на основе принципа минимизации рисков в обеспечении безопасности объектов?

а) Идентификация и сокращение потенциальных угроз и уязвимостей
б) Увеличение численности персонала безопасности
в) Только ограничение физического доступа
г) Использование только технических средств

4. Каким образом принцип резервирования влияет на обеспечение безопасности объектов?

а) Приводит к снижению эффективности мер по обеспечению безопасности б)
Увеличивает риск потери данных
в) Только усложняет систему безопасности
г) Обеспечивает сохранность информации и функционирование систем в случае отказов

5. Что представляет собой этап эксплуатации в жизненном цикле системы физической защиты?

а) Прототипирование

б) Ограничение только применением системы в)

Только разработка документации

г) Регулярное обслуживание и мониторинг состояния средств защиты в рабочем режиме

6. Каким образом этап модернизации влияет на эффективность системы физической защиты?

а) Позволяет внедрять новые технологии и обновлять средства защиты

б) Снижает эффективность системы

в) Только усложняет систему безопасности

г) Увеличивает риск инцидентов безопасности

7. Что означает принцип стандартизации в контексте интегрированных систем охраны?

а) Игнорирование стандартов безопасности

б) Использование единых стандартов для обеспечения совместимости компонентов

в) Только создание уникальных решений

г) Увеличение сложности системы

8. Каким образом принцип модульности влияет на масштабируемость интегрированных систем охраны?

а) Снижает масштабируемость системы

б) Позволяет легко добавлять или заменять отдельные компоненты системы

в) Только увеличивает стоимость системы

г) Приводит к снижению энергопотребления

9. Что включает в себя классификация интегрированных систем охраны по типу используемых технологий?

а) Только по типу электрических сигнализаций

б) Системы с видеонаблюдением, контролем доступа, детекторами движения и др.

в) Системы только с биометрическим контролем

г) Ограничение только системами с использованием роботов

10. Каким образом классификация интегрированных систем охраны по степени автоматизации влияет на эффективность системы?

а) Чем выше степень автоматизации, тем эффективнее система

б) Снижает эффективность системы

в) Только усложняет систему безопасности

г) Приводит к увеличению стоимости системы

11. Что представляют собой требования к энергопотреблению инженерных средств физической защиты?

а) Только высокое энергопотребление

б) Энергосберегающие технологии и низкое энергопотребление в)

Только устойчивость к отключениям электроэнергии

г) Ограничение только использованием альтернативных источников энергии

12. Каким образом требования к стойкости к воздействию окружающей среды влияют на долговечность инженерных средств?

а) Снижают долговечность

б) Обеспечивают стойкость к агрессивным факторам окружающей среды в)

Только увеличивают стоимость системы

г) Приводят к ограничению использования средств

13. Как инженерные конструкции обеспечивают физическую защиту серверного оборудования?

а) Использование серверных шкафов с замками и системами мониторинга б)

Только резервное копирование данных

в) Только видеонаблюдение

г) Все перечисленное

14. Каким образом инженерные решения могут предотвращать несанкционированный доступ к компьютерам и рабочим станциям?

а) Только использование антивирусного ПО
б) Только периодическая смена паролей
в) Использование систем биометрической идентификации и считывателей карт
г) Все перечисленное

15. Что включает в себя передача информации в информационных системах охранной сигнализации?

а) Только звуковые сигналы
б) Предупреждение, детализированное описание события и расположение объекта события
в) Только видеонаблюдение
г) Все перечисленное

16. Каким образом информационные системы охранной сигнализации обеспечивают интерактивное взаимодействие с операторами?

а) Только электронная почта
б) Использование телефонии, видеосвязи и интернет-каналов связи
в) Только радиосвязь
г) Все перечисленное

17. Что характеризует класс "датчиков проникновения"?

а) Только определение температуры
б) Обнаружение внешних воздействий, таких как взлом и проникновение в)
Только отслеживание уровня освещенности
г) Все перечисленное

18. Какие технические средства относятся к классу "датчиков взлома"?

а) Только датчики дыма
б) Герконовые датчики, штатные датчики и датчики стекловзлома
в) Только детекторы движения
г) Все перечисленное

19. Что включает в себя персонал охраны в системе обеспечения безопасности объекта?

а) Только физическое присутствие охранников
б) Квалифицированных охранников, операторов мониторинга и реагирования
в) Только системы дистанционного управления
г) Все перечисленное

20. Каким образом системы видеонаблюдения способствуют обеспечению безопасности объекта?

а) Только зафиксированные видеозаписи
б) Обнаружением и записью подозрительных событий, а также визуальным контролем
в) Только видимость камер и мониторов
г) Все перечисленное

Вариант № 3

1. Какие методы и средства проникновения могут быть представлены в модели нарушителя?

а) Только технические средства
б) Физические и технические средства, социальная инженерия
в) Только социальная инженерия
г) Полное отсутствие методов и средств

2. Что представляет собой социальная инженерия в контексте модели нарушителя?

а) Описание оборудования
б) Манипуляции и воздействие на человеческий фактор для достижения целей
в) Только предоставление информации
г) Технические средства

3. Что означает принцип соответствия в контексте обеспечения безопасности объектов?

а) Соблюдение стандартов и требований в области безопасности
б) Игнорирование стандартов безопасности

в) Только усложнение системы безопасности
г) Приводит к снижению эффективности мер по обеспечению безопасности

4. Каким образом принцип постоянного улучшения воздействует на систему безопасности объектов?

а) Способствует развитию и совершенствованию системы безопасности
б) Приводит к статичности системы
в) Только усложняет процесс управления безопасностью
г) Увеличивает риск инцидентов безопасности

5. Что означает этап вывода из эксплуатации в жизненном цикле системы физической защиты?

а) Снятие с эксплуатации устаревших средств и обеспечение безопасного вывода
б) Игнорирование проблем и использование устаревших средств

в) Только создание резервных копий данных
г) Ограничение только архивированием данных

6. Какие меры предпринимаются на этапе проектирования для обеспечения устойчивости системы физической защиты?

а) Выбор надежных средств защиты и учет
особенностей объекта б) Только составление плана
проектирования
в) Только тестирование средств защиты
г) Прототипирование

7. Что представляет собой принцип гетерогенности в интегрированных системах охраны?

а) Только использование единообразных компонентов
б) Использование разнообразных компонентов для оптимальной
функциональности
в) Ограничение только типов используемых технологий
г) Увеличение сложности системы

8. Как принцип открытости влияет на возможность интеграции с другими системами?

а) Обеспечивает совместимость и легкость интеграции с
различными системами б) Снижает возможность интеграции
в) Только усложняет систему безопасности
г) Приводит к увеличению стоимости системы

9. Что включает в себя состав интегрированных систем охраны в контексте видеонаблюдения?

а) Только камеры наблюдения
б) Только мониторы для просмотра
в) Камеры, видеорегистраторы, аналитическое ПО и системы
хранения данных
г) Ограничение только системами оповещения

10. Каким образом в состав интегрированных систем охраны включаются системы контроля доступа?

а) Приводит к снижению
эффективности системы
б) Только физическая охрана
в) Только системы видеонаблюдения
г) Считыватели карт и биометрические устройства, контроллеры доступа

11. Что означают требования к совместимости инженерных средств физической защиты?

а) Только возможность работы с определенными устройствами
б) Возможность интеграции и совместной работы с другими средствами
безопасности
в) Только использование единого поставщика оборудования
г) Ограничение только использованием собственных технологий

12. Каким образом требования к техническим характеристикам влияют на эффективность инженерных средств физической защиты?

а) Снижают эффективность использования
б) Обеспечивают высокие технические характеристики для
эффективной работы
в) Только усложняют систему безопасности
г) Приводят к увеличению стоимости системы

13. Какие инженерные конструкции применяются для защиты от физических угроз в помещениях с серверным оборудованием?

а) Только использование огнетушителей

б) Использование систем детекции движения и сигнализации

в) Только видеонаблюдение

г) Все перечисленное

14. Как инженерные решения обеспечивают безопасность хранения информации на бумажных носителях?

а) Только использование сейфов

б) Использование помещений с контролем доступа и системами тревожной сигнализации

в) Только периодическое перемещение документов

г) Все перечисленное

15. Что представляет собой централизованная обработка информации в системах охранной сигнализации?

а) Анализ и обработка поступающей информации с датчиков и сенсоров б) Только хранение информации

в) Только передача сигналов охраны

г) Все перечисленное

16. Каким образом информационные системы охранной сигнализации могут интегрироваться с другими системами безопасности?

а) Только с физической охраной

б) Использование стандартных протоколов для взаимодействия с видеонаблюдением, системами контроля доступа и другими

в) Только с системами звукового оповещения

г) Все перечисленное

17. Каким образом классифицируются акустические датчики в технических средствах обнаружения?

а) Только по уровню звукового давления

б) Все перечисленное

в) Только по времени срабатывания

г) По частотному спектру, длительности звукового сигнала и характеристикам шумового фона

18. Что представляют собой тепловизионные камеры в системах обнаружения?

а) Камеры, способные регистрировать инфракрасное излучение, что позволяет обнаруживать объекты по тепловым следам

б) Только обычные видеокамеры

в) Только фотокамеры

г) Все перечисленное

19. Что представляют собой системы контроля доступа в обеспечении безопасности объекта?

а) Только физические барьеры

б) Идентификация и ограничение доступа персонала посредством карт, биометрических данных и кодов доступа

в) Только видеонаблюдение

г) Все
перечисленное

20. Каким образом интегрированные системы охраны повышают эффективность безопасности объекта?

а) Только повышением стоимости оборудования
б) Совместным использованием данных и взаимодействием различных средств обеспечения безопасности
в) Только увеличением численности
охранного персонала
г) Все перечисленное

Вариант № 4

1. Каким образом модель нарушителя помогает в планировании мер по физической защите объекта?

а) Позволяет предвидеть возможные сценарии проникновения и принимать меры по их предотвращению
б) Не оказывает влияния на планирование мер по
физической защите в) Только оценивает внешний вид
нарушителя
г) Предоставляет только информацию о целях нарушителя

2. Какие меры безопасности могут быть приняты на основе анализа модели
нарушителя?

а) Усиление контроля доступа, обеспечение физической защиты,
обучение персонала
б) Только установка дополнительных камер наблюдения
в) Только проведение психологических
тестирований персонала г) Полное отсутствие мер
безопасности

3. Каким образом принцип разнообразия влияет на обеспечение безопасности объектов?

а) Использование различных методов и технологий для
предотвращения угроз
б) Уменьшение разнообразия с целью упрощения системы
безопасности
в) Только усложнение системы безопасности
г) Приводит к снижению эффективности мер по обеспечению безопасности

4. Как принцип гибкости влияет на адаптацию системы безопасности к изменяющимся условиям?

а) Позволяет системе быстро адаптироваться к новым угрозам и
требованиям б) Приводит к статичности системы безопасности
в) Только усложняет процесс управления
безопасностью
г) Увеличивает риск инцидентов
безопасности

5. Каким образом этап внедрения влияет на уровень подготовки персонала к работе с системой физической защиты?

а) Увеличивает сложность системы
безопасности б) Не влияет на
уровень подготовки персонала
в) Только проводит тестирование средств защиты

г) Предоставляет обучение персонала и обеспечивает переход в режим эксплуатации

6. Какие меры предпринимаются на этапе эксплуатации для предотвращения инцидентов безопасности?

а) Регулярное обучение персонала, мониторинг состояния системы и проведение аудитов безопасности

б) Только регулярное обслуживание средств защиты

в) Только изменение паролей доступа

г) Увеличение численности охраны

7. Что означает принцип голосовой связи в интегрированных системах охраны?

а) Игнорирование средств связи

б) Использование голосовой связи для оперативного взаимодействия в) Только использование текстовых сообщений

г) Увеличение энергопотребления

8. Каким образом принцип прозрачности влияет на восприятие и использование интегрированных систем охраны?

а) Обеспечивает простоту восприятия и управления системой

б) Затрудняет восприятие и управление системой

в) Только усложняет систему безопасности

г) Приводит к увеличению стоимости системы

9. Что включает в себя состав интегрированных систем охраны в контексте сигнализации?

а) Только звуковые сигнализаторы

б) Только датчики движения

в) Только системы видеонаблюдения

г) Детекторы движения, сенсоры дыма, газа, сигнализаторы и центральные блоки

10.Каким образом системы управления освещением входят в состав интегрированных систем охраны?

а) Только для декоративных целей

б) Только для снижения энергопотребления

в) Автоматическое освещение при нарушении безопасности

г) Приводит к увеличению энергопотребления

11. Что включает в себя требования к обновляемости программного обеспечения инженерных средств физической защиты?

а) Только возможность обновления на заводе

б) Возможность удаленного и регулярного обновления программного обеспечения

в) Только использование стандартного программного обеспечения

г) Приводит к снижению эффективности системы

12. Каким образом требования к безопасности работы инженерных средств влияют на обеспечение информационной безопасности предприятия?

а) Обеспечивают защиту от несанкционированного доступа и сохранность данных

б) Снижают безопасность

в) Только усложняют систему безопасности

г) Приводят к увеличению риска инцидентов безопасности

13. Каким образом инженерные конструкции могут предотвращать несанкционированный доступ к системам видеонаблюдения?

а) Только шифрование видеопотока
б) Использование физически защищенных камер и систем контроля доступа в) Только регулярная замена видеокамер
г) Все перечисленное

14. Как инженерные решения могут обеспечивать безопасность рабочих мест сотрудников?

а) Только периодическая проверка документов
б) Использование систем контроля доступа, замков и биометрических устройств
в) Только видеонаблюдение
г) Все перечисленное

15. Что включает в себя информационная база данных систем охранной сигнализации?

а) Только персональные данные сотрудников
б) Информацию о событиях, пользователях, настройках системы, датчиках и устройствах в) Только данные видеонаблюдения
г) Все перечисленное

16. Каким образом информационные системы охранной сигнализации могут обеспечивать аналитику и статистический анализ событий?

а) Только вручную через оператора
б) Автоматический сбор и анализ данных с целью выявления закономерностей и трендов
в) Только путем анализа видеозаписей
г) Все перечисленное

17. Какие технические средства обнаружения входят в класс "датчиков газов"?

а) Только детекторы движения
б) Только датчики температуры
в) Газовые анализаторы и сенсоры детекции вредных газов
г) Все перечисленное

18. Какие технические средства обнаружения относятся к классу "датчиков вибрации"?

а) Только датчики звука
б) Акселерометры и сенсоры вибрации
в) Только инфракрасные датчики движения
г) Все перечисленное

19. Какие принципы лежат в основе построения системы обеспечения безопасности объекта?

а) Только устойчивость системы
б) Проактивность, предсказуемость, принцип обратной связи и распределенности
в) Только действия охранного персонала
г) Все перечисленное

20. Что включает в себя принцип "проактивности" в системах обеспечения безопасности?

а) Предупреждение и предотвращение возможных угроз до их активации б) Только реактивные меры после возникновения события
в) Только обнаружение угроз
г) Все перечисленное

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	б	б	б	а
2	а	а	б	а
3	а	а	а	а
4	а	г	а	а
5	а	г	а	г
6	а	а	а	а
7	б	б	б	б
8	а	б	а	а
9	а	б	в	г
10	б	а	г	в
11	в	б	б	б
12	б	б	б	а
13	б	а	б	б
14	г	в	б	б
15	в	б	а	б
16	г	б	в	б
17	б	б	г	в
18	б	б	а	б
19	б	в	б	б
20	а	б	б	а

3.7. Типовые задания для промежуточного контроля по

МДК.03. 02 Инженерно-технические средства физической защиты объектов информатизации

1)Вопросы для подготовки к дифференцированному зачету

1. Инженерно-техническая защита
2. Физические средства
3. Аппаратные средства
4. Программные средства
5. Криптографические средства
6. ПК на предмет определения максимального расстояния, при котором информацию можно снять с ПК, физически не подключаясь к нему;
7. Оценивается система видеонаблюдения помещения, где расположен сервер;
8. Проверяются помещения, предназначенные для переговоров, на предмет наличия различных подслушивающих устройств;
9. Производится установка специального оборудования, призванного распознавать подслушивающие устройства
10. Утечки и несанкционированного доступа через технические средства обеспечения

производственной деятельности
11. Детекторы, индикаторы поля и тест-приёмники;
12. Анализаторы проводных коммуникаций;
13. Многофункциональные поисковые приборы;
14. Обнаружители скрытых видеокамер;
15. Нелинейные локаторы;
16. Комплексы радиомониторинга и пеленгования;
17. Средства защиты от утечки акустической информации;
18. Устройства противодействия радиоэлектронным средствам негласной аудиозаписи;
19. Устройства блокирования работы систем проводной, мобильной связи и передачи данных;
20. Устройства защиты от прослушивания телефонных переговоров;
21. Устройства защиты от утечки информации по цепям электропитания (фильтры помехоподавляющие электрические) и заземления;
22. Устройства защиты от утечки информации по каналам ПЭМИН;
23. Устройства хранения, копирования, уничтожения и восстановления информации;
24. Цифровые системы регистрации, звукозаписи и шумоочистки речевых сигналов;
25. Металлодетекторы ручные досмотровые;
26. Металлоискатели поисковые грунтовые, глубинные;
27. Металлодетекторы арочные стационарные досмотровые;
28. Программных средств сбора, анализа и обработки информации;
29. Радиоэкранирующих и радиопоглощающих материалов шумопоглощающих материалов.
30. Комплексное использование технических, программных и организационных средств
31. Информация как объект защиты
32. Требования к защищенности информации
33. Организационные меры защиты информации
34. Оценка вероятного противника
35. Оценка условий решения задачи защиты информации
36. Инженерно-технические меры защиты информации
37. Системы информационной безопасности
38. Принципы построения систем безопасности
39. Защита компьютерной информации
40. Угрозы несанкционированного доступа в сеть
41. Системы информационной безопасности сети
42. Принципы построения систем безопасности сети
43. Аппаратные средства защиты передаваемых данных
44. Разработка системы управления объектом защиты и безопасности
45. Постановка задачи проектирования
46. Анализ объекта защиты
47. Контролируемая зона
48. Возможные каналы утечки информации
49. Разработка политики защиты контролируемой зоны
50. Обеспечение защиты помещения проведения совещаний
51. Обеспечение защиты помещения руководителя
52. Обеспечение защиты помещения серверной
53. Разработка политики безопасности сети и коммуникаций
54. Интернет-шлюз + файерволл как основа системы управления
55. Выбор и конфигурирование аппаратных средств защиты данных
56. Защита данных средствами защиты информации и специального ПО
57. Описание настройки специального программного обеспечения защиты данных
58. Моделирование объектов защиты.

4. Требования к дифференцированному зачету по учебной и (или) производственной практике

Дифференцированный зачет по учебной и (или) производственной практике выставляется с учетом данных аттестационного листа (характеристики профессиональной деятельности обучающегося/студента на практике) с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

4.1. Оценочные материалы

Перечень вопросов к собеседованию по производственной практике

1. Краткая характеристика места практики
2. Требования по защите персональных данных
3. Требования по защите конфиденциальных данных предприятия
4. Системы контроля и управления доступом на предприятии
5. Способы ограничения доступа к информации
6. Признаки наличия вредоносного программного обеспечения
7. Средства защиты информации в компьютерных сетях
8. Средства обнаружения компьютерных атак
9. Способы предупреждения компьютерных атак
10. Программно-аппаратные средства уничтожения информации и носителей информации

4.2. Форма аттестационного листа (из дневника по практике)

АТТЕСТАЦИОННЫЙ ЛИСТ ПО УЧЕБНОЙ/ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

_____

ФИО обучающегося

обучающийся (аяся) на ____ курсе по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем успешно прошел(ла) учебную/производственную практику по профессиональному модулю **ПМ.03 «Защита информации техническими средствами»**
в объеме _____с «___» _____20__г. по «___» _____20___г.

в организации /на предприятии _____

наименование организации/предприятии, юридический адрес

Виды и качество выполнения работ

Виды работ, выполненных обучающимся(ейся) во время практики	Объем работ	Качество выполнения работ (оптимальный/средний/ допустимый уровень)
Итого		

Руководитель от предприятия

_____

(должность, фамилия, имя, отчество)

Дата _____ _____ /_____/
(*подпись*) *Расшифровка подписи*

Руководитель практики от ГБПОУ РД «КППК»

_____

(должность, фамилия, имя, отчество)

Дата _____ _____ /_____/
(*подпись*) *Расшифровка подписи*

5. Структура контрольно-оценочных материалов для экзамена (квалификационного)

Типовое задание для экзаменующегося

Текст задания:

Научно-внедренческое предприятие «Телесистемы» занимается прокладкой компьютерных сетей и разработкой программных комплексов для организаций нашего города. Численность работников в организации «Телесистемы» – примерно 80 человек. Одновременно находится в разработке до 30 проектов. Один разработчик может участвовать в нескольких проектах одновременно, степень секретности для каждого проекта индивидуальна. Одна организация может заказать в «Телесистемах» несколько разработок. В связи с большой востребованностью создаваемых программных продуктов, а также с появлением новых конкурирующих фирм, предоставляющих аналогичные услуги, охране и защите коммерческих секретов уделено усиленное внимание.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 **Данных о защищаемой информации.**

№ Эл. инф**.**	Элементы информации	Гриф КИ	Цена инф, руб.	Носитель информации	Местоположение источника информации

Создайте модель защиты в Visio.

6. Ведомость к экзамену квалификационному

ГБПОУ РД «КППК»

ЭКЗАМЕНАЦИОННАЯ ВЕДОМОСТЬ

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Профессиональный модуль ПМ.03 Защита информации техническими средствами

Дата проведения _____

ФИО обучающегося _____

Экзаменационный билет _____

Коды проверяемых компетенций	Основные показатели оценки результата	Формы и методы контроля и оценки	Соответствие/ не соответствие показателю (+/-)	Оценка (зачтено / не зачтено)
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Оценка результатов выполнения заданий Экспертная оценка документов производственной практики		
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики		

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики		
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики		
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики		
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	~ распознает задачу и/или проблему в профессиональном контексте; ~ анализирует задачу и/или проблему и выделяет её составные части; ~ определяет этапы решения задачи; ~ выявляет и осуществляет поиск информации, необходимой для решения задачи и/или проблемы; ~ составляет план действия; определяет необходимые ресурсы; ~ владеет актуальными методами работы в профессиональной и смежных сферах; ~ реализует составленный план; ~ оценивает результат и последствия своих действий, выделяет в нём сильные и слабые стороны	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач Экспертная оценка документов по учебной и производственной практике Экспертная оценка курсового проекта		

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	~ определяет задачи поиска информации; ~ определяет необходимые источники информации; ~ планирует процесс поиска; ~ структурирует получаемую информацию в соответствии с параметрами поиска; ~ выделяет наиболее значимое в перечне информации; ~ оценивает практическую значимость результатов поиска; ~ интерпретирует полученную информацию в контексте профессиональной деятельности; ~ оформляет результаты поиска	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач Экспертная оценка документов по учебной и производственной практике		
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	~ использует актуальную нормативно-правовую документацию по специальности; ~ применяет современную научно профессиональную терминологию; ~ определяет актуальность нормативно-правовой документации в профессиональной деятельности; ~ выстраивает траектории профессионального и личностного развития; ~ участвует в конкурсах профессионального мастерства; ~ участвует в мероприятиях профессиональной направленности (вебинары, семинары, конференции, круглые столы, форумы и т.д.)	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка портфолио. Экспертная оценка документов по учебной и производственной практике		
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	~ участвует в деловом общении для эффективного решения деловых задач; ~ планирует профессиональную деятельность; ~ организует работу коллектива и команды; ~ взаимодействует с коллегами, руководством, клиентами; ~ при групповом обсуждении задает вопросы для понимания идей других; ~ при групповом обсуждении: убеждается, что коллеги по группе поняли предложенную идею; ~ участвует в деятельности по выявлению ресурсов команды; ~ анализирует работу членов группы; ~ анализирует результаты выполненного задания; ~ презентует результаты работы группы; ~ защищает полученные командой результаты	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Наблюдение за выполнением групповых проектных работ. Экспертная оценка документов по учебной и производственной практике		

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	~ грамотно (устно и письменно) излагает свои мысли по профессиональной тематике на государственном языке; ~ проявляет толерантность в рабочем коллективе; ~ извлекает из устной речи (монолог, диалог, дискуссия) нужную информацию и логические связи, организующие эту информацию; ~ грамотно оформляет документы на государственном языке; ~ корректно общается с преподавателями и одногруппниками; соблюдает заданный жанр высказывания (служебный доклад, выступление на совещании / собрании, презентация товара / услуг);	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач. Экспертная оценка		
	~ корректно отвечает на вопросы, направленные на выяснение мнения (позиции); ~ задает четко сформулированные вопросы, направленные на получение необходимой информации.	документов по учебной и производственной практике. Экспертная оценка курсового проекта		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	~ соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; ~ понимать значимость своей специальности; ~ демонстрирует поведение на основе общечеловеческих ценностей	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка документов по учебной и производственной практике		
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	~ эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; ~ использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте.	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка документов по учебной и производственной практике		

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	~ эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик ~ участие в спортивных мероприятиях и/или мероприятиях направленных на формирование здорового образа жизни	Наблюдение за обучающимся во время прохождения учебной и производственной практики. Экспертная оценка портфолио		
ОК 09. Использовать информационные технологии в профессиональной деятельности	~ ориентируется в информационно-коммуникационных технологиях, применяемых в профессиональной деятельности; ~ применяет средства информатизации и информационных технологий для реализации профессиональной деятельности; ~ в профессиональной деятельности использует современное программное обеспечение; ~ представляет информацию в различных формах с использованием	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач.		
	~ разнообразного программного обеспечения; ~ способен адаптироваться в новых программных продуктах.	Экспертная оценка документов по учебной и производственной практике. Экспертная оценка курсового проекта		
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	~ понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); ~ понимает тексты на базовые профессиональные темы; ~ применяет в профессиональной деятельности инструкции на государственном и иностранном языке; ~ строит простые высказывания о себе и о своей профессиональной деятельности; ~ пишет простые связные сообщения на знакомые или интересующие профессиональные темы	Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач.		

Оценка результатов освоения
ПМ.03 Защита информации техническими средствами

Вид профессиональной деятельности «Защита информации техническими средствами»

Освоен с оценкой/не освоен

Председатель: _____ (И.О.Фамилия)

_____ (И.О.Фамилия)

_____ (И.О.Фамилия)