

государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»

Утверждаю

Заместитель директора



(О.В.Князева)

**КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ**

ПМ.03 Защита информации техническими средствами

основной образовательной программы
по специальности

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рабочей программы профессионального модуля ПМ.03 Защита информации техническими средствами.

Разработчик(и):

<u>ГБПОУ «ПХТТ»</u> (место работы)	<u>преподаватель</u> (должность)	<u>Л.М.Акбулякова</u> (И.О.Фамилия)
<u>ГБПОУ «ПХТТ»</u> (место работы)	<u>преподаватель</u> (должность)	<u>Е.А.Соковнина</u> (И.О.Фамилия)

Одобрено на заседании предметно-цикловой комиссии

Информационных технологий и программирования

Протокол № 9 от « 13 » 06 20 18 г

Председатель ПЦК Е.А. Соковнина

СОДЕРЖАНИЕ

Общие положения	4
1. Формы контроля и оценивания элементов профессионального модуля	4
2. Результаты освоения модуля, подлежащие проверке на экзамене (квалификационном).....	5
2.1. Общие/профессиональные компетенции, проверяемые дополнительно:.....	8
2.2. Требования к портфолио	9
3. Оценка освоения профессионального модуля.....	10
3.1. Типовые задания для текущего контроля по МДК.03.01. Техническая защита информации 10	
3.2. Типовые задания для рубежного контроля по МДК.03.01. Техническая защита информации 13	
3.3. Типовые задания для промежуточного контроля по МДК.03.01. Техническая защита информации	17
3.4. Типовые задания для текущего контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации:	18
3.5. Типовые задания для рубежного контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации:	20
3.6. Типовые задания для промежуточного контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	23
4. Требования к дифференцированному зачету по учебной и (или) производственной практике	25
4.1. Оценочные материалы.....	25
4.2. Форма аттестационного листа (из дневника по практике).....	26
5. Структура контрольно-оценочных материалов для экзамена (квалификационного).....	27
6. Ведомость к экзамену квалификационному	28

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 модулю является экзамен (квалификационный). Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

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.02.01. Программные и программно-аппаратные средства защиты информации	Дифференцированный зачет (6 семестр) Экзамен (7 семестр)	Тестирование Контрольная работа	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Тестирование; Контроль выполнения самостоятельной работы;
МДК.02.02 Криптографические средства защиты информации	Дифференцированный зачет (6 семестр)	Тестирование	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Контроль выполнения самостоятельной работы;
УП. 02	Дифференцированный зачет (7 семестры)	-----	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП 02	Дифференцированный зачет (8 семестр)	-----	Оценка выполнения работ и оформления отчетной документации на производственной практике

Профессиональный модуль ПМ.02	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	<ul style="list-style-type: none"> – 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

	<p>решения задачи и/или проблемы;</p> <ul style="list-style-type: none"> – 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
<p>ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности</p>	<ul style="list-style-type: none"> – 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
<p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие</p>	<ul style="list-style-type: none"> – 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.)
<p>ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами</p>	<ul style="list-style-type: none"> – участвует в деловом общении для эффективного решения деловых задач; – планирует профессиональную деятельность; – организует работу коллектива и команды; – взаимодействует с коллегами, руководством, клиентами;

	<ul style="list-style-type: none"> - 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
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста</p>	<ul style="list-style-type: none"> - 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.
<p>ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.</p>	<ul style="list-style-type: none"> - соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; - понимать значимость своей специальности; - демонстрирует поведение на основе общечеловеческих ценностей
<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.</p>	<ul style="list-style-type: none"> - эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; - использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте.

<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.</p>	<ul style="list-style-type: none"> - 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
<p>ОК 09. Использовать информационные технологии в профессиональной деятельности</p>	<ul style="list-style-type: none"> - 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.
<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке</p>	<ul style="list-style-type: none"> - 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		
		Портфолио	Курсовое проектирование	Промежуточная аттестация по практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – пояснительная записка оформлена грамотно на государственном языке; – выдержан научный стиль изложения материала; 	-	+	-
ОК 09. Использовать информационные технологии в профессиональной деятельности	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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.

2) Типовой тест для рубежного контроля

I. Физические средства защиты информации. Выберите один из 4 вариантов ответа:

- 1) средства, которые реализуются в виде автономных устройств и систем
- 2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- 3) это программы, предназначенные для выполнения функций, связанных с защитой информации
- 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

II. Технические средства защиты информации. Выберите один из 4 вариантов ответа:

- 1) средства, которые реализуются в виде автономных устройств и систем
- 2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- 3) это программы, предназначенные для выполнения функций, связанных с защитой информации
- 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

III. Утечка информации. Выберите один из 3 вариантов ответа:

- 1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- 2) ознакомление постороннего лица с содержанием секретной информации
- 3) потеря, хищение, разрушение или неполучение переданных данных

IV. Под изоляцией и разделением (требование к обеспечению ИБ) понимают. Выберите один из 2 вариантов ответа:

- 1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
- 2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

V. Виды технической разведки (по месту размещения аппаратуры). Выберите несколько из 7 вариантов ответа:

- 1) космическая
- 2) оптическая
- 3) наземная
- 4) фотографическая

- 5) морская
- 6) воздушная
- 7) магнитометрическая

VI. Основные группы технических средств ведения разведки. Выберите несколько из 5 вариантов ответа:

- 1) радиомикрофоны
- 2) фотоаппараты
- 3) электронные "уши"
- 4) дистанционное прослушивание разговоров
- 5) системы определения местоположения контролируемого объекта

VII. Инженерно-техническая защита –это

Запишите ответ _____

VIII. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

- 1) угрозой;
- 2) опасностью;
- 3) намерением;
- 4) предостережением.

IX. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ:

X.

XI. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

- 1) операционной системы, сетевого программного обеспечения
- 2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
- 3) операционной системы, системы управления базами данных;
- 4) сетевого программного обеспечения и системы управления базами данных.

XII. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

- 1) системой угроз;
- 2) системой защиты;
- 3) системой безопасности;
- 4) системой уничтожения.

XIII. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?
Запишите ответ:

XIV. Выделите группы, на которые делятся средства защиты информации:

- 1) физические, аппаратные, программные, криптографические, комбинированные;
- 2) химические, аппаратные, программные, криптографические, комбинированные;
- 3) физические, аппаратные, программные, этнографические, комбинированные;

XV. По функциональному назначению средства инженерно-технической защиты делятся на следующие группы :

Продолжите ответ _____

XVI. Надежным средством отвода наведенных сигналов на землю служит
Запишите ответ:

XVII. Установите соответствие
Укажите соответствие для всех 2 вариантов ответа:

- 1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
- 2) наука скрывающая содержимое секретного сообщения
__ стеганография
__ криптография

XVIII. Контроль доступа к информации обеспечивается последовательным использованием таких методов защиты информации...

Продолжите _____

XIX. Технический канал утечки информации...

Продолжите _____

XX. Укажите соответствие для всех 4 вариантов ответа:

- 1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
- 2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
- 3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

- защита информации от утечки по акустическому каналу
- Защита информации от утечки по визуально-оптическому каналу
- Защита информации от утечки по электромагнитным каналам
- Защита информации от утечки по материально-вещественному каналу

XXI. Разновидности угроз безопасности. Выберите несколько из 6 вариантов ответа:

- 1) техническая разведка
- 2) программные
- 3) программно-математические
- 4) организационные
- 5) технические
- 6) физические

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.

3.4. 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.

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

1)Типовой рубежный тест

- I. Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

1. правовым методам защиты информации

2. организационно-техническим методам защиты информации
 3. организационно-распорядительным методам защиты информации
 4. экономическим методам защиты информации
- II. Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:
1. собственник информации
 2. владелец информации
 3. пользователь
- III. Форма допуска, требуемая для работы со сведениями особой важности является:
1. первой формой допуска
 2. второй формой допуска
 3. третьей формой допуска
- IV. Форма допуска, требуемая для работы с совершенно секретными сведениями является:
1. первой формой допуска
 2. второй формой допуска
 3. третьей формой допуска
- V. Форма допуска, требуемая для работы с секретными сведениями является:
1. первой формой допуска
 2. второй формой допуска
 3. третьей формой допуска
- VI. В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:
1. каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
 2. каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания
 3. каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска
- VII. Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:
1. незаконного оборота информации
 2. взлома информации
 3. несанкционированного использования информации
- VIII. Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:
1. дезинформация

2. легендирование
 3. шпионаж
- IX. Какое направление защиты в основном применяется для охраны материальных ценностей?
1. инженерно-техническая
 2. организационно-техническая
 3. организационно-распорядительная
 4. нормативно-правовая
 5. экономическая
- X. Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?
1. контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
 2. инфракрасный светодиод лазерного принтера, посылающий кратковременные
 3. вспышки на электризованную поверхность фоточувствительного барабана
 4. модулированный по силе тока поток электронов, засвечивающий в определенном
 5. порядке пиксели люминофора электронно-лучевой трубки
 6. экран компьютерного монитора и глаза пользователя
 7. оптический канал связи
 8. все варианты могут быть отнесены к техническим каналам связи
- XI. Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?
1. визуально-оптический канал
 2. электромагнитный канал
 3. виброакустический канал
 4. материально-вещественный канал
- XII. Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:
1. визуально-оптического канала
 2. электромагнитного канала
 3. виброакустического канала
 4. материально-вещественного канала
- XIII. Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?
1. визуально-оптический канал
 2. электромагнитный канал
 3. виброакустический канал
 4. материально-вещественный канал
- XIV. Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радицепей

(линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

XV. Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

XVI. Примером какого канала утечки информации служит звук голоса человека?

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

XVII. По какому признаку делят на классы средства технической разведки (СТР) ?

1. по дальности канала
2. по форме допуска
3. по мощности
4. по степени финансирования

XVIII. Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле относят к ...

1. первому классу СРТ
2. второму классу СРТ
3. третьему классу СРТ

XIX. Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ...

1. первого класса
2. второго класса
3. третьего класса

3.6. 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 + фаерволл 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/предприятия, 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 «ПХТТ»

(должность, фамилия, имя, отчество)

Дата _____

(подпись)

/ _____ /
Расшифровка подписи

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

Типовое задание для экзаменуемого

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

государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»

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		

<p>ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа</p>	<p>Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа</p>	<p>Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики</p>		
<p>ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p>Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p>Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики</p>		
<p>ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации</p>	<p>Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации</p>	<p>Оценка результатов выполнения заданий Экспертная оценка документов учебной и производственной практики</p>		
<p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам</p>	<ul style="list-style-type: none"> – 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 	<p>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</p>		
<p>ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой</p>	<ul style="list-style-type: none"> – определяет задачи поиска информации; – определяет необходимые источники информации; – планирует процесс поиска; – структурирует получаемую информацию в соответствии с 	<p>Наблюдение за обучающимся во время теоретического обучения и</p>		

<p>для выполнения задач профессиональной деятельности</p>	<ul style="list-style-type: none"> – параметрами поиска; – выделяет наиболее значимое в перечне информации; – оценивает практическую значимость результатов поиска; – интерпретирует полученную информацию в контексте профессиональной деятельности; – оформляет результаты поиска 	<p>прохождения учебной практики. Вопросы по решению ситуационных задач Экспертная оценка документов по учебной и производственной практике</p>		
<p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие</p>	<ul style="list-style-type: none"> – 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.) 	<p>Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Экспертная оценка портфолио. Экспертная оценка документов по учебной и производственной практике</p>		
<p>ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами</p>	<ul style="list-style-type: none"> – 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 	<p>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</p>		
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста</p>	<ul style="list-style-type: none"> – 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); 	<p>Наблюдение за обучающимся во время теоретического обучения и прохождения учебной практики. Вопросы по решению ситуационных задач. Экспертная оценка</p>		

	<ul style="list-style-type: none"> – 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.	<ul style="list-style-type: none"> – 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.	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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.		

	<p>разнообразного программного обеспечения;</p> <ul style="list-style-type: none"> – способен адаптироваться в новых программных продуктах. 	<p>Экспертная оценка документов по учебной и производственной практике. Экспертная оценка курсового проекта</p>		
<p>ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке</p>	<ul style="list-style-type: none"> – 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 	<p>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</p>		

**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)