СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«УТВЕРЖДАЮ»
Директор ЧУ ПО «СТК»
_____ Е. А. Карпова
27.01.2020 г.

Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Цикловая комиссия по информатике и информационной безопасности**

Учебный план 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Учебный год начала подготовки 2020-2021

Квалификация **Техник по защите информации**

Форма обучения **очная**

Часов по учебному плану 290 Виды контроля в семестрах:
в том числе:
аудиторные занятия 168
самостоятельная работа 122

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		**5 (3.1)**		Итого	
Недель	18		13			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	36	36	26	26	62	62
Практические	54	54	52	52	106	106
Итого ауд.	90	90	78	78	168	168
Контактная работа	90	90	78	78	168	168
Сам. работа	84	84	38	38	122	122
Итого	174	174	116	116	290	290

Рабочая программа дисциплины

Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1551)

составлена на основании учебного плана:

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

утвержденного на заседании Педагогического Совета ЧУ ПО "СТК" 26.02.2021 протокол № 3.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	В результате изучения профессионального модуля студент должен освоить основной вид деятельности «Защита информации в информационно-телекоммуникационных системах
1.2	и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты» и соответствующие ему общие компетенции и
1.3	профессиональные компетенции:
1.4	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
1.5	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
1.6	Проводить техническое обслуживание, диагностику , устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
1.7	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
1.8	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	МДК.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Организационное и правовое обеспечение информационной безопасности
2.1.2	Телекоммуникационные системы и сети
2.1.3	Учебная практика
2.1.4	Электроника и схемотехника
2.1.5	14601 "Монтажник оборудования связи"
2.1.6	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)
2.1.7	Инженерная и компьютерная графика
2.1.8	Квалификационный экзамен
2.1.9	Основы алгоритмизации и программирования
2.1.10	Производственная практика
2.1.11	Учебная практика
2.1.12	Физика
2.1.13	Экономика и управление
2.1.14	Электротехника
2.1.15	Безопасность жизнедеятельности
2.1.16	Информатика
2.1.17	История
2.1.18	Математика
2.1.19	Основы информационной безопасности
2.1.20	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)
2.1.21	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК 2.3.: Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	
Знать:	
1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
3	Планировать и реализовывать собственное профессиональное и личностное развитие.
Уметь:	
1	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
2	Использовать информационные технологии в профессиональной деятельности.
3	Пользоваться профессиональной документацией на государственном и иностранном языке
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации;

ПК 2.2.: Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	
Знать:	
1	типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
2	основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	состав и возможности типовых конфигураций программно-аппаратных средств защиты информации
Уметь:	
1	особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах
2	основные способы противодействия
3	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
Владеть:	
1	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
2	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
3	шифрования информации.

ПК 2.1.: Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.	
Знать:	
1	типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
2	основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;
Уметь:	
1	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность
3	производить установку и настройку типовых программно-аппаратных средств защиты информации;
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации;

ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языках.	
Знать:	
1	основные понятия криптографии и типовые криптографические методы защиты информации;
2	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы

3	основные способы противодействия
Уметь:	
1	производить установку и настройку типовых программно-аппаратных средств защиты информации;
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность
3	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем

ОК 09.: Использовать информационные технологии в профессиональной деятельности.	
Знать:	
1	типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
2	основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;
Уметь:	
1	производить установку и настройку типовых программно-аппаратных средств защиты информации;
2	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
3	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации;

ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	
Знать:	
1	особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах
2	основные способы противодействия
3	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
Уметь:	
1	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность
3	производить установку и настройку типовых программно-аппаратных средств защиты
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 04.: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	
Знать:	
1	типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах
2	основные протоколы идентификации и аутентификации в телекоммуникационных системах;
3	состав и возможности типовых конфигураций программно-аппаратных средств защиты информации
Уметь:	

1	выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
3	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
Владеть:	
1	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
2	шифрования информации
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 03.: Планировать и реализовывать собственное профессиональное и личностное развитие.	
Знать:	
1	возможные угрозы безопасности информации в ИТКС;
2	способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё
3	типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
Уметь:	
1	выявлять и оценивать угрозы безопасности информации в ИТКС
2	проводить конфигурирование программных и программноаппаратных, в том числе криптографических средств защиты информации
3	проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации
Владеть:	
1	определения необходимых средств криптографической защиты информации;
2	использования программно-аппаратных криптографических средств защиты информации;
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 02.: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	
Знать:	
1	основные понятия криптографии и типовые криптографические методы защиты информации;
2	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
3	основные способы противодействия
Уметь:	
1	производить установку и настройку типовых программно-аппаратных средств защиты
2	определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
3	пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации
Владеть:	
1	шифрования информации.
2	применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
3	установки, настройки специализированного оборудования криптографической защиты информации

ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	
Знать:	
1	особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
2	основные способы противодействия
3	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы
Уметь:	
1	пользоваться терминологией современной криптографии, использовать типовые

	криптографические средства защиты информации;
2	□ производить установку и настройку типовых программно-аппаратных средств защиты информации;
3	□ определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
Владеть:	
1	□ применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
2	□ шифрования информации.
3	□ определения необходимых средств криптографической защиты информации;

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
3.1.2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
3.1.3	Планировать и реализовывать собственное профессиональное и личностное развитие.
3.1.4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
3.1.5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
3.1.6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
3.1.7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
3.1.8	Использовать информационные технологии в профессиональной деятельности.
3.2	**Уметь:**
3.2.1	установка, монтаж и настройка технических средств защиты информации;
3.2.2	техническое обслуживание технических средств защиты информации;
3.2.3	применение основных типов технических средств защиты информации;
3.2.4	выявление технических каналов утечки информации;
3.2.5	участие в мониторинге эффективности технических средств защиты информации;
3.2.6	диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;
3.2.7	проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации;
3.2.8	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
3.2.9	установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.
3.3	**Владеть:**
3.3.1	применять технические средства для криптографической защиты информации конфиденциального характера;
3.3.2	применять технические средства для уничтожения информации и носителей информации;
3.3.3	применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
3.3.4	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
3.3.5	применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
3.3.6	применять инженерно-технические средства физической защиты объектов информатизации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**
	Раздел 1.		
1.1	Предмет и задачи технической защиты информации. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации /Лек/	4	14

1.2	Основные параметры системы защиты информации /Пр/	4	20
1.3	Основные параметры системы защиты информации /Ср/	4	39
1.4	Общие положения защиты информации техническими средствами. Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации. /Лек/	4	22
1.5	Классификация способов и средств защиты информации. /Пр/	4	34
1.6	Классификация способов и средств защиты информации. /Ср/	4	45
1.7	Информация как предмет защиты.Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. /Лек/	5	6
1.8	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. /Пр/	5	6
1.9	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. /Ср/	5	2
1.10	Технические каналы утечки информации.Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. /Лек/	5	8
1.11	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации /Пр/	5	8
1.12	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации /Ср/	5	2
1.13	Методы и средства технической разведки. Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации. /Лек/	5	2
1.14	Тематика учебных занятий формируется образовательной организацией самостоятельно /Пр/	5	8
1.15	Тематика учебных занятий формируется образовательной организацией самостоятельно /Ср/	5	8
1.16	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей /Лек/	5	6
1.17	Измерение параметров физических полей /Пр/	5	10
1.18	Измерение параметров физических полей /Ср/	5	10
1.19	Физические процессы при подавлении опасных сигналов. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление. /Лек/	5	2
1.20	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. /Пр/	5	10
1.21	Алгоритм разложения произведения двух простых чисел на множители /Ср/	5	8
1.22	Системы защиты от утечки информации по акустическому каналу. Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу /Лек/	5	2

1.23	Защита от утечки по акустическому каналу /Пр/	5	10
1.24	Защита от утечки по акустическому каналу /Ср/	5	2
1.25	/ЗачётСОц/	5	6

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Вопросы для самоконтроля и текущей аттестации

1. Модель угроз НСД на предприятии
2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии
3. Проведение классификации ПО по требованиям ФСТЭК на предприятии
4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии
5. Построение модели нарушителя по требованиям ФСТЭК на предприятии
6. Построение модели нарушителя по требованиям ФСБ на предприятии
7. Модель угроз безопасности ИС персональных данных на предприятии
8. Комплексная модель защиты информации на предприятии.
9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
13. Проблема защиты информации в облачных хранилищах данных и ЦОДах
14. Защита сред виртуализации.

5.2. Темы письменных работ (контрольных и курсовых работ, рефератов)

1. Классификация способов и средств защиты информации.
2. Основные и вспомогательные технические средства, и системы.
3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.
4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.
5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
6. . Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.
7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
8. Технические средства для уничтожения информации и носителей информации, порядок применения.

5.3. Оценочные средства для промежуточной аттестации

1. Монтаж различных типов датчиков.
2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.
3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.
4. Рассмотрение системы контроля и управления доступом.
5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.
6. Рассмотрение датчиков периметра, их принципов работы.
7. Выполнение звукоизоляции помещений системы зашумления.
8. Реализация защиты от утечки по цепям электропитания и заземления.
9. Разработка организационных и технических мероприятий по заданию преподавателя;
10. Разработка основной документации по инженерно-технической защите информации.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.2.1 Перечень программного обеспечения

6.3.1.1	Open Office

6.2.2 Перечень информационных справочных систем и ресурсов сети Интернет

6.3.2.1	http://www.consultant.ru/ Справочная правовая система «КонсультантПлюс».
6.3.2.2	http://biblioclub.ru/ ЭБС «Университетская библиотека online»
6.3.2.3	http://library.tiei.ru/ - ЭЛЕКТРОННАЯ НАУЧНО-ОБРАЗОВАТЕЛЬНАЯ БИБЛИОТЕКА

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа,
7.2	занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и
7.3	индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для
7.4	самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.
7.5	Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения,
7.6	служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного
7.7	типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие
7.8	тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным
7.9	программам дисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены
7.10	компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную
7.11	информационно - образовательную среду

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание -обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Главная задача лекционного курса - сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной стр. 16

работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

При проведении учебных занятий обеспечиваются развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Для контроля знаний студентов по данной дисциплине необходимо проводить оперативный, рубежный и итоговый контроль.

Оперативный контроль осуществляется путем проведения опросов студентов на семинарских занятиях, проверки выполнения практических заданий, а также учета вовлеченности (активности) студентов при обсуждении мини-докладов, организации ролевых игр и т.п.

Контроль за самостоятельной работой студентов по курсу осуществляется в двух формах: текущий контроль и итоговый.

Рубежный контроль (аттестация) подразумевает проведение тестирования по пройденным разделам курса. В тестирование могут быть включены темы, предложенные студентам для самостоятельной подготовки, а также практические задания