Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Карпова Елизавета Александровна
Должность: директор
Дата подписания: 29.11.2023 11:38:06
Уникальный программный ключ:
ad9053b6a9e639199a21a41d1a80dd3f5c4065

СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

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

Инженерная и компьютерная графика

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 49
в том числе:
аудиторные занятия 36
самостоятельная работа 13

Виды контроля в семестрах:
зачеты с оценкой 2

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**2 (1.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	18	18	18	18
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	13	13	13	13
Итого	49	49	49	49

Рабочая программа дисциплины

Инженерная и компьютерная графика

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	Средства инженерной и компьютерной графики;
1.2	□ Методы и приёмы выполнения схем электрического оборудования и объектов сетевой
1.3	инфраструктуры;
1.4	□ Основные функциональные возможности современных графических систем;
1.5	□ Моделирование в рамках графических систем.
1.6	ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
1.7	ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного
1.8	выполнения профессиональных задач, профессионального и личностного развития.
1.9	ОК 5. Использовать информационно-коммуникационные технологии в профессиональной
1.10	деятельности.
1.11	ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
1.12	ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической
1.13	защиты и контроля информации в автоматизированных системах.
1.14	ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов
1.15	плановых и внеплановых контрольных проверок, при аттестации объектов, помещений,
1.16	программ, алгоритмов.
1.17	ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов
1.18	плановых и внеплановых контрольных проверок, при аттестации объектов, помещений,
1.19	технических средств.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	ОПЦ
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
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты
2.2.2	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
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	□ возможные угрозы безопасности информации в ИТКС;
3.1.2	□ способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
3.1.3	□ типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
3.1.4	□ криптографические средства защиты информации конфиденциального характера, которые применяются в информационнотелекоммуникационных системах и сетях;
3.1.5	□ порядок тестирования функций программных и программноаппаратных, в том числе криптографических средств защиты информации;
3.1.6	□ организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
3.1.7	□ порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации
3.2	**Уметь:**
3.2.1	□ выявлять и оценивать угрозы безопасности информации в ИТКС;
3.2.2	□ настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
3.2.3	□ проводить установку и настройку программных и программноаппаратных, в том числе криптографических средств защиты информации;
3.2.4	□ проводить конфигурирование программных и программноаппаратных, в том числе криптографических средств защиты информации;
3.2.5	□ проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
3.2.6	□ проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
3.2.7	□ проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации
3.3	**Владеть:**
3.3.1	□ установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
3.3.2	□ поддержании бесперебойной работы программных и программноаппаратных в том числе криптографических средств защиты информации в ИТКС;
3.3.3	□ защите информации от НСД и специальных воздействий в ИТКС с
3.3.4	использованием программных и программно-аппаратных в том числе
3.3.5	криптографических средств защиты в соответствии с предъявляемыми
3.3.6	требованиями

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**
	Раздел 1.		
1.1	Виды, содержание и форма конструкторских документов. Государственные нормы, определяющие качество конструкторских документов. /Лек/	2	4
1.2	Оформление чертежей: стандарты (ЕСКД); форматы чертежей основные и дополнительные их размеры и обозначение (ГОСТ 2.301-68); основная надпись чертежа её форма, размеры, порядок заполнения основных надписей и дополнительных граф (ГОСТ 2.104-68); масштабы (ГОСТ 2.302-68); линии чертежа и их конструкция (ГОСТ 2.303-68 /Пр/	2	4
1.3	1 Ознакомиться с ГОСТами: ГОСТ 2.301 – 68 Размеры основных форматов чертежных листов; ГОСТ 2.307 - 68 Определения и стандартные масштабы;ГОСТ 2.104 - 68 Форма, содержание и размеры граф основной надписи. 2 Выполнить упражнения в рабочей тетради: □ заполнить таблицу форматов □ вычертить деталь в заданном масштабе; □ вычертить разные типы линий чертежа /Ср/	2	1
1.4	Введение в автоматизированную систему программирования КОМПАС-ГРАФИК /Лек/	2	2
1.5	Выполнение упражнений с использованием АСП КОМПАС-ГРАФИК /Пр/	2	2
1.6	Повторить материал, изложенный в конспекте /Ср/	2	1
1.7	Шрифты чертёжные Содержание учебного материала ГОСТ 2. 304-68 /Лек/	2	2
1.8	Типы чертёжных шрифтов, их параметры (размер шрифта, толщина линии шрифта), конструкция прописных и строчных букв, цифр и знаков шрифта типа Б с углом наклона 750 Заполнение основной надписи с использованием АСП КОМПАС-ГРАФИК /Пр/	2	2
1.9	Упражнение в рабочей тетради. Выполнить буквы, цифры и надписи чертежным шрифтом типа Б с наклоном 750 /Ср/	2	1
1.10	Нанесение размеров на чертежах. ГОСТ 2.307.81, ГОСТ 2.3318-8 /Лек/	2	2
1.11	Основные правила нанесения размеров по ГОСТу на чертежах. Нанесение размеров с использованием АСП КОМПАС-ГРАФИК /Пр/	2	2
1.12	Практическая работа №1 Контур детали /Ср/	2	1
1.13	Геометрические построения и правила вычерчивания контуров технических деталей /Лек/	2	2
1.14	Геометрические построения и правила вычерчивания контуров технических деталей Сопряжение линий /Пр/	2	2
1.15	Изучить материал, изложенный в конспекте. Упражнение в рабочей тетради. Выполнить построение сопряжений, коробовых и лекальных кривых /Ср/	2	1
1.16	Ортогональное проецирование. /Лек/	2	2
1.17	Методы получения изображений и методы проецирования; Проецирование точки на три плоскости проекции. Комплексный чертеж точки /Пр/	2	2
1.18	Выполнить упражнения рабочей тетради: «Проецирование точки», «Проецирование прямой линии». /Ср/	2	2
1.19	Аксонометрические проекции /Лек/	2	2
1.20	Общие понятия об аксонометрических проекциях. Виды аксонометрических проекций: прямоугольные (изометрическая и диметрическая). Аксонометрические оси. Показатели искажения. Аксонометрические проекции плоскостей и окружностей. Построение изометрических проекций плоскости и окружности с использованием АСП КОМПАС-ГРАФИК /Пр/	2	2

1.21	Выполнить упражнение в рабочей тетради /Ср/	2	2
1.22	Проецирование геометрических тел /Лек/	2	2
1.23	Графическая работа №3 Геометрические тела.Г /Пр/	2	2
1.24	Выполнить упражнение в рабочей тетради. Изучить материал, изложенный в конспекте /Ср/	2	2
1.25	/ЗачётСОц/	2	2

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)

Проблемы обеспечения безопасности операционных систем.
2. Технологии аутентификации.
3. Аутентификация, авторизация и администрирование действий пользователя.
4. Пароли.
5. PIN-коды.
6. Методы надежного составления паролей.
7. Токены.
8. Смарт-карты.
9. Виртуальные ключи.
10. Программно-аппаратные модули доверенной загрузки.
11. АПМДЗ Криптон –Замок системный администратор.
12. Изучение настроек системного администратора АПМДЗ.
13. Сектор НЖМД.
14. Область памяти.
15. Файл, папка, каталог.
16. Разграничение доступа к объектам операционной системы.
17. Комплексная система организации управления доступом.
18. Инсталляция. Настройка.
19. Аудит безопасности операционной системы.
20. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.
52
20
21. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.
22. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ.
23. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
24. Концепция построения виртуальных защищенных сетей;.
25. Виртуальные защищенные сети.
26. Туннелирование.
27. Инкапсуляция пакетов.
28. Структура защищенного пакета.
29. Варианты построения защищенных каналов.
30. Защита на канальном уровне.
31. ПротоколыPPTP, L2F, L2TP.
32. Протоколы формирования защищенных каналов на сеансовом уровне.

33. Протоколы SSL, TLS, SOCKS.
34. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.
35. Защита на прикладном уровне.
36. Протоколы PAP, CHAP, S/Key, SSO, Kerberos.
38. Функционирование системы управления средствами защиты.
39. Аудит безопасности информационной системы.

5.3. Оценочные средства для промежуточной аттестации

Введение. Выдача заданий
2 Анализ поставленной задачи
3 Определение защищаемых информационных активов. Категорирование информации
4 Определение уязвимостей и угроз
5 Анализ и выбор возможных решений по защите
6 Анализ механизмов защиты
7 Анализ требуемых компонентов
8 Проектирование модели угроз
9 Настройка компонентов защиты
10 Конфигурирование пользовательских задач
11 Проектирование эксперимента по внедрению системы защиты
12 Нормативно-правовое обеспечение проекта
13 Расчет индекса ROSI
14 Подготовка пояснительной записки к курсовому проекту
15 Защита курсового проекта

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