

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная
безопасность»

Автор Голдовский Яков Михайлович, к.т.н.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Техническая защита информации

Направление подготовки:	<u>10.03.01 – Информационная безопасность</u>
Профиль:	<u>Безопасность компьютерных систем</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2018</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">Н.А. Клычева</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p>Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Б.В. Желенков</p>
---	--

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Техническая защита информации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих задач.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Проектно-технологическая деятельность:

- сбор и анализ исходных данных для обеспечения информационной безопасности с помощью средств технической защиты информации;
- разработка проектной и рабочей документации, оформление отчетов по законченным проектно-конструкторским работам;
- контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам.

Экспериментально-исследовательская деятельность:

- анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- подготовка данных и составление обзоров, рефератов, отчетов, научных публикаций и докладов на международных конференциях и семинарах, участие во внедрении результатов исследований и разработок.

Эксплуатационная деятельность:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Организационно-управленческая деятельность

- организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
- осуществление правового, организационного и технического обеспечения защиты информации;

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Техническая защита информации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Информатика:

Знания: современное состояние уровня и направлений развития вычислительной техники и программных средств, основные алгоритмы типовых численных методов решения математических задач, языки программирования, структуру локальных и глобальных компьютерных сетей

Умения: работать в качестве пользователя персонального компьютера, использовать внешние носители информации для обмена данными между машинами, создавать резервные копии данных и программ, использовать языки и системы программирования, работать с программными средствами общего назначения; использовать основные приемы обработки экспериментальных данных, подготовить проектно-конструкторскую документацию разрабатываемых изделий и устройств с применением электронно-вычислительных машин

Навыки: методами поиска и обмена информацией в глобальных и локальных компьютерных сетях, техническими и программными средствами защиты информации при работе с компьютерными сетями, включая навыки работы с программными средствами общего назначения, соответствующими современным требованиям мирового рынка, включая приемы антивирусной защиты.

2.2. Наименование последующих дисциплин

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации	<p>Знать и понимать: структуру отрасли, перечислять основные организации работающие в области информационной безопасности; знать принципы поиска и оценки информации; профессиональную терминологию в области информационной безопасности.</p> <p>Уметь: оценивать различные варианты реализации защиты данных в современных информационных системах.</p> <p>Владеть: навыками сбора и анализа данных, давать оценку произведенной работе, составлять суждение по вопросам информационной безопасности</p>
2	ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	<p>Знать и понимать: состав и назначение компонентов системы защиты информации, основные угрозы информационной безопасности и методы защиты от них; объяснять взаимосвязь объектов в информационной системе.</p> <p>Уметь: оценивать степень угрозы информационной безопасности для объекта и системы; использовать соответствующие методы защиты против наиболее вероятных видов атак.</p> <p>Владеть: основными приемами организации комплексной системы информационной безопасности, включая организационное, правовое и техническое обеспечение.</p>
3	ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	<p>Знать и понимать: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации.</p> <p>Уметь: проверять работоспособность элементов системы защиты с помощью необходимых технических средств</p> <p>Владеть: навыками по установке, настройке и обслуживанию технических средств защиты информации.</p>
4	ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	<p>Знать и понимать: принципы поиска и оценки информации; профессиональную терминологию в области информационной безопасности.</p> <p>Уметь: использовать средства глобальной сети и традиционные методы поиска информации находить и критически оценивать данные по вопросам информационной безопасности</p> <p>Владеть: : навыками анализа и обобщения данных, в том числе информации по проблемам информационной безопасности</p>

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 6
Контактная работа	48	48,15
Аудиторные занятия (всего):	48	48
В том числе:		
лекции (Л)	16	16
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	32	32
Самостоятельная работа (всего)	33	33
Экзамен (при наличии)	27	27
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	6	Раздел 1 РАЗДЕЛ 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ	2	6/3			6	14/3	
2	6	Тема 1.1 Тема 1.1. Основные понятия. Введение. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные.	2					2	
3	6	Раздел 2 РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	2	6/3			6	14/3	ПК1, Выполнение лаб.работ 20%
4	6	Тема 2.1 Тема 2.1. Природа возникновения угроз. Классификация угроз по преднамеренности проявления. Классификация по источнику угрозы. Классификация по степени воздействия на информационную систему. По способам доступа к ресурсам информационной системы.	2					2	
5	6	Раздел 3 РАЗДЕЛ 3. ПОЛИТИКА БЕЗОПАСНОСТИ	2	6/3			6	14/3	
6	6	Тема 3.1 Тема 3.1. Структура политики безопасности.	2					2	
7	6	Раздел 4 РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА	4	6/3			6	16/3	
8	6	Тема 4.1 Тема 4.1. Классификация криптографических алгоритмов. Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы.	2					2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
9	6	Тема 4.3 Тема 4.3. Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.	2					2	
10	6	Раздел 5 РАЗДЕЛ 5. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.	2	4/2			5	11/2	
11	6	Тема 5.1 Тема 5.1. Аутентификация, авторизация и администрирование действий пользователей.	2					2	
12	6	Раздел 6 РАЗДЕЛ 6. ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.	4	4/2			4	12/2	ПК2, Выполнение лаб. работ 80%
13	6	Тема 6.2 Тема 6.2. Цифровые сертификаты.. Виртуальная частная сеть.	2					2	
14	6	Тема 6.3 Тема 6.3. Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.	2					2	
15	6	Раздел 7 Итоговая информация						27	ЭК
16		Тема 1.2 Тема 1.2. Государственные структуры, отвечающие за защиту данных. Определение служебной тайны. Законодательство РФ в области информационной безопасности. Информационная безопасность коммерческой структуры. Типовой набор должностей, связанных с защитой данных на предприятии.;							
17		Тема 1.3 Тема 1.3. Международные стандартизирующие организации. Стандарты РФ в области информационной безопасности..							
18		Тема 2.2 Тема 2.2 Угрозы безопасности информационной системы.							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
19		Тема 2.3 Тема 2.3. Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам.							
20		Тема 3.2 Тема 3.2. Базовая политика безопасности.							
21		Тема 3.3 Тема 3.3 Специализированные политики безопасности.							
22		Тема 4.2 Тема 4.2. Симметричные криптоалгоритмы. Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования.							
23		Тема 5.2 Тема 5.2. Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA.							
24		Тема 5.3 Тема 5.3. Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран.							
25		Тема 6.1 Тема 6.1. Защита http-трафика. Характерные угрозы. Защищенный протокол httpd.							
26		Всего:	16	32/16			33	108/16	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 32 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	6	РАЗДЕЛ 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ	Стандарты и организации, работающие в области информационной безопасности.	6 / 3
2	6	РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Угрозы информационной безопасности	6 / 3
3	6	РАЗДЕЛ 3. ПОЛИТИКА БЕЗОПАСНОСТИ	Разработка политики безопасности	6 / 3
4	6	РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА	Шифрование и дешифровка	6 / 3
5	6	РАЗДЕЛ 5. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.	Защита от несанкционированного доступа	4 / 2
6	6	РАЗДЕЛ 6. ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.	Защита информации в глобальной сети.	4 / 2
ВСЕГО:				32/16

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы по дисциплине учебным планом не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины "Техническая защита информации" осуществляется в форме лекций, лабораторных занятий и выполнения курсового проекта.

Лекции проводятся в традиционной классно-урочной организационной форме в объеме 36 часов, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).

Лабораторный практикум (36 часов) проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения.

Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (49 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически заверченный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	6	РАЗДЕЛ 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ	1. Изучение стандартов в области информационной безопасности 2. Анализ и дополнительная проработка материала.3. Подготовка к лабораторным работам.4. Изучение учебной литературы из приведенных источников: [1, стр.1-6], [2 стр. 1-8], [3, стр. 1-3].	6
2	6	РАЗДЕЛ 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	1. Обзор существующих вирусов, троянских программ и сетевых червей. 2. Анализ и дополнительная проработка материала. 3. Подготовка к лабораторным работам.4. Изучение учебной литературы из приведенных источников: [1, стр.7-12], [2 стр. 9-16], [3, стр. 1-3].	6
3	6	РАЗДЕЛ 3. ПОЛИТИКА БЕЗОПАСНОСТИ	. Анализ и дополнительная проработка материала. 2. Разработка политики безопасности отдела. 3. Подготовка к лабораторным работам.4. Изучение учебной литературы из приведенных источников: [1, стр.13-18], [2 стр. 17-24], [3, стр. 1-3].	6
4	6	РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА	. Анализ и дополнительная проработка материала. 2. Разработка политики безопасности отдела. 3. Подготовка к лабораторным работам.4. Изучение учебной литературы из приведенных источников: [1, стр.13-18], [2 стр. 17-24], [3, стр. 1-3].	6
5	6	РАЗДЕЛ 5. ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.	1. Обзор протоколов аутентификации. 2. Анализ и дополнительная проработка материала. 3. Подготовка к лабораторным работам.4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3].	5
6	6	РАЗДЕЛ 6. ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ.	1. Обзор стандартов рамочного протокола IPSec. 2. Анализ и дополнительная проработка материала. 3. Подготовка к лабораторным работам.4. Изучение учебной литературы из приведенных источников: [1, стр.31-36], [2 стр. 41-48], [3, стр. 1-3].	4
ВСЕГО:				33

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Криптографическая защита компьютерной информации	Я.М. Голдовский, Б.В. Желенков, И.Е. Сафонова	М.:МИИТ, 2013 -36 с, 2013	Раздел 1, Раздел 2, Раздел 3, Раздел 4, Раздел 5, Раздел 6
2	Канальный уровень модели OSI	Б.В. Желенков	М.:МИИТ, 2011 -49 с, 2011	Раздел 1, Раздел 2, Раздел 3, Раздел 4, Раздел 5, Раздел 6

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Защита информации в вычислительных системах	В.И. Морозова, К.Э. Врублевский	М.:МИИТ, 2008 -122 с, 2008	Раздел 1, Раздел 2, Раздел 3, Раздел 4, Раздел 5, Раздел 6

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- Форум специалистов по информационным технологиям <http://citforum.ru/>
- Интернет-университет информационных технологий <http://www.intuit.ru/>
- Тематический форум по информационным технологиям <http://habrahabr.ru/>

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

MicrosoftWindows

MicrosoftOffice

Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

MicrosoftWindows

MicrosoftOffice

Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

№1329

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ
№1330

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран, 25 персональных компьютеров, 25 мониторов, 1 принтер, доска учебная.

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ
№1120

АРМ №7AN0AS423434 в составе:

- ноутбук Asus A7SV;
- адаптер питания;
- манипулятор «мышь»;
- телевизор Philips.

Средство защиты от НСД Dallas Lock 8.0-C

Устройство защиты объектов информатизации от утечки по техническим каналам «Соната-Р2»

Система виброакустической и акустической защиты «Соната-АВ» (модель 3М) в составе:

- генераторный блок «Соната-АВ»;
- аудиоизлучатель «АИ-65»;
- виброизлучатели «ВИ-45» - 8 шт.;
- виброизлучатели «ПИ-45» - 9 шт..

11. 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:

- познавательно-обучающая;
- развивающая;
- ориентирующе-направляющая;
- активизирующая;
- воспитательная;
- организующая;
- информационная.

Выполнение практических занятий 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 органичному дополнению лекционных курсов и самостоятельной 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 специалиста важна 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.

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.

Каждому студенту следует составлять еженедельный семестровый план работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были – по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной работы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к зачету и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.