

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

25 мая 2018 г.



Кафедра «Управление и защита информации»

Автор Алексеев Виктор Михайлович, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

**Защита информации в телекоммуникационных системах
железнодорожного транспорта**

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2018

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 16 15 мая 2018 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
---	---

Рабочая программа учебной дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: Заведующий кафедрой Баранов Леонид Аврамович
Дата: 15.05.2018

Москва 2018 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Защита информации в телекоммуникационных системах железнодорожного транспорта» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 «Компьютерная безопасность». Дисциплина «Защита информации в телекоммуникационных системах железнодорожного транспорта» относится к числу дисциплин специализации ПСК-8 профессионального цикла.

Целью преподавания дисциплины «Защита информации в телекоммуникационных системах железнодорожного транспорта» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС.

Задачами изучения дисциплины являются:

изучение основ устройства и принципов функционирования,

методологии проектирования и построения защищенных,

критериев и методов оценки защищенности КС,

средств и методов защиты от несанкционированного доступа (НСД) к информации.

Основной целью изучения учебной дисциплины «Защита информации в телекоммуникационных системах железнодорожного транспорта» является формирование у обучающегося компетенций для следующих видов деятельности:

- научно-исследовательской;

- проектной.

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

Научно-исследовательская деятельность:

сбор, обработка, анализ и систематизация научно-технической информации,

отечественного и зарубежного опыта по проблемам компьютерной безопасности;

участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах.

Проектная деятельность:

разработка и конфигурирование программно-аппаратных средств защиты информации;

разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов;

разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием;

проектирование программных и аппаратных средств защиты информации в соответствии с техническим заданием с использованием средств автоматизации проектирования.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Защита информации в телекоммуникационных системах железнодорожного транспорта" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Администрирование и управление Информационной безопасности компьютерных систем:

Знания: операционные системы ЛВС

Умения: уметь работать на удаленном компьютере

Навыки: методами обеспечения безопасности КС

2.1.2. Аппаратные средства вычислительной техники:

Знания: аппаратные средства компьютеров

Умения: конфигурировать аппаратные средства

Навыки: методами проектирования аппаратных средств

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-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований;	<p>Знать и понимать: классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации; основные принципы администрирования защищенных компьютерных систем; особенности реализации методов защиты информации современными программно-аппаратными средствами.</p> <p>Уметь: применять стандарты по оценке защищенности КС при анализе и проектировании систем защиты информации в КС.</p> <p>Владеть: методами подготовки обзоров и информацией по подготовке научных отчетов.</p>
2	ПК-7 способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем;	<p>Знать и понимать: технологии обнаружения компьютерных атак и их возможности; основные уязвимости и типовые атаки на современные компьютерные системы; возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности; методы защиты компьютерных сетей.</p> <p>Уметь: проводить анализ телекоммуникационных систем с точки зрения обеспечения информационной безопасности, разрабатывать модели и политику безопасности; уметь выполнять функции администратора безопасности защищенных компьютерных систем.</p> <p>Владеть: средствами администрирования сетевых программно-аппаратных комплексов защиты информации; средствами администрирования систем обнаружения компьютерных атак.</p>
3	ПСК-8.2 способностью разрабатывать проектные решения систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации.	<p>Знать и понимать: основные методы оценки защищенности</p> <p>Уметь: применять методы обеспечивающие защиту от воздействия внутренних и внешних угроз</p> <p>Владеть: методами оценки защищенности и составления отчетов по результатам обследований</p>

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

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 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 10
Контактная работа	72	72,15
Аудиторные занятия (всего):	72	72
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	36	36
Самостоятельная работа (всего)	72	72
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

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	10	<p>Раздел 1</p> <p>Информационная безопасность и уровни ее обеспечения</p> <p>1. Понятие "информационная безопасность"</p> <p>Составляющие информационной безопасности</p> <p>Система формирования режима информационной безопасности</p> <p>Нормативно-правовые основы информационной безопасности в РФ</p> <p>Стандарты информационной безопасности: "Общие критерии"</p> <p>2. Стандарты информационной безопасности распределенных систем</p> <p>Стандарты информационной безопасности в РФ</p> <p>Административный уровень обеспечения информационной безопасности</p> <p>Классификация угроз "информационной безопасности"</p>	4		2		20	26	
2	10	<p>Раздел 2</p> <p>Компьютерные вирусы и защита от них</p> <p>1. Вирусы как угроза информационной безопасности</p> <p>Классификация компьютерных вирусов</p> <p>2. Характеристика</p>	6		4		20	30	

№ 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
		"вирусоподобных" программ Антивирусные программы 3. Профилактика компьютерных вирусов Обнаружение неизвестного вируса							
3	10	Раздел 3 Информационная безопасность вычислительных сетей 1. Особенности обеспечения информационной безопасности в компьютерных сетях Сетевые модели передачи данных 2. Модель взаимодействия открытых систем OSI/ISO Адресация в глобальных сетях Классификация удаленных угроз в вычислительных сетях 3. Типовые удаленные атаки и их характеристика Причины успешной реализации удаленных угроз в вычислительных сетях Принципы защиты распределенных вычислительных сетей	6		8		12	26	ПК1, опросы
4	10	Раздел 4 Механизмы обеспечения "информационной безопасности» 1. Идентификация и аутентификация. 2. Криптография и шифрование. 3. Методы разграничение	8		8		10	26	

№ 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
		доступа. Регистрация и аудит. 4. Межсетевое экранирование. Технология виртуальных частных сетей (VPN)							
5	10	Раздел 5 Корпоративные защищенные сети 1. Введение в MPLS, TE и QoS. 2. Архитектура мультипротокольной коммутации пакетов по меткам (MPLS). 3. Защита в MPLS с использованием генератора специализированных последовательностей.	12		14		10	36	ПК2, опросы
6	10	Раздел 7 Зачет с оценкой						0	ЗаО
7		Всего:	36		36		72	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 36 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	10	РАЗДЕЛ 1 Информационная безопасность и уровни ее обеспечения	ПЗ 1. Стандартизация в области обнаружения атак. Технологии обнаружения компьютерных атак и их возможности. Типы атак.	2
2	10	РАЗДЕЛ 2 Компьютерные вирусы и защита от них	ПЗ 2. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Фильтрация пакетов	4
3	10	РАЗДЕЛ 3 Информационная безопасность вычислительных сетей	ПЗ 3. Туннелирование в VPN.	4
4	10	РАЗДЕЛ 3 Информационная безопасность вычислительных сетей	ПЗ 4. ПК 1 - текущ. контроль по разделам 1, 2, 3.	4
5	10	РАЗДЕЛ 4 Механизмы обеспечения "информационной безопасности»	ПЗ 4. Службы каталогов. LDAP. Open LDAP.	8
6	10	РАЗДЕЛ 5 Корпоративные защищенные сети	ПЗ 5. Протокол BGP4, IS-IS. Автономная система AS. Маршрутизация в MPLS.	6
7	10	РАЗДЕЛ 5 Корпоративные защищенные сети	ПЗ 6. ПК2- текущ. контроль по разделу 4, 5.	8
ВСЕГО:				36/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Защита информации в телекоммуникационных системах железнодорожного транспорта» осуществляется в форме лекций, лабораторных работ и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30% являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70% с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция.

Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса 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, а так же использованием компьютерной тестирующей системы.

В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относятся отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически завершённый объём 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 путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.

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	10	РАЗДЕЛ 1 Информационная безопасность и уровни ее обеспечения	Стандарты информационной безопасности в РФ 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1 с.6-14], [2, стр.3-6]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала по темам: Стандарты информационной безопасности в РФ Административный уровень обеспечения информационной безопасности Классификация угроз "информационной безопасности»	20
2	10	РАЗДЕЛ 2 Компьютерные вирусы и защита от них	Антивирусные программы Профилактика компьютерных вирусов 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [2, стр.60-84]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала по темам: Антивирусные программы Профилактика компьютерных вирусов	20
3	10	РАЗДЕЛ 3 Информационная безопасность вычислительных сетей	Типовые удаленные атаки и их характеристика 1. Подготовка к практическому занятию. 2. Подготовка к текущему контролю. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [1 с.227-245], [2, с.36-59], [доп. 1] 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала по темам: Типовые удаленные атаки и их характеристика Реализация удаленных угроз в вычислительных сетях	12

			Принципы защиты распределенных вычислительных сетей	
4	10	РАЗДЕЛ 4 Механизмы обеспечения "информационной безопасности»	<p>Регистрация и аудит Межсетевое экранирование</p> <ol style="list-style-type: none"> 1. Подготовка к практическому занятию. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1 с.105-168], [2, с. 23-35]. [доп. 1] 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Выполнение курсового проекта 7. Конспектирование изученного материала по темам: Регистрация и аудит Межсетевое экранирование 	10
5	10	РАЗДЕЛ 5 Корпоративные защищенные сети	<p>Защита в MPLS с использованием шифрования</p> <ol style="list-style-type: none"> 1. Подготовка к практическому занятию. 2. Подготовка к тестированию. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [1 с.169-204], [2, стр. 36-59], [доп. 1] 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала по теме: Защита в MPLS с использованием шифрования 	10
			ВСЕГО:	72

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	Средства защиты информации на железнодорожном транспорте	А.А. Корниенко, М.А. Еремеев, С.Е. Ададулов	М. : Маршрут, 2006, 0 НТБ МИИТ	Раздел 1 [6-14], Раздел 3 [227-245], Раздел 4 [105-168], Раздел 5 [169-204]
2	Безопасность коммуникационных сетей	В.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко	МИИТ. Центр компетентности "Защита и безопасность информации", 2007 НТБ МИИТ	Раздел 1 [3-6], Раздел 2 [60-84], Раздел 3 [36-59], Раздел 4 [23-35], Раздел 5 [36-59]
3	Разработка корпоративной сети на основе MPLS. Защита информации [Электронный ресурс] : учебно-метод. пособие по курс. работе для специалистов напр. "Компьютерная безопасность"	В. М. Алексеев	МИИТ, 2017 НТБ МИИТ (ЭЭ)	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Криптография	Н. Смарт	М. : Техносфера, 2006 НТБ МИИТ	Раздел 2 [22-52], Раздел 3 [71-88], Раздел 4 [122-148], Раздел 5 [162-203]
5	Компьютерные системы и сети	В.П. Косарев, Л.В. Еремин, О.В. Машникова и др.; Под ред. В.П. Косарева, Л.Б. Еремина	Финансы и статистика, 1999 НТБ (уч.2); НТБ (уч.4); НТБ (фб.); НТБ (чз.2)	Все разделы
6	Технические средства защиты информации	А.А. Титов	Томский государственный университет систем управления и радиоэлектроники, 2010	Все разделы

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

<http://library.miit.ru/> - электронно-библиотечная система Научно-технической библиотеки МИИТ.

<http://elibrary.ru/> - научно-электронная библиотека.

<http://robotosha.ru/>

www.chipinfo.ru.
http://siblec.ru/
http://autex.ru/
http://www.intuit.ru
http://twirpx.com
http://habrahabr.ru
http://semestr.ru
http://www.cisco.ru

Поисковые системы: Yandex, Google, Mail, база научно-технической информации
ВИНИТИ РАН.

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Для проведения практических занятий необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами:

Microsoft Office или Work 9,

интегрированная среда разработки программного обеспечения для эмуляции сетевого оборудования OmniGraffle;

среда разработки программного обеспечения HTML5 и PHP.

Для проведения практических занятий и выполнения курсовой работы необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ:

в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше) с поддержкой MPLS;

программные продукты Mac OS server, XSan.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET
4. Для проведения практических занятий: компьютерный класс; компьютеры с минимальными требованиями – Core 5, ОЗУ 4 ГБ, HDD 300 ГБ, wifi, USB 2.0.

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: 1. Познавательная-обучающая; 2. Развивающая; 3.

Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6.

Организирующая; 7. информационная.

Выполнение практических заданий и лабораторных работ 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 и лабораторных работ не сводится только к органическому 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 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 и лабораторных работ. Задачи практических занятий и лабораторных работ: 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 и лабораторной работе 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 и семестровый планы 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 учебы. 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 экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной

дисциплины и включающие терминологические задания.

Фонд оценочных средств являются 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.