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 Желенков Борис Владимирович, к.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Аудит информационной безопасности

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

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии  Н.А. Клычева	Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой  Б.В. Желенков

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Аудит информационной безопасности» является формирование компетенций по основам проведения аудита информационной безопасности (ИБ) на предприятии или в организации, изучение видов аудита, необходимых средств и методов для проведения аудита, получение навыков по разработке программы проведения аудита ИБ, выявлению уязвимостей и формированию рекомендаций по устранению уязвимостей.

Основными задачами дисциплины являются:
• ознакомление с целями и задачами проведения аудита информационной безопасности объекта защиты;
• изучение видов и форм проведения аудита;
• изучение стандартов ИБ;
• получение навыков по использованию методов проведения аудита ИБ;
• получение навыков по выявлению уязвимостей и формированию рекомендаций по совершенствованию системы ИБ.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):

Эксплуатационная:
• 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;

Проектно-технологическая:
• сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
• проведение проектных расчетов элементов систем обеспечения информационной
• безопасности;
• участие в разработке технологической и эксплуатационной документации;
• проведение предварительного технико-экономического обоснования проектных расчетов;

Экспериментально-исследовательская деятельность:
• сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
• проведение экспериментов по заданной методике, обработка и анализ их результатов;
• проведение вычислительных экспериментов с использованием стандартных программных средств.

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 "Аудит информационной безопасности" 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. Основы информационной безопасности :

Знания: основы формирования знаний по информационной безопасности; законодательную и нормативную базу ИБ; основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия; перспективы развития обеспечения информационной безопасности

Умения: оценивать область применения элементов информационной безопасности; использовать элементы информационной безопасности для решения практических задач; использовать средства, предоставляемые системой защиты и управлять системой информационной безопасности

Навыки: оценки направления действия ИБ;оценки работы элементов ИБ как отдельно, так и в системе;использования информационных ресурсов для совершенствования системы ИБ.

2.1.2. Основы управления информационной безопасностью:

Знания: принципы работы с информацией, основные угрозы информационной безопасности и методы защиты от них; основные нормативные документы, определяющие политику безопасности предприятиясовременные принципы разработки ИБ, процессов управления ИБ и направления их развития

Умения: использовать информационные системы для поиска необходимой информации, оценивать степень угрозы информационной безопасности эксплуатируемой системыанализировать текущее состояние ИБ на предприятии, определять цели и задачи, решаемые создаваемыми процессами управления ИБ; применять процессный подход к управлению к обеспечению информационной безопасности объекта защиты

Навыки: основными приемами обнаружения и предотвращения угроз информационной безопасности; навыками управления информационной безопасностью объектов, терминологией и методами построения СУИБ.

2.1.3. Программно-аппаратные средства защиты информации:

Знания: методы и средства конфигурирования и контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексамиэксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации

Умения: контролировать работу подсистем и изменять конфигурационные параметры при необходимости, применять методы и средства контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексамипроверять работоспособность элементов системы защиты с помощью необходимых технических средств

Навыки: навыками по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

2.1.4. Техническая защита информации:

Знания: концепции инженерно-технической защиты информации, основных угроз безопасности информации, порядка организации инженерно-технической защиты информации;основных руководящих и нормативных документов по инженерно-технической защите информации

Умения: выявлять угрозы и технические каналы утечки информации; контролировать эффективность мер защиты;

Навыки: Применять необходимые технические средства защиты информации для обеспечения ИБ.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Преддипломная практика

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-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать и понимать: стандарты по ИБ, порядок и стадии проведения аудита ИБ. Уметь: определять цели проведения аудита, моделировать угрозы, применять инструментальные необходимые средства, оформлять документацию по этапам аудита ИБ. Владеть: навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.
2	ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Знать и понимать: необходимые требования к безопасности информации на объекте информатизации. Уметь: организовывать и сопровождать процесс аттестации объекта информатизации по требованиям безопасности информации Владеть: навыками в организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации и интерпретировать полученные в процессе проведения аудита результаты
3	ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Знать и понимать: характеристики аппаратных и технических средств защиты информации необходимые для проведения аудита. Уметь: организовывать и проводить контрольные проверки работоспособности элементов системы защиты с помощью необходимых технических средств Владеть: навыками интерпретировать полученные в процессе проведения аудита результаты для получения оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.
4	ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Знать и понимать: основные принципы формального представления информации, понятия информационной безопасности, составные элементы подсистем и их характеристики. Уметь: искать и анализировать информацию, четко ставить цель и последовательно добиваться ее осуществления, определять уязвимости объектов защиты; осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов Владеть: навыками поиска и анализа информации,

№ п/п	Код и название компетенции	Ожидаемые результаты
		определения взаимосвязи явлений и объектов; навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
5	ПСК-1.4 способность проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей (ПСК-1.4);	Знать и понимать: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации. Уметь: проводить экспериментальное исследование работоспособности как отдельных элементов системы защиты, так и компьютерных систем с помощью необходимых технических средств с целью выявления уязвимостей. Владеть: навыками интерпретировать полученные результаты для получения оценки эффективности системы защиты компьютерных систем.

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

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 8
Контактная работа	36	36,15
Аудиторные занятия (всего):	36	36
В том числе:		
лекции (Л)	18	18
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	72	72
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1	ПК1
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 промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	8	Раздел 1 Аудит информационной безопасности.	2		2		10	14	
2	8	Тема 1.2 Виды, этапы и направления деятельности. Рассматриваются виды и этапы проведения аудита. Описываются направления проведения аудита: первичный аудит; технический аудит, контрольный аудит.	2		2		10	14	
3	8	Раздел 2 Нормативно-правовая база проведения аудита ИБ.	6		4		10	20	
4	8	Тема 2.1 Правовая база проведения аудита.	2		2			4	
5	8	Тема 2.2 Стандарты проведения аудита. Рассматривается структура международных и национальных стандартов в сфере аудита. Изучаются стандарты ISO 15408 и ISO 17799 и методика их применения для оценки и управления безопасностью информационных технологий.	2				10	12	
6	8	Тема 2.3 Стандарты проведения аудита. Рассматривается ГОСТ Р ИСО/МЭК 15408, CoBit, PCI DSS. Рассматриваются руководящие документы ФСТЭК	2		2			4	ПК1, выполнение лаб.работ 20%

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		России.							
7	8	Раздел 3 Методика и порядок проведения аудита ИБ.	8		8/6		40	56/6	
8	8	Тема 3.1 Стадии и методика проведения аудита. Описываются стадии проведения аудита: планирование, моделирование, тестирование, анализ, разработка предложений, документирование. Рассматриваются экспертно-аналитические, экспертно-инструментальные методы. Анализ бизнес-процессов организации. Моделирование направлений действий злоумышленника.	2				10	12	
9	8	Тема 3.3 Планирование аудита. Описывается процесс инициирования процедуры аудита его цель, объект обследования. Рассматриваются критерии оценки значимости информационных ресурсов и процессов обработки информации. Описывается порядок и форма представления отчетов.	2		2/2		10	14/2	
10	8	Тема 3.4 Моделирование угроз и тестирование. Рассматриваются цели и направления проведения моделирования. Описываются цели, методы и порядок проведения	2		2/2		10	14/2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		тестирования. Требования к размещению и использованию оборудования. Испытания функционирования системы защиты от НСД и защиты от утечки по техническим каналам. Тестирование рабочих станций (АРМ), серверов, межсетевых экранов, активного сетевого оборудования.							
11	8	Тема 3.5 Документирование этапов проведения аудита ИБ. Рассматриваются рекомендации по документированию: цель и методы обследования, проверка организационно-распорядительных документов, документирование результатов.	2		4/2		10	16/2	
12	8	Раздел 4 Инструментальные средства проведения аудита ИБ.	2		4/3		12	18/3	
13	8	Тема 4.1 Программное обеспечение для аудита ИБ Рассматриваются характеристики и обзор программных средств, применяемых для проведения аудита ИБ.	2		4/3		12	18/3	
14	8	Раздел 5 Дифференцированный зачет						0	ЗаО
15		Тема 1.1 Основные понятия. Описываются основные понятия, цели и задачи							

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		проведения аудита ИБ. Определяются моменты, когда необходимо проводить аудит, периодичность.							
16		Тема 3.2 Подготовка к аудиту ИБ. Описываются состав и роли участников, порядок, цель и методы сбора исходной информации. Общие исходные данные. Исходные данные об обрабатываемой информации. Исходные данные о системе обеспечения безопасности информации. Исходные данные о персонале. Сбор дополнительных исходных данных.							
17		Всего:	18		18/9		72	108/9	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 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	8	РАЗДЕЛ 1 Аудит информационной безопасности. Тема: Виды, этапы и направления деятельности.	Виды и этапы проведения аудита ИБ	2
2	8	РАЗДЕЛ 2 Нормативно-правовая база проведения аудита ИБ. Тема: Правовая база проведения аудита.	Законодательная база для проведения аудита ИБ.	2
3	8	РАЗДЕЛ 2 Нормативно-правовая база проведения аудита ИБ. Тема: Стандарты проведения аудита.	Стандарты для проведения аудита ИБ.	2
4	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема: Планирование аудита.	Подготовка к проведению аудита ИБ	2 / 2
5	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема: Моделирование угроз и тестирование.	Моделирование угроз ИБ	2 / 2
6	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема: Документирование этапов проведения аудита ИБ.	Документирование этапов и результатов проведения аудита ИБ.	4 / 2
7	8	РАЗДЕЛ 4 Инструментальные средства проведения аудита ИБ. Тема: Программное обеспечение для аудита ИБ	Программные средства для проведения аудита ИБ.	4 / 3
			ВСЕГО:	18/9

4.5. Примерная тематика курсовых проектов (работ)

Учебным планом не предусмотрено.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины “Аудит информационной безопасности” осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме в объеме 18 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).

Практические работы организованы с использованием технологий развивающего обучения. Практические работы (26) проводятся в виде упражнений по решению различных вариантов задач аналитического типа или задач разработки с применением интерактивных (диалоговых) технологий в виде мультимедийного лекционного материала (9).

Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (58 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям, подготовка к лекциям и практическим работам.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 4 раздела, представляющих собой логически завершенный 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	8	РАЗДЕЛ 1 Аудит информационной безопасности. Тема 2: Виды, этапы и направления деятельности.	Изучение терминологии аудита ИБ.	10
2	8	РАЗДЕЛ 2 Нормативно-правовая база проведения аудита ИБ. Тема 2: Стандарты проведения аудита.	Работа с учебными материалами и дополнительной литературой по изучению законодательной базы и стандартов ИБ.	10
3	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема 1: Стадии и методика проведения аудита.	Работа с учебными материалами и дополнительной литературой по изучению стадий и методик проведения аудита ИБ.	10
4	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема 3: Планирование аудита.	Работа с учебными материалами и дополнительной литературой по изучению подготовки и планированию аудита ИБ.	10
5	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема 4: Моделирование угроз и тестирование.	Работа с учебными материалами и дополнительной литературой по изучению выполнения моделирование угроз и тестирования системы защиты.	10
6	8	РАЗДЕЛ 3 Методика и порядок проведения аудита ИБ. Тема 5: Документирование этапов проведения аудита ИБ.	Изучение документирования этапов проведения аудита ИБ.	10
7	8	РАЗДЕЛ 4 Инструментальные средства проведения аудита ИБ. Тема 1: Программное обеспечение для аудита ИБ	Изучение инструментальных средств программного обеспечения для проведения аудита ИБ.	12
			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	Информационная безопасность и защита информации. 6-е изд	В.П. Мельников, С.А. Клейменов, А.М. Петраков	М. : Издательский центр "Академия", 2012	Все разделы
2	Информационная безопасность персональных компьютеров	Смирнов В.Ю. Смирнова О.В.	М.: МИИТ, 2009	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц

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 «искусство управления информационной безопасностью» http://www.iso27000.ru/
• Сайт федеральной службы по техническому и экспортному контролю (ФСТЭК) http://fstec.ru/

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

Microsoft Windows
Microsoft Office
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 практических занятий, лабораторных работ №1325 Программно-аппаратный комплекс «СОТСБИ»

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.