

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

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 июня 2019 г.



Кафедра «Управление и защита информации»

Автор Семенов Юрий Станиславович, к.ф.-м.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические протоколы

Специальность:	<u>10.05.01 – Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2019</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 25 июня 2019 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>Протокол № 21 24 июня 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
--	--

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основной целью изучения дисциплины «протоколы» является формирование у обучающегося компетенций для следующих видов деятельности:

контрольно-аналитическая;
эксплуатационная.

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

Контрольно-аналитическая деятельность:

- предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;
- применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

Эксплуатационная деятельность:

- установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения;
- установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем;
- проверка технического состояния и профилактические осмотры технических средств защиты информации;
- проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

Дисциплина «Криптографические протоколы» имеет целью ознакомление слушателей существующими подходами к анализу и синтезу криптографических протоколов, с государственными и международными стандартами в этой области. Дисциплина обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации, способствует освоению принципов корректного применения современных защищенных информационных технологий.

Задача дисциплины «Криптографические протоколы» – получение основополагающих знаний о свойствах, характеризующих защищенность криптографических протоколов, об основных механизмах, применяемых для обеспечения выполнения того или иного свойства безопасности протокола, а также основных уязвимостях протоколов.

Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: применение стандартных криптопротоколов и интернет-технологий, средств и методов хранения и передачи аутентификационной информации, основных протоколов идентификации и аутентификации абонентов, протоколов дистанционного принятия решений, математических моделей шифров, использование криптографических стандартов.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Криптографические протоколы" 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. Криптографические методы защиты информации:

Знания: основные принципы криптографии и защиты информации, алгоритмы шифрования RSA и Эль-Гамала

Умения: моделирование систем RSA и Эль-Гамала, построение больших простых чисел

Навыки: работа в кольцах вычетов и кольцах многочленов

2.1.2. Теоретико-числовые методы в криптографии:

Знания: конечные поля, группы обратимых элементов в кольцах вычетов

Умения: владение арифметикой конечных полей, алгоритмом Евклида

Навыки: работа в кольцах вычетов, нахождение произведений и обратных элементов в полях

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Защита программ и данных

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	ОПК-10 Способен администрировать подсистемы и средства защиты информации в компьютерных системах и сетях	ОПК-10.1 Выполняет задачи по администрированию подсистем и средств защиты информации в КС. ОПК-10.2 Выполняет задачи по администрированию подсистем и средств защиты информации в сетях.
2	ОПК-17 Способен контролировать корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях	ОПК-17.1 Владеет методами и средствами контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях. ОПК-17.2 Умеет применять на практике методы и средства контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях. ОПК-17.3 Умеет проводить дифференциацию и декомпозицию задач контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях. ОПК-17.4 Умеет анализировать результаты контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.
3	ОПК-6 Способен анализировать и учитывать текущее состояние и тенденции развития методов криптографической защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, средств технической защиты информации, сетей и систем передачи информации при решении профессиональных задач	ОПК-6.1 Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. ОПК-6.2 Строит, анализирует и реализует протоколы, в том числе криптографические, в современных программных комплексах. ОПК-6.3 Строит, анализирует и учитывает новые методы защиты в системах управления базами данных, сетей и систем передачи информации.
4	ОПК-8 Способен проводить анализ корректности реализации эффективных комбинаторных, теоретико-числовых и криптографических алгоритмов и протоколов применительно к конкретным условиям	ОПК-8.1 Строит, анализирует и реализует алгоритмы, в том числе криптографические, в современных программных комплексах. ОПК-8.2 Устанавливает причины, цели и условия изменения свойств алгоритмов и протоколов применительно к конкретным условиям. ОПК-8.3 Анализирует корректность комбинаторных, теоретико-числовых и криптографических алгоритмов в современных программных комплексах.
5	ПКО-11 Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации	ПКО-11.1 Обосновывает критерии и рассчитывает показатели эффективности защиты обрабатываемой информации. ПКО-11.2 Составляет методики тестирования, подбирает инструментарию и осуществляет проверку эффективности функционирования программных, программно-аппаратных и технических средств, подсистем защиты информации.

№ п/п	Код и название компетенции	Ожидаемые результаты
		ПКО-11.3 Выполняет работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации.
6	ПКО-6 Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	ПКО-6.1 Подбирает методики и инструментарий, определяет критерии и осуществляет проверку эффективности систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.

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 7
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)	36	36
Экзамен (при наличии)	36	36
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)	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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	7	Раздел 1 Понятие протокола, виды протоколов.	12		12		12	36	ПК1, Контрольная работа
2	7	Тема 1.1 Понятие протокола, отличия от криптосистем, примеры.	2		4		2	8	
3	7	Тема 1.2 Цели и предназначение протоколов.	2				2	4	
4	7	Тема 1.3 Криптостойкость протоколов.	2				2	4	
5	7	Тема 1.4 Виды криптопротоколов.	2		4		2	8	
6	7	Тема 1.5 Протоколы с нулевым разглашением.	2				2	4	
7	7	Тема 1.6 Аутентификация в информационных системах.	2		4		2	8	
8	7	Раздел 2 Стандарт. Криптопротоколы.	12		12		12	36	ПК2, Контрольная работа
9	7	Тема 2.1 Протокол Диффи-Хеллмана.	2		4		2	8	
10	7	Тема 2.2 Протокол Блюма.	2		4		2	8	
11	7	Тема 2.3 Протокол аутентификации Шнорра.	2				2	4	
12	7	Тема 2.4 Электронная подпись RSA.	2		4		2	8	
13	7	Тема 2.5 Крипт. хэш-функции.	2				2	4	
14	7	Тема 2.6 Электронная подпись Шнорра.	2				2	4	
15	7	Раздел 3 Другие виды криптопротоколов.	12		12		12	36	
16	7	Тема 3.1	2				2	4	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Протоколы, связанные с электронными платежами.							
17	7	Тема 3.2 Электронные купюры.	2				2	4	
18	7	Тема 3.3 Электронные деньги одного номинала.	2		4		2	8	
19	7	Тема 3.4 Электронные деньги разного номинала.	2		4		2	8	
20	7	Тема 3.5 Разделение секрета.	2		4		2	8	
21	7	Тема 3.6 Протоколы голосования.	2				2	4	
22	7	Экзамен						36	ЭК
23		Всего:	36		36		36	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	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема: Понятие протокола, отличия от криптосистем, примеры.	Практическое занятие №1 Понятие протокола, отличия от криптосистем, примеры	4
2	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема: Виды криптопротоколов.	Практическое занятие №2 Виды криптопротоколов	4
3	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема: Аутентификация в информационных системах.	Практическое занятие №3 Аутентификация в информационных системах	4
4	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема: Протокол Диффи-Хеллмана.	Практическое занятие №4 Протокол Диффи-Хеллмана	4
5	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема: Протокол Блюма.	Практическое занятие №5 Протокол Блюма	4
6	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема: Электронная подпись RSA.	Практическое занятие №6 Электронная подпись RSA	4
7	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема: Электронные деньги одного номинала.	Практическое занятие №7 Электронные деньги одного номинала	4
8	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема: Электронные деньги разного номинала.	Практическое занятие №8 Электронные деньги разного номинала	4

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
9	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема: Разделение секрета.	Практическое занятие №9 Разделение секрета	4
ВСЕГО:				36 / 0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты и работы не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Криптографические протоколы» осуществляется в форме лекций, практических занятий.

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

Практические занятия также организованы в традиционной классно-урочной организационной форме, с использованием технологий развивающего обучения. Также предполагается, что студенты могут делать небольшие 15-20-минутные доклады-презентации по разбираемым темам (возможны видеоконференции при подготовке докладов).

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. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, 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 для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения задач, решение индивидуальных лабораторных заданий с использованием.

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	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема 1: Понятие протокола, отличия от криптосистем, примеры.	Подготовка дом. заданий. [1], [2].	2
2	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема 2: Цели и предназначение протоколов.	Подготовка дом. заданий. [1], [2].	2
3	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема 3: Криптостойкость протоколов.	Подготовка дом. заданий. [1], [2].	2
4	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема 4: Виды криптопротоколов.	Подготовка дом. заданий. [1], [2].	2
5	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема 5: Протоколы с нулевым разглашением.	Подготовка дом. заданий. [1], [2].	2
6	7	РАЗДЕЛ 1 Понятие протокола, виды протоколов. Тема 6: Аутентификация в информационных системах.	Подготовка дом. заданий. [1], [2].	2
7	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема 1: Протокол Диффи-Хеллмана.	Подготовка дом. заданий/докладов. [1], [2].	2
8	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема 2: Протокол Блюма.	Подготовка дом. заданий/докладов. [1], [2].	2
9	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема 3: Протокол аутентификации Шнорра.	Подготовка дом. заданий/докладов. [1], [2].	2
10	7	РАЗДЕЛ 2	Подготовка дом. заданий/докладов. [1], [2].	2

		Стандарт. Криптопротоколы. Тема 4: Электронная подпись RSA.		
11	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема 5: Крипт. хэш- функции.	Подготовка дом. заданий/докладов. [1], [2].	2
12	7	РАЗДЕЛ 2 Стандарт. Криптопротоколы. Тема 6: Электронная подпись Шнорра.	Подготовка дом. заданий/докладов. [1], [2].	2
13	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема 1: Протоколы, связанные с электронными платежами.	Подготовка дом. заданий/докладов. [1], [2].	2
14	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема 2: Электронные купюры.	Подготовка дом. заданий/докладов. [1], [2].	2
15	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема 3: Электронные деньги одного номинала.	Подготовка дом. заданий/докладов. [1], [2].	2
16	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема 4: Электронные деньги разного номинала.	Подготовка дом. заданий/докладов. [1], [2].	2
17	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема 5: Разделение секрета.	Подготовка дом. заданий/докладов. [1], [2].	2
18	7	РАЗДЕЛ 3 Другие виды криптопротоколов. Тема 6: Протоколы голосования.	Подготовка дом. заданий/докладов. [1], [2].	2
ВСЕГО:				36

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	Основы современной криптографии	С.Г. Баричев, В.В. Гончаров, Р.Е. Серов	Горячая линия - Телеком, 2011 НТБ (фб.); НТБ (чз.1); НТБ (чз.2)	Все разделы
2	Введение в криптографию	В.В. Яценко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Яценко	МЦНМО, 2012 НТБ (фб.); НТБ (чз.2)	Все разделы
3	Введение в теоретико-числовые методы криптографии.	М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин	Лань, 2010 НТБ (фб.); НТБ (уч. 4)	Все разделы
4	Введение в криптосистемы с открытым ключом.	Н. А. Молдовян, А.А. Молдовян	БХВ-Петербург, 2005 НТБ (фб.); НТБ (чз. 2); НТБ (уч. 2)	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
5	Современная криптография: теория и практика.	Венбо Мао, под редакцией Ключиной Д.А.	Издательский дом Вильямс, 2005 НТБ (фб.)	Все разделы
6	Криптография в задачах и упражнениях	В.О. Осипян, К.В. Осипян	"Гелиос АРВ", 2004 НТБ (уч.3); НТБ (фб.); НТБ (чз.2)	Все разделы

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

<http://library.miit.ru/> - электронно-информационная система НТБ МИИТ

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

Поисковые системы: Yandex, Google, Mail.

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

Не требуется

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

Требования к аудиториям (помещениям, кабинетам) для проведения занятий с указанием соответствующего оснащения:

- Доска, мел, тряпка (губка) для стирания; возможно использовать компьютерное и мультимедийное оборудование: компьютер, проектор, экран.

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

Регулярно выполнять домашние задания, изучать дополнительные материалы, повторять темы из предыдущих семестров. Интересующимся студентам рекомендуется участвовать в студенческих олимпиадах.

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.

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 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. 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 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 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.