

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

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 апреля 2020 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Авторы: Голдовский Яков Михайлович, к.т.н.
Сафонова Ирина Евгеньевна, д.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность и защита информации



Направление подготовки: 09.03.01 – Информатика и вычислительная техника

Профиль: Вычислительные системы и сети

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2020

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 4 30 апреля 2020 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 style="text-align: center;">Протокол № 15 27 апреля 2020 г. Заведующий кафедрой</p>  <p style="text-align: right;">Б.В. Желенков</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: 4196
Подписал: Заведующий кафедрой Желенков Борис Владимирович
Дата: 27.04.2020

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина "Информационная безопасность и защита информации" предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Организационно-управленческой

- разработка политики информационной безопасности на уровне БД
- разработка регламентов и аудит системы безопасности данных на уровне БД
- подготовка отчетов о состоянии и эффективности системы безопасности на уровне БД
- контроль использования сетевых устройств и программного обеспечения
- администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Производственно-технологической

- разработка технических спецификаций на программные компоненты и их взаимодействие
- осуществляет разработку тестовых документов, включая план тестирования
- разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным
- разработка архитектуры ИС
- разработка прототипов ИС
- восстановление параметров программного обеспечения сетевых устройств
- размещение и соединение элементов электрических схем стандартных ячеек библиотеки

Проектной

- определение первоначальных требований заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ;
- разработка тестовых программ или генераторов тестовых программ для модели ИС на языках программирования целевой системы.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Информационная безопасность и защита информации" 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. 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

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

2.2.2. 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	ПКР-3 Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.	<p>ПКР-3.1 Знать общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; инструкции по установке администрируемых сетевых устройств; инструкции по эксплуатации администрируемых сетевых устройств; инструкции по установке администрируемого программного обеспечения; инструкции по эксплуатации администрируемого программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; модель ISO для управления сетевым трафиком; модели IEEE; защищенные протоколы управления; основные средства криптографии; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой администрируемой сети.</p> <p>ПКР-3.2 Уметь подключать и настраивать современные межсетевые экраны; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; работать с контрольно-измерительными аппаратными и программными средствами.</p> <p>ПКР-3.3 Владеть навыками параметризации операционных систем средств удаленного доступа; установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация; настройки средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов); документирования настроек средств обеспечения безопасности удаленного.</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 6
Контактная работа	80	80,15
Аудиторные занятия (всего):	80	80
В том числе:		
лекции (Л)	48	48
практические (ПЗ) и семинарские (С)	32	32
Самостоятельная работа (всего)	64	64
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), 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	6	Раздел 1 Введение в управление информационной безопасностью	10		4			10	24	
2	6	Тема 1.1 Основные понятия. Введение. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные. 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. Международные стандартизирующие организации. Стандарты РФ в области информационной безопасности.	8						8	
3	6	Раздел 2 Угрозы информационной безопасности	10		6			10	26	
4	6	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	8						8	ПК1, выполнение и защита лабораторных работ №1-3

№ 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
		ресурсам информационной системы. Угрозы безопасности информационной системы. Сетевая разведка: Sniffing; Ping-sweep, сканирование портов. Несанкционированный доступ: IP-spoofing; Man-in-the-middle; Подмена стороны. DOS-атака. DDOS-атака. Уязвимость программных приложений. Методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам. Компьютерные вирусы. Троянские программы. Сетевые черви. Пути распространения вредоносного программного кода. Программы удаления вредоносного программного кода. Обновления безопасности. Антивирусные программы.							
5	6	Раздел 3 Политика безопасности	6		4		10	20	
6	6	Тема 3.1 Структура политики безопасности. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности. Уровни решений политики безопасности: верхний, средний и нижний. Область применения политики безопасности. Выработка позиции организации. Роль руководителей подразделений. Роль администраторов сетей. Роль администраторов сервисов. Роль пользователя информационной системы. Санкции.	4					4	

№ 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
7	6	Раздел 4 Криптографическая защита	6		6		10	22	
8	6	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. Симметричные криптоалгоритмы. Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования. Асимметричные криптоалгоритмы. Алгоритм RSA. Алгоритм ДиффиХэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения.	4					4	
9	6	Раздел 5 Защита от несанкционированного доступа.	8		6		12	26	
10	6	Тема 5.1 Аутентификация, авторизация и администрирование действий пользователей. Основные принципы системы AAA. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер AAA. Фильтрация трафика.	4					4	ПК2, выполнение и защита практических работ № 4-6, выполнение курсовой работы

№ 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
		Списки доступа. Инспекция трафика. Традиционный межсетевой экран. Технология Zone-based firewall. Основные схемы применения межсетевых экранов. Методы анализа сетевой информации. Сигнатуры. Системы обнаружения вторжений (IDS). Системы предотвращения вторжений (IPS).							
11	6	Раздел 6 Защита информации в глобальной сети.	8		6		12	26	
12	6	Тема 6.1 Защита http-трафика Характерные угрозы. Защищенный протокол httpd. Цифровые сертификаты. Виртуальная частная сеть. Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec.	4					4	КР
13	6	Раздел 7 Итоговая аттестация						0	ЗаО
14		Всего:	48		32		64	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия 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 управление информационной безопасностью	«ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ»	4
2	6	РАЗДЕЛ 2 Угрозы информационной безопасности	«ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ»	6
3	6	РАЗДЕЛ 3 Политика безопасности	«СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ»	4
4	6	РАЗДЕЛ 4 Криптографическая защита	«НАСТРОЙКА АДМИНИСТРАТИВНОГО ДОСТУПА К МАРШРУТИЗАТОРУ»	6
5	6	РАЗДЕЛ 5 Защита от несанкционированного доступа.	«НАСТРОЙКА ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ»	6
6	6	РАЗДЕЛ 6 Защита информации в глобальной сети.	«НАСТРОЙКА ПРОТОКОЛА БЕЗОПАСНОСТИ IPSec»	6
ВСЕГО:				32/0

4.5. Примерная тематика курсовых проектов (работ)

4.5. Примерная тематика курсовых проектов (работ)

1. Разработать регламенты и аудит системы безопасности телефонной базы данных организации
2. Разработать регламенты и аудит системы безопасности БД поставщиков товаров и услуг организации
3. Разработать регламенты и аудит системы безопасности данных на уровне базы данных технической библиотеки
4. Разработать регламенты и аудит системы безопасности для БД товаров магазина
5. Разработать регламенты и аудит системы безопасности данных на уровне БД канц.товаров
6. Разработать регламенты и аудит системы безопасности для БД кадрового агентства.
7. Разработать регламенты и аудит системы безопасности для БД инвентаря спротивного клуба
8. Разработать регламенты и аудит системы безопасности данных на уровне БД оборудования для сетевых лабораторий
9. Разработать регламенты и аудит системы безопасности данных на уровне базы данных микропроцессоров

10. Разработать регламенты и аудит системы безопасности для БД студентов факультата ВУЗа
11. Разработать регламенты и аудит системы безопасности БД сетевого оборудования

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Информационная безопасность и защита информации» осуществляется в форме лекций, практических занятий и выполнения курсовой работы. Лекции проводятся в традиционной классно-урочной организационной форме в объеме 32 часа, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).

Практические занятия (32 часа) организованы с использованием технологий развивающего обучения.

Самостоятельная работа студента (72 часа) организована с использованием традиционных видов работы. К традиционным видам работы 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 управление информационной безопасностью	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №1. Изучение учебной литературы из приведенных источников: [1, стр.1-4], [2 стр. 14-25]. 3. Подготовка к выполнению курсовой работы.	10
2	6	РАЗДЕЛ 2 Угрозы информационной безопасности	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №2. Изучение учебной литературы из приведенных источников: [1, стр.4-8], [2 стр. 25-32]. 3. Подготовка к выполнению курсовой работы.	10
3	6	РАЗДЕЛ 3 Политика безопасности	1. Анализ и дополнительная проработка материала.. 2. Подготовка к выполнению практической работы №3. Изучение учебной литературы из приведенных источников: [1, стр.9-12], [2 стр. 33-187]. 3. Подготовка и выполнение курсовой работы.	10
4	6	РАЗДЕЛ 4 Криптографическая защита	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению работы №4. Изучение учебной литературы из приведенных источников: [1, стр.13-16], [2 стр. 188-204]. 3. Выполнение курсовой работы.	10
5	6	РАЗДЕЛ 5 Защита от несанкционированного доступа.	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №5. Изучение учебной литературы из приведенных источников: [1, стр.17-20], [2 стр. 205-236]. 3. Выполнению курсовой работы.	12
6	6	РАЗДЕЛ 6 Защита информации в глобальной сети.	1. Анализ и дополнительная проработка материала. 2. Подготовка к выполнению практической работы №6. Изучение учебной литературы из приведенных источников: [1, стр.21-36], [2 стр. 259-270]. 3. Выполнение курсовой работы и подготовка к защите курсовой работы.	12
ВСЕГО:				64

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.:МИИТЭлектронная библиотека МИИТ, http://library.miit.ru , 2013	36 сЭлектронная библиотека МИИТ http://library.miit.ru Разделы 1-6

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
2	Информационная безопасность: защита и нападение.	Бирюков А.А.	Издательство "ДМК Пресс"Электронная библиотека МИИТ, http://library.miit.ru , 2012	474 сЭлектронная библиотека МИИТ http://library.miit.ru Разделы 1-6

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)

Microsoft Windows

Microsoft Office

Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

Microsoft Windows

Microsoft Office

Подписка МИИТ, Контракт №0373100006514000379, дата договора 10.12.2014

Putty

Бесплатное использование (MIT)

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

Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, сетевое оборудование, рабочая станция преподавателя, проектор, экран, доска

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.

При подготовке студента важна не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. 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 экзамену. 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.