**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Голдовский Яков Михайлович, к.т.н.

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

## Основы информационной безопасности

| | |
|---|---|
| Направление подготовки: | 10.03.01 – Информационная безопасность |
| Профиль: | Безопасность компьютерных систем |
| Квалификация выпускника: | Бакалавр |
| Форма обучения: | очная |
| Год начала подготовки | 2019 |

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



Москва 2019 г.

# 1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Основы информационной безопасности» являются изучение студентами основных понятий информационной безопасности, изучение основных видов угроз информационной безопасности; получение представления об организации и принципах обеспечения информационной безопасности; знакомство с основами методов криптографического закрытия данных; получение навыков разработки политики безопасности предприятия, методами нарушения конфиденциальности, целостности и доступности информации; причинами, видами, каналами утечки и искажения информации.

Основными задачами дисциплины являются:
• освоение методов оценки степени угрозы информационной безопасности;
• изучение использования соответствующих методов защиты.;
• рассмотрение методов организации комплексной системы защиты информации;
• изучение студентами основных угроз информационной безопасности и методов защиты от них.
• процесса сбора, передачи, накопления и обработки информации;
• установление структуры угроз защищаемой информации;

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:
• осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
• организация работы малых коллективов исполнителей с учетом требований защиты информации;
• совершенствование системы управления информационной безопасностью;

• изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;
• контроль эффективности реализации политики информационной безопасности объекта.

## 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Основы информационной безопасности " 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. Основы вычислительной техники**:

Знания: роль информации, информационных технологий и информационной безопасности в современном обществе, основные принципы аналитического представления БФ и математические законы, позволяющие их обрабатывать для обеспечения формализации принятия решения.

Умения: интерпретировать состояния и действия объектов с помощью математических представлений БФ для принятия эффективных проектных решений.

Навыки: аналитическими методами синтеза комбинационных схем с заданными параметрами для обоснования принимаемых проектных решений в области проектирования систем информационной безопасности

### 2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Государственная итоговая аттестация

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 | ОПК-1 Способен представлять роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; | ОПК-1.1 Знать значение и роль информации, информационных технологий для обеспечения объективных потребностей личности, общества и государства.<br>ОПК-1.2 Уметь применять информационные технологии для поиска и обработки информации; анализировать информацию и информационных технологий с точки зрения информационной безопасности для современного общества.<br>ОПК-1.3 Владеть навыками использования информации, информационных технологий с учетом требования информационной безопасности в современном обществе. |
| 2 | ПКО-9 Способность проводить сбор, изучение научно-технической информации, отечественного и зарубежного опыта по вопросам обеспечения информационной безопасности. | ПКО-9.1 Знать методы поиска научно-технической информации.<br>ПКО-9.2 Уметь выбирать необходимую информацию в области информационной безопасности из отечественных и зарубежных источников.<br>ПКО-9.3 Владеть навыками изучения научно-технической информации, отечественного и зарубежного опыта по вопросам обеспечения информационной безопасности. |

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

### 4.1. Общая трудоемкость дисциплины составляет:

3 зачетных единиц (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 4 |
| Контактная работа | 32 | 32,15 |
| Аудиторные занятия (всего): | 32 | 32 |
| В том числе: | | |
| лекции (Л) | 16 | 16 |
| лабораторные работы (ЛР)(лабораторный практикум) (ЛП) | 16 | 16 |
| Самостоятельная работа (всего) | 76 | 76 |
| ОБЩАЯ трудоемкость дисциплины, часы: | 108 | 108 |
| ОБЩАЯ трудоемкость дисциплины, зач.ед.: | 3.0 | 3.0 |
| Текущий контроль успеваемости (количество и вид текущего контроля) | ПК1, ПК2 | ПК1, ПК2 |
| Виды промежуточной аттестации (экзамен, зачет) | 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 | 4 | Раздел 1 ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ | 3 | 2 | | | 12 | 17 | |
| 2 | 4 | Тема 1.1 Основные понятия Введение. Информация. и защита данных. Конфиденциальность информации. Целостность информации. Доступность информации. Служебная информация. Личные данные. | 1 | | | | | 1 | |
| 3 | 4 | Тема 1.2 Государственные структуры, отвечающие за защиту данных. Определение служебной тайны. Законодательство РФ в области информационной безопасности. Информационная безопасность коммерческой структуры. Типовой набор должностей, связанных с защитой данных на предприятии.; | 1 | | | | | 1 | |
| 4 | 4 | Тема 1.3 Международные стандартизирующие организации. | 1 | | | | | 1 | |
| 5 | 4 | Раздел 2 УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 2 | 4 | | | 12 | 18 | |
| 6 | 4 | Тема 2.1 Природа возникновения угроз. Классификация угроз по преднамеренности проявления. Классификация по источнику угрозы. Классификация по степени воздействия на информационную систему. По способам доступа к ресурсам информационной системы. | 1 | | | | | 1 | |
| 7 | 4 | Тема 2.2 Угрозы безопасности информационной системы и методы противодействия несанкционированному доступу, сетевой разведке и DOS-атакам. | 1 | | | | | 1 | |
| 8 | 4 | Раздел 3 ПОЛИТИКА БЕЗОПАСНОСТИ | 3 | 2 | | | 12 | 17 | |

| № 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 |
| 9 | 4 | Тема 3.1<br>Структура политики безопасности | 1 | | | | | 1 | ПК1, Контрольная работа №1 |
| 10 | 4 | Тема 3.2<br>Базовая политика безопасности. | 1 | | | | | 1 | |
| 11 | 4 | Тема 3.3<br>Специализированные политики безопасности | 1 | | | | | 1 | |
| 12 | 4 | Раздел 4<br>КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | 3 | 2 | | | 12 | 17 | |
| 13 | 4 | Тема 4.1<br>Классификация криптографических алгоритмов.<br>Основные определения. Назначение шифрования. Принципы криптографического закрытия информации. Простые методы шифрования. Таблица Вижинера. Шифрование с открытым и закрытым ключами. Основные виды атак на криптоалгоритмы. | 1 | | | | | 1 | |
| 14 | 4 | Тема 4.2<br>Симметричные криптоалгоритмы.<br>Блочные и потоковые криптоалгоритмы. Алгоритм DES. Алгоритм 3DES. Алгоритм AES. Вопросы стойкости криптоалгоритмов. проблема распределения ключей. Достоинства и недостатки симметричного шифрования. | 1 | | | | | 1 | |
| 15 | 4 | Тема 4.3<br>Асимметричные криптоалгоритмы.<br>Алгоритм RSA. Алгоритм Диффи-Хэлмана. Электронно-цифровая подпись. Достоинства и недостатки асимметричного шифрования и область его применения. | 1 | | | | | 1 | ПК2, Контрольная работа №2 |
| 16 | 4 | Раздел 5<br>ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. | 2 | 2 | | | 12 | 16 | |
| 17 | 4 | Тема 5.1<br>Аутентификация, авторизация и администрирование действий пользователей.<br>Основные принципы системы | 1 | | | | | 1 | |

| № 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 |
| | | ААА. Методы аутентификации: пароли, PIN и биометрические данные. Авторизация. Accounting. Сервер ААА. | | | | | | | |
| 18 | 4 | Тема 5.2 Фильтрация трафика. Списки доступа. Инспекция трафика. Традиционный межсетевой экран. | 1 | | | | | 1 | |
| 19 | 4 | Раздел 6 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. | 3 | 4 | | | 16 | 23 | |
| 20 | 4 | Тема 6.1 Защита http-трафика. Характерные угрозы. Защищенный протокол httpd. | 1 | | | | | 1 | |
| 21 | 4 | Тема 6.2 Цифровые сертификаты.. Виртуальная частная сеть. | 1 | | | | | 1 | |
| 22 | 4 | Тема 6.3 Туннелирование трафика. Виртуальные каналы. Архитектура VPN. Стандарты IPsec. | 1 | | | | | 1 | |
| 23 | 4 | Раздел 7 Итоговая аттестация | | | | | | 0 | ЗаО |
| 24 | | Всего: | 16 | 16 | | | 76 | 108 | |

### 4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 16 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 | 4 | РАЗДЕЛ 1 ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ | Стандарты и организации, работающие в области информационной безопасности. | 2 |
| 2 | 4 | РАЗДЕЛ 2 УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | Угрозы информационной безопасности | 4 |
| 3 | 4 | РАЗДЕЛ 3 ПОЛИТИКА БЕЗОПАСНОСТИ | Разработка политики безопасности | 2 |
| 4 | 4 | РАЗДЕЛ 4 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | Шифрование и дешифровка | 2 |
| 5 | 4 | РАЗДЕЛ 5 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. | Защита от несанкционированного доступа | 2 |
| 6 | 4 | РАЗДЕЛ 6 ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. | Защита информации в глобальной сети. | 4 |
| | | | ВСЕГО: | 16/0 |

### 4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы по дисциплине учебным планом не предусмотрены

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Основы информационной безопасности» осуществляется в форме лекций и практических занятий.
Лекции проводятся в традиционной классно-урочной организационной форме в объеме 34 часов, по типу управления познавательной деятельностью на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративными).
Практические занятия (34 часа) проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения.
Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (36 часа) 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 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 | 4 | РАЗДЕЛ 1<br>ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ | 1. Изучение стандартов в области информационной безопасности<br><br>2. Анализ и дополнительная проработка материала.<br>3. Подготовка к практическим занятиям.<br>4. Изучение учебной литературы из приведенных источников: [1, стр.1-6], [2 стр. 1-8], [3, стр. 1-3]. | 12 |
| 2 | 4 | РАЗДЕЛ 2<br>УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ | 1. Обзор существующих вирусов, троянских программ и сетевых червей.<br><br>2. Анализ и дополнительная проработка материала.<br>3. Подготовка к практическим занятиям.<br>4. Изучение учебной литературы из приведенных источников: [1, стр.7-12], [2 стр. 9-16], [3, стр. 1-3]. | 12 |
| 3 | 4 | РАЗДЕЛ 3<br>ПОЛИТИКА БЕЗОПАСНОСТИ | Анализ и дополнительная проработка материала.<br><br>2. Разработка политики безопасности отдела.<br>3. Подготовка к практическим занятиям.<br>4. Изучение учебной литературы из приведенных источников: [1, стр.13-18], [2 стр. 17-24], [3, стр. 1-3]. | 12 |
| 4 | 4 | РАЗДЕЛ 4<br>КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА | 1. Шифрование и дешифровка сообщений.<br><br>2. Анализ и дополнительная проработка материала.<br>3. Подготовка к практическим занятиям.<br>4. Изучение учебной литературы из приведенных источников: [1, стр.19-24], [2 стр. 25-32], [3, стр. 1-3]. | 12 |
| 5 | 4 | РАЗДЕЛ 5<br>ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. | 1. Обзор протоколов аутентификации.<br><br>2. Анализ и дополнительная проработка материала.<br>3. Подготовка к практическим занятиям.<br>4. Изучение учебной литературы из приведенных источников: [1, стр.25-30], [2 стр. 33-40], [3, стр. 1-3]. | 12 |
| 6 | 4 | РАЗДЕЛ 6<br>ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СЕТИ. | 1. Обзор стандартов рамочного протокола IPSec.<br><br>2. Анализ и дополнительная проработка материала.<br>3. Подготовка к практическим занятиям.<br>4. Изучение учебной литературы из приведенных источников: [1, стр.31-36], [2 стр. 41-48], [3, стр. 1-3]. | 16 |

| | |
|---|---|
| ВСЕГО: | 76 |

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

### 7.1. Основная литература

| № п/п | Наименование | Автор (ы) | Год и место издания Место доступа | Используется при изучении разделов, номера страниц |
|---|---|---|---|---|
| 1 | Криптографическая защита компьютерной информации | Я.М. Голдовский, Б.В. Желенков, И.Е. Сафонова | М.:МИИТ, 2013 НТБ МИИТ | Все разделы |
| 2 | Канальный уровень модели OSI | Б.В. Желенков | М.:МИИТ, 2011 НТБ МИИТ | Все разделы |

### 7.2. Дополнительная литература

| № п/п | Наименование | Автор (ы) | Год и место издания Место доступа | Используется при изучении разделов, номера страниц |
|---|---|---|---|---|
| 3 | Защита информации в вычислительных системах | В.И. Морозова, К.Э. Врублевский | М.:МИИТ, 2008 НТБ МИИТ | Все разделы |

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

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

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

MicrosoftWindows
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 лаборатория для проведения лабораторных занятий, занятий лекционного типа и практических занятий, групповых и индивидуальных консультаций
Маркерная доска, проектор, экран.
Комплекс лабораторных установок под управлением персонального компьютера для проведения лабораторных работ по защите информации.

## 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.