МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ


П.Ф. Бестемьянов

08 сентября 2017 г.

Кафедра «Управление и защита информации»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 1 06 сентября 2017 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 2 04 сентября 2017 г. Заведующий кафедрой  Л.А. Баранов

Москва 2017 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В курсе «Криптографические методы защиты информации» изучаются основные математические методы криптографии. Знания, приобретаемые студентами в процессе изучения этой дисциплины, используются в дисциплинах профессионального цикла, связанных с защитой информации. Цель преподавания дисциплины – обеспечить студентам знания в области теоретической криптографии и её прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности.

Компетенции, приобретаемые студентами, применяются для научно-исследовательской и проектной деятельности:

- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;
- разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов.

Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: основные задачи и понятия криптографии, понятие шифрования, примение принципов шифрования, построение криптографических систем и алгоритмов, применеие алгоритмов при защите информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Криптографические методы защиты информации" 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. Алгебра:

Знания: алгебра матриц, базисы, кольца, поля, группы, подстановки

Умения: решение систем линейных уравнений методом Гаусса, нахоождение обратных элементов в кольцах, работа с матрицами

Навыки: работы с алгебраическими структурами

2.1.2. Теоретико-числовые методы в криптографии:

Знания: конечные поля, группы обратимых элементов в кольцах вычетов

Умения: владение арифметикой конечных полей и алгоритмом Евклида

Навыки: работы в кольцах вычетов, нахождения произведений и обратных элементов в полях

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Криптографические протоколы

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-4 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать и понимать: основные задачи и понятия криптографии, понятие шифрования, принципы шифрования, принципы построения криптографических систем и алгоритмов, применение алгоритмов при защите информации. Уметь: использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки, применять стандарты в области криптографических методов информационной безопасности для проектирования, разработки и анализа защищенности информационных систем. Владеть: криптографическими понятиями, стандартными криптографическими алгоритмами, реализуемыми на компьютерах. приёмами математического моделирования в шифровании.
2	ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать и понимать: основы и методику проведения анализа объектов, систем и экспериментально-исследовательских работ при разработке системы защиты информации. Уметь: применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования. Владеть: приёмами и навыками работы с объектами и системами информационной безопасности с использованием отечественных и зарубежных стандартов.

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

4.1. Общая трудоемкость дисциплины составляет:

5 зачетных единиц (180 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 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)	58	58
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	174	174
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.83	4.83
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), 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 промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	6	Раздел 1 История и основные понятия криптографии	16		10/2	2	20	48/2	ПК1, Контрольная работа
2	6	Тема 1.1 История криптографии	2				3	5	
3	6	Тема 1.2 Основные понятия криптографии	2		2		2	6	
4	6	Тема 1.3 Виды шифров. Результаты К. Шеннона.	2		2		3	7	
5	6	Тема 1.4 Понятие криптоанализа.	2				2	4	
6	6	Тема 1.5 Криптостойкость шифров.	2		2		3	7	
7	6	Тема 1.6 Атаки на шифры.	2			2	2	6	
8	6	Тема 1.7 Статистический анализ шифр-текстов.	2		2/2		3	7/2	
9	6	Тема 1.8 Псевдослучайные последовательности и шифрование.	2		2		2	6	
10	6	Раздел 2 Математические принципы шифрования	16		12/4	2	20	50/4	ПК2, Контрольная работа
11	6	Тема 2.1 Алгоритмы быстрого возведения в степень по модулю.	2		2		3	7	
12	6	Тема 2.2 Алгоритм нахождения НОД.	2				2	4	
13	6	Тема 2.3 Алгоритм нахождения обратного элемента по модулю.	2		2		3	7	
14	6	Тема 2.4 Китайская теорема об остатках.	2		2		2	6	
15	6	Тема 2.5	2		2/2		3	7/2	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Генерирование случайных подстановок, шифры перестановок.							
16	6	Тема 2.6 Простые числа, их распределение, псевдопростые числа.	2				2	4	
17	6	Тема 2.7 Тесты на простоту. Тест Рабина-Миллера.	2		2		2	6	
18	6	Тема 2.8 Построение больших простых чисел.	2		2/2	2	3	9/2	
19	6	Раздел 3 Криптосистемы и понятие протокола	16		10/4	2	18	46/4	КР, Проверка и защита курсовой работы.
20	6	Тема 3.1 Блочное шифрование. Поточные шифры.	2		2		2	6	
21	6	Тема 3.2 Алгоритм шифрования RSA.	2		2/2		2	6/2	
22	6	Тема 3.3 Алгоритм шифрования Эль-Гамаля.	2		2/2		2	6/2	
23	6	Тема 3.4 Алгоритм шифрования Рабина.	2				2	4	
24	6	Тема 3.5 Криптографические хэш-функции.	2		2		2	6	
25	6	Тема 3.6 Понятие эллиптической кривой.	2		2		2	6	
26	6	Тема 3.7 Структура группы на эллиптической кривой.	2				4	6	
27	6	Тема 3.8 Понятие криптопротокола.	2			2	2	6	
28	6	Экзамен						36	ЭК
29		Всего:	48		32/10	6	58	180/10	

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 История и основные понятия криптографии Тема: Основные понятия криптографии	Практичесое занятие №1 Основные понятия криптографии.	2
2	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема: Виды шифров. Результаты К. Шеннона.	Практическое занятие №2 Виды шифров. Результаты К. Шеннона.	2
3	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема: Криптостойкость шифров.	Практическое занятие №3 Криптостойкость шифров.	2
4	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема: Статистический анализ шифр-текстов.	Практическое занятие №4 Статистический анализ шифр-текстов/интерактив.	2 / 2
5	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема: Псевдослучайные последовательности и шифрование.	Практическое занятие №5 Псевдослучайные последовательности и шифрование.	2
6	6	РАЗДЕЛ 2 Математические принципы шифрования Тема: Алгоритмы быстрого возведения в степень по модулю.	Практическое занятие №6 Алгоритмы быстрого возведения в степень по модулю.	2
7	6	РАЗДЕЛ 2 Математические принципы шифрования Тема: Алгоритм нахождения обратного элемента по модулю.	Практическое занятие №7 Алгоритм нахождения обратного элемента по модулю.	2
8	6	РАЗДЕЛ 2 Математические принципы шифрования Тема: Китайская теорема об остатках.	Практическое занятие №8 Китайская теорема об остатках.	2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
9	6	РАЗДЕЛ 2 Математические принципы шифрования Тема: Генерирование случайных подстановок, шифры перестановок.	Практическое занятие №9 Генерирование случайных подстановок, шифры перестановок/интерактив.	2 / 2
10	6	РАЗДЕЛ 2 Математические принципы шифрования Тема: Тесты на простоту. Тест Рабина-Миллера.	Практическое занятие №10 Тесты на простоту. Тест Рабина-Миллера.	2
11	6	РАЗДЕЛ 2 Математические принципы шифрования Тема: Построение больших простых чисел.	Практическое занятие №11 Построение больших простых чисел/интерактив.	2 / 2
12	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема: Блочное шифрование. Поточные шифры.	Практическое занятие №12 Блочное шифрование. Поточные шифры.	2
13	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема: Алгоритм шифрования RSA.	Практическое занятие №13 Алгоритм шифрования RSA/интерактив.	2 / 2
14	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема: Алгоритм шифрования Эль-Гамаля.	Практическое занятие №14 Алгоритм шифрования Эль-Гамаля/ интерактив.	2 / 2
15	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема: Криптографические хэш-функции.	Практическое занятие №15 Криптографические хэш-функции.	2
16	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема: Понятие эллиптической кривой.	Практическое занятие №16 Понятие эллиптической кривой.	2
			ВСЕГО:	32 / 10

4.5. Примерная тематика курсовых проектов (работ)

Цель курсовой работы – закрепление знаний по курсу и развитие у обучающихся навыков самостоятельной творческой работы.
Примерный список рекомендуемых тем: построение больших простых чисел, алгоритмы

шифрования RSA, алгоритмы шифрования Эль-Гамаля, вычисление символа Лежандра, Якоби, эллиптические кривые.
В ходе учебного процесса тематика работ может быть изменена с учётом пожеланий преподавателя и студентов.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Криптографические методы защиты информации» осуществляется в форме лекций, практических занятий и курсовой работы.
Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративные).
Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 22 часов. Остальная часть практического курса (10 часов) проводится с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, дискуссии (решение проблемных поставленных задач и исследование моделей); технологий, основанных на коллективных способах обучения (возможны видеоконференции при подготовке курсовых работ).
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.
Предполагаются консультации студентов по курсовой работе.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, представляющих собой логически завершенный 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, выполнение курсовой работы.

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 История и основные понятия криптографии Тема 1: История криптографии	Подготовка дом. заданий. Литература: [1], [2].	3
2	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 2: Основные понятия криптографии	Подготовка дом. заданий. Литература: [1], [2].	2
3	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 3: Виды шифров. Результаты К. Шеннона.	Подготовка дом. заданий. Литература: [1], [2].	3
4	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 4: Понятие криптоанализа.	Подготовка дом. заданий. Литература: [1], [2].	2
5	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 5: Криптостойкость шифров.	Подготовка дом. заданий. Литература: [1], [2].	3
6	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 6: Атаки на шифры.	Подготовка дом. заданий. Литература: [1], [2].	2
7	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 7: Статистический анализ шифр-текстов.	Подготовка дом. заданий. Литература: [1], [2].	3
8	6	РАЗДЕЛ 1 История и основные понятия криптографии Тема 8: Псевдослучайные последовательности и шифрование.	Подготовка дом. заданий. Литература: [1], [2].	2

9	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 1: Алгоритмы быстрого возведения в степень по модулю.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	3
10	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 2: Алгоритм нахождения НОД.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
11	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 3: Алгоритм нахождения обратного элемента по модулю.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	3
12	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 4: Китайская теорема об остатках.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
13	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 5: Генерирование случайных подстановок, шифры перестановок.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	3
14	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 6: Простые числа, их распределение, псевдопростые числа.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
15	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 7: Тесты на простоту. Тест Рабина-Миллера.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
16	6	РАЗДЕЛ 2 Математические принципы шифрования Тема 8: Построение больших простых чисел.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	3
17	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2

		Тема 1: Блочное шифрование. Поточные шифры.		
18	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 2: Алгоритм шифрования RSA.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
19	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 3: Алгоритм шифрования Эль-Гамаля.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
20	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 4: Алгоритм шифрования Рабина.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
21	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 5: Криптографические хэш-функции.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
22	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 6: Понятие эллиптической кривой.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
23	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 7: Структура группы на эллиптической кривой.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	4
24	6	РАЗДЕЛ 3 Криптосистемы и понятие протокола Тема 8: Понятие криптопротокола.	Подготовка дом. заданий, выполнение курсовой работы. Литература: [1], [2].	2
			ВСЕГО:	58

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: учебный курс.	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. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Ященко	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 Клюшиной Д.А.	Издательский дом Вильямс, 2005 НТБ (фб.)	Все разделы
6	Классическое введение в современную теорию чисел	К. Айерленд; Пер. с англ. С.П. Демушкина ; Под ред. А.Н. Паршина; Под Ред. А.Н. Паршин	Мир, 1987 НТБ (фб.)	Все разделы
7	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 указаниям 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.