МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

25 мая 2018 г.

Кафедра «Управление и защита информации»

Автор Клепцов Михаил Яковлевич, д.т.н., профессор

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации

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	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 15 мая 2018 г. Заведующий кафедрой  Л.А. Баранов

Москва 2018 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих.
Студенты должны научиться применять современные средства защиты информации предоставляемые сетевым оборудованием, являющимся самым уязвимым местом при попытке несанкционированного доступа.

Основными задачами дисциплины являются:
• Ознакомление с основными терминами и определениями.
• Ознакомление с основными типами угроз и атак.
• Изучение механизмов защиты административного интерфейса и разграничения прав доступа.
• Изучение технологии AAA.
• Изучение способов защиты информации в сетях.
• Изучение принципов построения виртуальных частных сетей.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
научно-исследовательская;
контрольно-аналитическая;
специализация №8.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
Научно-исследовательская деятельность:
сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;
изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;
подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.
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.
Специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем":
разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации" 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. Методы программирования:

Знания: современное состояние уровня и направлений развития вычислительной техники и программных средств, основные алгоритмы типовых численных методов решения математических задач, один из языков 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 навыками работы с программными средствами общего назначения, соответствующими современным требованиям мирового рынка, включая приемы антивирусной защиты.

2.1.2. Сети и системы передачи информации:

Знания: принципы работы сетевых протоколов и сетевых устройств, классификацию сетевого оборудования.методы и системы моделирования работы сети, сетевого оборудования и протоколовсовременные элементы архитектуры вычислительных сетей

Умения: оформлять документацию по СКСрассчитывать необходимые ресурсы для монтажа и определять методы поиска неисправностей в процессе настройки и отладки работы сети

Навыки: навыками систематизации информации и формулирования задач при эксплуатации СКС навыками использования монтажного оборудования и программно-аппаратных отладочных средств для введения сети в эксплуатацию

2.2. Наименование последующих дисциплин

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать и понимать: основные принципы и методики разработки математических моделей угроз, нарушителей и безопасности КС Уметь: проводить анализ и разрабатывать математические модели безопасности КС Владеть: навыками разработки и анализа моделей угроз, моделей нарушителя и моделей обеспечения безопасности
2	ПК-11 способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знать и понимать: основные этапы и методику проведения экспериментально-исследовательских работ при пректировании; требования по сертификации средств защиты информации Уметь: проводить экспериментально-исследовательские работы с учетом всех наложенных ограничений и требований Владеть: навыками участия в работах по исследованию средств защиты информации
3	ПК-3 способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать и понимать: отечественные и зарубежные стандарты в области компьютерной безопасности; современные методы анализа и оценки защищенности компьютерной системы; нормативные документы и методические материалы по методам обеспечения информационной безопасности компьютерных систем Уметь: проводить сбор и анализ исходных данных для проектирования систем защиты информации; проводить анализ проектных решений по обеспечению защищенности компьютерных систем Владеть: навыками сбора и анализа исходных данных для проектирования систем защиты информации; навыками применения современных методов и средства исследований для обеспечения информационной безопасности компьютерных систем;навыками подбора, изучения и обобщения научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем.
4	ПСК-8.3 способностью проводить анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и систем обеспечения информационной безопасности процессов их проектирования, создания и модернизации	Знать и понимать: принципы анализа систем обеспечения безопасности объектов информатизации Уметь: проводить анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем

№ п/п	Код и название компетенции	Ожидаемые результаты
		Владеть: навыками анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении на предмет их соответствия требованиям по обеспечению информационной безопасности

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

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 10
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)	25	25
Экзамен (при наличии)	45	45
ОБЩАЯ трудоемкость дисциплины, часы:	142	142
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.94	3.94
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 промежу-точной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	10	Раздел 1 Защита информации Основные термины и определения. Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. Рассматриваются основные направления действия системы защиты информации и принципы ее организации.	2		2		2	6	
2	10	Раздел 2 Политика защиты Сетевая безопасность. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними. Вирусы. Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.	6		6/4		5	17/4	

№ 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
3	10	Раздел 3 Защита сети Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.	6		6/6	1	5	18/6	ПК1
4	10	Раздел 4 Защита сетевых соединений Модели обороны. Рассматриваются существующие	8		8/6		5	21/6	

№ 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
		модели обороны, их преимущества и недостатки. Защита периметра сети. Описывается зонная архитектура защиты сети и ее компоненты. Контроль сервисов TCP/IP. Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Контроль доступа. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак.							
5	10	Раздел 5 Шифрование Механизмы шифрования. Рассматриваются различные варианты построения систем шифрования и их свойства. Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и	8		8/4	1	4	21/4	ПК2

№ 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
		схемы построения цифровой подписи, алгоритм DSA. Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне.							
6	10	Раздел 6 Построение виртуальных частных сетей с использованием IPSec Обзор технологии виртуальных частных сетей. Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки. Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE. Настройка IPSec VPN. Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.	6		6		4	16	
7	10	Экзамен						45	ЭК
8		Всего:	36		36/20	2	25	144/20	

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	10		Защита информации Основные термины и определения. Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. Рассматриваются основные направления действия системы защиты информации и принципы ее организации.	2
2	10		Политика защиты Сетевая безопасность. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними. Вирусы. Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.	6 / 4
3	10		Защита сети Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.	6 / 6

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
4	10		Защита сетевых соединений Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки. Защита периметра сети. Описывается зонная архитектура защиты сети и ее компоненты. Контроль сервисов TCP/IP. Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Контроль доступа. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак.	8 / 6
5	10		Шифрование Механизмы шифрования. Рассматриваются различные варианты построения систем шифрования и их свойства. Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA. Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне.	8 / 4
6	10		Построение виртуальных частных сетей с использованием IPSec Обзор технологии виртуальных частных сетей. Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки. Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE. Настройка IPSec VPN. Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.	6
			ВСЕГО:	36 / 20

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Программно-аппаратные средства защиты информации» осуществляется в форме лекций и практических занятий.
Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).
Курс практических занятий проводится с использованием сетевого оборудования и на специальных программных симуляторах, разработанных на кафедре, основанных на интерактивных (диалоговых) технологиях, в том числе на сетевом оборудовании (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы.
Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы относится отработка лекционного материала и отработка отдельных тем по учебным пособиям, подготовка к интерактивным практическим и лабораторным работам.
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	10		Защита информации Основные термины и определения. Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. Рассматриваются основные направления действия системы защиты информации и принципы ее организации.	2
2	10		Политика защиты Сетевая безопасность. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними. Вирусы. Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.	5
3	10		Защита сети Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.	5
4	10		Защита сетевых соединений Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки. Защита периметра сети. Описывается зонная архитектура защиты сети и ее компоненты. Контроль сервисов TCP/IP. Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Контроль доступа. Описываются средства контроля доступа с	5

			использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак.	
5	10		Шифрование Механизмы шифрования. Рассматриваются различные варианты построения систем шифрования и их свойства. Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA. Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне.	4
6	10		Построение виртуальных частных сетей с использованием IPSec Обзор технологии виртуальных частных сетей. Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки. Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE. Настройка IPSec VPN. Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.	4
			ВСЕГО:	25

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 построения опорных сетей ISP. Учебное пособие.	Желенков Б.В.	МИИТ, 2009 http://library.miit.ru/ УДК 681.3 Ж51	Все разделы
2	Проектирование кампусных сетей: Учебное пособие.	Голдовский Я.М.	МИИТ, 2009 http://library.miit.ru/ УДК 681.3 Г60	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам.	Голдовский Я.М. Желенков Б.В.	МИИТ, 2013 http://library.miit.ru/ УДК 681.3 Г60	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)

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:
Foxit Reader/Acrobat Reader
Microsoft Office (Power Point)
Установлен мультимедийный курс лекций.
Для проведения практических занятий необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:
Foxit Reader/Acrobat Reader
Microsoft Office (Word).
На рабочие места должны быть установлены программные разработки кафедры «Вычислительные системы и сети»:
Обучающая система «netlab»

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

Для проведения аудиторных занятий требуется специализированная лекционная аудитория с мультимедиа аппаратурой.
Для проведения лабораторных работ:
компьютеры с предустановленным Microsoft Windows не ниже Windows XP и процессором не ниже Pentium 4.
- маршрутизаторы Cisco;
- коммутаторы Cisco;
- соединительные кабели различных типов

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 лабораторных работ 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 лабораторных работ 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.
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.