МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Энергетический факультет

Кафедра Физики и техники связи

УТВЕРЖДАЮ:

Декан факультета

Мирошников С.Ф.

«____»_____20____г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.Б.35.01.Проектирование защищенных телекоммуникационных систем

на 252 часа(ов), 7 зачетных(ые) единиц(ы)

для направления подготовки (специальности) 10.05.02 – Информационная безопасность телекоммуникационных систем

составлена в соответствии с ФГОС ВО, утвержденным приказом Министерства образования и науки Российской Федерации от «___» _____ 20____ г. №_____

Специализация – Защита информации в системах связи и управления (для набора 2020)

Форма обучения очная

1. Организационно-методический раздел

1.1 Цель и задачи дисциплины (модуля)

Цель изучения дисциплины:

Дисциплина «Проектирование защищенных телекоммуникационных систем» имеет целью сформировать у учащихся знания о базовых принципах и подходах к проектированию защищенных телекоммуникационных систем и сетей, в том числе мультисервисных сетей связи, а
также обеспечить развитие практических навыков и способностей к решению прикладных задач
проектирования

Задачи изучения дисциплины:

Задача дисциплины – получение учащимися базовых знаний о процессе и методах проектирования современных телекоммуникационных систем и сетей, включая навыки по анализу
проектируемых систем и расчету показателей качества проектируемых систем.

1.2. Место дисциплины (модуля) в структуре ОП

Учебная дисциплина «Проектирование защищенных телекоммуникационных систем» является обязательной, входит в блок Б1.Б.35.01

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 7 зачетных(ые) единиц(ы), 252 часов.

Очная форма

Виды занятий	Распределение по семестрам		Всего часов
	9 семестр	10 семестр	
Общая трудоемкость			252
Аудиторные занятия, в т.ч.	68	48	116
лекционные (ЛК)	34	32	66
практические (семинарские) (ПЗ, СЗ)	17	16	33
лабораторные (ЛР)	17	0	17
Самостоятельная работа студентов (СРС)	40	24	64
Форма промежуточной аттестации в семестре	Зачет	Экзамен	36
Курсовая работа (курсовой проект) (КР, КП)	КП		

2. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Индекс компетенции	Содержание компетенции
ПК-1	Способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем
ПК-2	Способность формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов
ПК-5	Способность проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов
ПК-7	Способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования
ПСК – 10.1	Способность применять теорию сигналов и систем для анализа телекоммуникационных систем и оценки их помехоустойчивости
ПСК – 10.3	Способность оценивать возможности средств технических разведок в отношении к системам связи, управления и объектами информатизации

Планируемые результаты обучения по дисциплине для последовательного достижения уровней сформированности компетенций

Результат обучения	
Знать	Пороговый: общие принципы проектирования современных систем и сетей телекоммуникаций, включая мультисервисные сети связи

Знать	Стандартный: современную элементную базу телекоммуникационных систем
	Эталонный: основные стандарты, протоколы и интерфейсы, используемые в телекоммуникационных системах
Уметь	Пороговый: - выбирать эффективные модели сигналов, помех и каналов связи, методов формирования и преобразования сигналов в телекоммуникационных систем
	Стандартный: проводить анализ логических устройств, устройств телекоммуникационных систем на базе микропроцессорной техники
	Эталонный: - разрабатывать модели и проводить статистический анализ проектируемых систем и сетей телекоммуникаций ; проводить анализ показателей качества проектируемых сетей и систем телекоммуникаций
Владеть	Пороговый: навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений
	Стандартный: навыками оценки эффективности и оптимизации параметров телекоммуникационных систем
	Эталонный: навыками работы с системами автоматизированного проектирования и математического моделирования

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

Очная форма

Модуль	Номер раздела	Наименование раздела	Всего часов	Аудиторные занятия			СРС
				ЛК	ПЗ(СЗ)	ЛР	
1	1	Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров по специальности «Комплексное обеспечение информационной безопасности».	26	9	4	4	9
	2	Особенности построения и функционирования ИТКС с позиции обеспечения безопасности информации	22	9	4	0	9
	3	Угрозы безопасности информации в автоматизированных системах	27	9	5	4	9
2	4	Классификация мер и средств защиты информации в ИТКС	23	9	5	0	9
	5	Меры и средства защиты информации от несанкционированного доступа	30	10	5	6	9
3	6	Технологическая схема проектирования систем защиты информации в информационно – телекоммуникационных системах	24	10	5	0	9
	7	Требования по защите информации к автоматизированным системам и их реализация при проектировании	28	10	5	3	10
Итого			180	66	33	17	64

3.2. Лекционные занятия

Очная форма

Модуль	Номер раздела	Содержание лекционных занятий
	1	Структура курса. Разделы и темы. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы по курсу. Методика работы студентов по изучению курса. Знания и умения, которые должны быть получены в результате изучения курса
	2	Понятие автоматизированной системы. Основные классы ИТКС. Информация и элементы построения ИТКС как объекты обеспечения безопасности информации. Основные базовые сетевые технологии для ИТКС. Характеристика и особенности технологии Ethernet, Token Ring, Frame Relay с позиции защиты информации. Эволюция технологии Ethernet: особенности технологий Fast Ethernet, Gigabit Ethernet. Характеристика и особенности технологии ATM. Перспективы развития ATM-сетей.

1	3	Понятия "угрозы безопасности информации", "источника угрозы". Источники угроз безопасности информации. Причины и условия возникновения угроз безопасности информации. Понятия целостности, конфиденциальности и доступности информации. Система классификаторов для классификации угроз. Классификационная схема угроз безопасности информации и ее характеристика. Понятия природных, техногенных и антропогенных угроз, несанкционированного доступа, несанкционированного воздействия. Последствия реализации угроз безопасности информации. Дополнительная классификация сетевых угроз безопасности информации. Понятия удаленной внутрисегментной, межсегментной атаки в сети. Основные классы атак, реализуемых в сетях, функционирующих с использованием стека протоколов TCP/IP, и их характеристика. Возможные варианты реализации атак типа "Анализ сетевого трафика", "Отказ в обслуживании", "Подмена доверенного объекта", "Создания ложного объекта". Причины, обусловливающие возможность реализации сетевых атак. Оценка возможности реализации и опасности сетевых атак. Угрозы утечки информации по техническим каналам в ИТКС. Понятие технического канала утечки информации. Классификация технических каналов утечки. Краткая характеристика основных технических каналов утечки информации в ИТКС Угрозы программно-математического воздействия и особенности их реализации в ИТКС. Последствия от реализации вредоносных программ
2	4	Понятие меры и средства защиты информации. Общий подход к классификации мер и средств защиты информации. Система классификационных признаков и общая классификационная схема мер и средств защиты информации в ИТКС. Классификация и общая характеристика мер и средств защиты информации от угроз, связанных с несанкционированным доступом, в том числе от угроз физического доступа к элементам ИТКС, сетевых атак при подключении к глобальным сетям общего пользования, от угроз программно-математического воздействия. Классификация и общая характеристика мер и средств защиты информации от утечки по техническим каналам, а также от перехвата и съема информации при передаче по линиям телефонной связи. Классификация и краткая характеристика мер и средств контроля несанкционированного доступа к элементам ИТКС и к циркулирующей в них информации
	5	Меры и средства разграничения доступа в сетях. Криптографические и стеганографические способы и средства защиты информации в ИТКС. Основы построения частных виртуальных сетей. Специальные меры и средства защиты информации от программно-математического воздействия. Основы межсетевого экранирования: основные функции межсетевого экранирования, виды межсетевых экранов; сертифицированные средства межсетевого экранирования, способы применения межсетевых экранов в ИТКС

3	6	Общая характеристика процесса проектирования ИТКС. Основные направления защиты информации в ИТКС. Обобщенная структура системы защиты информации. Основные этапы проектирования систем защиты информации. Обобщенная технологическая схема проектирования систем защиты информации в ИТКС и ее характеристика. Понятия задачи, стратегии, концепции и способа защиты информации. Характеристика содержания работ при проектировании систем защиты информации для функционирующих и развертываемых ИТКС. Требования руководящих документов по порядку проектирования ИТКС в защищенном исполнении
	7	Количественный и качественный подходы к обоснованию требований по защите информации в ИТКС. Общий порядок обоснования требований Требования по защите информации, предъявляемые к автоматизированным системам. Классы защищенности информации в автоматизированных системах. Номенклатура и содержание требований к подсистемам защиты информации в компьютерных сетях в соответствии с действующими нормативными документами. Требования к элементам ИТКС по защите информации и к элементам систем защиты информации в ИТКС. Требования к межсетевым экранам как важнейшим средствам обеспечения защиты информации при межсетевом взаимодействии в ИТКС.

3.3. Практические (семинарские) занятия

Очная форма

Модуль	Номер раздела	Содержание практических(семинарских) занятий
	1	Структура курса. Разделы и темы. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы по курсу. Методика работы студентов по изучению курса. Знания и умения, которые должны быть получены в результате изучения курса
	2	Понятие автоматизированной системы. Основные классы ИТКС. Информация и элементы построения ИТКС как объекты обеспечения безопасности информации. Основные базовые сетевые технологии для ИТКС. Характеристика и особенности технологии Ethernet, Token Ring, Frame Relay с позиции защиты информации. Эволюция технологии Ethernet: особенности технологий Fast Ethernet, Gigabit Ethernet. Характеристика и особенности технологии ATM. Перспективы развития ATM-сетей.

1	3	Понятия "угрозы безопасности информации", "источника угрозы". Источники угроз безопасности информации. Причины и условия возникновения угроз безопасности информации. Понятия целостности, конфиденциальности и доступности информации. Система классификаторов для классификации угроз. Классификационная схема угроз безопасности информации и ее характеристика. Понятия природных, техногенных и антропогенных угроз, несанкционированного доступа, несанкционированного воздействия. Последствия реализации угроз безопасности информации. Дополнительная классификация сетевых угроз безопасности информации. Понятия удаленной внутрисегментной, межсегментной атаки в сети. Основные классы атак, реализуемых в сетях, функционирующих с использованием стека протоколов TCP/IP, и их характеристика. Возможные варианты реализации атак типа "Анализ сетевого трафика", "Отказ в обслуживании", "Подмена доверенного объекта", "Создания ложного объекта". Причины, обусловливающие возможность реализации сетевых атак. Оценка возможности реализации и опасности сетевых атак. Угрозы утечки информации по техническим каналам в ИТКС. Понятие технического канала утечки информации. Классификация технических каналов утечки. Краткая характеристика основных технических каналов утечки информации в ИТКС Угрозы программно-математического воздействия и особенности их реализации в ИТКС. Последствия от реализации вредоносных программ
2	4	Понятие меры и средства защиты информации. Общий подход к классификации мер и средств защиты информации. Система классификационных признаков и общая классификационная схема мер и средств защиты информации в ИТКС. Классификация и общая характеристика мер и средств защиты информации от угроз, связанных с несанкционированным доступом, в том числе от угроз физического доступа к элементам ИТКС, сетевых атак при подключении к глобальным сетям общего пользования, от угроз программно-математического воздействия. Классификация и общая характеристика мер и средств защиты информации от утечки по техническим каналам, а также от перехвата и съема информации при передаче по линиям телефонной связи. Классификация и краткая характеристика мер и средств контроля несанкционированного доступа к элементам ИТКС и к циркулирующей в них информации
	5	Меры и средства разграничения доступа в сетях. Криптографические и стеганографические способы и средства защиты информации в ИТКС. Основы построения частных виртуальных сетей. Специальные меры и средства защиты информации от программно-математического воздействия. Основы межсетевого экранирования: основные функции межсетевого экранирования, виды межсетевых экранов; сертифицированные средства межсетевого экранирования, способы применения межсетевых экранов в ИТКС

3	6	Общая характеристика процесса проектирования ИТКС. Основные направления защиты информации в ИТКС. Обобщенная структура системы защиты информации. Основные этапы проектирования систем защиты информации. Обобщенная технологическая схема проектирования систем защиты информации в ИТКС и ее характеристика. Понятия задачи, стратегии, концепции и способа защиты информации. Характеристика содержания работ при проектировании систем защиты информации для функционирующих и развертываемых ИТКС. Требования руководящих документов по порядку проектирования ИТКС в защищенном исполнении
	7	Количественный и качественный подходы к обоснованию требований по защите информации в ИТКС. Общий порядок обоснования требований Требования по защите информации, предъявляемые к автоматизированным системам. Классы защищенности информации в автоматизированных системах. Номенклатура и содержание требований к подсистемам защиты информации в компьютерных сетях в соответствии с действующими нормативными документами. Требования к элементам ИТКС по защите информации и к элементам систем защиты информации в ИТКС. Требования к межсетевым экранам как важнейшим средствам обеспечения защиты информации при межсетевом взаимодействии в ИТКС.

3.4. Лабораторные занятия

Очная форма

Модуль	Номер раздела	Содержание лабораторных занятий
	1	Структура курса. Разделы и темы. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы по курсу. Методика работы студентов по изучению курса. Знания и умения, которые должны быть получены в результате изучения курса

1	3	Понятия "угрозы безопасности информации", "источника угрозы". Источники угроз безопасности информации. Причины и условия возникновения угроз безопасности информации. Понятия целостности, конфиденциальности и доступности информации. Система классификаторов для классификации угроз. Классификационная схема угроз безопасности информации и ее характеристика. Понятия природных, техногенных и антропогенных угроз, несанкционированного доступа, несанкционированного воздействия. Последствия реализации угроз безопасности информации. Дополнительная классификация сетевых угроз безопасности информации. Понятия удаленной внутрисегментной, межсегментной атаки в сети. Основные классы атак, реализуемых в сетях, функционирующих с использованием стека протоколов TCP/IP, и их характеристика. Возможные варианты реализации атак типа "Анализ сетевого трафика", "Отказ в обслуживании", "Подмена доверенного объекта", "Создания ложного объекта". Причины, обусловливающие возможность реализации сетевых атак. Оценка возможности реализации и опасности сетевых атак. Угрозы утечки информации по техническим каналам в ИТКС. Понятие технического канала утечки информации. Классификация технических каналов утечки. Краткая характеристика основных технических каналов утечки информации в ИТКС Угрозы программно-математического воздействия и особенности их реализации в ИТКС. Последствия от реализации вредоносных программ
2	5	Меры и средства разграничения доступа в сетях. Криптографические и стеганографические способы и средства защиты информации в ИТКС. Основы построения частных виртуальных сетей. Специальные меры и средства защиты информации от программно-математического воздействия. Основы межсетевого экранирования: основные функции межсетевого экранирования, виды межсетевых экранов; сертифицированные средства межсетевого экранирования, способы применения межсетевых экранов в ИТКС
3	7	Количественный и качественный подходы к обоснованию требований по защите информации в ИТКС. Общий порядок обоснования требований Требования по защите информации, предъявляемые к автоматизированным системам. Классы защищенности информации в автоматизированных системах. Номенклатура и содержание требований к подсистемам защиты информации в компьютерных сетях в соответствии с действующими нормативными документами. Требования к элементам ИТКС по защите информации и к элементам систем защиты информации в ИТКС. Требования к межсетевым экранам как важнейшим средствам обеспечения защиты информации при межсетевом взаимодействии в ИТКС.

3.5. Организация самостоятельной работы

Очная форма

Модуль	Номер раздела	Содержание материала выносимого на самостоятельное изучение	Виды самостоятельной работы

4. Интерактивные формы образовательных технологий

Модуль	Номер раздела	Вид учебных занятий	Образовательные технологии	Количество часов
1-17	1-17	пр	Выполнение практических заданий	10

5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература

6.1.1. Печатные издания

1.Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей : учеб. пособие / под ред. В.Н. Гордиенко, М.С. Тверецкого. - Москва : Горячая линия-Телеком, 2008. - 392 с. : ил. - ISBN 978-5-9912-0010-3 : 345-00.
2. Цифровые и аналоговые системы передачи : учеб. / под ред. В.И. Иванова. - 2-е изд. - Москва : Горячая линия-Телеком, 2003. - 232 с. : ил. - ISBN 5-93517-116-3 : 137-50.

6.1.2. Издания из ЭБС

1. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей : Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям "Многоканальные телекоммуникационные системы", "Сети связи и системы коммутации", "Физика и техника оптической связи" направления "Телекоммуникации" / Алексеев Е.Б.; Гордиенко В.Н.; Крухмалев В.В.; Моченов А.Д.; Тверецкий М.С. - Moscow : Горячая линия - Телеком, 2012. - . - Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей [Электронный ресурс] : Учебное пособие для вузов / Е.Б. Алексеев, В.Н. Гордиенко, В.В. Крухмалев и др.; Под ред. В.Н. Гордиенко, М.С. Тверецкого. - 2-е изд., испр. - М. : Горячая линия - Телеком, 2012. - http://www.studentlibrary.ru/book/ISBN9785991202543.html. - ISBN 978-5-9912-0254-3 .

6.2. Дополнительная литература

6.2.1. Печатные издания

1. Халсалл, Ф. Передача данных, сети компьютеров и взаимосвязь открытых систем. - Москва : Радио и связь, 1995. - 408с. : ил. - ISBN 5-256-0006002 : 50-00.
2. Ковалевская, Л.В. Методы тестирования спектральных характеристик систем WDM : учеб. пособие. - Чита : ЗабГУ, 2015. - 108 с. - ISBN 978-5-9293-1481-0 : 108-00.
.

6.2.2. Издания из ЭБС

6.3. Базы данных, информационно-справочные и поисковые системы

Операционные системы Windows, стандартные офисные программы, электронные версии учебников, пособий, методических разработок, указаний и рекомендаций по всем видам учебной работы, предусмотренных рабочей программой, находящиеся в свободном доступе для студентов ЗабГУ.

7. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".
Программное обеспечение специального назначения:

8. Материально-техническое обеспечение дисциплины

Ауд. 08-210. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных кон-сультаций, текущего контроля и промежуточной аттестации. Комплект специализированной учебной мебели. Доска маркерная. Комплект мо-бильного оборудования, который организован в виде мобильного пере-движного многофункционального комплекса (устанавливается в аудито-рии по заявке преподавателя): ноутбук, мультимедийный проектор, эк-ран.
Ауд. 08-310. Кабинет информатики и Интернет-технологий . Лаборато-рия мультисервисных сетей . Учебная аудитория для проведения заня-тий семинарского типа, курсового и дипломного проектирования, науч-но-исследовательской работы, групповых и индивидуальных консульта-ций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся. Рабочие места на базе вычислительной техники и абонентские устройства, подключенные к сети «Интернет» с использо-ванием проводных и/или беспроводных технологий, с установленным офисным пакетом и набором необходимых для проведения исследова-ний дополнительных аппаратных и(или) программных средств, а также оборудованием для печати. Обеспечение доступа в электронную информационно-образовательную среду организации. Переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук. Комплект специальной учебной мебели. Стойка Hyperline, ASCON Energy Sustems, ЦАТС МС 240 Зав.№403.
Ауд. 08-20. Лаборатория систем коммутации. Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Ком-плект специальной учебной мебели. Стойка Hyperline, ASCON Energy Sustems, ЦАТС МС 240 Зав.№403, кабельрост ПВМ администратора станции. Доступ к сети Интернет и обеспечение доступа в электронную информационно-образовательную среду организации. Переносной мультимедийный к-т в составе: экран на треноге, мультимедиапроектор, ноутбук.

9. Методические рекомендации по организации изучения дисциплины

Лекции являются основным источником теоретического материала . Посещение и конспектирование лекций является
обязательной составляющей успешного освоения дисциплины обучающимися.
Для эффективного освоения материала дисциплины «Электромагнитные поля и волны» необходимо выполнение следующих требований:
- обязательное посещение всех лекционных и практических занятий, способствую-щее системному овладению материалом курса;
- все вопросы соответствующих разделов и тем по дисциплине необходимо фикси-ровать (на любых носителях информации);
- обязательное выполнение домашних заданий является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;

- обязательность личной активности каждого студента на всех занятиях по дисцип-лине;
- в случаях неясности каких-либо вопросов, обсуждаемых на занятиях, необходимо задать соответствующие вопросы преподавателю, а не оставлять их непонятыми;
- в случаях пропусков занятий по уважительным причинам студентам предоставля-ется право подготовки и представления заданий и ответов на вопросы изученного мате-риала, с расчетом на помощь преподавателя в его усвоении;
- в случаях пропусков без уважительной причины студент обязан самостоятельно изучить соответствующий материал;
- необходимым условием является самостоятельность и инициативность студентов при контроле набора баллов по дисциплине для успешного прохождения промежуточной аттестации.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов предполагает:
- самостоятельный поиск, обработку (анализ, синтез, обобщение и систематиза-цию), адаптацию необходимой по дисциплине информации;
- выполнение заданий для самостоятельной работы; - изучение и усвоение теоретического материала, представленного на лекционных
занятиях и в соответствующих литературных источниках (рекомендуемая основная и до-полнительная литература);
- самостоятельное изучение отдельных вопросов курса;
- подготовка к практическим и лабораторным занятиям, в соответствии с рекомен-дациями преподавателя (выполнение конкретных заданий, соответствующие организаци-онные действия и т.д.).

Порядок организации лабораторной работы студентов

Лабораторная работа студентов предполагает сознательной активной работы не только в лаборатории при сборке установки и проведении измерений, но и дома при под-готовке к измерениям, обработке результатов и составления отчета.

Выполнение лабораторной работы есть определенная последовательность действий:
— подготовка к эксперименту;
— проведение измерений;
— обработка полученных результатов;
— формулировка выводов и написание отчета.

Для грамотного и быстрого их выполнения должна сложиться определенная систе-ма знаний и умений (ориентировочная основа действия), которая обеспечит правильное и рациональное исполнение действия.

Поэтому выполнение каждой лабораторной работы необходимо начинать с изуче-ния ее описания и приведения знаний в систему, а именно:
— ясно представить себе общую цель данной конкретной лабораторной работы и после-довательность задач, решение которых приведет к достижению окончательной цели;
— знать, какое физическое явление изучается в данной работе, какими зависимостям свя-заны описывающие его величины;
— знать основные особенности объекта исследования
— изучить и уметь объяснить физические основы используемых в работе методов изме-рения искомых величин;— уметь нарисовать принципиальную схему используемой установки и знать назначение
каждого из ее узлов;
— знать последовательность выполнения этапов лабораторной работы;
— иметь общее представление об ожидаемых результатах проводимого эксперимента и уметь выбрать метод, нужный для их математической обработки

Порядок организации студентов на практическом занятии

На практических занятиях обобщаются и систематизируются знания, полученные на лекционных занятиях, и формируются умения решать типовые задачи. При решении задач студент должен уметь:
- выделять описываемое явление (объект), анализировать условие задачи;
- выполнять построение модели явления;
- формулировать выводы из модели;
- выявлять применения полученных знаний в профессиональной деятельности.

Разработчик/группа разработчиков: Свешников Игорь Вадимович зав. кафедрой ФиТС

Рассмотрена на заседании кафедры
(протокол от 24.05.2019 г. № 16)