

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

Энергетический факультет

Батухтин Андрей
Геннадьевич

«_____» _____ 20____
г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.06 Проектирование защищенных телекоммуникационных систем
на 252 часа(ов), 7 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 11.04.02 - Инфокоммуникационные
технологии и системы связи

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

Профиль – Безопасность инфокоммуникационных систем и сетей (для набора 2023)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

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:

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.

изучение способов представления информации, её преобразования, современные способы получения хранения и выдачи цифровой информации применительно к защищенным инфокоммуникационным системам и сетям

овладение основными методами и средствами получения, хранения, переработки информации в защищенных инфокоммуникационных системах и сетях

1.2. Место дисциплины (модуля) в структуре ОП

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

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

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

Виды занятий	Семестр 2	Семестр 3	Всего часов
Общая трудоемкость			252
Аудиторные занятия, в т.ч.	24	34	58
Лекционные (ЛК)	12	17	29
Практические (семинарские) (ПЗ, СЗ)	12	0	12
Лабораторные (ЛР)	0	17	17
Самостоятельная работа студентов (СРС)	84	74	158

Форма промежуточной аттестации в семестре	Зачет	Экзамен	36
Курсовая работа (курсовой проект) (КР, КП)			

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
ОПК-4	Способность разрабатывать и применять специализированное программно-математическое обеспечение для проведения исследований и решении проектно-конструкторских и научно-исследовательских задач	<p>Знать: основные методы обработки экспериментальных данных с помощью современного специализированного программно-математического обеспечения при решении научно-исследовательских задач</p> <p>Уметь: использовать современное специализированное программно-математическое обеспечение для решения задач приема, обработки и передачи информации и проведения исследований в области инфокоммуникаций</p> <p>Владеть: методами компьютерного моделирования и обработки информации с помощью специализированного программно-математического обеспечения</p>
ПК-1	Способность использовать современные достижения науки и передовые инфокоммуникационные технологии, методы проведения теоретических и экспериментальных исследований	Знать: технические характеристики и экономические показатели отечественных и зарубежных разработок в области радиоэлектронной техники, действующие нормативные требования и государственные

	<p>в научно-исследовательских работах в области ИКТиСС, ставить задачи исследования, выбирать методы экспериментальной работы с целью совершенствования и созданию новых перспективных инфокоммуникационных систем</p>	<p>стандарты</p> <p>Уметь: осуществлять патентный поиск, проводить сбор, анализ и систематизацию научно-исследовательской информации, формулировать цели и задачи научно-исследовательских работ в области создания и проектирования радиоэлектронных устройств и систем; разрабатывать техническое задание, требования и условия на разработку и проектирование радиоэлектронных устройств и систем</p> <p>Владеть: навыками разработки и анализа вариантов создания радиоэлектронного устройства или радиоэлектронной системы на основе синтеза накопленного опыта, изучения литературы и собственной интуиции; прогнозу последствий, поиск компромиссных решений в условиях многокритериальности</p>
ПК-2	<p>Способность самостоятельно выполнять экспериментальные исследования для решения научно-исследовательских и производственных задач с использованием современной аппаратуры и методов исследования</p>	<p>Знать: методики сбора, анализа и обработки статистической информации инфокоммуникационных систем</p> <p>Уметь: проводить исследования характеристик телекоммуникационного оборудования и оценки качества предоставляемых услуг</p> <p>Владеть: навыками анализа научно-технической проблемы на основе подбора и изучения литературных и патентных источников; навыками проведения экспериментальных работ по проверке достижимости технических характеристик, радиоэлектронной аппаратуры</p>
ПК-6	<p>Способность к разработке моделей</p>	<p>Знать: принципы построения</p>

	<p>различных технологических процессов и проверке их адекватности на практике, готовностью использовать пакеты прикладных программ анализа и синтеза инфокоммуникационных систем, сетей и устройств</p>	<p>технического задания, моделей технологических процессов и проверке их адекватности на практике, при проектировании средств и сетей связи и их элементов</p> <p>Уметь: осуществлять сбор и анализ исходных данных для расчета и проектирования деталей, узлов и устройств радиотехнических и инфокоммуникационных систем и/или их составляющих; осуществлять расчет основных показателей качества инфокоммуникационных систем и/или их составляющих; разрабатывать и оформлять конструкторскую и техническую документацию в соответствии с действующими нормативными документами с применением систем компьютерного проектирования</p> <p>Владеть: навыками проведения необходимых экономических расчетов и технико-экономических обоснований принятых решений по разработке инфокоммуникационных систем и/или их составляющих; современными отечественными и зарубежными пакетами программ для решения схемотехнических, системных и сетевых задач</p>
ПК-9	<p>Способность к проектированию, строительству, монтажу и эксплуатации радиоэлектронных средств инфокоммуникаций, направляющих сред передачи информации</p>	<p>Знать: технические характеристики и экономические показатели отечественных и зарубежных разработок в области радиоэлектронной техники; методическую и нормативную базу в области разработки и проектирования радиоэлектронных устройств, направляющих сред передачи информации инфокоммуникаций</p>

		<p>Уметь: формулировать цели и задачи проектирования радиоэлектронных устройств и систем; разрабатывать техническое задание, требования и условия на проектирование радиоэлектронных устройств и систем</p> <p>Владеть: навыками сбора исходных данных, необходимых для разработки проектной документации; современными компьютерными средствами, средствами коммуникации и связи</p>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для очной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			С Р С
					Л К	П З (С З)	Л Р	
1	1.1	Основные этапы проектирования защищенных информационных систем	Основные стадии создания защищенных информационных систем (ЗИС). Составление технического задания на ЗИС.	54	6	6	0	42
	1.2	Инциденты информационной безопасности в защищенных информационных системах	Понятие инцидентов информационной безопасности (ИБ). Нормативная база в сфере управления инцидентами ИБ.	54	6	6	0	42
2	2.1	Защита персональных данных	Обеспечение режима защиты информации о персональных данных (ПДн), и безопасности	35	5	0	10	20

			ПДн в организации					
	2.2	Защита от несанкционированного доступа в телекоммуникационных сетях.	Угрозы применения вредоносных программ (ВП). Меры и средства защиты информации от угроз несанкционированного доступа (НСД).	33	6	0	7	20
3	3.1	Проектирование систем защиты информации в телекоммуникационных сетях	Технологическая схема проектирования систем защиты информации. Требования по защите информации к автоматизированным системам и их реализация при проектировании.	40	6	0	0	34
Итого				216	29	12	17	158

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Основные этапы создания защищенных информационных систем (ЗИС). Составление технического задания на ЗИС.	Предмет, задачи и содержание курса. Значение и место курса в подготовке кадров по специальности «Комплексное обеспечение информационной безопасности». Разбиение проекта на этапы и определение ключевых параметров каждого из них. Рассмотрение методики построения IDEF.	6
	1.2	Понятие инцидентов и информационной безопасности (ИБ). Нормативная база в сфере управления	Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ. Реагирование на инциденты ИБ. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ. Сбор и фиксация информации об инцидентах ИБ: способ выявления инцидента ИБ; источник информации	6

		инцидентами ИБ.	об инциденте ИБ; содержание информации об инциденте ИБ, полученной от источника; сценарий реализации инцидента ИБ; дата и время выявления инцидента ИБ; состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности; способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования; информация об операторе связи и провайдере сети Интернет.	
2	2.1	Обеспечение режима защиты информации о персональных данных (ПДн), и безопасности ПДн в организации	Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных». Меры, по обеспечению безопасности ПДн при их обработке. Понятие угроз безопасности ПДн. Определение уровня защищенности ПДн. Структура и описание угрозы безопасности информации. Внешние и внутренние источники угроз. Типы внешних и внутренних нарушителей.	5
	2.2	Угрозы применения вредоносных программ (ВП). Меры и средства защиты информации от угроз несанкционированного доступа (НСД).	Понятие вредоносной программы. Общая классификация и основные виды ВП. Краткая характеристика основных ВП: файловых, загрузочных вирусов и макровирусов, сетевых червей, программных закладок и иных вредоносных программ. Резидентные и нерезидентные вирусы. Приемы инфицирования ТКС. Способы скрытия факта инфицирования ТКС. Полиморфик-вирусы, стелс-вирусы, руткиты. Направления развития ВП.	6
3	3.1	Технологическая схема проектирования систем защиты	Меры и средства разграничения доступа в сетях. Криптографические и стеганографические способы и средства защиты информации в ТКС. Основы построения частных	6

		информации. Требования по защите информации к автоматизированным системам и их реализация при проектировании.	виртуальных сетей. Специальные меры и средства защиты информации от программно-математического воздействия. Основы межсетевое экранирования: основные функции межсетевое экранирования, виды межсетевых экранов; сертифицированные средства межсетевое экранирования, способы применения межсетевых экранов в ТКС.	
--	--	---------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Основные стадии создания защищенных информационных систем (ЗИС). Составление технического задания на ЗИС.	Изучение государственных стандартов, содержащих требования к составлению технической документации на этапе планирования работ - ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение», ГОСТ 19.201-78 «ЕСКД Техническое задание. Требование к содержанию и оформлению» и ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы». Рассмотрение примера технического задания на разработку ЗИС.	6
	1.2	Понятие инцидентов и информационной безопасности (ИБ). Нормативная база в сфере управления инцидентами ИБ.	Сбор технических данных с компонентов информационной инфраструктуры; Поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформление; Распространение (передача) выделенной и оформленной содержательной (семантической) информации; Обеспечение наличия технических данных на этапах создания и	6

			эксплуатации информационной инфраструктуры.	
3				

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
2	2.1	Обеспечение режима защиты информации о персональных данных (ПДн), и безопасности ПДн в организации	Создание автоматизированной системы в сфере образования. Создание автоматизированной системы в банковской организации. Создание автоматизированной системы в сфере здравоохранения.	10
	2.2	Угрозы применения вредоносных программ (ВП). Меры и средства защиты информации от угроз несанкционированного доступа (НСД).	Создание автоматизированной системы по продаже ж/д билетов. Создание автоматизированной системы по продаже авиа-билетов.	7
3				

3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)
1	1.1	Изучение государственных стандартов, содержащих требования, устанавливаемые российским	Выполнение домашних контрольных работ; работа с электронными образовательными ресурсами	42

		<p>законодательством к стадиям создания автоматизированных систем – ГОСТ 19.102-77 «ЕСПД Стадии разработки», ГОСТ 24.601-86 «Автоматизированные системы. Стадии создания», ГОСТ 24.602-86 «Автоматизированные системы управления. Состав и содержание работ по стадиям создания» и ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». Понятие автоматизированной системы. Основные классы ТКС. Информация и элементы построения ТКС 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 АТМ. Перспективы развития АТМ-сетей.</p>		
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

	<p>1.2 Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных. 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</p>	<p>Выполнение домашних контрольных работ; работа с электронными образовательными ресурсами</p>	<p>42</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------	-----------

		<p>"Анализ сетевого трафика", "Отказ в обслуживании", "Подмена доверенного объекта", "Создания ложного объекта".</p> <p>Причины, обуславливающие возможность реализации сетевых атак. Оценка возможности реализации и опасности сетевых атак.</p> <p>Угрозы утечки информации по техническим каналам в ИТКС. Понятие технического канала утечки информации.</p> <p>Классификация технических каналов утечки. Краткая характеристика основных технических каналов утечки информации в ИТКС</p> <p>Угрозы программно-математического воздействия и особенности их реализации в ИТКС.</p> <p>Последствия от реализации вредоносных программ.</p>		
2	2.1	<p>Общая характеристика программных и программно-аппаратных закладок. Понятие уязвимости, виды уязвимостей. Структура записи уязвимости в базе CVE. Содержание несанкционированных действий. Схема общей классификации угроз безопасности информации. Понятие сетевой атаки.</p> <p>Классификация сетевых атак. Понятие базовой и</p>	<p>Выполнение домашних контрольных работ; работа с электронными образовательными ресурсами</p>	20

		частной модели угроз. Порядок анализа угроз и формирования частных моделей угроз		
	2.2	<p>Классы угроз безопасности информации, парируемых с использованием мер и средств защиты от НСД в ТКС. Общая классификационная схема для мер защиты информации в ТКС и ее элементах.</p> <p>Организационные, организационно-технические и технические меры защиты информации.</p> <p>Средства защиты от непосредственного виртуального доступа и воздействия вредоносными программами. Меры защиты информации от несанкционированного доступа, обусловленного применением сетевых технологий взаимодействия. Меры защиты информации при передаче по каналам связи.</p>	Выполнение домашних контрольных работ; работа с электронными образовательными ресурсами	20
3	3.1	<p>Общая характеристика процесса проектирования ТКС. Основные направления защиты информации в ТКС.</p> <p>Обобщенная структура системы защиты информации. Основные этапы проектирования систем защиты информации.</p> <p>Обобщенная технологическая схема проектирования систем</p>	Выполнение домашних контрольных работ; работа с электронными образовательными ресурсами	34

		<p>защиты информации в ТКС и ее характеристика.</p> <p>Понятия задачи, стратегии, концепции и способа защиты информации.</p> <p>Характеристика содержания работ при проектировании систем защиты информации для функционирующих и развертываемых ТКС.</p> <p>Требования руководящих документов по порядку проектирования ТКС в защищенном исполнении.</p>	
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

[Фонд оценочных средств](#)

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

5.1.1. 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 : 13750.

5.1.2. 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

2. 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.

5.2. Дополнительная литература

5.2.1. 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.

5.2.2. Издания из ЭБС

1. Технология проектирования систем защиты информации в информационно-телекоммуникационных системах [Электронный ресурс] [Электронный ресурс] : учеб. пособие / Ю. К. Язов. - Электрон.дан. (1 файл). - Воронеж : ВГТУ, 2004 - 1 электрон. опт. диск (CD-ROM). - Имеется вариант на бумажном носителе. - 30.00.

2. Волкова Т.В. Разработка систем распределенной обработки данных [Электронный ресурс]: учебно-методическое пособие/ Волкова Т.В., Насейкина Л.Ф.— Электрон.текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2012.- 330 с.- Режим доступа: <http://www.iprbookshop.ru/30127>.— ЭБС «IPRbooks».

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
Информационная система «Единое окно доступа к образовательным ресурсам».	http://window.edu.ru
Научная Электронная Библиотека	http://www.e-library.ru
Электронные версии учебников, пособий, методических разработок, указаний и рекомендаций по всем видам учебной работы, предусмотренных вузовской рабочей программой, находящиеся в свободном доступе для студентов, обучающихся в вузе, на внутрисетевом сервере.	http://www.zabgu.ru

6. Перечень программного обеспечения

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

Программное обеспечение специального назначения:

- 1) Autodesk AutoCad 2015
- 2) Cisco packet tracer

7. Материально-техническое обеспечение дисциплины

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закреплённой расписанием по факультету
Учебные аудитории для проведения практических занятий	
Учебные аудитории для проведения лабораторных занятий	
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закреплённой расписанием по кафедре
Учебные аудитории для текущей аттестации	

8. Методические рекомендации по организации изучения дисциплины

Лекции являются основным источником теоретического материала по дисциплине. Посещение и конспектирование лекций является обязательной составляющей успешного освоения дисциплины обучающимися.

Для эффективного освоения материала дисциплины необходимо выполнение следующих требований:

- обязательное посещение всех лекционных занятий, способствующее системному овладению материалом курса;
- все вопросы соответствующих разделов и тем по дисциплине необходимо фиксировать (на любых носителях информации);
- обязательная самостоятельная работа является важнейшим требованием и условием формирования целостного и системного знания по дисциплине;
- обязательность личной активности каждого студента на всех занятиях по дисциплине;
- 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 предоставляется право подготовки и представления заданий и ответов на вопросы изученного материала, 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 изучении дисциплины.

Порядок организации самостоятельной работы студентов

Самостоятельная работа студентов предполагает:

- самостоятельный поиск, обработку (анализ, синтез, обобщение и систематизацию), 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 дополнительная литература);
- самостоятельное изучение отдельных вопросов курса;
- подготовка к лабораторным занятиям, в соответствии с рекомендациями преподавателя (выполнение конкретных заданий, соответствующие организационные 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 подготовке к измерениям, обработке результатов и составлении 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 система знаний и умений (ориентировочная основа действия), которая обеспечит правильное и рациональное исполнение действия.

Поэтому выполнение каждой лабораторной работы необходимо начинать с изучения ее описания и приведения знаний в систему, а именно:

- ясно представить себе общую цель данной конкретной лабораторной работы и последовательность задач, решение которых приведет к достижению окончательной цели;
- знать, какие электронные устройства изучаются в данной работе, принципы его работы, какими зависимостям связаны описываемые его величины;
- знать основные особенности объекта исследования
- изучить и уметь объяснить физические основы используемых в работе методов измерения 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

Разработчик/группа разработчиков:
Сергей Борисович Таланов

Типовая программа утверждена

Согласована с выпускающей кафедрой
Заведующий кафедрой

_____ «___» _____ 20__ г.