МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ Н.А. Андреева
«29» 04 2024 г.

Основы информационной безопасности Б1.О.18

рабочая программа дисциплины

Кафедра **Информационная безопасность**
Направление подготовки **09.03.01. Информатика и вычислительная техника**
Профиль **Искусственный интеллект и машинное обучение**

Формы обучения **очная, заочная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО)), курсам (для заочной формы обучения (ЗФО))

Вид учебной работы	ОФО		ЗФО	
	ЗЕ	часов/сем.	ЗЕ	часов/курс
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5	3	108/3
Контактная работа, в том числе (по семестрам, курсам):		54/5		16/3
Лекции		18/5		4/3
Лабораторных работ		18/5		6/3
Практических занятий		18/5		6/3
Семинаров				
Самостоятельная работа		54/5		92/3
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам		1/5		1/3
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:
заведующий кафедрой ИБ, к.т.н., доцент Маршаков Д.В.

Рецензенты:
ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи»,
д.т.н., доцент Погорелов В.А.

Рабочая программа дисциплины
«Основы информационной безопасности»

Разработана в соответствии с ФГОС ВО:
ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ
Направление подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
УТВЕРЖДЕН Приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 929

Составлена на основании учебных планов
направления 09.03.01 Информатика и вычислительная техника
профиль "Искусственный интеллект и машинное обучение", одобренных Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от «28» марта 2024 г. №8.

Зав. кафедрой _____ Д.В. Маршаков

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины ***"Основы информационной безопасности"*** формирование у студентов систематических знаний о базах данных и технологиях, используемых при их разработке. Основное внимание уделяется приобретению знаний и умений, необходимых для работы с системами управления базами данных.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с ***проектной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-3: способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Знать:
- методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Уметь:
- решать стандартные задачи профессиональной деятельности с применением современных информационных технологий и программных средств, включая управление крупными массивами данных и их интеллектуальный анализ
Владеть:
- методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов с учетом соблюдения авторского права и требований информационной безопасности
ОПК-9: способен осваивать методики использования программных средств для решения практических задач
Знать:
- методики использования программных средств для решения практических задач - основные определения и понятия БД; принципы построения, работы, возможности реляционных баз данных - основные принципы использования программных средств для построения и управления БД
Уметь:
- выполнять сбор и структурирование данных, реализовывать принципы нормализации данных, разрабатывать схемы данных, таблицы данных и основные типовые запросы к БД, конструировать основные формы и отчеты БД - систематизировать и выполнять нормализацию данных, разрабатывать сложные схемы данных, конструировать сложные запросы, формы и отчеты, пользоваться инструментами решения нестандартных задач при работе с БД - выполнять построение таблиц данных и разработку типовых запросов в распределенных БД, управлять доступом к данным
Владеть:
- основными приемами проектирования и управления БД при решении профессиональных задач с использованием средств визуального проектирования - приемами проектирования и управления БД при решении нетиповых профессиональных задач

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.26 Введение в информационные технологии
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.13 Операционные системы
2	Б1.В.07 Сетевые технологии
3	Б3.01 Выполнение и защита выпускной квалификационной работы

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1. Очная форма обучения, 4 года (всего 108 часов, из них 54 часа аудиторных)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 5					
Модуль 1: Предмет информационной безопасности					
1.1	Лекция 1. Общие вопросы информационной безопасности и защиты данных. Исторические аспекты ИБ. Объекты защиты. Объекты информатизации, средства и системы обработки информации. Угрозы ИБ и их источники. Виды каналов утечки. Классификация технических каналов утечки конфиденциальной информации	Лек.	4	ОПК-3	Л1.1
1.2	Лекция 2. Организационное и правовое обеспечение информационной безопасности. Нормативные правовые акты Российской Федерации. Стратегия национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Нормативные правовые акты, методические и информационные документы ФСТЭК России.	Лек.	4	ОПК-3	Л1.1 Л1.2
1.3	Лекция №3. Модели разграничения доступа. Политика безопасности. Мандатная, дискреционная, ролевая модели разграничения доступа	Лек.	2	ОПК-3	Л1.1
1.4	Практическое занятие №1 Дискреционное управлением доступом (модели Харрисона-Руззо-Ульмана и типизированная матрицы доступов)	Пр.	4	ОПК-3	Л1.1
1.5	Практическое занятие №2 Управление распространением прав доступа на основе классической модели Take-Grant	Пр.	4	ОПК-3	Л1.1
1.6	Практическое занятие №3 Регламент проведения работ при осуществлении контроля защищенности информации от НСД	Пр.	2	ОПК-3	Л1.1
1.7	Кибератаки предприятий в XXI веке. Российские и зарубежные стартапы в области ИБ. Форензика как наука о расследовании киберпреступлений. Вредоносные приложения для Android и iOS (обзор,	СРС	30	ОПК-3	Л1.1 Л2.1

	конкретные примеры, последствия). Технология SIEM. История развития технологии распознавания образов. Информационная война и ее влияние на национальную безопасность государства. Защита персональных данных: регулировании в России и США.				
Модуль 2: Методы и средства обеспечения информационной безопасности					
2.1	Лекция №4. Методы и средства криптографической защиты информации Предмет криптографии. Стандарты и алгоритмы симметричного и асимметричного шифрования информации.	Лек.	2	ОПК-3	Л1.2 Л2.3
2.2	Практическое занятие №4 Принципы шифрования информации с закрытым ключом	Пр.	4	ОПК-3	Л1.1
2.3	Практическое занятие №5 Принципы шифрования информации с открытым ключом	Пр.	4	ОПК-3	Л1.1
2.4	Лекция №5. Методы и средства сетевой защиты информации Локальные и глобальные вычислительные сети и системы передачи информации. Модель взаимодействия открытых систем (OSI). Методы и средства защиты информации в локальных вычислительных сетях: межсетевое экранирование, системы обнаружения вторжений и атак, VPN	Лек.	2	ОПК-3	Л1.1 Л1.2
2.5	Лекция №6. Меры и средства защиты информации от несанкционированного доступа Общая характеристика и классификация мер и средств защиты информации от несанкционированного доступа (НСД). Вредоносное ПО. Антивирусные средства защиты информации.	Лек.	4	ОПК-3	Л1.1 Л2.1
2.6	Лабораторная работа №1 Установка и настройка программно-аппаратного комплекса защиты информации	Лаб.	4	ОПК-3	Л1.1 Л2.1 Л2.2
	Лабораторная работа №2 Настройка механизмов защиты информации в информационных (автоматизированных) системах	Лаб.	4	ОПК-3	Л1.1 Л2.1 Л2.2
2.7	Лабораторная работа №3 Установка и настройка средств сетевой безопасности	Лаб.	4	ОПК-3	Л1.1 Л3.1
2.8	Лабораторная работа №4 Установка и настройка антивирусных программ	Лаб.	2	ОПК-3	Л1.1 Л1.2
2.9	Лабораторная работа №5 Инструментальный контроль защищенности компьютерных систем	Лаб.	2	ОПК-3	Л1.1 Л1.2
2.10	Лабораторная работа №6 Восстановление системного и прикладного программного обеспечения после сбоев и отказов оборудования	Лаб.	2	ОПК-3	Л1.1 Л1.2
2.11	Виртуальные частные сети. Служба управления сетью. Иерархия средств защиты от информационных угроз.	СРС	24	ОПК-3	Л1.1 Л2.1

	Принципы защиты информационной системы. Шифрование. Метод Диффи-Хелмана. Хеш-функции. Атаки на транспортную инфраструктуру сети. Облачные сервисы и их безопасность.				
	Итого		108		

4.2. Заочная форма обучения, 5 лет (всего 108 часов, из них 24 часов аудиторных)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3					
Модуль 1: Предмет информационной безопасности					
1.1	Исторические аспекты ИБ. Объекты защиты. Объекты информатизации, средства и системы обработки информации. Угрозы ИБ и их источники. Виды каналов утечки. Классификация технических каналов утечки конфиденциальной информации	СРС	8	ОПК-3	Л1.1
1.2	Организационное и правовое обеспечение информационной безопасности. Нормативные правовые акты Российской Федерации. Стратегия национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Нормативные правовые акты, методические и информационные документы ФСТЭК России.	СРС	4	ОПК-3	Л1.1 Л1.2
1.3	Модели разграничения доступа. Политика безопасности. Мандатная, дискреционная, ролевая модели разграничения доступа	СРС	14	ОПК-3	Л1.1
1.4	Практическое занятие №1 Дискреционное управлением доступом (модели Харрисона-Руззо-Ульмана и типизированная матрицы доступов) Управление распространением прав доступа на основе классической модели Take-Grant Регламент проведения работ при осуществлении контроля защищенности информации от НСД	Пр.	2	ОПК-3	Л1.1
1.5	Кибератаки предприятий в XXI веке. Российские и зарубежные стартапы в области ИБ. Форензика как наука о расследовании киберпреступлений. Вредоносные приложения для Android и iOS (обзор, конкретные примеры, последствия). Технология SIEM. История развития технологии распознавания образов. Информационная война и ее влияние на национальную безопасность государства. Защита персональных данных: регулировании в России и США.	СРС	33	ОПК-3	Л1.1 Л2.1
Модуль 2: Методы и средства обеспечения информационной безопасности					
2.1	Лекция №1. Методы и средства криптографической защиты информации Предмет криптографии. Стандарты и алгоритмы симметричного и асимметричного шифрования информа-	Лек.	2	ОПК-3	Л1.2 Л2.3

	ции.				
2.2	Практическое занятие №2 Принципы шифрования информации с закрытым ключом	Пр.	2	ОПК-3	Л1.1
2.3	Практическое занятие №3 Принципы шифрования информации с открытым ключом	Пр.	2	ОПК-3	Л1.1
2.4	Лекция №2. Методы и средства сетевой защиты информации Локальные и глобальные вычислительные сети и системы передачи информации. Модель взаимодействия открытых систем (OSI). Методы и средства защиты информации в локальных вычислительных сетях: межсетевое экранирование, системы обнаружения вторжений и атак, VPN Общая характеристика и классификация мер и средств защиты информации от несанкционированного доступа (НСД). Вредоносное ПО. Антивирусные средства защиты информации	Лек.	2	ОПК-3	Л1.1 Л1.2
2.5	Лабораторная работа №1 Установка и настройка программно-аппаратного комплекса защиты информации Настройка механизмов защиты информации в информационных (автоматизированных) системах	Лаб.	2	ОПК-3	Л1.1 Л2.1 Л2.2
2.6	Лабораторная работа №2 Установка и настройка средств сетевой безопасности Установка и настройка антивирусных программ	Лаб.	2	ОПК-3	Л1.1
2.7	Лабораторная работа №3 Инструментальный контроль защищенности компьютерных систем Восстановление системного и прикладного программного обеспечения после сбоев и отказов оборудования	Лаб.	2	ОПК-3	Л1.1 Л1.2
2.8	Виртуальные частные сети. Служба управления сетью. Иерархия средств защиты от информационных угроз. Принципы защиты информационной системы. Шифрование. Метод Диффи-Хелмана. Хеш-функции. Атаки на транспортную инфраструктуру сети. Облачные сервисы и их безопасность.	СРС	24	ОПК-3	Л1.1 Л2.1
	Контроль		9		
	Итого		108		

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Олифер В.Г., Олифер Н.А.	Компьютерные сети. Принципы, технологии, протоколы.	СПб.: Питер, 2016. 992 с.	5
Л1.2	Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А.	Введение в информационную безопасность	М.: Гор. линия-Телеком, 2018. – 288 с.	Э1
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Малюк А.А.	Защита информации в информационном обществе	М.: Гор. линия-Телеком, 2015. – 230 с.	Э2
Л2.2	Е. Б. Белов, В.П. Лось, Р. В. Мещеряков, Д. А. Шелупанов	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558	Э3
Л2.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э4
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Жуковский А.Г., Жуковский Д.А., Швидченко С.А.	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2020. – 52 с.	РнД: СКФ МТУСИ, 2020	Э5

5.2. Электронные образовательные ресурсы	
Э1	https://znanium.com/catalog/document?id=42509
Э2	https://znanium.com/catalog/document?id=257570
Э3	https://znanium.com/catalog/document?id=233208
Э4	https://www.iprbookshop.ru/87995.html
Э5	http://www.skf-mtusi.ru/?page_id=659

5.3. Программное обеспечение	
П.1	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Secret Net Studio (лицензия)
П.4	Dallas Lock 8.0-К (лицензия)
П.5	Сканер-ВС (лицензия)
П.6	Kaspersky Endpoint Security (лицензия)

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном

6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет (ауд. 218, 305)
6.3 МТО рубежных контролей, зачетов, экзаменов	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Самостоятельная работа студента имеет существенное значение.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых аудиторных часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ.

Исследуемые схемы могут собираться из виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе