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.

Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем) Б1.В.04

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/5 сем
Контактная работа, в том числе (по семестрам, курсам):		54/5 сем
Лекции		18/5 сем
Лабораторных работ		18/5 сем
Практических занятий		18/5 сем
Семинаров		
Самостоятельная работа		18/5 сем
Контроль		36/5 сем
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		1/5 сем

Программу составил:
Доцент кафедры ИВТ к.т.н. Швидченко С. А.

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

Рабочая программа дисциплины
«Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного 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 «24» апреля 2024 г. № 9

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 **" Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)"** является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке безопасного программного обеспечения для решения задач в профессиональной деятельности, соответствующих общепрофессиональных компетенций в соответствии с ООП, а также основных знаний и умений в области разработки безопасного программного обеспечения.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-1: способен применять средства защиты информации прикладного и системного программного обеспечения для решения профессиональных задач
Знать:
- принципы разработки, внедрения, конфигурации и эксплуатации программных продуктов по защите информации и баз данных - принципы обслуживания и администрирования подсистем защиты информации прикладного и системного программного обеспечения.
Уметь:
- осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения - анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия
Владеть:
- навыками по обнаружению вредоносного программного обеспечения и ликвидации последствий его функционирования - навыками установки, конфигурации и эксплуатации программного обеспечения по защите информации

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.14 Информационные технологии и программирование
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.03 Защита информации от вредоносного программного обеспечения

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, 54 аудиторных часов, 18 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 3, Семестр 5					
Модуль 1: Основные понятия угроз и уязвимостей информационной безопасности при разработке ПО					
1.1	Лекция 1. Введение в дисциплину. базовая терминология. Угрозы и уязвимости информационной безопасности при разработке ПО. Безопасное ПО. Тестирование и анализ ПО. Фаззинг. Инструментальные среды и средства разработки и анализа ПО. Управление конфигурацией ПО. Документация разработчика ПО. Цели создание безопасного ПО и меры по их достижению.	Лек.	4	ПК-1	Л1.1,
1.2	Практическое занятие №1 Алгоритмы шифрования данных	Пр.	2	ПК-1	Л1.1, Л3,2.
1.3	Лабораторная работа №1 Методы поиска и сбора информации. Методика устранения компьютерной информации.	Лаб.	2	ПК-1	Л1.1, Л1,2. Л3.1
1.4	1. Знакомство с ГОСТ ГОСТ Р 56939-2016 2. Формирование требований к ПО и составление технического задания с учетом требований ГОСТ ГОСТ Р 56939-2016 3. Принципы безопасной разработки. Построение модели угроз.	СРС	4	ПК-1	Л1.2, Л1,3.
1.5	Лекция 2. Оосновные нормативно-правовые акты в области создания безопасного ПО Обзор основных ГОСТов: - ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения; - ГОСТ Р 56546-2015 Классификация уязвимостей информационных систем; - ГОСТ Р 58412-2019 Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО; - ГОСТ Р ИСО/МЭК 18045-2013 Методология оценки безопасности информационных технологий; - ГОСТ Р ИСО-МЭК 27034-1 Информационные технологии. Безопасность приложений. Часть 1. Безопасность приложений; - ГОСТ Р ИСО-МЭК 27034-7-2020 Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия	Лек.	2	ПК-1	Л1.2, Л1,4.
1.6	Практическое занятие №2 Защита от копирования	Пр.	4	ПК-1	Л1.1, Л3.2
1.7	Лабораторная работа №2 Уязвимости Windows. Защита от копирования переносных носителей	Лаб.	4	ПК-1	Л1.1, Л3.1

1.8	1. Реализация ПО. Анализ кода уязвимого приложения 2. Тестирование ПО на изменение плоскости атак. 3. Планирование реагирования на инциденты. 4. Фаззинг-тестирование ПО.	СРС	4	ПК-1	Л1.1, Л2.3.
1.9	Лекция 3. Угрозы, уязвимости, риски информационной безопасности при разработке по - их выявление и оценка. Угрозы безопасности информации при разработке ПО (по ГОСТ Р 58412-2019). Классификация уязвимостей информационных систем (по ГОСТ Р 56546—2015). Выявление угроз безопасности информации при разработке ПО. Оценка уровня доверия безопасности ПО (степени соответствия выявленной безопасности ПО предъявленным требованиям) (по ГОСТ Р ИСО-МЭК 27034-7). Методы и средства оценки рисков информационной безопасности при создании ПО.	Лек.	4	ПК-1	Л1.1, Л2.3.
1.10	Практическое занятие №3 Защита от побочного электромагнитного излучения и наводок.	Пр.	4	ПК-1	Л3.2
1.11	Лабораторная работа №3 Модели распространения программного обеспечения	Лаб.	4	ПК-1	Л3.1
Модуль 2: Безопасная разработка программного обеспечения (ПО)					
2.1	Лекция 4. Организационные и технические меры по разработке безопасного по, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО. Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры ПО. Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО. Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО. Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции ПО и поддержки приемки ПО. Меры по разработке безопасного ПО, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента инфраструктурой среды разработки ПО. Меры по разработке безопасного ПО, реализуемые в процессе менеджмента людскими ресурсами. Меры по разработке безопасного ПО, реализуемые при выполнении. Меры по разработке безопасного ПО, реализуемые при выполнении. Меры по разработке безопасного ПО, реализуемые при выполнении.	Лек.	4	ПК-1	Л1.1, Л1.1, Л1,3.
2.2	Практическое занятие №4 Виды шифров. алгоритмы распределения ключей	Пр.	2	ПК-1	Л3.2
2.3	Лабораторная работа №4 Аппаратные ключи защиты.	Лаб.	2	ПК-1	Л3.1

	количественная оценка стойкости парольной защиты.				
2.4	Лекция 5. Тестирование и анализ ПО Виды тестирования ПО. Статический анализ ПО. Динамический анализ ПО. Защита ПО от взлома и несанкционированного использования	Лек.	2	ПК-1	Л1.1, Л1,2.
2.5	Практическое занятие №5 Симметричные алгоритмы	Пр.	2	ПК-1	Л3.2
2.6	Лабораторная работа №5 Вредоносное программное обеспечение. Безопасная работа в Интернет	Лаб.	2	ПК-1	Л1.1, Л3.1.
2.7	1. Отечественные и зарубежные стандарты в области разработки безопасного ПО. 2. Обеспечение безопасной разработки на фазе формирования требований к ПО. 3. Обеспечение безопасной разработки на фазе проектирования ПО.	СРС	4	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4
2.8	Лекция 6. Инструментальные средства разработки безопасных программ Инструментальные средства для безопасной разработки в среде Windows: - Microsoft Threat Modeling Tool 2014 — средство моделирования атак; - SDL MiniFuzz File Fuzzer — средство фаззинг-тестирования; - Attack Surface Analyzer — анализатор плоскости атаки; - Анализатор кода C/C++ из состава Microsoft Visual Studio.	Лек.	2	ПК-1	Л1.3
2.9	Практическое занятие №6 Асиметричные алгоритмы	Пр.	4	ПК-1	Л1.2 Л3.2
2.10	Лабораторная работа №6 Обеспечение безопасности локальной сети. настройка параметров безопасности браузера	Лаб.	4	ПК-1	Л1.1, Л3.1
2.11	1. Обеспечение безопасной разработки на фазе реализации ПО 2. Обеспечение безопасной разработки на фазе тестирования ПО 3. Обеспечение безопасной разработки на фазах выпуска и поддержки ПО	СРС	6	ПК-1	Л1.1 Л1.2 Л1.3 Л1.4
	Контроль		36		
	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	Брылева А. А.	Программные средства создания интернет-приложений : учебное пособие / А. А. Брылева.	Минск : РИПО, 2019. - 377 с.	Э1
Л1.2	Лисьев Г. А., Романов П.Ю., Аскерко Ю.И.	Программное обеспечение компьютерных сетей и web-серверов : учебное пособие / Г.А. Лисьев, П.Ю. Романов, Ю.И. Аскерко	Москва : ИНФРА-М, 2023. — 145 с.	Э2
Л1.3	Коробко И. В.	Справочник системного администратора по программированию Windows : практическое руководство / И. В. Коробко	Санкт-Петербург : БХВ-Петербург, 2009. - 576 с.	Э3
Л1.4	Исаченко О. В.	Программное обеспечение компьютерных сетей : учебное пособие / О.В. Исаченко.	Москва : ИНФРА-М, 2022. — 158 с.	Э4

5.1.2 Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Клейн Т.	Дневник охотника за ошибками: путешествие через джунгли проблем безопасности программного обеспечения : практическое руководство	Москва : ДМК Пресс, 2015. - 240 с.	Э5
Л2.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика : учебное пособие	Москва : Директ-Медиа, 2020. - 270 с.	Э6
Л2.3	Петров А. А.	Компьютерная безопасность: криптографические методы защиты: практическое руководство	Москва : ДМК Пресс, 2008. - 448 с.	Э7
Л2.4	Чио К., Фримэн Д.	Машинное обучение и безопасность: защита систем с помощью данных и алгоритмов : практическое руководство / К. Чио, Д. Фримэн.	Москва : ДМК Пресс, 2020. - 388 с.	Э8

6.1.3 Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Швидченко С.А.	Методические указания для проведения лабораторных работ	Ростов н/Д: СКФ МТУСИ, 2022	Э9
Л3.2	Швидченко С.А.	Методические указания для проведения практических занятий	СКФ МТУСИ: Ростов-на-Дону, 2022 г.	Э10

5.2 Электронные образовательные ресурсы

Э1	https://znanium.com/catalog/product/1088292
Э2	https://znanium.com/catalog/product/1878635
Э3	https://znanium.com/catalog/product/1768239
Э4	https://znanium.com/catalog/product/1860121
Э5	https://znanium.com/catalog/product/1907788
Э6	https://znanium.com/catalog/product/1908082
Э7	https://znanium.com/catalog/product/1908428
Э8	https://znanium.com/catalog/product/1908430
Э9-Э10	http://www.skf-mtusi.ru/?page_id=659

5.3. Программное обеспечение		
П.1	1. AVAST Free Antivirus	Антивирусное ПО. Свободное, условно свободное или триал-версии.
	2. AVG AntiVirus Free	
	3. Dr.Web Antivirus	
	4. Антивирус Касперского	
	5. ESET NOD32 Антивирус	
	6. AVZ Antivirus	
	7. Avira Free Antivirus	
	8. Norton AntiVirus	
	9. McAfee Antivirus	
	10. Emsisoft Anti-Malware	
	11. BullGuard Antivirus	
	12. Protector Plus Antivirus	
	13. Panda Antivirus	
	14. Ashampoo Anti-Virus	
	14. G Data AntiVirus	
	16. K7 AntiVirus	
	17. VIRUSfighter	
	18. Twister Antivirus	
П.2	1. Wise Folder Hider	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
	2. Secure Folders	
	3. Anvide Lock Folder	
	4. Folder Lock	
	5. Easy File Locker	
	6. Folder Guard	
	7. DEKSI USB Security	
	8. Locker (защита папок и дисков)	
	9. Advanced Hider	
	10. Hide Folders XP	
	11. Hide Files	
П.3	1. TrustPort Tools	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
	2. Cryptic Disk	
	3. Locker (скрытие файлов)	
	4. Max File Encryption	
	5. Secure Disk	
	6. Masker 7.1	
	7. Fox Secret	
	8. HideInPicture 1.0	
	9. Шифровальщик	
	10. Advanced Encryption Package	
	11. Gpg4win	
	12. Cryptic Disk Professional	
	13. CyberSafe Files Encryption	
	14. Steganos Privacy Suite	
	15. Lavasoft Privacy Toolbox	
	16. pkiImage Free Edition	
П.4	1. Hetman Partition Recovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.
	2. Active File Recovery	
	3. R-Studio 7.6	

	4. Auslogics File Recovery	
	5. Active UNDELETE	
	6. Paragon Rescue Kit	
	7. Wise Data Recovery	
	8. Puran File Recovery	
	9. O&O DiskRecovery	
	10. Tenorshare Any Data Recovery	
	11. Power Data Recovery	
	12. GetDataBack	
	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
	2. FBackup	
	3. Backup4all	
	4. Uranium Backup Free	
	5. Simple Data Backup	
	6. Personal Backup	
	7. Back4Sure	
	8. SyncBackFree	
	9. Handy Backup	
	10. EASEUS Todo Backup 8.0 Free Edition	
	11. Exiland Backup Free 4.0	
	12. Nero BackItUp	
	13. Paragon Rescue Kit 14.0 Free	
	14. Action Backup	
	15. LimBackup	
	16. AVSbackup	
	17. ExtraBackup	
	18. Cobian Backup	
	19. Backup & Recovery 10 Build 9169 Free Edition	
	20. Information Backup System	
П.6	Linux (свободное ПО)	
П.7	LibreOffice (свободное ПО)	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
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

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 часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

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.

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 реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование: учебник для вузов [Электронный ресурс]/ В. К. Волк. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021.
2. Фомичева, С. Г. Разработка, проектирование и сопровождение приложений баз данных: учебное пособие / С. Г. Фомичева. — Норильск: ЗГУ им. Н.М. Федоровского, 2021. — 185 с.

3. Воробейкина, И. В. Программирование средств защиты информации: учебное пособие / И. В. Воробейкина. — Калининград: БГАРФ, 2021. — 70 с.
4. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с.
5. 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 экзамену осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к экзамену 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 экзамену, 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