

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  
А.Г. Жуковский  
« 29 » 08 2022 г.

**Методы оценки безопасности компьютерных систем Б1.О.39**  
рабочая программа дисциплины

Кафедра **«Информатика и вычислительная техника»**  
Направление подготовки **10.03.01 Информационная безопасность**  
Профиль **Безопасность компьютерных систем**  
Формы обучения **очная**

**Распределение часов дисциплины по семестрам (ОФ), курсам (ЗФ)**

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	5	180/8		
Контактная работа, в том числе (по семестрам, курсам):		90/8		
Лекции		30/8		
Лабораторных работ		30/8		
Практических занятий		30/8		
Семинаров				
Самостоятельная работа		90/8		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам, курсам				
Число экзаменов с разбивкой по семестрам (курсам)		1/8		

Программу составил:  
*доцент кафедры ИВТ к.э.н. Тимакин О.А.*

Рецензенты:  
*доцент кафедры ИВТ к.т.н. доцент Чикалов А.Н.*

Рабочая программа дисциплины  
**«Методы оценки безопасности компьютерных 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 2020г. N 1427.

Составлена на основании учебного плана  
направления **10.03.01 «Информационная безопасность»**, профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МГУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МГУСИ 25.04.2022 г.

Одобрена на заседании кафедры  
"Информатики и вычислительной техники"

Протокол от 29 08 2022 г. № 1

Зав. кафедрой  Соколов С.В.

**Визирование для использования в 20\_\_/20\_\_ уч. году**

Утверждаю

Зам. директора по УВР \_\_\_\_\_

- \_\_\_\_\_ 20\_\_ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры  
"Информатики и вычислительной техники"

Протокол от \_\_\_\_\_ 20\_\_ г. № \_

Зав. кафедрой \_\_\_\_\_ Соколов С.В.

**Визирование для использования в 20\_\_/20\_\_ уч. году**

Утверждаю

Зам. директора по УВР \_\_\_\_\_

- \_\_\_\_\_ 20\_\_ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры  
"Информатики и вычислительной техники"

Протокол от \_\_\_\_\_ 20\_\_ г. № \_

Зав. кафедрой \_\_\_\_\_ Соколов С.В.

**Визирование для использования в 20\_\_/20\_\_ уч. году**

Утверждаю

Зам. директора по УВР \_\_\_\_\_

- \_\_\_\_\_ 20\_\_ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры  
"Информатики и вычислительной техники"

Протокол от \_\_\_\_\_ 20\_\_ г. № \_

Зав. кафедрой \_\_\_\_\_ Соколов С.В.

## 1. Цели изучения дисциплины

Целями изучения дисциплины являются:

- формирование компетенций по основным разделам данного курса, изучение студентами основных методов оценки безопасности компьютерных систем, стандартов в этой области;
- получение представления об организации и принципах обеспечения информационной безопасности компьютерных систем;
- приобретение навыков применять современные методы оценки безопасности компьютерных систем.

## 2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности.

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

<b>Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)</b>	
<b>ОПК-1.4:</b> Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	
<b>Знать:</b>	
базовые понятия и принципы применения современных методов оценки безопасности компьютерных систем;	
<b>Уметь:</b>	
выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем	
<b>Владеть:</b>	
практическими навыками применения методов обеспечения безопасности компьютерных систем	
<b>УК-9:</b> Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	
<b>Знать:</b>	
базовые понятия и принципы применения обоснованных экономических решений в различных областях жизнедеятельности;	
<b>Уметь:</b>	
выявлять угрозы применения экономических решений в различных областях жизнедеятельности и определять их актуальность для современных компьютерных систем;	
<b>Владеть:</b>	
Практическими навыками применения обоснованных экономических решений в различных областях жизнедеятельности;	

## 3. Место дисциплины в структуре образовательной программы

**Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):**

1	Б1.О.34. Защита информации от утечки по техническим каналам
2	Б1.В.07. Защита информации от вредоносного программного обеспечения
3	Б1.О.35 Криптографические протоколы
4	Б1.О.37 Комплексное обеспечение защиты информации

**Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:**

1	Б1.О.40. Администрирование средств защиты информации в компьютерных системах и сетях
2	Б1.В.09 Моделирование систем защиты информации
3	Б1.В.11 Программирование систем на микроконтроллерах

#### 4. Структура и содержание дисциплины

##### Очная форма обучения, 4 года

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
<b>Курс 4, Семестр 8</b>					
<b>Модуль 1: Общие вопросы оценки безопасности компьютерных систем – 102 (60+42) часа</b>					
1.1	<u>Лекция 1. Введение.</u> Основные понятия курса. Модель нарушителя. Организационно-правовые вопросы защиты информации.	Лек.	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.2	Основные понятия курса. Модель нарушителя. Организационно-правовые вопросы защиты информации.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.3	<u>Лекция 2. : «Защита информации от ПЭМИН»</u> Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	Лек.	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.4	Защита информации от ПЭМИН	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.5	<u>Лекция 3. «Основы криптографии»</u> Понятия и определения; классификация шифров; блочные и поточные шифры.	Лек.	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.6	Основы криптографии	СРС	6	ОПК-1.4, УК-9	Л1.1, Л2.2, Л2.1, Л3.3
1.7	Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности.	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1, Л2.2
1.8	<u>Практическое занятие 1.</u> Оценка технологической безопасности программного продукта.	Пр.	10	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1, Л3.2
1.9	Специфические особенности защиты информации в компьютерных сетях.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1, Л3.1
1.10	Методы и средства защиты информационно-программного обеспечения на уровне операционных систем	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.11	Применение симметричных криптосистем для защиты компьютерной информации.	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.12	<u>Практическое занятие 2.</u> Оценка безопасности информационной системы по критериям СТСПЕС.	Пр.	10	ОПК-1.4,	Л1.1, Л1.2,

	Оценки пригодности компьютерных систем TCSEC (Оранжевая книга).			УК-9	Л2.2, Л3.2
1.13	Лабораторная работа 1. Модель нарушителя. Организационно-правовые вопросы защиты информации.	Лаб.	10	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.1
1.14	Лекция 4. «Основы теории защиты информации в компьютерных системах. Критерии информационной безопасности» Основные понятия теории защиты информации; угрозы безопасности; математические модели политики безопасности; общие критерии безопасности информационных технологий.	Лек.	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
1.15	Технологии идентификации и аутентификации в компьютерных сетях.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.1
1.16	Лабораторная работа 2. Защита информации от ПЭМИН. Каналы утечки информации из компьютерных систем; пассивные и активные методы защиты	Л.р.	10	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.1
<b>Модуль 2: Организация оценки безопасности компьютерных систем – 78 (30+48) часа</b>					
2.1	Лекция 5. «Специфические особенности защиты информации в компьютерных сетях» Разделение совместно используемых ресурсов. Расширение зоны контроля. Комбинация различных программно-аппаратных средств. Неизвестный периметр. Множество точек атаки. Сложность управления и контроля доступа к системе. Средства защиты информации от НСД. Способы несанкционированного доступа к информации и защиты от него в компьютерных системах.	Лек.	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1, Л2.2
2.2	Методы защиты внешнего периметра компьютерных сетей.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1, Л2.2
2.3	Безопасность компьютерных систем.	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
2.4	Методы обеспечения информационной безопасности .	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.1
2.5	Эксплуатация уязвимостей.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.1
2.6	Лекция 6. «Методы и средства защиты информационно-программного обеспечения на уровне операционных систем». Классы защищенности СВТ от НСД. Требования безопасности информации к операционным систе-	Лек.	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.2, Л2.3

	мам. Профили защиты операционных систем. Разграничение полномочий для групп и учетных записей пользователей. Локальная групповая политика				
2.7	Основы технологии виртуальных защищенных сетей VPN.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.2, Л2.3
2.8	Мероприятия по выявлению каналов утечки информации	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.3, Л2.4
2.9	Технологии обнаружения вторжений в компьютерных сетях.	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.4
2.10	<u>Лабораторная работа 3.</u> Классификация шифров. Блочные и поточные шифры.	Л.р.	10	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.1
2.11	Методы идентификации и аутентификации пользователей компьютерных систем.	СРС	4	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.2
2.12	Адаптивное управление безопасностью в компьютерных сетях	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л2.2
2.13	Особенности современных подходов к анализу информационной безопасности. Анализ методов функционирования современного Вредоносного программного обеспечения. Способы определения нарушений информационной безопасности. Программно-конфигурируемые сети	СРС	6	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.1
2.14	<u>Практическое занятие 3.</u> Оценка безопасности информационной системы по общим критериям	Пр.	10	ОПК-1.4, УК-9	Л1.1, Л1.2, Л3.6
Итого				180	

## 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	Милославская Н.Г., Сенаторов И.Ю., Толстой А.И.	Технические, организационные и кадровые аспекты управления информационной безопасностью	М.: Горячая линия –Телеком, 2014 г.- 154 с.	20
Л1.2	Милославская Н.Г., Сенаторов И.Ю., Толстой А.И.	Проверка и оценка деятельности по управлению информационной безопасностью	М.: Горячая линия –Телеком, 2014 г.- 123 с.	20

<b>5.1.2 Дополнительная литература</b>				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Малюк А.А., Горбатов В.С., и др.	Введение в информационную безопасность	М.: Горячая линия-Телеком, 2011. - 436с	10
Л2.2	Алферов А.П., Зубов А.Ю., и др.	Основы криптографии	М.:Гелиос АРВ, 2002 г. -367 с.	3
Л2.3	Ярочкин В.И.	Информационная безопасность	М.: Академический проект, 2003. – 425 с.	3
Л2.4	Девянин П.Н.	Модели безопасности компьютерных систем	М.: Горячая линия-Телеком, 2011. - 383с	5
<b>5.1.3 Методическое обеспечение для самостоятельной работы обучающихся</b>				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Мельников В.В.	Защита информации в компьютерных системах	М.: Финансы и статистика, 2014. – 368 с.	Э2
Л3.2	Романец Ю.В.	Защита информации в компьютерных системах и сетях	М.: Радио и связь, 2001. – 328 с.	Э4
Л3.3	Иванов М.А.	Криптографические методы защиты информации в компьютерных системах и сетях	М.: Электрон «Кудиц образ», 2001. – 386 с.	Э3
Л3.4	Руководящий документ Гостехкомиссии России	Средства вычислительной техники	М.: ГТК РФ, 1992..	Э5
Л3.5	Герасименко В.А.	Защита информации в автоматизированных системах обработки данных	М.: Энергоавтомиздат. 2016 г.	Э1
Л3.6	Червяков Н.И., Бабенко М.Г., Гладков А.В.	Вероятностные методы оценки состояния информационной безопасности: учебное пособие	Ставрополь: Северо-Кавказский Федеральный Университет. 2017. – 182 с., СКФ МТУСИ, 2016 г.	Э6
<b>5.2 Электронные образовательные ресурсы</b>				
Э1	<a href="http://www.iprbookshop.ru/73733/html">http://www.iprbookshop.ru/73733/html</a>			
Э2	<a href="http://www.iprbookshop.ru/61558/html">http://www.iprbookshop.ru/61558/html</a>			
Э3	<a href="http://www.iprbookshop.ru/24451/html">http://www.iprbookshop.ru/24451/html</a>			
Э4	<a href="http://www.iprbookshop.ru/29257/html">http://www.iprbookshop.ru/29257/html</a>			
Э5	<a href="http://www.iprbookshop.ru/73733/html">http://www.iprbookshop.ru/73733/html</a>			
Э6	<a href="http://www.iprbookshop.ru/92536/html">http://www.iprbookshop.ru/92536/html</a>			
<b>5.3 Программное обеспечение</b>				



П.1	MSWord лицензия
П.2	ОС Windows
П.3	PuTTY
П.4	Бесплатное использование (MIT)

## 6. Материально-техническое обеспечение дисциплины

<b>6.1 МТО лекционных занятий</b>	
1	Лекционная аудитория, оснащенная проектором, ПК (ноутбуком), экраном
<b>6.2 МТО лабораторных работ и практических занятий</b>	
1	Лабораторные стенды для физического моделирования (ауд. 310)
2	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет (ауд. 218, 101, 305)
<b>6.3 МТО рубежных контролей, зачетов, экзаменов</b>	
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**

#### **Источники, рекомендуемые для углубленного изучения учебного материала**

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 с.— Режим доступа: <http://www.iprbookshop.ru/72444.html>.— ЭБС «IPRbooks»
2. Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 84 с.— Режим доступа: <http://www.iprbookshop.ru/74381.html>.— ЭБС «IPRbooks»
3. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное <http://www.iprbookshop.ru/13936.html>.— ЭБС «IPRbooks»
4. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н.А. Руденков [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 368 с.— Режим доступа: <http://www.iprbookshop.ru/73732.html>.— ЭБС «IPRbooks»
5. Глотина И.М. Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]: учебно-методическое пособие/ Глотина И.М.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 141 с.— Режим доступа: <http://www.iprbookshop.ru/72538.html>.— ЭБС «IPRbooks»
6. Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для студ. Вузов. - М.: ФГБОУ "УМЦ ЖДТ", 95с. МИИТ НТБ, 2014
7. Мельников В. П., Куприянов А. И., Схиртладзе А. Г. Защита информации. - М.: Академия, МИИТ НТБ, 2014. -304 с

#### **Использование Интернет-ресурсов**

1. Электронная техническая библиотека <http://mexalib.com/cat/49>
2. Библиотека технической литературы  
<http://www.htbook.ru/radioelektronika/elektronika/analogovaya-shemotehnika>
3. Портал технических новостей <http://www.modlabs.net>
4. eLIBRARY.Ru [ Электронный ресурс]: электронная библиотека / Науч. электр. б\_ка.- МОСКВА.1999. – Режим доступа: <http://elibrary.ru> (дата обращения 15.09.2022). – Яз. рус., англ.

#### **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**