Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой

(к202) Информационные технологии и системы

Попов М.А., канд. техн. наук, доцент

27.05.2022

РАБОЧАЯ ПРОГРАММА

дисциплины **Защита информации от утечки по техническим каналам**

10.05.03 Информационная безопасность автоматизированных систем

Составитель(и): Ст. препод., Рак Е.В.

Обсуждена на заседании кафедры: (к202) Информационные технологии и системы

Протокол от 18.05.2022г. № 5

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 27.05.2022 г. № 7

г. Хабаровск
2022 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к202) Информационные технологии и системы

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Попов М.А., канд. техн. наук, доцент

Рабочая программа дисциплины Защита информации от утечки по техническим каналам

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1457

Квалификация **специалист по защите информации**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:	
в том числе:		зачёты (семестр)	8
контактная работа	62	РГР	8 сем. (2)
самостоятельная работа	46		
часов на контроль	36		

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	16 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Практические	16	16	16	16
Контроль самостоятельной работы	14	14	14	14
В том числе инт.	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	62	62	62	62
Сам. работа	46	46	46	46
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цели и задачи защиты информации от утечки информации по техническим каналам. Электромагнитные технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ). Технические каналы утечки акустической (речевой) информации. Способы и средства защиты объектов информатизации от утечки информации по техническим каналам. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. Методы и средства контроля защищенности информации, обрабатываемой СВТ. Методы и средства контроля защищенности речевой информации от утечки по техническим каналам.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.27
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационная безопасность киберфизических систем
2.1.2	Методы и средства криптографической защиты информации
2.1.3	Радиопередающие и радиоприемные устройства
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Техническая защита информации и средства контроля

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

Знать:

текущее состояние и тенденции развития методов и средств защиты информации от утечки по техническим каналам;
особенности построения, функционирования и защиты современных распределенных информационных систем и их коммуникационной среды:
особенности построения, функционирования и защиты информации в современных центрах обработки данных

Уметь:

проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурнотехнических решений, реализованных при построении ЭВМ и систем;
применять средства защиты от утечки по техническим каналам при решении задач профессиональной деятельности.
определять требования по защите коммуникационной среды распределенной информационной системы

Владеть:

навыками реализации вычислительных процедур на микропрограммном уровне при решении задач профессиональной деятельности;
методами проектирования и навыками эксплуатации систем и сетей передачи информации при решении задач профессиональной деятельности и
проектирования распределенных информационных систем, в том числе разработки приложений, реализующих параллельные вычисления

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

Знать:

основы диагностики и тестирования систем защиты информации автоматизированных систем
базовые методы анализа уязвимостей систем защиты информации и моделирования угроз информационной безопасности автоматизированных систем

Уметь:

проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем

Владеть:

базовыми навыками проведения диагностики и тестирования систем защиты информации автоматизированных систем

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание

	Раздел 1. Лекции						
1.1	Информация как объект защиты. Виды, источники и носители защищаемой информации. Задачи систем защиты информации. Демаскирующие признаки объектов. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.2	Характеристика технической разведки. Основные этапы добывания информации. Технология добывания информации. Способы несанкционированного доступа к конфиденциальной информации. Добывание информации без физического проникновения в контролируемую зону. Доступ к источникам информации без нарушения государственной границы. Показатели эффективности добывания информации. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.3	Общая характеристика ТКУИ. Определение ТКУИ. Место ТКУИ в общей системе угроз безопасности информации. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.4	Концепция и методы инженерно-технической защиты информации. Организационно-методические основы защиты информации. Методика принятия решения на защиту от утечки информации в организации. Организация защиты информации. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.5	Методы и средства защиты информации. Организация защиты речевой информации. Классификация помещений. Пассивные методы и средства защиты информации. Аппаратура и способы активной защиты помещений. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.6	Методы и средства защиты информации. Организация защиты информа-ции от утечки, возникающей при работе вычислительной техники за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.7	Методы и средства защиты информации. Организация защиты СВТ от несанкционированного доступа. Защита АРМ. Защита периметра сети. Средства обнаружения вторжений. Контроль информационной безопасности. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
1.8	Контроль эффективности мер защиты информации. Мероприятия по выявлению каналов утечки информации. Специальные проверки. Специальные обследования. Специальные исследования. /Лек/	8	2	ОПК-9 ОПК-13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 2. Лабораторные работы						

2.1	Выявление опасных сигналов, возникающих при работе средств вычислительной техники /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.2	Проведение измерений и выявление слабых сигналов от исследуемых технических средств /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.3	Оценка защищенности объектов от утечки информации по каналам ПЭМИН /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.4	Оценка эффективности генератора шума для защиты по каналу ПЭМИ /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.5	Освоение практических приёмов работы с системой «Шепот» /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.6	Оценка защищенности двери и стены от утечки информации по акустическому и виброакустическому каналам /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.7	Оценка защищенности окон от утечки информации по акустическому и виброакустическому каналам /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
2.8	Оценка защищенности вентиляции и батареи водяного отопления от утечки информации по акустическому и виброакустическому каналам /Лаб/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 3. Практические работы						
3.1	Выявление опасных сигналов, возникающих при работе средств вычислительной техники /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	2	
3.2	Оценка защищенности объектов от утечки информации по каналам ПЭМИН /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	2	

3.3	Оценка эффективности генератора шума для защиты по каналу ПЭМИ /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	2	
3.4	Проведение измерений и выявление слабых сигналов от исследуемых технических средств /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	2	
3.5	Оценка защищенности двери и стены от утечки информации по акустическому и виброакустическому каналам /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
3.6	Оценка защищенности окон от утечки информации по акустическому и виброакустическому каналам /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
3.7	Оценка защищенности вентиляции и батареи водяного отопления от утечки информации по акустическому и виброакустическому каналам /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
3.8	Освоение практических приёмов работы с системой «Шепот» /Пр/	8	2	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 4. Самостоятельная работа						
4.1	Изучение теоретического материала по лекциям, учебной литературе и интернет-ресурсам /Ср/	8	16	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
4.2	Оформление отчетов по лабораторным работам и подготовка к их защите /Ср/	8	16	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
4.3	Изучение технической документации и функционала технических средств защиты информации /Ср/	8	14	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	
	Раздел 5. РГР						
5.1	Оптимизация системы активной защиты вентиляции и батареи водяного отопления по акустиче-скому и виброакустическому каналам и оценка её эффективности /РГР/	8	16	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	0	

5.2	Подготовка к зачету /Зачёт/	8	20	ОПК-9 ОПК -13	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Н.А. Свинарев	Инструментальный контроль и защита информации	Воронеж: Воронежский государственный университет инженерных технологий, 2013, http://biblioclub.ru/index.php?page=book&id=255905
Л1.2	Прохорова О. В.	Информационная безопасность и защита информации: Учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014, http://biblioclub.ru/index.php?page=book&id=438331
Л1.3	Громов Ю.Ю.	Информационная безопасность и защита информации: учеб. пособие для вузов	Старый Оскол: ТНТ, 2016,
Л1.4	Аверченков В. И., Рытов М. Ю.	Организационная защита информации	Москва: Флинта, 2011, http://biblioclub.ru/index.php?page=book&id=93343

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Ададуров С.Е.	Информационная безопасность и защита информации на железнодорожном транспорте. в 2 - ч.: Учеб.	Москва: ФГБОУ, 2014,

6.1.3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Титов А. А.	Инженерно-техническая защита информации	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010, http://biblioclub.ru/index.php?page=book&id=208567
Л3.2	Буркова И.Н.	Измерение физических величин, обработка и представление результатов измерения: метод. пособие для выполн. лабораторных работ	Хабаровск: Издательство ДВГУПС, 2012,

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	ФСТЭК России	http://www.fstec.ru
Э2	Компания Код безопасности	http://www.securitycode.ru
Э3	ФСБ России	http://www.fsb.ru
Э4	Национальный отрытый институт	http://www.intuit.ru
Э5	Группа компаний МАСКОМ	http://www.mascom.ru/

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.3.1 Перечень программного обеспечения

Office Pro Plus 2007 - Пакет офисных программ, лиц.45525415

Windows 7 Pro - Операционная система, лиц. 60618367
Free Conference Call (свободная лицензия)
Zoom (свободная лицензия)
6.3.2 Перечень информационных справочных систем
Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
324	Учебная аудитория для проведения практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях»	Комплект учебной мебели, экран, автоматизированное рабочее место IZEC «Студент» в сборе 16 шт, Автоматизированное рабочее место IZEC «Преподаватель» в сборе, автоматизированное рабочее место IZEC «Диспетчер АСУ ТП» в сборе, сервер IZEC на платформе WOLF PASS 2U в сборе, сервер IZEC на платформе SILVER PASS 1U в сборе, Ноутбук HP 250 G6 15.6, МФУ XEROX WC 6515DNI, электронный идентификатор ruToken S 64 КБ, электронный идентификатор JaCarta-2 PRO/ГОСТ, средство доверенной загрузки Dallas Lock PCI-E Full Size, средство доверенной загрузки "Соболь" версия 4 PCI-E 5 шт, рупор измерительный широкополосный П6-124 зав. № 150718305 в комплекте с диэлектрическим штативом, кабель КИ-18-5м-SMAM-SMAM, индуктор магнитный ИРМ-500М Зав. № 015, пробник напряжения Я6-122/1М Зав. № 024, токосъемник измерительный ТК-400М Зав. № 87, антенна измерительная
424	Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Лаборатория электронных устройств регистрации и передачи информации	комплект учебной мебели, мультимедийный проектор, экран, компьютер преподавателя
201	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы	столы, стулья, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС, проектор
304	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, интерактивная доска, мультимедийный проектор, компьютер, система акустическая

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

С целью эффективной организации учебного процесса учащимся в начале семестра предоставляется учебно-методическое и информационное обеспечение, приведенное в данной рабочей программе.
В процессе обучения студенты должны, в соответствии с календарным планом, самостоятельно изучать теоретический материал по предстоящему занятию и формулировать вопросы, вызывающие у них затруднение для рассмотрения на лекционном, практическом или лабораторном занятии.
В назначенные дни студент имеет возможность получить консультации у ведущего преподавателя.
При проведении лабораторных (практических) работ от студента требуется выполнять все требования преподавателя. По результатам выполнения каждой лабораторной (практической) работы формируется отчет, который подлежит последующей защите. Правила оформления отчета и требования к содержанию находятся в методических указаниях к лабораторным (практическим) работам.
Перед осуществлением защиты лабораторной (практической) работы студенту необходимо освоить весь теоретический материал, имеющий отношение к данной лабораторной работе. Подготовка к защите лабораторной (практической) работы включает в себя самоподготовку и консультации.
После получения задания студенту предоставляется возможность подготовиться к ответу в течение не более академического часа. Аттестация в письменной форме проводится для всех студентов академической группы одновременно. При аттестации в форме собеседования преподаватель обсуждает со студентом один или несколько вопросов из учебной программы. При необходимости преподаватель может предложить дополнительные вопросы, задачи и примеры. Для проведения аттестации в письменной форме используется перечень вопросов, утвержденный заведующим кафедрой. В перечень включаются вопросы из различных разделов курса, позволяющие проверить и оценить теоретические знания студентов и умение применять их для решения практических задач.
По окончании ответа студента на вопросы преподаватель проставляет результаты сдачи. Лабораторная (практическая) работа остаются у преподавателя.
Для подготовки к промежуточной аттестации студенту рекомендуется ознакомиться со списком вопросов и успешно ответить на содержащиеся в них вопросы.
Для повышения качества подготовки и самопроверки знаний студентам рекомендуется систематически изучать учебные материалы, и отвечать на контрольные вопросы.