МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Угрозы информационной безопасности автоматизированных систем» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от 15.05.2025 , протокол № 9

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000EAAAF3
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью дисциплины «Угрозы информационной безопасности автоматизированных систем» является изучение основных типов угроз информационной безопасности, характерных для современных автоматизированных систем (АС) в защищенном исполнении, а также основных подходов к проведению количественного и качественного анализа информационных рисков.

Задачи дисциплины:

- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области анализа угроз информационной безопасности АС, оценки рисков информационных ресурсов предприятия;
- формирование у обучаемых целостного представления об управлении информационными рисками

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности	РД1	Знание	основные категории угроз информационной безопасности в автоматизированных системах, основные модели угроз и модели нарушителя в автоматизированных системах
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах	РД2	Знание	основные методы построения систем защиты от угроз нарушения конфиденциальности, целостности и доступности информации

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	Формирование ценностей	Целевые ориентиры
Формирование гражданской позиции и патриотизма		
Развитие патриотизма и гражданской ответственности	Гражданственность	Мотивированность
Формирование духовно-нравственных ценностей		
Формирование ответственного отношения к труду	Взаимопомощь и взаимоуважение	Любознательность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Служение Отечеству и ответственность за его судьбу	Самостоятельность
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Права и свободы человека	Соблюдение моральных принципов

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Угрозы информационной безопасности автоматизированных систем» относится к дисциплинам по выбору и направленно на расширение профессиональных компетенций Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Аудит информационной безопасности».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.ДВ.Б	8	4	55	36	0	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Введение в дисциплину.	РД1, РД2	10	0	0	36	Тест
2	Модели угроз и модели нарушителя	РД1, РД2	18	0	0	37	Тест
3	Анализ рисков и управление рисками.	РД1, РД2	8	0	0	33	Тест
Итого по таблице			**36**	**0**	**0**	**106**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение в дисциплину.

Содержание темы: Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Понятие угрозы информационной безопасности. Классификация угроз информационной безопасности. Основные категории угроз. Системный подход к перечислению угроз информационной безопасности. Нормативная база. Анализ автоматизированных систем. Понятие и анализ угроз информационной безопасности автоматизированных систем. Основы системного анализа. Классификация угроз информационной безопасности автоматизированных систем с использованием системного анализа. Нормативная база. Подход «Общих критериев». Методики STRIDE и DREAD.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

Тема 2 Модели угроз и модели нарушителя.

Содержание темы: Количественная оценка безопасности вычислительных систем. Основы оценки рисков: декомпозиция объектов и груз информационной безопасности автоматизированных систем. Дерево опасностей. Подход «Общих критериев». Методики оценки риска STRIDE и DREAD. Понятие модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя. Системный анализ и построение модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

Тема 3 Анализ рисков и управление рисками.

Содержание темы: Понятие анализа рисков. Количественный и качественный анализ рисков. Нормативная база: отечественные и зарубежные методологии и рекомендации. Особенности анализа рисков в АС кредитно-финансовых учреждений. Нечеткие модели методы анализа информационных рисков. Методики оценки рисков. Количественный и качественный анализ рисков. Нормативная база: отечественные и зарубежные методологии и рекомендации. Нечеткие модели методы анализа информационных рисков. Построение экспертных систем оценки рисков с использованием нечёткой логики.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: Лекция- дискуссия.

Виды самостоятельной подготовки студентов по теме: подготовка лекционным занятиям.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

В ходе изучения дисциплины «Угрозы информационной безопасности автоматизированных систем» студенты посещают аудиторные занятия (лекции, консультации). При изучении дисциплины предусмотрено применение инновационных технологий обучения, таких как интерактивные лекции - дискуссии в диалоговом режиме по обсуждению актуальных проблем, выступления с презентациями сообщений на согласованные с преподавателем и подготовленные дома темы, самостоятельное выполнение заданий и упражнений с последующим обсуждением методов их решения. Самостоятельная работа студентов предполагает работу с учебниками, учебными пособиями и практикумами, поиском информации по заданным темам в Интернет.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания,

методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070 (дата обращения: 15.10.2025).

2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569267 (дата обращения: 15.10.2025).

7.2 Дополнительная литература

1. Лапина, М. А., Административное право. Административный процесс : учебник / М. А. Лапина, Г. Ф. Ручкина, ; под ред. М. А. Лапиной, Г. Ф. Ручкиной. — Москва : Юстиция, 2022. — 576 с. — ISBN 978-5-4365-8286-3. — URL: https://book.ru/book/941808 (дата обращения: 26.10.2025). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2021. — 267 с. — ISBN 978-5-406-08259-1. — URL: https://book.ru/book/939292 (дата обращения: 26.10.2025). — Текст : электронный.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "BOOK.ru"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- Microsoft Office 2010 Standart
- СПС КонсультантПлюс: Версия Проф

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-1 : Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации	ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности
	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-1 «Способен разрабатывать проекты организационно-распорядительных документов регламентирующих информационную безопасность бизнес- процессов организации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-1.2к : Разрабатывает проекты организационно - распорядительных документов, регламентирующих бизнеспроцессы в соответствии с требованиями законодательства в части информационной безопасности	РД 1	Знание	основные категории угроз информационной безопасности в автоматизированных системах, основные модели угроз и модели нарушителя в автоматизированных системах	решение тестовых заданий

Компетенция ПКВ-2 «Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	

ПКВ-2.1к : Определяет угрозы безопасности информации, реализация которых может привести к нарушениям безопасности в информационных системах	РД 2	Знание	основные методы построения систем защиты от угроз нарушения конфиденциальности, целостности и доступности и нформации	решение тестовых заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : основные категории угроз информационной безопасности в автоматизированных системах, основные модели угроз и модели нарушителя в автоматизированных системах	1.1. Введение в дисциплину.	Опрос	Экзамен в устной форме
		1.2. Модели угроз и модели нарушителя	Опрос	Экзамен в устной форме
		1.3. Анализ рисков и управление рисками.	Опрос	Экзамен в устной форме
РД2	Знание : основные методы построения систем защиты от угроз нарушения конфиденциальности, целостности и доступности информации	1.1. Введение в дисциплину.	Опрос	Экзамен в устной форме
		1.2. Модели угроз и модели нарушителя	Опрос	Экзамен в устной форме
		1.3. Анализ рисков и управление рисками.	Опрос	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство		
	Участие в лекции- дискуссии	Экзамен	Итого
Лекционные занятия	80		80
Промежуточная аттестация		20	20
Итого	80	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции

от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обна руживает всестороннее, систематическое и глубокое знание учебного материала , усвоил основную литературу и знаком с дополнительной литературой, рекоме ндованной программой, умеет свободно выполнять практические задания, пред усмотренные программой, свободно оперирует приобретенными знаниями, уме ниями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: осно вные знания, умения освоены, но допускаются незначительные ошибки, неточн ости, затруднения при аналитических операциях, переносе знаний и умений на н овые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворитель но»	Студент демонстрирует сформированность дисциплинарных компетенций: в хо де контрольных мероприятий допускаются значительные ошибки, проявляется о тсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным к омпетенциям, студент испытывает значительные затруднения при оперировани и знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворите льно»	У студента не сформированы дисциплинарные компетенции, проявляется недос таточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворите льно»	Дисциплинарные компетенции не сформированы. Проявляется полное или прак тически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примерные темы для опроса

1. Основные понятия в области риск-менеджмента: угроза, уязвимость, атака, риск, оценка риска. Их взаимосвязь.
2. Место анализа рисков в общей схеме управления ИБ
3. Количественный подход к оценке рисков. Достоинства, недостатки подхода.
4. Качественный подход к оценке рисков. Достоинства, недостатки подхода.
5. Экономическая модель оценки рисков.
6. Вероятностная модель оценки рисков.
7. ГОСТ Р ИСО 31000-2010: принципы и схема процесса риск менеджмента.
8. Управление рисками и жизненный цикл информационной системы.
9. ГОСТ Р ИСО/МЭК 15408-1-2012 «Общие критерии оценки безопасности информационных технологий. Введение и общая модель». Основные понятия и их взаимосвязь.
10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Общие критерии оценки безопасности информационных технологий. Введение и общая модель». Профиль защиты
11. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Схема процесса менеджмента рисков. Модель PDCA.
12. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Этап «Установление контекста менеджмента риска».
13. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Этап «Идентификация риска»
14. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Этап «Оценка риска»
15. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Обработка риска. Мониторинг и пересмотр, передача и принятие риска.
16. Классификация угроз информационной безопасности.
17. Основные категории угроз.
18. Системный подход к перечислению угроз информационной безопасности. Нормативная база. Подход «Общих критериев».
19. Модели угроз и модели нарушителя Понятие модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и

зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя.

Краткие методические указания

Для подготовки к опросу студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программны й материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	6-7	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по с уществу излагает его, не допуская существенных неточностей в ответе на вопрос, правил ьно применяет теоретические положения при решении практических вопросов и задач.
3	2-5	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основ ного материала, но не усвоил его деталей, допускает неточности, недостаточно правильн ые формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной ч асти программного материала, допускает существенные ошибки.

5.2 Вопросы к экзамену

1. Понятие уровня зрелости организации с точки зрения управления рисками безопасности.
2. Область применения процесса определения угроз безопасности информации.
3. Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба.
4. Мониторинг и переоценка угроз безопасности информации.
5. Типы нарушителей. Виды и потенциал нарушителей.
6. Возможные способы реализации угроз безопасности информации.
7. Оценка вероятности (возможности) реализации угрозы безопасности информации.
8. Оценка степени возможного ущерба от реализации угрозы безопасности информации.
9. Определение актуальности угрозы безопасности информации.
10. Формирование экспертной группы.
11. Проведение экспертной оценки Определение показателя «затрачиваемое время».
12. Определение показателя «техническая компетентность нарушителя».
13. Определение показателя «знание нарушителем проекта и информационной системы».
14. Определение показателя «возможности нарушителя по доступу к информационной системе».
15. Определение показателя «оснащенность нарушителя».

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программны й материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по с уществу излагает его, не допуская существенных неточностей в ответе на вопрос, правил ьно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основ ного материала, но не усвоил его деталей, допускает неточности, недостаточно правильн ые формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной ч асти программного материала, допускает существенные ошибки.