МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ С.М. Пасмурнов

«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Методы проектирования защищённых распределённых информационных систем»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация «Обеспечение информационнной безопасности распределѐнных информационных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Язов Ю.К./

Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является изучение методов проектирования защищенных распределенных информационных систем, Case-технологий, RAD-технологий, международных стандартов и методов защиты данных.

1.2. Задачи освоения дисциплины

- изучение основных понятий и методов проектирования защищенных распределенных информационных систем;
- ознакомление с классификацией методов проектирования;
- знакомство с существующими классификациями стандартов разработку информационных систем.
- изучение основных принципов Case-технологий.
- изучение основных понятий и методов защиты данных.
- изучение RAD-технологии портативного создания приложений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы проектирования защищённых распределённых информационных систем» относится к дисциплинам базовой части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Методы проектирования защищённых распределённых информационных систем» направлен на формирование следующих компетенций:

ПК-2 - способностью создавать и исследовать модели автоматизированных систем

ПК-3 - способностью проводить анализ защищенности автоматизированных систем

ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации

ПСК-7.3–способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем;

ПСК-7.5 – способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-2	знать теоретические основы и основные методики информационного моделирования процессов и систем
	уметь выполнять информационное моделирование процессов и

	систем; осуществлять организацию контроля качества входной информации
	владеть навыками информационного моделирование процессов и систем; методами организации контроля качества входной информации
ПК-3	знает методологию проведения комплексного анализа защищенности автоматизированных систем
	умеет применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации
	владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах
ПК-9	знает основные угрозы безопасности информации и модели нарушителя
	умеет оценивать информационные риски в автоматизированных системах;
ПК-17	знает методологию проведения комплексного анализа защищенности и инструментального мониторинга распределённых информационных систем
	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных системах, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем
ПСК-7.3	знает основные требования к подсистеме аудита и политике аудита; знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем
	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных информационно-управляющих системах на транспорте, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем
	владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы
ПСК-7.5	знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем
	умеет проводить обследование подразделений организации (учреждения, предприятия) в целях определения их информационных потребностей

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Методы проектирования защищённых распределённых информационных систем» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		8

Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	36	36
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	36	36
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Теоретические основы проектирования информационных систем. Технологии проектирования ИС	Понятие ИС. Структура ИС. Основные понятия и структура проекта ИС. Требования к эффективности и надежности проектных решений. Основные компоненты технологии проектирования ИС. Характеристика применяемых технологий проектирования. Требования, предъ-являемые к технологии проектирования ИС.	6	6	6	18
2	Стандарты и профили в области информационных систем	Классификация стандартов на проектирование и разработку инфор-мационных систем. Международный стандарт ISO/IEC 12207. 1995-08-01. Стандарты комплекса ГОСТ34. Rational Unified Process (RUP). Microsoft Solution Framework (MSF). Extreme Programming (XP)	6	6	6	18
3	Моделирование функциональной области внедрения ИС	Анализ и моделирование функциональной области. Внедрения информационных систем. Методологии моделирования предметной области.	6	6	6	18
4	Каноническое проектирование ИС.	Стадии и этапы процесса проектирования ИС. Состав работ на пред проектной стадии, стадии технического и рабочего проектирования, стадии ввода в действие ИС, эксплуатации и сопровождения. Состав проектной документации. Состав, содержание и принципы организации информационного обеспечения ИС.	6	6	6	18

5	Автоматизированное проектирование ИС Типовое проектирование ИС	Основные принципы Case-технологии. Факторы эффективности Case-технологии. Функционально-ориентированный подход. Этапы проектирования. Объектно-ориентированный подход. Понятие типового элемента. Классификация типовых информационных систем и их характеристика. Методы конфигурирования типовой информационной системы	6	6	6	18
6	Проектирование процессов защиты данных	Основные понятия и методы защиты данных. Стандарты на создание систем защиты данных.	6	6	6	18
		Итого	**36**	**36**	**36**	**108**

5.2 Перечень лабораторных работ

Жизненный цикл ИС.

2.Методы и средства проектирования ИС.

3.Методика Oracle CDM.

4.Методология функционально-ориентированного моделирования.

5.Проектирование пользовательского интерфейса.

6.Классификация Case-средств проектирования и стратегия их выбора.

7. Примеры типовых информационных систем и их характеристика.

8.Проектирование системы защиты данных

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	знать теоретические основы и	знание теоретических основ и	Выполнение	Невыполнение

	основные методики информационного моделирования процессов и систем	основных методик информационного моделирования процессов и систем	работ в срок, предусмотренный в рабочих программах	работ в срок, предусмотренный в рабочих программах
	уметь выполнять информационное моделирование процессов и систем; осуществлять организацию контроля качества входной информации	уметь выполнять информационное моделирование процессов и систем; осуществлять организацию контроля качества входной информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками информационного моделирование процессов и систем; методами организации контроля качества входной информации	владение навыками информационного моделирование процессов и систем; методами организации контроля качества входной информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-3	знает методологию проведения комплексного анализа защищенности автоматизированных систем	знание методологии проведения комплексного анализа защищенности автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации	умеет применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах	владение навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-9	знает основные угрозы безопасности информации и модели нарушителя	знание основных угроз безопасности информации и модели нарушителя	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет оценивать информационные риски в автоматизированных системах;	умеет оценивать информационные риски в автоматизированных системах;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-17	знает методологию проведения комплексного анализа защищенности и инструментального мониторинга распределённых информационных систем	знание методологии проведения комплексного анализа защищенности и инструментального мониторинга распределённых информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных системах, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных системах, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает основные требования к подсистеме аудита и политике аудита; знает критерии оценки эффективности и надежности средств защиты программного обеспечения	знание основных требований к подсистеме аудита и политике аудита; знает критерии оценки эффективности и надежности средств защиты программного обеспечения	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	автоматизированных систем	автоматизированных систем		
ПСК-7.3	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных информационно-управляющих системах на транспорте, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных информационно-управляющих системах на транспорте, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	владение навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем	знание содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-7.5	умеет проводить обследование подразделений организации (учреждения, предприятия) в целях определения их информационных потребностей	умеет проводить обследование подразделений организации (учреждения, предприятия) в целях определения их информационных потребностей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	знать теоретические основы и основные методики информационного моделирования процессов и систем	знание теоретических основ и основных методик информационного моделирования процессов и систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-2	знать теоретические основы и основные методики информационного моделирования процессов и систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь выполнять информационное моделирование процессов и систем; осуществлять организацию контроля качества входной информации	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками информационного моделирование процессов и систем; методами организации контроля качества входной информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

ПК-3	знает методологию проведения комплексного анализа защищенности автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	умеет применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-9	знает основные угрозы безопасности информации и модели нарушителя	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	умеет оценивать информационные риски в автоматизированных системах;	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПК-17	знает методологию проведения комплексного анализа защищенности и инструментального мониторинга распределённых информационных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных системах, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ПСК-7.3	знает основные требования к подсистеме аудита и политике аудита; знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных информационно-управляющи х системах на транспорте, применять автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядител ьные документы по системе защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	автоматизированной системы			
ПСК-7.5	знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	умеет проводить обследование подразделений организации (учреждения, предприятия) в целях определения их информационных потребностей	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1.Понятие технологии и операции проектирования. Требования к технологии проектирования.

2.Понятие метода проектирования ИС, их классификация.

3.Основные стадии жизненного цикла проектирования ИС.

4.Модели жизненного цикла ИС.

5.Международный стандарт ISO/IEC 12207: 1995-08-01

6.Стандарты комплекса ГОСТ34

7.Методика Oracle CDM

8.Методологии структурного анализа Йодана/де Марко и Гейна-Сарсона (DFD -технология).

9.Диаграммы потоков данных: объекты диаграмм.

10.Диаграммы «сущность - связь». Сущности, отношения и связи.

11.Диаграммы переходов состояний. Назначение, объекты, правила и способы построения.

12.Последовательность работ при построении моделей данных по DFD-технологии.

13.Метод моделирования процессов (IDEF3).

14.Метод функционального моделирования SADT (IDEF0). Характеристика диаграмм. Типы взаимосвязей между блоками.

7.2.2 Примерный перечень заданий для решения стандартных задач

ПК-2 –	**способностью создавать и исследовать модели автоматизированных систем**
1.	Понятие жизненного цикла АИС.
2.	Процессы жизненного цикла АИС: основные, вспомогательные, организационн
3.	Стадии жизненного цикла АИС: моделирование, управление требованиями, ана
4.	проектирование, установка и сопровождение.
5.	Модели жизненного цикла АИС.
6.	Задачи и этапы проектирования автоматизированных систем в защищенном исп
7.	Методологии проектирования АИС.
8.	Организация работ, функции заказчиков и разработчиков.
9.	Требования к автоматизированной системе в защищенном исполнении.
10.	Работы на стадиях и этапах создания автоматизированных систем в защищенно исполнении

11.	Методы и модели описания систем.
12.	Качественные методы описания систем. Методика системного анализа.
13.	Качественные методы описания систем: методы типа мозговой атаки; методы типа
14.	сценариев; методы экспертных оценок; методы типа дерева целей; морфологические методы.
15.	Количественные методы описания систем.
16.	Характеристики уровней абстрактного описания систем: символический или лингвистический; теоретико-множественный; абстрактно-алгебраический; топологический; логико-математический; теоретико-информационный; динамический; эвристический
17.	Оценка качества и эффективности информационных систем. Показатели качества для выбора функциональных возможностей. Функциональная пригодность. Надежность.
18.	Средства структурного анализа. DFD (Data Flow Diagrams) – диаграммы потоков данны
19.	Средства структурного анализа. ERD (Entity-Relationship Diagrams) – диаграммы «сущнос□ь-связь»;
20.	Средства структурного анализа. STD (State Transition Diagrams) – диаграммы переходов состояний
ПК-3 – способностью проводить анализ защищенности автоматизированных систем	
1.	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации.
2.	Понятие автоматизированной (информационной) системы. Отличительные черты АИС
3.	Критерии классификации угроз. Методы оценки опасности угроз.
4.	Понятие уязвимости угрозы. Классификация уязвимостей.
5.	Организационные, правовые, программно-аппаратные, криптографические, технически меры защиты информации в автоматизированных системах.
6.	Управление промышленными предприятиями в стандарте MRP II
7.	Основные аспекты автоматизации деятельности предприятия на примере финансово-управленческих систем
8.	Области применения и примеры реализации информационных технологий управления корпорацией
9.	Распределенные БД в Oracle и Oracle в распределенных БД
10.	Администрирование распределенных систем на примере Oracle
21.	Управление политиками безопасности на уровне приложения
ПК-5 – способностью проводить анализ рисков информационной безопаснос автоматизированной системы	
1.	Бизнес-ориентированное управление ИТ на современном предприятии.
2	Виды программ технического обслуживания (стандартные программы).
3.	Значение технического обслуживания.
4.	Как обслуживаются высококритичные системы.
5.	Концепция управления ИТ-подразделением — IT Service Management.
6.	Функциональные требования. Вопросы гарантии и эффективности в европейском стандарте ITSEC
7.	Гарантии безопасности компьютерных систем в системе общих критериев
8.	Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев
9.	Основны□ угрозы безопасности информации в компьютерных системах
10.	Государственная политика в области безопасности компьютерных систем
ПК-17 – способностью проводить инструментальный мониторинг защищенности информаци в автоматизированной системе и выявлять каналы утечки информации	
1.	Порядок сертификации средств защиты информации для разработчика СЗИ.
2.	Порядок сертификации защищенных информационных систем

3.	Порядок лицензирования в области создания средств защиты информации и зац информационных систем
5.	Разработка политик безопасности щтя защищенных компьютерных систем
6.	Порядок аттестации защищенных компьютерных систем
7.	Критерии эффективности работы ИС.
8.	Оперативные мероприятия.
9.	Организация технического обслуживания ИТ.
10.	Плановые □ероприятия.
ПСК-7.3 – способностью проводить аудит защищенности информационно-технологи ресурсов распределенных информационных систем	
1.	Порядок внедрения SLM-снстемы.
2.	Порядок осуществления гарантии.
3.	Преимущества внедрения ITSM.
4.	Причины отказа в □арантийном обслуживании.
5.	Программы технического обслуживания.
6.	Разовые мероприятия.
7.	Расширенные программы технического обслуживания.
8.	Регламентные мероприятия.
9.	Содержание модели ITSM HP. Процессы взаимодействия и ИТ-служб.
10.	Содержание модели ITSM HP. Процессы проектирования и управления услугами.
ПСК-7.5 – способностью координировать деятельность подразделений и специалисто защите информации в организациях, в том числе на предприятии и в учреждении	
11.	Корпоративная стратегия управления человеческими ресурсами как основа кадров политики.
12.	Ценности, цели, принципы управления человеческими ресурсами: мировой опыт эффективных трудовых организаций.
13.	Особенности формирования кадровой политики, ориентированной на организацик социального управления,□приоритет социальных ценностей, социальной политик
14.	Основные уровни разработки кадровой политики.
15.	Основополагающие принципы формирования кадровой политики.
16.	Современные процессуальные теории мотивации.
17.	Понятие команды. Основные характеристики эффективной команды.
18.	Природа организационного лидерства. Функции лидеров.
19.	Понятие кадровой безопасности.
20.	Безопасность найма сотрудников.
21.	Административные методы обеспечения кадровой безопасности.

7.2.3 Примерный перечень заданий для решения прикладных задач

ПК-2 – способностью создавать и исследовать модели автоматизированных систем	
1.	*Что такое этап реализации?* а) построение выводов по данным, полученным путем имитации **б)** теоретическое применение результатов программирования в) **практическое применение модели и результатов моделирования.**
2.	*Для чего служит прикладное программное обеспечение?* **а)** планирования и организации алгоритмов управления объектом **б)** планирования и организации вычислительного процесса в ЭВМ; в) **реализация алгоритмов управления объектом**
3.	*Тождественная декомпозиция это операция, в результате которой…* **а) любая система превращается в саму себя;** б) средства декомпозиции тождественны; в) система тождественна

4.	*На что не ориентируются при выборе системы управления, состоящей из нескольких элементов?* **а)** на функциональную полноту. **б) на быстродействие и надежность;** **в)** *на определенное число элементов;*
5.	*Что понимается под программным обеспечением?* а) набор специальных программ для моделирования. б) **соответствующим образом организованный набор программ и данных;** в) набор специальных программ для работы САПР
6.	*Параллельная коррекция системы управления позволяет…* а) скорректировать АЧХ системы. б) **обеспечить введение интегралов и производных от сигналов ошибки;** в) осуществить интегральные законы регулирования
7.	*Модульность структуры состоит* **а) в разбиении программного массива на модули по функциональному признаку.** б) в построении модулей по иерархии в) на принципе вложенности с вертикальным управлением;
8.	*Результаты имитационного моделирования…* а) являются источником информации для построения реального объекта б) **носят случайный характер, отражают лишь случайные сочетания действующих факторов, складывающихся в процессе моделирования;** в) являются неточными и требуют тщательного анализа.
9.	*Какими могут быть средства декомпозиции?* а) реальными и нереальными. б) имитационными; в) **материальными и абстрактными;**
10.	*Что осуществляется на этапе подготовки данных?* а) описание модели на языке, приемлемом для используемой ЭВМ; б) определение границ характеристик системы, ограничений и измерителей показателей эффективности; в) **происходит отбор данных, необходимых для построения модели, и представлении их в соответствующей форме**
ПК-3 – способностью проводить анализ защищенности автоматизированных систем	
1.	*Как называется показатель, количественно выражающийся суммой ежегодных прямых и косвенных затрат на функционирование корпоративной системы защиты информации?* а) экономическая эффективность бизнеса б) общая величина затрат на внедрение системы ИБ в**) совокупная стоимость владения системой ИБ** г) коэффициент возврата инвестиций
2.	*Эффективность защиты информации это…* **а) степень соответствия результатов защиты информации поставленной цели.** б) мера или характеристика для оценки эффективности защиты информации. в) значения показателей эффективности защиты информации, установленные нормативными документами.
3.	*Показатель эффективности защиты информации –* **а) мера или характеристика для оценки эффективности защиты**

	информации. б) степень соответствия результатов защиты информации поставленной цели. в) значения показателей эффективности защиты информации, установленные нормативными документами
4.	*Нормы эффективности защиты информации –* **а) значения показателей эффективности защиты информации, установленные нормативными документами.** б) совокупность действий по разработке и/или практическому применению методов и средств контроля эффективности защиты информации в) степень соответствия результатов защиты информации поставленной цели
5.	*Мероприятие по контролю эффективности защиты информации –* а) **совокупность действий по разработке и/или практическому применению методов и средств контроля эффективности защиты информации.** б) степень соответствия результатов защиты информации поставленной цели в) значения показателей эффективности защиты информации, установленные нормативными документами
6.	*Категорирование защищаемой информации [объекта защиты] –* **а) установление градаций важности защиты защищаемой информации [объекта защиты].** б) степень соответствия результатов защиты информации поставленной цели в) значения показателей эффективности защиты информации, установленные нормативными документами
7.	*Метод [способ] контроля эффективности защиты информации –* **а) порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.** б) установление градаций важности защиты защищаемой информации [объекта защиты]. в) проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации
8.	*Контроль состояния защиты информации –* а) **проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.** б) установление градаций важности защиты защищаемой информации [объекта защиты]. в) проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.
9.	*Средство контроля эффективности защиты информации –* **а) техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.** б) проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации
10.	*Контроль организации защиты информации –* **а) проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.** б) проверка соответствия эффективности мероприятий по защите информации

	установленным требованиям или нормам эффективности защиты информации.
ПК-5 – способностью проводить анализ рисков информационной безопасности автоматизированной системы	
1.	*Что в сфере информационной безопасности принято считать риском?* а) **потенциальную возможность понести убытки из-за нарушения безопасности информационной системы** б) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней в) характеристику, которая делает возможным возникновение угрозы
2.	*Что принято считать ресурсом или активом информационной системы?* а) модель информационной системы б) все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет в) **именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите**
3.	*Что отличает риск от угрозы?* а) объем вероятных потерь б) **наличие количественной оценки возможных потерь и (возможно) оценки вероятности реализации угрозы** в) угроза и риск - понятия идентичные
4.	*Почему аналитический метод определения минимальных затрат при расчетах защиты информационной системы неприменим?* а) потому, что расчеты ресурсов подвержены флуктуациям, связанными с колебаниями на рынке услуг в сфере безопасности ИС **б) потому, что на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным** в) потому, что уровень защищенности информационной системы неадекватен затратам на ее защиту
5.	*Идентифицируется ли риск уязвимостью, через которую может быть реализована некая угроза в отношении определенного ресурса?* а) **да** б) нет в) да, но только в случае отсутствия угрозы
6.	*На какие ресурсы может быть направлена угроза?* а) только на информационные ресурсы б) только на аппаратные ресурсы **в) на любые виды ресурсов (информационный, аппаратный, программный и т.д.)**
7.	*Что представляет собой система с полным перекрытием?* а) система, в которой ведется учет всех вторжений, блокируются только вредоносные проникновения б) система, в которой имеются средства защиты на каждый возможный путь проникновения в) система, в которой обеспечивается селективная безопасность
8.	*Что происходит с размером ожидаемых потерь при увеличении затрат на защиту?* а) падает б) находится в зависимости от других факторов в) не изменяется
9.	*Каким параметром принято определять степень разрушительности?* а) коэффициентом разрушительности

	б) стоимостью ресурса в) коэффициентом риска
10.	*Что в сфере информационной безопасности принято считать риском?* а) **потенциальную возможность понести убытки из-за нарушения безопасности информационной системы** б) потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную систему, а также информацию, хранящуюся и обрабатывающуюся в ней в) характеристику, которая делает возможным возникновение угрозы
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
1.	*Какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну?* а) на проведение работ, связанных с созданием средств защиты информации на осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну б) какую лицензию должна получить испытательная лаборатория для проведения работ по сертификации средств защиты информации, используемых на объектах информатизации, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну? в) на деятельность по технической защите конфиденциальной информации **г) на деятельность по разработке и производству средств защиты конфиденциальной информации**
2.	*Кто выдает предписания на приостановление работ на аттестованном объекте информатизации?* а) **ФСТЭК России** б) орган по аттестации в) лицензиат, имеющий лицензию на ТЗКИ г) заявитель
3.	*Туннелирование может применяться для достижения следующих целей:* а) **передача через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается** б) расширение спектра поддерживаемых протоколов в) уменьшение нагрузки на сеть
4.	*Какие из перечисленных мер защиты относятся к организационным?* а) защита периметра сети с помощью межсетевого экрана б) **создание службы защиты информации** **в) определение порядка доступа к защищаемым объектам** г) использование антивирусных средств защиты
5.	*Какие из перечисленных характеристик не входят в систему обеспечения безопасности Клементса:* а) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов? б) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций в) O - набор защищаемых объектов; T - набор угроз; M - набор средств обеспечения безопасности; P- набор креативных функций; Z - набор виндикативных инструментов

	г) Р- набор креативных функций; Z - набор виндикативных инструментов
6.	*Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от:* **а) перехвата** **б) воспроизведения** **в) атак на доступность**
7.	*Аутентификация на основе пароля, переданного по сети в зашифрованном виде и снабженного открытой временной меткой, плоха, потому что не обеспечивает защиты от:* **а) перехвата** **б) воспроизведения** в) атак на доступность
8.	*Демилитаризованная зона располагается:* а) перед внешним межсетевым экраном **б) между межсетевыми экранами** в) за внутренним межсетевым экраном
9.	*К межсетевым экранам целесообразно применять следующие принципы архитектурной безопасности:* усиление самого слабого звена **эшелонированность обороны** **невозможность перехода в небезопасное состояние**
10.	Системы анализа защищенности помогают предотвратить: **известные атаки** новые виды атак нетипичное поведение пользователей
ПСК-7.3 – способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	
1	*Каким термином обозначается анализ регистрационной информации системы защиты?* мониторинг **аудит** аккредитация сертификация
2	*Какие компоненты присутствуют в модели системы защиты с полным перекрытием?* **область угроз** область рисков **защищаемая область** **система защиты** область безопасности
3	*Как называется возможность осуществления угрозы Т в отношении объекта О?* слабость неполнота **уязвимость** риск
4	*Чем характеризуется степень сопротивляемости механизма защиты?* **вероятностью его преодоления** количеством угроз, которым этот механизм препятствует величиной потерь в случае успешного прохождения стоимостью механизма защиты

5	*При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...* **0** 1
6	*Защищенность системы защиты определяется как величина…* обратная суммарному количеству рисков обратная остаточному риску **обратная уязвимости** равная сумме всех уязвимостей
7	*В чем заключается идеология открытых систем информационной безопасности?* в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы **в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре** в открытости информации о стоимости реализации конкретной системы защиты в открытости программных кодов средств защиты от производителей разных стран
8	*В чем заключается принцип минимизации привилегий?* выделение полных прав доступа только администраторам системы **выделение только тех прав, которые необходимы для реализации своих должностных обязанностей** выделение прав доступа в зависимости от величины возможного ущерба
9	*Что из нижеперечисленного относится к оперативным методам повышения безопасности?* систематическое тестирование предотвращение ошибок в CASE-технологиях обязательная сертификация **программная избыточность**
10	*Что из нижеперечисленного относится к мерам предотвращения угроз безопасности?* **систематическое тестирование** предотвращение ошибок в CASE-технологиях **обязательная сертификация** программная избыточность
ПСК-7.5 – способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	
1.	*Какие результаты должны быть получены в типовом проекте "Организация службы ИТ"?* **а) предложения по организационной структуре СИТ, включая проект Положения службе** **б) модель бизнес-процессов СИТ** **в) пакет документов, регламентирующих деятельность СИТ** г) процедура оценки эффективности СИТ д) бюджет СИТ е) штатная структура СИТ
2.	*Какая модель взаимодействия СИТ с компанией предполагает контрактные отношения?* а) базовая модель б) продвинутая модель

	в) модель аутсорсинга
3.	*К адаптивным структурам управления относятся:* **а) проектная** б) дивизиональная в) линейно-функциональная **г) матричная**
4.	*Достоинствами линейно-функциональной структуры являются:* а) стабильность (наиболее эффективны в стабильной среде) **б) экономия на управленческих расходах** **в) быстрое решение простых проблем, находящихся в компетенции одной функциональной службы** г) широкая специализация работников, которая расширяет их профессиональный горизонт **д) ориентация на действующие технологии и сложившийся рынок** **е) ориентация на ценовую конкуренцию** ж) большой объем полномочий функциональных и линейных руководителе, позволяющий быстро решать сложные проблемы
5.	*Недостатками линейно-функциональная структура являются:* а) неэффективность в стабильной среде **б) недостаточность полномочий у функциональных и линейных руководителей, которые "выталкивают" принятие решения на уровень вышестоящего руководителя, тем самым перегружая его текущими проблемами** в) **медленное принятие решения, поскольку обсуждение проблем происходит по всей иерархической цепочке снизу вверх внутри каждого функционального подразделения** **г) качество решений на высшем уровне определяется не столько компетентностью самих руководителей, сколько надежностью и достоверностью поступившей к ним информации** д) большие управленческие расходы **е) линейно-функциональная структура порождает "ведомственность" внутри предприятия** **ж) узкая специализация работников, которая сужает горизонт их профессионального видения, принижает общеорганизационные цели и задачи до функциональных** **з) ограничение возможности профессионального развития функциональных и особенно линейных руководителей (последние освобождаются от специализированных управленческих функций, сосредотачивая свое внимание на проблемах собственно производства)**
6.	*В соответствии с какими основными принципами производится структуризация компании по дивизионам:* **а) по продуктовому** б) по уровню зрелости бизнеса в) по уровню доходов **г) в зависимости от ориентации на конкретного потребителя** **д) по региональному** е) по уровню прибыли
7.	*Какая структура управления ведет к росту иерархичности управления?* **а) дивизиональная** б) линейно-функциональная в) матричная г) проектная

8.	Какие организационные структуры сравнительно-легко меняют свою форму, приспосабливаются к изменяющимся условиям? а) линейно-функциональные б) дивизиональные **в) матричные** **г) проектные**
9.	*Для каких структур управления характерен минимум бюрократической регламентации деятельности органов управления?* а) линейно-функциональные **б) адаптивные** в) дивизиональные **г) матричные** **д) проектные**
10.	*Какими признаками характеризуются адаптивные организационные структуры?* **а) способностью сравнительно легко менять свою форму** б) ориентацией на ускоренную реализацию типовых проектов **в) ограниченным действием во времени** **г) созданием временных органов управления**

7.2.4 Примерный перечень вопросов для подготовки к зачету

1.Подходы к построению и проектированию информационных систем. Основные принципы системного подхода к созданию ИС.

2.Понятие технологии и операции проектирования. Требования к технологии проектирования.

3.Классификация технологий проектирования ИС. Выбор технологии проектирования ИС.

4.Понятие метода проектирования ИС, их классификация.

5.Классификация средств проектирования ИС.

6.Основные стадии жизненного цикла проектирования ИС.

7.Модели жизненного цикла ИС.

8.Классификация стандартов на проектирование и разработку информационных систем.

9.Международный стандарт ISO/IEC 12207: 1995-08-01

10.Стандарты комплекса ГОСТ34

11.Методика Oracle CDM

12.Понятие профиля ИС. Процессы формирования, развития и применения профилей информационных систем.

13.Классификация структурных методологий. Сравнительный анализ.

14.Методологии структурного анализа Йодана/де Марко и Гейна-Сарсона (DFD - технология).

15.Диаграммы потоков данных: объекты диаграмм.

16.Диаграммы потоков данных: словари данных, спецификации процессов.

17.Диаграммы «сущность - связь». Сущности, отношения и связи.

18.Диаграммы «сущность - связь». Атрибуты, категоризация сущностей.

19.Диаграммы переходов состояний. Назначение, объекты, правила и способы построения.

20.Последовательность работ при построении моделей данных по DFD-технологии.

21.Метод моделирования процессов (IDEF3).

22.Метод функционального моделирования SADT (IDEF0). Характеристика диаграмм. Типы взаимосвязей между блоками.

23.Последовательность создания функциональных моделей SADT.

24.Понятие канонического проектирования, его особенности. Стадии и этапы процесса проектирования ИС.

25.Состав работ на предпроектной стадии.

26.Состав работ на стадии технического и рабочего проектирования.

27.Состав работ на стадии ввода в действие ИС, эксплуатации и сопровождения.

28.Состав, содержание и принципы организации информационного обеспечения ИС.

29.Проектирование пользовательского интерфейса.

30.Проектирование документальных и фактографических БД.

31.Назначение технико-экономического обоснования, его основные компоненты.

32.Назначение технического задания.

33.Понятие технического проекта ЭИС, его основные компоненты.

34.Методы внедрения проекта ЭИС и их особенности.

35.Внутримашинное информационное обеспечение ИС, его компоненты.

36.Внемашинное информационное обеспечение ИС, его компоненты.

37.Понятие CASE-технологии проектирования ИС. Основные принципы Case-технологии. Факторы эффективности Case-технологии.

38.Классификация CASE-средств, стратегия их выбора.

39.Функционально-ориентированное проектирование ИС с использованием CASE-средств.

40.Объектно-ориентированная технология проектирования в CASE-системах.

41.Особенности типового проектирования. Понятие типового элемента. Классификация и примеры типовых информационных систем и их характеристика.

42.Методы конфигурирования типовой информационной системы.

43.Технологии параметрически - ориентированного и модельно-ориентированного проектирования.

44.Принципы и особенности проектирования интегрированных ИС.

45.Открытые информационные системы. основные свойства и межсистемные интерфейсы

46.Стандартные методы совместного доступа к базам и программам в сложных информационных системах

47.Система управления информационными потоками как средство интеграции приложений ИС.

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Теоретические основы проектирования информационных систем. Технологии проектирования ИС	ПК-2, ПК-3, ПК-9, ПК-17, ПСК-7.3, ПСК-7.5	Тест, защита лабораторных работ
2	Стандарты и профили в области информационных систем	ПК-2, ПК-3, ПК-9, ПК-17, ПСК-7.3, ПСК-7.5	Тест, защита лабораторных работ
3	Моделирование функциональной области внедрения ИС	ПК-2, ПК-3, ПК-9, ПК-17, ПСК-7.3, ПСК-7.5	Тест, защита лабораторных работ
4	Каноническое проектирование ИС.	ПК-2, ПК-3, ПК-9, ПК-17, ПСК-7.3, ПСК-7.5	Тест, защита лабораторных работ
5	Автоматизированное проектирование ИС Типовое проектирование ИС	ПК-2, ПК-3, ПК-9, ПК-17, ПСК-7.3, ПСК-7.5	Тест, защита лабораторных работ
6	Проектирование процессов защиты данных	ПК-2, ПК-3, ПК-9, ПК-17, ПСК-7.3, ПСК-7.5	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на

бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная

1. Новиков С.Н. Проектирование защищённых телекоммуникационных систем [Электронный ресурс]: учебное пособие/ Новиков С.Н., Попков Г.В.— Электрон. текстовые данные.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2018.— 439 с.— Режим доступа: http://www.iprbookshop.ru/102152.html.

2. Грекул В.И. Проектирование информационных систем [Электронный ресурс]: учебное пособие/ Грекул В.И., Денищенко Г.Н., Коровкина Н.Л.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 299 с.— Режим доступа: http://www.iprbookshop.ru/97577.html.

Дополнительная

1. Бугров Ю.Г., Остапенко Г.А., Радько Н.М. Моделирование атак сети массового обслуживания [Электронный ресурс]:учеб. пособие. - Электрон. дан. (1 файл : 1248 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет"

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

- http://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ)
- http://e.lanbook.com/ (ЭБС Лань)
- http://znanium.com/ (ЭБС Знаниум)
- http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Методы проектирования защищённых распределённых информационных систем» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к	Готовиться к промежуточной аттестации следует систематически, в

промежуточной аттестации	течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.