

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»



УТВЕРЖДАЮ:

Ректор

/ Н.В. Дубив/

«31» августа 2020 г.

Рабочая программа учебной дисциплины

МЕТОДЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ
ИНФОРМАЦИОННЫХ СИСТЕМ»

образовательной программы высшего образования –
программы специалитета

10.05.03 — Информационная безопасность автоматизированных систем

Направленность: (специализация №7) обеспечение информационной безопас-
ности распределенных информационных систем

Формы обучения: очная

Рабочая программа дисциплины «Методы проектирования защищенных распределенных информационных систем» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения «28» августа 2020 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2020 года, протокол № 1.

Рабочую программу составил:
ст. преподаватель



С.В. Мельников

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент



Е.Н. Полякова

Специалист по учебно-методической
работе Учебно-методического
отдела



Г.В. Казанкова

Начальник Управления
образовательной деятельности



С.Н. Синецын

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	семестр
		7
Аудиторные занятия (контактная работа с преподавателем), всего часов		
в том числе:	64	64
Лекции		
Лабораторные работы	32	32
Практические занятия	32	32
Самостоятельная работа, всего часов		
в том числе:	80	80
Контрольная работа		
Подготовка к экзамену	18	18
Другие виды самостоятельной работы (подготовка к лабораторным работам и рубежному контролю)	27	27
35	35	35
Вид промежуточной аттестации	экзамен	экзамен
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	144	144

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Изучение дисциплины «Методы проектирования защищенных распределенных информационных систем» относится к вариативной части блока 1, сформированных при изучении следующих дисциплин:

- Информатика
- Основы теории защиты информации
- Основы информационной безопасности
- Информационная безопасность распределенных информационных систем
- Безопасность операционных систем
- Криптографические методы защиты информации
- Безопасность систем баз данных
- Безопасность сетей ЭВМ.

Дисциплина обеспечивает изучение дисциплин: «Техническая защита информации», «Разработка и эксплуатация защищенных автоматизированных систем», «Технология построения защищенных распределенных приложений», «Управление информационной безопасностью», а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является теоретическая и практическая подготовка студентов в области защищенных распределенных информационных систем в такой степени, чтобы они могли выбирать необходимые технические, алгоритмические, программные и технологические решения, уметь объяснить принципы их функционирования и правильно их использовать.

Задачами дисциплины:

- ознакомление студентов с современными подходами к проектированию, эксплуатации и модернизации информационных систем в целом, с концепциями обеспечения информационной безопасности распределенных информационных систем;
- изучение технологии функционирования защищенных распределенных информационных систем;
- использование принципов защиты для разработки и реализации механизмов защиты распределенных сетей;
- формирование у студентов системных представлений о каноническом, автоматизированном, типовом подходе к проектированию информационных систем с применением современных CASE-средств;
- формирование у студентов практических навыков использования CASE-средств для проектирования и модернизации баз данных и хранилищ данных;
- овладение навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

Компетенции, формируемые в результате освоения дисциплины:

- способность к самоорганизации и самообразованию (ОК-8);
- способность создавать и исследовать модели автоматизированных систем (ПК-2);
- способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
- способность участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);
- способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2).

В результате изучения дисциплины обучающийся должен:

знать

- принципы построения распределенных систем и объектно-ориентированных систем управления базами данных (для ОК-8, ПК-2, ПК-12);
- CASE-технологии для проектирования баз данных и хранилищ данных (для ПК-13);
- основы организации и функционирования распределенных систем, их стандарты, протоколы и предоставляемые сервисы (для ПК-2, ПК-9);

Уметь

- проектировать защищенные распределенные информационные системы (для ПК-9, ПК-13);
- определять и устранять основные угрозы информационной безопасности для защищенных распределенных систем (для ПСК-7.1, ПСК-7.2);

владеть

- терминологией и системным подходом построения защищенных распределенных систем (для ПК-9, ПСК-7.1);
- навыками анализа угроз информационной безопасности и уязвимостей в защищенных распределенных системах (для ПК-2, ПСК-7.2).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем	
			Лекции	Лабораторные работы
Рубеж 1	Тема 1.	Введение. Теоретические основы проектирования информационных систем (ИС)	2	2
	Тема 2	Технологии проектирования ИС	4	-
	Тема 3	Стандарты и профили в области ИС	4	2
	Тема 4	Моделирование функциональной области	4	2

		внедрения ИС		
Рубеж 2	Тема 5	Каноническое проектирование ИС		
	Тема 6	Автоматизированное проектирование ИС	4	6
	Тема 7	Типовое проектирование ИС	4	4
	Тема 8	Проектирование процессов защиты данных	4	-
	Тема 9	Управление проектированием ИС	4	16
		Всего:	32	32

4.2. Содержание лекционных занятий

Тема 1 Введение. Теоретические основы проектирования информационных систем (ИС).

Основные определения. Понятие ИС. Классы информационных систем. Структура однопользовательской и многопользовательской, малой и корпоративной, локальной и распределенной ИС, состав и назначение подсистем.

Основные понятия и структура проекта ИС. Формирование требований, концептуальное проектирование, спецификация приложений, разработка моделей, интеграция и тестирование ИС.

Жизненный цикл ИС. Понятие жизненного цикла. Основные, вспомогательные, организационные процессы жизненного цикла. Содержание и взаимосвязь процессов жизненного цикла ИС.

Модели жизненного цикла ИС. Каскадная модель с промежуточным контролем. Спиральная модель.

Тема 2 Технологии проектирования ИС

Основные компоненты технологии проектирования ИС. Методы и средства проектирования ИС. Характеристика применяемых технологий проектирования. Требования, предъявляемые к технологии проектирования ИС. Выбор технологии проектирования ИС.

Тема 3 Стандарты и профили в области ИС

Классификация стандартов на проектирование и разработку ИС. Международный стандарт ISO/IEC12207: 1995-08-01. Стандарты комплекса ГОСТ 34. Методика Oracle CDM. Rational Unified Process (RUP). Microsoft Solution Framework (MSF). Extreme Programming (XP).

Понятие профиля ИС. Цели, принципы и процессы формирования, развития и применения профилей информационных систем.

Тема 4 Моделирование функциональной области внедрения ИС

Анализ и моделирование функциональной области внедрения ИС. Основные понятия организационного бизнес-моделирования. Миссия компании, дерево цепей и стратегии их достижения. Процессные потоковые модели. Модели структур данных. Полная бизнес-модель компании. Проектирование организационно-функциональной структуры компании.

Методология функционально-ориентированного моделирования. Методология объектно-ориентированного моделирования.

Совместимость и переносимость прикладных программ между различными платформами. Две составные части технологии распределенных информационных систем – совместимость (взаимодействие систем) и переносимость прикладных программ между различными платформами. Основные аспекты

переносимости приложений и совместимости систем. Возможность переноса прикладных систем. Тестирование программ на переносимость.

Тема 5 Каноническое проектирование ИС

Стадии и этапы процесса проектирования ИС. Стандарт ГОСТ34.601-90. Формирование требований, разработка концепции ИС. Техническое задание. Состав работ на предпроектной стадии, стадии технического и рабочего проектирования, стадии ввода в действие ИС, эксплуатации и сопровождения. Эскизный проект. Технический проект. Рабочая документация. Ввод в действие. Сопровождение ИС.

Состав, содержание и принципы организации информационного обеспечения ИС. Проектирование пользовательского интерфейса. Проектирование документальных и фактографических баз данных.

Тема 6 Автоматизированное проектирование ИС

Основные принципы Case-технологии. Факторы эффективности Case-технологии. Классификация Case-средств проектирования и стратегия их выбора. Функционально-ориентированный подход. Этапы проектирования.

Объектно-ориентированный подход. Содержание RAD-технологии прототипного создания приложений.

Тема 7 Типовое проектирование ИС

Понятие типового элемента. Классификация и примеры типовых ИС и их характеристика. Методы конфигурирования типовой информационной системы. Технологии параметрически-ориентированного и модельно-ориентированного проектирования.

Тема 8 Проектирование процессов защиты данных

Уязвимости распределенных ИС на примере интранета. Причины уязвимости. Основные уязвимости ИС: уязвимости архитектуры клиент-сервер, уязвимости операционных систем, уязвимости систем управления базами данных, уязвимость систем электронного документооборота, уязвимость рабочих станций, уязвимость каналов связи, уязвимость сетевых протоколов. Слабости системных утилит, команд и сетевых сервисов. Слабости современных технологий программирования и ошибки в программном обеспечении.

Атаки на распределенные ИС и их классификация. Удаленные атаки на ИС, их классификация. Типовые удаленные атаки. Атаки с использованием сетевых протоколов. Информационные и сетевые ресурсы распределенных ИС как объекты атак.

Обеспечение ИБ в распределенных ИС. Четырехуровневая модель ИС. Специфика защиты ресурсов распределенной ИС на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Основные понятия и методы защиты данных. Стандарты на создание систем защиты данных. Проектирование системы защиты данных в ИБ.

Тема 9 Управление проектированием ИС

Организационные структуры проектирования ИС. Планирование и контроль проектных работ.

4.3 Лабораторные работы

№ темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
1	Введение. Теоретические основы проектирования информационных систем	<i>Лабораторная работа №1.</i> Модели жизненного цикла ИС. Работа со справочниками.	2
3	Стандарты и профили в области ИС	<i>Лабораторная работа №2.</i> Базовые стандарты. Профили. Документы, регистры накопления, отчеты.	2
4	Моделирование функциональной области внедрения ИС	<i>Лабораторная работа №3.</i> Разбор примеров на применение методологий SADT для проектирования ИС.	2
5	Каноническое проектирование ИС	<i>Лабораторная работа №4.</i> Разбор примеров на применение основные нотаций языка UML для проектирования ИС. Разработка технического задания для ИС	4
<i>1-ый рубежный контроль</i>		Тестирование	
6	Автоматизированное проектирование ИС	<i>Лабораторная работа №5.</i> Построение диаграмм различных ИС с помощью Case-средств.	2 4
8	Проектирование процессов защиты данных	<i>Лабораторная работа №6.</i> Специфика защиты ресурсов распределенной ИС на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям.	4
		<i>Лабораторная работа №7.</i> Реализация ИС по выполненному техническому заданию. Выбор модели проектирования. Определение подсистем.	4
		<i>Лабораторная работа №8.</i> Разработка информационной базы. Выборка данных из информационной базы. Составление отчетов.	2
		<i>Лабораторная работа №9.</i> Обеспечение целостности. Обеспечение безопасности ИС программными методами.	4
<i>2-ой рубежный контроль</i>		Тестирование	
Итого			2 32

4.4 Контрольная работа

В процессе контрольной работы у студентов формируются навыки ведения самостоятельной работы и разработки проектных решений по информационно-технологическому и программному обеспечению. Студенты учатся:

- анализировать информационную среду предметной области и устанавливать структурное представление и взаимосвязи с другими компонентами информационного пространства;
- анализировать информационные потоки, выстраивать логическую структуру проекта.

Выполнение контрольных работ способствует повышению теоретической и профессиональной подготовки студентов, а также лучшему усвоению учебного материала.

Студент выбирает одну из предложенных преподавателем тем, самостоятельно готовит презентацию и выносит на обсуждение.

Результат выполнения контрольной работы оформляется в виде пояснительной записки, объемом 15-20 страниц.

Методика выполнения контрольной работы изложена в методических указаниях к выполнению контрольной работе по дисциплине «Методы проектирования защищенных распределенных информационных систем».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано применение на лабораторных работах разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает подготовку к лабораторным работам, к рубежным контролям, выполнение контрольной работы и подготовку к экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела	3
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	28
Подготовка к рубежным контролям (по 2 часа на каждый рубеж)	4

Контрольная работа	18
Подготовка к экзамену	27
Всего:	80

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
4. Контрольная работа.
5. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание						
		Распределение баллов, 7семестр						
	Вид учебной работы:	Посещение лекций	Выполнение и защита лабораторной работы	Контрольная работа	Рубежный контроль №1	Рубежный контроль №2	Экзамен	
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)	Балльная оценка:	$1_6 \times 16 = 16_6$	$4_6 \times 9 = 36_6$	6	6	6	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и экзамене.	60 и менее баллов – неудовлетворительно; незачет; 61... 73 – удовлетворительно; зачет; 74... 90 – хорошо; 91... 100 – отлично						
3	Критерии допуска к промежуточной аттестации, возможности получения автоматически экзаменационной оценки «удовлетворительно» по дисциплине, возможность получения бонусных баллов	<p>Для допуска к промежуточной аттестации (экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и контрольную работу.</p> <p>Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов:</p> <p>- 68 для получения «автоматически» оценки «удовлетворительно».</p> <p>По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».</p>						

4	<p>Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра</p>	<p>В случае если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных работ.</p> <p>Формы дополнительных заданий (назначаются преподавателем):</p> <ul style="list-style-type: none"> - выполнение и защита пропущенной лабораторной работы – до 4 баллов Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении,
		<p>проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.</p>

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования. Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

Варианты тестовых заданий для рубежных контролей № 1 и № 2 состоят из 15 вопросов. На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Экзамен – в форме устного ответа на 2 вопроса. Перечень вопросов преподаватель выдает заранее. Время, отводимое студенту на подготовку вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

Результаты текущего контроля успеваемости и экзамена заносятся преподавателем в экзаменационную ведомость, которая сдается в организационный отдел института в день экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и экзамена

Примерные тестовые задания для рубежного контроля №1

1. Какие из следующих утверждений являются верными:

(Отметьте один правильный вариант ответа.)

Вариант 1. Распределенная система считается безопасной, если все передаваемые по сети данные – шифруются.

Вариант 2. Распределенная система в большинстве случаев будет системой, в которой присутствует параллельное выполнение потоков – либо на разных узлах, либо на одном.

Вариант 3. Масштабируемость – свойство, которым распределенная система обладает по определению.

2. Какие из перечисленных примеров не являются примерами распределенных систем:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

Вариант 1. несколько инструментальных сред программирования, расположенных на разных компьютерах.

Вариант 2. инструментальная среда программирования Eclipse.

Вариант 3. несколько инструментальных сред программирования, расположенных на разных компьютерах, взаимодействующих с системой контроля версий.

3. Какие из следующих утверждений являются верными:

(Отметьте один правильный вариант ответа.)

Вариант 1. Распределенная система всегда будет работать быстрее и надежнее монолитной системы.

Вариант 2. Разработка распределенной системы как правило более сложная задача, чем разработка монолитной системы.

Вариант 3. Разработка распределенных систем настолько сложная задача, что под силу только крупнейшим IT-компаниям.

Примерные тестовые задания для рубежного контроля №2

1. Какие из следующих утверждений являются верными:

(Ответ считается верным, если отмечены все правильные варианты ответов.)

Вариант 1. Модель сервиса часто используется при построении распределенных систем с высокими требованиями к надежности и производительности.

Вариант 2. Модель сервиса является лучшей из всех возможных моделей построения распределенной системы, однако чрезвычайно сложна в реализации, поэтому в настоящий момент практически нет примеров распределенных систем, построенных с ее использованием.

Вариант 3. Одна из самых больших сложностей при построении распределенных систем с использованием модели сервиса – обеспечение целостности и непротиворечивости данных, при их одновременной обработке несколькими серверами, образующими сервис.

2. Какие из следующих утверждений являются верными:

(Отметьте один правильный вариант ответа.)

Вариант 1. Архитектура "клиент-сервер" на текущий момент является морально-устаревшей и не должна выбираться в качестве модели при построении распределенных систем.

Вариант 2. Архитектура "клиент-сервер" является одной из возможных моделей построения распределенных систем, обладает как достоинствами, так и недостатками, что позволяет рекомендовать выбирать эту архитектуру в качестве базовой, для распределенных систем определенных классов.

Вариант 3. Архитектура "клиент-сервер" является лучшей архитектурой, для создания распределенной системы.

3. Открытость, применительно к распределенным системам означает:
(Отметьте один правильный вариант ответа.)

Вариант 1. Отсутствие шифрования передаваемых данных.

Вариант 2. Использование при разработке системы открытых стандартов и наличие только документирование интерфейсов.

Вариант 3. Предоставление конечному пользователю исходных кодов системы.

Примерный перечень вопросов к экзамену

1. Понятие информационной системы (ИС). Классы информационных систем.
2. Структура однопользовательской и многопользовательской, малой и корпоративной, локальной и распределенной ИС, состав и назначение подсистем.
3. Формирование требований, концептуальное проектирование, спецификация приложений, разработка моделей, интеграция и тестирование ИС.
4. Жизненный цикл ИС. Понятие жизненного цикла.
5. Основные, вспомогательные, организационные процессы жизненного цикла. Содержание и взаимосвязь процессов жизненного цикла ИС.
6. Модели жизненного цикла ИС.
7. Основные компоненты технологии проектирования ИС.
8. Методы и средства проектирования ИС.
9. Характеристика применяемых технологий проектирования.
10. Требования, предъявляемые к технологии проектирования ИС.
11. Выбор технологии проектирования ИС.
12. Классификация стандартов на проектирование и разработку ИС. Международный стандарт ISO/IEC12207: 1995-08-01.
13. Стандарты комплекса ГОСТ 34.
14. Методика Oracle CDM.
15. Rational Unified Process (RUP).
16. Microsoft Solution Framework (MSF).
17. Extreme Programming (XP).
18. Понятие профиля ИС. Цели, принципы и процессы формирования, развития и применения профилей информационных систем.
19. Анализ и моделирование функциональной области внедрения ИС.
20. Основные понятия организационного бизнес-моделирования.
21. Миссия компании, дерево цепей и стратегии их достижения.
22. Процессные потоковые модели.
23. Модели структур данных.
24. Полная бизнес-модель компании.
25. Проектирование организационно-функциональной структуры компании.

26. Методология функционально-ориентированного моделирования.
27. Методология объектно-ориентированного моделирования.
28. Совместимость и переносимость прикладных программ между различными платформами.
29. Две составные части технологии распределенных информационных систем. Возможность переноса прикладных систем.
30. Тестирование программ на переносимость.
31. Стадии и этапы процесса проектирования ИС.
32. Стандарт ГОСТ34.601-90.
33. Формирование требований, разработка концепции ИС.
34. Техническое задание.
35. Состав работ на предпроектной стадии, стадии технического и рабочего проектирования, стадии ввода в действие ИС, эксплуатации и сопровождения. Эскизный проект.
36. Технический проект.
37. Рабочая документация. Ввод в действие. Сопровождение ИС.
38. Состав, содержание и принципы организации информационного обеспечения ИС.
39. Проектирование пользовательского интерфейса.
40. Проектирование документальных и фактографических баз данных.
41. Основные принципы Case-технологии. Факторы эффективности Case-технологии.
42. Функционально-ориентированное проектирование ИС с использованием Case-средств.
43. Этапы проектирования.
44. Объектно-ориентированный подход.
45. Содержание RAD-технологии прототипного создания приложений.
46. Классификация и примеры типовых ИС и их характеристика.
47. Методы конфигурирования типовой информационной системы.
48. Технологии параметрически-ориентированного и модельно-ориентированного проектирования.
49. Уязвимости распределенных ИС на примере интранета. Причины уязвимости. Основные уязвимости ИС.
50. Слабости системных утилит, команд и сетевых сервисов.
51. Слабости современных технологий программирования и ошибки в программном обеспечении.
52. Атаки на распределенные ИС и их классификация.
53. Удаленные атаки на ИС, их классификация.
54. Типовые удаленные атаки.
55. Атаки с использованием сетевых протоколов.
56. Информационные и сетевые ресурсы распределенных ИС как объекты атак.
57. Обеспечение ИБ в распределенных ИС.
58. Четырехуровневая модель ИС.
59. Специфика защиты ресурсов распределенной ИС на примере интранета.
60. Выбор сетевой топологии интранета при подключении к другим внешним сетям.
61. Основные понятия и методы защиты данных.

62. Стандарты на создание систем защиты данных.
63. Проектирование системы защиты данных в ИБ.
64. Организационные структуры проектирования ИС.
65. Планирование и контроль проектных работ.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Заботина Н.Н. Проектирование информационных систем [Электронный ресурс] : учеб. Пособие/Н.Н. Заботина. – М. : НИЦ Инфра-М, 2013. – 331 с. – Режим доступа: <http://znanium.com/bookread.php?book=371912> (Дата обращения 24 января 2017)
2. Основы построения автоматизированных информационных систем: Учебник / В.А. Гвоздева, И.Ю. Лаврентьева. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 320 с. URL: <http://znanium.com/bookread.php?book=392285> (Дата обращения 24 января 2017)
3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф.Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: <http://znanium.com/bookread.php?book=335362> (Дата обращения 24 января 2017)
4. Вендров А.М. CASE-технологии. Современные методы и средства проектирования информационных систем. М.: Финансы и статистика, 2008.

7.2. Дополнительная учебная литература

1. Проектирование информационных систем: Учебное пособие / В.В. Коваленко. - М.: Форум: НИЦ ИНФРА-М, 2014. - 320 с.: 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-549-5, 300 экз. <http://znanium.com/bookread.php?book=473092>.
2. Методологии и технологии системного проектирования информационных систем: Учебник / Э.Р. Ипатова, Ю.В. Ипатов; РАО. - М.: Флинта: МПСИ, 2008. - 256 с.: 60x88 1/16. - (Инф.технологии). (о) ISBN 978-5-89349-978-0, 1000 экз. <http://www.znanium.com/bookread.php?book=161482>

7.3. Методическая литература

1. Мельников С.В. Методические указания к выполнению лабораторных работ по дисциплине «Методы проектирование защищенных распределенных информационных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. Курган, кафедра «БИАС». – 26 с.
2. Мельников С.В. Методические указания к выполнению контрольной работы по дисциплине «Методы проектирование защищенных распределенных

информационных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. Курган, кафедра «БИАС». – 14 с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. <http://www.intuit.ru> [On-line] – Интернет-университет информационных технологий.
2. <http://www.delphimaster.ru> [On-line] – Мастер DELPHI [On-line]

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. Среды программирования Borland Delphi 7 и MS Visual Studio 2010, СУБД VS SQL Server 2008, XSpider Education.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе ПК Pentium с установленным программным обеспечением MS Windows XP и с возможностью выхода в Интернет.

Аннотация к рабочей программе дисциплины
**«Методы проектирования защищенных распределенных
информационных систем»**

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Направленность: (специализация №7)
**Обеспечение информационной безопасности распределенных
информационных систем**

Трудоемкость дисциплины: 4 з.е. (144 академических часа)
Семестр: 7 (очная форма обучения)
Форма промежуточной аттестации: экзамен

Содержание дисциплины

Современный подход к проектированию, эксплуатации и модернизации распределенных защищенных информационных систем; формирование системного представления о каноническом, автоматизированном, типовом подходе к проектированию информационных систем с применением современных CASE-средств; использование их для проектирования и модернизации баз данных и хранилищ данных. Определять и устранять основные угрозы информационной безопасности для распределенных защищенных систем и администрирование систем. Основные стандарты построения и взаимодействия распределенных систем.