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:
Проректор по образовательной и
международной деятельности
_____ / А.А. Кирсанкин/

«____»_____ 2026 г.

Рабочая программа учебной дисциплины

МЕТОДЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

образовательной программы высшего образования –
программы специалитета
10.05.03 ─ Информационная безопасность автоматизированных систем

Специализация №5: Безопасность открытых информационных систем

Формы обучения: очная

Курган 2026

Рабочая программа дисциплины «Методы проектирования защищенных распределенных информационных систем» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (безопасность открытых информационных систем), утвержденным для очной формы обучения «26» июня 2026 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «03» июля 2026 года, протокол № 12.

Рабочую программу составил:
старший прподаватель Д.С. Иванов

Согласовано:

Заведующий кафедрой «БИАС»
канд. техн. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

2. 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:	**80**	**80**
Лекции	32	32
Лабораторные работы	32	32
Практические занятия	16	16
Самостоятельная работа, всего часов в том числе:	64	64
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (подготовка к лабораторным, практическим работам и рубежному контролю)	37	37
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 части блока 1, формируемая участниками образовательных отношений, 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 обучающихся 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 обучающихся 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 обучающихся системных представлений о каноническом, автоматизированном, типовом подходе к проектированию информационных систем с применением современных CASE-средств;

– формирование у обучающихся 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:

– Способен разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-5);

– Способен подготавливать и оформлять руководящую, эксплуатационную и организационно-распорядительную документацию на системы защиты информации (ПК-6);

Планируемые результаты обучения по дисциплине «Методы проектирования защищенных распределенных информационных систем», индикаторы достижения компетенций ПК -5, ПК-6, перечень оценочных средств.

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1 ПК-5	Знать: CASE-технологии для проектирования баз данных и хранилищ данных	З (ИД-1 ПК-5)	Знает: Принципы и правила построения USE-CASE, ER и других диаграмм	Вопросы теста
2.	ИД-2 ПК-5	Уметь: определять и устранять основные угрозы информационной безопасности для защищенных распределенных систем	У (ИД-2 ПК-5)	Умеет: определять и использовать основные угрозы информационной безопасности для защищенных распределенных систем	Комплекс имитационных задач
3.	ИД-3 ПК-5	Владеть: навыками анализа угроз информационной безопасности и уязвимостей в защищенных распределенных системах	В (ИД-3 ПК-5)	Владеет: навыками анализа угроз информационной безопасности и уязвимостей в защищенных распределенных системах	Комплекс имитационных задач
4.	ИД-1 ПК-6	Знать: основы организации и функционирования распределенных систем, их стандарты, протоколы и предоставляемые сервисы	З (ИД-1 ПК-6)	Знает: основы организации и функционирования распределенных систем, их стандарты, протоколы и предоставляемые сервисы	Вопросы теста
5.	ИД-2 ПК-6	Уметь: проектировать защищенные распределенные информационные системы	У (ИД-2 ПК-6)	Умеет: проектировать защищенные распределенные информационные системы	Вопросы для сдачи экзамена

6.	ИД-3 ПК-6	Владеть: терминологией и системным подходом построения защищенных распределенных систем	В (ИД-3 ПК-6)	Владеет: терминологией и системным подходом построения защищенных распределенных систем	Вопросы для сдачи экзамена

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лаб. работы	Практ. занятия
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	4	-
	Тема 4	Моделирование функциональной области внедрения ИС	4	4	-
	Тема 5	Каноническое проектирование ИС	4	-	-
	Рубежный контроль №1		-	2	-
Рубеж 2	*Тема 6*	Автоматизированное проектирование ИС	4	18	-
	Тема 7	Типовое проектирование ИС	4	-	-
	Тема 8	Проектирование процессов защиты данных	4	-	16
	Тема 9	Управление проектированием ИС	2	-	-
	Рубежный контроль №2		-	2	-
		Всего:	**32**	**32**	**16**

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 интернета. 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 использование 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 интернета. Выбор сетевой топологии интернета 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	*Лабораторная работа №1.*Модели жизненного цикла ИС. Работа со справочниками.	3
3	Стандарты и профили в области ИС	*Лабораторная работа №2.* Базовые стандарты. Профили. Документы, регистры накопления, отчеты.	3
4	Моделирование функциональной области внедрения ИС	*Лабораторная работа №3.* Общие принципы организации распределенных ИС. Представление компонентной объектной модели (COM).	4
	1-ый рубежный контроль	**Тестирование**	**2**
6	Автоматизированное проектирование ИС	*Лабораторная работа №4.* Построение и настройка маршрутизируемой ЛВС с высокой доступностью на основе протокола маршрутизации OSPF	6
		Лабораторная работа №5. Методы и средства защиты сетевой инфраструктуры от НСД, а также принципы проектирования сетей управления	6

№ темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
		Лабораторная работа №6. Основные технологии межсетевого экранирования, методы и средства управления безопасностью информационных потоков	6
	2-ой рубежный контроль	**Тестирование**	**2**
		Итого	**32**

4.4 Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий.

Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, обучающемуся следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов обучающихся.

Номер темы	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
8	Проектирование процессов защиты данных	*Практическая работа №1.* Создание моделей нарушителей в распределенной информационной систем.	2
		Практическая работа №2. Формирование общих требований к организации безопасности распределенных информационных систем с учетом анализа угроз и различных групп нарушителей	2
		Практическая работа №3. Формирование технического задания. Осуществление технического и рабочего проектирования.	4
		Практическая работа №4. Проектирование системы контроля доступа к объектам РИС	8
		Итого	**16**

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 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:	15
Введение. Теоретические основы проектирования информационных систем (ИС)	1
Технологии проектирования ИС	1
Стандарты и профили в области ИС	1
Моделирование функциональной области внедрения ИС	1
Каноническое проектирование ИС	1
Автоматизированное проектирование ИС	1
Типовое проектирование ИС	4
Проектирование процессов защиты данных	4
Управление проектированием ИС	1
Подготовка к лабораторным работам (по 1 часа на каждое занятие)	14
Подготовка к практическим работам (по 1 часа на каждое занятие)	4
Подготовка к рубежным контролям (по 2 часа на каждый рубеж)	4
Подготовка к экзамену	27
Всего:	**64**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ

6.1. Перечень оценочных средств

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

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	***Распределение баллов, 7семестр***						
		Вид учебной работы:	Посещение лекций	Выполнение и защита лабораторной работы	Выполнение и защита практической работы	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	До 16	До 18	До $24_б$	6	6	30
		Приме-чания:	16 лекций по 1,5 балла	До 1,5 баллов за 3-х часовую лабораторную работу, До 3-х баллов за 4-ти часо-вую до 4-х баллов за 6-ти часо-вую (2 л.р. 3-х ча-совых, 2 – 6-ти часовых)	До 6 баллов за практическую работу	На 8-ой лек-лекции.	На 16-ой лек-лекции.	
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	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения экзамена без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися 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 обучающемуся отводится 2 академических часа.

Баллы обучающемуся 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 обучающегося 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 обучающемуся 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 обучающегося.

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. Р*аспределенная система в большинстве случаев будет системой, в которой присутствует параллельное выполнение потоков - либо на разных узлах, либо на одном.

*Вариант 3. М*асштабируемость - 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 использование 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

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

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

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.

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. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

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

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Специализация №5
Безопасность открытых информационных систем

Трудоемкость дисциплины: 4 з.е. (144 академических часа)
Семестр: 7
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.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины
«Методы проектирования защищенных распределенных информационных систем»

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Д.С. Иванов/

Изменения утверждены на заседании кафедры «___» _____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___» _____20___ г.

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Д.С. Иванов /

Изменения утверждены на заседании кафедры «___» _____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___» _____20___ г.