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:
Первый проректор
_____ /Т.Р. Змызгова/
«____»_____ 2024 г.

Рабочая программа учебной дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

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

Форма обучения: очная

Курган 2024

Рабочая программа дисциплины «Информационная безопасность распределенных информационных систем» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения «28» июня 2024 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 августа 2024 года, протокол № 1

Рабочую программу составил:
канд. техн. наук, доцент Д.И. Дик

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		6
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**64**	**64**
Лекции	32	32
Лабораторные работы	32	32
Практические занятия	-	-
Самостоятельная работа, всего часов в том числе:	**44**	**44**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к лабораторным работам и рубежному контролю)	26	26
Вид промежуточной аттестации	**зачет с оценкой**	**зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность распределенных информационных систем» относится к вариативной части, формируемой участниками образовательных отношений Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Организация ЭВМ и вычислительных систем.
- Основы информационной безопасности.
- Криптографические методы защиты информации.
- Основы теории защиты информации.

Дисциплина обеспечивает изучение дисциплин: «Техническая защита информации», «Разработка и эксплуатация защищенных автоматизированных систем», «Методы проектирования защищенных распределенных информационных систем», «Технология построения защищенных распределенных приложений», а также выпускной квалификационной работы. В рамках изучаемой дисциплины формируются навыки работы с распределенной информационной системой на предприятии, с учетом ее особенностей, свойств и выполняемых функций.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Цель дисциплины «Информационная безопасность распределенных информационных систем» – ознакомить студентов с основами построения и эксплуатации информационных систем на базе автономных автоматизированных рабочих мест, и распределенных информационных систем.

Задачи дисциплины:

– ознакомление студентов с порядком создания информационных систем на базе АРМ;

– ознакомление студентов с порядком создания ИС в защищенном исполнении;

– ознакомление студентов с наиболее часто встречающимися техническими и программно-техническими методами и средствами защиты распределенных информационных систем;

– овладение основными теоретическими и практическими навыками проектирования и эксплуатации распределенных информационных систем;

Компетенции, формируемые в результате освоения дисциплины:

– способность оценивать эффективность систем защиты информации, функционирующих в открытых информационных системах (ПК-8);

– способность оценивать риски, связанные с осуществлением угроз информационной безопасности (ПК-10);

– способность анализировать уровень защищенности открытых информационных систем (ПК-11);

– способность устанавливать и настраивать средства и системы защиты информации в открытых информационных системах (ПК-16);

Индикаторы и дескрипторы части соответствующей компетенции, форми-

руемой в процессе изучения дисциплины «Информационная безопасность распределённых информационных систем», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Информационная безопасность распределенных информационных систем», индикаторы достижения компетенций ПК-8, ПК-10, ПК-11, ПК-16, 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$_{ПК-8}$	Знать: принципы построения и структуру систем защиты данных в распределенной ИС	З (ИД-1$_{ПК-8}$)	Знает: принципы построения и структуру систем защиты данных в распределенной ИС	Вопросы теста
2.	ИД-2 $_{ПК-8}$	Уметь: разрабатывать концепцию обеспечения информационной безопасности распределенных ИС	У (ИД-2$_{ПК-8}$)	Умеет: разрабатывать концепцию обеспечения информационной безопасности распределенных ИС	Комплект имитационных задач
3.	ИД-3 $_{ПК-8}$	Владеть: требованиями федеральных органов исполнительной власти по построению защищенных автоматизированных систем	В (ИД-3$_{ПК-8}$)	Владеет: требованиями федеральных органов исполнительной власти по построению защищенных автоматизированных систем	Вопросы для сдачи зачета
4.	ИД-1$_{ПК-10}$	Знать: классификацию угроз безопасности при обработке данных в распределенных ИС	З (ИД-1$_{ПК-10}$)	Знает: классификацию угроз безопасности при обработке данных в распределенных ИС	Вопросы теста
5.	ИД-2 $_{ПК-10}$	Уметь: проводить оценки рисков безопасности информации в распределенных ИС	У (ИД-2$_{ПК-10}$)	Умеет: проводить оценки рисков безопасности информации в распределенных ИС	Комплект имитационных задач
6.	ИД-3 $_{ПК-10}$	Владеть: способами оценки рисков распределенных ИС	В (ИД-3$_{ПК-10}$)	Владеет: способами оценки рисков распределенных ИС	Вопросы для сдачи зачета
7.	ИД-1$_{ПК-11}$	Знать: принципы построения и структуру систем защиты данных в распределенной ИС	З (ИД-1$_{ПК-11}$)	Знает: принципы построения и структуру систем защиты данных в распределенной ИС	Вопросы теста

8.	ИД-2 $_{ПК-11}$	Уметь: разрабатывать политику безопасности для распределенных ИС	У (ИД-2$_{ПК-11}$)	Умеет: разрабатывать политику безопасности для распределенных ИС	Комплект имитационных задач
9.	ИД-3 $_{ПК-11}$	Владеть: способами оценки рисков распределенных ИС	В (ИД-3$_{ПК-11}$)	Владеет: способами оценки рисков распределенных ИС	Вопросы для сдачи зачета
10.	ИД-1$_{ПК-16}$	Знать: принципы построения и структуру систем защиты данных в распределенной ИС	З (ИД-1$_{ПК-16}$)	Знает: принципы построения и структуру систем защиты данных в распределенной ИС	Вопросы теста
11.	ИД-2 $_{ПК-16}$	Уметь: разрабатывать концепцию обеспечения информационной безопасности распределенных ИС	У (ИД-2$_{ПК-16}$)	Умеет: разрабатывать концепцию обеспечения информационной безопасности распределенных ИС	Комплект имитационных задач
12.	ИД-3 $_{ПК-16}$	Владеть: навыками создания приложений распределенных систем на основе систем баз данных	В (ИД-3$_{ПК-16}$)	Владеет: навыками создания приложений распределенных систем на основе систем баз данных	Вопросы для сдачи зачета

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	**Номер темы**	**Наименование раздела, темы**	Количество часов контактной работы с преподавателем	
			Лекции	Лабораторные работы
Рубеж 1	1	Распределенные информационные системы	4	2
	2	Автоматизированные системы и их связь с информационной безопасностью распределенных ИС	4	-
	3	Теоретические основы построения защищенных распределенных информационных систем	4	-
	4	Коммуникация в распределенных ИС, проектирование системы защиты информации в распределенных ИС	4	14
Рубеж 2	5	Информационные системы в защищенном исполнении.	4	9
	6	Информационные системы в виде отдельных автоматизированных рабочих мест.	4	-
	7	Информационные системы как совокупность распределенных автоматизированных рабочих мест объединенных в локальные вычислительные сети.	4	-
	8	Защита распределенных информационных систем с доступом к глобальным сетям передачи	4	7

		информации.		
		Всего:	**32**	**32**

4.2. Содержание лекционных занятий

Тема 1. Распределенные информационные системы.

Распределенные информационные системы: основные понятия, основные бизнес-процеессы. Анализ угроз безопасности при обработке данных в распределенных ИС. Цели и задачи построения распределенных ИС, их место в современном информационном обществе. Классификация распределенных ИС, особенности работы

Тема 2. Автоматизированные системы и их связь с информационной безопасностью.

Автоматизированные системы и их связь с информационной безопасностью распределенных ИС. Концепция обеспечения информационной безопасности распределенных ИС. Принципы построения системы защиты распределенной ИС. Комплект типовых документов и нормативных (законодательных) актов по эксплуатации и разработке распределенных ИС. Проведение мониторинга аудита информационной безопасности в распределенных ИС. Модульная работа, примеры концепции.

Тема 3. Теоретические основы построения защищенных распределенных информационных систем.

Стандарты информационной безопасности. Стандарты информационной безопасности распределенных систем. Модель взаимодействия открытых систем OSI/ISO. Рекомендации X.800 для распределенных систем. Основное содержание оценочного стандарта ISO/IEC 15408. Рекомендации НТД РФ по построению защищенных распределенных информационных систем.

Тема 4. Коммуникация в распределенных ИС, проектирование системы защиты информации в распределенных ИС.

Безопасность сетевых подключений распределенных ИС. Сложные распределенные системы – сферы применения, актуальность для российских предприятий. Централизованная и децентрализованная модель организации распределенных ИС.

Тема 5. Информационные системы в защищенном исполнении.

Требования федеральных органов исполнительной власти по построению защищенных автоматизированных систем. Требования ФСТЭК, ФСБ по созданию защищенных автоматизированных систем и локальных вычислительных сетей. Аттестация объектов информатизации по требования по защите информации и сертификация средств технической и криптографической защиты информации.

6. Информационные системы в виде отдельных автоматизированных рабочих мест.

Аттестация АРМ на соответствие требованиям по защите информации. Исследования на наличие сверхнормативных ПЭМИ на альтернативных измерительных площадках, аттестованных по ГОСТ 51320-99 и

удовлетворяющих требованиям ГОСТ 51319-99, ГОСТ 51318-99. Высокочастотное облучение и высокочастотное навязывание.

Тема 7. Информационные системы как совокупность распределенных автоматизированных рабочих мест объединенных в локальные вычислительные сети.

Криптографические средства защиты информации при передачи между сегментами ЛВС. Сертифицированные по требованиям ФСТЭК РФ и ФСБ РФ межсетевые экраны с возможностью шифрования траффика по ГОСТ 28147-89. Сертифицированные по требования на наличие НДВ операционные системы и базы данных.

Тема 8. Защита распределенных информационных систем с доступом к глобальным сетям передачи информации

Методы и средства защиты ИС с доступом к глобальной сети INTERNET. Системы обнаружения вторжений, информационный обмен с системой электронного документооборота федерального казначейства, информационный обмен с банковскими системами, система межведомственного электронного взаимодействия.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
1	Распределенные информационные системы	*Лабораторная работа №1.* Оценка рисков информационной безопасности распределенных ИС	2
4	Коммуникация в распределенных ИС, проектирование системы защиты информации в распределенных ИС	*Лабораторная работа №2.* Механизмы резервного копирования данных в операционной системе Windows 2003 Server.	6
		Лабораторная работа №3. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра.	4
		Лабораторная работа №4. Экономическая оценка эффективности системы защиты информации в распределенных ИС.	4
5	Информационные системы в защищенном исполнении	*Лабораторная работа №5.* Оценка защищенности сетевых приложений.	4
	1-ый рубежный контроль	***Тестирование***	***1***
5	Информационные системы в защищенном исполнении	*Лабораторная работа №6.* Инвентаризация с помощью сетевого сканера.	4
8	Защита распределенных информационных систем с доступом к глобальным сетям передачи информации	*Лабораторная работа №7.* Оценка соответствия требованиям стандарта.	4
		Лабораторная работа №8. Оценка соответствия требованиям стандарта.	2
	2-ой рубежный контроль	***Тестирование***	***1***
	Итого		**32**

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. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, 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 зачету с оценкой.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем разделов	**6**
Распределение информационных систем	0,5
Автоматизированные системы и их связь с ИБ распределенных ИС	1
Теоретические основы построения защищенных распределенных ИС	0,5
Коммуникация в распределенных ИС, проектирование системы защиты информации в распределенных ИС	1
Информационные системы в защищенном исполнении	0,5
Информационные системы в виде отдельных автоматизированных рабочих мест	0,5
Информационные системы как совокупность распределенных автоматизированных рабочих мест объединенных в локальные вычислительные сети	1
Защита распределенных ИС с доступом к глобальным сетям передачи информации	1
Подготовка к лабораторным работам (по 1 часу на каждое занятие)	16

Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету с оценкой	18
Всего:	**44**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ.

2.Отчеты обучающихся по лабораторным работам.

3. Банк тестовых заданий к рубежным контролям № 1, № 2.

4. Вопросы к зачету с оценкой

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение лабораторной работы	Рубежный контроль №1	Рубежный контроль №2	Зачет с оценкой
		Балльная оценка:	$1_б$ x16=$16_б$	$5_б$ x 8 = $40_б$	7	7	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично					

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета 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 зачета с оценкой 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 (зачету с оценкой) 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 состоят для 1 и 2 рубежных контролей из 10 вопросов. На каждое тестирование при рубежном контроле студенту отводится 1 академических часа.

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

Баллы обучающимся 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%.

Зачет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета с оценкой заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежных контролей и зачета

1-ый рубежный контроль

1. Распределенные информационные системы – это…

а) ...система нескольких автономных вычислительных узлов, взаимодействующих для выполнения общей цели.

б) … набор независимых компьютеров, представляющийся их пользователям единой объединенной системой.

в) …совокупность логически взаимосвязанных баз данных, распределённых в компьютерной сети.

2. Классификация распределенных информационных систем по архитектуре.

а) двухзвенные и многозвенные информационные системы.

б) файл-серверные и клиент-серверные информационные системы.

в) персональные, групповые и корпоративные информационные системы.

2-ой рубежный контроль

1. Аттестация объектов информатизации – это…

а) … комплекс организационно-технических мероприятий, в результате которых посредством специального документа – "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

б) … комплексная проверка (аттестационные испытания) объекта информатизации в реальных условиях эксплуатации.

в) … проверка уровня подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации.

2. Система обнаружения вторжений — это …

а) … система, которая отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за несколькими хостами.

б) … система (или агент), которая ведет наблюдение и анализ данных, передаваемых с использованием специфичных для определенных приложений протоколов.

в) … программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Понятие распределенных информационных систем.
2. Анализ угроз безопасности при обработке данных в распределенных ИС.
3. Цели и задачи построения распределенных ИС, их место в современном информационном обществе.
4. Классификация распределенных ИС, особенности работы
5. Автоматизированные системы и их связь с информационной безопасностью распределенных ИС.
6. Концепция обеспечения информационной безопасности распределенных ИС. Принципы построения системы защиты распределенной ИС.
7. Стандарты информационной безопасности распределенных систем.
8. Модель взаимодействия открытых систем OSI/ISO.
9. Рекомендации X.800 для распределенных систем.
10. Основное содержание оценочного стандарта ISO/IEC 15408.
11. Рекомендации НТД РФ по построению защищенных распределенных информационных систем.
12. Безопасность сетевых подключений распределенных ИС.
13. Сложные распределенные системы.
14. Централизованная и децентрализованная модель организации распределенных ИС.
15. Требования федеральных органов исполнительной власти по построению защищенных автоматизированных систем.
16. Требования ФСТЭК, ФСБ по созданию защищенных автоматизированных систем и локальных вычислительных сетей.
17. Аттестация объектов информатизации по требования по защите информации.
18. Сертификация средств технической и криптографической защиты информации.
19. Аттестация АРМ на соответствие требованиям по защите информации.

20. Высокочастотное облучение и высокочастотное навязывание.

21. Криптографические средства защиты информации при передачи между сегментами ЛВС.

22. Сертифицированные по требования на наличие НДВ операционные системы и базы данных.

23. Методы и средства защиты ИС с доступом к глобальной сети INTERNET.

24. Системы обнаружения вторжений.

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. Э.Таненбаум, М.ванСтеен. Распределенные системы. Принципы и парадигмы/Э.Таненбаум, М. ван Стеен. — СПб.:Питер, 2003. – 877 с.

2. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 2 - Средства защиты в сетях. - М.: Горячая линия-Телеком, 2008, - 558 с.

3. Соколов, А. В. Защита информации в распределенных корпоративных сетях и системах/ А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК, 2002. – 656 с.

4. Царегородцев, А. В. Информационная безопасность в распределенных управляющих системах: монография / А.В. Царегородцев. – М.: Издательство Российского университета дружбы народов, 2003. – 217 с. – ISBN 5-209-02204-8

7.2 Дополнительная учебная литература:

1. ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».

2. Миков А.И., Замятина Е.Б. Распределенные системы и алгоритмы // INTUIT, 2007.

7.3 Методическая литература

1. Методические указания к выполнению лабораторных работ по дисциплине «Информационная безопасность распределенных автоматизированных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. Курган, кафедра БИАС, 2017. –12 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
«Информационная безопасность распределенных информационных систем»

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

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 6 (очная форма обучения)
Форма промежуточной аттестации: зачет с оценкой
Содержание дисциплины. Основные разделы

Введение. Нефункциональные требования к распределенным информационным системам. Стандарты распределенных информационных систем. Аудит распределенных информационных систем. Безопасность в распределенных информационных системах.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины «Информационная безопасность распределенных информационных систем»

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

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Дик Д.И. /

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

Заведующий кафедрой _____ «___»_____20___ г.

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

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Дик Д.И. /

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

Заведующий кафедрой _____ «___»_____20___ г.