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

КАТАСТРОФОУСТОЙЧИВОСТЬ 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 «Катастрофоустойчивость информационных систем» составлена в соответствии с учебными планами 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:
ст. преподаватель В.В. Москвин

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
		10
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**70**	**70**
Лекции	30	30
Лабораторные работы	40	40
Самостоятельная работа, всего часов в том числе:	**38**	**38**
Подготовка к экзамену	27	27
Другие виды самостоятельной работы (подготовка к лабораторным работам и рубежному контролю)	11	11
Вид промежуточной аттестации	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Изучение дисциплины «Катастрофоустойчивость информационных систем» относится к части, формируемой участниками образовательных отношений Блока1, сформированных при изучении следующих дисциплин: «Безопасность жизнедеятельности», «Безопасность операционных систем», «Техническая защита информации», «Языки программирования», «Основы информационной безопасности», «Информационная безопасность открытых систем» и «Операционные системы и сети».

Дисциплина поможет разработать комплекс мер по реализации проектов катастрофоустойчивых информационных систем в выпускных квалификационных работах.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Дисциплина «Катастрофоустойчивость информационных систем» имеет *целью* подготовить обучающихся, способных осуществить защиту информационных ресурсов и систем при катастрофах, авариях, стихийных бедствиях и их последствиях.

Задачами дисциплины являются:

- изучение основ и методов поиска рациональных решений построения катастрофоустойчивых информационных систем;
- изучение основных подходов к обеспечению информационной безопасности катастрофоустойчивых информационных систем;
- изучение принципов функционирования современных средств построения и аппаратно-программных платформ построения информационных систем.

Компетенции, формируемые в результате освоения дисциплины:

- способность разрабатывать требования по защите информации, технические задания на создание систем защиты и руководящие документы по защите информации в открытых информационных системах (ПК-3);
- способность разрабатывать и анализировать проектные решения по обеспечению автоматизированных систем (ПК-5);
-способность обеспечивать работоспособность систем защиты информации открытых информационных систем при возникновении нештатных ситуаций (ПК-15);

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Катастрофоустойчивость информационных систем», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Катастрофоустойчивость информационных систем», индикаторы достижения компетенций ПК-3, ПК-5, ПК-15, 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$_{ПК-3}$	Знать: комплексный подход к построению катастрофоустойчивых информационных систем	З (ИД-1$_{ПК-3}$)	Знает: комплексный подход к построению катастрофоустойчивых информационных систем	Вопросы теста
2.	ИД-2 $_{ПК-3}$	Уметь: использовать современные методы и средства, разрабатывать и оценивать варианты построения катастрофоустойчивых ИС	У (ИД-2$_{ПК-3}$)	Умеет: использовать современные методы и средства, разрабатывать и оценивать варианты построения катастрофоустойчивых ИС	Комплект имитационных задач
3.	ИД-3 $_{ПК-3}$	Владеть: терминологией и системным подходом построения катастрофоустойчивых информационных систем	В (ИД-3$_{ПК-3}$)	Владеет: терминологией и системным подходом построения катастрофоустойчивых информационных систем	Вопросы для сдачи экзамена
4.	ИД-1$_{ПК-5}$	Знать: комплексный подход к построению катастрофоустойчивых информационных систем	З (ИД-1$_{ПК-5}$)	Знает: комплексный подход к построению катастрофоустойчивых информационных систем	Вопросы теста
5.	ИД-2 $_{ПК-5}$	Уметь: использовать современные методы и средства, разрабатывать и оценивать варианты построения катастрофоустойчивых ИС	У (ИД-2$_{ПК-5}$)	Умеет: использовать современные методы и средства, разрабатывать и оценивать варианты построения катастрофоустойчивых ИС	Комплект имитационных задач
6.	ИД-3 $_{ПК-5}$	Владеть: навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых информационных систем	В (ИД-3$_{ПК-5}$)	Владеет: навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых информационных систем	Вопросы для сдачи экзамена
7.	ИД-1$_{ПК-15}$	Знать: методы и средства реализации катастрофоустойчивых информационных систем	З (ИД-1$_{ПК-15}$)	Знает: методы и средства реализации катастрофоустойчивых информационных систем	Вопросы теста
8.	ИД-2 $_{ПК-15}$	Уметь: использовать методы обеспечения	У (ИД-2$_{ПК-15}$)	Умеет: использовать методы обес-	Комплект имитационных задач

		катастрофоустойчивости ИС		печения катастрофоустойчивости ИС	
9.	ИД-3 $_{ПК-15}$	Владеть: терминологией и системным подходом построения катастрофоустойчивых информационных систем	В (ИД-3 $_{ПК-15}$)	Владеет: терминологией и системным подходом построения катастрофоустойчивых информационных 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	Лабораторные работы
Рубеж 1	*Тема 1.*	Национальные интересы и угрозы катастрофоустойчивости РФ в информационной сфере и их обеспечение	2	4
	Тема 2	Основные понятия катастрофоустойчивости информационной системы	2	6
	Тема 3	Модели и показатели функционирования катастрофоустойчивых ИС	2	-
	Тема 4	Методы обеспечения катастрофоустойчивости ИС	2	10
	Тема 5	Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф	2	8
	Тема 6	Оптимизация средств восстановления после отказов	2	-
Рубежный		*контроль №1*	-	2
Рубеж 2	*Тема 7*	Практические решения построения средств восстановления после катастроф	4	-
	Тема 8	Основы обеспечения информационной безопасности в катастрофоустойчивых центрах обработки информации (КЦОИ)	2	-
	Тема 9	Принципы построения организационно-режимных мер обеспечения безопасности информации	4	-
	Тема 10	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со	4	4

		стороны обслуживающего персонала к ресурсам ИС в особых режимах её функционирования		
	Тема 11	Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации	4	4
Рубежный контроль №2			-	2
Всего:			**30**	**40**

4.2. Содержание лекционных занятий

Тема 1. Национальные интересы и угрозы катастрофоустойчивости РФ в информационной сфере и их обеспечение.

Фундаментальное право на информацию. Федеральный закон «Об информации, информационных технологиях и о защите информации». Концепция национальной безопасности РФ. Доктрина информационной безопасности РФ. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Основные цели и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ.

Тема 2. Основные понятия катастрофоустойчивости информационной системы (ИС)

Понятия катастрофоустойчивости, живучести и отказоустойчивости. Информационные системы. Виды, архитектура, субъекты и объекты взаимодействия. Модель катастрофических воздействий. Моделирование и прогноз природных и техногенных катастроф. Уровни катастрофоустойчивости. Показатели и критерии функционирования катастрофоустойчивой информационной системы. Живучесть информационных систем. Отказоустойчивость и надежность. Разработка моделей оценки живучести ИС.

Тема 3. Модели и показатели функционирования катастрофоустойчивых ИС

Модель оценки информационной системы с позиции доступности. Модель оценки информационной системы по уровням катастрофоустойчивости. Модель оценки информационной системы с позиции живучести. Оценка эффективности катастрофоустойчивых решений. Структурный анализ катастрофоустойчивой ИС.

Тема 4. Методы обеспечения катастрофоустойчивости ИС.

Методика создания катастрофоустойчивой информационной системы. Классификация методов обеспечения катастрофоустойчивости. Стратегии резервирования. Кластеризация. Избыточные структуры. Резервные центры обработки данных. Выбор варианта катастрофоустойчивой конструкции центра обработки информации. Выбор стратегии восстановления в катастрофоустойчивой системе. Разработка модели оценки доступности информации в катастрофоустойчивых системах. Исследование готовности и доступности ИС. Исследование уровней катастрофойстойчивости на моделях

типовых ИС. Моделирование дестабилизирующих воздействий и их последствий на ИС. Разработка модели оценки катастрофоустойчивых решений.

Тема 5. Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф.

Постановка задачи. Вводные положения. Непротиворечивость базы данных (БД) приложения катастрофоустойчивого центра обработки информации информационно-телекоммуникационной системы (КЦОИ ИТС). Три состояния целостности БД. Нарушение непротиворечивости БД. Средства блокировки доступа. Четыре степени непротиворечивости БД по отношению к заданной транзакции. Неисправности и отказы. Четыре способа реализации обновления данных базы данных.

Тема 6. Оптимизация средств восстановления после отказов.

Постановка задачи. Классификация отказов в зависимости от логики восстановления приложения после возникновения таких отказов. Действия и процедуры восстановления после отказов. Примеры действий для обеспечения фиксации точек синхронизации целостности. Построение математической модели восстановления. Совместная оптимизация циклов восстановления по критерию максимальной пропускной способности системы.

Тема 7. Практические решения построения средств восстановления после катастроф.

Предварительные замечания. Требуемая доступность для разных уровней обработки информации в электронной платежной системе Банка России. Уровни катастрофоустойчивости. Соотношение стоимости обеспечения уровней катастрофоустойчивости и времени восстановления функционирования системы. Расчет ожидаемого времени восстановления для различных уровней катастрофоустойчивости. Зависимость затрат на реализацию катастрофоустойчивости от времени восстановления КЦОИ. Выбор уровня катастрофоустойчивости в зависимости от стоимости единицы времени простоя.

Тема 8. Основы обеспечения информационной безопасности в катастрофоустойчивых центрах обработки информации.

Особенности обеспечения информационной безопасности в КЦОИ. Основные принципы построения системы информационной безопасности КЦОИ. Подход к построению модели нарушителя в ИТС. Защита от угроз со стороны обслуживающего персонала в катастрофоустойчивом ЦОИ**.**

Тема 9. Принципы построения организационно-режимных мер обеспечения безопасности информации

Система документации. Формирование организационной структуры обеспечения информационной безопасности КЦОИ. Разработка технологических процедур и порядка обеспечения информационной безопасности при их выполнении на КЦОИ. Определение порядка назначения прав и полномочий по доступу к ресурсам КЦОИ. Разработка процедуры контроля достаточности и работоспособности системы информационной безопасности КЦОИ.

Тема 10. Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам ИС в особых режимах её функционирования

Общие положения. Решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам КЦОИ при изменении режима его работы. Шесть компонентов системы разграничения доступа, функционирующей на обоих вычислительных комплексах КЦОИ. Пять режимов работы/взаимодействия вычислительных установок основной (1-я) и резервной (2-я) площадок. Сопровождение прикладных программных комплексов в составе КЦОИ.

Тема 11. Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации

Состав и последовательность проведения мероприятий и выполнения работ при переносе управления обработки. Условия их проведения. Основные группы мероприятий, проводимых заблаговременно и в процессе переноса обработки. Перечень функциональных групп, обеспечивающих перенос обработки. Типовые роли основных участников переноса обработки. Состав функциональных групп, участвующих в процессе переноса управления обработки. Основные задачи, решаемые участниками, и проводимые ими мероприятия по переносу обработки. Условия их проведения.

4.3 Лабораторные занятия

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
1	Национальные интересы и угрозы катастрофоустойчивости РФ в информационной сфере и их обеспечение.	*Лабораторная работа №1* Понятие национальной безопасности. Виды защищаемой информации	4
2	Основные понятия катастрофоустойчивости информационной системы	*Лабораторная работа №2* Расчет показателей доступности информационно-телекоммуникацион-ных систем	6
4	Методы обеспечения катастрофоустойчивости ИС	*Лабораторная работа №3* Разработка *м*етодов обеспечения катастрофоустойчивости	10
5	Выбор рациональных решений по организации средств восстановления информационных систем после отказов и катастроф	*Лабораторная работа №4* Средства обеспечения катастрофоустойчивости	4
		Лабораторная работа №5 Разработка технического задания на катастрофоустойчивые системы	4
	1-ый рубежный контроль	***Тестирование***	***2***
10	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны	*Лабораторная работа №6* Организация работ по развертыванию катастрофоустойчивых решений	4

	обслуживающего персонала к ресурсам ИС в особых режимах её функционирования		
11	Типовой сценарий переноса обработки в случае частичного или полного выхода из строя центра обработки информации	*Лабораторная работа №7* Планы восстановления после катастроф	4
	2-ой рубежный контроль	***Тестирование***	***2***
	Итого		**40**

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 разбор 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 самостоятельное изучение разделов дисциплины, 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.
Подготовка к лабораторным работам (по 1 часу на каждую работу)	7
Подготовка к рубежным контролям (по 2 часа на каждый контроль)	4
Подготовка к экзамену	27
Всего:	**38**

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 по лабораторным 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, 10 семестр***					
		Вид учебной работы:	Посещение лекций	Выполнение и защита лабораторной работы	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	$1_б$ х 15=$15_б$	$6_б$ х 7 = $42_б$	6	7	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; незачет; 61…73 – удовлетворительно; зачет; 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 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 письменных ответов на контрольные вопросы. Перед проведением рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. На рубежный контроль 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 рубежных контролей каждого обучающегося и заносит в ведомость учета текущей успеваемости.

Экзамен проводится в традиционной форме, по билетам. Билет состоит из 2 вопросов. Вопросы к экзамену доводятся до обучающихся на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа обучающемуся отводится 1 астрономический час.

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. Источники угроз безопасности информации могут быть:

1. Антропогенными
2. Техногенными
3. Стихийными
4. Все вышеперечисленные

2. Что позволяет выявить аудит информационной безопасности?

1. Оценить текущую безопасность функционирования корпоративной информационной системы
2. Оценить и спрогнозировать риски, а также управлять их влиянием на бизнес-процессы компании
3. Корректно и обосновано подойти у вопросу обеспечения безопасности информационных активов компании
4. Все вышеперечисленное

3. Что характерно для низкого уровня политики информационной безопасности?

1. Политика информационной безопасности служит для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности
2. Политика информационной безопасности определяет отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации
3. Политика информационной безопасности относится к отдельным элементам информационных систем и участкам обработки и хранения информации и описывает конкретные процедуры и документы, связанные с обеспечением информационной безопасности.

4. Политика информационной безопасности является средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.

Примерные тестовые задания для рубежного контроля №2

1. Какой из перечисленных видов нарушителей имеет наибольший потенциал?

1. Конкурирующие организации
2. Специальные службы иностранных государств
3. Лица, обеспечивающие функционирование информационных систем
4. Экстремистские группировки

2. Защита беспроводных соединений, применяемых в информационной системе, необходимы для информационных систем:

1. 1 Класса защищенности информационной системы
2. 2 Класса защищенности информационной системы
3. 3 Класса защищенности информационной системы
4. Всех классов защищенности

3. Исходя из каких критериев происходит категорирование объектов критической информационной инфраструктуры?

1. Социальная значимость
2. Политическая значимость
3. Экономическая значимость
4. Все вышеперечисленные

Примерный перечень вопросов к экзамену

1. Классификация угроз, приводящих к катастрофам в информационных системах
2. Классификация информационных систем
3. Модель информационной системы
4. Методы обеспечения катастрофоустойчивости
5. Характеристика уровней катастрофоустойчивости
6. Кластеризация информационных систем и вопросы их катастрофоустойчивости
7. Организационные меры по обеспечению катастрофоустойчивости
8. Живучесть информационных систем
9. Технологии отказоустойчивости
10. Показатели катастрофоустойчивости
11. Количественные оценки катастрофоустойчивых решений
12. Выбор варианта катастрофоустойчивой конструкции центра обработки информации
13. Модель оценки информационной системы с позиции доступности
14. Модель оценки информационной системы по уровням катастрофоустойчивости
15. Модель оценки информационной системы с позиции живучести
16. Оценка эффективности катастрофоустойчивых решений

17. Структурный анализ катастрофоустойчивой информационной систем
18. Три состояния целостности БД. Нарушение непротиворечивости БД.
19. Средства блокировки доступа.
20. Четыре способа реализации обновления данных базы данных.
21. Классификация отказов в зависимости от логики восстановления приложения после возникновения таких отказов.
22. Действия и процедуры восстановления после отказов.
23. Построение математической модели восстановления.
24. Уровни катастрофоустойчивости. Соотношение стоимости обеспечения уровней катастрофоустойчивости и времени восстановления функционирования системы.
25. Расчет ожидаемого времени восстановления для различных уровней катастрофоустойчивости.
26. Выбор уровня катастрофоустойчивости в зависимости от стоимости единицы времени простоя.
27. Основные принципы построения системы информационной безопасности КЦОИ.
28. Защита от угроз со стороны обслуживающего персонала в катастрофоустойчивом ЦОИ.
29. Система документации. Формирование организационной структуры обеспечения информационной безопасности КЦОИ.
30. Разработка технологических процедур и порядка обеспечения информационной безопасности при их выполнении на КЦОИ.
31. Определение порядка назначения прав и полномочий по доступу к ресурсам КЦОИ.
32. Разработка процедуры контроля достаточности и работоспособности системы информационной безопасности КЦОИ.
33. Решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам КЦОИ при изменении режима его работы.
34. Шесть компонентов системы разграничения доступа, функционирующей на обоих вычислительных комплексах КЦОИ. Пять режимов работы/взаимодействия вычислительных установок основной (1-я) и резервной (2-я) площадок.
35. Сопровождение прикладных программных комплексов в составе КЦОИ.
36. Состав и последовательность проведения мероприятий и выполнения работ при переносе управления обработки. Условия их проведения.
37. Основные группы мероприятий, проводимых заблаговременно и в процессе переноса обработки.
38. Перечень функциональных групп, обеспечивающих перенос обработки.
39. Типовые роли основных участников переноса обработки.
40. Состав функциональных групп, участвующих в процессе переноса управления обработки.

41. Основные задачи, решаемые участниками, и проводимые ими мероприятия по переносу обработки. Условия их проведения.

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. Трахгенгерц Э.А. Компьютерные методы подготовки к противодействию группе прогнозируемых катастроф. [Электронный ресурс]. В 2-х томах. Том 1. Методы и средства. - М.: СИНТЕГ, 2009, - 172 с. Том 2. Реализация решений. - М.: СИНТЕГ, 2009, - 224 с. URL: http://producm.ru/upload/books/11.pdf .

2. Безопасность жизнедеятельности: учебник для студ. высш. учеб. заведений / [Л.А. Михайлов, В.М. Губанов, В.П. Соломин и др.]; под ред. Л.А. Михайлова. - 2-е изд., стер. - М.: Издательский центр «Академия», 2009. – 272 с.

7.2 Дополнительная учебная литература

1. Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том I – Угрозы, уязвимости, атаки и подходы к защите [Электронный ресурс]: С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Горячая линия–Телеком, 2006. URL: https://www.twirpx.com/file/975534/ .

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

1. ЭБС htt://www.znanium.com/
2. ЭБС htt://www.studentlibrary.ru
3. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
4. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
5. http://elibrary.ru/. Научная электронная библиотека
6. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

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

КАТАСТРОФОУСТОЙЧИВОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специальность: (специализация №5)

Безопасность открытых информационных систем

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 10 (очная форма обучения)
Форма промежуточной аттестации: экзамен

Содержание дисциплины. Основные разделы.

Катастрофоустойчивость в системе национальной безопасности РФ. Методы обеспечения катастрофоустойчивости автоматизированных систем. Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем. Организация функционирования катастрофоустойчивых автоматизированных систем.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу
учебной дисциплины
«КАТАСТРОФОУСТОЙЧИВОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

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

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Москвин В.В. /

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

Заведующий кафедрой _____ «___»_____20___ г.

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

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Москвин В.В. /

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

Заведующий кафедрой _____ «___»_____20___ г.