МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

УТВЕРЖДАЮ

Проректор по учебной работе

_____ Зарипов Н.Г.

«02» 09 2015 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

«КАТАСТРОФОУСТОЙЧИВОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Направление подготовки кадров высшей квалификации

10.06.01 Информационная безопасность

Программа

Методы и системы защиты информации, информационная безопасность

Квалификация выпускника

Исследователь. Преподаватель-исследователь

Форма обучения – очная

Уфа 2015

Содержание

1. Место дисциплины в структуре образовательной программы

Дисциплина «Катастрофоустойчивость информационных систем» является дисциплиной по выбору вариативной части.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки научно-педагогических кадров высшей квалификации (аспирантура) 10.06.01 «Методы и системы защиты информации, информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации от "30" июля 2014 г. № 874 и приказа Министерства образования и науки Российской Федерации от 30.04.2015 N 464 "О внесении изменений в федеральные государственные образовательные стандарты высшего образования (уровень подготовки кадров высшей квалификации)". Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины является подготовка научно-педагогических кадров высшей квалификации, способных решать совокупность задач, связанных с обеспечением защищённости объектов различного уровня информатизации и производственного персонала в условиях воздействия дестабилизирующих факторов среды, приводящих к возникновению катастроф, аварий, стихийных бедствиях, и их последствиях.

Задачи:

- сформировать знания об основных концепциях катастрофоустойчивости информационной системы;
- сформировать знания об основных методах и технологиях создания катастрофоустойчивых систем на различных этапах жизненного цикла;
- сформировать знания основополагающих принципов оценки катастрофоустойчивости системы и математических методов, используемых при оценке катастрофоустойчивости информационных систем;
- сформировать знания о принципах и стратегии выбора наиболее эффективных катастрофоустойчивых решений;
- приобрести навыки применения методов повышения отказоустойчивости и катастрофоустойчивости информационных систем;
- сформировать знания об основных нормативно-правовых актах в области построения катастрофоустойчивой информационной системы.

Дисциплина является самостоятельным элементом в системе подготовки научно-педагогических кадров высшей квалификации. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- Методы и системы защиты информации, информационная безопасность.

В дисциплине «Катастрофоустойчивость информационных систем» определяются теоретические основы и практические навыки, при освоении которых аспирант способен приступить к прохождению научно-исследовательской практики и выполнять научные исследования в соответствующей предметной области.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность.	ОПК-1	Базовый	Предыдущие этапы получения высшего образования
2	Способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	ОПК-2	Базовый	Предыдущие этапы получения высшего образования
3	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.	ОПК-3	Пороговый	Методы и системы защиты информации, информационная безопасность

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность.	ОПК-1	Повышенный	Научные исследования
2	Способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	ОПК-2	Повышенный	Научные исследования

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	ОПК-1	Цели исследования, основные методологические подходы исследования процессов обеспечения информационной безопасности	Использовать методологии и методы научного исследования на уровнях теоретического познания и эмпирического исследования	Системными правилами выявления причин нарушения системных принципов функционирования объектов в области обеспечения информационной безопасности.
2	Способность разрабатывать частные методы ис-	ОПК-2	научные основы развития теории и создания,	синтезировать усовершенствованные решения в самостоя-	навыком оценки состояния развития перспективного

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
	следования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;		перспективных объектов профессиональной деятельности	тельной научно-исследовательской деятельности с использованием современных информационно-коммуникационных технологий	научного направления по имеющейся информации; формализации знаний

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 7 зачетных единиц (252 часа).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.	
	3 семестр	4 семестр
Лекции (Л)	6	4
Практические занятия (ПЗ)	8	6
Самостоятельная работа	76	62
Подготовка и сдача экзамена	-	36
Подготовка и сдача зачета	9	-
Вид итогового контроля (зачет, экзамен)	зачет с оценкой	экзамен

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая аспирантам	Виды интерактивных образовательных технологий
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	Основные понятия катастрофоустойчивости информационной системы (ИС) 1. Понятия катастрофоустойчивости, живучести и отказоустойчивости 2. Информационные системы. 3. Виды, архитектура, субъекты и объекты взаимодействия. 4. Модель катастрофических воздействий 5. Моделирование и прогноз природных и техногенных катастроф. 6. Уровни катастрофоустойчивости 7. Показатели и критерии функционирования катастрофоустойчивой информационной системы. 8. Живучесть информационных систем 9. Отказоустойчивость и надежность. 10. Разработка моделей оценки живучести ИС	2	4			61	67	Р 6.1 №1, ч. 1 Р 6.1 №2, гл. 1-3 Р 6.1 №3, Р.1 Р 6.2 №1, ч. 2 Р 6.2 №2, Домен 5 Р 6.2 №3 Р 6.2 №4	При проведении лекционных занятий: – лекция классическая; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
2	Модели и показатели функционирования катастрофоустойчивых ИС 1. Модель оценки информационной системы с позиции доступности 2. Модель оценки информационной системы по уровням катастрофоустойчивости 3. Модель оценки информационной системы с позиции живучести 4. Оценка эффективности катастрофоустойчивых решений 5. Структурный анализ катастрофоустойчивой ИС	4	4			61	69	Р 6.1 №2, гл. 4-6 Р 6.2 №1, ч. 3 Р 6.2 №2, Домен 5 Р 6.2 №3 Р 6.2 №4	При проведении лекционных занятий: – лекция классическая; лекция-визуализация; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.

3	Методы обеспечения катастрофоустойчивости ИС 1. Методика создания катастрофоустойчивой информационной системы 2. Классификация методов обеспечения катастрофоустойчивости 3. Стратегии резервирования 4. Кластеризация 5. Избыточные структуры 6. Резервные центры обработки данных. 7. Выбор варианта катастрофоустойчивой конструкции центра обработки информации 8. Выбор стратегии восстановления в катастрофоустойчивой системе 9. Разработка модели оценки доступности информации в катастрофоустойчивых системах 10. Исследование готовности и доступности ИС 11. Исследование уровней катастрофойстойчивости на моделях типовых ИС 12. Моделирование дестабилизирующих воздействий и их последствий на ИС 13. Разработка модели оценки катастрофоустойчивых решений	4	6			61	71	Р 6.2 №2 Р 6.2 №3 Р 6.2 №4	При проведении лекционных занятий: – лекция классическая; лекция-визуализация; При проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
	Всего	10	14			183	207		

Занятия, проводимые в интерактивной форме, составляют 25 % от общего количества аудиторных часов по дисциплине «Катастрофоустойчивость информационных систем».

Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
1	1	1. Основные системотехнические принципы построения информационно-телекоммуникационной системы (ИТС). 1. Проблемы традиционного системотехнического подхода к реализации ИТС. 2. Подходы к созданию системы территориально-распределенной обработки информации (СТРОИ) на основе центров обработки информации коллективного пользования (ЦОИ КП).	2
2	1	1. Активное резервирование и режимы функционирования ЦОИ КП в составе катастрофоустойчивой СТРОИ.	2
3	2	1. Выбор рациональных решений по организации средств восстановления ЦОИ ИТС после отказов и катастроф. 2. Принципы построения организационно–режимных мер обеспечения безопасности информации в ЦОИ КП.	2
4	2	1. Требования к системно-техническим решениям по обеспечению комплексной защиты информации в ЦОИ КП. 2. Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам ЦОИ КП в особых режимах его функционирования.	2
5	3	1. Пример системотехнического решения по регламенту перехода с основной площадки ЦОИ КП на резервную площадку ЦОИ КП.	2
6	3	1. Организационный регламент перехода с основной площадки ЦОИ КП на резервную площадку ЦОИ КП.	2
7	3	1. Типовой сценарий переноса обработки в случае частичного или полного выхода из строя КЦОИ КП.	2

4. Учебно-методическое обеспечение самостоятельной работы аспирантов

Тема 1. Катастрофоустойчивость банковских систем

- Повышение готовности банковских систем.
- Удаленный резервный вычислительный центр автоматизированной банковской системы и процессинговой системы банка.
- План обеспечения непрерывной работы и восстановления работоспособности в кризисных ситуациях.

Тема 2. Резервные центры обработки данных

- Сертификация на уровень отказоустойчивости (Tier III Facility, Tier III Design).
- «Холодная» организации резервного центра обработки данных
- «Горячая» организации резервного центра обработки данных
- «Зеркальная» организации резервного центра обработки данных

Тема 3. Стратегии восстановления и резервирования в системах высокой доступности

- Локальная непрерывная репликация.
- Кластер с непрерывной репликацией.
- Кластеры единой копии.

Тема 4. Программно-аппаратная избыточность в информационных системах

- Международные стандарты, направленные на обеспечение технологической безопасности

Тема 5. Виртуализация как часть стратегии обеспечения непрерывность деятельности

- Документирование планов обеспечения непрерывности деятельности организации и восстановления после аварий.
- Паравиртуализация.
- Полная (аппаратная) виртуализация.
- Виртуализация уровня операционной системы.

5. Фонд оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Уровень освоения, определяемый этапом формирования компетенции	Наименование оценочного средства*
1	Основные понятия катастрофоустойчивости информационной системы (ИС)	ОПК-1	Повышенный уровень	Р
2	Модели и показатели функционирования катастрофоустойчивых ИС	ОПК-2	Повышенный уровень	КА, Т
3	Методы обеспечения катастрофоустойчивости ИС			

Вопросы к зачету с оценкой и 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 системы

Критерии оценки:

- оценка «отлично» выставляется, если дан полный, развернутый ответ, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий.
- оценка «хорошо» выставляется, если раскрыт теоретический вопрос, однако допущены неточности в определении основных понятий. При этом неполно освящены второстепенные детали, однако в полной мере освоены методы формального описания моделей оценки катастрофоустойчивости ИС, методы оценки эффективности катастрофоустойчивых решений.
- оценка «удовлетворительно» ставится, если при ответе на теоретические вопросы допущено несколько существенных ошибок в толковании основных понятий. Заметны пробелы в знании основных методов и формальных моделей. Задача не решена до конца или при решении допущены грубые ошибки.
- оценка «неудовлетворительно» ответ на вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий.

Типовые оценочные материалы

Раздел дисциплины «Катастрофоустойчивость информационных систем»

1. Кейс-задача

Раздел дисциплины «Модели и показатели функционирования катастрофоустойчивых ИС»

Задание:

1. Разработайте сценарий деградации информационной системы с использование теории графов

2. Кейс-задача

Раздел дисциплины «Модели и показатели функционирования катастрофоустойчивых ИС»

Задание:

1. Разработайте модель дестабилизирующих факторов для автоматизированной банковской системы

3. Кейс-задача

Раздел дисциплины «Методы обеспечения катастрофоустойчивости ИС»

Задание:

1. Разработайте план мероприятий по поддержанию непрерывности деятельности для автоматизированных систем управления технологическими процессами.

Кейс – это пакет заданий, индивидуальных или групповых, которые очерчивают реальную проблему, не имеющую единственного и очевидного решения. Для поисков оригинального выхода аспирант должен проанализировать проблемную ситуацию, используя знания по изучаемой дисциплине, предложить решения и обосновать выбор именно этих вариантов. Применение кейс-метода позволяет развивать навыки работы с разнообразными источниками информации, а также компетентностные качества личности (аналитические, практические, творческие, коммуникативные, социальные умения).

Методика выполнения кейс-задания включает в себя следующие этапы: индивидуальная самостоятельная работа аспирантов с материалами кейса (идентификация проблемы, формулировка ключевых альтернатив, предложение решения или рекомендуемого действия); работа в малых группах по согласованию видения ключевой проблемы и ее решений; презентация и проверка результатов малых групп на общей дискуссии.

Критерии оценки:

- оценка «отлично» выставляется, если дан полный, развернутый ответ, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий.
- оценка «хорошо» выставляется, если раскрыт теоретический вопрос, однако допущены неточности в определении основных понятий. При этом неполно освящены второстепенные детали, однако в полной мере освоены методы формального описания моделей оценки катастрофоустойчивости ИС, методы оценки эффективности катастрофоустойчивых решений.
- оценка «удовлетворительно» ставится, если при ответе на теоретические вопросы допущено несколько существенных ошибок в толковании основных понятий. Заметны пробелы в знании основных методов и формальных моделей. Задача не решена до конца или при решении допущены грубые ошибки.
- оценка «неудовлетворительно» ответ на вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий.

4. Комплект заданий для контрольной работы

Раздел (тема) дисциплины «Методы обеспечения катастрофоустойчивости ИС»

1. Какие процедуры должны быть выполнены для восстановления систем и данных после системного сбоя?
A. Восстановление с резервных копий
B. Проведение параллельного тестирования
C. Выполнение процедур восстановления
D. Выполнение сквозного тестирования

2. Что является одним из первых шагов при разработке плана обеспечения непрерывности бизнеса?
A. Определение имеющихся средств резервного копирования
B. Принятие решения, нужно ли компании выполнять сквозное, параллельное тестирование или моделирование
C. Проведение анализа воздействия на бизнес (BIA)
D. Разработка плана возобновления бизнеса

3. Насколько часто следует тестировать план обеспечения непрерывности бизнеса?
A. Не реже одного раза в десять лет
B. Только после изменений инфраструктуры или окружения
C. Не реже одного раза в два года
D. Когда в компании происходят существенные изменения

4. Одним из важных шагов в процессе тестирования процедур восстановления является ведение записей обо всех существенных шагах и произошедших событиях. Что из перечисленного ниже является не менее важным?
A. Спланировать следующее тестирование, при котором будут учтены возникшие проблемы
B. Убедиться, что назначен человек, который готов ответить на вопросы прессы
C. Подготовить отчет для руководства об этих шагах и событиях
D. Определить наиболее важные бизнес-функции

5. Что из перечисленного ниже является наименее важным при проведении оценки рисков, связанных с потенциальными чрезвычайными ситуациями?
A. Сбор информации из отчетов специальных агентств, которые позволяют оценить вероятность природных катаклизмов в определенной местности
B. Идентификация ключевых функций компании и требований бизнеса

C. Идентификация критичных систем, обеспечивающих работу компании
D. Оценка потенциальных потерь и негативного воздействия на компанию в зависимости от продолжительности простоя

6. Действия, выполняемые сразу после возникновения чрезвычайной ситуации, должны быть направлены на предотвращение человеческих жертв и вреда здоровью людей, а также на
B. Минимизацию дальнейших повреждений
C. Защиту доказательств и улик
D. Оценку масштабов повреждений

7. Что из перечисленного ниже является наилучшим способом обеспечения гарантированной возможности восстановления данных с резервных лент и их использования на «теплой» площадке?
A. Взять ленты с внешней площадки и проверить их работу на оборудовании основной площадки
B. Попросить поставщика внешней площадки протестировать их и пометить те, которые прочитались
C. Протестировать их на системе поставщика, которую не планируется использовать в случае аварии
D. Дважды в месяц составлять опись лент, хранящихся на площадке поставщика

8. Что из перечисленного ниже лучше всего описывает отличия «горячей» площадки от «теплой» или «холодной»?
A. Это площадка, на которой установлены жесткие диски, контроллеры и ленточные приводы
B. Это площадка, на которой установлены все необходимые компьютеры, серверы и телекоммуникационные системы
C. Это площадка, на которой проложена электрическая проводка, установлена централизованная система вентиляции воздуха и фальшполы
D. Это мобильная площадка, которая может стоять на парковке возле здания компании

9. Что из перечисленного ниже лучше всего описывает создание удаленных журналов (remote journaling)?
A. Резервное копирование больших объемов данных на внешнюю площадку
B. Резервное копирование журнала транзакций на удаленную площадку
C. Одновременная запись транзакций на два зеркальных сервера, установленных на основной площадке
D. Сохранение транзакций на носителе информации другого типа

10. Что из перечисленного ниже требуется для внешней площадки, на которой хранятся носители информации с резервными копиями данных компании?
A. Площадка должна находиться в 10-15 минутах езды от основной площадки, чтобы резервные копии были легкодоступны
B. На площадке должны быть установлены все необходимые компьютеры и серверы, смонтирован фальшпол
C. Площадка должна охраняться вооруженной охраной
D. Площадка должна быть защищена от несанкционированного доступа

11. Что из перечисленного ниже не может быть выявлено при проведении анализа воздействия на бизнес (BIA)?
A. Подходит ли компании параллельное тестирование или тестирование с полным прерыванием
B. Какая область может наиболее пострадать с функциональной и финансовой точки зрения в при аварии или чрезвычайной ситуации
C. Какие системы наиболее критичны для компании и должны быть максимально защищены
D. Какая продолжительность простоя приемлема для компании и не окажет катастрофического воздействия на ее бизнес

12. Для каких областей компании рекомендуется подготовка плана действий в непредвиденных ситуациях?
A. Наиболее важных функциональных и финансовых областей
B. Областей, в которых находятся критичные системы
C. Всех областей
D. Областей, без которых компания не сможет «выжить»

13. Кто утверждает план обеспечения непрерывности бизнеса?
A. Комитет по планированию
B. Руководитель каждого подразделения
C. Руководство
D. Внешнее лицо

14. В каком из перечисленных ниже пунктов приведена правильная последовательность шагов разработки плана непрерывности бизнеса?
A. Инициирование проекта, разработка стратегии, проведение анализа воздействия на бизнес, разработка плана, внедрение, тестирование и поддержка плана
B. Разработка стратегии, инициирование проекта, проведение анализа воздействия на бизнес, разработка плана, внедрение, тестирование и поддержка плана
C. Внедрение и тестирование, инициирование проекта, разработка стратегии, проведение анализа воздействия на бизнес, разработка плана
D. Разработка плана, инициирование проекта, разработка стратегии, проведение анализа воздействия на бизнес, внедрение, тестирование и поддержка плана

15. Что является самым важным при разработке плана обеспечения непрерывности бизнеса?
A. Анализ воздействия на бизнес
B. Внедрение, тестирование и дальнейшее следование плану
C. Участие всех и каждого подразделений компании
D. Поддержка руководства

16. В процессе разработки, тестирования и поддержки плана обеспечения непрерывности бизнеса крайне важно обеспечить надлежащее взаимодействие и коммуникации. Почему?
A. Это является одним из требований регуляторов к этому процессу
B. Чем больше людей говорят об этом плане и участвуют в его создании, тем выше уровень осведомленности о нем
C. Это не важно для разработки плана, тем более что такое взаимодействие будет отрывать людей от важной работы и может нанести ущерб производительности работы компании
D. Руководство вероятно поддержит это

17. Чтобы получить реальную поддержку руководства и одобрение плана, требуется реальная потребность в этом бизнеса компании. Что из перечисленного ниже является наименее важным для возникновения такой потребности?
A. Требования законодательства и регуляторов
B. Уязвимость компании к авариям и чрезвычайным ситуациям
C. Как другие компании решают эти вопросы
D. Максимальное воздействие, которое может выдержать компания в случае возникновения чрезвычайной ситуации

18. Что из перечисленного ниже описывает параллельное тестирование?
A. Оно проводится, чтобы убедиться, что определенные системы могут работать на альтернативной площадке
B. Все подразделения получают копию плана восстановления после аварий и «проходят» по нему

C. Представители от каждого подразделения собираются вместе и совместно проводят это тестирование
D. Выполнение операций в обычном режиме прекращается

19. Что из перечисленного ниже описывает структурированное сквозное тестирование?
A. Оно проводится, чтобы убедиться, что критичные системы могут работать на альтернативной площадке
B. Все подразделения получают копию плана восстановления после аварий и «проходят» по нему
C. Представители от каждого подразделения собираются вместе и совместно проводят это тестирование
D. Выполнение операций в обычном режиме прекращается

20. Когда компания может считать, что чрезвычайная ситуация закончилась?
A. Когда люди пересчитаны и находятся в безопасности
B. Когда выполнение всех операций и весь персонал возвращены на основную площадку
C. Когда выполнение операций перенесено на альтернативную внешнюю площадку
D. Когда официальные лица объявили об этом

21. Что из перечисленного ниже не имеет отношения к соглашению о взаимной помощи (reciprocal agreement)?
A. Соглашение имеет юридическую силу
B. Это дешевое решение
C. Оно может быть использовано сразу после аварии
D. Может оказаться очень сложным реализовать это на площадке, на которой уже обрабатываются данные другой компании

22. Что из перечисленного ниже является описанием «холодной» площадки?
A. Она полностью оборудована и готова к работе компании на ней уже через несколько часов
B. Она частично оборудована средствами обработки данных
C. Она полностью настроена, но это дорогое решение
D. На ней обеспечены только самые необходимые возможности, оборудования на ней нет

23. В каком из приведенных ниже пунктов наиболее полно перечислены компоненты плана восстановления после аварий?
A. Оборудование, программное обеспечение, люди, аварийные процедуры, процедуры восстановления
B. Люди, оборудование, внешняя альтернативная площадка
C. Программное обеспечение, взаимодействие устройств, люди, оборудование, вопросы, связанные с руководством
D. Оборудование, аварийные процедуры, программное обеспечение, идентифицированные риски

24. Что из перечисленного ниже не является преимуществом «горячей» площадки?
A. Предлагает широкий выбор оборудования и программного обеспечения
B. Постоянно доступна
C. Может быть запущена в работу всего за несколько часов
D. Возможно проведение ежегодного тестирования

25. Планы восстановления после аварий могут поддерживаться в актуальном состоянии при выполнении ряда условий. Что из перечисленного ниже не является таким условием?
A. Сделать восстановление после аварий частью любого бизнес-решения
B. Внести это в должностные инструкции сотрудников
C. Регулярно проводить учения по использованию плана
D. Сделать копии плана и хранить их на внешней площадке

Критерии оценки:

- оценка «отлично» выставляется аспиранту, если верно решено 21-25 заданий;
- оценка «хорошо» выставляется аспиранту, если верно решено 17-20 заданий;
- оценка «удовлетворительно» выставляется аспиранту, если верно решено 10-6 заданий;
- оценка «неудовлетворительно» выставляется аспиранте, если верно решено менее 10 заданий;

5. Темы для рефератов

1. Классификация угроз, приводящих к катастрофам в информационных системах
2. Методы обеспечения катастрофоустойчивости
3. Характеристика уровней катастрофоустойчивости
4. Кластеризация информационных систем и вопросы их катастрофоустойчивости
5. Организационные меры по обеспечению катастрофоустойчивости
6. Живучесть информационных систем
7. Технологии отказоустойчивости
8. Модель оценки информационной системы с позиции доступности
9. Модель оценки информационной системы по уровням катастрофоустойчивости
10. Модель оценки информационной системы с позиции живучести
11. Оценка эффективности катастрофоустойчивых решений

Критерии оценки:

Критерии оценки реферата

№	Критерий оценки	Баллы
1.	Умение сформулировать цель и задачи работы	9
2.	Умение работать с научной литературой (полнота научного обзора, грамотность цитирования)	9
3.	Полнота и логичность раскрытия темы	9
4.	Степень самостоятельности мышления	9
5.	Корректность выводов	8
6.	Реальная новизна работы	8
7.	Трудоемкость работы	14
8.	Культура оформления текста (соответствие требованиям оформления, стилистика изложения, грамотность)	14
9.	Эрудированность автора в рассматриваемой области (владение материалом, терминологией, знакомство с современным состоянием проблемы)	6
10.	Качество ответов на вопросы (полнота, аргументированность, умение реагировать на критику, готовность к дискуссии)	14

Критерии перевода баллов в оценку

Количество баллов	Оценка
0-25	«Неудовлетворительно»
26-50	«Удовлетворительно»
51-75	«Хорошо»
76-100	«Отлично»

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная литература

1. *Малафеев С. И.* Надежность технических систем. Примеры и задачи [Электронный ресурс]: / С. И. Малафеев, А. И. Копейкин - Санкт-Петербург [и др.]: Лань, 2012 - 320 с.

2. *Сигачева, Т.Н.* Надежность сложных технических систем: учеб. пособие/ Т.Н. Сигачева, Л.Б. Уразбахтина. – Уфа: УГАТУ, 2010.– 148 с.

3. *Половко, А. М.* Основы теории надежности: учебник для вузов/ А.М. Половко, А.Н. Гуров. – СПб.: БХВ-Санкт-Петербург, 2006. – 702с.

6.2 Дополнительная литература

1. Острейковский, В.А. Теория надежности: учебник для вузов/ В.А. Острейковский. – М.: Высшая школа, 2003. - 463с.

2. Харрис Ш. ISSP. Полное содержание перевода книги «CISSP All-In-One Exam Guide» // [Электронный ресурс]: http://dorlov.blogspot.ru/2011/05/issp-cissp-all-in-one-exam-guide.html (дата обращения: 02.11.2015).

3. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. [Электронный ресурс]: www.comsec.spb.ru/matherials/gosts/gost15408-2-2002.pdf (дата обращения: 02.11.2015)

4. ГОСТ Р МЭК 61508-4-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. [Электронный ресурс]: www.gosthelp.ru/gost/gost44280.html (дата обращения: 02.11.2015)

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступом к м электронным ресурсам и информационным справочным системам, перечисленным в таблице

Таблица

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
	Электронная база диссертаций РГБ	836206	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №1330/0208-14 от 02.12.2014
	СПС «КонсультантПлюс»	1806347	По сети УГАТУ.	Договор 1392/0403 -14от 10.12.14
	СПС «Гарант»	4 946588	По сети УГАТУ	ООО «Гарант-Регион, договор 291/-0107-14, от25.04.14
	Научная электронная библиотека (eLIBRARY)* http://elibrary.ru/	8384 журнала	По сети УГАТУ после регистрации в ЭБ на площадке библиотеки УГАТУ	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
	Научный полнотекстовый	1	По сети УГАТУ	Доп. соглашение

	журнал Science http://www.sciencemag.org			№13 SCI к ЛД №76-РН 2011 от 01.09.2011
	Научный полнотекстовый журнал Nature компании Nature Publishing Group* http://www.nature.com/	1	По сети УГАТУ	Доп. соглашение №13 Ng к ЛД №76-РН 2011 от 01.09.2011

6.4 Методические указания к практическим занятиям

Практические занятия являются обязательным компонентом учебного процесса, который является дополнением к лекционной форме обучения и предназначается для более углубленной проработки тем, затронутых на лекции.

Как правило, темы практических занятий включают в себя вопросы курса, для обсуждения которых требуется специальная подготовка аспирантов и соискателей с использованием рекомендуемой учебной литературы, источников и лекций. Методической особенностью практических занятий по данному курсу является применение двух основных форм работы с аспирантами и соискателями:

1) аудиторной – в виде выступления или устного обсуждения изучаемых тем;

2) самостоятельной – включающей изучение лекционного материала, учебной, монографической литературы и первоисточников, подготовку и написание реферата и докладов.

Подготовку к практическому занятию следует вести в следующем порядке:

Внимательно ознакомиться с планом практического занятия, списком рекомендуемой литературы;

Прочитать конспект лекций по теме практического занятия;

Обратиться к рекомендуемой учебной литературе по данной теме;

Внимательно изучить и постараться усвоить основные понятия изучаемой темы, так как эффективное освоение курса невозможно без владения специальной терминологией;

В ходе изучения темы практического занятия необходимо подготовить тезисы или конспект в тетради для практических занятий. Особенно это касается вопросов, предназначенных для самостоятельного изучения. Эти записи могут быть использованы на практических занятиях как подсказка при публичном выступлении.

Работу с литературой следует начинать с анализа списка рекомендуемой литературы по дисциплине, перечисленного в рабочей программе. Каждая тема из разделов тематического плана дисциплины и каждый вид занятий снабжен ссылками на источники литературы, что значительно упрощает поиск необходимой информации. Выбрав нужный источник, следует найти интересующий раздел по оглавлению или алфавитному указателю, а также одноименный раздел конспекта лекций или учебного пособия. В случае возникших затруднений в понимании учебного материала следует обратиться к другим источникам, где изложение может оказаться более доступным. Необходимо отметить, что работа с литературой не только полезна как средство более глубокого изучения любой дисциплины, но и является неотъемлемой частью профессиональной деятельности будущего исследователя.

6.5 Методические указания к практическим занятиям

Методические рекомендации по выполнению практических работ по дисциплине разработаны к.т.н., доцентом кафедры «Вычислительная техника и защита информации» А.М. Вульфиным в электронном виде.

7. Методические указания по освоению дисциплины

Формы работы аспирантов: лекционные занятия, практические занятия, написание рефератов, выполнение контрольных работ, решение кейс-задач.

Дисциплина «Катастрофоустойчивость информационных систем» разбита на модули, представляющие собой логически завершенные части курса и являющиеся теми комплексами знаний и умений, которые подлежат контролю.

Контроль освоения тем включает в себя выполнение письменных контрольных работ.

Для максимального усвоения дисциплины рекомендуется проведение письменного тестирования аспирантов по материалам лекций. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

В качестве организованной самостоятельной работы аспиранта рекомендуется использовать написание рефератов по выбранной заранее тематике. При написании реферата аспирант должен в соответствии с требованиями к оформлению работ сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

Предлагается:

- в первом разделе рассмотреть базовые понятия в области катастрофоустойчивости, живучести и отказоустойчивости информационных систем;

- во втором разделе рассмотреть методику исследования информационной системы с позиции катастрофоустойчивости;

- в третьем разделе обратить внимание на методы обеспечения катастрофоустойчивости;

- в четвёртом разделе акцентировать внимание на математических моделях оценки катастрофоустойчивости информационных систем;

Решения типовых тестовых заданий

1. Какие процедуры должны быть выполнены для восстановления систем и данных после системного сбоя?
A. Восстановление с резервных копий
B. Проведение параллельного тестирования
C. Выполнение процедур восстановления
D. Выполнение сквозного тестирования
В таких ситуациях нужно следовать процедурам восстановления, которые наверняка включают в себя процесс восстановления данных с резервных носителей информации. Процедуры восстановления могут включать в себя шаги по восстановлению систем «с нуля», применению необходимых патчей, настройке, обеспечению всего необходимого для того, чтобы обеспечить отсутствие негативного влияния на продуктивность работы компании. Для этих целей может потребоваться внедрение избыточных систем.

2. Что является одним из первых шагов при разработке плана обеспечения непрерывности бизнеса?
A. Определение имеющихся средств резервного копирования
B. Принятие решения, нужно ли компании выполнять сквозное, параллельное тестирование или моделирование
C. Проведение анализа воздействия на бизнес (BIA)
D. Разработка плана возобновления бизнеса
Анализ воздействия на бизнес (BIA) включает в себя идентификацию критичных систем и функций компании, проведение интервью с представителями каждого подразделения компании. Анализ воздействия на бизнес должен проводиться после получения полной поддержки руководства, он направлен на выявление угроз, перед лицом которых стоит компания, и величины потенциального ущерба от реализации этих угроз.

3. Насколько часто следует тестировать план обеспечения непрерывности бизнеса?
A. Не реже одного раза в десять лет

B. Только после изменений инфраструктуры или окружения
C. Не реже одного раза в два года
D. Когда в компании происходят существенные изменения
Этот план следует тестировать, когда в компании происходят существенные изменения, но не реже одного раза в год.

4. Одним из важных шагов в процессе тестирования процедур восстановления является ведение записей обо всех существенных шагах и произошедших событиях. Что из перечисленного ниже является не менее важным?
A. Спланировать следующее тестирование, при котором будут учтены возникшие проблемы
B. Убедиться, что назначен человек, который готов ответить на вопросы прессы
C. Подготовить отчет для руководства об этих шагах и событиях
D. Определить наиболее важные бизнес-функции
По окончании выполнения процедур восстановления, результаты этих процедур должны быть сообщены людям, которые отвечают за соответствующую деятельность. Обычно этими людьми является руководство определенного уровня. Если процедуры отработали успешно, руководство должно знать об этом, а если возникли проблемы, руководство тем более должно быть поставлено в известность.

5. Что из перечисленного ниже является наименее важным при проведении оценки рисков, связанных с потенциальными чрезвычайными ситуациями?
A. Сбор информации из отчетов специальных агентств, которые позволяют оценить вероятность природных катаклизмов в определенной местности
B. Идентификация ключевых функций компании и требований бизнеса
C. Идентификация критичных систем, обеспечивающих работу компании
D. Оценка потенциальных потерь и негативного воздействия на компанию в зависимости от продолжительности простоя
Вопрос касается количественной оценки рисков, которая требует расчета предполагаемого воздействия на бизнес определенных чрезвычайных ситуаций. Ключевыми элементами анализа воздействия на бизнес являются:

- *Определение ключевых функций компании и требований бизнеса*
- *Определение критичных систем, необходимых для функционирования компании*
- *Определение потенциального ущерба и воздействия на компанию, определение времени, которое компания может «продержаться» без этих систем*

Сбор информации из отчетов специальных агентств, которые позволяют оценить вероятность природных катаклизмов в определенной местности, является важным аспектом при определении вероятности определенных природных угроз, но это не очень важно при количественной оценке потенциального ущерба.

8. Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации – 5-301, 5-314, 5-313, 5-317.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-417 – лаборатория защиты информации;
- 5-418 – лаборатория технических средств защиты информации.

Вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

- компьютерная техника:
    - Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150

/ PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5" 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;

- программное обеспечение:
  - Программный комплекс – операционная система Microsoft Windows (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Office (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Project Professional (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – операционная система Microsoft Visio Pro (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования)
  - Kaspersky Endpoint Security для бизнеса (лицензии 13C8-140128-132040, 500 users).
  - Dr.Web® Desktop Security Suite (КЗ) +ЦУ (AH99-VCUN-TPPJ-6k3L, 415 рабочих станций).
  - ESET Smart Security Business (EAV-8424791, 500 пользователей).
  - Контур информационной безопасности SearchInform (UEI-2349-87, 25 пользователей).
  - Secret Net (IEK-109869, 25пользователей).
  - InfoWatch Traffic Monitor Enterprise (IWES-S3-DE, 25пользователей).
  - Seagate Central Discovery для ОС Windows (WOS-65-GT5, 25пользователей).

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

9. Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ

согласования рабочей программы

Направление подготовки: 10.06.01 Информационная безопасность
код и наименование

Направленность подготовки (программа): Методы и системы защиты информации, информационная безопасность

Дисциплина: Катастрофоустойчивость информационных систем

Учебный год 2015 / 2016

РЕКОМЕНДОВАНА заседанием кафедры Вычислительная техника и защита информации
наименование кафедры

протокол № 13 от "7" апреля 2015 г.
Заведующий кафедрой _____ Васильев В.И.
подпись расшифровка подписи

Исполнители:
К. техн. н., доцент _____ Вульфин А.М.
должность подпись расшифровка подписи

СОГЛАСОВАНО:

Заведующий кафедрой[1]
_____ Васильев В.И. 10. апреля 2015
наименование кафедры *личная подпись* *расшифровка подписи* *дата*

Председатель НМС по УГСН 10.06.01 Информационная безопасность
протокол № 10 от "11" 12 2014 г.

_____ Васильев В.И
личная подпись *расшифровка подписи*

Библиотека _____ С.Р. Муравьева 20.02.15.
личная подпись *расшифровка подписи* *дата*
Т.В. Дементьева

Начальник отдела аспирантуры _____ Р.К. Фаттахов 21.02.15.
личная подпись *расшифровка подписи* *дата*

Рабочая программа зарегистрирована в ООПМА и внесена в электронную базу данных

Начальник _____ И.А. Лакман 20 апреля 15
личная подпись *расшифровка подписи* *дата*

[1] Согласование осуществляется с выпускающими кафедрами (для рабочих программ, подготовленных на кафедрах, обеспечивающих подготовку для других направлений и специальностей)

1616