МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

РЕКОМЕНДОВАНО
К УТВЕРЖЕНИЮ
Декан факультета
магистерской подготовки
_____ **Ашуралиева Р.К.**
«02» 03 2020 г.

УТВЕРЖДАЮ
Врио ректора ДГТУ,
Председатель методического
совета ДГТУ
_____ **Суракатов Н.С.**
«03» 03 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина М1.В.ДВ.3 Организация и обеспечение отказоустойчивости и безопасности
код и наименование дисциплины по ООП

для направления 09.04.01 «Информатика и вычислительная техника»
код и направление направления подготовки

по профилю Сети ЭВМ и телекоммуникации
наименование магистерской программы

факультет Магистерской подготовки
наименование факультета, где ведется дисциплина (практика)

кафедра Управление и информатика в технических системах и вычислительной техники
наименование кафедры, за которой закреплена дисциплина (практика)

Квалификация выпускника (степень) Магистр
бакалавр, магистр (специалист)

Форма обучения очная курс 2 семестр (ы) 3
очная, заочная, др

Всего трудоемкость в зачетных единицах (часах) 3 ЗЕТ (108)

лекции 9 час экзамен - семестр

практические (семинарские) занятия - час зачет 3 семестр

лабораторные занятия 17 час самостоятельная работа 82 час

курсовой проект (работа, РГР) - семестр

И.о. зав. кафедрой _____ подпись Асланов Т.Г.

Начальник УО _____ подпись Магомаева Э.В.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению подготовки 09.04.01 «Информатика и вычислительная техника»

Программа одобрена на заседании выпускающей кафедры
от «28» 02 2020 года, протокол № 6.

И.о. зав. кафедрой по данному направлению _____ Асланов Т.Г.
подпись

ОДОБРЕНО

Методической комиссией по УГС(Н)
09.00.00 – Информатика и вычислительная техника

Председатель М.К.

_____ Абдулгалимов А.М.
подпись

«28» 02 2020 г.

АВТОР ПРОГРАММЫ
К.т.н., ст. преп. Т.Г. Асланов
_____
подпись

1. Цели освоения дисциплины

Целью данной дисциплины является обзор современных проблем в сфере информационной безопасности в информационных системах, а также обзор направлений развития программы информационной безопасности России.

2. Место дисциплины в структуре ООП магистратуры

Дисциплина «Организация и обеспечение отказоустойчивости и безопасности» представляет собой вариативную часть дисциплин по выбору учебного плана.

Дисциплина «Организация и обеспечение отказоустойчивости и безопасности» основывается на изучении таких дисциплин как: «Вычислительные системы» и «Моделирование и оптимизация вычислительных сетей».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Организация и обеспечение отказоустойчивости и безопасности»

Выпускник, освоивший программу магистратуры, должен обладать следующими компетенциями:

общекультурными (ОК):

– способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень (ОК-1);

– способностью понимать роль науки в развитии цивилизации, соотношение науки и техники, иметь представление о связанных с ними современных социальных и этических проблемах, понимать ценность научной рациональности и ее исторических типов (ОК-2);

общепрофессиональными (ОПК):

– владением, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, способностью применять специальную лексику и профессиональную терминологию языка (ОПК-4);

– владением методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях (ОПК-5);

– способностью анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями (ОПК-6)

профессиональными компетенциями (ПК):

– знанием методов оптимизации и умение применять их при решении задач профессиональной деятельности (ПК-3);

– способностью выбирать методы и разрабатывать алгоритмы решения задач управления и проектирования объектов автоматизации (ПК-12);

– способностью к созданию программного обеспечения для анализа, распознавания и обработки информации, систем цифровой обработки сигналов (ПК-15);

В результате освоения дисциплины обучающийся должен:

Знать: способы совершенствования и развития своего интеллектуального и

общекультурного уровня; роль науки в развитии цивилизации; основы профессионального общения на иностранном языке; современные тенденции развития в области получения, передачи, хранения и переработки данных; научные основы применения компьютерных технологий; основные, наиболее эффективные методы решения задач оптимизации; методы проектирования объектов автоматизации; методы создания программного обеспечения для анализа, распознавания и обработки информации, систем цифровой обработки сигналов.

Уметь: совершенствовать знания в выбранной области для решения профессиональных задач; анализировать социальные и этические проблемы науки и техники; формулировать основные положения технической документации на иностранном языке; применять вычислительную технику для решения практических задач; использовать типовые программные продукты, ориентированные на решение научных, проектных и технологических задач; правильно формулировать и классифицировать задачи оптимизации; применять методы проектирования объектов автоматизации; создавать программное обеспечение для анализа, распознавания и обработки информации, систем цифровой обработки сигналов.

Владеть: технологиями анализа, синтеза и оценки общекультурных и профессиональных знаний; навыками рационального мышления; навыком применения одного из иностранных языков на уровне социального и профессионального общения; методами и средствами работы в глобальных компьютерных сетях; методиками сбора, переработки и представления научно-технических материалов по результатам исследований к опубликованию в печати, а также в виде обзоров, рефератов, отчетов, докладов и лекций; основными, наиболее эффективными методами решения задач оптимизации; средами проектирования; навыками создания программного обеспечения для анализа, распознавания и обработки информации, систем цифровой обработки сигналов.

4. Содержание дисциплины «Организация и обеспечение отказоустойчивости и безопасности»

4.1 Содержание дисциплины

№	Раздел дисциплины Тема лекции и вопросы	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по срокам текущих аттестаций в семестре) Форма промежуточной аттестации (по семестрам)
				ЛК	ПЗ	ЛБ	СР	
а	б	в	г	д	е	ж	з	и
1	Лекция 1 **ТЕМА:** Основные понятия отказоустойчивости информационной системы (ИС). 1. Понятия отказоустойчивости,	3	1	2	0	4	16	Входная контрольная работа

	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 отказоустойчивости. 7. Показатели и критерии функционирования отказоустойчивой информационной системы. 8. Живучесть информационных систем. 9. Отказоустойчивость и надежность. 10. Разработка моделей оценки живучести ИС.							
2	Лекция 2 **ТЕМА:** Модели и показатели функционирования отказоустойчивых ИС. 1. Модель оценки информационной системы с позиции доступности. 2. Модель оценки информационной системы по уровням отказоустойчивости.		5	2	0	4	17	Аттестационная контрольная работа 1
3	Лекция 2 **ТЕМА:** Модели и показатели функционирования отказоустойчивых ИС. 1. Модель оценки информационной системы с позиции живучести. 2. Оценка эффективности отказоустойчивых решений. 3. Структурный анализ отказоустойчивой ИС.		9	2	0	4	16	Аттестационная контрольная работа 2
4	Лекция 3 **ТЕМА:** Методы обеспечения отказоустойчивости ИС. 1. Методика создания отказоустойчивой информационной системы. 2. Классификация методов обеспечения отказоустойчивости. 3. Стратегии резервирования. 4. Кластеризация. 5. Избыточные структуры. 6. Резервные центры обработки данных.		13	2	0	4	17	Аттестационная контрольная работа 3
5	Лекция 3 **ТЕМА:** Методы обеспечения отказоустойчивости ИС. 1. Выбор варианта отказоустойчивой конструкции центра обработки информации. 2. Выбор стратегии восстановления в отказоустойчивой системе. 3. Разработка модели оценки доступности информации в отказоустойчивых системах. 4. Исследование готовности и доступности ИС. 5. Исследование уровней отказоустойчивости на моделях		17	1	0	1	16	

	типовых ИС. 6. Моделирование дестабилизирующих воздействий и их последствий на ИС. 7. Разработка модели оценки отказоустойчивых решений.							
Итого:				9	0	17	82	Зачет

4.2 Содержание практических занятий

Практические занятия учебным планом не предусмотрено.

4.3 Содержание лабораторных занятий

№ п/п	№ по содержанию дисциплины	Наименование лабораторного занятия	Количество часов	Рекомендуемая литература и методические разработки (№ источника из списка литературы)
1	1	Лабораторная работа по информационным системам.	4	1-4
2	2	Лабораторная работа по оценке информационной системы по уровням отказоустойчивости.	4	1-4
3	3	Лабораторная работа по оценке эффективности отказоустойчивых решений.	4	1-4
4	4	Лабораторная работа по стратегии резервирования.	2	1-4
5	5	Лабораторная работа по разработке модели оценки доступности информации в отказоустойчивых системах.	3	1-4
Итого:			17	

4.4 Тематика для самостоятельной работы студента

N п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Количество часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля СРС
1	Понятия отказоустойчивости, живучести и отказоустойчивости. Информационные системы. Виды, архитектура, субъекты и объекты взаимодействия. Модель катастрофических воздействий. Моделирование и прогноз природных и техногенных катастроф. Уровни отказоустойчивости. Показатели и критерии функционирования отказоустойчивой информационной системы. Живучесть информационных систем. Отказоустойчивость и надежность. Разработка моделей оценки живучести ИС.	16	1-4	Опрос
2	Модель оценки информационной системы с позиции доступности. Модель оценки информационной	17	1-4	Опрос

	системы по уровням отказоустойчивости.			
3	Модель оценки информационной системы с позиции живучести. Оценка эффективности отказоустойчивых решений. Структурный анализ отказоустойчивой ИС.	16	1-4	Опрос
4	Методика создания отказоустойчивой информационной системы. Классификация методов обеспечения отказоустойчивости. Стратегии резервирования. Кластеризация. Избыточные структуры. Резервные центры обработки данных.	17	1-4	Опрос
5	Выбор варианта отказоустойчивой конструкции центра обработки информации. Выбор стратегии восстановления в отказоустойчивой системе. Разработка модели оценки доступности информации в отказоустойчивых системах. Исследование готовности и доступности ИС. Исследование уровней отказоустойчивости на моделях типовых ИС. Моделирование дестабилизирующих воздействий и их последствий на ИС. Разработка модели оценки отказоустойчивых решений.	16	1-4	Опрос
Итого:		82		

5. Образовательные технологии

В ходе проведения занятий используются такие методы обучения как презентация, применение компьютерной техники.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

6.1 Перечень вопросов по проверке входных знаний студентов

1. Исторический подход к защите информации в КС.
2. Информация – предмет защиты.
3. Информация – объект защиты.
4. Случайные угрозы информации в КС.
5. Преднамеренные угрозы информации в КС.
6. Защита информации в КС от случайных угроз.
7. Способы повышения надежности и отказоустойчивости КС.
8. Защита информации в КС от преднамеренных угроз.
9. Основные способы НСД.
10. Физическая защита ПЭВМ от НСД.
11. Назначение и функции аппаратных устройств защиты ПЭВМ.
12. Идентификация и аутентификация пользователей.

13. Идентификация и аутентификация компонент обработки информации.
14. Разграничение доступа к информации и компонентам ее обработки.
15. Криптографическое закрытие информации на ВЗУ и в процессе обработки.
16. Подсистема аудита.
17. Программные и аппаратные закладки.
18. Организационные меры защиты информации в КС.
19. Назначение и структура стандартов информационной безопасности.
20. Классы и требования защищенности автоматизированных систем.
21. Классификация компьютерных вирусов.
22. Методы обнаружения известных и неизвестных вирусов.
23. Профилактика заражения вирусами КС.
24. Действия пользователя при обнаружении заражения КС вирусами.
25. Средства восстановления работоспособности КС.
26. Основы построения защищенных операционных систем.
27. Функции администратора защищенной ОС по созданию и управлению учетными записями пользователей
28. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS.
29. Организация аудита ресурсов и событий системы защиты ОС.
30. Специфические угрозы безопасности информации в базах данных.
31. Средства защиты баз данных.
32. Управление распределенными данными.
33. Угрозы безопасности информации в компьютерных сетях.
34. Задачи и направления обеспечения информационной безопасности в сетях передачи данных.
35. Службы и механизмы информационной безопасности в сетях передачи данных.
36. Защита информации при межсетевом взаимодействии.
37. Сегментация сложных локальных сетей.
38. Обеспечение безопасного обмена конфиденциальной информацией.
39. Классификация и применение межсетевых экранов.
40. Межсетевой экран – пакетный фильтр.
41. Межсетевой экран – посредник прикладного уровня.
42. Системы контроля содержания.
43. Сканеры безопасности.
44. Обеспечение защиты информации средствами VPN.
45. Системы обнаружения атак.

6.2. Задания для текущих аттестаций

6.2.1. *Контрольные вопросы для первой аттестации*

1. Понятия отказоустойчивости, живучести и отказоустойчивости.
2. Информационные системы.
3. Виды, архитектура, субъекты и объекты взаимодействия.
4. Модель отказических воздействий.
5. Моделирование и прогноз природных и техногенных отказ.

6. Уровни отказоустойчивости.

7. Показатели и критерии функционирования отказоустойчивой информационной системы.

8. Живучесть информационных систем.

9. Отказоустойчивость и надежность.

10. Разработка моделей оценки живучести ИС.

11. Модель оценки информационной системы с позиции доступности.

12. Модель оценки информационной системы по уровням отказоустойчивости.

13. Модель оценки информационной системы с позиции живучести.

14. Оценка эффективности отказоустойчивых решений.

6.2.2. *Контрольные вопросы для второй аттестации*

1. Живучесть информационных систем.
2. Отказоустойчивость и надежность.
3. Разработка моделей оценки живучести ИС.
4. Модель оценки информационной системы с позиции доступности.
5. Модель оценки информационной системы по уровням отказоустойчивости.
6. Модель оценки информационной системы с позиции живучести.
7. Оценка эффективности отказоустойчивых решений.
8. Структурный анализ отказоустойчивой ИС.
9. Методика создания отказоустойчивой информационной системы.
10. Классификация методов обеспечения отказоустойчивости.
11. Стратегии резервирования.
12. Кластеризация.
13. Избыточные структуры.
14. Резервные центры обработки данных.

6.2.3. *Контрольные вопросы для третей аттестации*

1. Структурный анализ отказоустойчивой ИС.
2. Методика создания отказоустойчивой информационной системы.
3. Классификация методов обеспечения отказоустойчивости.
4. Стратегии резервирования.
5. Кластеризация.
6. Избыточные структуры.
7. Резервные центры обработки данных.
8. Выбор варианта отказоустойчивой конструкции центра обработки информации.
9. Выбор стратегии восстановления в отказоустойчивой системе.
10. Разработка модели оценки доступности информации в отказоустойчивых системах.
11. Исследование готовности и доступности ИС.
12. Исследование уровней отказоустойчивости на моделях типовых ИС.
13. Моделирование дестабилизирующих воздействий и их последствий на ИС.
14. Разработка модели оценки отказоустойчивых решений.

6.3. Перечень вопросов по проверке остаточных знаний

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

6.4. Задания для промежуточной аттестации

6.4.1 *Контрольные вопросы для проведения зачета*

1. Понятия отказоустойчивости, живучести и отказоустойчивости.
2. Информационные системы.
3. Виды, архитектура, субъекты и объекты взаимодействия.
4. Модель отказических воздействий.
5. Моделирование и прогноз природных и техногенных отказ.
6. Уровни отказоустойчивости.
7. Показатели и критерии функционирования отказоустойчивой информационной системы.
8. Живучесть информационных систем.
9. Отказоустойчивость и надежность.
10. Разработка моделей оценки живучести ИС.
11. Модель оценки информационной системы с позиции доступности.
12. Модель оценки информационной системы по уровням отказоустойчивости.
13. Модель оценки информационной системы с позиции живучести.
14. Оценка эффективности отказоустойчивых решений.
15. Структурный анализ отказоустойчивой ИС.
16. Методика создания отказоустойчивой информационной системы.
17. Классификация методов обеспечения отказоустойчивости.
18. Стратегии резервирования.

19. Кластеризация.

20. Избыточные структуры.

21. Резервные центры обработки данных.

22. Выбор варианта отказоустойчивой конструкции центра обработки информации.

23. Выбор стратегии восстановления в отказоустойчивой системе.

24. Разработка модели оценки доступности информации в отказоустойчивых системах.

25. Исследование готовности и доступности ИС.

26. Исследование уровней отказоустойчивости на моделях типовых ИС.

27. Моделирование дестабилизирующих воздействий и их последствий на ИС.

28. Разработка модели оценки отказоустойчивых решений.

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

Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой

№ п/п	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор(ы)	Издательство и год издания	Количество изданий	
				В библиотеке	На кафедре
ОСНОВНАЯ					
1	Функциональная реконфигурация отказоустойчивых систем : монография	Тарасов А.А.	Москва : Логос, 2012	IPR BOOKS iprbookshop.ru/13015.html	
2	Математические модели и схемные решения отказоустойчивых непозиционных вычислительных систем : коллективная монография	Калмыков И.А.	Ставрополь : Северо-Кавказский федеральный университет, 2016	IPR BOOKS iprbookshop.ru/69400.html	
ДОПОЛНИТЕЛЬНАЯ					
3	Вычислительные системы, сети и телекоммуникации : учебное пособие по дисциплине «Вычислительные системы, сети и телекоммуникации» для студентов, обучающихся	Буцык С.В.	Челябинск : Челябинский государственный институт культуры, 2016	IPR BOOKS iprbookshop.ru/56399.html	

	по направлению 09.03.03 Прикладная информатика (уровень бакалавриата)				
4	Сети связи : учебное пособие по дисциплине «Сети связи и системы коммутации»	Росляков А.В.	Самара : Поволжский государственный университет телекоммуникаций и информатики, 2017	IPR BOOKS iprbookshop.ru/75406.html	

8. Материально-техническое обеспечение дисциплины (модуля)

Семинарские занятия по дисциплине проводятся в аудитории с презентационной техникой и учебной мебелью.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению и профилю подготовки 09.04.01 – Информатика и вычислительная техника. Рецензент от выпускающей кафедры по направлению _____ Меркухин Е.Н.