МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Современные проблемы математической логики и теории алгоритмов Б1.В.ДВ.6

Направление подготовки: 02.04.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Математические основы и программное обеспечение информационной безопасности и защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Михайлов В.Ю.

Рецензент(ы):
Пшеничный П.В.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2016

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Михайлов В.Ю. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Valery.Mikhailov@kpfu.ru

1. Цели освоения дисциплины

Целью преподавания дисциплины является формирование у студентов фундаментальных знаний в области математической логики и теории алгоритмов, являющихся основой математического обеспечения современных компьютерных и информационных технологий;

получение представлений о математической логике и теории алгоритмов как базе для самостоятельного изучения и решения проблем новых ИКТ;

приобретение представлений о новейших тенденциях развития инструментария математической логики и теории алгоритмов;

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.6 Дисциплины (модули)" основной образовательной программы 02.04.02 Фундаментальная информатика и информационные технологии и относится к дисциплинам по выбору. Осваивается на 2 курсе, 3 семестр.

"Современные проблемы математической логики и теории алгоритмов " входит в состав префессиональных дисциплин. Читается на 2 курсе, в 3 семестре.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способность к абстрактному мышлению, анализу, синтезу
ОК-3 (общекультурные компетенции)	готовность к саморазвитию, самореализации, использованию творческого потенциала
ОПК-3 (профессиональные компетенции)	способность использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий
ОПК-4 (профессиональные компетенции)	способность самостоятельно приобретать и использовать в практической деятельности новые знания и умения, в том числе, в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять своё научное мировоззрение
ОПК-5 (профессиональные компетенции)	способность использовать углублённые знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов
ПК-1 (профессиональные компетенции)	способность проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-13 (профессиональные компетенции)	способность разрабатывать аналитические обзоры состояния области прикладной математики и информационных технологий
ПК-14 (профессиональные компетенции)	способность выполнять работу экспертов в ведомственных, отраслевых или государственных экспертных группах по экспертизе проектов, тематика которых соответствует направленности (профилю) программы магистратуры
ПК-16 (профессиональные компетенции)	способность участвовать в деятельности профессиональных сетевых сообществ по конкретным направлениям
ПК-2 (профессиональные компетенции)	способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий
ПК-3 (профессиональные компетенции)	способность разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач проектной и производственно-технологической деятельности
ПК-4 (профессиональные компетенции)	способность разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств, а также разрабатывать абстрактные методы их тестирования
ПК-5 (профессиональные компетенции)	способность управлять проектами, планировать научно-исследовательскую деятельность, анализировать риски, управлять командой проекта
ПК-6 (профессиональные компетенции)	способность к углубленному анализу проблем, постановке и обоснованию задач научной и проектно-технологической деятельности

В результате освоения дисциплины студент:

1. должен знать:

- основные понятия математической логики и теории алгоритмов: высказывание, нормальные и совершенные нормальные формы, предикат, исчисление, аксиоматическая система, формальный вывод, алгоритм, алгоритмическая система, алгоритмически неразрешимая проблема др.;
- основы логики высказываний, логики предикатов, алгебры множеств, теории алгоритмов;
- приёмы, методы и способы математической формализации логических задач;

2. должен уметь:

- исследовать различные логические задачи;
- применять полученные знания для абстрактного проектирования логических структур;
- формулировать и решать задачи в научных областях, связанных с современными компьютерными и информационными технологиями

3. должен владеть:

- методологией математической логики

- приёмами и формализованными схемами, помогающими анализировать, моделировать и решать различные логические задачи.

-применять полученные знания в своей дальнейшей профессиональной и научной деятельности, применять при написании магистерской диссертации.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 3 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Темпоральные логики в задачах верификации реактивных систем и параллельных программ. Логики Прайора и Пнуели. Логики линейного времени LTL и ветвящегося времени CTL.	3		2	2	0	письменное домашнее задание
2.	Тема 2. Общая схеме подхода model checking. Алгоритмы проверки истинности темпоральных формул на моделях Крипке.	3		2	2	0	письменное домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Символьная верификация. Построение пропозициональных формул, описывающих структуры Крипке и темпоральные операторы.	3		2	2	0	письменное домашнее задание
4.	Тема 4. Эпистемические и темпоральные логики в задачах информационной безопасности. Формализация коммуникационных протоколов. Динамическая эпистемическая логика.	3		2	2	0	письменное домашнее задание
5.	Тема 5. Логический криптоанализ. Построение пропозициональных формул, описывающих обратные функции для класса автоматных функций и функций быстро вычислимых по Тьюрингу.	3		2	2	0	письменное домашнее задание
6.	Тема 6. Бинарные решающие диаграммы (OBDD). Алгоритмы построения OBDD.Работа со свободно распространяемыми библиотеками BDD.	3		2	2	0	письменное домашнее задание
7.	Тема 7. Решение задачи выполнимости с использованием подходов, используемых в теории ИИ. Алгоритм Дэвиса-Патнем. Алгоритм имитации обжига. Генетические алгоритмы.	3		2	2	0	контрольная работа
.	Тема . Итоговая форма контроля	3		0	0	0	экзамен

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
	Итого			14	14	0	

4.2 Содержание дисциплины

Тема 1. Темпоральные логики в задачах верификации реактивных систем и параллельных программ. Логики Прайора и Пнуели. Логики линейного времени LTL и ветвящегося времени CTL.

лекционное занятие (2 часа(ов)):

Анализ выразительных возможностей темпоральных логик Прайора, Пнуели, LTL, CTL. Аксиоматика и дедуктивные свойства.

практическое занятие (2 часа(ов)):

Примеры формализации требований к работе реактивных систем и параллельных программ на языках логик LTL и CTL.

Тема 2. Общая схеме подхода model checking. Алгоритмы проверки истинности темпоральных формул на моделях Крипке.

лекционное занятие (2 часа(ов)):

Описание алгоритмов разметки для проверки выполнимости на моделях для формул логики CTL. Описание алгоритмов построения автоматов Бюхи для проверки выполнимости на моделях для формул логики LTL.

практическое занятие (2 часа(ов)):

Разбор примеров верификации работы простых реактивных систем и параллельных программ.

Тема 3. Символьная верификация. Построение пропозициональных формул, описывающих структуры Крипке и темпоральные операторы.

лекционное занятие (2 часа(ов)):

Описание и оценка сложности алгоритмов построения пропозициональных формул, описывающих отношение достижимости в структурах Крипке. Описание и оценка сложности алгоритмов построения пропозициональных формул, описывающих состояния структуры Крипке, в которых истинна данная темпоральная формула.

практическое занятие (2 часа(ов)):

Примеры описаний структур Крипке и темпоральных операторов.

Тема 4. Эпистемические и темпоральные логики в задачах информационной безопасности. Формализация коммуникационных протоколов. Динамическая эпистемическая логика.

лекционное занятие (2 часа(ов)):

Анализ проблем уязвимости сетевых протоколов. Формализация задач обеспечения безопасности протоколов на языках темпоральных логик и динамической эпистемической логики.

практическое занятие (2 часа(ов)):

Примеры описаний простых коммуникационных протоколов на языках темпоральных и эпистемических логик.

Тема 5. Логический криптоанализ. Построение пропозициональных формул, описывающих обратные функции для класса автоматных функций и функций быстро вычислимых по Тьюрингу.

лекционное занятие (2 часа(ов)):

Общая схема логического криптоанализа. Основные алгоритмы моделирования работы вычислительных автоматов с помощью пропозициональных логик. Сведение задач криптоанализа к проблеме выполнимости логических формул.

практическое занятие (2 часа(ов)):

Логический криптоанализ простых схем кодирования типа кода Цезаря.

Тема 6. Бинарные решающие диаграммы (OBDD). Алгоритмы построения OBDD.Работа со свободно распространяемыми библиотеками BDD.

лекционное занятие (2 часа(ов)):

Описание алгоритмов построения BDD. Оценка их сложности. Построение BDD для формул, используемых в алгоритмах символьной верификации.

практическое занятие (2 часа(ов)):

Работа со свободно распространяемыми библиотеками построения BDD. Примеры решения головоломок типа "волк-коза-капуста".

Тема 7. Решение задачи выполнимости с использованием подходов, используемых в теории ИИ. Алгоритм Дэвиса-Патнем. Алгоритм имитации обжига. Генетические алгоритмы.

лекционное занятие (2 часа(ов)):

Описание алгоритмов ИИ в применении к решению задачи проверки выполнимости пропозициональных формул.

практическое занятие (2 часа(ов)):

Работа со свободно распространяемыми библиотеками, реализующими алгоритм DPLL.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Темпоральные логики в задачах верификации реактивных систем и параллельных программ. Логики Прайора и Пнуели. Логики линейного времени LTL и ветвящегося времени CTL.	3		подготовка домашнего задания	6	домашнее задание
2.	Тема 2. Общая схеме подхода model checking. Алгоритмы проверки истинности темпоральных формул на моделях Крипке.	3		подготовка домашнего задания	6	домашнее задание
3.	Тема 3. Символьная верификация. Построение пропозициональных формул, описывающих структуры Крипке и темпоральные операторы.	3		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Эпистемические и темпоральные логики в задачах информационной безопасности. Формализация коммуникационных протоколов. Динамическая эпистемическая логика.	3		подготовка домашнего задания	6	домашнее задание
5.	Тема 5. Логический криптоанализ. Построение пропозициональных формул, описывающих обратные функции для класса автоматных функций и функций быстро вычислимых по Тьюрингу.	3		подготовка домашнего задания	6	домашнее задание
6.	Тема 6. Бинарные решающие диаграммы (OBDD). Алгоритмы построения OBDD.Работа со свободно распространяемыми библиотеками BDD.	3		подготовка домашнего задания	7	домашнее задание
7.	Тема 7. Решение задачи выполнимости с использованием подходов, используемых в теории ИИ. Алгоритм Дэвиса-Патнем. Алгоритм имитации обжига. Генетические алгоритмы.	3		подготовка к контрольной работе	7	контрольная работа
	Итого				44	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лабораторных занятий и самостоятельной работы студентов.

Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

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

Тема 1. Темпоральные логики в задачах верификации реактивных систем и параллельных программ. Логики Прайора и Пнуели. Логики линейного времени LTL и ветвящегося времени CTL.

домашнее задание , примерные вопросы:

Задания на формализацию требований к реактивным системам и параллельным программам на языках логик LTL и CTL.

Тема 2. Общая схеме подхода model checking. Алгоритмы проверки истинности темпоральных формул на моделях Крипке.

домашнее задание , примерные вопросы:

Подробный разбор алгоритмов выполнения темпоральных операторов на моделях Крипке.

Тема 3. Символьная верификация. Построение пропозициональных формул, описывающих структуры Крипке и темпоральные операторы.

домашнее задание , примерные вопросы:

Построение булевских формул, описывающих условие истинности требований темпоральных формул на моделях Крипке.

Тема 4. Эпистемические и темпоральные логики в задачах информационной безопасности. Формализация коммуникационных протоколов. Динамическая эпистемическая логика.

домашнее задание , примерные вопросы:

Задания на формализацию условий устойчивости коммуникационных протоколов на языке динамической эпистемической логики.

Тема 5. Логический криптоанализ. Построение пропозициональных формул, описывающих обратные функции для класса автоматных функций и функций быстро вычислимых по Тьюрингу.

домашнее задание , примерные вопросы:

Задания на формализацию работы автоматных функций. Формализация описания обратных функций.

Тема 6. Бинарные решающие диаграммы (OBDD). Алгоритмы построения OBDD.Работа со свободно распространяемыми библиотеками BDD.

домашнее задание , примерные вопросы:

Работа с библиотеками построения BDD.

Тема 7. Решение задачи выполнимости с использованием подходов, используемых в теории ИИ. Алгоритм Дэвиса-Патнем. Алгоритм имитации обжига. Генетические алгоритмы.

контрольная работа , примерные вопросы:

Примерное задание контрольной работы: Записать на языке логики CTL следующие высказывания: 5.1. При любом функционировании системы (на любом пути) из любого состояния системы всегда обязательно вернемся в состояние рестарта. 5.2. Не существует такого режима работы прибора, при котором интенсивность облучения пациента превысит 0.01 радиан в сек. 5.3. В любом режиме, если противопожарная система включается, то на это обязательно предварительно была получена санкция капитана.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. примерные вопросы для экзамена - Приложение1.

Примеры билетов к экзамену.

Билет 1.

1. Темпоральные операторы логики CTL.
2. Алгоритмы построения BDD.

Билет 2.

1. Сравнительный анализ выразительных средств логик LTL и CTL.
2. Сведение ограниченной проблемы остановки к задаче выполнимости БФ.

7.1. Основная литература:

1. Математическая логика[Электронный ресурс]: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2012. - 399 с. . - Режим доступа: http://www.znanium.com/bookread.php?book=242738

2. Теория алгоритмов[Электронный ресурс]: Учебное пособие / В.И. Игошин. - М.: ИНФРА-М, 2012. - 318 с. . - Режим доступа: http://www.znanium.com/bookread.php?book=241722

7.2. Дополнительная литература:

1. Ершов Ю. Л. Математическая логика / Ю.Л. Ершов, Е.А. Палютин. - 6-е изд., испр. - М.: ФИЗМАТЛИТ, 2010. - 432 с. Режим доступа: http://znanium.com/bookread2.php?book=395379

2. Кузнецов А. С. Теория вычислительных процессов/КузнецовА.С., ЦаревР.Ю., КнязьковА.Н. - Красноярск.: СФУ, 2015. - 184 с. Режим доступа: http://znanium.com/bookread2.php?book=549796

3. Методы научного познания: Учебное пособие / С.А. Лебедев. - М.: Альфа-М: НИЦ ИНФРА-М, 2014. - 272 с. URL: http://znanium.com/bookread.php?book=450183

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет--портал ресурсов по математическим наукам - http://www.math.ru/

Интернет--портал ресурсов по математическим наукам - http://www.allmath.com/

Интернет-портал со статьями по алгоритмике и программированию - http://algolist.manual.ru/

Электронная библиотека по техническим наукам - http://techlibrary.ru

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Современные проблемы математической логики и теории алгоритмов" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

лабораторные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 02.04.02 "Фундаментальная информатика и информационные технологии" и магистерской программе Математические основы и программное обеспечение информационной безопасности и защиты информации .

Автор(ы):
Михайлов В.Ю. _____
"__" _____ 201 __ г.

Рецензент(ы):
Пшеничный П.В. _____
"__" _____ 201 __ г.