

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ярославский государственный университет им. П.Г. Демидова»

Факультет информатики и вычислительной техники

УТВЕРЖДАЮ
Декан факультета
информатики и вычислительной техники



Д.Ю. Чалый

«_24_»_мая__ 2022 г.

Рабочая программа дисциплины

«Специальная дисциплина в соответствии с темой диссертации на соискание ученой степени кандидата наук по научной специальности 1.2.3 Теоретическая информатика, кибернетика»

программы подготовки научных и научно-педагогических кадров в аспирантуре

Форма обучения очная

Программа одобрена на заседании факультета информатики и вычислительной техники от «_15_» марта 2022 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины является знание ключевых положений основополагающих дисциплин соответствующего профиля подготовки аспиранта.

2. Место дисциплины в структуре программы аспирантуры

Данная дисциплина относится к разделу обязательные дисциплины (2.1.3) и направлена на подготовку к сдаче кандидатского экзамена по специальной дисциплине в соответствии с темой диссертации на соискание ученой степени кандидата наук по научной специальности 1.2.3 Теоретическая информатика, кибернетика.

3. Планируемые результаты освоения дисциплины:

В результате освоения дисциплины аспирант должен:

Знать:

- основные теоретические положения базовых разделов теоретической информатики и кибернетики

Уметь:

- выполнять обзоры результатов научных исследований
- проводить научные исследования
- применять современные алгоритмы решения прикладных задач

Владеть:

- навыками исследовательской и прикладной деятельности в соответствующих отраслях прикладной математики и информатики

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 8 зачетных единиц, 288 акад. часов
Дисциплина изучается в течение четырех семестров.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости
			лекции	практические	лабораторные	консультации	самостоятельная работа	Форма промежуточной аттестации (по семестрам)
1.	Алгебра логики. Исчисление предикатов первого порядка.	2	2			1	33	
2.	Отношения и функции	2	2			1	33	
	Всего за семестр	2	4			2	66	Зачет
3.	Автоматы, языки и грамматики	3	2				34	
4.	Основы построения трансляторов							

								Зачет
	Всего за семестр	3	4				68	
5.	Теория алгоритмов	4	2			1	34	
6.	Сложность алгоритмов	4	2			1	34	
								Зачет
	Всего за семестр	4	4				68	
7.	Методы хранения и обработки данных	5	2			1	15	
8.	Теория криптографии	5	2			1	15	
							36	Экзамен
	Всего за семестр	5	4			2	66	
	Всего		16			4	268	

Содержание разделов дисциплины:

Тема 1. Алгебра логики. Исчисление предикатов первого порядка.

Булевы функции, канонические формы задания булевых функций.

Понятие полной системы. Критерий полноты Поста.

Исчисление высказываний. Общезначимость, доказуемость. Теорема о полноте.

Исчисление предикатов первого порядка. Понятие интерпретации.

Выполнимость и общезначимость формулы первого порядка.

Понятие модели.

Теорема о полноте исчисления предикатов первого порядка.

Тема 2. Отношения и функции

Отношение эквивалентности и разбиения. Фактор множества.

Отношения частичного порядка.

Теоретико-множественное и алгебраическое определения решетки, их эквивалентность.

Свойства решеток. Булевы решетки. Полные решетки.

Тема 3. Автоматы, языки и грамматики

Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе.

Конечные автоматы. ДКА и НКА. Минимизация конечных автоматов.

Алгебры регулярных выражений. Теорема Клини о регулярных языках.

Контекстно-свободные языки и грамматики, их свойства. Магазинные автоматы.

Тема 4. Основы построения трансляторов

Структура оптимизирующего транслятора. Промежуточные представления программы: последовательность символов, последовательность лексем, синтаксическое дерево, абстрактное синтаксическое дерево. Уровни промежуточного представления: высокий, средний, низкий. Формы промежуточного представления.

Анализ исходной программы в компиляторе. Автоматные (регулярные) грамматики и сканирование, контекстно свободные грамматики и синтаксический анализ, организация таблицы символов программы, имеющей блочную структуру, хеш-функции. Нисходящие (LL(1)-грамматики) и восходящие (LR(1)-грамматики) методы синтаксического анализа. Атрибутные грамматики и семантические программы, построение абстрактного синтаксического дерева.

Тема 5. Теория алгоритмов

Понятие алгоритма и его уточнения: машины Тьюринга, нормальные алгоритмы Маркова, рекурсивные функции.

Эквивалентность различных формальных моделей алгоритмов.

Понятие об алгоритмической неразрешимости. Примеры алгоритмически неразрешимых проблем.

Тема 6. Сложность алгоритмов

Понятие сложности алгоритмов. Классы P и NP.

Полиномиальная сводимость задач.

Теорема Кука об NP-полноте задачи выполнимости булевой формулы.

Примеры NP-полных задач, подходы к их решению. Точные и приближенные комбинаторные алгоритмы.

Примеры эффективных (полиномиальных) алгоритмов: быстрые алгоритмы поиска и сортировки; полиномиальные алгоритмы для задач на графах и сетях (поиск в глубину и ширину, о минимальном остове, о кратчайшем пути, о назначениях).

Тема 7. Методы хранения и обработки данных

Основные понятия реляционной и объектной моделей данных. Теоретические основы реляционной модели данных (РДМ). Реляционная алгебра, реляционное исчисление.

Функциональные зависимости и нормализация отношений.

Основные структуры данных, алгоритмы обработки и поиска. Сравнительная характеристика методов хранения и поиска данных. Методы индексирования.

Основные принципы управления транзакциями, журнализацией и восстановлением.

Постреляционные базы данных (NoSQL).

Интеллектуальные системы машинного обучения. Machine Learning.

Тема 8. Теория криптографии

Коды с исправлением ошибок. Алфавитное кодирование. Методы сжатия информации.

Задачи обеспечения конфиденциальности и целостности информации. Теоретико-информационный и теоретико-сложностный подходы к определению

криптографической стойкости. Американский стандарт шифрования DES и российский стандарт шифрования данных ГОСТ 28147-89. Системы шифрования с открытым ключом (RSA). Цифровая подпись. Методы генерации и распределения ключей.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание аспирантов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания аспирантом в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы аспирантов. На консультациях по просьбе аспирантов рассматриваются наиболее сложные разделы дисциплины, преподаватель отвечает на вопросы аспирантов, которые возникают у них в процессе самостоятельной работы.

6. Перечень основной и дополнительной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Яблонский С. В. Введение в дискретную математику: Учебное пособие для вузов. М.: Высшая школа, 2003. 384с.
2. Хаггарти Р. Дискретная математика для программистов: учеб. пособие для вузов. 2-е доп. изд. М.: Техносфера, 2005. 399 с.
3. Шептунов М. В. Дискретная математика для бакалавриата: учеб. пособие для вузов. М.: Горячая линия - Телеком, 2017. 114 с.
4. Ахо, Сети Р., Ульман Дж. Компиляторы: принципы, техника реализации и инструменты. М., 2001.
5. Рублев, В.С. Основы теории алгоритмов: учеб. пособие для вузов. М.: Научный мир, 2008. 127 с.
6. Котов В.Е., Сабельфельд В.К. Теория схем программ. М.: Наука, 1991.
7. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. М.: Вильямс, 2012. 1290 с.
8. Вирт Н. Алгоритмы и структуры данных. 2-е изд., испр. СПб.: Невский Диалект, 2001. 352с.
9. Кнут Д. Искусство программирования. Т. 1 – 3. М., СПб., Киев: ИД «Вильямс», 2000.
10. Введение в криптографию / Под ред. В.В. Яценко. СПб.: МЦНМО, 2001.
11. Дейт К.Дж. Введение в системы баз данных. М.: Вильямс, 1999.

б) дополнительная литература

1. Горелов В. П. , Горелов С. В. , Сальников В. Г. Докторантам, аспирантам, соискателям учёных степеней и учёных званий: практическое пособие. М.: Директ-Медиа, 2016. http://biblioclub.ru/index.php?page=book_view_red&book_id=428233
2. Клименко А. В. , Несмелова М. Л. , Пономарев М. В. Инновационное проектирование оценочных средств в системе контроля качества обучения в вузе: учебное пособие. - М.: Прометей, 2015. http://biblioclub.ru/index.php?page=book_view_red&book_id=437272
3. Татур Ю. Г. Высшее образование: методология и опыт проектирования: учебно-методическое пособие. - М.: Логос, 2006. http://biblioclub.ru/index.php?page=book_view_red&book_id=84742
4. Дейтел Г. Введение в операционные системы. М.: Мир, 1987.
5. Когаловский М.Р. Энциклопедия технологий баз данных. М.: Финансы и статистика, 2002.
6. Компьютерные сети. Учебный курс Microsoft Corporation, 1997.
7. Матфик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
8. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.
9. Лукьянов А. В. Современные операционные системы: метод. указания. Ярославль: ЯрГУ, 2012. 43 с.
10. Назаров С. В., Широков А. И. Современные операционные системы: учеб. пособие для вузов. 2-е изд., испр. и доп. М.: БИНОМ. Лаборатория знаний, 2013. 367 с.
11. Дадян Э. Г., Зеленков Ю. А. Методы, модели, средства хранения и обработки данных: учебник для вузов. М.: Вузовский учебник; ИНФРА-М, 2017. 168 с.
12. Внуков А. А. Защита информации: Учебное пособие. 2-е изд. М.: Издательство Юрайт, 2017. 261 с.
13. Седжвик Р. Фундаментальные алгоритмы на C++. М.: ДиаСофтЮП, 2002. 687 с.
14. Таненбаум Э. Современные операционные системы. 3-е изд. СПб.: Питер, 2014. 1115 с.
15. Лесковец Ю., Раджараман А., Ульман Д. Анализ больших наборов данных. М.: ДМК Пресс, 2016. 497 с.
16. Парфенов Ю. П. ПОСТРЕЛЯЦИОННЫЕ ХРАНИЛИЩА ДАННЫХ. Учебное пособие для вузов; под науч. ред. Папуловской Н.В.: 2019 <https://biblio-online.ru/viewer/postrelyacionnye-hranilischa-dannyh-438577#page/1>
17. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для вузов. 2-е изд., стер. М.: Академия, 2014. 331 с.

18. Лафоре Р. Объектно-ориентированное программирование в С++. 4-е изд. СПб.: Питер, 2014. 923 с.
19. Шолле Франсуа. Глубокое обучение на Python. — СПб.: Питер, 2018. — 400 с.

в) ресурсы сети «Интернет» (при необходимости)

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
2. Портал государственных образовательных стандартов высшего образования (<http://fgosvo.ru>).
3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав следующие помещения:

- учебные аудитории для проведения лекций;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения промежуточной аттестации;
- помещения для самостоятельной работы.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ЯрГУ.

Автор:

Заведующий кафедрой
теоретической информатики, д.ф.-м.н.
(должность, ученая степень)

_____ Е.В. Кузьмин
(подпись) (Фамилия И.О.)

Приложение №1 к рабочей программе дисциплины
«Специальная дисциплина в соответствии с темой диссертации
на соискание ученой степени кандидата наук»
по научной специальности 1.2.3 Теоретическая информатика, кибернетика

Оценочные материалы
для проведения текущей и/или промежуточной аттестации
аспирантов по дисциплине

1. Контрольные задания и (или) иные материалы,
используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы:

1. Ознакомление с основной и дополнительной литературой по тематике лекций.
2. Ознакомление с периодической литературой по тематике лекций и подготовка обзоров современного состояния проблемы.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к зачету (2 семестр):

1. Алгебра логики. Булевы функции, канонические формы задания булевых функций. Понятие полной системы. Критерий полноты Поста.
2. Исчисление высказываний. Общезначимость, доказуемость. Теорема о полноте.
3. Исчисление предикатов первого порядка. Понятие интерпретации. Выполнимость и общезначимость формулы первого порядка.
4. Понятие модели. Теорема о полноте исчисления предикатов первого порядка.
5. Отношения и функции. Отношение эквивалентности и разбиения. Фактор множества.
6. Отношения частичного порядка. Теоретико-множественное и алгебраическое определения решетки, их эквивалентность. Свойства решеток. Булевы решетки. Полные решетки.

Список вопросов к зачету (3 семестр):

1. Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе.
2. Конечные автоматы. ДКА и НКА. Минимизация конечных автоматов.
3. Алгебры регулярных выражений. Теорема Клини о регулярных языках.
4. Контекстно-свободные языки и грамматики, их свойства. Магазины автоматы.
5. Основы построения трансляторов. Структура оптимизирующего транслятора. Промежуточные представления программы: последовательность символов, последовательность лексем, синтаксическое дерево.
6. Анализ исходной программы в компиляторе. Автоматные (регулярные) грамматики и сканирование, контекстно свободные грамматики и синтаксический анализ, организация таблицы символов программы, имеющей блочную структуру, хеш-функции.
7. Нисходящие (LL(1)-грамматики) и восходящие (LR(1)-грамматики) методы синтаксического анализа. Атрибутные грамматики и семантические программы, построение абстрактного синтаксического дерева.

Список вопросов к зачету (4 семестр):

1. Понятие алгоритма и его уточнения: машины Тьюринга, нормальные алгоритмы Маркова, рекурсивные функции. Эквивалентность данных формальных моделей алгоритмов.
2. Понятие об алгоритмической неразрешимости. Примеры алгоритмически неразрешимых

- проблем.
3. Понятие сложности алгоритмов. Классы P и NP. Полиномиальная сводимость задач. Теорема Кука об NP-полноте задачи выполнимости булевой формулы. Примеры NP-полных задач.
 4. Подходы к решению NP-полных задач. Точные и приближенные комбинаторные алгоритмы.
 5. Примеры эффективных (полиномиальных) алгоритмов: быстрые алгоритмы поиска и сортировки; полиномиальные алгоритмы для задач на графах и сетях (поиск в глубину и ширину, о минимальном остове, о кратчайшем пути, о назначениях).

Список вопросов к экзамену.

Кандидатский экзамен по специальной дисциплине проводится устно по экзаменационным билетам.

Каждый экзаменационный билет содержит три вопроса.

На подготовку к ответу дается от 60 до 120 минут.

1. Булевы функции, канонические формы задания булевых функций.
2. Понятие полной системы. Критерий полноты Поста.
3. Исчисление высказываний. Общезначимость, доказуемость. Теорема о полноте.
4. Исчисление предикатов первого порядка. Понятие интерпретации. Выполнимость и общезначимость формулы первого порядка.
5. Понятие модели. Теорема о полноте исчисления предикатов первого порядка.
6. Отношения и функции. Отношение эквивалентности и разбиения. Фактор множества.
7. Отношения частичного порядка. Теоретико-множественное и алгебраическое определения решетки, их эквивалентность. Свойства решеток. Булевы решетки. Полные решетки.
8. Формальные языки и способы их описания. Классификация формальных грамматик. Их использование в лексическом и синтаксическом анализе.
9. Конечные автоматы. ДКА и НКА. Минимизация конечных автоматов.
10. Алгебры регулярных выражений. Теорема Клини о регулярных языках.
11. Контекстно-свободные языки и грамматики, их свойства. Магазиновые автоматы.
12. Структура оптимизирующего транслятора. Промежуточные представления программы: последовательность символов, последовательность лексем, синтаксическое дерево.
13. Анализ исходной программы в компиляторе. Автоматные (регулярные) грамматики и сканирование, контекстно-свободные грамматики и синтаксический анализ, организация таблицы символов программы, имеющей блочную структуру, хеш-функции.
14. Нисходящие (LL(1)-грамматики) и восходящие (LR(1)-грамматики) методы синтаксического анализа. Атрибутные грамматики и семантические программы, построение абстрактного синтаксического дерева.
15. Понятие алгоритма и его уточнения: машины Тьюринга, нормальные алгоритмы Маркова, рекурсивные функции.
16. Эквивалентность различных формальных моделей алгоритмов.
17. Понятие об алгоритмической неразрешимости. Примеры алгоритмически неразрешимых проблем.
18. Понятие сложности алгоритмов. Классы P и NP. Полиномиальная сводимость задач.
19. Теорема Кука об NP-полноте задачи выполнимости булевой формулы.
20. Примеры NP-полных задач, подходы к их решению. Точные и приближенные комбинаторные алгоритмы.
21. Примеры эффективных (полиномиальных) алгоритмов: быстрые алгоритмы поиска и сортировки; полиномиальные алгоритмы для задач на графах и сетях (поиск в глубину и ширину, о минимальном остове, о кратчайшем пути, о назначениях).
22. Основные понятия реляционной и объектной моделей данных. Теоретические основы реляционной модели данных. Реляционная алгебра, реляционное исчисление. Функциональные зависимости и нормализация отношений.
23. Основные структуры данных, алгоритмы обработки и поиска. Сравнительная характеристика методов хранения и поиска данных. Методы индексирования. Основные принципы управления транзакциями, журнализацией и восстановлением.
24. Постреляционные базы данных (NoSQL).
25. Интеллектуальные системы машинного обучения. Machine Learning.
26. Коды с исправлением ошибок. Алфавитное кодирование. Методы сжатия информации.
27. Задачи обеспечения конфиденциальности и целостности информации. Теоретико-

информационный и теоретико-сложностный подходы к определению криптографической стойкости.

28. Системы шифрования с открытым ключом (RSA). Цифровая подпись. Методы генерации и распределения ключей.

2.1 Описание процедуры выставления оценки

По итогам зачета выставляется одна из оценок: «зачтено», «незачтено».

Правила выставления оценки на зачете:

Устный ответ студента на зачете оценивается по 2-х балльной системе.

Отметка «зачтено» ставится, если:

- знания отличаются глубиной и содержательностью, дается полный исчерпывающий ответ, как на основные вопросы к зачету, так и на дополнительные;
- аспирант свободно владеет научной терминологией;
- ответ аспиранта структурирован, содержит анализ существующих теорий, научных школ, направлений и их авторов;
- ответ аспиранта логично и доказательно раскрывает проблему, предложенную для решения;
- ответ аспиранта характеризуется глубиной, полнотой и не содержит фактических ошибок;
- ответ аспиранта иллюстрируется примерами, в том числе из собственной научно-исследовательской деятельности;
- аспирант демонстрирует умение аргументировано вести диалог и научную дискуссию;
- аспирант демонстрирует навыки поиска и обработки научной информации и экспериментальных данных.

Отметка «незачтено» ставится, если:

- ответ аспиранта обнаружил незнание или непонимание сущностной части дисциплины;
- содержание вопросов не раскрыто, допускаются существенные фактические ошибки, которые аспирант не может исправить самостоятельно;
- на большую часть дополнительных вопросов по содержанию зачета аспирант затрудняется дать ответ или не дает верных ответов;
- аспирант не демонстрирует навыки поиска и обработки научной информации и экспериментальных данных.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется аспиранту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом дисциплины; осуществляет межпредметные связи; умеет связывать теорию с практикой. Аспирант дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует научную терминологию.

Оценка «Хорошо» выставляется аспиранту, ответ которого на экзамене в целом соответствует указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются аспирантом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется аспиранту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. При ответах аспирант допускает ошибки в определении и раскрытии отдельных понятий, формулировке положений, которые аспирант затрудняется исправить самостоятельно.

При аргументации ответа аспирант не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется аспиранту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой, не устанавливает межпредметные связи; допускает грубые ошибки при определении сущности раскрываемых понятий, явлений, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов аспиранта.

Оценка «Неудовлетворительно» выставляется также аспиранту, который взял экзаменационный билет, но отвечать отказался.