

**Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

УТВЕРЖДАЮ

Проректор по учебной работе,
качеству образования – первый

проректор



_____ Т.А. Хагуров

_____ 09 _____ 2019 г.

**ПРОГРАММА
ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ
ПО ТЕОРИИ ПРОГРАММНЫХ СИСТЕМ**

(для поступления на направление подготовки магистратуры
02.04.02 – Фундаментальная информатика и информационные технологии)

г. Краснодар
2019 г.

Программа вступительного испытания
по теории программных систем
для поступающих на направление подготовки магистратуры
02.04.02 – Фундаментальная информатика и информационные технологии

Дискретная математика

Совершенная дизъюнктивная нормальная форма представления булевых функций. Построение СДНФ по таблице истинности. Сокращенная. Совершенная конъюнктивная нормальная форма представления булевых функций. Построение СКНФ по таблице истинности. Задача минимизации нормальных форм булевых функций. Полнота и замкнутость множеств булевых функций. Классы булевых функций, сохраняющих 0, сохраняющих 1. Самодвойственные и монотонные булевы функции. Класс линейных булевых функций. Формулировка теоремы Поста. Основные тавтологии исчисления высказываний. Аксиомы и правила вывода исчисления высказываний. Понятие предиката. Логические и кванторные операции над предикатами. Формулы над предикатами. Равносильность формул, нормальные формы над предикатами. Правила комбинаторики и комбинаторные объекты (сочетания, размещения, перестановки). Основные понятия теории графов. Изоморфизм. Отдельные виды графов (полные, вполне несвязные, простые цепи, простые циклы, полные двудольные), соотношение между количеством вершин и ребер. Деревья, соотношение между количеством вершин и ребер (доказательство). Связность графов, мосты и точки сочленения. Неравенства для вершинной и реберной связности. Понятие планарности графа. Соотношение между количеством вершин, ребер и граней в плоском графе. Теорема Понтрягина – Куратовского. Род графа. Раскраски графов. Хроматическое число, теорема о четырех красках.

Анализ сложности алгоритмов

Понятия временной и емкостной сложности алгоритма. Функции сложности, сложность данных. Минимальная, максимальная и средняя оценки сложности. Методы анализа временной сложности алгоритмов, содержащих повторяющиеся действия (циклы типа for). Методы анализа временной сложности алгоритмов, содержащих повторяющиеся действия (циклы типа while, repeat). Анализ сложности рекурсивных алгоритмов. Линейная рекурсия, нелинейная рекурсия, рекуррентные уравнения для функций сложности. Классы сложности задач. Классы задач полиномиальной сложности и класс NP. Сложность задачи перемножения квадратных матриц размера $n \times n$. Примеры задач из класса NP. Гипотеза $P \neq NP$. NP-полные задачи.

Архитектура вычислительных систем и низкоуровневые языки

Системы адресации в ЭВМ и структуры машинных команд. Регистры, их назначение. Система команд архитектуры Intel. Язык ассемблера архитектуры Intel: описание данных, арифметические команды, команды управления.

Объектно-ориентированное программирование

Наследование в объектно-ориентированном программировании. Инкапсуляция в объектно-ориентированном программировании. Полиморфизм в объектно-ориентированном программировании.

Параллельное программирование

Основные понятия и обозначения сетей Петри. Свойства сетей Петри. Применение сетей Петри для моделирования взаимодействия параллельных вычислительных процессов. Примеры. Понятие распределенных систем и методы синхронизации в распределенных системах.

Типы данных в языках программирования

Простые и сложные типы данных в языках программирования. Пояснить примерами основное назначение. Примеры языков, поддерживающих различные системы типизации. Типы данных, реализуемые аппаратно.

Формальные грамматики, языки и методы трансляции

Понятие формальной грамматики. Правила вывода, вывод, сентенциальная форма, предложение, язык. Понятие синтаксического дерева. Основные атрибуты. Связь вывода и синтаксического дерева. Восстановление вывода по дереву. Классификация формальных грамматик по Хомскому. Нотация грамматик в Нормальной Бэкусовой Форме (НБФ). Расширение метанотации формальной грамматики символами скобок () и {}. Модифицированная БФ. Понятие конечного распознавателя. Основные нотации представления и описания. Детерминированный конечный распознаватель и его минимизация. Недетерминированный конечный распознаватель и его преобразование к детерминированному конечному распознавателю. Регулярные выражения и система переходов. Преобразование системы переходов к недетерминированному конечному распознавателю. Распознаватели с магазинной памятью. Устройство управления. Описание. Основные этапы трансляции. Назначение, цели и задачи. Лексический анализ. Понятие лексем, основные таблицы, диаграмма лексического сканера. Генерация машинного кода. Основные этапы и средства. Промежуточный язык, основная функция. Обратная польская запись (ОПЗ) как промежуточный язык при генерации машинного кода. Преобразование выражений и операторов в ОПЗ. Преобразование ОПЗ в машинный код. Синтаксический анализ. Цель. Разбор и его виды. Проблемы нисходящего разбора и их связь с представлениями грамматик. Нисходящий разбор по методу направляющих символов. Восходящий разбор. Характерные особенности. Поиск фраз. Характерные особенности формальных грамматик для восходящего разбора.

Криптографическая защита информации в программных системах

Понятие криптосистемы, классификация криптосистем, условие стойкости. Симметричное шифрование: блочные шифры, s-блоки, р-блоки. Шифры Фейстеля и шифры не – Фейстеля. DES. Поточковые шифры. Гаммирование, линейный регистр сдвига и усложнители. Примеры криптосистем. Асимметричное шифрование: общий подход, примеры алгоритмов. Криптографические протоколы: распределение ключей, хеширование, электронная подпись.

Основная литература

1. Новиков Ф.А. Дискретная математика. – СПб: Питер, 2012.
2. Харрари Ф. Теория графов. – М.: Книжный дом «Либроком», 2015.
3. Ахо А., Лам М., Сети Р., Ульман Д. Компиляторы: принципы, технологии и инструментарий: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2014.
4. Миков А.И. Распределенные компьютерные системы и алгоритмы. – Ростов-на-Дону, изд. ЮФУ, 2014.
5. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стенографии. – М.: Горячая линия – Телеком, 2011.

Дополнительная литература

1. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Том 1. Синтаксический анализ. – М.: Мир, 1978.
2. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Том 2. Компиляция. – М.: Мир, 1978.
3. Хантер Р. Основные концепции компиляторов. – М.: Вильямс, 2005.
4. Хоар Ч. Взаимодействующие последовательные процессы. – М.: Мир, 1989.
5. Шнайер Б. Прикладная криптография. криптографии. Алгоритмы, протоколы, исходные тексты на языке Си. М.: Триумф, 2002.