

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

**Национальный исследовательский ядерный университет «МИФИ»
(НИЯУ МИФИ)**

УТВЕРЖДАЮ

Проректор НИЯУ МИФИ

_____ О.В. Нагорнов

«__» _____ 2018 г

Ответственный секретарь
приемной комиссии

_____ И.В. Цветков

«__» _____ 2018 г

Программа вступительного испытания

по направлению подготовки магистров

09.04.01 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»

Форма обучения

Очная

Москва 2018

ОБЩИЕ ПОЛОЖЕНИЯ

Программа вступительного испытания сформирована на основе федеральных государственных образовательных стандартов высшего образования.

Форма проведения испытания:

Вступительное испытание в магистратуру проводится в форме собеседования с обязательным оформлением ответов на вопросы билета в письменном виде. Собеседование проводится с целью выявления у абитуриента объема знаний, необходимых для обучения в магистратуре.

Структура испытания:

Испытание состоит из ответов на вопросы билета и дополнительные вопросы в рамках программы вступительного испытания.

Оценка испытания:

Оценка за собеседование выставляется по 100-балльной шкале. Минимальный балл, необходимый для успешного прохождения собеседования и дальнейшего участия в конкурсе ежегодно устанавливается приемной комиссией НИЯУ МИФИ.

Критерии оценки результатов испытания:

100-95 баллов - даны исчерпывающие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует глубокие теоретические знания, умение сравнивать и оценивать различные научные подходы, пользоваться современной научной терминологией.

94-90 баллов - даны полные, достаточно глубокие и обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания, умение пользоваться современной научной терминологией.

89-85 баллов - даны обоснованные ответы на вопросы, поставленные экзаменационной комиссией, абитуриент демонстрирует хорошие знания.

84-80 баллов - даны в целом правильные ответы на вопросы, поставленные экзаменационной комиссией, при этом абитуриент недостаточно аргументирует ответы.

79-0 баллов – абитуриент демонстрирует непонимание основного содержания теоретического материала, поверхностность и слабую аргументацию суждений или допущены значительные ошибки.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Математические основы информатики и вычислительной техники (ИВТ)

Логические переменные и логические функции. Простые и сложные функции. Элементарные функции от двух переменных.

Понятия полноты (базиса) системы логических функций.

Основные законы алгебры логики. Представление логических функций в базисе «И», «ИЛИ», «НЕ».

Нормальные и совершенные нормальные дизъюнктивные и конъюнктивные формы.

Представление логических функций в базисе «И-НЕ» и «ИЛИ-НЕ».

Системы счисления. Выбор системы счисления. Способы представления чисел (с фиксированной и плавающей запятой) и их форматы.

Зависимость полей форматов чисел от диапазона и точности представления чисел.

Прямой, обратный и дополнительный коды, модифицированные коды: особенности выполнения арифметических операций.

Базовые понятия теории автоматов. Регулярные и контекстно-свободные языки.

Детерминированные и недетерминированные конечные автоматы. Регулярные выражения и их связь с детерминированными конечными автоматами.

Автоматы с магазинной памятью. Понятие грамматики, классификация грамматик по Хомскому.

Алгоритмы разбора (восходящий, нисходящий). Нормальная форма Хомского для контекстно-свободных грамматик, алгоритмы Кока-Янгера-Касами.

Понятие машины Тьюринга и ее применение.

Графы: определение, ориентированный и неориентированный графы, взвешенные графы. Понятие пути в графе, длина пути. Представление графа.

Алгоритмы обхода графа: поиск в ширину, поиск в глубину.

Поиск кратчайшего пути в графе. Алгоритм Дейкстры.

Топологическая сортировка. Поиск сильно связанных компонентов.

Определение вероятности и вероятностного пространства. Определение и свойства условной вероятности.

Вероятность произведения событий. Независимость событий.

Формула полной вероятности. Формулы Байеса.

Определение случайной величины. Функция распределения случайной величины, её свойства. Совместное распределение случайных величин.

Математическое ожидание и дисперсия случайной величины, их свойства. Начальные и центральные моменты случайной величины.

Ковариация, коэффициент корреляции.

Независимость случайных величин. Независимость случайных величин, являющихся функциями от независимых случайных величин.

Проверка статистических гипотез. Понятие статистического критерия. Понятие уровня значимости и статистической мощности.

Ошибки первого и второго рода. Понятие доверительного интервала.

Векторы и матрицы. Операции над векторами и матрицами.

Произведение матриц. Методы «быстрого» умножения матриц, алгоритмы Штрассена и Винограда.

Обратная матрица. Критерий обратимости матрицы. Свойства обратной матрицы.

Ранг матрицы.

Понятие линейной зависимости. Критерий линейной зависимости.

Критерий вырожденности матрицы.

Элементарные преобразования над матрицами. Применение матричных вычислений в ИВТ.

Понятие производной для функций от одной и нескольких переменных.

Дифференцируемость функции, ее дифференциал.

Свойства производной. Производная и дифференциал сложной и обратной функций.

Производные основных элементарных функций. Производные функций, заданных параметрически.

Производные и дифференциалы высших порядков. Понятие частной производной.

Первообразная. Основные свойства первообразной. Таблица первообразных.

Неопределенный интеграл и его основные свойства. Основные правила интегрирования.

Двойные и тройные интегралы. Криволинейные интегралы.

Скалярные и векторные поля. Градиент, дивергенция, ротор.

2. Компьютерные сети

Понятие компьютерной сети. Основные компоненты и понятия. Классификация сетевых инфраструктур.

Понятия топологии сети, различные метрики для оценки сетевых инфраструктур.

Современные топологии компьютерных сетей и принципы построения компьютерных сетей.

Принципы организации сетевого взаимодействия. Понятия стека протоколов.

Сетевые модели DoD и OSI/ISO. Назначение уровней. Примеры протоколов. Межуровневая инкапсуляция данных в сетевых моделях.

Синхронный и асинхронный методы передачи данных. Самосинхронизация.

Методы борьбы с перегрузками в сети. Примеры (ECN, congestion window, buffer-to-buffer credits и т.п.).

Современные протоколы для проводных сетей (Ethernet, FibreChannel, конвергентные сети и т.д.).

Ethernet: задачи, ограничения, структура кадра.

Алгоритм работы прозрачного моста, алгоритм обучения Ethernet-коммутатора.

Дополнительные сервисы канального уровня в сетях Ethernet: виртуальные сети, агрегирование каналов, борьба с петлями коммутации.

Задачи протоколов сетевых уровней на примере протоколов IPv4 и IPv6.

Проблема адресации, схемы адресации, методы автоматического назначения сетевых адресов.

Проблема фрагментации дейтаграмм и ее решение. Структура заголовка протоколов IPv4 и IPv6.

Понятие маршрутизации в компьютерных сетях. Статическая и динамическая маршрутизация.

Понятие таблицы маршрутизации на примере IPv4 сетей. Протоколы динамической маршрутизации, основные понятия и алгоритмы на примере RIPv2 и OSPFv3.

Задачи транспортного уровня. Основы адресации.

Основные протоколы транспортного уровня (TCP, UDP): решаемые задачи и ограничения, структура заголовка.

Основные алгоритмы TCP-протокола: установление/завершение соединения, передача сегментов, действия при потере сегментов, борьба с перегрузками в сети.

Проблемы адресации в глобальных сетях. Понятия доменного имени.

Инфраструктура DNS: принципы адресации и организации инфраструктуры, структура пакета DNS протокола, основные типы доменных записей и их применение.

Понятие трансляции адресов, задачи NAT шлюза и принципы функционирования.

Защита информации в компьютерных сетях. Основные инфраструктурные решения (брандмауэры, VPN-шлюзы) и протоколы.

Стек протоколов IP Security. Основные протоколы (AH, ESP, ISAKMP), их задачи, особенности применения, структура пакетов.

3 Операционные системы

Назначение и функции операционных систем (ОС).

Режимы мультипрограммирования. Планирование в различных режимах. Алгоритмы работы планировщика.

Универсальные операционные системы и ОС специального назначения. Классификация операционных систем.

Модульная структура построения ОС и их переносимость.

Управление процессором. Понятие процесса и ядра. Сегментация виртуального адресного пространства процесса.

Средства защиты информации в ОС. Права доступа.

Файловая система. Средства управления файлами.

Средства обработки сигналов. Понятие событийного программирования.

Средства коммуникации процессов.

Механизм реализации виртуальной памяти. Стратегия подкачки страниц.

4 Базы данных

Понятие базы данных, системы баз данных, системы управления базами данных. Назначение и основные компоненты системы баз данных, системы управления базами данных.

Понятие модели данных. Назначение моделей данных; структурная, целостная и манипуляционная части модели данных. Классификация моделей данных.

Модель данных «сущность – связь»: назначение, основные характеристики, структурные и целостные компоненты.

Сетевая и иерархическая модели данных: общая характеристика, особенности представления структуры данных средствами данных моделей.

Реляционная модель данных: общая характеристика, основные структурные компоненты. Понятие схемы отношения. Представление ограничений целостности средствами реляционной модели данных.

Манипуляционная часть реляционной модели данных. Реляционная алгебра и реляционное исчисление.

Язык SQL: общая характеристика. Средства языка для описания структуры базы данных и ограничений целостности; для модификации данных и формирования запросов к данным.

Проектирование реляционной базы данных. Функциональные зависимости, декомпозиция отношений. Понятие нормализации отношений. Нормальные формы.

Физическая организация базы данных. Организация доступа к данным. Понятие индексов. Разновидности индексов (на основе деревьев, хеш-индексы).

Защита баз данных. Понятие транзакции. Свойства транзакции.

5. Защита информации

Модель криптосистемы с секретным ключом. Абсолютно стойкий шифр. Блочные и поточные шифры. Свойства гаммирования.

Модель криптосистемы с открытым ключом. Односторонние функции. Односторонние функции с секретом. Криптосистема RSA. Ранцевая криптосистема. Криптографические протоколы. Протокол выработки общего секретного ключа. Протокол классической электронной цифровой подписи. Протокол разделения секрета. Протоколы доказательства с нулевым разглашением знаний. Хеш-функции. Требования к качественной хеш-функции. Основные конструкции. Парадоксы дней рождения и атаки на хеш-функции. Задачи защиты информации, решаемые криптографическими методами. Примеры. Причины ненадежности криптосистем. Примеры. Методы защиты информации от случайных деструктивных воздействий. Примеры. Стохастические методы защиты информации. Примеры. Методы контроля целостности информации. Коды MAC, MD5, HMAC. CRC-коды. Разрушающие программные воздействия (РПВ). Виды РПВ. Методы антивирусной защиты. Перспективные методы защиты от РПВ. Скрытые каналы передачи данных. Технологии распределенного реестра.

6. Программирование

Основные этапы решения задач на компьютере. Критерии качества программы. Жизненный цикл программы. Методологии программирования.

Способы записи алгоритма. Программа на языке высокого уровня в соответствии с методологией структурного программирования.

Стандартные типы данных. Логический и физический уровни представления данных. Представление данных различных типов и структур в различных языках программирования.

Инструкции языка программирования для описания алгоритмов. Структура программы в соответствии с методологией структурного программирования.

Рекурсивные определения и алгоритмы. Программирование рекурсивных алгоритмов. Способы конструирования и верификации программ.

Основы объектно-ориентированного программирования. Общая характеристика объектно-ориентированных языков программирования.

Основные понятия объектно-ориентированного подхода. Структура программы в соответствии с методологией объектно-ориентированного программирования.

Назначение и использование механизма перегрузки функций, операторов, на примере некоторого объектно-ориентированного языка программирования.

Использование механизма наследования в объектно-ориентированных языках программирования. Понятие статического и динамического связывания.

Динамические структуры данных на примере линейных списков. Линейный список как абстрактный тип данных.

Литература

1. Гуров В.В., Чуканов В.О. Основы теории и организации ЭВМ. – М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2009. – 272 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2010. – 918 с.
3. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. – М.: НИЯУ МИФИ, 2012. – 400 с.
4. Х.М. Дейтел, П.Дж. Дейтел. Как программировать на С++. 3-е изд. – М.: ЗАО «Издательство БИНОМ», 1998, 2001.
5. Брауде Э.Д. Технология разработки программного обеспечения. – СПб.: Питер, 2004. – 656 с.
6. Таненбаум Э. Современные операционные системы. – СПб.: Питер, 2010. – 1040 с.
7. А.Б. Вавренюк, О.К. Курышева, С.В. Кутепов, В.В. Макаров. Операционные системы. Основы UNIX (практическое руководство): учебное пособие (Высшее образование: Бакалавриат) – М.: ИНФРА-М, 2015. – 184 с.
8. Конноли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение. Теория и практика. Уч. пос. – М.: Издательский дом «Вильямс», 2003. – 1120 с.
9. Л.И. Шустова, О.В.Тараканов. Базы данных: Учебник. – М.: ИНФРА-М, 2016. – 304 с. + доп. Материалы [Электронный ресурс; Режим доступа <http://www.znaniium.com>].
10. Хопкрофт, Джон, Мотвани, Раджив, Ульман, Джеффри, Д. Введение в теорию автоматов, языков и вычислений = Introduction to Automata Theory, Languages, and Computation. — М.: «Вильямс», 2002. — С. 528. — ISBN 0-201-44124-1.
11. Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн. Алгоритмы: построение и анализ, 3-е издание = Introduction to Algorithms, Third Edition. — М.: «Вильямс», 2013. — 1328 с. — ISBN 978-5-8459-1794-2.
12. Вентцель Е.С. Теория вероятностей: Учеб. для вузов. — 6-е изд. стер. — М.: Высш. шк., 1999.— 576 с.
13. Фихтенгольц Г. М. Курс дифференциального и интегрального исчисления (в трёх томах). Издательство: ФИЗМАТЛИТ, 2008.