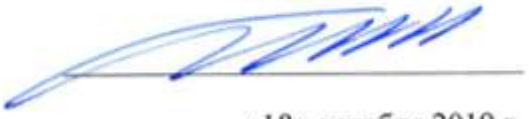
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

Утверждена решением
Ученого Совета факультета
от «18» декабря 2019 года
(протокол № 8)

Декан факультета
вычислительной математики и кибернетики
академик Соколов И.А.



«18» декабря 2019 г.

Программа реализации блока «ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ»

Направление подготовки:
01.04.02 Прикладная математика и информатика
Направленность подготовки (магистерские программы):

"Большие данные: инфраструктуры и методы решения задач"
"Высокопроизводительные вычисления и суперкомпьютерные технологии"
"Математическое и программное обеспечение защиты информации"
"Перспективные вычислительные технологии и сети"
"Прикладные интернет-технологии"
"Программное обеспечение вычислительных сетей"

Уровень подготовки: **магистратура**

Квалификация выпускника: **МАГИСТР**

Форма обучения: **очная**

Москва 2019 г.

1. Наименование: Государственная итоговая аттестация

2. Уровень высшего образования: магистратура

3. Направление подготовки: 01.04.02 Прикладная математика и информатика

Профиль программы:

реализуется для следующих магистерских программ в рамках направления подготовки 01.04.02 Прикладная математика и информатика:

- "Большие данные: инфраструктуры и методы решения задач"
- "Программное обеспечение вычислительных сетей"
- "Математическое и программное обеспечение защиты информации"
- "Высокопроизводительные вычисления и суперкомпьютерные технологии"
- «Прикладные интернет-технологии»
- "Перспективные вычислительные технологии и сети"

4. Место дисциплины в структуре ООП: базовая часть ОПОП, блок 4 «Государственная итоговая аттестация, 4 семестр (очная форма обучения).

5. Перечень компетенций, которыми должен овладеть обучающийся в результате освоения образовательной программы:

Выпускник, освоивший программу магистратуры должен обладать следующими универсальными компетенциями:

УК-1. Способен формулировать научно обоснованные гипотезы, создавать теоретические модели явлений и процессов, применять методологию научного познания в профессиональной деятельности.

УК-2. Способен использовать философские категории и концепции при решении социальных и профессиональных задач.

УК-3. Способен разрабатывать и реализовывать проекты, предусматривая и учитывая проблемные ситуации и риски на всех этапах выполнения проекта.

УК-4. Способен организовывать и осуществлять руководство деятельностью коллектива (группы) на основе социального и профессионального взаимодействия, вырабатывая и реализуя стратегию совместного достижения поставленной цели.

УК-5. Способен осуществлять письменную и устную коммуникацию на государственном языке Российской Федерации в процессе академического и профессионального взаимодействия с учетом культурного контекста общения на основе современных коммуникативных технологий.

УК-6. Способен осуществлять письменную и устную коммуникацию на иностранном языке (иностранных языках) в процессе межкультурного взаимодействия в академической и профессиональной сферах на основе современных коммуникативных технологий.

УК-7. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.

УК-8. Способен определять и реализовывать приоритеты личностного и профессионального развития на основе самооценки.

Выпускник, освоивший программу магистратуры должен обладать следующими **общепрофессиональными компетенциями:**

ОПК-1. Способен формулировать и решать актуальные задачи в области фундаментальной и прикладной математики.

ОПК-2. Способен совершенствовать и реализовывать новые математические и компьютерные методы решения прикладных задач.

ОПК-3. Способен создавать и анализировать математические модели профессиональных задач, учитывать ограничения и границы применимости моделей, интерпретировать полученные математические результаты.

ОПК-4. Способен комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ОПК-5. Способен представлять результаты профессиональной деятельности в соответствии с нормами и правилами, принятыми в профессиональном сообществе.

Профессиональные компетенции выпускника, освоившего программу магистратуры

Научно-исследовательский тип задач профессиональной деятельности:

ПК-1. Способен в рамках задачи, поставленной специалистом более высокой квалификации, определять теоретическую основу и методологию исследования, разрабатывать план исследования в области прикладной математики и информатики;

ПК-2. Способен в рамках задачи, поставленной специалистом более высокой квалификации, проводить научные исследования и (или) осуществлять разработки в области прикладной математики и информатики с получением научного и (или) научно-практического результата;

ПК-3. Способен готовить отдельные документы, связанные с проводимой научно-исследовательской работой.

Производственно-технологический тип задач профессиональной деятельности:

ПК-4. Способен модифицировать и применять актуальные алгоритмы компьютерной математики, а также реализовывать их в современных программных комплексах.

ПК-5. Способен разрабатывать системное и прикладное программное обеспечение.

ПК-6. Способен разрабатывать и применять современные алгоритмические и программные решения в области информационно-коммуникационных технологий.

6. Объем в зачетных единицах с указанием количества академических или астрономических часов, соотнесенные с планируемыми результатами освоения образовательной программы:

Объем государственной итоговой аттестации составляет 9 зачетных единиц, в том числе 6 зачетные единицы - подготовка и защита выпускной квалификационной работы, 3 зачетные единицы - подготовка и сдача государственного экзамена.

7. Входные требования для прохождения итоговой государственной аттестации:

к государственной итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по соответствующей образовательной программе высшего образования.

8. Содержание государственной итоговой аттестации:

государственная итоговая аттестация обучающихся организаций проводится в форме: государственного междисциплинарного экзамена по магистерской программе, а также защиты выпускной квалификационной работы.

А. Программа государственного междисциплинарного экзамена:

Государственный междисциплинарный экзамен носит комплексный характер, проводится по одной или нескольким дисциплинами (или) модулям образовательной

программы, результаты освоения которых имеют определяющее значение для профессиональной деятельности выпускников.

Б. Программа выпускной квалификационной работы:

Выпускная квалификационная работа представляет собой выполненную обучающимся письменную работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности. Защита выпускной квалификационной работы представляет собой выступление обучающегося с устным докладом перед государственной экзаменационной комиссией, об основных результатах подготовленной выпускной квалификационной работы.

9. Учебно-методические материалы для самостоятельной работы обучающегося к подготовке к государственной итоговой аттестации:

А. Подготовка к государственному междисциплинарному экзамену:

Государственный междисциплинарный экзамен проводится в устной форме. В ходе государственного междисциплинарного экзамена обучающийся должен ответить на поставленные в экзаменационном билете вопросы, разработанные в соответствии с программой проведения государственного междисциплинарного экзамена по соответствующей магистерской программе (см. Приложение).

Б. Подготовка выпускной-квалификационной работы (магистерской диссертации):

Требования к оформлению выпускной квалификационной работы:

Результатом научно-исследовательской деятельности обучающегося является выпускная квалификационная работа, выполненная в соответствии с требованиями «Положения о магистерской диссертации факультета ВМК МГУ имени М.В. Ломоносова» (утверждено на заседании Ученого совета ВМК МГУ имени М.В. Ломоносова 30 ноября 2016 г.).

Типовые вопросы к защите выпускной квалификационной работы:

- Обоснуйте актуальность темы выпускной квалификационной работы.
- В чем состоит практическая значимость, выполненной выпускной квалификационной работы?
- В чем новизна результатов работы?
- Сформулируйте цели и задачи выпускной квалификационной работы.

10. Фонд оценочных средств государственной итоговой аттестации:

Критерии и процедуры оценивания обучающегося на государственной итоговой аттестации:

А. Критерии оценивания на государственном междисциплинарном экзамене:

Для оценки готовности выпускника к видам профессиональной деятельности и степени сформированности компетенций государственная экзаменационная комиссия заслушивает устный ответ обучающегося на вопросы, представленные в экзаменационном билете.

Оценка «отлично» ставится если:

- ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы;

- демонстрируются глубокие знания в области фундаментальных основ прикладной математики и информатики;

- ответ формулируется развернуто и уверенно, содержит четкие формулировки определений и теорем.

Оценка «хорошо» ставится, если:

- ответы на поставленные вопросы излагаются систематизировано и последовательно;
- материал излагается уверенно;
- экзаменуемый обнаруживает твёрдое знание программного материала;
- ответ демонстрирует способность магистранта применять знание теории к решению задач профессионального характера.

Оценка «удовлетворительно» ставится, если:

-допускаются нарушения в последовательности изложения;

-демонстрируется поверхностное знание вопроса;

-имеются затруднения с выводами;

Оценка «неудовлетворительно» ставится, если:

материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний;

обучающийся не понимает сущности процессов и явлений.

Б. Критерии оценивания выпускной квалификационной работы:

Для оценки готовности выпускника к видам профессиональной деятельности и степени сформированности компетенций, государственная экзаменационная комиссия заслушивает выступление обучающегося о подготовленной выпускной квалификационной работе.

оценка «отлично» выставляется за глубокое раскрытие темы, качественное оформление работы, содержательность доклада и презентации;

оценка «хорошо» выставляется при соответствии вышеперечисленным критериям, но при наличии в содержании работы и её оформлении небольших недочётов или недостатков в представлении результатов к защите;

оценка «удовлетворительно» выставляется за неполное раскрытие темы, выводов и предложений, носящих общий характер, отсутствие наглядного представления работы и затруднения при ответах на вопросы;

оценка «неудовлетворительно» выставляется за слабое и неполное раскрытие темы, несамостоятельность изложения материала, выводы и предложения, носящие общий характер, отсутствие наглядного представления работы и ответов на вопросы.

Оценочные средства государственной итоговой аттестации

Показатели достижения результатов обучения при прохождении государственной итоговой аттестации, обеспечивающие определение соответствия (или несоответствия) индивидуальных результатов государственной итоговой аттестации студента поставленным целям и задачам (основным показателям оценки результатов итоговой аттестации) и компетенциям, приведены в таблице.

Код	Наименование компетенции	Сформированные компетенции и показатели оценки результатов	
		Государственный экзамен	Подготовка и защита ВКР
УК-1	Способен формулировать научно обоснованные гипотезы, создавать теоретические модели явлений и процессов, применять методологию научного познания в профессиональной деятельности.		Подготовка и защита ВКР, раздел в ВКР

Код	Наименование компетенции	Сформированные компетенции и показатели оценки результатов	
УК-2	Способен использовать философские категории и концепции при решении социальных и профессиональных задач.		Подготовка и защита ВКР, раздел в ВКР
УК-3	Способен разрабатывать и реализовывать проекты, предусматривая и учитывая проблемные ситуации и риски на всех этапах выполнения проекта.		Подготовка и защита ВКР, раздел в ВКР
УК-4	Способен организовывать и осуществлять руководство деятельностью коллектива (группы) на основе социального и профессионального взаимодействия, вырабатывая и реализуя стратегию совместного достижения поставленной цели.		Подготовка и защита ВКР, раздел в ВКР
УК-5	Способен осуществлять письменную и устную коммуникацию на государственном языке Российской Федерации в процессе академического и профессионального взаимодействия с учетом культурного контекста общения на основе современных коммуникативных технологий.		Подготовка и защита ВКР, раздел в ВКР
УК-6	Способен осуществлять письменную и устную коммуникацию на иностранном языке (иностранных языках) в процессе межкультурного взаимодействия в академической и профессиональной сферах на основе современных коммуникативных технологий.		Подготовка и защита ВКР, раздел в ВКР
УК-7	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.		Подготовка и защита ВКР, раздел в ВКР
УК-8	Способен определять и реализовывать приоритеты личностного и профессионального развития на основе самооценки.		Подготовка и защита ВКР, раздел в ВКР
ОПК-1	Способен формулировать и решать актуальные задачи в области фундаментальной и прикладной математики.	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ОПК-2	Способен совершенствовать и реализовывать новые математические и компьютерные методы решения прикладных задач.	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ОПК-3	Способен создавать и анализировать математические модели профессиональных задач, учитывать ограничения и границы применимости моделей, интерпретировать полученные математические результаты.		Подготовка и защита ВКР, раздел в ВКР

Код	Наименование компетенции	Сформированные компетенции и показатели оценки результатов	
ОПК-4	Способен комбинировать и адаптировать современные информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.		Подготовка и защита ВКР, раздел в ВКР
ОПК-5	Способен представлять результаты профессиональной деятельности в соответствии с нормами и правилами, принятыми в профессиональном сообществе.		Подготовка и защита ВКР, раздел в ВКР
ПК-1	Способен в рамках задачи, поставленной специалистом более высокой квалификации, определять теоретическую основу и методологию исследования, разрабатывать план исследования в области прикладной математики и информатики;	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-2	Способен в рамках задачи, поставленной специалистом более высокой квалификации, проводить научные исследования и (или) осуществлять разработки в области прикладной математики и информатики с получением научного и (или) научно-практического результата;	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-3	Способен готовить отдельные документы, связанные с проводимой научно-исследовательской работой.	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-4	Способен модифицировать и применять актуальные алгоритмы компьютерной математики, а также реализовывать их в современных программных комплексах.	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-5	Способен разрабатывать системное и прикладное программное обеспечение.		Подготовка и защита ВКР, раздел в ВКР
ПК-6	Способен разрабатывать и применять современные алгоритмические и программные решения в области информационно-коммуникационных технологий.	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР

ПРИЛОЖЕНИЕ

ПРОГРАММА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОГО МЕЖДИСЦИПЛИНАРНОГО ЭКЗАМЕНА ПО МАГИСТЕРСКИМ ПРОГРАММАМ

Магистерская программа "Большие данные: инфраструктуры и методы решения задач"

Общая часть

1. Модель цепной реакции в диффузионном приближении. Расчет критической массы реактора.

2. Модель Лотки-Вольтерра. Периодические колебания численности популяций.

3. Раскраски графов, хроматическое число графа. Критерий двухцветности графа. Теорема об оценке хроматического числа графа. Теорема Брукса (только формулировка). ([1] стр. 152-153, 32)

4. Наследственные свойства графов. Теорема об оценке наибольшего числа ребер в графе с наследственным свойством. Теорема о наибольшем числе ребер в графе без треугольников. Теорема Турана (только формулировка). [1] (Литература. Харари Ф. Теория графов. М.: Мир, 1973.)

5. Симплекс-метод для канонической задачи линейного программирования: идея метода и ее реализация, выбор стартовой угловой точки. См. материалы курса на сайте

6. Итерационные методы минимизации: скорейшего спуска, проекции градиента и Ньютона. См. материалы курса на сайте

7. Алгоритмы планирования процессов в современных ОС.

8. Методы синхронизации процессов и методы предотвращения тупиковых ситуаций в операционных системах.

9. Классификации архитектур вычислительных систем. Способы организации высокопроизводительных систем и основные принципы функционирования. Характеристики производительности, реальная и пиковая производительность, ускорение и эффективность.

10. Основные средства разработки для систем с общей и распределенной памятью. Основные характеристики пакетов OpenMP, Posix Threads, MPI, поддержка многопоточности в современном C++.

11. Эталонная модель Взаимодействия Открытых Систем (OSI). Функции уровней. Функции подуровня управления доступом к среде в многоабонентской сети. Назначение устройств объединения сетей: концентраторов, мостов, коммутаторов, маршрутизаторов.

12. Маршрутизация в глобальной компьютерной сети Интернет. Таблицы маршрутизации. Методы продвижения дейтаграмм (Forwarding). Задача выбора маршрутов (Routing): основные алгоритмы, их достоинства и недостатки.

Специальная часть

1. Архитектура распределенной инфраструктуры Hadoop. Парадигма распределенного программирования MapReduce. Архитектура YARN.

2. Общие характеристики NoSQL баз данных, и их преимущества. CAP теорема. Классификация NoSQL баз данных. Архитектура и модель данных HBase.

3. Разрешение сущностей. Выявление дубликатов, удаление дубликатов, установление связей

между сущностями из разных исходных коллекций.

4. Слияние данных. Стратегии разрешения конфликтов. Функции разрешения конфликтов. Слияние данных на основе операции Union. Слияние данных на основе операции Join.

5. Конъюнктивные запросы. Ответы, интерпретация запроса. Поглощение запросов. Ответы с учетом взглядов. Переписывание запросов. Гомоморфизм запросов, теорема о гомоморфизме запросов. Алгоритм проверки поглощения запросов, пример поглощения.

6. Подход Local-As-View к виртуальной интеграции реляционных ресурсов. Bucket-алгоритм переписывания запросов. Корректность переписывания. Примеры локальной и глобальной схем, взглядов (представлений), переписывания запроса.

7. Обмен данными – общая схема, формальная постановка задачи. Порождающие кортежи зависимости (tgd). Универсальные решения в обмене данными. Свойства универсальных решений. Процедура погони.

8. Многомерная модель данных. Факты, измерения, параметры. Иерархия измерений. Подходы к реализации многомерной модели. Схемы звезда и снежинка.

9. Иерархические и спектральные алгоритмы обнаружения сетевых сообществ.

10. Модели эпидемий.

11. Доверительные интервалы для среднего, для доли. Построение доверительного интервала на основе бутстрепа. Связь между проверкой гипотез и доверительными интервалами.

12. Проверка гипотез. Ошибки I и II рода. Достигаемый уровень значимости. Критерий согласия Пирсона (хи-квадрат).

13. Поиск аномалий в данных с помощью методов кластеризации. Постановка задачи. Методы DBSCAN, K-means и другие.

14. Поиск аномалий во временных рядах. Постановка задачи. Авторегрессионная модель ARMA

15. Модели прогнозирования на основе деревьев решений. Алгоритмы CHAID, CART, C4.5: критерии поиска разбиений, параметры ограничения роста и обрубания дерева.

16. Классическая линейная модель регрессии: описание модели, основные ограничения, метод наименьших квадратов

Магистерская программа

"Программное обеспечение вычислительных сетей"

Общая часть

1. Модель цепной реакции в диффузионном приближении. Расчет критической массы реактора.

2. Модель Лотки-Вольтерра. Периодические колебания численности популяций.

3. Раскраски графов, хроматическое число графа. Критерий двухцветности графа. Теорема об оценке хроматического числа графа. Теорема Брукса (только формулировка). ([1] стр. 152-153, 32)

4. Наследственные свойства графов. Теорема об оценке наибольшего числа ребер в графе с наследственным свойством. Теорема о наибольшем числе ребер в графе без треугольников. Теорема Турана (только формулировка). [1] (Литература. Харари Ф. Теория графов. М.: Мир, 1973.)

5. Симплекс-метод для канонической задачи линейного программирования: идея метода и ее реализация, выбор стартовой угловой точки. См. материалы курса на сайте

6. Итерационные методы минимизации: скорейшего спуска, проекции градиента и Ньютона. См. материалы курса на сайте

7. Алгоритмы планирования процессов в современных ОС.

8. Методы синхронизации процессов и методы предотвращения тупиковых ситуаций в операционных системах.

9. Классификации архитектур вычислительных систем. Способы организации высокопроизводительных систем и основные принципы функционирования. Характеристики производительности, реальная и пиковая производительность, ускорение и эффективность.

10. Основные средства разработки для систем с общей и распределенной памятью. Основные характеристики пакетов OpenMP, Posix Threads, MPI, поддержка многопоточности в современном C++.

11. Эталонная модель Взаимодействия Открытых Систем (OSI). Функции уровней. Функции подуровня управления доступом к среде в многоабонентской сети. Назначение устройств объединения сетей: концентраторов, мостов, коммутаторов, маршрутизаторов.

12. Маршрутизация в глобальной компьютерной сети Интернет. Таблицы маршрутизации. Методы продвижения дейтаграмм (Forwarding). Задача выбора маршрутов (Routing): основные алгоритмы, их достоинства и недостатки.

Специальная часть

1. Концепция Глобальной информационной инфраструктуры (GII)

2. Соглашение и спецификация сервиса сетевых протоколов (Рекомендация X210)

3. Средства нотации языка UML для описания статической структуры модели системы (Static Structure diagram). Классификаторы на диаграмме статической структуры. Отношения мужу классификаторами на диаграмме статической структуры.

4. Средства нотации языка UML используемые для описания поведения моделируемой системы. Диаграммы кооперации объектов (Collaboration diagram)

5. Архитектура распределенной инфраструктуры Hadoop. Парадигма распределенного программирования map-reduce. Архитектура YARN. Характеристика языков программирования высокого уровня над Hadoop (Hive, Pig, Jaql).

6. Общие характеристики NoSQL баз данных и их преимущества. CAP теорема. Классификация NoSQL баз данных. Архитектура и модель данных HBase.

7. Стек протоколов TCP/IP. Функции уровней. Основные протоколы, их назначение и основные характеристики.

8. Методы передачи данных, основные понятия: модуляция, цифровое кодирование, мультиплексирование и его виды.

9. Основные понятия и определения, относящиеся к информационной безопасности. Алгоритмы симметричного шифрования.

10. Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. MAC и способы обеспечения целостности сообщения. Алгоритмы RSA и Диффи-Хеллмана. Инфраструктура открытого ключа.

11. Функциональные области сетевого управления. Краткая характеристика, основные задачи, ожидания пользователей.

12. Основные особенности семейства стандартов SNMP. Структура баз данных управляющей информации, поддерживаемые операции, взаимодействие с протоколами нижележащих уровней

13. HTTP протокол: структура, команды, заголовки, поддержка сессий.

14. Java servlets: модель, жизненный цикл, контейнеры, основные классы.

Магистерская программа

"Математическое и программное обеспечение защиты информации"

Общая часть

1. Модель цепной реакции в диффузионном приближении. Расчет критической массы реактора.

2. Модель Лотки-Вольтерра. Периодические колебания численности популяций.

3. Раскраски графов, хроматическое число графа. Критерий двухцветности графа. Теорема об оценке хроматического числа графа. Теорема Брукса (только формулировка). ([1] стр. 152-153, 32)

4. Наследственные свойства графов. Теорема об оценке наибольшего числа ребер в графе с наследственным свойством. Теорема о наибольшем числе ребер в графе без треугольников. Теорема Турана (только формулировка). [1] (Литература. Харари Ф. Теория графов. М.: Мир, 1973.)

5. Симплекс-метод для канонической задачи линейного программирования: идея метода и ее реализация, выбор стартовой угловой точки. См. материалы курса на сайте

6. Итерационные методы минимизации: скорейшего спуска, проекции градиента и Ньютона. См. материалы курса на сайте

7. Алгоритмы планирования процессов в современных ОС.

8. Методы синхронизации процессов и методы предотвращения тупиковых ситуаций в операционных системах.

9. Классификации архитектур вычислительных систем. Способы организации высокопроизводительных систем и основные принципы функционирования. Характеристики производительности, реальная и пиковая производительность, ускорение и эффективность.

10. Основные средства разработки для систем с общей и распределенной памятью. Основные характеристики пакетов OpenMP, Posix Threads, MPI, поддержка многопоточности в современном C++.

11. Эталонная модель Взаимодействия Открытых Систем (OSI). Функции уровней. Функции подуровня управления доступом к среде в многоабонентской сети. Назначение устройств объединения сетей: концентраторов, мостов, коммутаторов, маршрутизаторов.

12. Маршрутизация в глобальной компьютерной сети Интернет. Таблицы маршрутизации. Методы продвижения дейтаграмм (Forwarding). Задача выбора маршрутов (Routing): основные алгоритмы, их достоинства и недостатки.

Специальная часть

1. Формальные модели шифров. Примеры. Симметрические и асимметрические криптосистемы. Стойкость шифров. Совершенные шифры. Теорема Шеннона.

2. Делимость в кольце целых чисел. Алгоритм Евклида. Обоснование криптосистемы RSA.

3. Конечные группы. Смежные классы и фактор-группа. Теорема Лагранжа.

4. Примитивные многочлены. Построение ЛРП максимального периода.

5. Конечные поля. Строение конечных полей. Теорема о примитивном элементе. Алгоритм

вычисления дискретного логарифма.

6. Основы эллиптической криптографии. Группы точек эллиптической кривой. Теорема Хассе.

7. Стандарты шифрования ГОСТ-28147-89 и AES-2001

8. Протоколы аутентификации и ЭЦП. Общие принципы. Стандарты ГОСТ-Р-34-10-94, ГОСТ-Р-34-10-2001, DSS.

9. Протоколы аутентификации и хеш-функции. Хеш-алгоритм HD-5. Стандарты Р-34-10-94 и SHA.

10. Протоколы распределения ключей. Протокол передачи секретных сеансовых ключей. Протокол Kerberos. Открытое распределение секретных ключей.

11. Протоколы разделения секрета. Пороговые схемы. Групповой и индивидуально-групповой протокол разделения секрета.

Магистерская программа

"Прикладные Интернет-технологии"

Общая часть

1. Модель цепной реакции в диффузионном приближении. Расчет критической массы реактора.

2. Модель Лотки-Вольтерра. Периодические колебания численности популяций.

3. Раскраски графов, хроматическое число графа. Критерий двухцветности графа. Теорема об оценке хроматического числа графа. Теорема Брукса (только формулировка). ([1] стр. 152-153, 32)

4. Наследственные свойства графов. Теорема об оценке наибольшего числа ребер в графе с наследственным свойством. Теорема о наибольшем числе ребер в графе без треугольников. Теорема Турана (только формулировка). [1] (Литература. Харари Ф. Теория графов. М.: Мир, 1973.)

5. Симплекс-метод для канонической задачи линейного программирования: идея метода и ее реализация, выбор стартовой угловой точки. См. материалы курса на сайте

6. Итерационные методы минимизации: скорейшего спуска, проекции градиента и Ньютона. См. материалы курса на сайте

7. Алгоритмы планирования процессов в современных ОС.

8. Методы синхронизации процессов и методы предотвращения тупиковых ситуаций в операционных системах.

9. Классификации архитектур вычислительных систем. Способы организации высокопроизводительных систем и основные принципы функционирования. Характеристики производительности, реальная и пиковая производительность, ускорение и эффективность.

10. Основные средства разработки для систем с общей и распределенной памятью. Основные характеристики пакетов OpenMP, Posix Threads, MPI, поддержка многопоточности в современном C++.

11. Эталонная модель Взаимодействия Открытых Систем (OSI). Функции уровней. Функции подуровня управления доступом к среде в многоабонентской сети. Назначение устройств объединения сетей: концентраторов, мостов, коммутаторов, маршрутизаторов.

12. Маршрутизация в глобальной компьютерной сети Интернет. Таблицы маршрутизации. Методы продвижения дейтаграмм (Forwarding). Задача выбора маршрутов (Routing): основные алгоритмы, их достоинства и недостатки.

Специальная часть

1. Типы веб-ресурсов.

2. Языки разметки для описания веб-ресурсов.

3. Каскадные таблицы стилей для формирования веб-страниц.

4. Семейство протоколов TCP/IP.

5. Методы проекирования коммерческих веб-ресурсов.

6. Основные этапы конструирования веб-ресурсов.

7. Веб-серверы.

8. Технологии программирования веб-приложений.

9. Веб-сервисы.

10. Инструментальные средства конструирования веб-ресурсов.

Магистерская программа

"Высокопроизводительные вычисления и суперкомпьютерные технологии"

Общая часть

1. Модель цепной реакции в диффузионном приближении. Расчет критической массы реактора.

2. Модель Лотки-Вольтерра. Периодические колебания численности популяций.

3. Раскраски графов, хроматическое число графа. Критерий двухцветности графа. Теорема об оценке хроматического числа графа. Теорема Брукса (только формулировка). ([1] стр. 152-153, 32)

4. Наследственные свойства графов. Теорема об оценке наибольшего числа ребер в графе с наследственным свойством. Теорема о наибольшем числе ребер в графе без треугольников. Теорема Турана (только формулировка). [1] (Литература. Харари Ф. Теория графов. М.: Мир, 1973.)

5. Симплекс-метод для канонической задачи линейного программирования: идея метода и ее реализация, выбор стартовой угловой точки. См. материалы курса на сайте

6. Итерационные методы минимизации: скорейшего спуска, проекции градиента и Ньютона. См. материалы курса на сайте

7. Алгоритмы планирования процессов в современных ОС.

8. Методы синхронизации процессов и методы предотвращения тупиковых ситуаций в операционных системах.

9. Классификации архитектур вычислительных систем. Способы организации высокопроизводительных систем и основные принципы функционирования. Характеристики производительности, реальная и пиковая производительность, ускорение и эффективность.

10. Основные средства разработки для систем с общей и распределенной памятью. Основные характеристики пакетов OpenMP, Posix Threads, MPI, поддержка многопоточности в

современном C++.

11. Эталонная модель Взаимодействия Открытых Систем (OSI). Функции уровней. Функции подуровня управления доступом к среде в многоабонентской сети. Назначение устройств объединения сетей: концентраторов, мостов, коммутаторов, маршрутизаторов.

12. Маршрутизация в глобальной компьютерной сети Интернет. Таблицы маршрутизации. Методы продвижения дейтаграмм (Forwarding). Задача выбора маршрутов (Routing): основные алгоритмы, их достоинства и недостатки.

Специальная часть

1.Методы статической и динамической балансировки загрузки процессоров: сдваивания, геометрического параллелизма, коллективного решения, конвейерного параллелизма, диффузной балансировки загрузки.

2. Декомпозиция расчетных сеток: критерии и методы.

3. Параллельные алгоритмы сортировки данных.

4. Архитектура нейронной сети: устройство нейрона, связи между нейронами, распространение сигналов между нейронами, типы НС (прямого распространения, рекуррентные)

5. Два режима работы НС (обучение, вычисление): цель и основные принципы. Клеточные автоматы: определение, элементарные клеточные автоматы, классификация Вольфрама, двумерные клеточные автоматы, типы окрестностей, игра "Жизнь", параллельная реализация.

6. Системы Линденмайера: определение, D0L системы, графическая интерпретация, другие типы L-систем: контекстно-свободные, стохастические, параметрические, особенности параллельной реализации.

7. Генетические алгоритмы: операторы генетических алгоритмов, особенности кодирования (двоичное, целочисленное, непрерывное, перестановками), сходимость генетических алгоритмов (теория схем), островная модель, клеточные генетические алгоритмы.

8. Методы роевой оптимизации: понятие роевых алгоритмов, принципы Рейнолдса, метод роя частиц, муравьиные алгоритмы, алгоритм бактериального поиска, пчелиные алгоритмы.

Магистерская программа

"Перспективные вычислительные технологии и сети"

1. Последовательная и параллельная сложность алгоритмов, информационный граф и ресурс параллелизма алгоритмов.

2. Архитектурные особенности графических процессоров, направленные на массивно-параллельные вычисления. Методы эффективной организации параллельных вычислений на графических процессорах.

3. Основные принципы организации оптических и беспроводных систем передачи данных.

4. Сети хранения данных - архитектура и основные сервисы.

5. Принципы организации и основные достоинства MPLS технологии.

6. Программно-конфигурируемые сети (SDN). Основные принципы, архитектура и преимущества. Протокол OpenFlow. Структура OpenFlow контроллера и коммутатора. Примеры применения.

7. Виртуализация сетевых сервисов (NFV). Основные принципы, этапы развития,

архитектура, преимущества. Примеры применения.

8. Качество сервиса в компьютерных сетях: модели распределения ресурсов сети и методы борьбы с перегрузками.

9. Основные подходы математического моделирования компьютерных сетей. Прототипирование компьютерных сетей: преимущества, недостатки, ограничения применимости.

10. Динамическое планирование задач в ИУС РВ. Схемы планирования Rate Monotonic (фиксированные приоритеты) и Earliest Deadline First (динамические приоритеты). Оценка времени отклика задач для схемы Rate Monotonic.

11. Понятие наихудшего времени выполнения программы (WCET). Факторы, влияющие на WCET. Фазы анализа WCET. Использование абстрактной интерпретации для выявления недопустимых путей. Анализ влияния конвейера на время выполнения программы.

12. Архитектура интегрированной модульной авионики (ИМА), её основные преимущества, примеры типов модулей (шина VME). Статико-динамическая схема планирования вычислений в системах ИМА.

13. V-образный жизненный цикл (ЖЦ) программного обеспечения. Основные виды инструментальных средств поддержки ЖЦ, их отнесение к фазам ЖЦ. Структура комплекса стендов для поэтапной интеграции ПО и аппаратуры ИУС РВ на восходящей фазе ЖЦ.

14. Средние и эмпирические операционные характеристики стратегий распознавания (классификаторов, регрессий). Проблема переобучения. Проблема устойчивости решений. Роль обучающей, валидационной и контрольной выборок при построении распознающей системы. Скользящий контроль (кросс-валидация). Регуляризация на примере линейной регрессии.

15. Ансамбли классификаторов. Основные этапы работы типичного базового классификатора, возможность коррекции на разных этапах. Бэггинг и случайные подпространства. Бустинг. Случайный лес как композиция основных подходов к построению ансамбля.

16. Задача кластеризации как фундаментальная задача интеллектуального анализа данных, сопоставление с операцией группирования и задачей классификации. Различные постановки: разбиение, стохастическая, нечёткая, иерархическая, упорядочивание, однокластерная (последовательная). Примеры методов кластеризации для разных постановок.

17. Дискреционные управление доступом. Модели HRU и Take-Grant. Задача проверки безопасности системы защиты от НСД.

18. Методы аутентификации в сети. Протокол аутентификации Kerberos.

19. Пасивные и активные сетевые атаки (снифинг, спуфинг, MITM, имперсонация).

20. Коммуникационные протоколы. Ошибки, возникающие при передаче сообщений. Задача надежного обмена сообщениями. Симметричные протокол скользящего (раздвижного) окна: устройство протокола и обоснование его корректности. Протокол альтернирующего бита.[1, стр. 83-94]

21. Задача маршрутизации. Алгоритм Флойда-Уоршалла построения кратчайших путей в графе. Алгоритм маршрутизации Туэга: описание алгоритма, обоснование его корректностии оценка сложности по числу обменов сообщениями.[1, стр. 113-128]

22. Общие принципы дедуктивной верификации программ. Операционная семантика императивных программ. Формальная постановка задачи верификации программ. Логика Хоара: правила вывода и свойства. Автоматизация проверки правильности программ. [4, с. 4770]

23. Темпоральная логика деревьев вычислений CTL. Синтаксис и семантика CTL. Примеры спецификаций моделей в терминах формул CTL. Темпоральная логика линейного времени PLTL. Синтаксис и семантика PLTL. Свойства живости и безопасности. Ограничения справедливости. Задача верификации моделей (model-checking).[2, с. 55-63]

24. Временные автоматы как формальные модели распределенных систем реального времени. Вычисления временных автоматов. Примеры использования временных автоматов для моделирования встроенных систем. Зеноновские вычисления. Синтаксис и семантика Timed CTL. Задача верификации моделей программ реального времени. Программно-инструментальное средство верификации моделей программ реального времени UPPAAL. [2, 344-353]

25. Дискретные цепи Маркова. Метод вложенных цепей Маркова при исследовании систем массового обслуживания.

26. Процессы гибели и рождения. Исследование марковских систем обслуживания с помощью теории процессов гибели и рождения.

27. Понятие антагонистической игры. Верхнее и нижнее значения конечных и бесконечных антагонистических игр. Седловая точка. Необходимые и достаточные условия существования седловой точки. Теорема Фон Неймана о существовании седловой точки у вогнуто-выпуклых функций

28. Понятие потока в сети. Задача о максимальном потоке. Алгоритмы Форда-Фалкерсона и Карзанова. Теорема о максимальном потоке и минимальном разрезе. Сведение задачи составления допустимого расписания с прерываниями для многопроцессорной системы при заданных директивных интервалах к задаче о максимальном потоке в сети.

29. Псевдополиномиальные алгоритмы решения задач: разбиение, рюкзак, расписание для многопроцессорной системы (число процессоров фиксировано).

30. Метод ветвей и границ на примере минимаксной задачи теории расписаний Приближенныеалгоритмы решения NP-трудных задач: упаковка в контейнеры, рюкзак, коммивояжер, расписание для многопроцессорной системы, вершинное покрытие. Оценки их сложности и погрешности.