

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

УТВЕРЖДЕНА
решением Ученого совета ф-та ВМК
Протокол № 4 от 25.04.2018

Декан факультета
вычислительной математики и кибернетики
академик РАН Моисеев Е.И.



Программа реализации блока
«ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ»

Направление подготовки:

01.04.02 Прикладная математика и информатика

Профили подготовки:

"Большие данные: инфраструктуры и методы решения задач"

"Программное обеспечение вычислительных сетей"

"Математическое и программное обеспечение защиты информации"

"Прикладные Интернет-технологии"

"Технологии параллельного программирования и высокопроизводительные вычисления"

Уровень подготовки: **МАГИСТАТУРА**

Квалификация выпускника: **магистр**

Форма обучения: **очная**

Москва 2018 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"
- "Прикладные Интернет-технологии"
- "Технологии параллельного программирования и высокопроизводительные вычисления"

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:**

- Способность формулировать научно обоснованные гипотезы, создавать теоретические модели явлений и процессов, применять методологию научного познания в профессиональной деятельности (УК-1).
- Готовность к саморазвитию, самореализации, использованию творческого потенциала (УК-2).
- Способность осуществлять письменную и устную коммуникацию на иностранном языке (иностраннных языках) в процессе межкультурного взаимодействия в академической и профессиональной сферах на основе современных коммуникативных технологий (УК-3).
- Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (УК-4).

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

- Способность совершенствовать и реализовывать новые математические и компьютерные методы решения актуальных задач в области фундаментальной и прикладной математики, в том числе руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОПК-1).
- Способность создавать и анализировать математические модели профессиональных задач, учитывать ограничения и границы применимости моделей, интерпретировать полученные математические результаты (ОПК-2).

- Способность с учетом основных требований информационной безопасности комбинировать и адаптировать современные информационные технологии для решения задач в области прикладной математики и информатики, а также для расширения и углубления своих знаний в смежных сферах деятельности (ОПК-3).
- Способность осуществлять письменную и устную коммуникацию на государственном языке Российской Федерации в процессе профессионального и академического взаимодействия, связанного с профессиональной деятельностью, с учетом культурного контекста общения на основе современных коммуникативных технологий (ОПК-4).
- Способность использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов (ОПК-5).

Профессиональные компетенции выпускника, освоившего программу магистратуры

- Способность самостоятельно и в составе научного коллектива проводить научные исследования и получать новые научные результаты на основе обладания фундаментальными знаниями, понимания актуальных концепций, принципов и теорий, связанных с прикладной математикой и информатикой (ПК-1).
- Способность понимать, совершенствовать и применять в научно-исследовательской деятельности современный математический аппарат (ПК-2).
- Способность самостоятельно и в составе производственного коллектива разрабатывать и применять актуальные алгоритмы компьютерной математики, а также реализовывать их в современных программных комплексах (ПК-3).
- Способность комбинировать и адаптировать для целей профессиональной деятельности современные средства разработки программного обеспечения и методы параллельной обработки данных, разрабатывать системное и прикладное программное обеспечение, системы обработки и анализа данных, сетевые технологии (ПК-4).
- Способность структурировать общую схему решения прикладной задачи в соответствии с ее спецификой, а также определить совокупность и особенности применения математических методов и программных решений для каждого из этапов полученной схемы (ПК-5).
- Способность прогнозировать последствия своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций (ПК-6).

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	Способность формулировать научно обоснованные гипотезы, создавать теоретические модели явлений и процессов, применять методологию научного познания в профессиональной деятельности		Подготовка и защита ВКР, раздел в ВКР
УК-2	Готовность к саморазвитию, самореализации, использованию творческого потенциала		Подготовка и защита ВКР, раздел в ВКР
УК-3	Способность 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-4	Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения		Подготовка и защита ВКР, раздел в ВКР
ОПК-1	Способность совершенствовать и реализовывать новые математические и компьютерные методы решения актуальных задач в области фундаментальной и прикладной математики, в том числе руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ОПК-2	Способность создавать и анализировать математические модели профессиональных задач, учитывать ограничения и границы применимости моделей, интерпретировать полученные математические результаты	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ОПК-3	Способность с учетом основных требований информационной безопасности комбинировать и адаптировать современные информационные технологии для решения задач в области прикладной математики и информатики, а также для расширения и углубления своих знаний в смежных сферах деятельности		Подготовка и защита ВКР, раздел в ВКР
ОПК-4	Способность осуществлять письменную и устную коммуникацию на государственном языке Российской Федерации в процессе профессионального и академического взаимодействия, связанного с профессиональной деятельностью, с учетом	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР

	культурного контекста общения на основе современных коммуникативных технологий		
ОПК-5	Способность использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов		Подготовка и защита ВКР, раздел в ВКР
ПК-1	Способность самостоятельно и в составе научного коллектива проводить научные исследования и получать новые научные результаты на основе обладания фундаментальными знаниями, понимания актуальных концепций, принципов и теорий, связанных с прикладной математикой и информатикой	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-2	Способность понимать, совершенствовать и применять в научно-исследовательской деятельности современный математический аппарат	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-3	Способность самостоятельно и в составе производственного коллектива разрабатывать и применять актуальные алгоритмы компьютерной математики, а также реализовывать их в современных программных комплексах	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-4	Способность комбинировать и адаптировать для целей профессиональной деятельности современные средства разработки программного обеспечения и методы параллельной обработки данных, разрабатывать системное и прикладное программное обеспечение, системы обработки и анализа данных, сетевые технологии	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-5	Способность структурировать общую схему решения прикладной задачи в соответствии с ее спецификой, а также определить совокупность и особенности применения математических методов и программных решений для каждого из этапов полученной схемы	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР
ПК-6	Способность прогнозировать последствия своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	Экзаменационный билет	Подготовка и защита ВКР, раздел в ВКР

ПРИЛОЖЕНИЕ

ПРОГРАММА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОГО МЕЖДИСЦИПЛИНАРНОГО ЭКЗАМЕНА ПО МАГИСТЕРСКИМ ПРОГРАММАМ

(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.

Магистерская программа

"Большие данные: инфраструктуры и методы решения задач"

1. Архитектура распределенной инфраструктуры Hadoop. Парадигма

распределенного программирования MapReduce. Архитектура YARN.

- Chuck Lam. Hadoop in Action Tom White. Hadoop: The Definitive Guide, 3rd Edition

- IBM Course: "Hadoop Fundamentals" (BD001)
<https://bigdatauniversity.com/learn/hadoop/>

- Programming Pig: Dataflow Scripting with Hadoop, By Alan Gates, Publisher: O'Reilly Media

- Programming Hive: Data Warehouse and Query Language for Hadoop By Edward Capriolo, Dean Wampler, Jason Rutherglen, Publisher: O'Reilly Media

- Jaql documentation. http://www-01.ibm.com/support/knowledgecenter/SSPT3X_3.0.0/com.ibm.swg.i...

- Материалы лекций: http://synth_serv/synthesis/student/BigData/seminar-hadoop/hadoop2015

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

- Apache HBase web site: <http://hbase.apache.org/>

- George, Lars. HBase The Definitive Guide (O'Reilly 2011)

- "Brewer's CAP Theorem" posted by Julian Browne, January 11, 2009. <http://www.julianbrowne.com/article/viewer/brewers-cap-theorem>

- Материалы лекций: http://synth_serv/synthesis/student/BigData/seminar-hadoop/hadoop2015

3. Разрешение сущностей. Выявление дубликатов, удаление дубликатов, установление связей между сущностями из разных исходных коллекций.

- А.Е. Вовченко, Л.А. Калиниченко, Д.Ю. Ковалев. Методы разрешения сущностей и слияния данных в ETL-процессе и их реализация в среде Hadoop. Информатика и ее применения, т. 8, вып. 4, 2014.

- Peter Christen, Data Matching. Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection. Springer Data-Centric Systems and Applications, 2012

- Материалы лекций: http://synth_serv/synthesis/student/BigData/seminar-information-extracti...

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

- А.Е. Вовченко, Л.А. Калиниченко, Д.Ю. Ковалев. Методы разрешения сущностей и слияния данных в ETL-процессе и их реализация в среде Hadoop. Информатика и ее применения, т. 8, вып. 4, 2014.

- J. Bleiholder, F. Naumann. Data Fusion. ACM Computing Survey 2009.

- Материалы лекций: http://synth_serv/synthesis/student/BigData/seminar-information-extracti...

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.

- Serge Abiteboul, Ioana Manolescu. Web Data Management. Cambridge University Press, 2011. - <http://webdam.inria.fr/Jorge/html/wdmch10.html> (раздел 9.2)
- 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.
- Serge Abiteboul, Ioana Manolescu. Web Data Management. Cambridge University Press, 2011. - <http://webdam.inria.fr/Jorge/html/wdmch10.html> (раздел 9.4)
- 7. Обмен данными – общая схема, формальная постановка задачи. Порождающие кортежи зависимости (tgd). Универсальные решения в обмене данными. Свойства универсальных решений. Процедура погони.
- Ronald Fagin, Phokion G. Kolaitis, Renée J. Miller, Lucian Popa: Data exchange: semantics and query answering. Theor. Comput. Sci. 336(1): 89-124 (2005) - <http://dblab.cs.toronto.edu/project/dataexchange/docs/tcs05.pdf>
- Phokion G. Kolaitis. A Tutorial on Schema Mappings & Data Exchange DEIS '10. -<http://synthesis.ipi.ac.ru/synthesis/student/BigData/master-course-warehousing/DW16-2-DataExchange.pdf>
- 8. Многомерная модель данных. Факты, измерения, параметры. Иерархия измерений. Подходы к реализации многомерной модели. Схемы звезда и снежинка.
- Кристиан Йенсен, Торбен Бэч. Технология многомерных баз данных. <http://www.osp.ru/os/2002/01/180958/>
- Christian S. Jensen, Torben Bach Pedersen, and Christian Thomsen. Multidimensional Databases and Data Warehousing. Morgan & Claypool, 2010. (раздел 2)
- Data Warehouse Design. - <http://synthesis.ipi.ac.ru/synthesis/student/BigData/lectures/DW%204%20Data%20Warehouse%20Design.pdf> (разделы Logical Modeling, Physical Modeling)
- 9. Иерархические и спектральные алгоритмы обнаружения сетевых сообществ.
- М. Newman. Networks: an Introduction. Oxford University Press, 2010. Глава 11.
- 10. Модели эпидемий.
- М. Newman. Networks: an Introduction. Oxford University Press, 2010. Глава 17
- 11. Доверительные интервалы для среднего, для доли. Построение доверительного интервала на основе бутстрепа. Связь между проверкой гипотез и доверительными интервалами.
- Лагутин М. Б. Наглядная математическая статистика. 2007. (Глава 11)
- 12. Проверка гипотез. Ошибки I и II рода. Достижимый уровень значимости. Критерий согласия Пирсона (хи-квадрат).
- Лагутин М. Б. Наглядная математическая статистика. 2007. (Главы 12, 13)
- 13. Поиск аномалий в данных с помощью методов кластеризации.

Постановка задачи. Методы DBSCAN, K-means и другие.

- К. В. Воронцов. Машинное обучение, курс лекций. Курс - <https://goo.gl/uMEYfp>, слайды: <https://goo.gl/poJpyi>, видео: <https://goo.gl/QtdMFz>

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

- С. Aggarwal. Outlier analysis. Springer, 2013. (Глава 8)

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

- Hastie, Tibshirani and Friedman. The Elements of Statistical Learning. – Springer-Verlag, 2009. – 763 pages. <http://statweb.stanford.edu/~tibs/ElemStatLearn/>

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

- Андерсон Т. Введение в многомерный статистический анализ. – М.: Наука, 1963

- Болч К., Хуань К.Дж. Многомерные статистические методы для экономики. – М.: Статистика, 1979.

- Кулаичев А.П. Методы и средства комплексного анализа данных. – М.: Форум-Инфра-М, 2006.

Магистерская программа

"Программное обеспечение вычислительных сетей"

1. Концепция Глобальной информационной инфраструктуры (ГИИ)
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 между 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"

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 MD-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"

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 проектирования 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
"Технологии параллельного программирования и
высокопроизводительные вычисления"

1. Методы статической и динамической балансировки загрузки процессоров: удваивания, 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.