

**АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН (МОДУЛЕЙ)
ООП ВЫСШЕГО ОБРАЗОВАНИЯ – ПРОГРАММЫ МАГИСТРАТУРЫ
Направление подготовки 01.04.02 «Прикладная математика и информатика»**

Направленность программы (магистерская программа)
«Программное обеспечение вычислительных сетей»

Английский язык

Курс английского языка направлен как на дальнейшее развитие таких видов речевой деятельности, как чтение, аудирование, письменная речь в профессионально значимых ситуациях, так и на формирование умений переводческой деятельности, которые также являются частью профессиональной коммуникативной компетенции выпускника. Наибольшее внимание при обучении уделяется продуктивным видам речевой деятельности (письменная речь и говорение), интегративным умениям чтения, аудирования и письменной речи (аннотирование, резюмирование), а также различным видам перевода.

Модуль "Философия"

Современная философия и методология науки

Цель дисциплины – формирование у слушателя целостного видения науки, понимания им специфики научной деятельности, характера исторического развития науки, ее взаимодействия с другими сферами человеческой деятельности.
Задачи дисциплины – заложить теоретические предпосылки для выработки умения анализировать реальную научную деятельность на основе теоретической концепции науки, выявлять специфический характер различных областей науки (специфику понимания строгости, обоснованности, доказательности научного знания, методов его получения, функций научного знания и др.), дифференцировать знание на научное и вненаучное на основе критериев научности.- ориентировать слушателя на понимание исторически изменяющегося характера науки (и ее параметров), восприятия ее за пределами науки в других областях культуры, а также связей науки и общества.- ознакомить с существующими концепциями науки, которые позволяют глубже понимать природу, сущность науки, перспективы развития самой науки, общества, активно использующего науку, и культуру, их породившую.

История и методология прикладной математики и информатики

Целью курса является краткое изложение основных фактов, событий и идей в ходе многовековой истории развития математики в целом и одного из её важнейших направлений – «прикладной» (вычислительной) математики, зарождения и развития вычислительной техники и программирования. В курсе делается попытка представить математику как единое целое, где тесно перемежаются проблемы так называемой «чистой» и «прикладной» математики, граница между которыми зачастую весьма условная. Показывается роль математики и информатики в истории развития цивилизации, Дается характеристика научного творчества наиболее выдающихся учёных - генераторов научных идей. Особое внимание уделяется развитию математики и информатики в России.

Математическое моделирование

Основные задачи и методы анализа данных

В наши дни практически каждый специалист должен иметь представление о возможностях и ограничениях, которые возникают при использовании существующего арсенала методов и технологий анализа данных. Предлагаемый курс должен создать у слушателя представление о задачах и технологиях аналитической деятельности как связь теории и доступного современного инструментария. Рассматриваются основные инструменты прикладной статистики, статистического распознавания, машинного обучения, а также лежащие в их основе математические методы. Развиваются навыки формализации и решения аналитических задач в рамках современных распространенных технологий.

Идентификация и слияние сущностей в больших данных

В настоящем курсе изучаются методы и инструменты интеграции информации из различных источников больших данных (в масштабе Веба, социальных сред (Twitter, LinkedIn, ...), блогов, публикаций в средствах массовой информации, машинных логов, сенсорных данных, и пр.

Большие данные обычно являются неструктурированными (чаще всего текстовыми), слабоструктурированными (например, в виде XML, JSON, баз данных NoSQL). Вместе с тем, образуются также и структурированные большие данные как, например, результат наблюдений (измерений) современными инструментами, накопления многочисленных таблиц в Вебе.

Развитые методы интеграции (ETL) не ориентированы на большие данные. Современные ИТ платформы включают распределенные инфраструктуры типа Hadoop, обеспечивающие параллельную обработку и анализ таких разнотипных больших данных на основе парадигмы MapReduce, при этом методы интеграции (ETL) над Hadoop практически отсутствуют.

В курсе рассматриваются современные методы извлечения сущностей (Entity Resolution) и методы слияния данных (Data Fusion) в разрезе интеграции больших данных. В практической части курса рассматриваются масштабируемые методы, реализуемые на языках Java и HPL, и выполняющиеся в распределенных инфраструктурах типа Hadoop.

Введение в криптографию

1. Основные понятия и задачи криптографии. Криптографические методы обеспечения информационной безопасности. Формальное определение шифра. (криптосистемы). Алгебраическая и вероятностная модели шифра. Симметрические и асимметрические шифры. Шифры простой замены и перестановки, криптосистемы RSA и Эль Гамала. Табличное гаммирование. Понятие односторонней функции и односторонней функции с секретом.

2. Краткий исторический обзор развития криптографии. Шифры атбаш, Считала, табличка Энея, квадрат Полибия. Шифр Цезаря, шифровальный диск Альберти. Шифр простой биграммной замены де ла Порта.. Шифры Виженера, Ришелье, Наполеона. Шифр Вернама, дисковый шифратор «Энигма».

3. Блочные и поточные шифры. Математическая модель шифра замены. Атаки на шифр, стойкость шифра, совершенный шифр, теорема Шеннона, имитостойкость шифров. Режимы использования блочных шифров. Стандарты шифрования ГОСТ 28147-89 и DES.

4. Универсальные методы криптоанализа. Метод полного перебора. Аналитический метод. Метод «встреча по середине». Метод «разделяй и побеждай». Методы криптоанализа при неравновероятной гамме. Расстояние единственности, теоремы Шеннона. Перекрытие гаммы. Корреляционные атаки на поточные шифры. Криптоанализ шифра Виженера.

5. Статистические методы криптоанализа. Линейный и дифференциальный криптоанализ блочных шифров. Примеры атак на блочные шифры.

6. Криптографические протоколы. Протоколы аутентификации электронно-цифровой подписи (ЭЦП). Формальная модель протокола ЭЦП на основе односторонней функции. Понятие хэш-функции .. Методы построения хэш-функций. Элементарные свойства хэш-функций. Ключевые и бесключевые хэш-функции. Метод коллизий для хэш-функций.

7. Ключевые системы. Управление ключами. Предварительное распределение секретных ключей. Пересылка ключей. Протокол открытого распределения ключей. Инфраструктура открытых ключей. Центр сертификации открытых ключей. Система управления сертификатами. Федеральная инфраструктура открытых ключей.

8. Криптографические средства и методы защиты данных программного обеспечения. Основные требования обеспечения безопасности данных в программных системах. Средства и методы защиты. Ключевая система и ключевые носители. Контроль целостности программного обеспечения.

Модуль Программное обеспечение современных вычислительных комплексов

Современные операционные системы

В курсе «Современные операционные системы» рассматриваются базовые концепции функционирования операционных систем, утилиты, обеспечивающие подсистемы, процессы и

управление процессами, управление файловыми системами и устройствами хранения данных, элементы обеспечения безопасности и защиты от несанкционированного доступа.

Курс «Современные операционные системы» направлен на формирование у студентов компетенций, необходимых для решения задач системного администрирования, включающих в себя:

- самостоятельное администрирование операционных систем;
- управление учетными записями и правами пользователей;
- решение проблем функционирования операционных систем.

Сетевые технологии

Задачи курса «Сетевые технологии» - формирование у слушателей структурированного представления о современных сетевых технологиях, включая принципы передачи данных в современных сетях, технологии локальных и глобальных сетей, проблемы информационной безопасности в современных сетях и основные подходы к их решению, овладение слушателями терминологией, необходимой для описания современных сетевых технологий. Курс является вводным к другим курсам магистратуры: технологии сети Интернет, телекоммуникационные технологии, математические основы безопасности ИТ.

Распределенное и параллельное программирование

Количество ядер в современных процессорах уже измеряется десятками, в графических ускорителях – тысячами, а в суперкомпьютерах – миллионами. Многоядерные вычислительные системы широко применяются в машинном обучении, науках о материалах, биоинформатике, автоматизации проектирования, вычислительной химии и физике. Эффективно использовать эту значительную вычислительную мощность – непростая задача, требующая применения современных подходов, составляющих основное содержание предлагаемого спецкурса.

Целью освоения дисциплины «Архитектура и программное обеспечение высокопроизводительных вычислительных систем» является получение студентами знаний в области параллельных и распределенных вычислений, выработка у студентов навыков разработки, отладки и исследования производительности параллельных программ. Задачи дисциплины состоят в изучении и практическом освоении современных суперкомпьютерных технологий..

Профессиональный

Язык Java и разработка Java-приложений

Цель курса - дать слушателям знания и навыки в разработке систем на языке программирования Java. Данный курс является предварительным курсом для курсов основанных на технологиях использующих язык Java. Для иллюстрации возможностей языка Java и получения практических навыков в работе с языком Java используется проект по разработке настольных игр: разновидностей шахмат и других игр, а также алгоритмов для этих игр. Для изучения возможностей программирования пользовательского интерфейса системы используется предложенная фирмой IBM библиотека SWT. Эта библиотека используется как основа для построения интерфейса пользователя в среде разработки Eclipse.

Управление разно-структурированными большими данными

В курсе рассматривается специальный вид стека для параллельных архитектур оперирования данными в аналитических приложениях Big Data. Эти архитектуры полностью отличаются от архитектур суперкомпьютеров. Параллельная архитектура оперирования данными основана на кластере процессоров, обычно соединяемых быстрой сетью (например, гигабитной Ethernet). Центральной в таком архитектурном стеке является парадигма программирования, называемая MapReduce. Свободно распространяемая реализация такого стека включает HDFS, Hadoop Distributed File System, и поддержку MapReduce (в Hadoop). Такие архитектуры поддерживают разно-структурированные данные, которые могут быть представлены в разнообразных моделях данных (структурированных, слабоструктурированных, неструктурированных).

В курсе рассматриваются основные идеи и подходы параллельных архитектур оперирования разно-структурированными данными. Рассматриваются вопросы реализации различных алгоритмов в среде map-reduce (таких как матрично-векторное умножение, поддержка SQL-подобных операций и

операций реляционной алгебры), сравнения реализации таких операций с традиционными. Map-reduce программирование в курсе изучается применяя собственно язык map-reduce Hadoop'a наряду с декларативными языками над Hadoop'ом (такими как PigLatin, Hive, Jaql (IBM)).

Также в курсе рассматриваются перспективные методы анализа данных (в дополнении к MapReduce) в среде Hadoop 2.0, основанные на парадигме распределения ресурсов YARN (Yet Another Resource Negotiator). Yarn поддерживает выполнение любых программ, которые могут выполняться параллельно, и позволяет уйти от традиционной парадигмы программирования в Hadoop (map-shuffle-reduce). Это позволяет эффективно программировать сложные задачи, такие как ETL, обработку графов (Giraph), массивно параллельные алгоритмы машинного обучения и моделирования в среде Hadoop. Данная область является широко перспективной и открыта для множества исследований.

В комбинации с Hadoop'ом в курсе рассматриваются базы данных NoSQL (такие как HBase). Их использование совместно с Hadoop'ом изучается на примерах приложений. Подходы к интеграции Hadoop'a в хранилище данных также рассматриваются. В курсе рассматриваются методы применения аналитики данных над Hadoop'ом на примере методов извлечения информации из текстовых документов.

Анализ информационных технологий

Курс посвящен изучению современного состояния международной системы стандартов в области информационных технологий (ИТ), образующей научно-методологический базис области ИТ и играющей основополагающую роль в процессах цифровизации мировой экономики и жизни социума, а также изучению принципов организации и функционирования международной системы стандартизации. В курсе подробно рассматривается современное состояние системы международных стандартов в сфере подготовки ИТ-кадров с актуальными профессиональными цифровыми навыками. Приводится описание модели цифровых навыков, а также средств и стандартов их спецификации, рассматриваются современные подходы к развитию цифровых навыков. Значительное внимание уделяется изучению концепции открытых систем и связанных с ней базовых стандартов, а также практической реализации этой концепции посредством аппарата профилирования и тестирования конформности (соответствия), при этом особое внимание уделяется методологическим аспектам и стандартам, направленным на решение проблемы интероперабельности и масштабируемости информационных систем, облачных сервисов, приложений Интернета Вещей. Значительную часть курса занимает изучение процессных стандартов системной и программной инженерии, включая стандарты процессов жизненного цикла систем (ГОСТ Р ИСО/МЭК 15288), стандарты процессов жизненного цикла программных средств (ГОСТ Р ИСО/МЭК 12207) и стандарты управления ИТ-услугами (ГОСТ Р ИСО/МЭК 20000). Отдельная тема посвящена изучению стандартов менеджмента качества ГОСТ Р ИСО/МЭК 9000, 9001, 9004, 10013. Рассматриваются модель системы менеджмента качества (СМК), основные принципы построения СМК для образовательных организаций. Завершается курс обзором онтологических и эталонных моделей систем стандартов таких областей, как, Интернет Вещей, Умные города, Большие Данные, определяющих концептуальный контекст для разработки приложений цифровой экономики.

Объектно-ориентированные CASE-технологии

В курсе дается систематическое изучение основных понятий современных объектно-ориентированных CASE-систем. Рассматривается графическая нотация разработанного консорциумом OMG (Object Management Group) унифицированного языка моделирования UML (Unified Modeling Language), являющегося фактическим стандартом графических обозначений, используемых в методах объектно-ориентированного анализа и проектирования программного обеспечения. В курсе также изучается метамодель языка UML (модель самого языка UML, описанная средствами языка UML) используемая для описания семантики языка UML. Классы метамодели определяют структуру репозитория объектно-ориентированных CASE-систем, обеспечивая переносимость моделей проектируемого программного обеспечения между различными CASE-системами. Цель курса - дать целостные знания о стандартном языке CASE-систем – унифицированном языке моделирования UML. Позволить учащимся использовать язык UML для проектирования программных систем с помощью CASE-инструментов. Дать учащимся необходимые

знания и навыки, позволяющие им принять участие в реализации языка UML в составе CASE-инструментов и других систем программирования.

Технологии сети Интернет

Задачами курса являются: формирование у слушателей целостного представления об устройстве и функционировании сети Интернет, аппаратных и программных компонентах, обеспечивающих работу Интернет, и их взаимосвязях, понимания терминологии, формирование начальных навыков создания фрагментов сети Интернет и управления ими.

В курсе излагаются и обсуждаются основные технологии и протоколы сети Интернет. Курс состоит из трех больших тем: обеспечение передачи данных в сети Интернет, базовые протоколы передачи данных, информационная безопасность в сети Интернет, основные проблемы, алгоритмы и протоколы, всемирная паутина, ее протоколы, языки и технологии.

Проводится лабораторная работа по настройке статической маршрутизации, службы имен (DNS) и межсетевого экрана.

Стандарты, протоколы, сервисы интернета вещей

В результате изучения дисциплины студент должен: Получить базовые сведения по архитектуре систем Интернета Вещей (IoT), существующим и разрабатываемым стандартам Интернета Вещей, сетевым протоколам, сбору и агрегации данных в системах Интернета Вещей, анализу данных и системам безопасности. В курсе изучаются основные стандарты и открытые решения в области Интернета Вещей, основные сетевые протоколы, применяемые в системах Интернета Вещей, а также методы обеспечения безопасности. Результаты обучения: понимание принципов построения систем IoT, умение взаимодействовать с заказчиками систем IoT, понимание основных элементов систем IoT и умение строить архитектуру для реализации систем IoT, умение взаимодействовать с программистами при реализации систем IoT. Умение разбираться в методах обработки и анализа информации, применяемых в системах IoT, понимание организации систем кибербезопасности в IoT

Современные технологии баз данных

В курсе рассматриваются вопросы, связанные с моделями данных. Рассматриваются такие модели данных как структурированные файлы, иерархические и сетевые модели, объектные базы данных, реляционная модель представления данных, а также современные NoSQL базы данных. Слушатели курса в итоге должны получить знания по базовым элементам, лежащим в основе моделирования данных и выборе подходящих моделей в разработках приложений.

Рассматриваются положения, лежащие в основе реляционной модели данных, как наиболее часто используемой в коммерческих приложениях. Операции реляционной алгебры, нормальные формы. SQL – как основа взаимодействия с реляционными базами. Определение данных (DDL), операции модификации данных (DML). Поддержка SQL операций на уровне сервера. Курсоры, триггеры, сохраненные процедуры. Планы и оптимизация запросов. Доступ к данным из прикладных приложений DB Lib API, Embedded SQL. Стандартные интерфейсы для доступа, такие как JDBC, ODBC, OLE DB, ADO, а также ORM системы. При рассмотрении распределенных базы данных описываются многофазные транзакции и репликация данных. Раздел посвященный многоуровневым приложениям включает рассмотрение 3-х уровневых систем (серверов приложений) и мониторов транзакций. Раздел посвященный NoSQL системам включает рассмотрение распределенных файловых систем (Apache Hadoop), а также таких моделей данных, как key-value системы, модель хранения данных на базе семейства столбцов, документарные и графовые базы.

Тестирование безопасности компьютерных систем

В курсе рассматриваются основные методы и технологии, которые методы и технологии, которые используются "этичными" хакерами в анализе защищенности компьютерных систем. Подробно рассматриваются вопросы уязвимости веб-приложений, а также изучаются классические сетевые атаки на компоненты современных сетей связи.