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

Направленность программы (магистерская программа)
«Математическое и программное обеспечение защиты информации»

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.

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.

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.

Модуль Математическое моделирование

Непрерывные математические модели

Излагаются и обсуждаются методы математического моделирования физических, биологических и экономических процессов. Выводятся уравнения, составляющие основу рассматриваемых моделей. Обсуждаются постановки задач. Подробно изучаются методы решения задач, которые возникают в процессе моделирования этих процессов. Приводиться также обзор некоторых результатов в области суперкомпьютерного моделирования.

Дискретные и вероятностные модели

В части посвященной Дискретным моделям рассматриваются способы представления таких функций и их основные свойства, а также вопросы полноты и выразимости; разбираются основные свойства графов, деревья и остовные деревья, раскраски графов, экстремальные графы и теория Рамсея. Приводятся примеры применения свойств дискретных функций и графов в различных областях.

В части посвященной Вероятностным моделям изучаются принципы выбора математических моделей реальных явлений и процессов, протекающих в условиях стохастической неопределенности. Основной упор делается на описание асимптотических аппроксимаций и на энтропийный подход. Значительное внимание уделяется обсуждению условий применимости вероятностных моделей и, в частности, предельных теорем теории вероятностей. Обсуждаются обобщения классических предельных теорем на выборки случайного объема.

Оптимизация и численные методы

Излагаются и обсуждаются методы исследования и решения задач оптимизации и операторных уравнений в гильбертовых пространствах. Рассматриваются вопросы существования решений, условия оптимальности и основные итерационные вычислительные процедуры градиентного типа и метода Ньютона. В конечномерных пространствах для задач линейного и квадратичного программирования описываются конечно-шаговые алгоритмы симплекс-метода и метода сопряженных градиентов.

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 подходов 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.

Архитектура и программное обеспечение высокопроизводительных вычислительных систем

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 под-ходов, 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..

Сложность комбинаторных алгоритмов

Примеры задач с оценкой временной сложности. Нижние и верхние оценки сложности алгоритмов поиска. Нижние и верхние оценки сложности алгоритмов сортировки.
Некоторые общие результаты о сложности алгоритмов. Вычислимые функции, их нумерация. Теоремы о существовании общерекурсивной функции, трудно вычислимой хотя бы в одной точке, в бесконечном числе точек и почти всюду. Регулярные языки и автоматы. Теорема о регулярности

языка, распознаваемого со следом константной или слабо растущей длины. Несуществование задач с временной сложностью на машине Тьюринга по порядку между n и nlogn.
Метод динамического программирования. Алгоритм поиска кратчайших путей между всеми парами вершин в графе. Алгоритм для задачи об оптимальном порядке умножения матриц.
Метод «разделяй и властвуй» для построения быстрых алгоритмов. Быстрые алгоритмы для умножения чисел и матриц.
Метод расширения модели для построения быстрых алгоритмов. Алгоритмы обычного и булевского умножения матриц с битовыми операциями. Алгоритмы транзитивного замыкания графа.
Некоторые классы сложности. Определения классов P и NP. Примеры языков из NP, замкнутость класса P относительно полиномиального сведения. Теорема Кука об NP-полноте задачи о выполнимости конъюнктивной нормальной формы. Доказательство NP-полноты других задач. Полиномиальный алгоритм для распознавания 2-выполнимости.
Задачи оптимизации. Жадный алгоритм для задачи о кратчайшем остовном дереве. Задачи коммивояжёра, её NP-трудность, теорема о приближённых алгоритмов для неё.

Математические основы теории информации

Целями освоения дисциплины «Математические основы теории информации» являются:

1) Обеспечение приобретения знаний и умений в соответствии с государственным образовательным стандартом, содействие фундаментализации образования, формирование естественнонаучного мировоззрения и развитие системного мышления.

2) Ознакомление магистров с основными понятиями дисциплины, такими как: энтропия вероятностной схемы, источник информации, компрессия информации, теоремами кодирования в связи с передачей информации по каналам связи.

3) Овладение навыками работы с литературойпо дисциплине, навыками библиографических исследований.

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 РСА и Эль Гамаля. Табличное гаммирование. Понятие односторонней функции и односторонней функции с секретом.

2. Краткий исторический обзор развития криптографии. Шифры атбаш, Сцитала, табличка Энея, квадрат Полибия. Шифр Цезаря, шифровальный диск Альберти. Шифр простой биграмной 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. Ифраструктура открытых ключей. Центр сертификации открытых ключей. Система управления сертификатами. Федеральная ифраструктура 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.

Математические основы криптологии

Целью освоения дисциплины является развитие математического мышления, как культурной формы деятельности, определяемой как структурными особенностями математического знания, так и местом математики в системе наук.

В частности, ставятся следующие задачи:

1) создать представление о том, как возникали и развивались основные математические методы, модели и понятия, применямые в криптологии;

2) определить роль и место криптологии в системе математических знаний;

3) выяснить характер и особенности развития криптологии в XX веке, оценить вклад, внесенный в криптологию великими учеными прошлого века;

4) проанализировать, каков исторический путь отдельных математических дисциплин и теорий, в какой связи с потребностями людей и задачами других наук шло развитие криптологиии;

5) установить связи между различными разделами математики и криптологией;

6) овладеть навыками работы с литературой, особенностями библиографического поиска, научиться правильно цитировать и ссылаться на использованные материалы.

Теоретические основы компьютерной безопасности

Курс «Теоретические основы компьютерной безопасности» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Целью преподавания курса является изложение основополагающих моделей компьютерной безопасности.

Задачи дисциплины - изложить основные понятия и модели компьютерной безопасности; дать основы для анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности.

Теория кодирования

Целями освоения дисциплины «Теория кодирования» являются:

1) Обеспечение приобретения знаний и умений в соответствии с государственным образовательным стандартом, содействие фундаментализации образования формирование естественнонаучного мировоззрения и развития системного мышления.

2) Ознакомление магистров с основными понятиями дисциплины, такими как: код исправляющий ошибки, в частности линейный код; характеристики и параметры кодов; методами кодирования и декодирования, методами построения кодов с заданными корректирующими свойствами.

3) Овладение навыками работы с литературой по дисциплине, навыками библиографических исследований

Криптографические протоколы

В курсе «Криптографические протоколы» вводятся основные понятия, связанные с криптографическими протоколами и рассматриваются основные свойства, характеризующие безопасность. Особое внимание уделяется схемам электронной цифровой подписи, протоколам идентификации, протоколам с нулевым разглашением, протоколам распределения и передачи ключей. Приводятся примеры атак на криптографические протоколы, а также описывается влияние конструктивных особенностей протоколов на их свойства.

Курс «Криптографические протоколы» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Целью преподавания курса является изложение основополагающих принципов построения криптографических протоколов и примеров реализации этих принципов на практике.

Задачи дисциплины - изложить основные свойства, характеризующие безопасность; дать введение в основные криптографические протоколы; привести основные уязвимости криптографических протоколов дать основы синтеза криптографических протоколов; дать основы математических методов, используемых в анализе и при построении криптографических протоколов.

Булевы функции в кодировании и криптографии

В курсе систематически излагаются результаты о криптографических свойствах булевых функций и отображений. Для понимания излагаемого материала курса достаточно сведений содержащихся в университетских курсах по линейной алгебре, теории групп, теории конечных полей и полиномов, комбинаторике. В качестве рабочего аппарата используется дискретное преобразование Фурье, а также некоторые понятия и утверждения из теории кодирования.