**Бакалавриат**

**АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН (МОДУЛЕЙ)**

**Направление подготовки 01.03.02 "Прикладная математика и информатика"**

**Направленность программы**

**Математические методы обработки информации и принятия решений**

**Кафедра Информационной безопасности**

**3 курс**

### Уравнения математической физики

Постановки задач для уравнений параболического типа. Принцип максимума и его следствия. Метод разделения переменных. Уравнения Лапласа и Пуассона. Гармонические функции. Формулы Грина и их следствия. Основные методы решения краевых задач. Уравнение колебаний и постановка задач для уравнений гиперболического типа. Формула Даламбера и ее следствия. Метод разделения переменных. Задача с данными на характеристиках.

### Функциональный анализ

Излагаются начальные главы функционального анализа: теория меры и интеграл Лебега, банаховы и гильбертовы пространства, линейные операторы, теория Фредгольма, элементы спектральной теории.

**Вероятностные модели**

Целью освоениякурса «Вероятностные модели» является изучение принципов 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. В качестве примера к конкретным прикладным задачам строятся вероятностные модели процессов эволюции финансовых индексов.

**Методы машинного обучения**

Курс «Методы машинного обучения» посвящен современным методам предобработки и анализа данных, а также задачам прогнозирования вещественной переменной (регрессия), дискретной переменной (классификация). Также в курсе рассматриваются такие основные задачи обучения по прецедентам как кластеризация и понижение размерности. Изучаются методы их решения, как классические, так и новые, созданные за последние 10–15 лет. Рассматриваются продвинутые методы ансамблирования (XGBoost, CatBoost, стэкинг и т.д). Студентам также предлагается ознакомиться с байесовской теорией классификации. Упор делается на глубокое понимание математических основ, взаимосвязей, достоинств и ограничений рассматриваемых методов.

Программа курса предназначена для студентов уже знакомых с основами линейной алгебры, математического анализа, теории вероятности. Знание математической статистики, методов оптимизации и языка программирования Python желательно, но не обязательно.

**Методы оптимизации**

Для задач оптимизации в гильбертовом пространстве обсуждаются вопросы существования оптимальных решений, необходимые и достаточные условия оптимальности в форме вариационного неравенства и правила множителей Лагранжа. Рассматриваются основные итерационные методы приближённого решения задач оптимизации: градиентные, Ньютона, штрафов, а также симплекс-метод решения задач линейного программирования; исследуются свойства их сходимости. Излагаются основы теории двойственности, а также основные идеи, формулировки и схемы применения принципа максимума Л. С. Понтрягина к задачам оптимального управления и метода регуляризации А. Н. Тихонова к некорректно поставленным задачам оптимизации.

**Оптимальное управление**

Годовой курс оптимальное управление читается в 5-м и 6-м семестрах.

В 5-м семестре исследуется линейная задача быстродействия.С помощью аппарата опорных функций исследуются классические вопросы оптимального управления: управляемость, теорема существования оптимального управления, необходимые условия оптимальности в форме принципа максимума Л.С. Понтрягина, достаточные условия оптимальности. Полученные результаты применяются для исследования линейной задачи оптимального управления с терминальным функционалом и свободным правым концом.

В 6-м семестре изучается нелинейная задача оптимального управления с интегральным функционалом. Формулируется и доказывается теорема о необходимых условиях оптимальности с привлечением техники вариаций Макшейна. На примере нелинейной задачи быстродействия подробно изучаются идеи метода динамического программирования. Рассматриваются различные примеры задач оптимального управления, включая задачи с особыми режимами и задачи на бесконечном промежутке времени.

**Основы кибернетики**

Курс «**Основы кибернетики**» (ранее «Элементы кибернетики»), создателем и основным лектором которого был чл.-корр. РАН С.В. Яблонский, читается на факультете ВМК с первых лет его существования. Он является продолжением курса «Дискретная математика» и посвящён изложению основных моделей, методов и результатов математической кибернетики, связанных с теорией дискретных управляющих систем (УС), с задачей схемной или структурной реализации дискретных функций и алгоритмов.

В нём рассматриваются различные классы УС (классы схем), представляющие собой дискрет­ные математические модели различных типов электронных схем, систем обработки информации и управления, алгоритмов и программ. Для базовых классов УС (схем из функциональных элементов, формул, контактных схем, автоматных схем), а также некоторых других типов УС, ставятся и изучаются основные задачи теории УС: задача минимизации дизъюнктивных нормальных форм (ДНФ), задача эквивалентных преобразований и структурного моделирования УС, задача синтеза УС, задача повышения надёжности и контроля УС из ненадёжных элемен­тов и др. В программу курса входят классические результаты К. Шеннона, С.В. Яблонского, Ю.И. Журавлева и О.Б. Лупанова, а также некоторые результаты последних лет. Показывается возможность практического применения этих результатов на примере задачи проектирования СБИС, которые составляют основу программно-аппаратной реализации алгоритмов.

**Статистическая физика**

Курс посвящен введению в статистическую физику, изучающую основные закономерности поведения макроскопических сред, т.е. тел, состоящих из огромного числа отдельных частиц – атомов и молекул. Курс включает разделы термодинамики, молекулярной физики и статистической физики. Основное внимание уделяется изучению равновесных процессов: начала термодинамики, основные распределения статистической физики, энтропия, термодинамические потенциалы, статистическая сумма, реальные газы. Заключительная часть курса посвящена изложению теории флуктуаций и основ физической кинетики.

**Теоретические основы информационной безопасности**

В курсе систематически излагаются основы теоретической компьютерной безопасности. Рассматриваются основные математический модели управления доступам в компьютерных системах: модели дискреционного доступа, модели мандатного управления доступом, модели обеспечения целостности при доступе к ресурсу. Рассматриваются также различные модели невлияния в компьютерных системах. Уделяется внимание моделям аудита компьютерных систем. В завершении курса рассматриваются подходы к построению систем обнаружения вторжений компьютерных атак.

**Экономика**

**Целью дисциплины** является формирование у студентов экономического мышления и целостного представления о процессах и явлениях хозяйственной жизни, ее проблемах и способах их решения.

**Задачи:**

* познакомить студентов с базовыми экономическими категориями и институтами;
* показать закономерности экономического развития;
* раскрыть особенности поведения фирмы и домашнего хозяйства в условиях современной смешанной экономики;
* познакомить студентов с основами грамотного финансового поведения;

показать необходимость и задачи государственного регулирования в условиях открытой экономики.

**Численные методы**

Данный курс направлен на развитие навыков у студентов в решении типовых задач алгебры, математического анализа, обыкновенных дифференциальных уравнений и уравнений в частных производных. Рассматриваются те методы, которые выдержали испытание практикой и применяются для решения реальных прикладных задач. Устанавливаются связи между различными разделами математики и численными методами. Теоретический материал иллюстрируется на лекциях примерами с результатами расчетов.

**Случайные процессы**

В рамках данного курса рассматриваются основные модели теории случайных процессов такие как цепи Маркова с дискретным и непрерывным временем, корреляционная теория случайных процессов, стохастический интеграл, линейные стохастические дифференциальные уравнения, стационарные процессы. Более подробно исследованы свойства винеровского и пуассоновского процессов. Во второй части курса рассмотрены некоторые прикладные задачи теории случайных процессов: линейные преобразования стационарных процессов и задачи о наилучшей линейной оценки (прогноз и фильтрация).

**Криптографические свойства дискретных функций**

В курсе изучаются основные криптографические свойства булевых функций (систем булевых функций), формировавшиеся в ходе развития математических методов криптографического анализа. Рассматривается преобразование Фурье(Адамара) булевых функций и свойства их спектральных представлений. Изучаются основные понятия групповой эквивалентности булевых функций. Доказывается ряд важных криптографических свойств функций, связанных с их группами инерции и пространствами линейных структур. Исследуются свойства автокорреляционной функции и функции взаимной корреляции. Вводятся понятия нелинейности(максимальной нелинейности), корреляционной иммунности и алгебраической иммунности булевых функций и описывающие их параметры. Доказываются критерии наличия этих свойств у функции. Анализируются связи между различными криптографическими свойствами функций. В рамках курса обосновывается эффективность ряда алгоритмов решения в процессе криптоанализа вычислительно трудных задач. Изучение опирается на курсы алгебры и дискретной математики.

**Математические основы криптологии**

В курсе даётся систематическое изложение основных алгебраических объектов, которые применяются в криптографии. Основное внимание уделяется основам теории чисел и теории групп подстановок. Особо рассматриваются вопросы строения конечных полей и конечных групп.

**Программно-аппаратные средства защиты информации**

В курсе рассматриваются базовые программно-аппаратные средства защиты информации. Даётся введение в управление рисками информационной безопасности. Изучаются основные модели и средства управления доступом в компьютерных системах. Изучается физическая безопасность и безопасность окружения. Также уделяется внимание российскому м международному законодательству в области защиты информации.

**Элементы криптографического анализа**

Курс посвящён основам криптографического анализа базовых криптографических примитивов: блочных и потоковых шифров, хэш-функций и схем электронно- цифровой подписи. Рассматриваются статистические методы анализа, корреляционные методы, линейный и дифференциальный методы, а также методы, основанные на парадоксе о днях рождения. В рамках курса предусмотрен практикум по криптоанализу модельных шифров.

**4 курс**

**Математические модели в экономике**

Цель данного курса - познакомить слушателей с различными математическими моделями в экономике такими, как модель межотраслевого баланса, модель экономического планирования и оптимального экономического роста, модель конкурентного равновесия, а также с некоторыми разделами математики такими, как теория неотрицательных матриц и её приложения в экономике.

**Теория игр и исследование операций**

Курс разбит на три части. В первой излагается теория антагонистических игр, теоремы существования седловых точек, свойства оптимальных смешанных стратегий, методы решения матричных и выпуклых непрерывных игр в смешанных стратегиях, приводятся классические модели игр («нападение-оборона» и дуэли), рассматриваются многошаговые игры с полной информацией. Во второй части рассматриваются неантагонистические игры двух и многих лиц. Основные ее разделы: существование и методы поиска ситуаций равновесия ( в том числе в смешанных стратегиях для биматричных игр), оптимальные стратегии игрока-лидера в иерархических играх двух лиц. В третьей части рассматривается теория принятия решений: многокритериальная оптимизация, ядра бинарных отношений, общая модель операции и подход к ее исследованию на основе принципа гарантированного результата, необходимые условия для оптимальных стратегий и некоторые задачи оптимального распределения ресурсов.

### Дополнительные главы дискретной математики и кибернетики

Курс состоит из четырех частей. В первой части излагаются основы теории функций многозначной логики. Доказываются критерии полноты и устанавливается ряд существенных отличий функций многозначной логики от булевых функций. Во второй части изучаются ограниченно – детерминированные (автоматные) функции. Основное внимание уделяется способам задания автоматных функций : деревьями, каноническими уравнениями, диаграммами Мура и схемами из автоматных элементов. Третья часть посвящена машинам Тьюринга и вычислимым функциям. Доказывается вычислимость частично рекурсивных функций. В четвертой части доказывается теорема Форда и Фалкерсона о максимальном потоке в сети.

**Базы данных**

Курс начинается с рассмотрения основных понятий систем управления базами данных (СУБД). Выделяются ключевые отличия СУБД от файловой системы и основные черты таких дореляционных моделей данных как иерархическая, сетевая и модель данных инвертированных таблиц. Далее рассматривается реляционная модель данных (включая механизмы манипулирования) и теория проектирования реляционных БД на основе процедуры нормализации. После этого описывается процесс проектирование БД с использованием диаграмм «сущность-связь» и диаграмм классов языка UML и рассматриваются постреляционные модели данных: объектно-ориентированная модель, объектно-реляционные расширения SQL, "истинная" реляционная модель. В рамках курса также рассматриваются базовые средства языка SQL для определения и изменения схемы базы данных, выборки и модификации данных, авторизации доступа и управления транзакциями.

**Суперкомпьютеры и параллельная обработка данных**

Данный курс ориентирован на получение базовых знаний и практических навыков в области параллельных вычислений, методов параллельной обработки данных, технологий параллельного программирования и суперкомпьютерных технологий. Материал иллюстрируется примерами суперкомпьютерных систем и технологий, где параллелизм проявляется особенно ярко. Вместе с этим, показывается исключительно важная роль суперкомпьютерных систем как неотъемлемой части формируемой цифровой экономики. В процессе изложения рассматриваются три составные части параллельных вычислений: архитектуры параллельных вычислительных систем, технологии параллельного программирования и информационная структура программ и алгоритмов, и показывается тесная связь этих частей между собой.

**Лингвистическая культура (на английском языке)**

Целью освоения дисциплины является ознакомление студентов с лингвострановед-ческой культурой как важной частью подготовки современных специалистов. Профессиональная подготовка специалистов включает совершенствование переводческих навыков, которые невозможны без знаний специфических социокультурных условий функционирования иностранного языка. Лингвистическая культура является неотъемлемой частью переводческого профессионализма и делового общения.

**Введение в теорию сложности вычислений**

Курс посвящён теории вычислительной сложности алгоритмов. Рассматриваются две модели вычислений: однородная и неоднородная. Вводятся основные сложностные классы, в том числе P, NP и PSPACE, изучается их соотношение друг с другом. Значительная часть курса посвящена вероятностным алгоритмам и вычислениям с оракулом. Также в курсе рассматривается полиномиальная иерархия сложностных классов.

**Коды аутентификации и хэш-функции**

В курсе даётся систематическое изложение теории криптографических хэш-функций. Рассматриваются вопросы синтеза хэш-функции и изучаются базовые конструкции. Уделяется внимание вопросам криптоанализа хэш-функций, рассматриваются угрозы поиска коллизий и вычисления второго прообраза. Помимо хэш-функций в курсе изучаются родственные им коды аутентификации. Большое внимание уделяется практическим заданиям и примерам.

**Криптопротоколы**

Курс посвящён вопросам синтеза и анализа криптографических протоколов. Вводится понятие криптографического протокола, приводятся базовые свойства безопасности, которым должен удовлетворять стойкий криптографический протокол. Рассматриваются примитивные игровые протоколы, различные схемы электронной цифровой подписи, протоколы идентификации, протоколы доказательства с нулевым разглашением, протоколы передачи и распределения ключей, протоколы разделения секрета, электронные деньги в рамках модели Брэнда. В курсе также даётся введение в эллиптические кривые и их приложения в криптографии.

**Методы теории чисел в криптографии**

Курс посвящен углубленному изучению методов теории чисел, которые применяются в криптографии. Рассматриваются основные понятия, определения и факты теории чисел, изучаются вопросы строения конечных полей, полец и групп, которые часто применяются в криптографических задачах. Даются основы теории распределения простых чисел, приводятся методы решения линейных сравнений и систем и методы решения сравнений второй степени. Центральное место курса занимают основы теории делимости, и её использование при решении диофантовых уравнений, основы теории арифметических функций и теории цепных дробей. Подробно рассматриваются криптографические свойства логарифмической функции.

### Пакеты прикладных программ

Курс посвящен обзору современного математического программного обеспечения, применяемого в математических исследованиях. Излагаются основные возможности пакетов, их технические характеристики, примеры использования в различных областях математики.

**Безопасность программного обеспечения и сетей**

В данном курсе **рассматриваются**:

* основные понятия, определения и факты безопасности программного обеспечения и сетей;
* основные понятия локальных вычислительных сетей;
* основные понятия стека TCP/IPи модели OSI;
* основы теории и стандартные методы программирования на языках C/C++/Python.

По итогам обучения студенты **научатся**:

* извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов;
* демонстрировать способность к анализу и синтезу;
* разрабатывать программные модули на языках C/C++/Python.
* владеть методами использования теории построения политик безопасности компьютерных систем;
* проводить анализ угроз и поиска уязвимостей в компьютерных системах.