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

Направленность программы (магистерская программа)
«Информационная безопасность компьютерных систем»

Английский язык

Задачи дисциплины:
-совершенствовать навыки чтения и понимания научной литературы по профессиональной тематике на английском языке;
-помочь развитию логического мышления учащихся, умения выделить основную и второстепенную информацию, аргументировать и резюмировать прочитанное;
-научить студентов магистратуры принципам написания реферата, академического эссе и аннотаций профессионального текста на английском языке;
-обучить представлению результатов исследования в виде презентаций и дискуссий профессиональной направленности на английском языке;
- совершенствовать навыки понимания публичной речи;
- познакомить студентов магистратуры с современными требованиями цитирования, оформления ссылок на источники и библиографического списка в собственных научных работах и статьях на английском языке;
- повысить общеобразовательный, культурный и политический кругозор студентов.

Правоведение

Содержание дисциплины охватывает круг вопросов, связанных с теорией государства и права, юридической ответственностью, конституционное государственное право, административное право, гражданское право и трудовое право. Целью курса является формирование у студентов общего представления о правовой науке, о правах и свободах человека и гражданина, овладение основными отраслями права, выработка навыков пользования нормативными актами. Задачи курса: ознакомить студентов с основными принципами правоведения, сформировать у них правовое сознание; привить им навыки анализа государственно-правовых явлений, в повышении уровня их правовой культуры в целом, научить составлению и использованию нормативных и правовых документов, относящихся к будущей профессиональной деятельности, умению предпринимать необходимые меры по восстановлению нарушенных прав.

Русский язык и культура речи

Целями освоения дисциплины являются: формирование умения устанавливать связь между языковыми знаками русского языка и явлениями отражаемой этими знаками действительности; овладение сознательным умением извлекать полный и точный смысл из предъявленного речевого сообщения; формирование умения создавать речевые произведения разных стилей и жанров в соответствии с замыслом производителя речи, условиями общения и характером отношений с адресатом; совершенствование представления о русском языке как о культурной ценности, нуждающейся в сохранении и постоянном развитии в соответствии с динамикой жизни и потребностями российского общества.

Суперкомпьютерное моделирование и технологии

Суперкомпьютерное моделирование является определяющим фактором развития научно-технического прогресса. Решение прорывных задач современности невозможно без использования суперкомпьютеров. Курс посвящен изучению базовых основ суперкомпьютерного моделирования. В курсе рассматриваются вопросы современного состояния развития суперкомпьютерных технологий, включая суперкомпьютерные аппаратно-программные платформы, математические модели решаемых на суперкомпьютерных задач и алгоритмов их решения, параллельные технологии реализации таких задач на суперкомпьютерах. Неотъемлемой частью курса является выполнение студентами практических заданий на суперкомпьютерах МГУ и высокопроизводительных вычислительных системах ряда научных организаций. Особенностью курса является широкое участие в его проведении специалистов из различных научных областей, связанных с применением суперкомпьютерных технологий. Этот подход позволяет обеспечить

квалифицированный междисциплинарный подход, являющийся основой суперкомпьютерного моделирования.

Современная философия и методология науки

Целью дисциплины является формирование у слушателя целостного видения науки, понимания им специфики научной деятельности, характера исторического развития науки, ее взаимодействия с другими сферами человеческой деятельности. В курсе представлены основные темы философии ЕРассматриваются основные положения учения о науке как познавательной деятельности, как социальном институте, как виде человеческой деятельности, как элементе культуры.

История и методология прикладной математики и информатики

В рамках курса рассматриваются основные факты, события и идеи многовековой истории развития математики в целом и одного из ее важнейших направлений – «прикладной» - вычислительной математики, зарождения и развития вычислительной техники и программирования. Показывается роль математики и информатики в истории развития цивилизации. Дается характеристика научного творчества наиболее выдающихся ученых – генераторов научных идей. Особое внимание уделяется развитию математики и информатики в России.

Курс нацелен на формирование математического мировоззрения будущих магистров, выстраивание общего контекста математического мышления как культурной формы деятельности, определяемой как структурными особенностями математического знания, так и местом математики в системе наук.

Модуль «Криптография с секретным ключом»

Анализ и синтез блоковых и потоковых шифров

В дисциплине рассматриваются вопросы синтеза и анализа блоковых и потоковых шифров. Основное внимание уделяется методам построения криптографических примитивов, их автоматным моделям и описанию основных криптографических свойств. Далее рассматриваются способы построения фильтрующих и комбинированных генераторов с последующим анализом криптографических характеристик. Большое внимание уделяется вопросам линеаризации указанных генераторов, кроме того, изучаются различные способы применения для анализа шифров различных комбинаторных объектов, графов, блок-схем, кодов Грея и т.д. Рассматриваются способы построения потоковых шифров на основе применения подстановок. При этом изучаются основные свойства групп подстановок, рассматриваются различные подходы к их классификации (теоремы Бернсайда, Маннинга и т.д.). Способы построения и анализа блоковых шифров изучаются на примерах известных шифров DES, AES, IDEA, ГОСТ 28147-89. Рассматриваются способы применения линейного и дифференциального анализа блоковых шифров.

Генераторы псевдослучайных чисел их применение в криптографии

В курсе изучаются генераторы псевдослучайных чисел, представляющие собой автономные автоматы, методы синтеза и анализа таких автоматов, а также различные (существенные для криптографии) свойства последовательностей, генерируемых этими автоматами. Отличительной особенностью курса является использование методов неархимедовой эргодической теории: выходные последовательности автоматов рассматриваются как орбиты динамических систем в соответствующих фазовых пространствах, снабженных неархимедовой метрикой и естественной вероятностной мерой (нормированной мерой Хаара); при этом статистические свойства последовательностей определяются эргодическими свойствами систем.

Модуль «Криптография с открытым ключом и криптографические протоколы»

Теоретико-числовые и алгебраические модели в криптографии

В курсе дается обзор алгебраических и теоретико-числовых конструкций, используемых в криптографии. Большое внимание уделяется решению теоретико-числовых уравнений, а также теоретико-числовым алгоритмам. Обсуждаются основные результаты теории конечных полей и колец, арифметических функций, характеров, цепных дробей, диофантовых приближений.

Синтез и анализ криптосистемы с открытым ключом

В курсе дается общая теория криптосистем с открытым ключом. Рассматриваю криптосистемы, стойкость которых основывается на сложности некоторых задач из теории чисел и теории целочисленных решёток. Изучаются вопросы формального обоснования стойкости рассматриваемых криптосистем. Для каждой криптосистемы приводятся типовые уязвимости и атаки, эксплуатирующие указанные уязвимости. Уделяется внимание вопросам практической реализации как самих криптосистем, так и атак на них.

Модуль «Математические методы компьютерной безопасности»

Защита информации в распределенных информационных системах

В курсе рассматриваются вопросы наилучших практик в области обеспечения информационной безопасности. Строится цепочка от модели бизнес-процессов к модели обеспечения информационной безопасности. Изучаются методы построения архитектуры безопасности распределенных информационных систем.

Теория информации и теория кодирования

В курсе даются основы теории оптимального алфавитного кодирования, алгебраической теории кодирования. Рассматриваются дискретные источники без памяти, эргодические дискретные источники, двоичный симметричный канал связи. Для указанных источников доказываются основные теоремы кодирования. Для двоичного симметричного канала связи вводится пропускная способность и доказывается прямая теорема Шеннона. Рассматриваются основные классы алгебраических кодов, исправляющих ошибки: код Хэмминга, коды БЧХ, коды Рида-Соломона, коды Рида-Маллера. Особое внимание уделяется вопросам декодирования алгебраических кодов, в частности, подробно изучается алгоритм декодирования большого класса кодов - алгоритм Берлекэмпа-Мэсси.

Стеганография и скрытые каналы

В курсе рассматриваются вопросы построения и анализа методов стеганографии и скрытых каналов.

Поиск уязвимостей в программных системах и сетевых протоколах

В курсе изучаются основные понятия компьютерной безопасности. Исследуются угрозы и пути построения атак на электронные компоненты компьютеров, операционные системы и другие приложения. Рассматриваются основные атаки и угрозы в компьютерных сетях и приложениях. Определяются основы обеспечения безопасности программного обеспечения и сетей в компьютерных системах.

Модуль «Математические основы информационной безопасности»

Математическая криптография

В курсе изучаются математические модели криптографических протоколов и примитивов, особое внимание уделяется моделям противника, а именно атакам и угрозам информационной безопасности. Изучаются математически строгие определения стойкости наиболее важных криптографических протоколов. Доказываются фундаментальные результаты о необходимых и достаточных условиях существования стойких криптографических протоколов.

Тестирование безопасности компьютерных систем

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