22.09

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий
_____ С.А. Герасименко
(подпись, расшифровка подписи)
"26" сентября 2015 г.

ПРОГРАММА ПРАКТИКИ

«Б.2.В.П.1 Преддипломная практика»

Вид производственная практика
учебная, производственная

Тип практика по получению профессиональных умений и опыта профессиональной деятельности

Способ проведения выездная
стационарная практика, выездная практика

Форма непрерывная
непрерывная, дискретная

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Оренбург 2015

500731

Программа практики «*Б.2.В.П.1 Преддипломная практика***» /сост. О.А. Пихтилькова, А.Н. Благовисная - Оренбург: ОГУ, 2015**

Содержание

1 Цели и задачи освоения практики

Цель (цели) практики:
- приобретение опыта профессиональной деятельности;
- систематизация материалов для выполнения выпускной квалификационной работы.
Задачи:
- формирование умения использовать методы научно-исследовательской работы для решения прикладных, практических и инновационных задач;
- проведение исследований по теме выпускной квалификационной работы;
- систематизация представлений о последних достижениях и современных проблемах математики и компьютерных наук.

2 Место практики в структуре образовательной программы

Практика относится к обязательным дисциплинам (модулям) вариативной части блока 2 «Практики»

Пререквизиты практики: *Б.1.Б.11 Численные методы, Б.1.Б.14 Фундаментальная и компьютерная алгебра, Б.1.Б.24 Компьютерная геометрия и графика, Б.1.В.ОД.2 Пакеты прикладных программ в математике, Б.1.В.ОД.3 Криптографические методы защиты информации, Б.1.В.ОД.7 Теория кодирования, сжатия и восстановления информации, Б.1.В.ОД.9 Методы оптимизации, Б.1.В.ОД.10 Современные средства разработки программного обеспечения, Б.1.В.ОД.12 Методы алгебраической геометрии в криптографии, Б.1.В.ДВ.2.1 Дискретный анализ, Б.1.В.ДВ.3.1 Криптографические свойства булевых функций, Б.1.В.ДВ.3.2 Комбинаторный анализ, Б.1.В.ДВ.4.1 Актуальные проблемы фундаментальной и компьютерной алгебры, Б.1.В.ДВ.4.2 Дифференциально-геометрические структуры на многообразиях, Б.1.В.ДВ.5.2 Анализ сложности алгоритмов, Б.1.В.ДВ.6.1 Защита программ и данных, Б.1.В.ДВ.6.2 Основы криптоанализа, Б.2.В.У Учебная практика*

Требования к входным результатам обучения, необходимым для освоения практики

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
Знать: *- основные идеи, расчетные формулы, алгоритмы, условия применения, оценки устойчивости и скорости сходимости (для итерационных методов) для следующих численных методов:* *- решения нелинейных уравнений (метод бисекций, метод Ньютона, метод хорд, метод простых итераций);* *- решения систем линейных алгебраических уравнений (метод Гаусса, LU-алгоритм, метод скалярной 3-х точечной прогонки, метод квадратных корней, метод вращения, метод Зейделя, метод верхней релаксации, итерационные методы с Чебышевским набором параметров);* *- решения систем нелинейных уравнений (методы простых и покоординатных итераций, метод Ньютона и его модификации: сведение к методу простых итераций, двухступенчатый метод, аппроксимационный аналог, разностная (дискретная) модификация;* *- решения частичной проблемы собственных значений матрицы (степенной метод, метод скалярных произведений и метод частных Релея);* *- решения полной проблемы собственных значений*	ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
(итерационный метод вращения Якоби, LR-алгоритм); *- интерполирования (алгебраическими многочленами Лагранжа и Ньютона; нелокальными кубическими сплайнами);* *- восстановления функций (метод наименьших квадратов);* *- интегрирования (формулы левых, правых, средних прямоугольников, трапеции, Симпсона; общий вид формул Ньютона-Котеса);* *- дифференцирования (метод неопределенных коэффициентов, формулы вычисления первой производной таблично заданной функции с первым и вторым порядками точности, формулы вычисления второй производной);* *- решения задачи Коши для обыкновенных дифференциальных уравнений (далее - ОДУ) (метод Эйлера, предиктор-корректор, методы Рунге-Кутта);* *- решения краевых задач для гиперболического уравнения (на примере одномерного уравнения конвективного переноса) с помощью явных и неявных конечно-разностных схем;* *- решения краевых задач для одномерного параболического уравнения (на примере уравнения диссипации, конвекции, кинетики) с помощью неявных конечно-разностных схем.* *Иметь представление о явных конечно-разностных схемах;* *- решения двумерных нестационарных задач;* *- решения двумерных стационарных задач;* *- постановки физических задач для уравнения конвективного переноса, уравнения диссипации, конвекции, кинетики;* *- свойства решений уравнения конвективного переноса,* *- уравнения диссипации, конвекции, кинетики;* *- постановки двумерных стационарных и нестационарных задач на основе уравнения диссипации, конвекции, кинетики;* *- метод установления решения стационарных задач;* *- перспективы развития численных методов;* *- сущность и этапы вычислительного эксперимента;* *- область использования математических моделей и вычислительного эксперимента в его будущей профессиональной деятельности;* *- содержание ключевых понятий и определений, используемых в теории и практике решения алгебраических задач;* *- базовые разделы математики;* *- основные тенденции развития науки в соответствующей области, общее представление о развитии современного образования;* *- математические основы криптоанализа;* **Уметь:** *- выбрать дискретную модель для решения учебной математической задачи;* *- оценить погрешность и исследовать иные характеристики используемого численного метода;* *- спроектировать вычислительный алгоритм для решения учебной математической задачи;* *- разработать программу реализации вычислительного алгоритма;* *- осуществить интерпретацию полученного результата, используя различные формы его представления (графики, таблицы, диаграммы и т.д.);* *- применять прикладное программное обеспечение для решения задач профессиональной деятельности, науке и образовании;* *- использовать математические методы при решении*	деятельности

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
криптографических задач; *- осуществлять отбор и представление материала, характеризующего достижения науки с учетом специфики направления подготовки;* *- решать задачи алгебры, математической логики, теории чисел, дискретной математики, теории вероятностей и математической статистики, возникающие при раскрытии шифров;* **Владеть:** *- основными приемами исследования численных методов;* *- технологией выбора численного метода для решения определенного класса задач;* *- навыками пользования прикладного программного обеспечения для решения задач в профессиональной деятельности, науке и образовании* *- основными криптографическими методами;* *- навыками интерпретации математических моделей процессов передачи, преобразования информации и раскрытия шифров.*	
Знать: *- основные понятия вычислительной геометрии и компьютерной графики; представление различных геометрических структур данных;* *- основные алгоритмы вычислительной геометрии и компьютерной графики; основные алгоритмы формирования изображений;* *- основные возможности и функции математических пакетов Mathcad и Matlab, функции для выполнения аналитических и численных вычислений, методы построения различного вида графиков;* *- комбинаторные конфигурации;* *- формулы подсчета;* *- формулы обращения;* *- производящие функции;* *- операции над производящими функциями;* *- элементарные производящие функции;* **Уметь:** *- разрабатывать программы для решения задач обработки геометрической информации;* *- реализовать вычислительные методы решения задач линейной алгебры, интегрирования и дифференцирования, использовать графические возможности математических пакетов Mathcad и Matlab;* *- решать задачи используя различные комбинаторные конфигурации;* *- решать задачи используя алгебраический метод;* *- решать задачи с производящими функциями;* **Владеть:** *- навыками использования основных алгоритмов вычислительной геометрии и компьютерной графики при разработке программ; применения методов вычислительной геометрии и компьютерной графики при решении новых теоретических и прикладных задач;* *- навыками вычисления выражений различной сложности, нахождения пределов, производных и интегралов, решения уравнений и систем уравнений с помощью математических пакетов Mathcad и Matlab;* *-приемами комбинаторных рассуждений.*	ОПК-2 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Знать:	ОПК-3 способностью к

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
- основные источники (учебники, монографии, периодические издания, интернет-ресурсы и т.п.), отражающие современное состояние развития фундаментальной и компьютерной алгебры; *- приемы организации самостоятельной работы при решении дифференциально-геометрических задач;* **Уметь:** *- находить, обрабатывать и анализировать публикации, содержащие теоретические сведения и практические результаты в области фундаментальной и компьютерной алгебры;* *- самостоятельно планировать и осуществлять поиск и переработку математической информации в соответствии с поставленными задачами;* **Владеть:** *- навыками анализа проблем в области фундаментальной и компьютерной алгебры;* *- навыками самостоятельного изучения учебной и научной литературы, в том числе математической литературы, поиска необходимых методов исследования и интерпретации.*	самостоятельной научно-исследовательской работе
Знать: *- сущность и этапы вычислительного эксперимента;* *- эффективные численные методы для стандартных задач;* *- область использования математических моделей и вычислительного эксперимента в его будущей профессиональной деятельности;* *- принципы построения научного исследования в соответствующей области наук;* *- основные операторы системы программирования Matlab;* *- основные алгоритмы решения криптографических задач;* *- способы задания булевых функций в криптографических конструкциях;* *- характеристики булевых функций, обеспечивающие криптографическую стойкость шифрам;* *- области применения булевых функций, обладающих криптографическими свойствами;* *- основные методы комбинаторного анализа;* *- непрерывные методы в дискретной математике;* *- методы математического анализа в решении комбинаторных задач;* **Уметь:** *- выбрать дискретную модель для решения математической задачи;* *- спроектировать вычислительный алгоритм для решения математической задачи;* *- разработать программу реализации вычислительного алгоритма;* *- осуществить интерпретацию полученного результата, используя различные формы его представления (графики, таблицы, диаграммы и т.д.);* *- обосновать актуальность, новизну, теоретическую и практическую значимость собственного исследования, определять методологию исследования;* *- делать выводы из проведенного исследования и определять перспективы дальнейшей работы, анализировать собранный эмпирический материал и делать достоверные выводы;* *- отстаивать собственную научную концепцию в дискуссии;* *- составлять и отлаживать программы в среде Matlab;* *- решать криптографические задачи с использованием современных вычислительных систем;*	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
- находить криптографические характеристики булевых функций, в том числе и с применением современных вычислительных систем; *- находить булевы функции с требуемыми криптографическими свойствами;* *- решать задачи различными методами комбинаторного анализа;* **Владеть:** *- технологией программирования численных методов алгебры, анализа, решения дифференциальных уравнений;* *- основными приемами проектирования и реализации вычислительного эксперимента;* *- основными приемами интерпретации и визуализации численных результатов для стандартных учебно-профессиональных задач;* *- навыками работы с источниками научной литературе;* *- способностью реализовывать программно с помощью математического пакета Matlab и использовать на практике математические алгоритмы;* *- методами решения криптографических задач с использованием современных вычислительных систем;* *- методами реализации криптографических конструкций, использующих аппарат теории криптографических булевых функций, на основе современных вычислительных систем;* *- приемами комбинаторных рассуждений с реализацией программного использования математических алгоритмов на практике.*	
Знать: *- основные криптографические протоколы;* *- основные понятия теории групп, колец, полей, используемые в криптографических методах алгебраической геометрии;* *- основные элементы дискретного анализа;* *- основные формулы, леммы, теоремы дискретного анализа;* *- методы оценки сложности алгоритмов,* *- основные принципы организации рекурсивных алгоритмов;* *- основные алгоритмы сортировки и поиска данных;* *- алгоритмы целочисленной арифметики;* *- способы перебора комбинаторных объектов;* *- основные понятия криптоанализа,* *- математические основы теории стойких шифров;* **Уметь:** *- программно реализовывать основные криптографические протоколы;* *- решать задачи теории эллиптических кривых, возникающие при создании и исследовании криптографических конструкций;* *- решать задачи перебора перестановок;* *- решать экстремальные задачи, связанные с перестановками;* *- генерировать комбинаторные объекты;* *- анализировать разработанный алгоритм, вычислять его сложность в лучшем и худшем случае;* *- организовать перебор с возвратом;* *- реализовать на языке программирования динамические структуры данных;* *- применять знания из различных разделов математики при решении задач криптоанализа;* **Владеть:** *- способностью к определению общих форм и закономерностей криптографии;*	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
- алгоритмами на эллиптических кривых, используемыми в задачах защиты информации; *- способностью использования математического аппарата дискретного анализа;* *- методами доказательства различных утверждений в области дискретного анализа;* *- навыками реализации основных рекурсивных алгоритмов обработки данных на ЭВМ;* *- навыками написания программ для обработки больших массивов данных;* *- навыками использования стандартных библиотек при разработке собственных программ;* *- простейшими математическими методами решения задач криптоанализа.*	
Знать: *- методы теории групп, колец, полей, векторных пространств;* *- формулировки классических задач теории эллиптических кривых, используемых в криптографических приложениях;* *- строки, операции над строками;* *- функции от строк;* *- скользящие суммы;* *- суффиксное дерево.* *- понятия конечноопределенной группы, диаграммы ван Кампена, граф группы;* *- геометрические методы задания элементов группы;* *- постановки основных алгоритмических проблем комбинаторной теории групп;* *- лексикографический порядок на членах многочленов нескольких переменных;* *- понятие идеала кольца многочленов;* *- понятие базиса идеала кольца многочленов;* *- теорему Гильберта о базисе;* *- понятие равносильности систем алгебраических уравнений;* *- понятие базиса Грёбнера идеала кольца многочленов;* *- постановку задачи вхождения многочлена в идеал;* *- основные задачи, решаемые средствами дифференциальной геометрии и топологии;* *- постановки классических задач криптоанализа;* **Уметь:** *- сформулировать и доказать основные результаты изучаемых разделов, применять алгебраические методы;* *- адаптировать постановки классических задач теории эллиптических кривых для криптографических целей;* *- решать задачу точного поиска;* *- решать задачу приближенного поиска;* *- решать задачу о максимальном совпадении двух строк;* *- исследовать на алгоритмическую неразрешимость массовые проблемы, относящиеся к комбинаторной теории групп;* *- сводить одни алгоритмические проблемы комбинаторной теории групп к другим;* *- проводить символьные преобразования многочленов;* *- исследовать системы алгебраических уравнений на совместность, эквивалентность, конечность;* *определять корректность математической формулировки как*	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
классических, так и прикладных задач; *- формулировать математические задачи, лежащие в основе создания стойких криптографических конструкций;* **Владеть:** *- понятийным аппаратом алгебраической теории в прикладных задачах;* *- навыками постановки задач криптографии на основе аппарата теории эллиптических кривых;* *- способностью аргументировано доказывать математические утверждения, используя знания различных областей математики;* *- навыками постановки задач комбинаторной теории групп и теории систем алгебраических уравнений;* *- навыками постановки математических задач с использованием аппарата дифференциальной геометрии и топологии;* *- навыками постановки практических задач криптографии.*	
Знать: *- методы и приемы исследования (оценки)погрешности/ошибки аппроксимации, устойчивости, скорости сходимости (для итерационных методов), условий применения для численных методов следующих классов задач:* *- решения нелинейных уравнений (метод бисекций, метод Ньютона, метод хорд, метод простых итераций);* *- решения систем линейных алгебраических уравнений (далее – СЛАУ): прямые методы (метод Гаусса, LU-алгоритм, метод скалярной 3-х точечной прогонки) и итерационные методы (метод Зейделя, метод верхней релаксации, итерационные методы с Чебышевским набором параметров);* *- решения систем нелинейных уравнений (методы простых и покоординатных итераций, метод Ньютона и его модификации);* *- решения частичной проблемы собственных значений матрицы (степенной метод, метод скалярных произведений и метод частных Релея);* *- решения полной проблемы собственных значений (итерационный метод вращения Якоби, LR-алгоритм);* *- интерполирования таблично заданной функции (алгебраическими многочленами Лагранжа и Ньютона; нелокальными кубическими сплайнами);* *- восстановления функций (метод наименьших квадратов);* *- интегрирования (формулы левых, правых, средних прямоугольников, трапеции, Симпсона; общий вид формул Ньюто-на-Котеса);* *- дифференцирования (формулы вычисления первой производной таблично заданной функции с первым и вторым порядками точности, формулы вычисления второй производной);* *- решения задачи Коши для обыкновенных дифференциальных уравнений (далее – ОДУ) (метод Эйлера, предиктор-корректор, методы Рунге-Кутта);* *- решения краевых задач для гиперболического уравнения (на примере одномерного уравнения конвективного переноса) с помощью явных и неявных конечно-разностных схем;* *- решения краевых задач для параболического уравнения (на примере одномерного уравнения диссипации, конвекции, кине-* *тики) с помощью неявных конечно-разностных схем. Иметь*	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
представление о явных конечно-разностных схемах; *- решения двумерных стационарных и нестационарных задач;* *- новые научные результаты, связанные с алгеброй;* *- формулировки утверждений и теорем теории эллиптических кривых, связанных с задачами защиты информации;* *- понятие сжатие текстов;* *- понятие помехоустойчивость;* *- симметричное шифрование;* *- формулировки ключевых теорем комбинаторной теории групп и теории систем алгебраических уравнений;* *- основные методы доказательства математических утверждений о дифференциально-геометрических структурах на многообразиях;* **Уметь:** *- оценить погрешность и исследовать иные характеристики используемого численного метода;* *- использовать современные методы для исследования и решения научных и практических задач; использовать новые знания и применять их в своей профессиональной деятельности;* *- доказывать утверждения и теоремы теории эллиптических кривых, связанных с задачами защиты информации;* *- решать задачи шифрования с открытым ключом;* *- решать задачи используя хеширование.* *- применять методы преобразования слов, задающих элементы группы;* *- строить диаграммы ван Кампена;* *- находить базис Грёбнера идеала кольца многочленов;* *- решать задачу вхождения в идеал;* *- решать системы алгебраических уравнений;* *- излагать доказательство и грамотно формулировать полученный результат;* **Владеть:** *- основными приемами исследования численных методов;* *- технологией выбора численного метода для решения определенного класса задач;* *способностью проводить научные исследования и получать новые научные результаты;* *- различными методами вывода основных результатов теории эллиптических кривых.* *- способностью строго доказательства математических теорем, утверждений, предусматривающего анализ и синтез хода рассуждений;* *- различными методами вывода основных результатов комбинаторной теории групп и теории систем алгебраических уравнений;* *- навыками доказательства различных утверждений дифференциальной геометрии и топологии и умением предвидеть возможные сферы применения доказанных утверждений, в том числе в теории групп и алгебры Ли, дифференциально-геометрических структур на многообразиях, неевклидовой геометрии.*	
Знать: *- современные тенденции развития теории и практики компьютерной математики;* **Уметь:** *- анализировать полученные в процессе исследования результаты и*	ПК-4 способностью публично представлять собственные и известные научные результаты

Предварительные результаты обучения, которые должны быть сформированы у обучающегося до начала изучения практики	Компетенции
излагать полученные результаты ясным научным языком, пользуясь научными терминами в соответствии с их смыслом; **Владеть:** *- основными методами представления полученных результатов в виде научной статьи, доклада.*	

Постреквизиты практики: *Отсутствуют*

3 Требования к результатам обучения по практике

Процесс изучения практики направлен на формирование следующих результатов обучения

Планируемые результаты обучения по практике, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: *- принципы функционирования профессионального коллектива;* **Уметь:** *- работать в коллективе, эффективно выполнять задачи профессиональной деятельности;* *- понимать роль корпоративных норм и стандартов;* **Владеть:** *- приемами взаимодействия с сотрудниками, выполняющими различные профессиональные задачи и обязанности.*	ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия
Знать: *- основные источники (учебники, монографии, периодические издания, инернет-ресурсы и т.п.), отражающие современное состояние развития математики и компьютерных наук;* **Уметь:** *- применять модели фундаментальной и компьютерной математики в решении конкретной задачи;* **Владеть:** *- навыками анализа проблем в области математики и компьютерных наук.*	ОПК-3 способностью к самостоятельной научно-исследовательской работе
Знать: *- современные компьютерные технологии, применяемые при решении задач математики и компьютерных наук;* **Уметь:** *- представлять решение конкретной задачи в виде алгоритма и применить для решения современные вычислительные системы;* **Владеть:** *- навыками реализации различных алгоритмов на основе современных программных комплексов.*	ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
Знать: *- основные понятия, концепции, результаты, задачи и методы теории и практики в области математики и компьютерных наук;* **Уметь:** *- адаптировать постановки классических задач для приложений;* **Владеть:** *- навыками постановки математических задач, возникающих в приложениях.*	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики
Знать: *- формулировки утверждений и теорем различных разделов математики;*	ПК-3 способностью строго доказать утверждение, сформулировать результат,

Планируемые результаты обучения по практике, характеризующие этапы формирования компетенций	Формируемые компетенции
Уметь: - *доказывать утверждения и теоремы различных разделов математики;* **Владеть:** - *различными методами вывода результатов в области математики и компьютерных наук.*	увидеть следствия полученного результата
Знать: - *принципы, методы обработки и представления информации;* **Уметь:** - *применять технические средства обработки и представления знаний;* **Владеть:** - *технологиями представления данных.*	ПК-4 способностью публично представлять собственные и известные научные результаты

4 Трудоемкость и содержание практики

4.1 Трудоемкость практики

Общая трудоемкость практики составляет 9 зачетных единиц (324 академических часов).

Вид работы	Трудоемкость, академических часов	
	8 семестр	всего
Общая трудоёмкость	**324**	**324**
Контактная работа:	**15,25**	**15,25**
Консультации	5	5
Индивидуальная работа и инновационные формы учебных занятий	10	10
Промежуточная аттестация	0,25	0,25
Самостоятельная работа:	**308,75**	**308,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

4.2 Содержание практики

Практика может проводиться на выпускающей кафедре алгебры и дискретной математики, в научных подразделениях вуза, а также на договорных началах в государственных, муниципальных, общественных, коммерческих и некоммерческих организациях, предприятиях и учреждениях, осуществляющих научно-исследовательскую деятельность, на которых возможно изучение и сбор материалов, связанных с выполнением выпускной квалификационной работы.

Работа студентов в период преддипломной практики организуется в соответствии с логикой работы над выпускной квалификационной работой. При прохождении преддипломной практики студент разрабатывает в окончательном виде основные положения ВКР и проводит их экспериментальную апробацию.

№ 1 Организационный этап

Уточнение плана проведения работ по написанию ВКР во время преддипломной практики. Формулировка цели и задач исследования. Уточнение выбора методов исследования и плана проведения экспериментальных работ.

№ 2 Исследовательский этап

Сбор теоретического и практического материала по теме ВКР и выполнение индивидуальных заданий руководителя.

Обработка собранных материалов, формирование первого варианта ВКР.

№ 3 Заключительный этап

Подготовка отчета и представление чернового варианта ВКР на предзащиту.

Формы отчетности по преддипломной практике:
- дневник практики;
- отчет по преддипломной практике.

Дневник практики является отчетным документом, характеризующим и подтверждающим прохождение студентом преддипломной практики, в котором отражается текущая работа студента в процессе практики:

- выданное студенту индивидуальное задание на преддипломную практику и сбор материалов к ВКР;

- календарный план выполнения студентом программы практики с отметками о полноте и уровне его выполнения;

- анализ состава и содержания выполненной студентом практической работы с указанием структуры, объемов, сроков выполнения и ее оценки руководителем практики;

- краткая характеристика и оценка работы студента научным руководителем в период прохождения практики.

Кроме заполнения разделов дневника, студент должен подготовить отчет по практике.

Содержание отчета по научно-исследовательской работе студента по результатам заключительного этапа исследования обсуждается и утверждается с научным руководителем ВКР.

5 Учебно-методическое обеспечение практики

5.1 Учебная литература

1. Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации. / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидорова. – Москва: Горячая линия-Телеком, 2014. – 304 с.

2. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – РИОР, 2013. – Режим доступа: http://znanium.com/bookread2.php?book=405000

3. Кнауб, Л.В. Теоретико-численные методы в криптографии: учебное пособие [Электронный ресурс] / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов, Сибирский Федеральный университет. – Красноярск: Сибирский федеральный университет, 2011. - 160 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=229582

4. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности «Информационные системы и технологии» / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – Москва: Академия, 2012. – 332 с.

5. Романьков, В.А. Алгебраическая криптография [Электронный ресурс] / В.А. Романьков. – Омск: Омский государственный университет, 2013. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=238045

6. Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Текст] : [монография] / [Н. И. Червяков [и др.]. - Москва : Физматлит, 2012.

7. Фефилов, А.Д. Методы и средства защиты информации в сетях / А.Д. Фефилов. - М. : Лаборатория книги, 2011. - 105 с. : ил., табл. - ISBN 978-5-504-00608-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=140796

8. Разработка моделей криптографической защиты информации : монография / В.Г. Шубович,

В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова», Министерство образования и науки РФ. - Ульяновск : УлГПУ, 2013. - 128 с. : схем. - Библиогр.: с. 108-112. - ISBN 978-5-86045-640-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=278070 (04.05.2017).

9. Инструментальный контроль и защита информации : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

10 Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] /Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 511с. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998

5.2 Интернет-ресурсы

1. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал Math-Net.Ru — это современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России)
2. http://intuit.ru/ (сайт института дистанционного обучения "ИНТУИТ")
3. http://cryptography.ru/about/ (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий)

5.3 Программное обеспечение современных информационно-коммуникационных технологий

Для выполнения практической части работы используется любая из доступных на момент написания работ сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение практики

Учебные аудитории для самостоятельной работы.

Для докладов используется переносной мультимедийный комплект: ноутбук, проектор, экран.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

К программе практики прилагается:

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.

ЛИСТ
согласования программы практики

Направление подготовки: 02.03.01 Математика и компьютерные науки
код и наименование

Профиль: Алгоритмы и приложения компьютерной математики

Практика: Б.2.В.П.1 Преддипломная практика

Форма обучения: очная
(очная, очно-заочная, заочная)

Год набора 2015

РЕКОМЕНДОВАНА заседанием кафедры
Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 2 от "26" 09 2015 г.

Ответственный исполнитель, заведующий кафедрой
Кафедра алгебры и дискретной математики — подпись — О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
доцент — подпись — О.А. Пихтилькова
должность *подпись* *расшифровка подписи*

ст. преподаватель — подпись — А.Н. Благовисная
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки — личная подпись — расшифровка подписи
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
личная подпись — Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
личная подпись — И.В. Кронова
личная подпись *расшифровка подписи*

Начальник отдела информационных образовательных технологий ЦИТ
личная подпись — Е.В. Дырдина
личная подпись *расшифровка подписи*

№41847

Дополнения и изменения в рабочей программе на 2016 год набора

Направление подготовки: 02.03.01 Математика и компьютерные науки (программа академического бакалавриата)

Профиль: Алгоритмы и приложения компьютерной математики (бакалавр)

Дисциплина: Б.2.В.П.1 Преддипломная практика

Форма обучения: очная

Внесенные изменения на 2016 год набора

УТВЕРЖДАЮ
Декан факультета математики и информационных технологий _____ С.А. Герасименко
(подпись, расшифровка подписи)
"26" февраля 2016 г.

В рабочую программу вносятся следующие изменения:

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Бабенко, Л. К. Параллельные алгоритмы для решения задач защиты информации. / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидорова. – Москва: Горячая линия-Телеком, 2014. – 304 с.
2. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – РИОР, 2013. – Режим доступа: http://znanium.com/bookread2.php?book=405000
3. Кнауб, Л.В. Теоретико-численные методы в криптографии: учебное пособие [Электронный ресурс] / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов. Сибирский Федеральный университет. – Красноярск: Сибирский федеральный университет, 2011. – 160 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=229582
4. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений, обучающихся по специальности «Информационные системы и технологии» / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – Москва: Академия, 2012. – 332 с.
5. Романьков, В.А. Алгебраическая криптография [Электронный ресурс] / В.А. Романьков. – Омск: Омский государственный университет, 2013. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=238045
6. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [Н. И. Червяков [и др.]. – Москва: Физматлит, 2012.
7. Фефилов, А.Д. Методы и средства защиты информации в сетях [Электронный ресурс] / А.Д. Фефилов. – М.: Лаборатория книги, 2011. – 105 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=140796
8. Разработка моделей криптографической защиты информации: монография [Электроный ресурс] / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова», Министерство образования и науки РФ. - Ульяновск : УлГПУ, 2013. – 128 с.: Режим доступа: http://biblioclub.ru/index.php?page=book&id=278070 (04.05.2017).
9. Инструментальный контроль и защита информации [Электронный ресурс] / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др.; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». –

Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=255905

10. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс] /Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 511с. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998

11. Алгебраические структуры и их приложения: учебное пособие [Электронный ресурс] / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А. Тихомиров; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск: САФУ, 2015. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=436142

5.4 Интернет-ресурсы

1. http://eqworld.ipmnet.ru/indexr.htm (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
2. http://intuit.ru/ (сайт института дистанционного обучения "ИНТУИТ").
3. http://cryptography.ru/about/ (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий).
4. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России).

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Windows.
2. Офисный пакет Microsoft Office (Word, Excel, Power Point).
3. Среда разработки Visual Studio.

6 Материально-техническое обеспечение дисциплины

Для выполнения заданий предназначен компьютерный класс (ауд. № 1605), подключенный к локальной сети ОГУ и сети Интернет, оснащенный всем необходимым оборудованием.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

Рабочая программа пересмотрена и одобрена на заседании кафедры алгебры и дискретной математики 17.02.16, протокол №7 / О.А. Иващенко /
(дата, номер протокола заседания кафедры, подпись зав. кафедрой)

СОГЛАСОВАНО:

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

Дополнения и изменения в рабочей программе на 2017 год набора

Направление подготовки: 02.03.01 Математика и компьютерные науки (программа академического бакалавриата)

Профиль: Алгоритмы и приложения компьютерной математики (бакалавр)

Дисциплина: Б.2.В.П.1 Преддипломная практика

Форма обучения: очная

Внесенные изменения на 2017 год набора
УТВЕРЖДАЮ
Декан факультета математики и информационных технологий _____ С.А. Герасименко
(подпись, расшифровка подписи)
"28" февраля 2017 г.

В рабочую программу вносятся следующие изменения:

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст]: пер. с англ. / Г. Биркгоф, Т. К. Барти.– 2-е изд., стер. – СПб.: Лань, 2005. – 400 с.

2. Винберг, Э.Б. Алгебра [Электронный ресурс] / Э.Б. Винберг. – НЦНМО, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=63299

3. Глухов, М. М. Математическая логика. Дискретные функции. Теория алгоритмов / М. М. Глухов, А. Б. Шишков. - СПб.: Лань, 2012. – 416 с.

4. Кострикин, А.И. Введение в алгебру: учебник [Электронный ресурс] / А.И. Кострикин. – Москва: МЦНМО, 2009. – Ч. 1. Основы алгебры. – 273 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=63140

5. Кострикин, А.И. Введение в алгебру: учебник / А.И. Кострикин. – Москва: МЦНМО, 2009. – Ч. 3. Основные структуры алгебры. – 272 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=62951

6. Нестеров, С.А. Основы информационной безопасности: учебное пособие [Электронный ресурс] / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – СПб.: Издательство Политехнического университета, 2014. – 322 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=363040

7. Панкратьев, Е.В. Элементы компьютерной алгебры: учебник [Электронный ресурс] / Е.В. Панкратьев; Национальный Открытый Университет «ИНТУИТ». – Москва: Интернет-Университет Информационных Технологий, 2007. – 247 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=233322

8. Пихтильков, С. А. Фундаментальная и компьютерная алгебра [Электронный ресурс]: учебное пособие для студентов, обучающихся по программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / С. А. Пихтильков, О. А. Пихтилькова, Л. Б. Усова: М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т». – Электрон. текстовые дан. (1 файл: 0.58 Мб). – Оренбург: ОГУ, 2016. – 116 с.

9. Прохорова, О.В. Информационная безопасность и защита информации: учебник [Электронный ресурс] / О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального

образования «Самарский государственный архитектурно-строительный университет». – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331

10. Спицын, В.Г. Информационная безопасность вычислительной техники: учебное пособие [Электронный ресурс] / В.Г. Спицын; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск: Эль Контент, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=208694

5.2 Дополнительная литература

1. Алферов А.П. Основы криптографии: учеб. пособие для вузов / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2005. – 480с.

2. Долозов, Н.Л. Программные средства защиты информации: конспект лекций [Электронный ресурс] / Н.Л. Долозов, Т.А. Гультяева; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск: НГТУ, 2015. – 63 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438307

3. Лапонина, О.Р. Криптографические основы безопасности [Электронный ресурс] / О.Р. Лапонина. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=429092

4. Фороузан, Б.А. Математика криптографии и теория шифрования [Электронный ресурс]/Б.А. Фороузан. – М.: Национальный Открытый Университет «ИНТУИТ», 2016, 511с. Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=428998

5. Алгебраические структуры и их приложения: учебное пособие [Электронный ресурс] / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А. Тихомиров; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск: САФУ, 2015. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=436142

5.4 Интернет-ресурсы

1. http://eqworld.ipmnet.ru/indexr.htm (международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).
2. http://intuit.ru/ (сайт института дистанционного обучения "ИНТУИТ").
3. http://cryptography.ru/about/ (сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий).
4. http://www.mathnet.ru/index.phtml/?option_lang=rus (общероссийский математический портал, современная информационная система, предоставляющая российским и зарубежным математикам различные возможности в поиске информации о математической жизни в России).
5. https://arxiv.org/ (крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии).

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Операционная система Windows.
2. Офисный пакет Microsoft Office (Word, Excel, Power Point).
3. Для выполнения заданий практики используется любая из доступных на момент выполнения работ сред программирования, имеющихся в распоряжении лаборатории кафедры. Среда и язык программирования выбираются студентами самостоятельно в соответствии с их индивидуальными учебными возможностями и предпочтениями.

6 Материально-техническое обеспечение дисциплины

Для выполнения заданий предназначен компьютерный класс (ауд. № 1605), подключенный к локальной сети ОГУ и сети Интернет, оснащенный всем необходимым оборудованием.

Для получения необходимой информации и самостоятельной работы студентов используются web-ресурсы Интернет и информационная библиотечная система.

Рабочая программа пересмотрена и одобрена на заседании кафедры алгебры и дискретной математики 21.02.17 протокол № 7 / О.А. Дистанкова
(дата, номер протокола заседания кафедры, подпись зав. кафедрой)

СОГЛАСОВАНО:

Заведующий отделом комплектования научной библиотеки

_____ Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета

_____ И.В. Крючкова
личная подпись *расшифровка подписи*