

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ

Проректор по учебной работе и
образовательным инновациям

О.Н.Здрок

« 23 » декабря 2021 г.

Регистрационный № 10146

ПРОГРАММА

УЧЕБНОЙ ВЫЧИСЛИТЕЛЬНОЙ ПРАКТИКИ

для специальности:

1-31 03 09 Компьютерная математика и системный анализ

2021 г.

СОСТАВИТЕЛИ:

К.Г. Атрохов, старший преподаватель кафедры дифференциальных уравнений и системного анализа механико-математического факультета БГУ;

А.В. Кушнеров, старший преподаватель кафедры дифференциальных уравнений и системного анализа механико-математического факультета БГУ;

О.А. Лаврова, доцент кафедры дифференциальных уравнений и системного анализа механико-математического факультета БГУ, кандидат физико-математических наук, доцент;

Д.Н. Чергинец, доцент кафедры дифференциальных уравнений и системного анализа механико-математического факультета БГУ, кандидат физико-математических наук;

Н.Л. Щеглова, доцент кафедры дифференциальных уравнений и системного анализа механико-математического факультета БГУ, кандидат физико-математических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой дифференциальных уравнений и системного анализа Белорусского государственного университета (протокол №12 от 28.05.2021);

Советом механико-математического факультета Белорусского государственного университета (протокол № 8 от 29.06.2021)

Заведующий кафедрой дифференциальных уравнений и системного анализа



Л.Л. Голубева

Декан механико-математического факультета



С.М. Босяков

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа предназначена для студентов 1 и 2 курса специальности 1-31 03 09 Компьютерная математика и системный анализ очной формы получения высшего образования I степени.

В соответствии с учебными планами специальности № G31-1-019/уч. от 25.05.2021 и № G31-1-004/уч.ин. от 31.05.2021 учебная вычислительная практика проводится дважды: во 2 семестре – «Вычислительная 1», в 4 семестре – «Вычислительная 2». Продолжительность каждой практики составляет 2 недели (108 часов), трудоемкость – 3 зачетные единицы.

Программа разработана в соответствии:

- с Кодексом Республики Беларусь об образовании от 13 января 2011 г.;
- с пунктом 4 Положения о практике студентов, курсантов, слушателей, утвержденного постановлением Совета Министров Республики Беларусь от 03.06.2010 № 860;
- с постановлением Министерства образования Республики Беларусь от 06.04.2015 г. «Порядок разработки и утверждения учебных программ и программ практики для реализации содержания образовательных программ высшего образования»
- с постановлением Министерства образования Республики Беларусь от 20.03.2012 г. № 24 «Об утверждении Инструкции о порядке и особенностях прохождения практики студентами, которым после завершения обучения присваиваются педагогические квалификации»;
- с Положением о практике Белорусского государственного университета от 07.02.2014 (Приказ № 46 – ОД).

Практика является обязательным компонентом высшего образования. Учебная практика является видом учебно-воспитательного процесса, предназначенного для подготовки студентов к профессиональной деятельности, в основном путем самостоятельного решения предусмотренных программой реальных заданий исследовательского характера. Вычислительная практика на первом курсе в основном нацелена на совершенствование компетенций, получаемых при освоении дисциплин «Компьютерная математика» и «Введение в специальность». На втором курсе вычислительная практика по тематике заданий близка к дисциплине «Математические основы защиты информации».

Основной *целью* учебной вычислительной практики является развитие навыков компьютерного моделирования при выполнении индивидуальных заданий, связанных со специальностью.

Основными *задачами* учебной вычислительной практики на первом курсе являются:

- ознакомление студентов с современным состоянием вычислительной техники и ее программного обеспечения;

- исследование и разработка моделей, алгоритмов, методов, программных решений, инструментальных средств по тематике выполняемых научно-исследовательских проектов;
- разработка и исследование математических, информационных и имитационных моделей в определенной предметной области.

На втором курсе *задачами* учебной вычислительной практики являются:

- исследование и разработка моделей, алгоритмов, методов, программных решений, инструментальных средств, применяемых в криптографии;
- развитие способности реализации алгоритмов на языках программирования Wolfram Language и Python;
- совершенствование навыков работы в команде.

В результате прохождения практики студент должен

знать:

- правила осуществления работ и требования техники безопасности;
- основные методы, способы и средства получения, хранения, обработки информации;
- современные информационные технологии;
- методы решения научно-технических и информационных задач;
- идеологию и основные принципы работы с системами компьютерной математики: *Mathematica*, Python;
- компьютерные пакеты для подготовки электронных научных документов: LaTeX, *Mathematica*, MS Word;
- принципы построения математических и компьютерных моделей.

уметь:

- решать типовые задачи математики и информатики;
- применять современные информационные технологии и методы реализации решения прикладных задач.
- проводить научные исследования в области математики, математических методов системной интеграции, проектирования и создания информационных систем, моделирования и проектирования компьютерных комплексов для решения научных, народнохозяйственных и др. задач;
- анализировать, проектировать, разрабатывать и реализовывать программные компоненты этих комплексов;
- работать самостоятельно и в команде;

владеть:

- практическими навыками и умениями для профессиональной деятельности по получаемой специальности;
- современными приёмами и методами поиска и использования научно-технической информации, редактировать, реферировать математические и компьютерные разработки, статьи, готовить рукописи к печати;

- навыками самостоятельной научно-исследовательской работы по избранной специальности;
- системным и сравнительным анализом;
- навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;
- навыками устной и письменной коммуникаций, способностью к межличностным коммуникациям.

В качестве баз для проведения учебной вычислительной практики, как правило, выбираются кафедры и учебные лаборатории механико-математического факультета БГУ. Вычислительная практика может проводиться на предприятиях, в учреждениях и организациях.

Допускается совмещение практики с теоретическим обучением.

Учебная вычислительная практика студентов организуется деканатом механико-математического факультета совместно с кафедрой дифференциальных уравнений и системного анализа.

Все поставленные перед практикантом задачи должны выполняться им самостоятельно в тесном взаимодействии с руководителем практики от кафедры. Его помощь в ходе выполнения работ должна заключаться в консультациях, пояснениях и проверке выполненных работ.

Защита индивидуальных заданий может быть организована в виде докладов с презентацией перед учебной группой.

Дифференцированный зачет студент сдает руководителю практики от кафедры в течение первых двух недель после окончания практики в соответствии с графиком образовательного процесса. При этом критериями оценки являются актуальность тематики заданий, достоверность полученных результатов, степень самостоятельного выполнения заданий, креативность, объем проделанной работы.

Если практика проходит после летней экзаменационной сессии, то дифференцированный зачет студент может сдавать руководителю практики от кафедры в течение первых двух недель следующего учебного года.

СОДЕРЖАНИЕ ПРАКТИКИ

При прохождении практики студенты изучают:

- математические методы, используемые в информатике, экономике и финансовой деятельности;
- состояние современных информационных технологий и их использование в различных сферах деятельности;
- оборудование, аппаратуру, электронно-вычислительную технику, контрольно-измерительные приборы и инструменты, используемые в учебном процессе, научных исследованиях и практической работе;
- создание и обеспечение безопасных и здоровых условий труда при работе с вычислительной техникой.

При прохождении практики студенты разрабатывают, реализуют и исследуют:

- математические структуры и модели;
- математические модели в информационных, экономических и финансовых системах;
- алгоритмы и методы решения задач в рамках полученных математических моделей;
- информационные технологии и программное обеспечение для решения полученных задач;
- автоматизированные системы управления в целом и отдельные их модули.

Во время прохождения учебной вычислительной практики каждый студент получает индивидуальное задание.

Примерный перечень тем по учебной практике на первом курсе

Раздел 1. Компьютерное моделирование с *Mathematica*.

Тема 1. Создание электронного научного документа в среде *Mathematica*.

Тема 2. Восстановление некоторого закона на основе заданных его свойств.
Моделирование Гамма-функции.

Тема 3. Функциональный подход в программировании на примерах решения задач планиметрии. Основы графики.

Тема 4. Методология объектно-ориентированного анализа, проектирования и программирования на примере моделирования классической головоломки «Ханойские башни».

Тема 5. Рекурсия, локальные преобразования, объектно-ориентированный подход при моделировании доски Гальтона.

- Тема 6. Метод неопределенных коэффициентов в задаче разложения рациональной дроби на сумму дробей.
- Тема 7. Операторы Map-группы и функции повторного действия при описании итерационных процессов. Моделирование конформных отображений.

Раздел 2. Основные принципы программирования в Python.

- Тема 1. Элементы символьной математики. Решение задач механики и планиметрии.
- Тема 2. Матричное описание геометрических объектов. Правильный многоугольник Рело.
- Тема 3. Структура данных бинарное дерево. Сортировка числовой последовательности.
- Тема 4. Структура данных стек. Вычисление арифметического выражения по постфиксной записи.
- Тема 5. Работа со строковыми данными. Лексический анализ текста.
- Тема 6. Конечный автомат. Лексический анализ текста.

Примерный перечень тем по учебной практике на втором курсе

Раздел 3. Теоретико-числовые алгоритмы криптографии

- Тема 1. Криптовалюта Биткоин. Алгоритмы формирования транзакции.
- Тема 2. Проект “Large Bitcoin Collider”.
- Тема 3. Эллиптическая кривая secp256k1. Её свойства.
- Тема 4. Криптовалюта Биткоин. Хранение ключей.
- Тема 5. Эллиптические кривые. Квадратные уравнения в группе точек эллиптической кривой.
- Тема 6. Криптовалюта Peercoin. Proof of Work vs Proof of Stake.
- Тема 7. Криптовалюта Cardano. Proof of Work vs Proof of Stake.
- Тема 8. Поиск двухблочных коллизий функции хеширования md5.
- Тема 9. Поиск одноблочных коллизий функции хеширования md5.
- Тема 10. Функция хеширования SHA-3.
- Тема 11. Суперсингулярные эллиптические кривые.
- Тема 12. Эллиптические кривые. Проективные координаты.
- Тема 13. Неприводимые и примитивные многочлены.
- Тема 14. Оптимальные нормальные базисы.

Тема 15. Гауссовы нормальные базисы.

Тема 16. Конгруэнтные числа и эллиптические числа.

Тема 17. Спаривание Вейля на эллиптических кривых.

Тема 18. Спаривание Тейта на эллиптических кривых.

Тема 19. Ро-метод Полларда нахождения дискретного логарифма.

Тема 20. Алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых.

Тема 21. Тестирование чисел на простоту с помощью эллиптических кривых.

Тема 22. Дискретное логарифмирование в поле Z_p . Алгоритм COS.

Тема 23. Решение полиномиальных уравнений в поле $GF(p)$, p – простое.

Тема 24. Шифр Виженера. Частотный анализ.

Тема 25. Криптовалюта Биткоин. Алгоритм выбора монет при формировании платежа.

Тема 26. Дискретный логарифм. Умножение по правилу сложения (исследовательская тема).

Тема 27. Асимптотика неаналитических интегралов (тема по математическому анализу).

Тема 28. Вычисление обратного элемента в поле Z_p . Расширенный алгоритм Евклида vs Малая теорема Ферма.

Тема 29. Скрученные эллиптические кривые Эдвардса.

Тема 30. Стратегии ставок на футбольные матчи.

Тема 31. Стратегии скрещивания CryptoKitties.

При получении значимых результатов индивидуальная работа студента может представляться на конкурсы, конференции, выставки.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

1. Требования к содержанию и оформлению индивидуального задания и отчета по практике

Руководитель практики от кафедры выдает студенту индивидуальное задание на практику и помогает составить календарный план работы на период практики.

Индивидуальное задание должно соответствовать специальности студентов и отражать основные направления развития информационных технологий. Тема индивидуального задания должна выбираться и формулироваться таким образом, чтобы:

- быть актуальной, то есть исследования и разработки могли иметь научное и практическое значение;
- иметь внутреннюю цельность, то есть не состоять из многих слабо связанных друг с другом частей;
- предлагаемые в задании исследования и разработки были выполнимы за время практики;
- выполнение задания в полном объеме позволяло получить весомые, обоснованные и защищаемые результаты.

Четко сформулированные задания позволяют легко контролировать ход практики, оперативно вносить изменения при минимальном ухудшении качества ее прохождения.

В течение последней недели практики студент составляет письменный отчет о выполнении программы практики. Оформленный отчет представляется на рецензирование руководителю практики от кафедры.

Отчет по практике должен содержать:

- титульный лист;
- задание на вычислительную практику;
- содержание (оглавление);
- введение;
- основную часть отчета;
- заключение;
- список использованных источников;
- приложения.

Во введении должны быть отражены:

- цель практики;
- перечень работ, выполненных в процессе практики.

В основную часть отчета необходимо включить:

- описание организации работы в процессе практики;

- описание выполненной работы по разделам программы практики и индивидуального задания;
- описание практических задач, решаемых студентом за время прохождения вычислительной практики;
- анализ наиболее сложных и характерных случаев, изученных студентом;
- указания на затруднения, которые возникли при прохождении практики;
- изложение спорных вопросов, которые возникли при прохождении практики, и их решение.

Заключение должно содержать:

- описание навыков, приобретенных за время практики;
- характеристику информационно-программных продуктов, изученных при прохождении вычислительной практики;
- предложения и рекомендации студента, сделанные в ходе практики.

3.2. Методические указания для студентов и руководителей практики

Основной формой обучения при прохождении практики является самостоятельная работа студента, которая состоит из следующих элементов:

- изучение теоретического материала;
- выполнение индивидуальных заданий;
- проведение вычислительных экспериментов;
- формулировка выводов и рекомендаций.

При изучении теоретического материала следует переходить к следующему разделу только после правильного понимания предыдущего. Полезно вести список литературных источников с краткой аннотацией каждого источника. Рекомендуется широкое применение поиска требуемой информации в Internet, с сохранением нужных web-адресов. Выводы, полученные при изучении теоретического материала, оформляются в виде обзора с обязательными ссылками на источники информации.

Выполнение индивидуальных заданий имеет большое значение, так как приучает студента к необходимому в работе порядку, дисциплине, правильному планированию рабочего времени. Руководителю необходимо указывать время, отводимое для выполнения задания, вид требуемого результата. Не следует перегружать студента заданиями и выдавать несколько заданий одновременно.

При проведении исследований, вычислительных и иных экспериментов выясняется умение студента применять полученные знания для впервые рассматриваемых задач. Руководителю практики следует точно определить степень трудности решения задачи и возможности практиканта. Исследование или эксперимент должны завершаться выводами и рекомендациями по применению полученных результатов.

Если в процессе работы у студента возникают вопросы, разрешить которые самостоятельно не удастся, то он обращается к руководителю для получения от него консультации. Студент должен точно указать, в чем он испытывает затруднение, характер затруднения и предполагаемый план действий.

3.3. Организация практики в виде работы в команде

На втором курсе практика может проходить в форме работы в команде над проектом. Руководитель практики назначает директоров команд из числа студентов с наиболее высоким средним баллом за первый курс. Директора набирают в свои команды сотрудников из числа оставшихся студентов группы. В командах могут быть следующие должности:

- директор;
- системный аналитик;
- математик;
- программист;
- тестировщик;
- другая должность на усмотрение директора.

В командах может быть несколько человек с одинаковой должностью в зависимости от специфики темы проекта. Команда как правило состоит из 4-6 человек.

Требования к должностям.

1. Директор

- выбирает тему проекта из предложенных руководителем или предлагает свою тему и согласует её с руководителем практики;
- формирует команду, распределяет обязанности;
- организует работу команды;
- контактирует с каждым членом команды, разрешает возникающие проблемы;
- принимает решения, касающиеся выполнения проекта;
- контролирует выполнение работы точно в срок;
- пишет отчет руководителю о проделанной работе с характеристикой каждого члена команды.

2. Системный аналитик (Бизнес-аналитик)

- контактирует с заказчиком (руководитель практики) для выявления требований к проекту и формулировки задач, а также при возникновении вопросов и проблем при реализации проекта;
- совместно с математиком и программистом пишет техническое задание для программиста;
- пишет стандарт;

- готовит презентацию.

3. Математик

- анализирует и решает поставленные наукоемкие задачи:
 - разрабатывает алгоритмы;
 - исследует алгоритмы на: детерминированность, полиномиальность, возможность выдавать неправильный ответ или не выдавание ответа;
 - исследует криптостойкость.
- в процессе работы взаимодействует с программистом и системным аналитиком;
- пишет стандарт.

4. Программист

- изучает поставленные задачи;
- изучает и анализирует текущее техническое задание;
- советует, указывает на недоработки и неясные ему моменты в техническом задании системному аналитику и математику;
- программирует;
- пишет комментарии к коду.

5. Тестировщик

- изучает и анализирует поставленные задачи, тех. задание и код программы;
- проверяет соответствие технического задания поставленным задачам;
- проверяет соответствие кода программы техническому заданию;
- выбирает способ тестирования кода программы;
- тестирует код программы;
- при наличии ошибок отправляет проект на доработку;
- предоставляет отчет о проделанной работе руководителю.

Руководитель практики

- разрабатывает темы проектов, указывая на особо интересующие его моменты в данных темах;
- назначает директоров;
- консультирует всех студентов при помощи электронной почты, социальных сетей и на практике в аудитории;
- проверяет стандарт, код программы и отчеты;
- зачет проходит в форме беседы с командой после того как команда:
 - вышлет файлы по почте и руководитель с ними ознакомится;
 - выступит с презентацией.

К защите практики необходимо предоставить ссылку на <https://github.com> (работа в команде проходит при помощи git), где размещены:

- Стандарт (синонимы в зависимости от специфики темы проекта: техническое описание проекта, научно-популярная статья, учебное пособие);
- Код с описанием (как правило в *Mathematica* или Python);
- Выступление с презентацией;
- Характеристика каждого члена команды (что было поручено, что сделано, личностные характеристики).