МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.
_____
«__» _____ 202_ г.

Рабочая программа дисциплины (модуля)

Практика «Алгоритмы теории чисел» дисциплины «Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)»

Направление подготовки бакалавриата
09.03.01 Информатика и вычислительная техника
Профиль подготовки бакалавриата
Вычислительные машины, комплексы, системы и сети

Квалификация (степень)
Бакалавр

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Молчанов В. А.		22.09.21
Председатель НМК	Кондратова Ю.Н.		22.09.2021
Заведующий кафедрой	Тяпаев Л.Б.		22.09.21
Специалист Учебного управления			

1. Цели освоения дисциплины

Целью Практики «Алгоритмы теории чисел» по дисциплине «Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)» является овладение классическими теоретико-числовыми методами и алгоритмами, такими как:

- вычисления в кольцах вычетов;
- методы решения систем линейных уравнений над конечными полями и конечными кольцами;
- алгоритмы проверки простоты целых чисел;
- методы факторизации целых чисел;
- алгоритмы дискретного логарифмирования.

Задачами дисциплины являются: углубление математического образования и развитие практических навыков в области прикладной математики и информатики; формирование у студентов научного представления об основных положениях, понятиях и достижениях современной теории чисел; изучение теоретических основ информатики; освоение современных теоретико-числовых методов.

2. Место дисциплины в структуре ООП

Практика (дисциплина) «Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)» (Б2.О.01) является обязательной практикой части, формируемой участниками образовательных отношений, Блока 2 «Практика» учебного плана ООП бакалавриата по направлению 09.03.01-« Информатика и вычислительная техника», профилю «Вычислительные машины, комплексы, системы и сети». На ее изучение отводится 108 часов. Согласно учебному плану направления и профиля подготовки данный курс в четвертом семестре заканчивается зачетом.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин ««Информатика и программирование», «Алгебра», «Дискретная математика», «Математическая логика и теория алгоритмов».

Компетенции, сформированные при изучении данной дисциплины, необходимы при изучении дисциплин «Введение в криптографию», «Теория кодирования и передачи данных».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода,	**1.1.УК-1.** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	Знать основные понятия теории чисел и методы их применения в компьютерной науке. Уметь находить решения

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
вырабатывать стратегию действий	**1.2.УК-1.** Осуществляет поиск алгоритмов решения поставленной проблемной ситуации на основе доступных источников информации. Определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей детальной разработке. Предлагает способы их решения. **1.3.УК-1.** Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности	поставленной проблемной ситуации с помощью методов теории чисел. Владеть навыками эффективного решения алгоритмических задач теории чисел и ее приложений.
УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(-ых) языке(ах).	**УК-4.1**. Знать: литературную форму государственного языка, основы устной и письменной коммуникации на иностранном языке, функциональные стили родного языка, требования к деловой коммуникации. **УК-4.2**. Уметь: выражать свои мысли на государственном, родном и иностранном языке в ситуации деловой коммуникации. **УК-4.3.** Владеть: практический опыт составления текстов на государственном и родном языках, опыт перевода текстов с иностранного языка на родной, опыт говорения на государственном и иностранном языках.	Знать основные источники информации по теории алгоритмов и теории чисел; способы извлечения необходимой информации из электронных и бумажных носителей, основные методы теории чисел, направления их применения в прикладных областях; формулировки основных результатов теории чисел, методы их доказательства, возможные сферы их приложений. Уметь использовать методы и приемы формализации задач; разрабатывать математические модели процессов и явлений, относящихся к исследуемому объекту; разрабатывать основные алгоритмы математических моделей на базе языков и

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
		пакетов прикладных программ; решать типовые задачи теории чисел; формулировать и обосновывать основные результаты теории алгоритмов и теории чисел. Владеть методами формализации задач, навыками математического моделирования процессов и явлений, относящихся к исследуемому объекту; навыками построения основных алгоритмов математических моделей на базе языков и пакетов прикладных программ; основной терминологией, методами и и понятийным аппаратом теории алгоритмов и теории чисел.
УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.	**УК-6.1.** Знать: основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда. **УК-6.2.** Уметь: планировать свое рабочее время и время для саморазвития. формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей. **УК-6.3.** Владеть: практический опыт получения дополнительного образования, изучения	Знать способы извлечения необходимой информации из электронных и бумажных носителей в предложенной для исследования предметной области; основные факты теории чисел и выбранной предметной области, направления ее применения в приложениях; формулировки основных результатов, возможные сферы их связи и приложения в других областях математического знания и дисциплинах естественно-научного содержания. Уметь анализировать задачи, выделяя их базовые составляющие; осуществлять декомпозицию задачи; находить и критически анализировать информацию, необходимую для решения

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	дополнительных образовательных программ.	проблемы предметной области. Владеть навыками выбора оптимального решения для поставленной задачи.
ПК-3. Способен интегрировать аппаратные и программные средства в составе информационных и автоматизированных систем.	**ПК-3.1.** Знать: интерфейсы взаимодействия внутренних модулей системы **ПК-3.2.** Уметь: писать программный код процедур интеграции программных модулей **ПК-3.3.** Владеть: навыками использования выбранной среды программирования для разработки процедур интеграции программных модулей.	Знать интерфейсы взаимодействия внутренних модулей системы. Уметь интегрировать аппаратные и программные средства в составе информационных и автоматизированных систем. Владеть навыками использования выбранной среды программирования для разработки процедур интеграции программных модулей.
ПК-4. Способен разрабатывать компоненты программно-аппаратных комплексов и баз данных, используя современные инструментальные средства и технологии программирования.	**ПК-4.1.** Знать: компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними **ПК-4.2.** Уметь: использовать выбранную среду программирования **ПК-4.3.** Владеть: навыками разработки программного обеспечения.	Знать компоненты программно-технических архитектур, их приложения и интерфейсы взаимодействия с ними. Уметь выбирать и профессионально использовать среду программирования. Владеть навыками разработки программного обеспечения программно-аппаратных комплексов и баз данных .

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)	Формы текущего контроля успеваемости *(по неделям семестра)* Формы промежуточной аттестации *(по*

								семестрам)
				лекции	Практические занятия		КСР	
					Общая трудоемкость	Из них – практическая подготовка		
1	Арифметические операции над целыми числами и многочленами	4	1	–	10	10	–	Тестирование программ. Обсуждение очередного задания.
2	Непрерывные дроби	4	2	–	10	10	–	Тестирование программ. Обсуждение очередного задания.
3	Квадратичные вычеты	4	3	–	10	10	–	Тестирование программ. Обсуждение очередного задания.
	Решение систем линейных уравнений над конечными полями	4	4-5	2	16	16	2	Тестирование программ. Обсуждение очередного задания.
	Проверка чисел на простоту	4	6-7	–	18	18	–	Тестирование программ. Обсуждение очередного задания.
	Построение больших простых чисел	4	8	–	10	10	–	Тестирование программ. Обсуждение очередного задания.
	Факторизация целых чисел	4	9-10	–	18	18	–	Тестирование программ. Обсуждение очередного

								задания.
	Дискретное логарифмирование	4	13-14	–	16	16	–	Тестирование программ. Обсуждение очередного задания.
Промежуточная аттестация								Зачет Защита проекта
Итого		**4**		**108**	**108**			

Содержание дисциплины

Арифметические операции над целыми числами и многочленами. Сложность арифметических операций. Свойства функции оценки сложности. Сложность арифметических операций с целыми числами. Сложность алгоритма Евклида. Сложность операций в кольце вычетов. Приложения модулярной арифметики.

Непрерывные дроби. Определение непрерывной дроби. Подходящие дроби, свойства подходящих дробей. Представление действительных чисел непрерывными дробями. Приложения непрерывных дробей.

Квадратичные вычеты. Определение квадратичного вычета. Задачи существования квадратичных вычетов и вычисления квадратных корней. Определение и свойства символов Лежандра и Якоби. Вычисление квадратных корней по простому модулю. Вычисление квадратных корней по составному модулю. Целые числа Блюма. Генератор псевдослучайных чисел BBS. Вероятностное шифрование.

Решение систем линейных уравнений над конечными полями. Решение систем линейных уравнений методом Гаусса. Алгоритм Ланцоша. Алгоритм Видемана.

Проверка чисел на простоту. Распределение простых чисел. Элементарные методы проверки простоты чисел. Решето Эратосфена. Тест на основе малой теоремы Ферма. Свойства чисел Кармайкла. Тест Соловея-Штрассена. Тест Рабина-Миллера.

Построение больших простых чисел. Критерий Люка. Метод Маурера. Числа Мерсенна.

Факторизация целых чисел. Метод Ферма. ρ-метод Полларда. (p-1)-метод Полларда.

Дискретное логарифмирование в конечном поле. Задача дискретного логарифмирования в циклической группе. Алгоритм Гельфонда-Шенкса. ρ-метод Полларда. Дискретное логарифмирование в конечном поле.

План лабораторных занятий

На лабораторных занятиях студенты под руководством преподавателя самостоятельно выполняют задания лабораторных работ с практической

реализацией основных теоретико-числовых алгоритмов в форме компьютерных программ с использованием языков программирования высокого уровня.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1-2	Арифметические операции над целыми числами и многочленами	№1
3-4	Непрерывные дроби	№2
5-6	Квадратичные вычеты	№3
7-8	Решение систем линейных уравнений над конечными полями	№ 5
9-10	Проверка чисел на простоту	№ 6
11	Построение больших простых чисел	№ 7
12-13	Факторизация целых чисел.	№ 8
14-15	Дискретное логарифмирование в конечном поле.	№ 9

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как проведение коллоквиумов по ключевым для приложений темам, привлечение студентов к работе в научном семинаре кафедры, к переводам текстов из зарубежных изданий по дисциплине, демонстрация работы компьютерных программ по прикладной универсальной алгебре и теории автоматов, встречи со специалистами из профильных организаций и фирм.

При проведении занятий по данному курсу используются следующие активные и интерактивные формы обучения: контрольные работы, коллоквиумы.

В рамках практической подготовки по данной дисциплине используются кейс-задания, выполнение которых направлено на формирование таких профессиональных действий как применение современного математического аппарата и фундаментальных концепций при решении прикладных задач с помощью информационных технологий; разработка алгоритмических и программных решений в области компьютерных наук. Примеры кейс-заданий приведены в фонде оценочных средств дисциплины.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

В рамках самостоятельной работы студенты более углубленно осваивают преподаваемый материал и могут проявить себя в научно-исследовательской работе, тематика которой предполагается тесно связанной с изучаемым материалом.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, контрольные вопросы, вопросы для проведения промежуточной аттестации (*зачёт*).

Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе Практики «Алгоритмы теории чисел» по дисциплине «Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)»

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
5	25	0	0	20	0	25	30	**100**
6	10	20	0	15	0	25	30	**100**

Программа оценивания учебной деятельности студента

Лекции

Не предусмотрены

Лабораторные занятия

Не предусмотрены

Практические занятия

Посещаемость, опрос, активность и др. – от 0 до 25 баллов.

Самостоятельная работа

Выполнение лабораторных работ в течение семестра – от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Не предусмотрены.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *зачёт*, проводимый в виде устного собеседования.

При проведении промежуточной аттестации

ответ на «отлично» / «зачтено» оценивается от 25 до 30 баллов;

ответ на «хорошо» / «зачтено» оценивается от 15 до 24 баллов;

ответ на «удовлетворительно» / «зачтено» оценивается от 5 до 14 баллов;

ответ на «неудовлетворительно» / «не зачтено» оценивается от 0 до 4 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 4-й семестр по Практике «Алгоритмы теории чисел» по дисциплине «Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)» составляет **100** баллов

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Прикладная универсальная алгебра» в оценку (зачет)

50 баллов и более	«зачтено»
меньше 50 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины

В разделе литературы желательно указывать издания (учебные и учебно-методические пособия), изданные в 2012-2021 гг. (по гуманитарным, социальным и экономическим изданиям в 2017-2021 гг.).

В списке литературы необходимо отдавать предпочтение источникам, размещенным в электронных библиотеках (ЭБС), на которые есть ссылки из электронного каталога ЗНБ СГУ

http://library.sgu.ru//cgi-bin/irbis64r_plus/cgiirbis_64_ft.exe?IS_FIRST_AUTH=false&Z21ID=GUEST&C21COM=F&I21DBN=AUTHOR&P21DBN=NIKA&Z21FLAGID=1

, при этом в списке литературы обязательно указывать ссылку на источник.

В списке литературы указывается как минимум 3 источника, но не более 8.

а) литература:

1) Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М. М. Глухов [и др.]. - Москва : Лань, 2011. - 394 с. : табл. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1116-0 : Б. ц. URL: https://e.lanbook.com/book/1540. Загл. с экрана. Яз. рус.

2) Бухштаб, А. А. Теория чисел [Электронный ресурс] : учеб. пособие / А. А. Бухштаб. - Москва : Лань", 2015. - 384 с. : ил. ; 21 см. - (Классическая учебная литература по математике) (Учебники для вузов. Специальная литература). - Библиогр. в тексте. - ISBN 978-5-8114-0847-4 : Б. ц. URL: https://e.lanbook.com/book/65053. Загл. с экрана. Яз. рус.

3) Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии [Текст] : учеб. пособие / А. В. Черемушкин. - Москва : МЦНМО, 2002. - 103, [1] с. - Библиогр.: с. 100-103 (59 назв.). - ISBN 5-94057-060-7.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Visual C++ 4.2, Visual Studio 2010, Visual Studio 2012, Visual Studio 2013, Visual Studio 2015

2) Свободное программное обеспечение: Java Developers Kit, NetBeans IDE, Eclipse, CPython, Jython, IronPython.

9. Материально-техническое обеспечение дисциплины

Для проведения практических занятий необходим компьютерный класс со стандартным программным обеспечением и доступом к сети Интернет.

В отведенных для занятий аудиториях имеются учебные доски для визуализации информации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника и профилю подготовки «Вычислительные машины, комплексы, системы и сети».

Программа одобрена на заседании кафедры дискретной математики и информационных технологий Протокол №2 от 22.09.2021 года

Автор

Профессор кафедры дискретной математики и информационных технологий, д.ф.-м.н., профессор В. А. Молчанов