

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Д. А. Таюрский

» _____ 20__ г.

подписано электронно-цифровой подписью

Программа дисциплины

Общая алгебра и теория чисел

Направление подготовки: 01.03.04 - Прикладная математика

Профиль подготовки: Математическое моделирование

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
 - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Кугураков В.С. (кафедра теоретической кибернетики, отделение фундаментальной информатики и информационных технологий), Vladimir.Kugurakov@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-10	Готовность применять математический аппарат для решения поставленных задач, способностью применить соответствующую процессу математическую модель и проверить ее адекватность, провести анализ результатов моделирования, принять решение на основе полученных результатов
ПК-12	Способность самостоятельно изучать новые разделы фундаментальной математики

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

роль языка алгебраических структур при описании различных объектов исследования;

Должен уметь:

ориентироваться в иерархии алгебраических структур;

Должен владеть:

теоретическими знаниями о базовых алгебраических системах - группах, кольцах, полях и др.;

Должен демонстрировать способность и готовность:

приобрести навыки использования алгебраического аппарата при решении прикладных задач.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.20 Дисциплины (модули)" основной профессиональной образовательной программы 01.03.04 "Прикладная математика (Математическое моделирование)" и относится к дисциплинам по выбору.

Осваивается на 3 курсе в 6 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 36 часа(ов), в том числе лекции - 0 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 6 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1	Тема 1. Введение. Множества и отображения. Арифметика целых					

чисел. Введение в алгебраические структуры.

6

0

0

12

12

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Группы. Кольца и поля. Многочлены и кольца многочленов.	6	0	0	12	12
3.	Тема 3. Теория полей. Строение конечных полей.	6	0	0	12	12
	Итого		0	0	36	36

4.2 Содержание дисциплины (модуля)

Тема 1. Введение. Множества и отображения. Арифметика целых чисел. Введение в алгебраические структуры.

Введение. Предмет дисциплины Общая алгебра и теория чисел. Исторические сведения о развитии данного раздела математики. Роль и место общей алгебры в системе математического образования. Множества и отображения. Отношения эквивалентности. Факторизация отображений. Арифметика целых чисел. Основная теорема арифметики. НОД и НОК. Алгоритм деления в \mathbb{Z} . Некоторые теоретико-числовые функции. Мультипликативные функции. Функции Мебиуса и Эйлера. Формула обращения Мебиуса. Сравнения в \mathbb{Z} . Полная и приведенная системы вычетов по $\text{mod } n$. Теоремы Эйлера и Ферма. Китайская теорема об остатках.

Тема 2. Группы. Кольца и поля. Многочлены и кольца многочленов.

Введение в алгебраические структуры. Множества с бинарной операцией. Gruppoиды. Полугруппы. Моноиды. Группы. Кольца и поля. Группы. Симметрическая и знакопеременная группы. Морфизмы групп. Теорема Кэли. Смежные классы по подгруппе. Теорема Лагранжа. Циклические группы. Нормальные подгруппы. Факторгруппы. Мультипликативная группа целых чисел по $\text{mod } n$. Кольца и поля. Общие свойства колец. Типы колец. Сравнения. Кольцо классов вычетов по $\text{mod } n$. Факторкольца. Гомоморфизмы и идеалы колец. Области целостности и поля. Характеристика кольца и поля. Простые поля. Многочлены и кольца многочленов. Элементарные свойства многочленов. Алгоритм Евклида. Однозначность разложения на простые множители. Факториальность евклидовых колец. Поле отношений целостного кольца. Поле рациональных функций. Простейшие дроби. Корни многочленов. Интерполяционные формулы.

Тема 3. Теория полей. Строение конечных полей.

Теория полей. Присоединение. Простые расширения полей. Конечные и алгебраические расширения. Алгебраическое замыкание. Поля разложения. Конечные поля Гауа. Строение конечных полей. Характеризация конечных полей. Циклическая мультипликативная группа поля. Единственность конечного поля заданного порядка. Критерий подполя. Корни многочленов. Разложение многочленов на неприводимые сомножители. Представление элементов конечных полей. Вычисления в конечных полях. Некоторые приложения конечных полей.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

М. Анохин, Блочные криптографические алгоритмы. - Отличный краткий обзор современного состояния криптоанализа на русском языке. - <http://www.cryptography.ru/db/msg.html?mid=1162999&uri=node4.html>

Материалы онлайн-курсов Массачусетского Технологического Института - <http://ocw.mit.edu/index.htm>

Портал математических интернет-ресурсов - <http://www.math.ru/>

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Бухштаб А.А. Теория чисел. - <http://eek.diary.ru/p54405820.htm>

Википедия - http://ru.wikipedia.org/wiki/%D2%E5%E8%FF_%F7%E8%F1%E5%EB

Дэвенпорт Г. Высшая арифметика. Введение в теорию чисел. - <http://eek.diary.ru/p54405820.htm>

З. И. Борович, И. Р. Шафаревич Теория чисел. - <http://eek.diary.ru/p54405820.htm>

Кузьмин М.С. - <http://inc.istu.ru/index.php/remository?func=fileinfo&id=253>

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лабораторные работы	Самостоятельная работа предполагает выполнение письменных домашних работ. Практические задания, выполняемые, как правило, вне аудитории, предназначены для усвоения общих методов решения задач определенного типа. Работа заключается в самостоятельной проработке пройденных на занятиях тем. Закрепить навыки можно лишь в результате самостоятельной работы.

Вид работ	Методические рекомендации
самостоятельная работа	Обучение происходит в форме лабораторных занятий, а также самостоятельной работы студентов. Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для более глубокого понимания разделов дисциплины "Общая алгебра и теория чисел" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения. Самостоятельная работа предполагает выполнение письменных домашних работ. Практические задания, выполняемые, как правило, вне аудитории, предназначены для усвоения общих методов решения задач определенного типа. Работа заключается в самостоятельной проработке пройденных на занятиях тем. Закрепить навыки можно лишь в результате самостоятельной работы.
зачет	Заключительная часть самостоятельной работы - подготовка к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. При подготовке к экзамену нужно использовать конспекты лекций, литературу и источники из интернета, данные преподавателем. Лучше, если можно перевыполнить план, тогда всегда будет резерв времени. Для подготовки необходимо использовать конспекты лекций, рекомендуемую литературу и источники из интернета.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 01.03.04 "Прикладная математика" и профилю подготовки "Математическое моделирование".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.20 Общая алгебра и теория чисел

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.03.04 - Прикладная математика

Профиль подготовки: Математическое моделирование

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

Основная литература:

1. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - (Высшее образование) ISBN 978-5-369-01450-9
Режим доступа: <http://znanium.com/bookread2.php?book=495249>
2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. Режим доступа: <http://znanium.com/bookread.php?book=402686>
3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. Режим доступа: <http://znanium.com/bookread.php?book=405000>

Дополнительная литература:

1. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с.- Режим доступа: <http://znanium.com/catalog.php?bookinfo=441493>
2. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие. - Казань: Казанский университет, 2012. - 138 с. - Режим доступа: <http://kpfu.ru/docs/F366166681/mzi.pdf>

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.20 Общая алгебра и теория чисел

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 01.03.04 - Прикладная математика

Профиль подготовки: Математическое моделирование

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.