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: 01.04.04 - Прикладная математика
Профиль подготовки: Классические и квантовые методы обработки информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

Содержание

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-2	Способен к проведению научно-исследовательских разработок по отдельным разделам темы
ПК-3	Способен применять знания и методы дисциплин естественно-научного и математического цикла при проведении научных исследований, в том числе математического и компьютерного моделирования и высокопроизводительных вычислений

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

и понимать роль языка алгебраических структур при описании различных объектов исследования,

обладать теоретическими знаниями о базовых алгебраических системах - группах, кольцах, полях, векторных пространствах

и ориентироваться в иерархии алгебраических структур

Должен уметь:

о применять алгебраические и теоретико-числовые методы при описании и анализе блочных и поточных шифров

Должен владеть:

терминологией общей алгебры и теории чисел,

навыками использования алгебраического аппарата при решении прикладных задач,

методикой решения алгебраических уравнений над конечными полями,

алгебраическими методами построения генераторов псевдослучайных чисел

Должен демонстрировать способность и готовность:

использования абстрактного алгебраического аппарата при решении прикладных задач в теории кодирования и криптографической защиты информации.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.05 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.04 "Прикладная математика (Классические и квантовые методы обработки информации)" и относится к вариативной части.

Осваивается на 2 курсе в 3 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 - 28 часа(ов), в том числе лекции - 0 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 28 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 44 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет в 3 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. Тема 1. Введение. Предмет дисциплины ?Общая алгебра и теория чисел?. Множества и отображения.	3	0	0	2	8
3.	Тема 3. Тема 3. Арифметика целых чисел. Модулярная арифметика. китайская теорема об остатках.	3	0	0	4	6
4.	Тема 4. Тема 4. Алгебраические структуры. бинарные алгебры. Полугруппы, Моноиды. Группы.	3	0	0	6	8
6.	Тема 6. Тема 5. Кольца,, тела и поля.	3	0	0	6	10
7.	Тема 7. Тема 6. Многочлены и кольца многочленов.	3	0	0	4	6
8.	Тема 8. Тема 7. Теория полей. Строение конечных полей.	3	0	0	6	6
	Итого		0	0	28	44

4.2 Содержание дисциплины (модуля)

Тема 1. Тема 1. Введение. Предмет дисциплины ?Общая алгебра и теория чисел?. Множества и отображения.

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. Сюръективные и инъективные отображения. Конечные, счетные и континуальные множества, Факторизация отображений.

Тема 3. Тема 3. Арифметика целых чисел. Модулярная арифметика. китайская теорема об остатках.

Арифметика целых чисел.

Основная теорема арифметики. НОД и НОК. Ал-горитм деления в Z. Некоторые теоретико-числовые функции. Мультипликативные функции. Функции Мебиуса и Эйлера. Формула обращения Мебиуса. Сравнения в Z. Полная и приведенная системы вычетов по mod n.

Теоремы Эйлера и Ферма.

Китайская теорема об остатках.

Тема 4. Тема 4. Алгебраические структуры. бинарные алгебры. Полугруппы, Моноиды. Группы.

Алгебраические структуры.

Множества с бинарной операцией.

Группоиды как ассоциативные группоиды.. Полугруппы. нейтральные и обратимые элементы. Моноиды. Группы. Симметрическая и знакопеременная группы. Смежные классы по подгруппе. Нормальные делители. Факторгруппы. Аддитивная группа целых чисел по модулю натурального числа.

Тема 6. Тема 5. Кольца,, тела и поля.

Кольца и поля.

Общие свойства колец. Типы колец.

Сравнения. Кольцо классов вычетов по mod n.

Гомоморфизмы и идеалы колец. Фактор-кольца. Характеристика кольца и поля.

Области целостности и поля. Простые поля.

Равенства Шенемана для полей положительной характеристики..

Характеристика кольца и поля.

Про-стые поля.

Тема 7. Тема 6. Многочлены и кольца многочленов.

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 мно-гочленов. Интерполяционные формулы.

Поле разложения многочлена.

Тема 8. Тема 7. Теория полей. Строение конечных полей.

Теория полей.

Присоединение. Простые расширения полей.

Конечные и алгебраические расширения.

Алгебраическое замыкание. Поля разложения.

Конечные поля Галуа.

Число элементов конечного поля.

Конечное поле как фактор-кольца многочленов по идеалу, порожденному неприводимым многочленом.

Цикличность мультипликативной группы конечного поля.

Вычмсления в еонечных полях.

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

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)

1. Материалы онлайн-курсов Массачусетского Технологического Института - 2. - http://ocw.mit.edu/index.htm

3. Онлайн-курсы лучших университетов мира - - https://www.coursera.org

6. Онлайн-курсы Стенфордского Университета - - http://online.stanford.edu

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

Вид работ	Методические рекомендации
лабораторные работы	Лабораторные работы проводятся в аудиторные часы, и с использованием материала, преподаваемого в аудитории. Дополнительного изучения материала вне аудитории не требуется. Необходимо понимание организации процесса разработки программного обеспечения. Базовые знания разработки ПО (стадии, базовое понимание разработки архитектуры ПО).
самостоя-тельная 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 ″Обшая 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	Для подготовки к зачету следует повторить все письменные записи, изучить основную и дополнительную литературу, рекомендованные интернет-ресурсы. Приветствуется самостоятельное изучение дополнительного материала по теме. Оценивается владение материалом, способность оперировать изученными терминами и определениями. Возникшие вопросы студент должен задать в течении курса и во время консультации.

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.

Специализированная лаборатория.

Специализированная лаборатория.

Специализированная лаборатория.

Специализированная лаборатория.

Специализированная лаборатория.

Специализированная лаборатория.

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 01.04.04 "Прикладная математика" и магистерской программе "Классические и квантовые методы обработки информации".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.05 Общая алгебра и теория чисел

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.04.04 - Прикладная математика

Профиль подготовки: Классические и квантовые методы обработки информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2020

Основная литература:

1. Глухов, М.М. Алгебра [Электронный ресурс] : учебник / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. - Электрон. дан. - Санкт-Петербург : Лань, 2015. - 608 с. - URL: https://e.lanbook.com/book/67458 - (дата обращения: 10.03.2020).

2. Власов Е.Г. Конечные поля в телекоммуникационных приложениях. Теория и применение FEC, CRC, М-последовательностей/ - М.: НИЦ ИНФРА-М, 2016. - 280 с. - (Наука и практика) ISBN 978-5-16-009437-3. - Режим доступа: http://znanium.com/bookread2.php?book=441970 (дата обращения: 10.03.2020).

3. Глибичук А.А., Ильинский Д.В., Мусатов А.М. и др. Основы комбинаторики и теории чисел. Сборник задач: Учебное пособие / - Долгопрудный: Интеллект, 2015. - 104 с. ISBN 978-5-91559-201-7 - Режим доступа: http://znanium.com/catalog.php?bookinfo=538904

4. Смолин, Ю.Н. Алгебра и теория чисел: учеб. пособие / Ю.Н. Смолин. - 5-е изд., стер.-Москва : ФЛИНТА, 2017. - 464 с. - ISBN 978-5-9765-0050-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1034573 (дата обращения: 10.03.2020). - Режим доступа: по подписке.

Дополнительная литература:

Ляпин, Е. С. Упражнения по теории групп : учебное пособие / Е. С. Ляпин, А. Я. Айзенштат, М. М. Лесохин. - 2-е изд., стер. - Санкт-Петербург : Лань, 2010. - 272 с. - ISBN 978-5-8114-1015-6. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/528

(дата обращения: 10.03.2020). - Режим доступа: для авториз. пользователей.

2. Ляпин, Е. С. Курс высшей алгебры : учебник / Е. С. Ляпин. - 3-е изд.,стер. - Санкт-Петербург : Лань, 2009. - 368 с. - ISBN 978-5-8114-0909-9. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/246 (дата обращения: 10.03.2020). - Режим доступа: для авториз. пользователей.

3. Виноградов, И. М. Основы теории чисел : учебное пособие / И. М. Виноградов. - 14-е изд., стер. - Санкт-Петербург : Лань, 2020. - 176 с. - ISBN 978-5-8114-5329-0. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/139285 (дата обращения: 10.03.2020). - Режим доступа: для авториз. пользователей.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.05 Общая алгебра и теория чисел

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

Направление подготовки: 01.04.04 - Прикладная математика
Профиль подготовки: Классические и квантовые методы обработки информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2020

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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.