МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт математики и механики им. Н.И. Лобачевского

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
проф. Таюрский Д.А.
"___"_____20___ г.

Программа дисциплины

Дополнительные главы прикладной алгебры Б1.В.ДВ.05.01

Направление подготовки: 01.04.01 - Математика
Профиль подготовки: Алгебра
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2019
Автор(ы): Насрутдинов М.Ф. , Тронин С.Н.
Рецензент(ы): Ильин С.Н.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Тронин С. Н.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Института математики и механики им. Н.И. Лобачевского :
Протокол заседания УМК No ____ от "____" _____ 20__г.

Содержание

Программу дисциплины разработал(а)(и) заместитель директора по образовательной деятельности Насрутдинов М.Ф. (Высшая школа информационных технологий и интеллектуальных систем, КФУ), Marat.Nasrutdinov@kpfu.ru ; профессор, д.н. (доцент) Тронин С.Н. (кафедра компьютерной математики и информатики, отделение педагогического образования), Serge.Tronin@kpfu.ru

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

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики
ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах
ПК-5	Способен находить и извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов и т.п.
ПК-6	Способен составлять научные обзоры, рефераты и отчеты по тематике проводимых исследований, а также подготовить научную публикацию
ПК-7	Обладать навыками преподавания математики и информатики в средней школе, специальных учебных заведениях, высших учебных заведениях на основе полученного фундаментального образования

Выпускник, освоивший дисциплину:

Должен знать:

Основы алгебраической техники, используемой в алгебраической криптографии как разделе прикладной алгебры.

Должен уметь:

Конструировать новые криптографические протоколы на алгебраических платформах, и анализировать уже известные.

Должен владеть:

Основами алгебры, применяемой в криптографии, и основами криптографии с открытым ключом.

Должен демонстрировать способность и готовность:

-применять методы абстрактной алгебры в приложениях (теории кодирования и криптографии).

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.05.01 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.01 "Математика (Алгебра)" и относится к дисциплинам по выбору.
Осваивается на 1 курсе в 2 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 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 42 часа(ов), в том числе лекции - 14 часа(ов), практические занятия - 28 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 66 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен во 2 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. Основные принципы криптографии с открытым ключом	2	3	3	0	12
2.	Тема 2. Криптография с открытым ключом на платформах коммутативных групп	2	4	10	0	12
3.	Тема 3. Криптография с открытым ключом на платформах некоммутативных групп	2	4	8	0	24
4.	Тема 4. Криптография на кольцевых платформах. Криптосистема NTRU и постквантовая криптография.	2	3	7	0	18
	Итого		14	28	0	66

4.2 Содержание дисциплины

Тема 1. Основные принципы криптографии с открытым ключом

Симметричное и асимметричное шифрование. Проблема распределения ключей, цифровая подпись, аутентификация. Основные принципы криптографии с открытым ключом. Шифры, подписи, протоколы формирования общего секретного ключа. Описание алгоритма RSA: алгоритм создания открытого и секретного ключей, шифрование и расшифрование, корректность схемы, пример, криптоанализ RSA.

Тема 2. Криптография с открытым ключом на платформах коммутативных групп

Алгоритм Диффи - Хеллмана. Задача Диффи - Хеллмана и задача дискретного логарифмирования. Вычислительная задача Диффи - Хеллмана и задача дискретного логарифмирования в конечном поле. Алгоритм Диффи - Хеллмана с тремя и более участниками. Криптографическая стойкость. Криптография с открытым ключом на платформах коммутативных групп. Эллиптическая криптография.

Тема 3. Криптография с открытым ключом на платформах некоммутативных групп

Криптография с открытым ключом на платформах некоммутативных групп. Группы кос как подходящая алгебраическая платформа. Группа кос и ее свойства. Протоколы для обмена ключами: протокол Аншель-Аншеля-Гольдфельда, протокол обмена ключами Стикеля. Протоколы шифрования и дешифрования. Протоколы аутентификации. Основы безопасности протоколов.

Другие примеры базовых групп: группа Томпсона, группа Григорчука, матричные группы.

Тема 4. Криптография на кольцевых платформах. Криптосистема NTRU и постквантовая криптография.

Проблемы криптостойкости и квантовые компьютеры. Криптографическая система с открытым ключом NTRU. Кольца усечённых многочленов. Генерация открытого ключа. Шифрование и расшифрование. Стойкость к атакам: полный перебор, встреча посередине, атака на основе множественной передачи сообщения, атака на основе решётки, атака на основе подобранного шифротекста.

Криптография на кольцевых платформах.

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".

Положение от 29 декабря 2018 г. № 0.1.1.67-08/328 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет".

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"".

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет"".

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 2			
	Текущий контроль		
1	Письменное домашнее задание	ПК-4 , ПК-1	1. Основные принципы криптографии с открытым ключом 2. Криптография с открытым ключом на платформах коммутативных групп
2	Презентация	ПК-6 , ПК-5	3. Криптография с открытым ключом на платформах некоммутативных групп
3	Письменное домашнее задание	ПК-7	4. Криптография на кольцевых платформах. Криптосистема NTRU и постквантовая криптография.
	Экзамен	ПК-1, ПК-4, ПК-5, ПК-6, ПК-7	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Семестр 2					
Текущий контроль					

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Письменное домашнее задание	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	1 3
Презентация	Превосходный уровень владения материалом. Высокий уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения полностью соответствуют задачам презентации. Использованы надлежащие источники и методы.	Хороший уровень владения материалом. Средний уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения в основном соответствуют задачам презентации. Использованные источники и методы в основном соответствуют поставленным задачам.	Удовлетворительный уровень владения материалом. Низкий уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения слабо соответствуют задачам презентации. Использованные источники и методы частично соответствуют поставленным задачам.	Неудовлетворительный уровень владения материалом. Неудовлетворительный уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения не соответствуют задачам презентации. Использованные источники и методы не соответствуют поставленным задачам.	2
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.	

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Семестр 2

Текущий контроль

1. Письменное домашнее задание

Темы 1, 2

1. Вычислите значение функции Эйлера \varphi(2018).
2. Вычислить с проверкой a в степени n по модулю p.
3. Вычислить с проверкой обратное к элементу a по модулю p.
4. По заданным простым числам реализовать шифрование по схеме RSA
5. В системе RSA с открытым ключем (187, 7) зашифровать сообщение 34.
6. В системе RSA с открытым ключем (187, 7) расшифруйте сообщение 111.
7. Сообщение, состоящее из 5 букв русского алфавита, зашифровано следующим образом: буквы закодированы числами от 1 до 32 (по порядку в алфавите без Ё) и зашифрованы с помощью RSA. Известен один из параметров открытого ключа: e=3. Найдите недостающий параметр и расшифруйте сообщение: 121-1-376-247-125 (необходимо использование компьютера)
8. Реализовать процедуру распределения ключей по протоколу Диффи-Хеллмана (необходимо использование компьютера, представить отчет о выполнении).
9. Реализовать алгоритм шифрования методом Эль Гамаля.
10. Реализовать алгоритм шифрования методом RSA.

2. Презентация

Тема 3

Возможные темы докладов

1. Слепая подпись Чаума
2. Слепая подпись на основе ЭЦП Шнорра
3. Применение затемненных (слепых) подписей. Платежные системы .
4. Протокол Anshel-Anshel-Goldfeld
5. Цифровая подпись Kahrobaei and Kouparis
6. Протокол Стикельса
7. Цифровая подпись Кахробая-Росенберга-Хабиб
8. Протокол Anshel-Anshel-Goldfeld для группоидов
9. Исправленная цифровая подпись Kahrobaei and Kouparis для группоидов
10. Протокол Стикельса для группоидов
11. Примеры базовых групп: группа Томпсона. Свойства, реализация протокола на группе.
12. Примеры базовых групп: группа Григорчука. Свойства, реализация протокола на группе.
13. Примеры базовых групп: матричные группы. Свойства, реализация протокола на группе.

3. Письменное домашнее задание

Тема 4

Пример задания (вычисление групп точек эллиптических кривых).

Задания выполняются в паре. По точкам эллиптической кривой y^2=x^3+ax+b \mod p, где a и b - день и месяц рождения студента, p - одно из простых значений 43, 47, 53, выполнить следующее:

1. Получить множество конечных точек эллиптической кривой;
2. Выбрать генерирующую точку G=(x,y)
3. Выбрать случайное целое s- свою собственную секретную часть ключа;
4. Найти свой открытый ключ P=sG
5. Из оставшихся конечных точек построить собственный алфавит, необходимый для дальнейшего шифрования(для возможности декодирования шифротекста использовать все точки);
6. Указать количество N точек на этой кривой с учетом точки в бесконечности;
7. Проверить значение N по теореме Хассе.
8. Передать преподавателю и своему напарнику a)построенныйалфавит, b)выбранную генерирующую точку G, c)свой открытый ключ P,d)значение N.
9. Используя открытый ключ своего напарника Q и свое секретное значение s сгенерировать независимо от действий напарника общий секретный ключ K по формуле K=sQ.
10. Используя собственный алфавит и общий секретный ключ K провести шифрование по системе Диффи-Хеллмана некоторого предложения и передать полученный шифротекст (по возможности, в буквенном виде) своему напарнику.
11. Получить от напарника его шифротекст, который расшифровать по алфавиту напарника, также используя общий секретный ключ K.

Экзамен

Вопросы к экзамену:

1. Протоколы формирования общего секретного ключа. Примеры.
2. Протоколы шифрования с открытым ключом. Примеры.
3. Протоколы цифровой подписи. Примеры.
4. Протоколы аутентификации. Примеры.
5. Эллиптические кривые над конечными полями.
6. Криптографические протоколы на платформе группы точек эллиптической кривой.
7. Некоторые протоколы на платформах других коммутативных групп.
8. Группы кос и их алгебраические и алгоритмические свойства.
9. Основные протоколы обмена ключами на групповых платформах.
10. Протокол Anshel-Anshel-Goldfeld.
11. Некоторые протоколы на кольцевых платформах.
12. Постквантовая криптография. Криптосистема NTRU

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 2			
Текущий контроль			
Письменное домашнее задание	Обучающиеся получают задание по освещению определённых теоретических вопросов или решению задач. Работа выполняется письменно дома и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1 3	15 15
Презентация	Обучающиеся выполняют презентацию с применением необходимых программных средств, решая в презентации поставленные преподавателем задачи. Обучающийся выступает с презентацией на занятии или сдаёт её в электронном виде преподавателю. Оцениваются владение материалом по теме презентации, логичность, информативность, способы представления информации, решение поставленных задач.	2	20
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

1. Чикрин Д.Е. Теория информации и кодирования: курс лекций / Д.Е. Чикрин. Казань: Казанский университет, 2013. 116 с.- Режим доступа: http://dspace.kpfu.ru/xmlui/bitstream/handle/net/21172/50_000337.pdf

2. Баранова Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб.пособие / Е. К. Баранова. - М.: РИОР: ИНФРА-М, 2013. - 183 с. - Режим доступа:

http://znanium.com/bookread.php?book=415501

3. 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/bookread.php?book=441493

4. Аверченков В.И. Криптографические методы защиты информации [Электронный ресурс] / Аверченков В.И. - М. : ФЛИНТА, 2017. - 215 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976529472.html

7.2. Дополнительная литература:

1. Аграновский А.В. Практическая криптография: алгоритмы и их программирование [Электронный ресурс] / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - 256 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN5980030026.html

2. Сидельников В.М. Теория кодирования. [Электронный ресурс] / Сидельников В.М. - М. : ФИЗМАТЛИТ, 2008. - 324 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785922109437.html

3. Штарьков Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] / Штарьков Ю.М. - М. : ФИЗМАТЛИТ, 2013. - 288 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785922115179.html

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

Заметки по теории кодирования - www.mccme.ru/~anromash/courses/coding-theory-05-2016.pdf

Курс лекций по дискретному анализу - http://vyalyy.narod.ru/da2-090419.pdf

Курс лекций по прикладной алгебре - http://www.machinelearning.ru/wiki/index.php?title=%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%B

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

Вид работ	Методические рекомендации
лекции	Студентам необходимо посещать лекции и вести конспект лекций вслед за изложением материала преподавателем. Рекомендуется прорабатывать конспект в течение дня после лекции и просматривать его вновь накануне следующей лекции. В случае обнаружения ошибок или возникновения вопросов по предыдущему материалу необходимо обратиться к преподавателю.
практические занятия	Для подготовки к практическим занятиям студенту рекомендуется предварительно прорабатывать как лекционный материал, так и материал предыдущих практических занятий. Основой для подготовки служит добросовестное выполнение домашнего задания. Для успешного решения задач первой части курса студентам рекомендуется вспомнить материал, освоенный в предыдущих семестрах в рамках базовых математических дисциплин. Подготовку к семинарам (практическим занятиям, лабораторным занятиям) следует начинать с изучения теоретической части (лекционного материала) с определениями основных понятий, выводом формул и доказательством теорем. Особое внимание следует обращать на определения основных понятий и формулировки основных теорем. Необходимо подробно разбирать примеры, которые поясняют определения и теоремы. При разборе теорем необходимо учитывать, что все предположения теоремы должны использоваться в доказательстве ее утверждения, при этом необходимо понимать, в каком месте доказательства используется то или иное предположение теоремы. После изучения теоретического материала следует приступить к решениям задач по данной теме. Для многих задач курса существуют алгоритмы для их решения.
самостоя-тельная работа	Самостоятельная работа студентов состоит из двух основных частей - проработка лекционного материала и выполнения домашних заданий. Для освоения теоретического и практического материала, в случае, когда конспектов оказывается недостаточным, или для более детальной проработки отдельных тем рекомендуется использовать литературу, указанную в соответствующем разделе. Все возникающие вопросы рекомендуется заранее четко сформулировать и впоследствии обсудить с преподавателем.
письменное домашнее задание	Письменные домашние задания предназначены для самостоятельной проработки лекционного материала и овладения практическими навыками его применения для решения задач. Для освоения теоретического и практического материала, в случае, когда конспектов оказывается недостаточным, или для более детальной проработки отдельных тем рекомендуется использовать литературу, указанную в соответствующем разделе. Все возникающие вопросы рекомендуется заранее четко сформулировать и впоследствии обсудить с преподавателем/

Вид работ	Методические рекомендации
презентация	Доклад (презентация) - это сообщение по заданной теме, с целью внести знания из дополнительной литературы, систематизировать материал, проиллюстрировать примерами, развивать навыки самостоятельной работы с научной литературой. Тема доклада должна быть согласована с преподавателем и соответствовать теме занятия. Студент в ходе работы над докладом отрабатывает умение ориентироваться в материале и отвечать на дополнительные вопросы слушателей, самостоятельно обобщить материал и сделать выводы в заключении. Докладом также может стать презентация реферата студента, соответствующая теме занятия. Студент обязан подготовить и выступить с докладом в строго отведенное время преподавателем, и в срок. Обычно выступление состоит из трех частей: вступление, основная часть и заключение. Вступление должно содержать: название доклада, сообщение основной идеи, краткое перечисление рассматриваемых вопросов. Основная часть, в которой выступающий должен глубоко раскрыть суть затронутой темы, обычно строится по принципу отчета. Задача основной части - представить достаточно данных для того, чтобы слушатели и заинтересовались темой и захотели ознакомиться с материалами. Заключение - это ясное четкое обобщение и краткие выводы.
экзамен	Залогом успешной сдачи экзамена является работа в течение всего семестра. Непосредственную подготовку к экзамену рекомендуется разделить на два этапа. На первом этапе прорабатываются все экзаменационные вопросы и формулируются вопросы к преподавателю в рамках консультации по разделам, недостаточно подробно описанным в рамках лекционного курса или более трудным в освоении материала. После консультации происходит окончательная проработка и закрепление материала по всем экзаменационным вопросам.

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

Освоение дисциплины "Дополнительные главы прикладной алгебры" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Пакет офисного программного обеспечения Microsoft Office 2010 Professional Plus Russian

Браузер Mozilla Firefox

Adobe Reader XI

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе " БиблиоРоссика", доступ к которой предоставлен обучающимся. В ЭБС " БиблиоРоссика " представлены коллекции актуальной научной и учебной литературы по гуманитарным наукам, включающие в себя публикации ведущих российских издательств гуманитарной литературы, издания на английском языке ведущих американских и европейских издательств, а также редкие и малотиражные издания российских региональных вузов. ЭБС "БиблиоРоссика" обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и 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 "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.

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

Освоение дисциплины "Дополнительные главы прикладной алгебры" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

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 01.04.01 "Математика" и магистерской программе Алгебра .