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. Д.А. Таюрский
_____ « 01 » июня 2021 г.

подписано электронно-цифровой подписью

Программа дисциплины

Дополнительные главы прикладной алгебры

Направление подготовки: 01.04.01 - Математика
Профиль подготовки: Анализ на многообразиях
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2021

Содержание

Программу дисциплины разработал(а)(и): доцент, к.н. Корнеева Н.Н. (Кафедра алгебры и математической логики, отделение математики), Natalia.Korneeva@kpfu.ru ; доцент, к.н. Насрутдинов М.Ф. (кафедра компьютерной математики и информатики, отделение педагогического образования), Marat.Nasrutdinov@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-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики
ПК-5	Способен преподавать математику и информатику в средней школе, специальных учебных заведениях, высших учебных заведениях на основе полученного фундаментального образования

Обучающийся, освоивший дисциплину (модуль):

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 (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.05.03 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.01 "Математика (Анализ на многообразиях)" и относится к дисциплинам по выбору части ОПОП ВО, формируемой участниками образовательных отношений.

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 - 43 часа(ов), в том числе лекции - 14 часа(ов), практические занятия - 28 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 1 часа(ов).

Самостоятельная работа - 65 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, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)						Самостоятельная работа
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
1.	Тема 1. Основные принципы криптографии с открытым ключом	2	3	0	3	0	0	0	12
2.	Тема 2. Криптография с открытым ключом на платформах коммутативных групп	2	4	0	10	0	0	0	12
3.	Тема 3. Криптография с открытым ключом на платформах некоммутативных групп	2	4	0	8	0	0	0	24
4.	Тема 4. Криптография на кольцевых платформах. Криптосистема NTRU и постквантовая криптография.	2	3	0	7	0	0	0	17
Итого			14	0	28	0	0	0	65

4.2 Содержание дисциплины (модуля)

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 науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

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)

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%BD%D

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.

Вид работ	Методические рекомендации
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.
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)

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.

Мультимедийная аудитория.

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 01.04.01 "Математика" и магистерской программе "Анализ на многообразиях".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.05.03 Дополнительные главы прикладной алгебры

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.04.01 - Математика

Профиль подготовки: Анализ на многообразиях

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2021

Основная литература:

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие для вузов / Л. М. Мартынов. - 2-е изд., стер. - Санкт-Петербург : Лань, 2022. - 456 с. - ISBN 978-5-8114-9346-3. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/189446 (дата обращения: 03.03.2021). - Режим доступа: для авториз. пользователей.

2. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. - Москва : ФОРУМ : ИНФРА-М, 2022. - 240 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1875764 (дата обращения: 03.03.2021). - Режим доступа: по подписке.

3. Аверченков, В. И. Криптографические методы защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, С. А. Шпичак. - 2-е изд., стер. - Москва : ФЛИНТА, 2017. - 215 с. - ISBN 978-5-9765-2947-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1090754 (дата обращения: 03.03.2021). - Режим доступа : по подписке.

Дополнительная литература:

1. Аграновский А.В., Практическая криптография: алгоритмы и их программирование: учебное пособие / Аграновский А.В., Хади Р.А. - Москва : СОЛОН-ПРЕСС, 2009. - 256 с. - ISBN 5-98003-002-6 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN5980030026.html (дата обращения: 03.03.2021). - Режим доступа : по подписке.

2. Сидельников, В. М. Теория кодирования: учебное пособие / В. М. Сидельников. - Москва: ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/544713 (дата обращения: 03.03.2021). - Режим доступа : по подписке.

3. Штарьков, Ю. М. Универсальное кодирование. Теория и алгоритмы : учебное пособие / Ю. М. Штарьков. - Москва : ФИЗМАТЛИТ, 2013. - 288 с. - ISBN 978-5-9221-1517-9. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/59667 (дата обращения: 03.03.2021). - Режим доступа: для авториз. пользователей.

4. Чикрин Д.Е. Теория информации и кодирования: курс лекций / Д.Е. Чикрин. Казань: Казанский университет, 2013. - 116 с. - Текст : электронный. - URL: http://dspace.kpfu.ru/xmlui/bitstream/handle/net/21172/50_000337.pdf (дата обращения: 03.03.2021). - Режим доступа: открытый.

5. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие / Баранова Е.К. - Москва:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 183 с. (Высшее образование: Бакалавриат) ISBN 978-5-369-01169-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/959916

(дата обращения: 03.03.2021). - Режим доступа: по подписке.

6. Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/441493 (дата обращения: 03.03.2021). - Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.05.03 Дополнительные главы прикладной алгебры

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

Направление подготовки: 01.04.01 - Математика

Профиль подготовки: Анализ на многообразиях

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2021

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.