

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



» 20 г.

подписано электронно-цифровой подписью

Программа дисциплины

Математические основы информационной безопасности Б1.О.04

Направление подготовки: 02.04.02 - Фундаментальная информатика и информационные технологии

Профиль подготовки: Наука о Данных

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2019

Автор(ы): Ишмухаметов Ш.Т.

Рецензент(ы): Латыпов Р.Х.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.

Протокол заседания кафедры № ____ от "____" 20__ г.

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК № ____ от "____" 20__ г.

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы
2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования
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
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
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
 - 6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания
 - 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
 - 6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)
 - 7.1. Основная литература
 - 7.2. Дополнительная литература
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 к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), Shamil.Ishmukhametov@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
ОПК-3	Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования
ОПК-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности

Выпускник, освоивший дисциплину:

Должен знать:

основные концепции информационной безопасности;

Должен уметь:

ориентироваться в вопросах разработки надежных систем защиты и видах угроз информационной безопасности.

Должен владеть:

теоретическими знаниями о математических основах построения криптографических алгоритмов;

Должен демонстрировать способность и готовность:

навыков оценки безопасности информационных систем.

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

Данная учебная дисциплина включена в раздел "Б1.О.04 Дисциплины (модули)" основной профессиональной образовательной программы 02.04.02 "Фундаментальная информатика и информационные технологии (Наука о Данных)" и относится к обязательным дисциплинам.

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 6 зачетных(ые) единиц(ы) на 216 часа(ов).

Контактная работа - 36 часа(ов), в том числе лекции - 18 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 18 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 162 часа(ов).

Контроль (зачёт / экзамен) - 18 часа(ов).

Форма промежуточного контроля дисциплины: экзамен 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	
N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Алгебраические структуры: группы, кольца, поля.	3	2	0	2	27
2.	Тема 2. Расширения конечных полей.	3	2	0	2	27
3.	Тема 3. Производящие функции.	3	3	0	3	27
4.	Тема 4. Рекуррентные уравнения.	3	3	0	3	27
5.	Тема 5. Мультипликативные функции. Дзета функция Римана.	3	4	0	4	27
4.2 Содержание дисциплины						
Тема 1. Алгебраические структуры: группы, кольца, поля.						
6. методы факторизации натуральных чисел.		3	4	0	4	27
Введение в алгебраические структуры. Определение, свойства, применение алгебраических структур. Группы. Теорема Лагранжа. Конечные поля. Неприводимые многочлены в конечных полях. Критерий неприводимости многочленов в конечных полях. Операции с многочленами. Вычисление обратного многочлена по модулю неприводимого многочлена.						

Тема 2. Расширения конечных полей.

Решение уравнений первого и второго порядка в конечных полях. Построение неприводимых многочленов. Нахождение обратных элементов и вычисление частных. Расширенный алгоритм Евклида для многочленов. Примитивные многочлены. Алгоритм нахождения неприводимых многочленов. Сепарабельные расширения полей.

Тема 3. Производящие функции.

Примеры, приводящие к производящим функциям. Рекуррентные уравнения. Построение таблицы приводящих функций. Производящая функция ряда частичных сумм. Дифференцирование и интегрирование производящих функций. Решение рекуррентных уравнения 2-ого порядка. Формула включений и исключений. Решение задач на формулу включений и исключений.

Тема 4. Рекуррентные уравнения.

Использование производящих функций для решения рекуррентных уравнений. Построение рекуррентного уравнения для рядов Фибоначчи. Оценка метода сортировки вставкой. Контрольная работа по теме:

- Найти производящую функцию последовательности $\{n^2+2n\}$
- Вычислить ряд частичных сумм для ряда $\{3^n+2, n=0,1,2,\dots\}$.
- Решить рекуррентное уравнение $a_{(n+2)}=-3_{(n+1)}-2a_n, a_0=-2, a_1=-6$
- Сколько существует натуральных чисел, не превосходящих 1000, которые делятся на 5, но не делятся на 2 и 3?

Тема 5. Мультипликативные функции. Дзета функция Римана.

Модулярная арифметика. Решение сравнений 1 и второго порядка. Формула Эйлера. Функция Эйлера и формула для ее вычисления. Функция Мебиуса. Формула инверсии Мебиуса. Использование формулы для оценки функции распределения простых чисел. Проблема тысячелетия Римана. Ее связь с распределением простых чисел.

Тема 6. Субэкспоненциальные методы факторизации натуральных чисел.

Эллиптические кривые. Вычисления на эллиптических кривых. Алгоритм Шенкса вычисления кратной точки. Алгоритмы факторизации натуральных чисел. Метод Ленстры факторизации натуральных чисел. Оценка сходимости метода. Выбор параметров первой и второй стадий метода. Факторизация методом решета числового поля.

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 профессионального 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"".

Ишмухаметов Ш.Т. Математические основы защиты информации - <http://kpfu.ru/docs/F366166681/mzi.pdf>

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 3			
	Текущий контроль		
1	Контрольная работа	ОПК-1	1. Алгебраические структуры: группы, кольца, поля.
2	Контрольная работа	ОПК-3	3. Производящие функции.
3	Лабораторные работы	УК-1	6. Субэкспоненциальные методы факторизации натуральных чисел.
	Экзамен	ОПК-3, ОПК-4	

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 3						
Текущий контроль						

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Контрольная работа	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 2
Лабораторные работы	Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.	Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном соответствует её целям.	Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.	Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки и умения не освоены. Результат лабораторной работы не соответствует её целям.	3
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 3

Текущий контроль

1. Контрольная работа

Тема 1

Выполнение домашних заданий, подготовка к контрольной работе. Оценивается в баллах, добавляемых в первую половину успеваемости студентов. Пример варианта контрольной работы:

1. Дано конечное поле GF(37). Найти наименьшее значение примитивного элемента.
2. Дано конечное поле GF(p), $p=17$. Найти наименьший квадратичный невычет 'a' поля GF(p) и рассмотреть поле GF(p^2), полученное добавлением к GF(p) неприводимого многочлена x^2-a . Найти в поле GF(p^2) сумму, разность, произведение и отношение элементов по модулю x^2-a . $z_1=7+16x$ и $z_2=5+7x$.
3. Вычислить значение функции Эйлера для $n=117$.
4. Дано конечное F(p), $p=13$ и неприводимый многочлен P(x) x^3+x+1 . Найти отношение многочленов $(10x^2+9x+6)/(2x^2+4)$ по модулю P(x).

2. Контрольная работа

Тема 3

Пример варианта контрольной работы:

Найти производящую функцию последовательности $\{n^3\}$

Вычислить ряд частичных сумм для ряда $\{3n-2, n=0, 1, 2, ?\}$.

Решить рекуррентное уравнение $a_{(n+2)}=2a_{(n+1)}+3a_n$, $a_0=0, a_1=-5$

Сколько существует 4-х значных натуральных чисел, которые содержат в своем разложении хотя бы одну из цифр 3 или 5.

3. Лабораторные работы

Тема 6

Задание на лабораторную работу:

Лабораторная работа 1. Многочлены в конечном поле. Необходимо написать комплекс программ для действий с многочленами над полем GF_2={0,1}. Программа должна выполнять следующие операции с многочленами: сложение, вычитание, умножение, вычисление обратного по модулю другого многочлена, деление многочленов в модулярном кольце многочленов по модулю неприводимого многочлена.

Описание работы.

Оп. Многочленом степени n над полем GF_2={0,1} называется многочлен вида $P_n(x)=x^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$, где все коэффициенты a_i принимают значения 0 или 1.

Оп. Многочлен $P_n(x)$ называется неприводимым ([1], с.52), если его нельзя разложить в произведение двух многочленов над полем GF_2={0,1} меньших степеней.

В кольце всех многочленов над полем GF_2={0,1} возможны операции сложения, вычитания и умножения многочленов. Также возможно возведение многочлена в положительную целую степень.

В модулярном кольце GF_2(G_n), где G_n ? неприводимый многочлен степени n все результаты приводятся по модулю многочлена G_n. Элементами такого кольца являются многочлены степени $n-1$. Результат операций умножения и возведения в степень таких многочленов приводит к многочлену более высокой степени, поэтому необходимо результат умножения или возведения в степень поделить на G_n и получить остаток, который будет иметь степень, меньшую n . Можно также искать полиномы, обратные к заданному полиному, по модулю G_n.

Экзамен

Вопросы к экзамену:

Группы, кольца, определения и примеры. Кольцо вычетов Z_n. Операции в Z_n.

Конечные поля. Теорема о том, что Z_p является полем при простом модуле p.

Теорема Лагранжа о порядках элементов групп.

Полная и приведенные системы вычетов Z_n. Теоремы о полной и приведенной системе вычетов.

Функция Эйлера и ее свойства. Теорема о мультипликативности функции Эйлера. Формула для вычисления ф.Эйлера.

Теорема Эйлера $a^{(\phi(n))} \bmod n = 1$.

Теорема $\sum_{d|n} \phi(d) = n$.

Порядок элементов конечного поля. Теорема о существовании примитивного элемента в конечном поле. Число примитивных элементов в конечном поле.

Вычеты. Символ Лежандра. Критерий Эйлера (с доказательством).

Свойства символа Лежандра. Мультипликативность. Закон квадратичной взаимности Гаусса. Вычисление символа Лежандра. Пример.

Квадратичные вычеты. Теорема о существовании неприводимых многочленов 2-й и 3-й степени над полем F_p.

Расширения конечных полей с использованием неприводимых многочленов. Теорема о существовании конечных полей F_(p^2) и F_(p^3). Вычисления в полях многочленов.

Проблема вычисления дискретного логарифма в конечных полях. Алгоритм Шенкса ?giant & baby steps?.

Проблема факторизации больших чисел. Алгоритм Ферма.

Решение рекуррентных уравнений. Задача о некоммутативном размене. Вывод выражения для члена ряда Фибоначчи.

Производящие функции. Операции над числовыми рядами $\sum_{n=0}^{\infty} a_n z^n$.

Дифференцирование и интегрирование производящих функций.

Построение таблицы основных производящих функций.

Решение рекуррентных уравнений с использованием производящих функций.

Числа Каталана. Свертка Дирихле. Вывод формулы для ряда Каталана.

Формула для члена ряда частичных сумм (с выводом).

Формула включений и исключений. Пример.

Базельская проблема. Дзета-функция Римана. Вычисление Эйлером $\zeta(2)$ и $\zeta(4)$.

Классический алгоритм Евклида вычисления НОД.

Бинарный и k-арный алгоритмы вычисления НОД.

Алгоритм Лемера для ускорения алгоритма Евклида.

Дроби Фарея. Нахождение дроби Фарея для действительного $a \in (0;1)$. Оценка сложности алгоритма.

Аппроксимирующий алгоритм вычисления НОД. Пример.

Алгоритмы быстрого умножения длинных чисел. Школьное умножение столбиком и его сложность. Алгоритм Карацубы и его оценка сложности. Алгоритм быстрого преобразования Фурье. Оценка его сложности. Пример

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

В КФУ существует 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 3			
Текущий контроль			
Контрольная работа	Контрольная работа проводится в часы аудиторной работы. Обучающиеся получают задания для проверки усвоения пройденного материала. Работа выполняется в письменном виде и сдается преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1 2	15 15
Лабораторные работы	В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.	3	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:

- Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. - 416 с. - Режим доступа: <http://znanium.com/bookread2.php?book=775200>
- Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. - М.: ИНФРА-М, 2018. - Режим доступа: <http://znanium.com/bookread2.php?book=925825>
- Партика Т. Л. Информационная безопасность : учеб. пособие / Т.Л. Партика, И.И. Попов. - 5-е изд., перераб. и доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 432 с. - Режим доступа: <http://znanium.com/bookread2.php?book=915902>

4. 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. -Режим доступа: <http://znanium.com/bookread2.php?book=495249>

5. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=75515

6. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: <http://znanium.com/bookread2.php?book=405313>

7.2. Дополнительная литература:

1. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. - Режим доступа: <http://znanium.com/catalog/product/944503>

2. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - Режим доступа: <http://znanium.com/bookread.php?book=474838>

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: <http://znanium.com/bookread.php?book=503511>

4. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - Режим доступа: <http://znanium.com/bookread.php?book=491597>

5. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - Режим доступа: <http://znanium.com/bookread.php?book=169345>

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

Интернет-портал образовательных ресурсов по ИТ - <http://www.intuit.ru>

Интернет-портал ресурсов по математике - <http://www.math.ru>

Электронная библиотека ресурсов по техническим наукам - <http://techlibrary.ru>

электронное пособие - http://www.ksu.ru/f9/bin_files/metod_tzis!113.doc

электронное пособие - http://www.ksu.ru/f9/bibl/Monograph_ishm.pdf

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

Вид работ	Методические рекомендации
лекции	Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.
лабораторные работы	Лабораторные занятия призваны дать такой практический навык, а также навыки программирования криптографических алгоритмов и их внедрения в информационные системы. В ходе выполнения работ происходит отработка знаний студентов по программированию криптографических алгоритмов, изучаются специальных разделы программирования комплексных систем информационной безопасности.
самостоятельная работа	Самостоятельная работа предполагает выполнение домашних работ при подготовке к контрольной работе и выполнении компьютерной программы. Самостоятельная работа выполняется в несколько этапов. Сначала предполагается изучение теоретического материала. Также рекомендуется каждый раздел программы сопровождать практической работой, выполняя лабораторные занятия.

Вид работ	Методические рекомендации
контрольная работа	Также для выполнения контроля успеваемости студентов проводится контрольная работа, которая призвана показать основные практические навыки решения задач, связанных с математическим обеспечением задач информационной безопасности. При подготовке к контрольной работе рекомендуется обращаться внимание на основные задачи, решенные в течение семестра, периодически решать аналогичные задачи, программировать основные вычислительные алгоритмы, чтобы лучше понять их тонкости.
экзамен	При подготовке к экзамену рекомендуется разбить материал на смысловые блоки и изучать его, выписывая краткое содержание блока. По каждому блоку надо составить контрольные вопросы и самостоятельно составить краткие ответы по вопросам. Прочитав лекции, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

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

Освоение дисциплины "Математические основы информационной безопасности" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Пакет офисного программного обеспечения Microsoft Office 2010 Professional Plus Russian

Adobe Reader XI

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.

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

Освоение дисциплины "Математические основы информационной безопасности" 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 оборудование 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 02.04.02 "Фундаментальная информатика и информационные технологии" и магистерской программе "Наука о Данных".