

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 защиты информации и информационной безопасности

Направление подготовки: 09.04.03 - Прикладная информатика

Профиль подготовки: Информационная безопасность экономических систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2018

## **Содержание**

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

Программу дисциплины разработал(а)(и) 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 ОПОП ВО**

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

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-4	Способен применять на практике новые научные принципы и методы исследований
ОПК-7	Способен использовать методы научных исследований и математического моделирования в области проектирования и управления информационными системами

Обучающийся, освоивший дисциплину (модуль):

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 (модуля) в структуре ОПОП ВО**

Данная дисциплина (модуль) включена в раздел "Б1.О.03 Дисциплины (модули)" основной профессиональной образовательной программы 09.04.03 "Прикладная информатика (Информационная безопасность экономических систем)" и относится к обязательным дисциплинам.

Осваивается на 1 курсе в 1 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 - 126 часа(ов).

Контроль (зачёт / экзамен) - 54 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 1 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. Алгебраические структуры: группы, кольца, поля.		1	2	0	20

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Расширения конечных полей.	1	2	0	2	20
3.	Тема 3. Производящие функции.	1	2	0	3	20
4.	Тема 4. Рекуррентные уравнения.	1	4	0	3	20
5.	Тема 5. Мультиплективные функции. Дзета функция Римана.	1	4	0	4	22
6.	Тема 6. Субэкспоненциальные методы факторизации натуральных чисел.	1	4	0	4	24
Итого			18	0	18	126

#### 4.2 Содержание дисциплины (модуля)

##### Тема 1. Алгебраические структуры: группы, кольца, поля.

Введение в алгебраические структуры. Определение, свойства, применение алгебраических структур. Группы. Теорема Лагранжа. Конечные поля. Неприводимые многочлены в конечных полях.

##### Тема 2. Расширения конечных полей.

Решение уравнений в конечных полях. Построение неприводимых многочленов. Нахождение обратных элементов и вычисление частных.

##### Тема 3. Производящие функции.

Примеры, приводящие к производящим функциям. Рекуррентные уравнения. Построение таблицы приводящих функций. Дифференирование и интегрирование производящих функций.

##### 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.

##### Тема 5. Мультиплективные функции. Дзета функция Римана.

Молулярная арифметика. Решение сравнений 1 порядка. Эйлера. Формула для вычисления функции Эйлера. Функция Мебиуса. Формула инверсии Мебиуса. Формула включений и исключений. Решение задач. Использование формулы для оценки функции распределения простых чисел.

##### Тема 6. Субэкспоненциальные методы факторизации натуральных чисел.

Эллиптические кривые. 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 №14-55-996н/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  
Ишмухаметов Ш.Т. Математические основы защиты информации - <http://kpfu.ru/docs/F366166681/mzi.pdf>

## **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)**

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](http://www.ksu.ru/f9/bin_files/metod_tzis!113.doc)

электронное пособие - [http://www.ksu.ru/f9/bibl/Monograph\\_ishm.pdf](http://www.ksu.ru/f9/bibl/Monograph_ishm.pdf)

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

Вид работ	Методические рекомендации
лекции	Теоретический курса материала 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.

Вид работ	Методические рекомендации
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, изучение специальных разделов программирования алгоритмов сетевого взаимодействия.
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.
экзамен	Рекомендуется разбивать 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)**

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 09.04.03 "Прикладная информатика" и магистерской программе "Информационная безопасность экономических систем".

**Приложение 2**  
к рабочей программе дисциплины (модуля)  
**Б1.О.03 Математические основы защиты информации и информационной безопасности**

**Перечень литературы, необходимой для освоения дисциплины (модуля)**

Направление подготовки: 09.04.03 - Прикладная информатика

Профиль подготовки: Информационная безопасность экономических систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2018

**Основная литература:**

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. - 416 с URL: <http://znanium.com/bookread2.php?book=775200>
2. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. ? М. : ИНФРА-М, 2018. URL: <http://znanium.com/bookread2.php?book=945331>
3. 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. URL: <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. URL:<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](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. URL: <http://znanium.com/bookread2.php?book=405313>

**Дополнительная литература:**

1. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. ISBN 978-5-9775-1884-0  
<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. - ЭБС 'Знаниум': <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. - ЭБС 'Знаниум': <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. - ЭБС 'Знаниум': <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. - ЭБС 'Знаниум': <http://znanium.com/bookread.php?book=169345>

**Приложение 3**  
к рабочей программе дисциплины (модуля)  
Б1.О.03 Математические основы защиты информации и  
информационной безопасности

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

Направление подготовки: 09.04.03 - Прикладная информатика

Профиль подготовки: Информационная безопасность экономических систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2018

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.