

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



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.



\_\_\_\_\_ 20\_\_ г.

подписано электронно-цифровой подписью

### Программа дисциплины

Математические основы защиты информации и информационной безопасности Б1.Б.3

Направление подготовки: 02.04.02 - Фундаментальная информатика и информационные технологии

Профиль подготовки: Математические основы и программное обеспечение информационной безопасности и защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

**Автор(ы):**

Ишмухаметов Ш.Т.

**Рецензент(ы):**

Латыпов Р.Х.

### **СОГЛАСОВАНО:**

Заведующий(ая) кафедрой: Латыпов Р. Х.

Протокол заседания кафедры No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_ г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_ г

Регистрационный No 974015

Казань  
2015

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

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. Цели освоения дисциплины

Данный курс входит в систему специализации по направлению информационной безопасности и является продолжением курсов "Основы информационной безопасности" и "Информационная безопасность в сетях". В ходе этого курса студенты должны получить основные знания о математических основах построения криптографических алгоритмов, понятия о вычислительной сложности односторонних функций, используемых в криптографии, методах построения надежных систем защиты и о возможных атаках.

### 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел "Б1.Б.3 Дисциплины (модули)" основной образовательной программы 02.04.02 Фундаментальная информатика и информационные технологии и относится к базовой (общепрофессиональной) части. Осваивается на 1 курсе, 1 семестр.

"Математические основы защиты информации и информационной безопасности" входит в состав общенаучных дисциплин. Читается на 1 курсе, в 1 семестре.

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способностью к абстрактному мышлению, анализу, синтезу
ОК-2 (общекультурные компетенции)	готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения
ОПК-3 (профессиональные компетенции)	способностью использовать и применять углубленные теоретические и практические знания в области фундаментальной информатики и информационных технологий
ОПК-4 (профессиональные компетенции)	способностью самостоятельно приобретать и использовать в практической деятельности новые знания и умения, в том числе, в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять своё научное мировоззрение
ОПК-5 (профессиональные компетенции)	способностью использовать углублённые знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов
ПК-1 (профессиональные компетенции)	способностью проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива
ПК-13 (профессиональные компетенции)	способностью разрабатывать аналитические обзоры состояния области прикладной математики и информационных технологий

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-14 (профессиональные компетенции)	способностью выполнять работу экспертов в ведомственных, отраслевых или государственных экспертных группах по экспертизе проектов, тематика которых соответствует направленности (профилю) программы магистратуры
ПК-16 (профессиональные компетенции)	способностью участвовать в деятельности профессиональных сетевых сообществ по конкретным направлениям
ПК-2 (профессиональные компетенции)	способностью использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий
ПК-3 (профессиональные компетенции)	способностью разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач проектной и производственно-технологической деятельности

В результате освоения дисциплины студент:

1. должен знать:

основные концепции информационной безопасности;

2. должен уметь:

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

3. должен владеть:

теоретическими знаниями о математических основах построения криптографических алгоритмов;

4. должен демонстрировать способность и готовность:

навыков оценки безопасности информационных систем.

#### 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 1 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

#### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

##### Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Алгебраические структуры: группы, кольца, поля.	1		4	0	0	домашнее задание
2.	Тема 2. Расширения конечных полей.	1		4	0	0	домашнее задание
3.	Тема 3. Производящие функции.	1		6	0	0	домашнее задание
4.	Тема 4. Реккурентные уравнения.	1		6	0	0	контрольная работа домашнее задание
5.	Тема 5. Мультипликативные функции. Дзета функция Римана.	1		4	0	0	домашнее задание
6.	Тема 6. Субэкспоненциальные методы факторизации натуральных чисел.	1		4	0	0	
	Тема . Итоговая форма контроля	1		0	0	0	экзамен
	Итого			28	0	0	

## 4.2 Содержание дисциплины

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

#### лекционное занятие (4 часа(ов)):

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

### Тема 2. Расширения конечных полей.

#### лекционное занятие (4 часа(ов)):

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

### Тема 3. Производящие функции.

#### лекционное занятие (6 часа(ов)):

Примеры, приводящие к производящим функциям. Реккурентные уравнения. Построение таблицы приводящих функций. Дифференцирование и интегрирование производящих функций.

### Тема 4. Реккурентные уравнения.

#### лекционное занятие (6 часа(ов)):

Использование производящих функций для решения реккурентных уравнений. Построение реккурентного уравнеия для рядов Фибоначчи. Оценка метода сортировки вставкой. Контрольная работа по теме.

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

### лекционное занятие (4 часа(ов)):

Молярная 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.

### лекционное занятие (4 часа(ов)):

Эллиптические кривые. Метод Ленстры факторизации натуральных чисел. Оценка сходимости метода. Выбор параметров первой и второй стадий метода. Факторизация методом решета числового поля.

## 4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Алгебраические структуры: группы, кольца, поля.	1		подготовка домашнего задания	8	домашнее задание
2.	Тема 2. Расширения конечных полей.	1		подготовка домашнего задания	8	домашнее задание
3.	Тема 3. Производящие функции.	1		подготовка домашнего задания	8	домашнее задание
4.	Тема 4. Рекуррентные уравнения.	1		подготовка домашнего задания	4	домашнее задание
				подготовка к контрольной работе	4	контрольная работа
5.	Тема 5. Мультипликативные функции. Дзета функция Римана.	1		подготовка домашнего задания	6	домашнее задание
6.	Тема 6. Субэкспоненциальные методы факторизации натуральных чисел.	1		подготовка домашнего задания	6	домашнее задание
	Итого				44	

## 5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

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.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения. Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы. Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

## **6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов**

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

### **Тема 3. Производящие функции.**

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

### **Тема 4. Рекуррентные уравнения.**

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

контрольная работа , примерные вопросы:

1. Найти производящую функцию последовательности  $\{(n+1)(2^n - n)\}$  2. Вычислить сумму ряда  $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots$  ? 3. Решить рекуррентное уравнение  $a_{n+2} = a_{n+1} + 2a_n$ ,  $a_0 = 3, a_1 = -1$

### **Тема 5. Мультипликативные функции. Дзета функция Римана.**

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме. Обсуждение. Решение типовых задач.

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы по изучаемой теме.

### **Тема . Итоговая форма контроля**

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные вопросы для экзамена - Приложение 1.

1. Алгебраические структуры: группы, кольца, поля. Теорема Лагранжа о порядке элемента группы.
2. Конечные поля. Расширения конечных полей. Вычисление обратных элементов в поле.
3. Модулярная арифметика. Решение сравнений 1 порядка.
4. Символ Лежандра. Его свойства и вычисление.
5. Производящие функции числовых последовательностей. Определение и основные свойства. Примеры.

6. Дифференцирование и интегрирование производящих функций.
7. Таблица производящих функций.
8. Вычисление производящей функции ряда Фибоначчи.
9. Полные и приведенные системы вычетов в кольце  $\mathbb{Z}_n$ .
10. Мультипликативные функции. Функция Эйлера. Формула для вычисления функции Эйлера. Теорема Эйлера о порядке элемента в  $\mathbb{Z}_n$ .
11. Функция Мебиуса. Теорема о сумме значений функции Мебиуса по всем делителям натурального числа  $n$ .
12. Формула инверсии Мебиуса. Формула включений/исключений. Ее использование для вычисления функции простых чисел  $\pi(x)$ .
13. Функция Мангольда и ее свойства. Функция деления.
14. Произведение (конволюция) Дирихле. Мультипликативность конволюции мультипликативных функций.
15. Инверсия Дирихле. Теорема об инверсии Дирихле мультипликативной функции.
16. Ряды Дирихле. Дзета-функция Римана. Произведение рядов Дирихле.
17. Теорема Эйлера о сумме ряда обратных квадратов
18. Свойства дзета-функции Римана. Формула произведения Эйлера
19. Формула суммирования Эйлера-Маклорена (без доказательства).
20. Нахождение асимптотической формулы для частичной суммы гармонического ряда и ряда обратных квадратов.
21. Формулы Стирлинга и ее вывод с помощью формулы суммирования Эйлера-Маклорена.
22. Гладкие и гладкостепенные числа. Формула Бухштаба вычисления числа  $u$ -гладких чисел.
23. Факторизация натуральных чисел. Метод Ленстры факторизации на эллиптических кривых.
24. Анализ сходимости метода факторизации Ленстры с помощью изучения распределения гладко-степенных чисел.
25. Метод квадратичного решета факторизации натуральных чисел. Основные параметры метода и их выбор.

### 7.1. Основная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - . - Режим доступа: <http://kpfu.ru/docs/F366166681/mzi.pdf>
2. Столов Е.Л. Генераторы случайных чисел в системах компьютерной безопасности [Электронный ресурс]. - Казань, 2014. - Режим доступа: <http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf>.
3. Информационная безопасность [Электронный ресурс]: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. . - Режим доступа: <http://www.znaniyum.com/bookread.php?book=420047>
4. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. . - Режим доступа: <http://www.znaniyum.com/bookread.php?book=405000>

### 7.2. Дополнительная литература:

1. Маскаева А. М. Основы теории информации: Учебное пособие / А.М. Маскаева. - М.: Форум: НИЦ ИНФРА-М, 2014. - 96 с. - ЭБС "Знаниум": <http://znaniyum.com/bookread.php?book=429571>
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://znaniyum.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>

### **7.3. Интернет-ресурсы:**

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)

## **8. Материально-техническое обеспечение дисциплины(модуля)**

Освоение дисциплины "Математические основы защиты информации и 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. 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, УМК, 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 профессионального образования (ФГОС ВПО) нового поколения.

лекции и лабораторные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером)

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 02.04.02 "Фундаментальная информатика и информационные технологии" и магистерской программе Математические основы и программное обеспечение информационной безопасности и защиты информации .

Автор(ы):

Ишмухаметов Ш.Т. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Латыпов Р.Х. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.