

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



подписано электронно-цифровой подписью

**Программа дисциплины**  
Основы криптографии БЗ.ДВ.2

Направление подготовки: 010400.62 - Прикладная математика и информатика  
Профиль подготовки: Системное программирование, математическое моделирование  
Квалификация выпускника: бакалавр  
Форма обучения: очно-заочное  
Язык обучения: русский

**Автор(ы):**

Латыпов Р.Х.

**Рецензент(ы):**

Пшеничный П.В.

**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 9153914

Казань  
2014

## 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) директор института вычислительной математики Латыпов Р.Х. Директорат Института ВМ и ИТ Институт вычислительной математики и информационных технологий, Roustam.Latypov@kpfu.ru

### 1. Цели освоения дисциплины

1. Ввести слушателей читателя в те области арифметики, как классические, так и самые современные, которые находятся в центре внимания приложений теории чисел, особенно криптографии. Предполагается, что знание высшей алгебры и теории чисел ограничено самым скромным знакомством с их основами; по этой причине излагаются также необходимые сведения из этих областей математики. Авторами избран алгоритмический подход, причем особое внимание уделяется оценкам эффективности методов, предлагаемых теорией.
2. Ознакомить студентов с основными достижениями теории помехоустойчивого кодирования: существующие ограничения и основные линейные коды: Хэмминга, БЧХ, Рида-Маллера, Рида-Соломона.
3. Значительное внимание уделяется изучению широко используемых криптографических алгоритмов симметричного и асимметричного шифрования, а также криптографических хэш-функций.

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

Данная учебная дисциплина включена в раздел "Б3.ДВ.2 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 3, 4 курсах, 6, 7 семестры.

"Основы криптографии" входит в состав профессиональных дисциплин. Читается на 4 курсе в 7 семестре.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-6 (профессиональные компетенции)	способность осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в сети Интернет и из других источников
ПК-8 (профессиональные компетенции)	способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций

В результате освоения дисциплины студент:

1. должен знать:

методы научной криптографии

2. должен уметь:

формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций

3. должен владеть:

приемами целенаправленного поиска информации о новейших научных и технологических достижениях в сети Интернет

4. должен демонстрировать способность и готовность:

основные результаты теории чисел и алгебры, понимать проблемы сложности алгоритмов, основные аспекты безопасности и основные угрозы безопасности

4. должен демонстрировать способность и готовность:

знаниями по основным разделам криптографии

4. должен демонстрировать способность и готовность:

ориентироваться в вопросах стандартов безопасности и законодательства в области защиты информации

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

Общая трудоемкость дисциплины составляет 7 зачетных(ые) единиц(ы) 252 часа(ов).

Форма промежуточного контроля дисциплины зачет в 6 семестре; экзамен в 7 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. Сложность алгоритмов	6	1-3	0	0	6	домашнее задание
2.	Тема 2. Сведения из теории чисел	6	4-6	0	0	6	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	6	7-9	0	0	6	домашнее задание
4.	Тема 4. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	6	10-12	0	0	6	домашнее задание
5.	Тема 5. Симметричное шифрование: обзор современных шифров.	6	13-18	0	0	12	контрольная работа

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.	7	1-3	0	0	6	домашнее задание
7.	Тема 7. Проблема распределения ключей и протоколы распределения ключей.	7	4-6	0	0	6	домашнее задание
8.	Тема 8. Система шифрования RSA	7	7-9	0	0	6	домашнее задание
9.	Тема 9. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.	7	10-12	0	0	6	домашнее задание
10.	Тема 10. Протокол электронного голосования	7	13-18	0	0	12	контрольная работа
·	Тема . Итоговая форма контроля	6		0	0	0	зачет
·	Тема . Итоговая форма контроля	7		0	0	0	экзамен
	Итого			0	0	72	

## 4.2 Содержание дисциплины

### Тема 1. Сложность алгоритмов

#### *лабораторная работа (6 часа(ов)):*

Теория алгоритмов, оценка сложности

### Тема 2. Сведения из теории чисел

#### *лабораторная работа (6 часа(ов)):*

Основные сведения из теории чисел

### Тема 3. Алгебраические структуры, конечные поля

#### *лабораторная работа (6 часа(ов)):*

Теория конечных полей, алгебраические структуры

### Тема 4. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.

#### *лабораторная работа (6 часа(ов)):*

Основные угрозы и аспекты безопасности. Законодательство в области безопасности

### Тема 5. Симметричное шифрование: обзор современных шифров.

#### *лабораторная работа (12 часа(ов)):*

Метод симметричного шифрования. Современные шифры

### **Тема 6. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.**

#### **лабораторная работа (6 часа(ов)):**

Метод ассимметричного шифрования. Односторонние функции и новые задачи криптографии

### **Тема 7. Проблема распределения ключей и протоколы распределения ключей.**

#### **лабораторная работа (6 часа(ов)):**

Распределения ключей. Протоколы распределения ключей

### **Тема 8. Система шифрования RSA**

#### **лабораторная работа (6 часа(ов)):**

Система шифрования RSA

### **Тема 9. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.**

#### **лабораторная работа (6 часа(ов)):**

Протоколы проверки аутентичности. Протоколы распределения секрета. Протоколы цифровой подписи

### **Тема 10. Протокол электронного голосования**

#### **лабораторная работа (12 часа(ов)):**

Протокол электронного голосования

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

<b>N</b>	<b>Раздел Дисциплины</b>	<b>Семестр</b>	<b>Неделя семестра</b>	<b>Виды самостоятельной работы студентов</b>	<b>Трудоемкость (в часах)</b>	<b>Формы контроля самостоятельной работы</b>
1.	Тема 1. Сложность алгоритмов	6	1-3	подготовка домашнего задания	12	домашнее задание
2.	Тема 2. Сведения из теории чисел	6	4-6	подготовка домашнего задания	12	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	6	7-9	подготовка домашнего задания	12	домашнее задание
4.	Тема 4. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	6	10-12	подготовка домашнего задания	12	домашнее задание
5.	Тема 5. Симметричное шифрование: обзор современных шифров.	6	13-18	подготовка к контрольной работе	24	контрольная работа
6.	Тема 6. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.	7	1-3	подготовка домашнего задания	12	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
7.	Тема 7. Проблема распределения ключей и протоколы распределения ключей.	7	4-6	подготовка домашнего задания	12	домашнее задание
8.	Тема 8. Система шифрования RSA	7	7-9	подготовка домашнего задания	12	домашнее задание
9.	Тема 9. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.	7	10-12	подготовка домашнего задания	12	домашнее задание
10.	Тема 10. Протокол электронного голосования	7	13-18	подготовка к контрольной работе	24	контрольная работа
	Итого				144	

## 5. Образовательные технологии, включая интерактивные формы обучения

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

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. Сложность алгоритмов

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по темам: Теория алгоритмов, оценка сложности

### Тема 2. Сведения из теории чисел

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по теме: Основные сведения из теории чисел

### Тема 3. Алгебраические структуры, конечные поля

домашнее задание , примерные вопросы:



Изучение литературы и выполнения упражнений по темам: Теория конечных полей  
Алгебраические структуры

**Тема 4. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.**

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по темам: Основные угрозы и аспекты безопасности. Законодательство в области безопасности

**Тема 5. Симметричное шифрование: обзор современных шифров.**

контрольная работа , примерные вопросы:

Проверка знаний по темам: Метод симметричного шифрования. Современные шифры

**Тема 6. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.**

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по темам: Метод ассимметричного шифрования. Односторонние функции и новые задачи криптографии

**Тема 7. Проблема распределения ключей и протоколы распределения ключей.**

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по темам: Распределения ключей. Протоколы распределения ключей

**Тема 8. Система шифрования RSA**

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по темам: Система шифрования RSA

**Тема 9. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.**

домашнее задание , примерные вопросы:

Изучение литературы и выполнения упражнений по темам: Протоколы проверки аутентичности. Протоколы распределения секрета. Протоколы цифровой подписи

**Тема 10. Протокол электронного голосования**

контрольная работа , примерные вопросы:

Проверка знаний по темам: Протокол электронного голосования

**Тема . Итоговая форма контроля**

**Тема . Итоговая форма контроля**

Примерные вопросы к зачету и экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные вопросы для экзамена:

1. Теория алгоритмов, оценка сложности
2. Основные сведения из теории чисел
3. Теория конечных полей, алгебраические структуры
4. Основные угрозы и аспекты безопасности.
5. Законодательство в области безопасности
6. Метод симметричного шифрования.
7. Современные шифры
8. Односторонние функции и новые задачи криптографии
9. Распределения ключей.
10. Протоколы распределения ключей
11. Система шифрования RSA
12. Протоколы проверки аутентичности.
13. Протоколы распределения секрета.



14. Протоколы цифровой подписи
15. Протокол электронного голосования

### **7.1. Основная литература:**

1. Громкович, Юрай. Теоретическая информатика : Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Юрай Громкович ; Пер. с нем.; Под ред. Б. Ф. Мельникова .- Издание 3-е .- Санкт-Петербург : БХВ-Петербург, 2010 .- 336 с.
2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с.  
<http://znanium.com/bookread.php?book=441493>
3. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с.  
<http://znanium.com/bookread.php?book=415501>
4. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.  
<http://znanium.com/bookread.php?book=402686>

### **7.2. Дополнительная литература:**

1. Масленников М.Е. Практическая криптография / Михаил Масленников .- СПб. : БХВ-Петербург, 2003 .- 458с.
2. Латыпов Р.Х. Математические основы кодирования информации и криптографии : учеб. пособие / Р. Х. Латыпов ; Казан. гос. ун-т .- Казань : [КГУ], 2005 .- 59 с.

### **7.3. Интернет-ресурсы:**

- Криптографические средства защиты информации - <http://infosecmd.narod.ru/gl5.html>  
Криптографические средства защиты информации - <http://infosecmd.narod.ru/gl5.html>  
Криптографические средства защиты информации - <http://infosecmd.narod.ru/gl5.html>  
Криптографические средства защиты информации - <http://infosecmd.narod.ru/gl5.html>  
Криптографические средства защиты информации - <http://infosecmd.narod.ru/gl5.html>

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

Освоение дисциплины "Основы криптографии" предполагает использование следующего материально-технического обеспечения:

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 010400.62 "Прикладная математика и информатика" и профилю подготовки Системное программирование, математическое моделирование .

Автор(ы):

Латыпов Р.Х. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Пшеничный П.В. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.