

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Оренбургский государственный университет»

Кафедра алгебры и дискретной математики

## **РАБОЧАЯ ПРОГРАММА**

### **ДИСЦИПЛИНЫ**

*«Б.1.В.ОД.3 Криптографические методы защиты информации»*

Уровень высшего образования

**БАКАЛАВРИАТ**

Направление подготовки

02.03.01 Математика и компьютерные науки  
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики  
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа академического бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики

наименование кафедры

протокол № 7 от "21" февраля 2017г.

Заведующий кафедрой

Кафедра алгебры и дискретной математики

наименование кафедры

подпись

О.А. Пихтилькова

расшифровка подписи

Исполнители:

директор

должность

[подпись]

подпись

Носов В.В.

расшифровка подписи

должность

подпись

расшифровка подписи

СОГЛАСОВАНО:

Председатель методической комиссии по направлению подготовки

02.03.01 Математика и компьютерные науки

код наименование

личная подпись

О.А. Пихтилькова

расшифровка подписи

Заведующий отделом комплектования научной библиотеки

личная подпись

Н.Н. Грицай

расшифровка подписи

Уполномоченный по качеству факультета

личная подпись

И.В. Крючкова

расшифровка подписи

## 1 Цели и задачи освоения дисциплины

**Цель (цели)** освоения дисциплины: ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами.

### **Задачи:**

- 1. Сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер.
- 2. Сформировать базовые теоретические понятия (возможно, на элементарном уровне), лежащие в основе процесса защиты информации.
- 3. Дать представление о роли компьютера, как о центральном месте в области криптографии, взявшем на себя большинство функций традиционной компьютерной деятельности, включающей реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей, автоматизацию работы по анализу перехвата и раскрытию шифров.
- 4. Научить использованию криптографических алгоритмов в широко распространенных программных продуктах.

## 2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.14 Фундаментальная и компьютерная алгебра, Б.1.Б.22 Языки и технологии программирования, Б.1.В.ОД.7 Теория кодирования, сжатия и восстановления информации, Б.1.В.ОД.11 Алгебраические системы, Б.1.В.ОД.14 Теоретико-числовые методы в криптографии*

Постреквизиты дисциплины: *Б.1.В.ДВ.6.1 Защита программ и данных, Б.2.В.П.1 Преддипломная практика*

## 3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

| Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций   | Формируемые компетенции  |
|---|--|
| <p><b><u>Знать:</u></b><br/>Алгебру целых, комплексных, действительных и <math>p</math>-адических чисел</p> <p><b><u>Уметь:</u></b><br/>Производить вычисления в различных алгебраических системах</p> <p><b><u>Владеть:</u></b><br/>Основными методами алгебры, геометрии, математического анализа теории вероятностей и математической статистики</p> | ОПК-1 готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и |

|  |   |
|--|---|
| Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций  | Формируемые компетенции   |
|  | случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности  |
| <p><b>Знать:</b><br/>Основные способы и методы решения математических задач</p> <p><b>Уметь:</b><br/>Формулировать задачи на математическом языке</p> <p><b>Владеть:</b><br/>Математическим аппаратом решения стандартных задач с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>   | ОПК-4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем |
| <p><b>Знать:</b><br/>содержание ключевых понятий и определений, используемых в теории и практике применения информационных технологий в науке и образовании, информационные ресурсы и базы данных по научно-исследовательской теме</p> <p><b>Уметь:</b><br/>применять прикладное программное обеспечение для решения задач в профессиональной деятельности, науке и образовании, самостоятельно расширять и углублять знания в области информационных технологий</p> <p><b>Владеть:</b><br/>навыками пользования прикладного программного обеспечения для решения задач в профессиональной деятельности, науке и образовании, навыками использования интернет-технологий; навыками компьютерной обработки вычислительных задач</p> | ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области   |

## 4 Структура и содержание дисциплины

### 4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 академических часов).

| Вид работы  | Трудоемкость, академических часов |              |
|---|-----------------------------------|--------------|
|   | 6 семестр                         | всего        |
| <b>Общая трудоёмкость</b>   | <b>144</b>                        | <b>144</b>   |
| <b>Контактная работа:</b>   | <b>53,25</b>                      | <b>53,25</b> |
| Лекции (Л)  | 18                                | 18           |
| Практические занятия (ПЗ)   | 34                                | 34           |
| Консультации  | 1                                 | 1            |
| Промежуточная аттестация (зачет, экзамен)   | 0,25                              | 0,25         |
| <b>Самостоятельная работа:</b><br>- самостоятельное изучение разделов (перечислить);<br>- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);<br>- подготовка к практическим занятиям;<br>- подготовка к коллоквиумам;<br>- подготовка к рубежному контролю и т.п.) | <b>90,75</b>                      | <b>90,75</b> |

| Вид работы   | Трудоемкость, академических часов |       |
|--|-----------------------------------|-------|
|  | 6 семестр                         | всего |
| <b>Вид итогового контроля (зачет, экзамен, дифференцированный зачет)</b> | <b>экзамен</b>                    |       |

Разделы дисциплины, изучаемые в 6 семестре

| № раздела | Наименование разделов                     | Количество часов |                   |    |    |                |
|-----------|---|------------------|-------------------|----|----|----------------|
|           |   | всего            | аудиторная работа |    |    | внеауд. работа |
|           |   |                  | Л                 | ПЗ | ЛР |                |
| 1         | История криптографии. Классические шифры. | 8                | 2                 | 6  |    | 12             |
| 2         | Математические основы криптографии.       | 10               | 4                 | 6  |    | 14             |
| 3         | Классификация шифров                      | 10               | 4                 | 6  |    | 12             |
| 4         | Хэш-функции                               | 6                | 2                 | 4  |    | 14             |
| 5         | Криптография с открытым ключом            | 8                | 2                 | 6  |    | 14             |
| 6         | Электронные цифровые подписи              | 4                | 2                 | 2  |    | 14             |
| 7         | Протоколы                                 | 6                | 2                 | 4  |    | 12             |
|           | Итого:                                    | 144              | 18                | 34 |    | 92             |
|           | Всего:                                    | 144              | 18                | 34 |    | 92             |

## 4.2 Содержание разделов дисциплины

**1 История криптографии. Классические шифры.** Шифр Атбаш, Квадрат Полибия Шифр Сцитала, Шифр Цезаря, Шифр Тритемия, Квадрат Виженера, Шифрующие таблицы Шифр Плейфера Двойной квадрат

**2 Математические основы криптографии.** Основные понятия теории вероятности и математической статистики. Случайные числа, генератор случайных чисел. Сравнения первой и второй степеней. Первообразные корни и индексы. Оценка сложности алгоритмов. Классы задач P и NP. Примеры NP-полных задач.

**3 Классификация шифров.** Шифры замены и шифры перестановки, композиционные шифры. Симметричные асимметричные. Шифры однозначной и многозначной замены. Поточные и блочные. Одноалфавитный шифр замены и многоалфавитный. Шифры гаммирования.

**4 Хэш-функции.** Алгоритм MD5, Алгоритм MD5 для вычисления хэш-функции, Алгоритм SHA-1, Алгоритм SHA-1 для вычисления хэш-функции, Алгоритм RIPEMD-160, Алгоритм RIPEMD-160 для вычисления хэш-функции, ГОСТ Р34.11-94. Функция хеширования, Алгоритм ГОСТ для вычисления хэш-функции.

**5 Криптография с открытым ключом.** СХЕМА ДИФФИ-ХЭЛЛМАНА. Протокол формирования общего ключа по открытому каналу связи. Протокол взаимной аутентификации. КРИПТОСИСТЕМА RSA. Формирование системы RSA. Алгоритм шифрования. Алгоритм дешифрования. Цифровая подпись. СХЕМА ЭЛЬ-ГАМАЛЯ. Алгоритм формирования схемы Эль-Гамалы. Алгоритм формирования цифровой подписи. Проверка подписи. Алгоритм расшифрования. СХЕМА ШНОРРА. Алгоритм формирования схемы Шнорра. Алгоритм формирования цифровой подписи. Проверка подписи. Протокол аутентификации. Задача о рюкзаке. Алгоритм формирования криптографической системы. Схема шифрования текста. Схема дешифрования текста

**6 Электронные цифровые подписи.** Стандарт электронной цифровой подписи DSS. Формирование системы DSS. Формирование подписи DSS. Алгоритм проверки подписи DSS.

**7 Протоколы. Понятие протокола. Простейший протокол. Протокол с арбитром и без. Атака на протокол.**

### **4.3 Практические занятия (семинары)**

| № занятия | № раздела | Тема                               | Кол-во часов |
|-----------|-----------|------------------------------------|--------------|
| 1,2,3     | 1         | Классические шифры.                | 6            |
| 4,5,6     | 2         | Математические основы криптографии | 6            |
| 7,8,9     | 3         | Классификация шифров               | 6            |
| 10,11     | 4         | Хэш-функции                        | 4            |
| 12,13,14  | 5         | Криптография с открытым ключом     | 6            |
| 15        | 6         | Электронные цифровые подписи       | 2            |
| 16,17     | 7         | Протоколы                          | 4            |
|           |           | Итого:                             | 34           |

## **5 Учебно-методическое обеспечение дисциплины**

### **5.1 Основная литература**

**1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>**

**2. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=229582> (02.12.2018).**

### **5.2 Дополнительная литература**

**1. Фефилов, А.Д. Методы и средства защиты информации в сетях / А.Д. Фефилов. - М. : Лаборатория книги, 2011. - 105 с. : ил., табл. - ISBN 978-5-504-00608-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=140796>**

### **5.3 Периодические издания**

...

### **5.4 Интернет-ресурсы**

- [http://cryptography.ru/info/введение\\_в\\_теорию\\_сложности\\_вычислен/](http://cryptography.ru/info/введение_в_теорию_сложности_вычислен/) – Введение в теорию сложности вычислений
- [http://cryptography.ru/info/курс\\_лекций\\_м-и-анохина/](http://cryptography.ru/info/курс_лекций_м-и-анохина/) – Математическая криптография

**5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий**

Операционная система MS Windows, пакет офисных программ Libre Office.

## **6 Материально-техническое обеспечение дисциплины**

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой подключенной к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду ОГУ.

### ***К рабочей программе прилагаются:***

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.