

УДК 004.056(07)  
М645

**Рецензенты:**

кафедра информатики, информационных технологий и защиты информации  
Липецкого государственного педагогического университета  
им. П.П. Семенова-Тян-Шанского  
(зав. кафедрой канд. техн. наук, доц. Скуднев Д.М.);  
Малыш В.Н., д-р техн. наук, проф.,  
заведующий кафедрой гуманитарных и естественнонаучных дисциплин  
Липецкого филиала Российской академии народного хозяйства и  
государственной службы при Президенте Российской Федерации

**Мирошников, А.И.**

М645 Основы информационной безопасности и защита информации: учебное пособие / А.И. Мирошников, А.С. Сысоев. – Липецк: Изд-во Липецкого государственного технического университета, 2022. – 107 с. – Текст: непосредственный.

ISBN 978-5-00175-160-1

В пособии описаны основные понятия криптографии, приводятся классические и актуальные методы построения криптографических систем, а также освещена базовая теория криптоанализа. Пособие содержит задания для практических и лабораторных работ для закрепления изученного материала.

Учебное пособие предназначено для студентов направлений подготовки бакалавриата, получающих углублённую подготовку в сфере информационных технологий. Пособие также будет полезно инженерам, аспирантам, научным работникам и специалистам в области защиты информации.

Табл. 16. Ил. 24. Библиогр.: 5 назв.

УДК 004.056(07)

Печатается по решению редакционно-издательского совета ЛГТУ.

ISBN 978-5-00175-160-1

© ФГБОУ ВО «Липецкий государственный технический университет», 2022  
© Мирошников А.И., Сысоев А.С., 2022

## Содержание

|   |     |
|---|-----|
| Введение . . . . .  | 4   |
| 1. Основные понятия криптографии . . . . .  | 5   |
| 1.1. Введение в информационную безопасность . . . . .   | 5   |
| 1.2. Принципы построения защищенной информационной системы  | 10  |
| 1.3. Криптография. Основные понятия . . . . .   | 13  |
| 1.4. Классические криптосистемы . . . . .   | 17  |
| 2. Симметричные криптографические системы . . . . .   | 23  |
| 2.1. Поточное шифрование . . . . .  | 23  |
| 2.2. Блочное шифрование . . . . .   | 25  |
| 3. Асимметричные криптографические системы . . . . .  | 55  |
| 3.1. Криптосистемы с открытым ключом . . . . .  | 55  |
| 3.2. Однонаправленные функции . . . . .   | 56  |
| 3.3. Примеры асимметричных криптографических систем. . . . .  | 58  |
| 4. Системы электронной цифровой подписи. Идентификация и аутен-<br>тификация пользователей в сети . . . . . | 63  |
| 4.1. Системы электронной цифровой подписи . . . . .   | 63  |
| 4.2. Системы электронной цифровой подписи с дополнительными<br>функциональными свойствами . . . . .         | 74  |
| 4.3. Модели безопасности . . . . .  | 77  |
| 5. Алгоритмы криптоанализа . . . . .  | 81  |
| 5.1. Основные понятия и определения . . . . .   | 81  |
| 5.2. Универсальные методы криптоанализа . . . . .   | 81  |
| 5.3. Методы криптоанализа асимметричных криптосистем. . . . .   | 87  |
| 6. Задания для практических и лабораторных работ . . . . .  | 89  |
| Заключение . . . . .  | 101 |
| Список рекомендуемой литературы . . . . .   | 102 |
| Библиографический список . . . . .  | 106 |