

ВЫСШЕЕ ОБРАЗОВАНИЕ



С. В. Запечников, О. В. Казарин, А. А. Тарасов

# КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ



СООТВЕТСТВУЕТ  
ПРОГРАММАМ  
ВЕДУЩИХ НАУЧНО-  
ОБРАЗОВАТЕЛЬНЫХ  
ШКОЛ

УМО рекомендует  
УМО ВО рекомендует

**Юрайт**  
ИЗДАТЕЛЬСТВО

# Оглавление

Предисловие .....	6
Условные обозначения .....	8
Введение .....	9
<b>Глава 1. Основные положения криптографии и базовые криптографические понятия .....</b>	<b>13</b>
1.1. Основные понятия и определения современной криптографии .....	14
1.2. Классическая и математическая криптография .....	19
1.3. Стойкость криптографических схем: неформальное введение .....	21
1.3.1. Классическая криптография .....	21
1.3.2. Математическая криптография .....	26
<i>Литература</i> .....	29
<i>Контрольные вопросы и задания</i> .....	30
<i>Задания для самостоятельной работы</i> .....	30
<b>Глава 2. Краткая история криптографии .....</b>	<b>34</b>
2.1. Эпоха донаучной криптографии .....	35
2.2. Криптография XX века .....	45
<i>Литература</i> .....	48
<i>Контрольные вопросы и задания</i> .....	49
<i>Задания для самостоятельной работы</i> .....	50
<b>Глава 3. Базовые криптографические методы и схемы криптографической защиты информации .....</b>	<b>52</b>
3.1. Криптосистемы с секретным ключом .....	53
3.2. Криптосистемы с открытым ключом .....	63
3.3. Схемы электронной подписи .....	72
3.3.1. Общая идея схем электронной подписи .....	72
3.3.2. Описание схем электронной подписи .....	75
3.3.3. Примеры схем электронной подписи .....	77
3.3.4. Процедуры арбитража .....	78
3.4. Схемы построения хэш-функций .....	79
3.4.1. Общая идея хэш-функций .....	79
3.4.2. Описание хэш-функций .....	81
3.4.3. Практические аспекты построения хэш-функций .....	82
3.5. Схемы построения псевдослучайных генераторов .....	85
3.5.1. Описание псевдослучайного генератора .....	85
3.5.2. Пример псевдослучайного генератора .....	86

3.6. Схемы вероятностного шифрования .....	87
3.6.1. Описание схем вероятностного шифрования .....	87
3.6.2. Пример схемы вероятностного шифрования .....	88
3.7. Интерактивные системы доказательств.....	89
3.7.1. Интерактивные системы доказательств с нулевым разглашением .....	89
3.7.2. Пример интерактивной системы доказательств .....	91
<i>Литература</i> .....	94
<i>Контрольные вопросы и задания</i> .....	95
<i>Задания для самостоятельной работы</i> .....	96
<b>Глава 4. Криптографические протоколы .....</b>	<b>97</b>
4.1. Основы теории криптографических протоколов .....	97
4.2. Протоколы аутентификации .....	103
4.3. Протоколы распределения ключей .....	119
4.3.1. Протоколы, основанные на симметричных криптосхемах .....	122
4.3.2. Протоколы, основанные на асимметричных криптосхемах .....	129
4.4. Протоколы образования защищенных каналов передачи данных .....	138
4.5. Разновидности протоколов электронной подписи .....	146
4.5.1. Протокол конфиденциальной подписи .....	146
4.5.2. Протокол мультиподписи .....	148
4.5.3. Протокол групповой подписи .....	149
4.5.4. Протокол подписи вида онлайн/офлайн .....	151
4.5.5. Протокол подписи с ограниченным жизненным циклом .....	152
4.5.6. Протокол затемненной подписи .....	153
4.6. Банковские криптографические протоколы (протоколы финансовой криптографии) .....	154
4.6.1. Вводная часть .....	154
4.6.2. Электронные платежи .....	155
4.6.3. Электронные монеты .....	162
4.6.4. Электронные бумажники .....	169
4.7. Протоколы конфиденциальных вычислений .....	174
4.7.1. Общие положения и краткий экскурс в историю .....	174
4.7.2. Обобщенные модели конфиденциальных вычислений .....	176
4.7.3. Пример протокола конфиденциального вычисления функции .....	180
<i>Литература</i> .....	181
<i>Контрольные вопросы и задания</i> .....	187
<i>Задания для самостоятельной работы</i> .....	188
<b>Глава 5. Нормативное обеспечение в области криптографической защиты информации .....</b>	<b>192</b>
5.1. Законодательство Российской Федерации о нормативном регулировании криптографической защиты информации .....	192
5.1.1. Федеральный закон «Об информации, информационных технологиях и о защите информации» .....	193
5.1.2. Федеральный закон «О персональных данных» .....	193
5.1.3. Федеральный закон «Об электронной подписи» .....	194

5.2. Нормативные правовые акты и документы, определяющие технические требования в криптографической сфере .....	195
<i>Литература</i> .....	203
<i>Контрольные вопросы и задания</i> .....	205
<i>Задания для самостоятельной работы</i> .....	206
<b>Глава 6. Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке .....</b>	<b>209</b>
6.1. Организации, осуществляющие разработку средств криптографической защиты информации .....	210
6.2. Линейка продуктов «КриптоПро» .....	211
6.3. Средства криптографической защиты информации «Крипто БД» .....	213
6.4. Линейка продуктов Secret Disk .....	215
6.5. Продукция ФГУП «НТЦ «Атлас» .....	216
6.6. Продукция ОАО «ИнфоТеКС» .....	217
6.7. Другие продукты и услуги в области криптографической защиты информации .....	218
<i>Литература</i> .....	223
<i>Контрольные вопросы и задания</i> .....	224
<i>Задания для самостоятельной работы</i> .....	225
<b>Заключение .....</b>	<b>226</b>
<b>Приложения</b>	
Приложение А. Необходимые сведения из алгебры и алгебраической геометрии .....	230
Приложение Б. Необходимые сведения из теории вероятностей .....	234
Приложение В. Необходимые сведения из теории чисел .....	236
Приложение Г. Необходимые сведения из теории алгоритмов .....	241
Приложение Д. Необходимые сведения из теории сложности вычислений .....	251
Приложение Е. Веб-страницы ученых-криптографов .....	256
Приложение Ж. Перечень страниц сети Интернет криптографической направленности .....	257
Приложение З. Учебные курсы по криптографическим дисциплинам, представленные в сети Интернет .....	259
Приложение И. Отечественные нормативные акты, регламентирующие деятельность в области криптографической защиты информации (выдержки, извлечения) .....	260
<b>Предметный указатель .....</b>	<b>305</b>
<b>Именной указатель .....</b>	<b>308</b>