

УДК 519.5+681.325.3(075.8)
ББК 32.973.202-018.2
К92

Издание доступно в электронном виде по адресу
ebooks.bmstu.press/catalog/274/book2082.html

Факультет «Информатика и системы управления»
Кафедра «Защита информации»

*Рекомендовано Научно-методическим советом
МГТУ им. Н.Э. Баумана в качестве учебного пособия*

Рецензент
профессор МАИ *Р.Б. Мазена*

Куприянов, А. И.
К92 Исследование криптографических методов защиты информации :
учебное пособие / А. И. Куприянов, В. Ф. Макаров. — Москва : Изда-
тельство МГТУ им. Н. Э. Баумана, 2019. — 109, [1] с. : ил.

ISBN 978-5-7038-5059-6

Изложены основные теоретические положения и практические приемы криптографических преобразований сообщений в информационно-телекоммуникационных системах. Рассмотрены такие преобразования, как шифрация, защита и аутентификация информации, стеганографические приемы сокрытия передачи сообщений и методы идентификации объектов информационного взаимодействия.

Для студентов, обучающихся в МГТУ им. Н.Э. Баумана по программе специалитета по направлению подготовки «Информационная безопасность» и изучающих раздел дисциплины «Основы криптографических методов защиты информации».

УДК 519.5+681.325.3(075.8)
ББК 32.973.202-018.2

ISBN 978-5-7038-5059-6

© МГТУ им. Н.Э. Баумана, 2019
© Оформление. Издательство
МГТУ им. Н.Э. Баумана, 2019

Оглавление

Предисловие	3
Основные сокращения	5
Введение	6
Контрольные вопросы	10
1. ИССЛЕДОВАНИЕ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ	11
1.1. Принципы симметричной (одноключевой) криптографии	11
1.2. Практические симметричные криптоалгоритмы	14
1.3. Стандарты симметричных криптосистем	24
1.4. Экспериментальное исследование алгоритмов симметричного криптографического преобразования	29
Контрольные вопросы	30
2. АЛГОРИТМЫ ПРЕОБРАЗОВАНИЯ СООБЩЕНИЙ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ С ОТКРЫТЫМ КЛЮЧОМ	31
2.1. Алгоритм криптографической системы RSA	32
2.2. Алгоритм криптографической системы на основе вычисления дискретных логарифмов в конечном поле — алгоритм Эль Гамала	35
2.3. Алгоритм функционирования криптографической системы на основе дискретного логарифмирования в метрике эллиптических кривых	39
2.4. Экспериментальное исследование криптографических систем с открытым ключом	44
Контрольные вопросы	47
3. КОМПЛЕКСИРОВАНИЕ КРИПТОСИСТЕМ С ОТКРЫТЫМ И ЗАКРЫТЫМ КЛЮЧОМ	49
3.1. Преимущества и недостатки одно- и двухключевых криптосистем	49
3.2. Преобразование Диффи — Хеллмана в системах криптографии с открытым ключом	50
3.3. Алгоритм автоматического формирования парных симметричных ключей шифрования — дешифрования открытых сообщений на рабочих станциях абонентов информационно- телекоммуникационной системы	52

3.4. Экспериментальное исследование алгоритма Диффи — Хеллмана автоматического формирования парных симметричных ключей шифрования — дешифрования	53
Контрольные вопросы.....	54
4. АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ	55
4.1. Принцип аутентификации сообщений посредством электронной цифровой подписи.....	55
4.2. Алгоритм RSA формирования и аутентификации электронной цифровой подписи	59
4.3. Алгоритм Эль Гамала (EGSA) формирования электронной цифровой подписи	63
4.4. Алгоритм DSA формирования электронной цифровой подписи.....	67
4.5. Алгоритм формирования электронной цифровой подписи на основе разложения на множители больших простых чисел.....	71
4.6. Алгоритм формирования электронной цифровой подписи по ГОСТ Р34.10–2012	74
4.7. Экспериментальное исследование методов аутентификации электронных сообщений	78
Контрольные вопросы.....	80
5. СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ	81
5.1. Принципы стеганографии	81
5.2. Экспериментальное исследование алгоритмов стеганографических преобразований.....	84
Контрольные вопросы.....	85
6. МЕТОДЫ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЯХ.....	86
6.1. Принципы идентификации объектов	86
6.2. Методы аутентификации на основе паролей	89
6.3. Механизмы аутентификации санкционированных пользователей	90
6.4. Протоколы аутентификации с нулевой передачей знаний	92
6.5. Экспериментальное исследование методов идентификации	101
Контрольные вопросы.....	106
Литература.....	107