

УДК 681.3.066 (075.8)
ББК 32.973-018.2
Б43

Издание доступно в электронном виде на портале *ebooks.bmstu.ru*
по адресу: <http://ebooks.bmstu.ru/catalog/229/book210.html>

Факультет «Робототехника и комплексная автоматизация»
Кафедра «Системы автоматизированного проектирования»

*Рекомендовано Научно-методическим советом МГТУ
им. Н.Э. Баумана в качестве учебного пособия по дисциплине
«Методы и средства защиты компьютерной информации»*

Рецензенты: д-р техн. наук, профессор *Н. И. Сельвесюк*,
канд. техн. наук, доцент *Н. В. Чичварин*

Беломойцев Д. Е.

Б43 Основные методы криптографической обработки данных:
учеб. пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Ро-
дионов. — М. : Изд-во МГТУ им. Н. Э. Баумана, 2014. — 76,
[4] с. : ил.

ISBN 978-5-7038-3833-4

Рассмотрены основные принципы и методы криптографиче-
ской обработки информации. Приведены сведения о структуре
и функциях криптосистем для обработки данных.

Для студентов 4-го курса, изучающих дисциплину «Мето-
ды и средства защиты информации».

УДК 681.3.066 (075.8)
ББК 32.973-018.2

ISBN 978-5-7038-3833-4

© МГТУ им. Н.Э. Баумана, 2014
© Оформление. Издательство
МГТУ им. Н.Э. Баумана, 2014

Оглавление

Введение	3
1. Симметричные криптосистемы	5
1.1. Принципы построения симметричных криптосистем ...	5
1.2. Шифры перестановки.....	9
1.3. Шифры замены	10
1.4. Современные симметричные криптосистемы	12
2. Асимметричные криптосистемы	29
2.1. Криптоконцепция Диффи – Хеллмана	29
2.2. Криптозащита Меркля – Хеллмана.....	33
2.3. Криптосистема RSA	38
2.4. Криптосистема Эль-Гамала	43
3. Хеширование данных	49
3.1. Однонаправленные хеш-функции.....	49
3.2. Современные алгоритмы хеширования.....	53
4. Криптографические протоколы.....	56
4.1. Разновидности криптографических протоколов	56
4.2. Электронные деньги.....	60
4.3. Протокол «подбрасывания монеты по телефону».....	61
4.4. Протокол разделения секрета	65
4.5. Протокол подписания контракта.....	66
4.6. Протокол тайного голосования	75
Литература.....	77