

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

М.С. Жуковский, С.А. Безносюк

КВАНТОВАЯ КРИПТОГРАФИЯ

Учебное пособие



Барнаул

Издательство
Алтайского государственного
университета
2013

УДК 541.1(075.8)

ББК 24.5я73

Ж 864

Рецензенты:

доктор физ.-мат. наук, профессор **В.В. Поляков** (АлтГУ),
доктор физ.-мат. наук, профессор **В.А. Плотников** (АлтГУ)

Ж 864 **Жуковский, М.С.**

Квантовая криптография [Текст] : учебное пособие /
М.С. Жуковский, С.А. Безносюк. – Барнаул : Изд-во Алт.
ун-та, 2013. – 44 с.

ISBN 978-5-7904-1486-2

Рассматриваются основные понятия новой дисциплины – квантовой криптографии, которая основывается на фундаментальных принципах квантовой механики и позволяет вывести процедуры дешифровки на принципиально новый уровень. Изложены фундаментальные основы квантово-механического подхода применительно к задачам криптографии и понятные схемы базовых алгоритмов, пригодных для программной реализации, что позволяет использовать пособие как источник заданий для программистов.

УДК 541.1(075.8)

ББК 24.5я73

*Издание опубликовано в рамках реализации
Программы стратегического развития
Алтайского государственного университета*

ISBN 978-5-7904-1486-2

© Жуковский М.С., Безносюк С.А., 2013
© Оформление. Издательство Алтайского
государственного университета, 2013

ОГЛАВЛЕНИЕ

Введение.....	3
Глава 1. Краткая история шифрования.....	5
1.1. Подстановочные шифры.....	5
1.2. Блочные шифры.....	7
1.3. Абсолютно стойкие шифры.....	10
1.4. Двухключевая система. Шифр RSA.....	11
Глава 2. Квантовая механика и информация.....	18
2.1. Принцип действия протокола BB84.....	18
2.2. Основы алгоритмов квантового шифрования.....	22
2.3. Технологии взлома квантовой криптографической системы.....	37
Заключение.....	40
Библиографический список.....	41

Учебное издание

**Марк Сергеевич Жуковский,
Сергей Александрович Безносюк**

КВАНТОВАЯ КРИПТОГРАФИЯ

Учебное пособие

Редактирование и подготовка
оригинал-макета: *Е.М. Федяева*

ЛР 020261 от 14.01.1997 г.

Подписано в печать 19.11.2013. Формат 60x84(1/16)

Бумага офсетная. Усл. печ. л. 2.6.

Тираж 300 экз. Заказ 359.

Издательство Алтайского государственного университета

Типография Алтайского государственного университета:

656049, Барнаул, ул. Димитрова, 66