УДК 003.26:004.056
ББК 32.973.26-018.2+81.1
Б79

Печатается по решению редакционно-издательского совета
Московского государственного технического университета ГА

Рецензенты: канд. техн. наук, проф. В.И. Петров;
канд. техн. наук С.А. Полосин

Болелов Э.А.

Б79 Криптографические методы защиты информации: учебное пособие. - М.: МГТУ ГА, 2013. – 80 с. 5 табл., 22 ил., лит.: 12 наим.

ISBN 978-5-86311-887-1

Данное учебное пособие издается в соответствии с рабочей программой учебной дисциплины «Криптографические методы защиты информации» по Учебному плану специальности 090302 для студентов IV курса очной формы обучения.

В учебном пособии приведены основные понятия теории ассиметричных криптосистем, представлены основные типы криптосистем, схемы реализации и стандарты электронных подписей, рассмотрены методы криптоанализа ассиметричных криптосистем.

Рассмотрено и одобрено на заседаниях кафедры 07.03.13г. и методического совета 27.02.13г.

ББК 32.973.26-018.2+81.1
Св. тем. план 2013 г.
поз. 33

БОЛЕЛОВ Эдуард Анатольевич

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Часть II
Ассиметричные криптосистемы

Редактор Л.Е. Паталова

Подписано в печать 21.05.13г.

Печать офсетная	Формат 60x84/16	4,65 уч.-изд. л.
4,69 усл. печ. л.	Заказ № 1620/	Тираж 100 экз.

Московский государственный технический университет ГА
125993 Москва, Кронштадтский бульвар, д.20
Редакционно-издательский отдел
125493 Москва, ул. Пулковская, д. 6а

ISBN 978-5-86311-887-1