УДК 004.056.55(075.8)
К 736

Рецензенты:

д-р техн. наук, проф. *В.И. Гужов,*
канд. техн. наук, доцент *Г.В. Трошина*

Работа подготовлена на кафедре защиты информации

Котов Ю.А.

К 736 Приложения шифров. Криптоанализ: учебное пособие / Ю.А. Котов. – Новосибирск: Изд-во НГТУ, 2019. – 76 с.

ISBN 978-5-7782-3902-9

Представлены приложения шифров для аутентификации данных и субъектов, формирования электронно-цифровой подписи, основные подходы к генерации псевдослучайных числовых последовательностей и криптоанализу шифров.

Предназначено для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность» и специальности 10.05.03 «Информационная безопасность автоматизированных систем».

УДК 004.056.55(075.8)

Котов Юрий Алексеевич

ПРИЛОЖЕНИЯ ШИФРОВ
КРИПТОАНАЛИЗ

Учебное пособие

Редактор *М.О. Мокшанова*
Выпускающий редактор *И.П. Брованова*
Корректор *И.Е. Семенова*
Дизайн обложки *А.В. Ладыжская*
Компьютерная верстка *Н.В. Гаврилова*

Налоговая льгота – Общероссийский классификатор продукции
Издание соответствует коду 95 3000 ОК 005-93 (ОКП)

Подписано в печать 28.05.2019. Формат 60 × 84 1/16. Бумага офсетная
Тираж 50 экз. Уч.-изд. л. 4,41. Печ. л. 4,75. Изд. № 317/18. Заказ № 937. Цена договорная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20

ISBN 978-5-7782-3902-9

ОГЛАВЛЕНИЕ