

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ. ЧАСТЬ 1 Основы криптографии: Учебное пособие / А.С. Овсянников, М.А. Бурова. - Самара: ПГУТИ, 2011. – 113 с.

Приведены основные понятия и определения информационной безопасности в компьютерных системах.

Изложены классические методы блочного и потокового шифрования, рассмотрены стандарты шифрования DES; ГОСТ 28147-89 и система криптозащиты сообщений PGP.

Рассчитано на студентов ФИСТ ПГУТИ очной и заочной форм обучения, обучающихся по специальности “Информационные системы и технологии” и изучающих дисциплину “Информационная безопасность и защита информации в компьютерных системах” в рамках лекционных и лабораторных занятий.

Разработано на кафедре информационных систем и технологий.

Может быть рекомендовано для студентов, обучающихся по направлениям “Информационные системы” и “Информатика и вычислительная техника”

#### **Рецензенты:**

Д.т.н., проф., зав. кафедрой ИСТ СамГУПС **А.М. Косолапов**

к.т.н, доцент кафедры СС ПГУТИ **И.И. Корнилов**