

А

Методические разработки к лабораторным работам по дисциплине  
«Средства обеспечения информационной безопасности в сетях передачи  
данных» / Сост. к.т.н., доц. А.В.Крыжановский,  
д.т.н., проф. А.А. Нерсисянц -Самара, 2005.-140 с. , ил.

Приведены методические указания к лабораторным работам, относящимся к основным разделам криптографии: симметричные и асимметричные криптосистемы, электронная цифровая подпись, управление криптографическими ключами и идентификация. Все методические указания снабжены краткими теоретическими сведениями.

Методические разработки утверждены на заседании кафедры ПДС 7.06.2005 г., протокол № 8.

Редактор- д.т.н., проф. Б.Я.Лихтциндер  
Рецензент-д.т.н. проф. В.Г. Карташевский

## Содержание

### Лабораторная работа №1

ИЗУЧЕНИЕ ОТЕЧЕСТВЕННОГО СТАНДАРТА ШИФРОВАНИЯ ГОСТ 28147-89.....3

### Лабораторная работа №2

ИЗУЧЕНИЕ АЛГОРИТМА ШИФРОВАНИЯ С ОТКРЫТЫМ КЛЮЧОМ RSA.....27

### Лабораторная работа №3

ИЗУЧЕНИЕ ПОСИМВОЛЬНОГО ШИФРОВАНИЯ НА ОСНОВЕ КРИПТОСИСТЕМЫ RSA.....41

### Лабораторная работа №4

ИЗУЧЕНИЕ АЛГОРИТМА ДИФФИ-ХЕЛЛМАНА ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ.....54

### Лабораторная работа №5

ИЗУЧЕНИЕ АЛГОРИТМА ИДЕНТИФИКАЦИИ ГИЛЛОУ-КУИСКУОТЕРА.....84

### Лабораторная работа №6

ИЗУЧЕНИЕ АЛГОРИТМА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ RSA.....113

### Приложение 1

ПОСЛЕДОВАТЕЛЬНОСТЬ ПРОСТЫХ ЧИСЕЛ.....136