

Задачи и методические указания для практических по дисциплине « Средства обеспечения информационной безопасности в сетях передачи данных» /Сост. к.т.н., доцент А.В.Крыжановский, к.т.н., доцент Н.В.Киреева, к.т.н., доцент В.В.Пугин – Самара, 2008-61 с.,ил.

Приведены краткие теоретические сведения, тексты задач и решения к ним по основным аспектам информационной безопасности: симметричные и асимметричные криптосистемы, политика безопасности, электронная цифровая подпись, распределение ключей в компьютерной сети, протоколы идентификации и аутентификации.

Методические разработки утверждены на заседании кафедры ПДС 12.03.2008 г. протокол № 5.

Редактор – д.т.н., профессор Б.Я.Лихтциндер

Рецензент – д.т.н., профессор В.Г. Карташевский

## Содержание

### Занятие 1

Традиционные симметричные криптосистемы.....	4
1.1 Основные понятия и определения.....	4
1.2 Шифры перестановки.....	6
1.2.1 Шифрующие таблицы.....	6
1.2.2 Шифрование магическими квадратами.....	9
1.3 Шифры простой замены.....	11
1.3.1 Шифрование на основе квадрата Полибия.....	11
1.3.2 Система шифрования Цезаря.....	12
1.3.3 Система Цезаря с ключевым словом.....	13
1.3.4 Шифрующие таблицы Трисемуса.....	14
1.3.5 Биграммный шифр Плейфейра.....	16

### Занятие 2

Методы шифрования.....	18
2.1 Метод перестановок на основе маршрутов Гамильона.....	18
2.2 Аналитические методы шифрования.....	20

### Занятие 3

Асимметричная криптосистема RSA. Расширенный алгоритм

Евклида.....	23
--------------	----

### Занятие 4

Политика безопасности.....	28
----------------------------	----

### Занятие 5

Алгоритмы электронной цифровой подписи.....	32
5.1 Алгоритм цифровой подписи RSA.....	32
5.2 Алгоритм цифровой подписи Эль Гамала (EGSA).....	35

### Занятие 6

Распределение ключей в компьютерной сети.....40

    6.1 Алгоритм открытого распределения ключей Диффи-Хеллмана.....40

Занятие 7

    Протоколы идентификации с нулевой передачей знаний.....44

        7.1 Упрощенная схема идентификации с нулевой передачей знаний.....44

        7.2 Параллельная схема идентификации с нулевой  
        передачей зна-  
        ний.....46

    Приложение.....50

