

Методические указания и контрольные задания по дисциплине
«Средства обеспечения информационной безопасности в телекоммуникационных системах» /Сост.к.т.н., доцент А.В.Крыжановский, к.т.н., доцент Н.В.Киреева, к.т.н., доцент В.В.Пугин – Самара, 2008-50 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 7.02.2008 г. протокол № 2.

Редактор – д.т.н., профессор Б.Я.Лихтциндер
Рецензент – д.т.н., профессор В.Г. Карташевский

Содержание

Исходные данные.....	4
Задание 1 Традиционные симметричные криптосистемы.....	7
1.1 Основные понятия и определения.....	7
1.2 Шифры перестановки.....	8
1.2.1 Шифрующие таблицы.....	8
1.2.2 Шифрование магическими квадратами.....	11
1.3 Шифры простой замены.....	12
1.3.1 Шифрование на основе квадрата Полибия.....	12
1.3.2 Система шифрования Цезаря.....	13
1.3.3 Система Цезаря с ключевым словом.....	13
1.3.4 Шифрующие таблицы Трисемуса.....	14
1.3.5 Биграммный шифр Плейфейра.....	15
Задание 2 Методы шифрования.....	17
2.1 Метод перестановок на основе маршрутов Гамильтона.....	17
2.2 Аналитические методы шифрования.....	18
Задание 3 Асимметричная криптосистема RSA. Расширенный алгоритм Евклида.....	22
Задание 4 Алгоритмы электронной цифровой подписи.....	27
4.1 Алгоритм цифровой подписи Эль Гамала (EGSA).....	27
Занятие 5 Распределение ключей в компьютерной сети.....	31
5.1 Алгоритм открытого распределения ключей Диффи-Хеллмана.....	31
Приложение.....	35