2642

Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«Липецкий государственный технический университет»

Кафедра автоматизированных систем управления

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к проведению лабораторных работ по курсу
«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

В.А. Алексеев

Липецк 2009

Электронный архив библиотеки ЛГТУ

2642

Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«Липецкий государственный технический университет»

Кафедра автоматизированных систем управления

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к проведению лабораторных работ по курсу
«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

В.А. Алексеев

Утверждаю к печати		Проректор по учебной работе
Объем	1,0 печ.л.	Ю.П. Качановский
Тираж	100 экз.	«___» _____________ 2010 г.

Липецк 2010

ŋqdqɏeɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè

2642

Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«Липецкий государственный технический университет»

Кафедра автоматизированных систем управления

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к проведению лабораторных работ по курсу
«МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

В.А. Алексеев

Липецк 2009

УДК 681.3.067(07)

А-471

Рецензент: к.т.н. П.А. Домашнев

Алексеев, В.А.

А471 Методы и средства криптографической защиты информации [Текст] / Методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / В.А. Алексеев, Липецк: ЛГТУ, 2009. – 16 с.

Методические указания посвящены криптографическим методам и средствам защиты информации. Цель приведенных лабораторных работ состоит в изучении существа симметричных и асимметричных криптосистем, в получении студентами практических навыков программирования криптографических средств защиты информации в прикладных программных приложениях.

Предназначены для студентов направления 230100.62 «Информатика и вычислительная техника», специальностей 230102.65 «Автоматизированные системы обработки информации и управления» и 010503.65 «Математическое обеспечение и администрирование информационных систем».

Табл. 2. Рис. 3. Библиогр.: 7 назв.

Лабораторная работа №2

Реализация симметричной криптосистемы

Цель работы

Изучить принципы работы и классификацию симметричных криптосистем, особенности современных алгоритмов, получить практические навыки программирования симметричных криптографических алгоритмов.

Теоретические сведения

Современные криптосистемы по количеству используемых в операциях шифрования и дешифрования ключей делятся на:

1. Симметричные – в общем случае в таких системах ключ дешифрования может быть легко получен из ключа шифрования и наоборот. Обычно для шифрования и дешифрования используют один и тот же ключ, который называют секретным.

2. Асимметричные (с открытым ключом) – для шифрования и дешифрования используются различные ключи, которые не могут быть получены один из другого за разумное время.

Симметричные криптосистемы обладают высокой производительностью и используются для шифрования больших объемов данных при передаче по сети или при организации криптографически защищенного хранения данных.

Обозначим: M – передаваемое сообщение (открытый текст), K – секретный ключ. Тогда $C = E_K[M]$ - шифрованное сообщение, полученное при криптопреобразовании исходного сообщения $E[]$ с ключом K. Операция дешифрования $D[]$ является обратной операции шифрования: $D_K[C] = D_K[E_K[M]] = M$.

Симметричные криптосистемы основаны на 2-х базовых операциях преобразования исходного (открытого) текста: подстановке и перестановке. Подстановка состоит в замене символов исходного сообщения символами шифра по определенному правилу (правило может быть достаточно сложным). Перестановка – в «перемешивании» символов исходного сообщения. В