А.М. Голиков

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
ОСНОВЫ КРИПТОГРАФИИ
КРИПТОГРАФИЯ

Методические указания по практическим занятиям и семинарам по дисциплинам «Основы криптографии», «Криптографические методы и средства защиты информации» и «Криптография»

2008

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИСТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

УТВЕРЖДАЮ
Заведующий кафедрой РТС

_____ Г.С. Шарыгин
“____” ___ 2008 г.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
ОСНОВЫ КРИПТОГРАФИИ
КРИПТОГРАФИЯ

Методические указания по практическим занятиям и семинарам по дисциплинам «Основы криптографии», «Криптографические методы и средства защиты информации» и «Криптография»

Разработчик

Доцент каф. РТС, к.т.н.

_____ А.М. Голиков

“____” _____ 2008г.

2008

Рекомендовано к изданию кафедрой радиотехнических систем Томского государственного университета систем управления и радиоэлектроники

Голиков А.М. Криптографические методы и средства защиты информации.
Основы криптографии. Криптография. Методические указания по выполнению курсовой работы. - Томск: Том. гос. ун-т систем управления и радиоэлектроники, 2008. – 7 с.

Приводятся указания по выполнению курсовой работы по дисциплине «Криптографические методы и средства защиты информации» для студентов специальности 090106 - Информационная безопасность телекоммуникационных систем и 210403 – Защищенные системы связи.

СОДЕРЖАНИЕ

1. ЦЕЛЬ ПРОВЕДЕНИЯ ЗАНЯТИЙ

Практические занятия направлены на закрепление и расширение знаний, полученных на лекциях.

Практические занятия направлены на изучение основ криптографии.

Предусмотрен тестовый контроль полученных знаний в объеме, предусмотренном рейтинговой раскладкой для данной дисциплины. Тестовый контроль проводится в виде контрольных работ по изучаемым темам.

2. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины студенты (слушатели) должны

<u>иметь представление:</u>

• об основных этапах исторического развития криптографии;

• о методах и критериях оценки надежности защиты информации;

<u>знать и уметь использовать:</u>

• основные понятия и термины криптографии;

• основные характеристики открытых ("осмысленных") текстов;

• основные классы шифров и их характеристики;

<u>владеть:</u>

• методами анализа простейших шифров (простая замена, перестановка);

3. СОДЕРЖАНИЕ ЗАНЯТИЙ

Занятие №1.

Тема. Практическое использование шифров перестановки (2 часа).

Содержание. Маршрутные перестановки. Одиночная перестановка по ключу. Двойная перестановка. Магические квадраты.

Форма проведения. Решение задач.

Тематический план.

Самоподготовка по литературе по проведению практических занятий
- 2 часа.
Вводная информация по теме - 30 минут. Решение задач - 40 минут. Тестовая контрольная - 10 минут.

Занятие №2.

Тема. Практическое использование шифров простой замены (4 часа).
Содержание. Шифр Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Биграммный шифр Плейфера.
Форма проведения. Решение задач.
Тематический план.
Самоподготовка по литературе по проведению практических занятий
- 4 часа.
Вводная информация по теме - 60 минут. Решение задач - 80 минут. Тестовая контрольная - 20 минут.

Занятие №3.

Тема. Практическое использование шифров сложной замены (2 часа). Содержание. Шифр Виженера. Двойной квадрат Уитстона.

Биграммный шифр Порта.
Форма проведения. Решение задач. Тематический план.
Самоподготовка по литературе по проведению практических занятий
- 2 часа.
Вводная информация по теме - 30 минут. Решение задач - 40 минут. Тестовая контрольная - 10 минут.

Занятие №4.

Тема. Арифметические основы криптографии (4 часа).
Содержание. Взаимно простые числа. Наибольший общий делитель. Алгоритм Евклида. Расширенный алгоритм Евклида. Наименьшее общее кратное. Свойства сравнений. Функция Эйлера. Теорема Эйлера. Модулярная арифметика. Китайская теорема об остатках.
Форма проведения. Решение задач.
Тематический план.
Самоподготовка по литературе по проведению практических занятий

- 4 часа.

Вводная информация по теме - 60 минут. Решение задач - 80 минут. Тестовая контрольная - 20 минут.

Занятие №5.

Тема. Алгебраические основы криптографии (3 часа). Содержание. Поля. Сложение, умножение, деление в поле Галуа. Группы. Кольца.

Форма проведения. Решение задач. Тематический план.

Самоподготовка по литературе по проведению практических занятий

- 2 часа.

Вводная информация по теме - 45 минут.

Решение задач - 60 минут. Тестовая контрольная - 15 минут.

Занятие №6.

Тема. Блочные и поточные шифры (3 часа). Содержание. ГОСТ 28147-89. DES. AES. RC4.

Форма проведения. Решение задач. Тематический план.

Самоподготовка по литературе по проведению практических занятий - 2 часа.

Вводная информация по теме - 45 минут. Решение задач - 60 минут. Тестовая контрольная - 15 минут.

4. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии - М.: Гелиос АРВ, 2001. - 480 с, ил.

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных сетях - М.: Радио и связь, 2001. - 376 с: ил.

3. Введение в криптографию / Под ред. В.В. Ященко. - 3-е изд., доп. - М: МЦНМО: "ЧеРо", 2000. - 288 с.

4. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография - СПб.: Лань, 2000. 224 с, ил.

5. В.Жельников. Криптография от папируса до компьютера. М.: ABF, 1996.

6. Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н. Поточные шифры. - М: КУДИЦ-ОБРАЗ, 2003. - 336 с.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: ТРИУМФ, 2002 - 816 с.

8. К.Шеннон. Работы по теории информации и кибернетике.-М.:ИЛ, 1963.

9. А.Саломаа. Криптография с открытым ключом.-М., 1995.

10. У.Диффи, М.Э.Хеллман. Защищенность и имитостойкость. Введение в криптографию. ТИИЭР, т. 67, N 3, 1979.

11.Рябко Б.Я., Фионов А.Н.. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005. – 229 с.