МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»
(ТУСУР)

Кафедра автоматизированных систем управления

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Методические указания по выполнению лабораторных работ по дисциплине «Методы и средства защиты компьютерной информации» направления подготовки 010500.62 "Прикладная математика и информатика" (квалификация (степень) "бакалавр")

2012

Горитов А.Н.
Информационная безопасность: методические указания по выполнению лабораторных работ по дисциплине «Методы и средства защиты компьютерной информации» направления подготовки 010500.62 "Прикладная математика и информатика" (квалификация (степень) "бакалавр") / А.Н. Горитов. – Томск: ТУСУР, 2012. – 6 с.

Методические указания разработаны в соответствии с решением кафедры автоматизированных систем управления

Составитель: д.т.н., профессор каф. АСУ А.Н. Горитов

Методические указания утверждены на заседании кафедры автоматизированных систем управлениям 28 июня 2012 г., протокол № 15

СОДЕРЖАНИЕ

1. Цель и задачи дисциплины

1.1 Цели преподавания дисциплины

Дисциплина «Методы и средства защиты компьютерной информации» имеет своей целью освоение методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2 Задачи изучения дисциплины

Для достижения поставленной цели выделяются задачи курса:

- изучение теоретических основ защиты информации в компьютерных системах;
- практическая апробация доступных технологий и средств защиты компьютерной информации;
- самостоятельная аналитическая работа с целью изучения и поиска решения актуальных задач компьютерной и сетевой безопасности.

В результате изучения дисциплины студент должен:

Знать: правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов.

Уметь: применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях.

Владеть: методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.

1.3 Перечень дисциплин и разделов (тем), необходимых студентам для изучения данной дисциплины

Дисциплина «Методы и средства защиты компьютерной информации» входит в цикл специальных дисциплин (СД.Ф.1).

Настоящей дисциплине должно предшествовать изучение дисциплин:

«Информатика», «Алгебра и геометрия», «Математический анализ», «Дискретная математика».

Знания и навыки, полученные при изучении этой дисциплины, используются при изучении дисциплин: «Сети ЭВМ и телекоммуникации» и подготовки выпускной квалификационной работе.

2. Лабораторный практикум

Лабораторный практикум дисциплины "Методы и средства защиты компьютерной информации" позволяет получить практические навыки использования методов защиты информации.

2.1 Порядок выполнения лабораторных работ

1) изучить теоретический материал по теме лабораторной работы;
2) составить программу на одном из алгоритмических языков программирования для заданного варианта задания;
3) выполнить отладку составленной программы и показать преподавателю;
4) составить и защитить отчет по лабораторной работе.

2.2 Лабораторные работы

1. Блочное симметричное шифрование
2. Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей
3. Асимметричное шифрование
4. Электронная цифровая подпись (ЭЦП)
5. Практическое применение криптографии с открытым ключом. Пакет PGP
6. Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI

2.3 Контрольные вопросы

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.
13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.
17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.
30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. Опишите алгоритм RSA.
35. Опишите алгоритм цифровой подписи RSA.
36. Опишите алгоритм цифровой подписи Эль-Гамаля.
37. Опишите алгоритм цифровой подписи DSA (DSS).

38. Опишите алгоритм цифровой подписи ГОСТ Р3410-94.
39. Что такое сертификат открытого ключа?
40. Чем отличается аутентификация от идентификации?
41. Что такое авторизация?
42. Принципы использования многоразовых паролей?
43. Как получают одноразовые пароли?
44. Как используются сертификаты при аутентификации пользователей?

3. Учебно-методические материалы по дисциплине

3.1 Основная литература

1. Основы защиты информации: Учебное пособие. В 3 ч. / А.А.Шелупанов и др. – Томск: В-Спектр, 2007. (81 экз.)

2. Бацула А. П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (25 экз.)

3.2 Дополнительная литература

1. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2005. – 144 с. (50 экз.)

2. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов и др. – М.: Горячая линия – Телеком, 2006. – 544 с. (50 экз.)

3. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред.: С. А. Клейменов. – М.: Academia, 2006. – 330 с. (30 экз.)

4. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М.: Academia, 2006. - 253 с. (50 экз.)

5. Алферов А. П. и др. Основы криптографии: Учебное пособие для вузов. 3-е изд., испр. и доп. - М.: Гелиос АРВ, 2005. – 479 с. (30 экз.)

6. Смарт Н. Криптография: учебник для вузов: пер. с англ. / пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М.: Техносфера, 2005. – 525 с. (10 экз.)

3.3 Учебно-методические пособия

1. Спицын В. Г., Столярова Н. А. Защита информации и информационная безопасность: Учебное пособие. – Томск: ТМЦДО, 2006. – 196 с. (15 экз.)

2. Бойченко И.В. Информационная безопасность: лабораторный практикум / И.В. Бойченко, П.В. Кориков. – Томск: ТУСУР, 2007. – 65 с. (48 экз.)