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

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методические указания по выполнению лабораторных работ по дисциплине «Информационная безопасность» направления подготовки 010400.62 "Прикладная математика и информатика" (квалификация (степень) "бакалавр")

Томск-2011

Горитов А.Н.
Информационная безопасность: методические указания по выполнению лабораторных работ по дисциплине «Информационная безопасность» направления подготовки 010400.62 "Прикладная математика и информатика" (квалификация (степень) "бакалавр") / А.Н. Горитов. – Томск: ТУСУР, 2011. – 7 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 30 августа 2011 г., протокол № 1

СОДЕРЖАНИЕ

1. Цель и задачи дисциплины....4
2. Методы и форма организации обучения....4
3. Место дисциплины в структуре ООП....5
4. Лабораторный практикум....5
4.1 Порядок выполнения лабораторных работ....5
4.2 Лабораторные работы....5
4.3 Контрольные вопросы....5
5. Учебно-методические материалы по дисциплине....6
5.1 Основная литература....6
5.2 Дополнительная литература....6
5.3 Учебно-методические пособия....7

1. Цель и задачи дисциплины

Цель дисциплины - ознакомить студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации при проектировании информационных систем (ИС).

Задачи изучения дисциплины состоят в том, что в результате ее изучения студенты должны:

– **иметь** представление об использовании основных положений теории информационной безопасности в различных областях ИС и иметь представление о направлении развития и перспективах защиты информации;

– **знать** правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;

– **уметь** применять методы защиты компьютерной информации при проектировании ИС в различных предметных областях.

2. Методы и форма организации обучения

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

общекультурные компетенции (ОК):

1) способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (**ОК-5**);

2) способность работать в коллективе и использовать нормативные правовые документы в своей деятельности (**ОК-13**).

профессиональные компетенции (ПК):

1) способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии (**ПК-2**);

2) способностью понимать и применять в исследовательской и прикладной деятельности современный математический аппарат (**ПК-3**);

3) способностью решать задачи производственной и технологической деятельности на профессиональном уровне, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования (**ПК-9**);

4) способностью применять в профессиональной деятельности современные языки программирования и языки баз знаний, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии (**ПК-10**).

Для успешного освоения дисциплины применяются различные образовательные технологии, которые обеспечивают достижение планируемых результатов обучения согласно основной образовательной программе, с учетом требований к объему занятий в интерактивной форме.

Интерактивные формы обучения, которые используются в данном курсе, включают: «Работа в команде» и «Поисковый метод».

Для контроля освоения компетенций используются следующие формы контроля: защита лабораторных работ, опрос по изучаемым разделам дисциплины, тесты.

3. Место дисциплины в структуре ООП

Дисциплина «Информационная безопасность» относится к числу дисциплин вариативной части профессионального цикла ООП. «Информационная безопасность» как учебная дисциплина в системе подготовки бакалавров по направлению 010400 связана с дисциплинами учебного плана: «Алгебра и геометрия», «Математическая логика и теория алгоритмов», «Организация и функционирование ЭВМ», «Архитектура компьютеров», «Языки и методы программирования».

Знания и навыки, полученные при изучении этой дисциплины, используются в последующей дисциплине профессионального цикла: «Программное обеспечение ЭВМ и сетей» и при подготовке выпускной квалификационной работы.

4. Лабораторный практикум

Лабораторный практикум дисциплины "Информационная безопасность" позволяет получить практические навыки использования методов защиты информации.

4.1 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.

4.2 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

4.3 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?

5. Учебно-методические материалы по дисциплине

5.1 Основная 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.)

5.2 Дополнительная литература

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.)

5.3 Учебно-методические пособия

7. Спицын В. Г., Столярова Н. А. Защита информации и информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2002. – 158 с. (40 экз.)

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