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 самостоятельной и индивидуальной работе студентов по дисциплине «Методы и средства защиты компьютерной информации» специальности 230105 "Программное обеспечение вычислительной техники и автоматизированных систем"

2012

Горитов А.Н.
Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов по дисциплине «Методы и средства защиты компьютерной информации» 230105 "Программное обеспечение вычислительной техники и автоматизированных систем" / А.Н. Горитов. – Томск: ТУСУР, 2012. – 8 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

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

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:

Иметь представление: об использовании основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перспективах защиты информации.

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.

2. Методы и форма организации обучения

Процесс изучения дисциплины «Методы и средства защиты компьютерной информации» направлен на формирование у учащихся понимания важности информации в современном мире, ущербе, который может принести искажение или уничтожение информации и о методах ее защиты.

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

3. Место дисциплины в структуре ООП

Дисциплина «Методы и средства защиты компьютерной информации» относится к числу дисциплин вариативной части профессионального цикла. «Информационная безопасность» как учебная дисциплина в системе подготовки бакалавров по направлению 080801.65 связана с дисциплинами учебного плана: «Математика», «Дискретная математика», «Информатика и программирование», «Основы алгоритмизации и языки программирования», «Вычислительные системы, сети и телекоммуникации», «Операционные системы».

Знания и навыки, полученные при изучении этой дисциплины, используются в дисциплине профессионального цикла: «Проектирование информационных систем» и выпу-

скной квалификационной работе.

4. Содержание дисциплины

4.1 Теоретический материал

Тема 1 Законодательные и правовые основы защиты компьютерной информации информационных технологий

Законодательство Российской Федерации в области информационной безопасности. Информация как объект юридической и физической защиты. Государственные информационные ресурсы. Защита государственной тайны как особого вида защищаемой информации. Защита конфиденциальной информации, в том числе интеллектуальной собственности и коммерческой тайны. Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.

Тема 2 Проблемы защиты информации в АСОИУ

основные определения по защите информации. Основные задачи защиты информации. Классификация и общий анализ угроз безопасности информации. Классификация каналов несанкционированного получения информации. Оценка уязвимости информации.

Тема 3 Теоретические основы компьютерной безопасности

Архитектура электронных систем обработки данных; формальные модели; модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем; стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем; особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; концепция защищенного ядра; методы верификации; защищенные домены; применение иерархического метода для построения защищенной операционной системы; исследование корректности систем защиты; методология обследования и проектирования защиты; модель политики контроля целостности.

Тема 4 Современные криптосистемы для защиты компьютерной информации

Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернома.

Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернома.

Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. Аддитивные поточные шифры. Методы генерации криптографически качественных псевдослучайных последовательностей. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.

Асимметричные системы шифрования (системы с открытым ключом). Понятия однонаправленной функции и однонаправленной функции с лазейкой.

Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля.

Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости.

Тема 5 Электронная цифровая подпись: анализ и переспективы

Общие сведения об электронной цифровой подписи (ЭЦП). Алгоритм ЭЦП в симметричной криптосистеме. Алгоритм ЭЦП в асимметричной криптосистеме. Проблема обмена открытыми ключами при ЭЦП. Сложные математические задачи и алгоритмы ЭЦП с открытыми ключами. Алгоритм DSA. Алгоритм ГОСТ Р34.10–94. Стандарт ЭЦП Р34.10–2001.

Тема 6 Математические основы криптографических методов

Основные понятия и определения теории информации (количество информации, энтропия сообщения, норма языка и т.п.). Практическое применение теории информации, путаница и диффузия. Элементы теории сложности проблем. Классы сложности проблем. Теория чисел (арифметика вычетов, малая теорема Ферма, теорема Эйлера, разложение числа на простые сомножители). Генерация простого числа. Дискретные логарифмы в конечном поле.

Тема 7 Методы идентификации и проверки подлинности пользователей компьютерных систем

Основные понятия и концепции. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователя. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись.

Тема 8 Методы защиты программ от излучения и разрушающих программных воздействий (программных закладок и вирусов)

Классификация способов защиты. Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.

Тема 9 Защита компьютерных сетей от удаленных атак

Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.

Программно-аппаратные средства защиты ПЭВМ и сетей; методы средства ограничения доступа к компонентам сети; методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям: методы и средства хранения ключевой информации; защита программ от изучения; защита от разрушающих программных воздействий; защита от изменений и контроль целостности.

Тема 10 Комплексная защита процесса обработки информации в компьютерных системах

Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Постановка задач оптимизации систем защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. Перспективы КЗИ: защищенные информационные технологии.

4.2 Лабораторные работы

1. Изучение ППП систем криптографической защиты информации, классическая

криптография и распределение ключей.

2. Практическое применение криптографии с открытым ключом. Пакет PGP.

3. Электронная цифровая подпись (ЭЦП)

4. Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI

4.3 Темы для самостоятельного изучения

1. Блочный шифр BLOWFISH.
2. Блочный шифр RC5.
3. Блочный шифр RC6.
4. Блочный шифр IDEA.

4.4 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.)