

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 к практическим занятиям
по дисциплине "Информационная безопасность" направления подготовки
010400.62 "Прикладная математика и информатика"
(квалификация (степень) "бакалавр")

Томск-2011

Горитов А.Н.

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

© ТУСУР, каф. АСУ, 2011

© Горитов А.Н. 2011

СОДЕРЖАНИЕ

| | |
|--|---|
| 1. Цель и задачи дисциплины..... | 4 |
| 2. Методы и форма организации обучения..... | 4 |
| 3. Место дисциплины в структуре ООП | 5 |
| 4. Практические занятия | 5 |
| 4.1 Федеральные законы в области информационной безопасности | 5 |
| 4.2 Политики безопасности. Основные модели политики безопасности | 5 |
| 4.3 Симметричные криптографические методы | 5 |
| 4.4 Поточные шифры. Криптографические хеш-функции | 6 |
| 4.5 Математические основы криптографических методов | 6 |
| 4.6 Криптография с открытым ключом | 6 |
| 4.7 Электронная цифровая подпись | 7 |
| 4.8 Методы идентификации и проверки подлинности пользователей | 7 |
| 5. Список литературы | 7 |
| 5.1 Основная | 7 |
| 5.2 Дополнительная | 7 |
| 5.3 Учебно-методические пособия | 8 |

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) способностью 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. Практические занятия

4.1 Федеральные законы в области информационной безопасности

Основы российского законодательства в сфере защиты информации: закон об информации, информационных технологиях и защите информации; закон о государственной тайне; закон о защите персональных данных; закон об электронной цифровой подписи. Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации.

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.

4.2 Политики безопасности. Основные модели политики безопасности

Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.

Контрольные вопросы

1. Что такое «политика безопасности»?
2. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
3. В каких случаях применяются модели безопасности?
4. Основные модели политик безопасности?

4.3 Симметричные криптографические методы

Симметричные системы шифрования (системы с секретным ключом): поточные шифры, блочные шифры. 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, ско-

рость работы на различных платформах, режимы пользования.

Контрольные вопросы

1. Принципы, используемые для повышения стойкости шифра?
2. Приведите схему и объясните принцип работы блочного шифра.
3. Дайте характеристику шифра DES.
4. Дайте характеристику шифра ГОСТ 28147-89.
5. Перечислите основные различия между DES и ГОСТ 28147-89.
6. Что такое – режим применения блочного шифра?

4.4 Поточные шифры. Криптографические хеш-функции

Принципы поточного шифрования. Алгоритм RC4.

Функция хеширования MD5. Основные сведения о функциях хеширования SHA-1, RIPEMD-160, SHA-256, SHA-512. Хеш-функции на базе блочных шифров.

Контрольные вопросы

1. Чем отличается поточное и блочное шифрование.
2. Дайте характеристику шифра RC4.
3. Основные свойства криптографических хеш-функций.
4. Принципы работы хеш-функции.
5. Особенности построения хеш-функции на базе блочного шифра.

4.5 Математические основы криптографических методов

Основные понятия и определения теории информации. Основные теоремы теории чисел (арифметика вычетов, малая теорема Ферма, теорема Эйлера, разложение числа на простые сомножители). Наибольший общий делитель. Алгоритм Евклида. Обобщенный алгоритм Евклида. Возведение в степень по модулю. Дискретные логарифмы в конечном поле. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Элементы теории сложности проблем. Классы сложности проблем.

Контрольные вопросы

1. Опишите операцию приведения по модулю.
2. Какими свойствами обладает операция приведения по модулю?
3. Приведите определение простого числа.
4. Какие два числа называются взаимно простыми?
5. Определите понятие обратного значения по модулю.
6. Сформулируйте малую теорему Ферма.
7. Дайте определение функции Эйлера.
8. Сформулируйте теорему Эйлера.
9. Перечислите свойства простых чисел.

4.6 Криптография с открытым ключом

Основные способы использования алгоритмов с открытым ключом. Шифр Шамира. Шифр Эль-Гамала. Алгоритм RSA. Вопросы стойкости. Задача распределения ключей. Метод Диффи-Хеллмана

Контрольные вопросы

1. Чем отличается криптография с открытым ключом от симметричных шифров?

2. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
3. Опишите алгоритм Шамира.
4. Опишите алгоритм Эль-Гамала.
5. Опишите алгоритм RSA.

4.7 Электронная цифровая подпись

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.

Контрольные вопросы

1. Опишите алгоритм цифровой подписи RSA.
2. Опишите алгоритм цифровой подписи Эль-Гамала.
3. Опишите алгоритм цифровой подписи DSA (DSS).
4. Опишите алгоритм цифровой подписи ГОСТ Р3410-94.
5. Что такое сертификат открытого ключа?

4.8 Методы идентификации и проверки подлинности пользователей

Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации, использующие пароли и PIN-коды: на основе многозначных паролей, на основе однозначных паролей, на основе сертификатов. Строгая аутентификация, основанная: на симметричных алгоритмах, на асимметричных алгоритмах, на однонаправленных хеш-функциях. Биометрическая аутентификация пользователя.

Контрольные вопросы

1. Чем отличается аутентификация от идентификации?
2. Что такое авторизация?
3. Принципы использования многозначных паролей?
4. Как получают однозначные пароли?
5. Как используются сертификаты при аутентификации пользователей?

5. Список литературы

5.1 Основная

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

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.)