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

ЗАЩИТА ИНФОРМАЦИИ

Методические указания по самостоятельной и индивидуальной работе студентов по дисциплине «Защита информации» направления подготовки 230100.62 "Информатика и вычислительная техника"
(квалификация (степень) "бакалавр")

Томск-2011

Горитов А.Н.
Защита информации: методические указания по самостоятельной и индивидуальной работе студентов по дисциплине «Защита информации» направления подготовки 230100.62 "Информатика и вычислительная техника" (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 управлениям 30 августа 2011 г., протокол № 1

СОДЕРЖАНИЕ

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 «Защита информации» направлен на формирование следующих компетенций:

общекультурные компетенции (ОК):

1) способностью понимать сущность и значение информации в развитии современного информационного общества; владеть основными методами, способами и средствами получения, хранения, переработки информации **(ОК-11);**

2) способностью работать с информацией в глобальных компьютерных системах **(ОК-13)**.

профессионально-специализированные компетенции (ПСК):

1) Осуществлять отладку программ **(ПСК-11);**

2) Использовать методы и средства разработки тестовых сценариев и тестового кода **(ПСК-14).**

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 «Защита информации» относится к числу дисциплин базовой части профессионального цикла. «Защита информации» как учебная дисциплина в системе подготовки бакалавров по направлению 230100.62 связана с дисциплинами учебного плана: «Математика», «Дискретная математика», «Программирование».

Знания и навыки, полученные при изучении этой дисциплины, используются при выполнении бакалаврской квалификационной работы.

4. Содержание дисциплины

4.1 Теоретический материал

Тема 1. Введение в информационную безопасность.

Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации, связь проблем ИБ с развитием информационных технологий (ИТ) и процессами глобализации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Обзор и параметры классификации угроз безопасности информации. Принципы защиты информации. Классы средств защиты информации. Государственная стратегия обеспечения ИБ в России.

Тема 2. Законодательные и правовые основы защиты компьютерной информации.

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.

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

Тема 3. Математические методы и модели в задачах защиты информации.

Основные понятия криптографии. 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. Основные понятия и определения. Классификация симметричных систем шифрования: поточные шифры, блочные шифры.

Блочные шифры. Сеть Фейштеля. Алгоритм TEA. Алгоритм DES. Алгоритм ГОСТ 28147-89. Сравнение алгоритмов DES и ГОСТ 28147-89. Модификация алгоритма DES: тройной DES с двумя и тремя ключами. Алгоритм AES. Режимы выполнения алгоритмов шифрования: EBC, CBC, CFB и OFB.

Потоковые шифры. Алгоритм RC4.

Тема 4. Математические основы криптографических методов.

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.

Тема 5. Криптография с открытым ключом.

Криптография с открытым ключом. Основные способы использования алгоритмов с открытым ключом. Шифр Шамира. Шифр Эль-Гамаля. Алгоритм RSA. Вопросы стойкости.

Задача распределения ключей. Метод Диффи-Хеллмана.

Криптографические хеш-функции. Функция хеширования MD5. Основные сведения

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

Электронная цифровая подпись. Общие сведения об электронной цифровой подписи (ЭЦП). Основные процедуры цифровой подписи. Алгоритм ЭЦП RSA. Алгоритм ЭЦП Эль-Гамаля. Алгоритм ЭЦП DSA. Алгоритм ГОСТ Р34.10–94. Стандарт ЭЦП Р34.10–2001. Вопросы стойкости ЭЦП. Сертификат открытого ключа.

Тема 6. Методы идентификации и аутентификации пользователей.

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

Тема 7. Межсетевые экраны и VPN сети.

Межсетевые экраны. Режим функционирования межсетевых экранов и их основные компоненты. Экранирующий маршрутизатор. Шлюзы сетевого уровня. Прикладной шлюз. Основные схемы сетевой защиты на базе межсетевых экранов. Формирование политики межсетевого взаимодействия. Персональные межсетевые экраны.

Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей (VPN). Основные понятия и функции. Классификация VPN сетей. Основные варианты архитектуры VPN. Достоинства применения технологии VPN.

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 8. Защита компьютерных систем от вредоносных программ.

Вредоносные программы и их классификация. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.

Тема 9. Комплексная защита информации.

Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Постановка задачи оптимизации системы 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 Практические занятия

1. Принципы защиты информации. Методы оценки уязвимости информации.
2. Федеральное законодательство о защите информации.
3. Государственные стандарты и руководящие документы.
4. Современные приложения криптографии.
5. Математические основы криптографических методов.
6. Методы идентификации и аутентификации.
7. Основные технологии построения защищенных информационных систем.
8. Место информационной безопасности информационной системы в национальной безопасности страны. Концепция информационной безопасности.

9. Комплексная система обеспечения информационной безопасности.

4.3 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

4.4 Темы для самостоятельного изучения

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

4.5 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.)