МИНОБРНАУКИ РОССИИ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ИНФОРМАТИКИ

«Утверждаю»:
Декан
_____ Сущенко С.П.
«17» января 2011 г.

Программа учебной дисциплины
МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки
230700 Прикладная информатика

Наименование магистерской программы
Системы корпоративного управления

Квалификация (степень) выпускника
Магистр

Форма обучения
Очная

Томск
2010

1. Цели освоения дисциплины

Целями освоения дисциплины «Математические основы защиты информации и информационной безопасности» являются углубление фундаментальных знаний в области современных информационных технологий, в частности, формирование основ знаний по криптографии, протоколам и принципам кодирования секретным и открытым ключом, изучение важнейших алгоритмов в этой области, овладение средствами разработки и исследования таких алгоритмов.

2. Место дисциплины в структуре ООП магистратуры

Данная учебная дисциплина входит в раздел «М.1. Общенаучный цикл. Вариативная часть» ООП по направлению подготовки 230700 «Прикладная информатика».

Для изучения дисциплины необходимы компетенции, сформированные у обучающихся в результате освоения дисциплин «дискретная математика», «основы программирования», «алгоритмы и анализ сложности», «теория вероятностей и математическая статистика» ООП подготовки бакалавра, а также дисциплины «Теория информации и кодирование» ООП подготовки магистра.

Для того чтобы приступить к изучению дисциплины «Математические основы защиты информации и информационной безопасности», студент должен обладать следующими знаниями и умениями:

- знать основы компьютерных технологий и языков программирования;
- иметь твердые знания основных структур данных в программировании;
- знать основы теория вероятностей и математической статистики;
- знать основные понятия теории информации, принципы разработки эффективных алгоритмов кодирования;
- уметь строить алгоритмы решения поставленных задач;
- уметь разрабатывать программы для ЭВМ;
- уметь выполнять анализ сложности алгоритмов и программ.

Данная учебная дисциплина входит в набор дисциплин профессионального цикла, ориентированных на изучение методов и моделей разработки программного обеспечения. Данная дисциплина предваряет производственную практику по профилю «Управление проектами по разработке программного обеспечения».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Математические основы защиты информации и информационной безопасности»

Данная дисциплина способствует формированию следующих компетенций, предусмотренных ФГОС-3 по направлению подготовки ВПО 230700 «Прикладная информатика»:

- «способность на практике применять новые научные принципы и методы исследований (ПК-3)» в части математических методов защиты информации;
- «способность формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок (ПК-6)»;
- «способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций (ПК-9)»;
- «способность анализировать и оптимизировать прикладные и информационные процессы (ПК-13)»;
- «способность применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС (ПК-15)» в части математических методов защиты информации;

- «способность проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС (ПК-17)»;

- «способность использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций (ПК-26)»;

- «способность организовывать работу команды разработчиков программного обеспечения, умение осуществлять кооперацию со смежниками, инвесторами, заинтересованными сторонами (СК-8)» в части организовывать работу команды разработчиков программного обеспечения;

- «умение осуществлять выбор технических и экономических моделей сопровождения и эволюции программного обеспечения (СК-10)».

В результате освоения дисциплины обучающийся должен:

- Знать: основные понятия криптографии, криптографические протоколы, принципы разработки эффективных алгоритмов кодирования секретным и открытым ключом и электронного подписывания данных, методы исследования этих алгоритмов.

- Уметь: разрабатывать и реализовывать в виде программ эффективные алгоритмы, доказывать корректность алгоритмов, анализировать временную и пространственную сложность алгоритмов криптографии.

- Владеть: способами разработки эффективных алгоритмов криптографии, методами доказательства корректности алгоритмов, методами исследования временной и пространственной сложности алгоритмов криптографии.

4. Структура и содержание дисциплины «Математические основы защиты информации и информационной безопасности»

Общая трудоемкость дисциплины составляет 3 зачетных единиqs, 108 часов, из них лекции – 32 часов, лабораторные работы – 32 часа, самостоятельная работа – 44 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
				Лекции	Лабораторные работы	Самостоятельные работы	
1	Основные понятия и протоколы.	2	1-5	8	–	6	Письменный контроль по теории.
2	Методы симметричного шифрования	2	6-10	8	12	10	Письменный контроль по теории. Контроль реализации программ
3	Потоковые шифры	2	11-15	8	8	10	Письменный контроль по теории. Контроль реализации программ
4	Шифрование открытым ключом и электронное подписывание	2	16-20	8	12	10	Письменный контроль по теории. Контроль реализации программ
5	Промежуточная	2	21			8	Экзамен

	аттестация						

1. Основные понятия и протоколы

Предмет криптографии. Терминология в криптографии. Принципы обеспечения конфиденциальности в информационных системах. Протоколы секретного шифрования симметричным ключом. Простейшие ранние алгоритмы секретного шифрования. Методы вскрытия: метод грубой силы, частотный анализ, «встреча посередине». Влияние длины ключа на надежность метода. Проблема распространения ключей. Шифрование открытым ключом. Проблема достоверности открытого ключа. Протоколы электронной подписи.

2. Методы симметричного шифрования

Простые блочные методы шифрования. Кодирование и декодирование текста подстановочным и перестановочным кодом. Надежность симметричных методов шифрования. Требования к устойчивости метода. Операция XOR и кодирование одноразовым блокнотом. Кодирование и декодирование текста комбинированным кодом, образованным из подстановочного, перестановочного кодов, а также сдвига и операции XOR. Алгоритм шифрования DES.

3. Потоковые шифры

Понятие потокового шифра. Использование истинно случайных последовательностей для кодирования и декодирования текста. Линейные конгруэнтные генераторы. Сдвиговый регистр с линейной обратной связью. Алгоритм генерации случайного потока символов RS4 с переменной длиной ключа.

4. Шифрование открытым ключом и электронное подписывание

Проблема распространения ключей, метод Диффи-Хелмана. Метод RSA. Проблема генерации простых чисел. Методы разложения чисел на множители. Генерация длинных простых чисел с помощью малой теоремы Ферма. Вычисление НОД для длинных чисел. Генерация длинных ключей для метода RSA. Комбинированное применение метода RSA и симметричного алгоритма шифрования для шифрования открытым ключом. Однонаправленные функции, их вычисление. Комбинированное применение метода RSA и однонаправленной функции для электронного подписывания. Возможные уязвимости метода RSA и способы их устранения.

Лабораторный практикум

Все лабораторные работы выполняются в виде разработки архитектуры программ, реализации на одном из языков программирования (например, Паскаль, Делфи, Си) и их тестирования на специально подготовленных тестах.

1 Реализация алгоритмов кодирования и декодирования текста подстановочным кодом.

2. Реализация алгоритмов кодирования и декодирования текста перестановочным кодом.

3. Реализация алгоритмов кодирования и декодирования текста комбинированным кодом, образованным из подстановочного, перестановочного, а также сдвига и операции XOR.

4. Реализация алгоритма шифрования DES.

5. Реализация алгоритма генерации случайного потока символов RS4 и реализация с его помощью кодирования и декодирования текста.

6. Реализация алгоритма разложения чисел на множители (для коротких чисел).

7. Реализация алгоритма разложения чисел на множители (для длинных чисел).

8. Реализация алгоритма генерации длинных простых чисел с помощью малой теоремы Ферма.

9. Реализация алгоритма вычисления НОД для длинных чисел.

10. Реализация алгоритма генерации длинных ключей для метода RSA.

11. Полная реализация алгоритма RSA для шифрования открытым ключом и электронного подписывания.

5. Образовательные технологии

В ходе преподавания дисциплины используются следующие образовательные технологии:

- лекции в сопровождении иллюстративного материала в форме презентаций,
- лабораторные занятия в компьютерном классе,
- самостоятельная работа студентов,
- активные и интерактивные формы занятий:
- лекции-консультации,
- лекции с разбором конкретных ситуаций,
- самостоятельное проектирование и программирование алгоритмов кодирования,
- мастер-классы экспертов.

Удельный вес занятий, проводимых в интерактивных формах, составляет не менее 30% аудиторных занятий.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Виды самостоятельной работы студентов:

1) повторение и самостоятельное изучение основного теоретического материала и ознакомление с дополнительной литературой, интернет-ресурсами;

2) выполнение индивидуальных проектов, разработка программ, реализующих отдельные алгоритмы в соответствии с заданием преподавателя.

В качестве учебно-методического обеспечения самостоятельной работы используется основная и дополнительная литература по предмету, Интернет-ресурсы, материал лекций, указания, выданные преподавателем при проведении лабораторных работ.

Темы индивидуальных лабораторных заданий имеют общий шаблон: разработать и реализовать программу, выполняющую некоторый алгоритм по заданию преподавателя. При этом некоторые из программ (требующие наибольших временных затрат от студентов) должны выполняться небольшими группами студентов (по 2-3 человека) с самостоятельным планированием и распределением работы внутри группы.

Пример задания для самостоятельной работы:

Реализовать алгоритмы шифрования и дешифрования произвольного файла перестановочным кодом.

Задание на СРС:

1. Спроектировать программу шифрования, на вход которой вначале поступает секретный ключ, затем имя файла, который требуется зашифровать. Программа на основе ключа должна сгенерировать перестановку, а по ней зашифровать входной файл. На выходе программы – зашифрованный файл.

2. Спроектировать программу дешифрования, на вход которой вначале поступает секретный ключ, затем имя файла, который требуется дешифровать. Программа на основе ключа должна сгенерировать обратную перестановку, а по ней дешифровать входной файл. На выходе программы – дешифрованный файл.

3. Запрограммировать протестировать и отладить программы шифрования и дешифрования. Для этого подготовить тестовые файлы с различным содержимым.

Контроль самостоятельной работы студентов.
Текущий контроль – еженедельный контроль по реализации отдельных алгоритмов.

Промежуточная аттестация по итогам освоения дисциплины включает письменные опросы на 5,10,15 неделях семестра, зачет по теоретическим вопросам и по практической реализации отдельных алгоритмов по окончанию курса. Общая оценка составляется на основе результатов контроля во время контрольных недель и заключительного зачета.

Вопросы и задания для промежуточной аттестации:

1. Принципы обеспечения конфиденциальности в информационных системах.
2. Протоколы секретного шифрования симметричным ключом.
3. Простые методы шифрования. Кодирование и декодирование текста подстановочным и перестановочным кодом.
4. Вскрытие методов шифрования. Требования к устойчивости метода.
5. Операция XOR и кодирование одноразовым блокнотом.
6. Кодирование и декодирование текста комбинированным кодом, образованным из подстановочного, перестановочного кодов, а также сдвига и операции XOR.
7. Алгоритм шифрования DES.
8. Алгоритм генерации случайного потока символов RS4 и его применение для кодирования и декодирования текста.
9. Сдвиговый регистр с линейной обратной связью.
10. Однонаправленные функции, их вычисление.
11. Методы разложения чисел на множители.
12. Генерация длинных простых чисел с помощью малой теоремы Ферма.
13. Вычисление НОД для длинных чисел.
14. Генерация длинных ключей для метода RSA.
15. Комбинированное применение метода RSA и симметричного алгоритма шифрования для шифрования открытым ключом.
16. Комбинированное применение метода RSA и однонаправленной функции для электронного подписывания.
17. Возможные уязвимости метода RSA и способы их устранения.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

	Список основной литературы:				Элек-трон-ный вари-ант
	Автор	Название	Изд-во	Год издания	
1.	Шнайер Б.	Прикладная криптография: Пер. с англ.	М.: Триумф	2002	есть
2	Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.	Основы криптографии.	М.: Гелиос АРВ	2005	

3	Кнут Д.	Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы: Пер. с англ.	М.: Мир	1977	
4	Шнайер Б., Фергюссон Н.	Практическая криптография: Пер. с англ.	М.: Вильямс	2005	
5	Грушо А.А., Применко Э.А., Тимонина Е.Е.	Теоретические основы компьютерной безопасности: Учебное пособие.	М.: Академия	2009	
	Список дополнительной литературы				
	Автор	Название	Изд-во	Год	
1	Галатенко В.А.	Стандарты информационной безопасности. Курс лекций: Учебное пособие.	М.: Интернет-университет информационных технологий	2004	
2	Нечаев В.	Элементы криптографии: Основы теории защиты информации: Учебное пособие для вузов	М.: Высшая школа	1999	

в) программное обеспечение и Интернет-ресурсы:
1. Транслятор с языка Си или Паскаль в операционной системе Windows или Linux.
2. Программа для проведения презентаций – Power Point или аналогичная.
3. Интернет-браузер – Microsoft Explorer или аналогичный.

8. Материально-техническое обеспечение дисциплины

Лекционная аудитория должна быть оборудована проекционным оборудованием: компьютером и проектором, а также программными средствами для их функционирования.

Компьютерный класс, компьютеры должны быть объединены в локальную сеть с выходом в Интернет.

Программа составлена в соответствии с требованиями ФГОС-3 ВПО с учетом рекомендаций и ПрООП ВПО по направлению подготовки «Прикладная информатика».

Автор – д.т.н., профессор кафедры теоретических основ информатики Ю.Л. Костюк
Рецензент – к.т.н, доцент, зав. кафедрой теоретических основ информатики А.Л. Фукс

Программа одобрена на заседании кафедры теоретических основ информатики ТГУ
от 21.12.2010 , протокол № 08/10