КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Специальности 090301,090302,090303

Основные сведения

- Цикл – профессиональных дисциплин
- Позиция в примерном УП –

  8,9 семестры (090301),

  7,8 семестры (090302),

  6,7 семестры (090303),
- Объем – 6(090301), 5(090302), 4(090303) зач.ед.
- Форма контроля – в примерном учебном плане: зачет, экзамен

Цель

Целью изучения дисциплины «Криптографические методы защиты информации» является освоение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи

Задачи дисциплины – дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов синтеза и анализа шифров;
- математических методов, используемых в оценке стойкости криптосистем.

Межпредметные связи.

Изучение дисциплины базируется на знаниях, умениях и навыках по дисциплинам :

- Алгебре
- Теория вероятностей и математической статистике
- Математической логике и теории алгоритмов
- Дискретной математике
- Теории информации
- Информатики
- Основам информационной безопасности
- Теоретико-числовым методам в криптографии

Межпредметные связи. Обеспечивает дисциплины:

- Специальность 090301
  - «Криптографические протоколы»
  - «Основы построения защищенных компьютерных сетей»
  - «Основы построения защищенных баз данных»
- Специальность 090302
  - «Проектирование защищённых ТКС»
  - «Информационная безопасность ТКС»
- Специальность 090303
  - «Управление информационной безопасностью»

Знать

- основные криптографические примитивы и их использование в решении основных задач защиты информации;
- математические модели шифров;
- требования к шифрам и основные характеристики шифров;
- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;
- базовые криптографические протоколы;

Уметь

- корректно применять симметричные и асимметричные криптографические алгоритмы;
- эффективно использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах;
- применять математические методы описания и исследования криптосистем;
- оценивать криптографическую стойкость шифров

Владеть

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками математического моделирования в криптографии;
- навыками использования ПЭВМ в анализе простейших шифров;
- навыками работы с научно-технической литературой в области криптографии

Разделы дисциплины

- Введение в криптографию
- Основные классы шифров и их свойства
- Надёжность шифров
- Методы синтеза и анализа криптографических алгоритмов с секретным ключом
- Методы синтеза и анализа криптографических алгоритмов с открытым ключом
- Хеш-функции и их криптографические приложения

Раздел 1. Введение в криптографию

- Тема 1.1. Исторический обзор. Открытые сообщения и их характеристики
- Тема 1.2. Основные задачи и понятия криптографии

Раздел 2. Основные классы шифров и их свойства

- Тема 2.1. Шифры перестановки
- Тема 2.2. Поточные шифры замены
- Тема 2.3. Блочные шифры замены

Раздел 3. Надёжность шифров

- Тема 3.1. Основы теории К.Шеннона
- Тема 3.2. Вопросы имитозащиты
- Тема 3.3. Помехоустойчивость шифров

Раздел 4. Методы синтеза и анализа криптографических алгоритмов с секретным ключом

- Тема 4.1. Принципы построения криптографических алгоритмов
- Тема 4.2. Типовые генераторы псевдослучайных последовательностей
- Тема 4.3. Генераторы на основе линейных регистров сдвига
- Тема 4.4. Методы усложнения ЛРП
- Тема 4.5. Методы анализа криптографических алгоритмов

Раздел 5. Методы синтеза и анализа криптографических алгоритмов с открытым ключом

- Тема 5.1. Системы шифрования с открытым ключом.
- Тема 5.2. Алгоритмы цифровых подписей.
- Тема 5.3. Алгоритмы идентификации
- Тема 5.4. Алгоритмы распределения ключей

Раздел 6. Хэш-функции и их криптографические приложения

- Тема 6.1. Хеш-функции и аутентификация сообщений
- Тема 6.2. Конструкции MAC на основе симметричного шифрования

Литература

- Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
- Словарь криптографических терминов. Под ред. Погорелова Б.А., Сачкова В.Н. М.: МЦНМО, 2006.
- Черёмушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. М.: Издательский дом «Академия», 2009.
- Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.
- Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. М.: КУДИЦ-ОБРАЗ, 2002.
- Фомичев В.М. Дискретная математика и криптология. М.: “ДИАЛОГ· МИФИ”, 2003.
- Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.

Литература

- Маховенко Е.Б., Ростовцев А.Г. Теоретическая криптография. Спб: АНО НПО «Профессионал», 2004.
- Черёмушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.
- Зубов А.Ю., Овчинников В.Н., Зязин А.В., Рамоданов С.В. Олимпиады по математике и криптографии. М.: МЦНМО, 2006.
- Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005.
- Зубов А.Ю. Математики кодов аутентификации // М.:Гелиос АРВ, 2007.
- Коблиц Н. Курс теории чисел и криптографии. М.:ТВП, 2001.
- Мао В. Современная криптография. Теория и практика. М.: Издательский дом “Вильямс”, 2005.

Спасибо за внимание!

Объем и виды учебной работы

Вид учебной работы	Всего часов	Семестры	
		7	8
Аудиторные занятия (всего)	78	38	40
В том числе:	-	-	-
Лекции	46	18	28
Практические занятия (ПЗ)	32	20	12
Семинары (С)	-	-	-
Лабораторные работы (ЛР)	-	-	-
Самостоятельная работа (всего)	64	34	30
В том числе:	-	-	-
Курсовой проект (работа)	-	-	-
Расчетно-графические работы	-	-	-
Реферат	-	-	-
Другие виды самостоятельной работы	-	-	-
Вид промежуточной аттестации (зачет, экзамен)	38	2	36