Белорусский государственный университет

УТВЕРЖДАЮ
Декан гуманитарного факультета
_____ В.Е. Гурский
(подпись)
29.05.14г.
(дата утверждения)
Регистрационный № УД-2014-1684/р.

Криптографические методы защиты информации

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности:
1-31 03 07 Прикладная информатика (по направлениям)

Факультет Гуманитарный

Кафедра Информационных технологий

Курс (курсы) 3

Семестр (семестры) 5

Лекции 34

Экзамен 5

Практические (семинарские) занятия

Зачет

Лабораторные занятия 34

Курсовая работа (проект)

Аудиторных часов по учебной дисциплине 68

Форма получения высшего образования очная

Всего часов по учебной дисциплине 140

Составил(а) О.В. Дубровина

2014 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Основной целью дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике. Содержание курса направлено на ознакомление студентов с математическими основами теории шифрования, историей развития криптографии, включая современные тенденции, основными алгоритмами шифрования и криптографическими протоколами обмена информацией.

В результате изучения дисциплины обучаемый должен

знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- методы построения и блочных и поточных криптосистем, функций хэширования, криптосистем с открыты ключом и систем электронной цифровой подписи;

уметь:

- применять полученные знания для создания защищенных систем и
- проводить простейший анализ стойкости алгоритмов;
- применять хэш-функциии и электронную цифровую подпись при обмене коммерческой информацией;
- уметь пользоваться научно-технической литературой в области криптографии.

Объем дисциплины (часов):
всего (7 семестр)
34 - лекционные занятия
34 – практические занятия

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

№ п/п	Наименование разделов, тем	Количество часов				
		Аудиторные				Самост. работа
		Лекции	Практ., семинары	Лаб. занятия	КСР	
1.	Проблемы информационной безопасности. Общие принципы построения криптографических алгоритмов	2		4		4
2.	Симметричные криптосистемы. Алгоритмы блочного шифрования	6		6		8
3.	Симметричные криптосистемы. Алгоритмы поточного шифрования	4		4		6
4.	Асимметричные криптосистемы	6		6		4
5.	Хэш-функции	6		4		4
6.	Электронная цифровая подпись	4		4		4
7.	Криптографические протоколы	2		2		2
8.	Алгоритмы шифрования данных на основе эллиптических кривых	2		2		4
9.	Стеганографические методы защиты информации	2		2		4

Учебно-методическая карта

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		Лекции	Практические (семинарские) занятия	Лабораторные занятия	Контролируемая самостоятельная работа студента			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1.	Проблемы информационной безопасности. Введение. Современное состояние, перспектива и ретроспектива. Информационные системы, средства, каналы, сети и среды. Основные понятия и определения информационной безопасности.	1				Практические работы выполняются на базе сетевых компьютерных классов	[1,3]	
2.	Общие принципы построения криптографических алгоритмов Основные задачи защиты информации. Классификация алгоритмов. Классификация угроз. Стойкость алгоритмов. Концепция теоретической и практической стойкости К. Шеннона. Простейшие алгоритмы.	1		4			[1,2]	отчет
3.	Симметричные криптосистемы. Алгоритмы блочного шифрования Принципы построения блочных шифров. Схема Фейстеля. Примеры блочных алгоритмов (DES, ГОСТ 28147-89, IDEA, Rijndael). Режимы использования блочных шифров. Методы анализа алгоритмов блочного шифрования, рекомендации по использованию	6		6			[1,2]	отчет

4.	Симметричные криптосистемы. Алгоритмы поточного шифрования Принципы построения поточных шифросистем. Линейные регистры сдвига. Усложнение реккурентных последовательностей. Синхронизация поточных шифросистем. Шифры, не распространяющие ошибки. Примеры поточных шифров (A5, SEAL). Методы анализа поточных шифров.	4		4			[1,2]	отчет
5.	Асимметричные криптосистемы Основные принципы. Арифметика больших чисел. Кольца вычетов. Шифросистемы RSA, Эль-Гамаля. Стойкость	6		6			[1,2]	отчет
6.	Хэш-функции Общие сведения. Типы функций хэширования. Возможные атаки на функции хэширования. СТБ 1176.1-99. Целостность данных. Требования к хэш-функциям. Стойкость	6		4	2		[2,3]	отчет
7.	Электронная цифровая подпись Общие положения. ЦП на основе алгоритмов с открытыми ключами. Цифровая подпись Эль-Гамаля. Схема RSA. Примеры (DSS-федеральный стандарт США, ГОСТ-Р 34.10-94, СТБ 1176.2-99). Оноразовые ЦП.	4		4	2		[2,3]	отчет
8.	Криптографические протоколы Общие сведения. Формальные методы анализа, BAN-логика. Протоколы аутентификации. Протоколы распределения ключей	2		2			[1,2]	отчет
9.	Алгоритмы шифрования данных на основе эллиптических кривых Математические понятия. Аналог алгоритма Диффи-Хеллмана обмена ключами	2		2			[5]	отчет
10.	Стеганографические методы защиты информации Математические понятия. Скрытие данных методом стеганографии.	2		2			[4]	отчет

ИНФОРМАЦИОННАЯ ЧАСТЬ

Литература

Основная

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
3. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. – Мн: БГУ, 2003.
4. Конахович Г.Ф., Пузыренко А.Ю. Цифровая стеганография. Теория и практика. Киев: МК-Пресс, 2006.
5. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. М.,Изд-во РГСУ, 2004.

Дополнительная

1. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Лань, 2000.
2. Иванов М А. Криптография. Криптографические методы защиты информации в компьютерных системах и сетях. – М: Кудиц-образ, 2001
3. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа, 1999.
4. Ященко В.В. Введение в криптографию. – М.: МЦНМО-ЧеРо, 1999.
5. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М: ДМК, 2000.
6. Баричев С., Гончаров В., Серов Р. Основы современной криптографии. М.: Горячая линия-Телеком, 2011.
7. Смарт Н. Криптография. М.: Техносфера, 2006.