Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

«Утверждаю»
Председатель Ученого совета,
Ректор КарГТУ, академик НАН РК
_____ Газалиев А.М.
«____» _____ 2013г.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

Дисциплина Krip 3213 «Криптология»

Модуль МО 19 «Математическое обеспечение»

Специальность 5В100200 – «Системы информационной безопасности»

Факультет информационных технологий

Кафедра – «Информационные технологии и безопасность»

2013

Предисловие

Программа обучения по дисциплине для студента (syllabus) разработана: старшим преподавателем кафедры ИТБ Мурых Е.Л.

Обсуждена на заседании кафедры «Информационные технологии и безопасность»

Протокол № _____ от «____»_____2013г.
Зав. кафедрой _____ Коккоз М.М. «____»_____2013г.

Одобрена учебно-методическим советом факультета информационных технологий

Протокол № _____ от «_____»_____2013г.
Председатель _____Д.У. Капжаппарова. «____»_____ 2013г.

Сведения о преподавателе и контактная информация

Мурых Елена Львовна, старший преподаватель

Кафедра «Информационные технологии и безопасность» находится в главном корпусе КарГТУ (Б.Мира, 56), аудитория 429, контактный телефон 56-75-98 доб. 1028.

Трудоемкость дисциплины

Семестр	Количество кредитов	ECTS	Вид занятий					Количество часов СРС	Общее количество часов	Форма контроля
			количество контактных часов			количество часов СРСП	всего часов			
			лекции	практические занятия	лабораторные занятия					
5	3	5	15	15	15	45	90	30	135	КР

Характеристика дисциплины

Дисциплина «Криптология» является компонентой по выбору цикла базовых дисциплин.

Цель дисциплины

Дисциплина «Криптология» ставит целью изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи дисциплины

Задачи дисциплины следующие:

– дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов разработки шифров; математических методов, используемых в криптографии.

В результате изучения данной дисциплины студенты должны:

иметь представление:

- о месте криптографической защиты в системе информационной безопасности;

- о современных алгоритмах шифрования и криптографических протоколах обмена информацией;

знать:

– основные задачи и понятия криптографии;

– требования к шифрам и основные характеристики шифров;

– частотные характеристики открытых текстов и их применение к анализу простейших симметричных криптосистем;

– типовые поточные и блочные шифры, а также асимметричные криптосистемы;

– основные криптографические протоколы системы шифрования с открытыми ключами;

уметь:

– применять математические методы описания и исследования криптосистем;

– оценивать криптографическую стойкость шифров;

приобрести практические навыки:

– использования типовых криптографических алгоритмов;

– математического моделирования в криптографии.

Пререквизиты

Для изучения данной дисциплины необходимо усвоение следующих дисциплин: «Информатика», «Математика», «Алгоритмические языки и программирование».

Постреквизиты

Знания, полученные при изучении дисциплины «Криптография» используются при освоении следующих дисциплин: «Проектирование систем защиты информации».

Тематический план дисциплины

Наименование раздела, (темы)	Трудоемкость по видам занятий, ч.				
	лекции	практические	лабораторные	СРСП	СРС
1	2	3	4	5	6
1. Угрозы безопасности в компьютерных системах. Защита информации.	1			3	3
2. Основные понятия и задачи криптологии.	1			3	3
3. Математические основы криптографии.	2	4	2	10	10
4. Криптография. Моноалфавитные, полиалфавитные шифры. Шифры замены и перестановки.	1	1	2	6	6
5. Симметричные криптографические системы.	2	2	2	6	6
6. Несимметричные криптографические системы.	2	2	3	8	8
7. Криптографический протокол. Криптосистема RSA.	2	2	2	3	3
8. Блочные шифры. Поточные шифры.	1			10	10

9. Электронная цифровая подпись (ЭЦП). Хеш-функция.	1	2	2	3	3
10. Криптоанализ. Атака на шифр, частотный анализ. Стойкость шифра. Абсолютно стойкий шифр.	2	2	2	3	3
ИТОГО:	15	15	15	45	45

Перечень практических (семинарских) занятий

1. Математические основы криптографии
2. Моноалфавитные, полиалфавитные шифры. Шифры замены и перестановки.
3. Симметричные криптографические системы.
4. Несимметричные криптографические системы
5. Криптосистема RSA.
6. Хеш-функция
7. Атака на шифр, частотный анализ.

Перечень лабораторных занятий

Лабораторная работа № 1 Изучение основ криптографии.

Лабораторная работа № 2 Разработка программы для шифрования методами замены и перестановки.

Лабораторная работа № 3 Разработка программы для шифрования методами симметричных систем шифрования.

Лабораторная работа № 4 Разработка программы для шифрования методами асимметричных систем шифрования

Лабораторная работа № 5 Разработка программы постановки электронной цифровой подписи по алгоритму RSA.

Лабораторная работа № 6 Разработка программы для выработки Hash – функции.

Лабораторная работа № 7 Изучения методов криптоанализа.

Тематика курсовых проектов (работ)

Разработка программного обеспечения «Криптосистемы с открытым ключом».

Разработка программного обеспечения «Симметричные криптосистемы».

Разработка программного обеспечения «Цифровая подпись».

Темы контрольных заданий для СРС

Рассмотреть принципы защиты хранимых паролей от взлома.

2. Рассмотреть принципы защиты хранимых паролей в сети.

3. Разработать генератор случайных чисел на основе регистров сдвига по одной из моделей.

4. Рассмотреть методику и составить программы для работы с модульной арифметикой для получения модуля большого числа разрядной сетки машины.

5. Рассмотреть модель умножения больших чисел модульной арифметики с помощью одного из методов ускорения.

6. Рассмотреть модель возведения в степень больших чисел модульной арифметики с помощью одного из методов ускорения.

7. Рассмотреть реализацию линейного конгруэнтного генератора на больших числах (свыше разрядной сетки машины).

8. Рассмотреть реализацию отдельных блоков ГОСТ 28147-89 для 32 битовой машины.

9. Составит модель блока шифрования в режиме простой замены на основании разработанных ранее процедур.

10. Рассмотреть модель получения Hash в стандарте SHA.

Критерии оценки знаний студентов

Экзаменационная оценка по дисциплине определяется как сумма максимальных показателей успеваемости по рубежным контролям (до 60%) и итоговой аттестации (курсовой проект) (до 40%) и составляет значение до 100%.

Политика и процедуры

При изучении дисциплины «Криптология» прошу соблюдать следующие правила:

1. Не опаздывать на занятия.

2. Не пропускать занятия без уважительной причины, в случае болезни предоставлять справку, в других случаях – объяснительную записку.

3. Иметь все необходимое для проведения занятия.

5. Активно участвовать в учебном процессе.

6. В срок выполнять необходимую для освоения дисциплины самостоятельную работу.

7. Быть терпимыми, открытыми, откровенными и доброжелательными к сокурсникам и преподавателям.

График выполнения и сдачи заданий по дисциплине

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи	Баллы
1	2	3	4	5	6	7
Посещаемость	Контроль посещаемости		В течении семестра	текущий	еженедельно	1
Отчет по СРС	Углубление знаний по теме «Угрозы безопасности в компьютерных системах. Защита информа-	[1], [2], [3] [5]	2 недели	текущий	2 неделя	1

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи	Баллы
	ции»					
Защита лабораторной работы №1	Изучение основ криптографии	[1], [2], [3], [5], [12],[11]	1 неделя недели	текущий	2 неделя	2
Защита лабораторной работы №2	Разработка программы для шифрования методами замены и перестановки	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	3 неделя	2
Отчет по СРС	Углубление знаний по теме «Основные понятия и задачи криптологии.»	[1], [2], [3] [5]	2 недели	текущий	3 неделя	1
Защита лабораторной работы №3	Разработка программы для шифрования методами симметричных систем шифрования	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	4 неделя	3
Отчет по СРС	Углубление знаний по теме «Математические основы криптографии.»	[1], [2], [3], [5], [6],[10]	2 недели	текущий	5 неделя	1
Защита лабораторной работы №4	Разработка программы для шифрования методами асимметричных систем шифрования	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	5 неделя	3
Отчет по СРС	Углубление знаний по теме «Криптография. Моноалфавитные, полиалфавитные шифры. Шифры замены и	[1], [2], [3], [5], [6],[10]	2 недели	текущий	6 неделя	1

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи	Баллы
	перестановки.					
Защита лабораторной работы №5	Разработка программы постановки электронной цифровой подписи по алгоритму RSA.	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	6 неделя	3
Отчёт по практическим занятиям	Проверка практических и теоретических навыков	Вся основная и дополнительная литература	1 неделя	текущий	6 неделя	4
Письменный опрос	Проверка теоретических знаний и практических навыков	[1-19] конспекты лекций	1 контактный час	рубежный	7 неделя	10
Отчет по СРС	Углубление знаний по теме «Симметричные криптографические системы.»	[1], [2], [3], [5], [6],[10]	2 недели	текущий	7 неделя	1
Защита лабораторной работы №6	Разработка программы для выработки Hash – функции.	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	7 неделя	2
Отчет по СРС	Углубление знаний по теме «Несимметричные криптографические системы.»	[1], [2], [3], [10], [14],	2 недели	текущий	9 неделя	1
Отчет по СРС	Углубление знаний по теме «Криптографический протокол. Криптосистема RSA»	[1], [2], [3], [10],	2 недели	текущий	10 неделя	1

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи	Баллы
Отчет по СРС	Углубление знаний по теме «Блочные шифры. Поточные шифры.»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	12 неделя	1
Отчет по СРС	Углубление знаний по теме «Электронная цифровая подпись (ЭЦП). Хеш-функция..»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	13 неделя	1
Отчет по СРС	Углубление знаний по теме «Криптоанализ. Атака на шифр, частотный анализ. Стойкость шифра. Абсолютно стойкий шифр.»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	14 неделя	1
Защита лабораторной работы №7	Изучения методов криптоанализа..	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	14 неделя	3
Отчёт по практическим занятиям	Проверка практических и теоретических навыков	Вся основная и дополнительная литература	1 неделя	текущий	14 неделя	4
Письменный опрос	Проверка теоретических знаний и практических навыков	[1-19] конспекты лекций	1 контактный час	рубежный	14 неделя	10
Курсовой проект	Проверка усвоения дисциплины	[1-19] конспекты лекций	3 часа	Итоговый	В период сессии	40
Итого						100

Список основной литературы

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: Учеб. Пособие. - М.: Академия, 2009. - 412 с.
2. Арутюнов В.В. Защита информации: Учебно-методическое пособие. - М.: Либерея-Бибинформ, 2010. - 56 с.
3. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: учеб. пособие. - Владивосток: Изд-во ДВГТУ, 2010. - 318 с.
4. Бузов Г. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. - М.: Горячая Линия - Телеком,-2010, - 240 с.
5. Шаньгин В. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2010, - 544 с.
6. Шаньгин Ф. Комплексная защита информации в корпоративных системах. Учебное пособие. - М.: Форум, 2010, - 592 с.
7. Щербаков В., Ермаков С., Безопасность беспроводных сетей. Стандарт IEEE 802.11. - М.: РадиоСофт, 2010, - 256 с.
8. Хореев П.Б. Методы и средства защиты информации в компьютерных системах. - М.: Академия, 2007. 256 с.
9. Белов Е. Б. и др. Основы информационной безопасности: Учеб. пособие. М.: Горячая линия-Телеком, 2006. - 544 с.
10. Ярочкин В.И. Информационная безопасность: Учебник. - М.: Академический проект, Трикста, 2005. - 544 с.
11. Садердинов А.А. Информационная безопасность предприятия: Учеб. Пособие,- М.: Дашков и К, 2005. - 336 с.
12. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. - М.: Горячая линия-Телеком, 2004. - 280с.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: ТРИУМФ, 2003. - 400 с.
14. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - 452 с.

Список дополнительной литературы

15. Проскурин В.Г. Защита программ и данных. - М.: Академия, 2011, - 208 с.
16. Касперский К. Фундаментальные основы хакерства (искусство дизассемблирования). - М.: Солон-Р, 2008. - 288 с.
17. Ященко В.В. Введение в криптографию. Новые математические дисциплины. - М.: МЦНМО Питер, 2001. - 287 с.
18. Хорев А. А. Способы и средства защиты информации. Учеб. пособие. -М.: МОРФ, 2000.-316 с.
19. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: Кудиц-образ, 2001.- 363 с

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

по дисциплине Krip 3213 «Криптология»

Модуль МО 19 «Математическое обеспечение»

Гос. изд. лиц. №50 от 31.03.04

Подписано к печати _____ 20__г. Формат 90х60/16 Тираж ____ экз.

Объем _____ уч. изд. л. Заказ №_____ Цена договорная .

100027 Издательство КарГТУ Караганда, Бульвар Мира, 56