Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

«Утверждаю»
Председатель Ученого совета,
Ректор КарГТУ, академик НАН РК
_____ Газалиев А.М.
«____» _____ 2015г.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

Дисциплина MOSZI 3214 «Математическое обеспечение систем защиты информации»

Модуль МО 19 «Математическое обеспечение»

Специальность 5В100200 – «Системы информационной безопасности»

Факультет информационных технологий

Кафедра – «Информационные технологии и безопасность»

2015

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 «____»_____2015г.
Зав. кафедрой _____ Коккоз М.М. «____»_____2015г.

Одобрена учебно-методическим советом факультета информационных технологий

Протокол № _____ от «_____»_____2015г.
Председатель _____Д.У. Капжаппарова. «____»_____ 2015г.

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		30	45	90	45	135	Э

Характеристика дисциплины

Дисциплина «Математическое обеспечение систем защиты информации» является вузовской компонентой цикла базовых дисциплин.

Цель дисциплины

Дисциплина «Математическое обеспечение систем защиты информации» ставит целью изучение и освоение математических методов криптологии, необходимые для описания математических моделей программно-реализуемых шифров и расчета их криптографических характеристик.

Задачи дисциплины

Задачи дисциплины следующие:

- изучение основных понятий и принципов теории информации;
- изучение основных понятий модулярной арифметики, алгоритмов, теорем, законов, функций теории чисел и полей, применяемых при криптографировании и шифровании информации,
- навыков, и знаний для реализации и использования их на практике;

В результате изучения данной дисциплины студенты должны:

иметь представление:

– о криптоалгоритмах и криптопротоколах, составляющих основу криптографической защиты информации в современных компьютерных сетях и их криптографические свойства;

знать:

- основные задачи криптографии, основные математические модели шифров для криптосистем;
- понятия однонаправленных функций и однонаправленных функций с секретом, понятия случайной и псевдослучайной последовательностей;
- методы построения больших простых чисел, методы распределения ключей;
- криптосистемы на базе эллиптических кривых;
- основные математические методы и алгоритмы, лежащие в основе краптосистем и криптоанализа;

уметь:

– использовать методы криптографии при решении задач в своей профессиональной деятельности;

- выявлять перспективные направления в области защиты информации и информационной безопасности;

приобрести практические навыки:

– использования математических основ криптографических методов защиты информации;

- применения математических основ криптографических методов создания электронной цифровой подписи (ЭЦП).

- поиска решений в области защиты информации и информационной безопасности.

Пререквизиты

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

Постреквизиты

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

Тематический план дисциплины

Наименование раздела, (темы)	Трудоемкость по видам занятий, ч.				
	Лекции	практические	Лабораторные	СРСП	СРС
1. Основы теории чисел.	1		4	3	3
2. Простые числа. Разложение чисел на множители.	1			3	3
3. Наибольший общий делитель. Алгоритм Евклида. Расширенный алгоритм Евклида. Алгоритм Евклида для многочленов	2		8	3	3
4. Теория сравнений	2			3	3
5. Первообразные корни	1			3	3
6. Дискретное логарифмирование.	1			6	6
7. Китайская теорема об остатках	1		2	3	3
8. Кольцо целых чисел	2		6	6	6
9. Вычислительные алгоритмы, алгоритмы получения псевдослучайные последовательностей.	1		6	6	6
10. Эллиптические кривые.	1			6	6
11. Арифметические операции над большими числами	1		4	3	3
ИТОГО:	15	-	30	45	45

Перечень лабораторных занятий

1. Исследование теории чисел.
2. Исследование алгоритма Евклида.
3. Китайская теорема об остатках
4. Кольцо целых чисел
5. Генерация псевдослучайных последовательностей.
6. Тестирование чисел на простоту и построение больших простых чисел.

Темы контрольных заданий для СРС

1. Основы теории чисел.
2. Простые числа. Разложение чисел на множители.
3. Наибольший общий делитель. Алгоритм Евклида.

4. Теория сравнений
5. Первообразные корни
6. Дискретное логарифмирование.
7. Китайская теорема об остатках
8. Кольцо целых чисел
9. Алгоритмы получения псевдослучайные последовательностей.
10. Эллиптические кривые.
11. Арифметические операции над большими числами

Критерии оценки знаний студентов

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

Политика и процедуры

При изучении дисциплины «Математическое обеспечение систем защиты информации» 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
Посещаемость	Контроль посещаемости		В течении семестра	текущий	еженедельно	1
Отчет по СРС	Углубление знаний по теме «Основы теории чисел»	[1], [2], [3] [5]	2 недели	текущий	2 неделя	1
Защита лабораторной работы №1	Исследование теории чисел.	[1], [2], [3], [5], [12],[11]	1 неделя недели	текущий	2 неделя	5
Отчет по СРС	Углубление знаний по теме «Простые числа. Разложение чисел на множители.»	[1], [2], [3] [5]	2 недели	текущий	3 неделя	1
Отчет по СРС	Углубление знаний по теме «Наибольший общий дели-	[1], [2], [3], [5], [6],[10]	2 недели	текущий	5 неделя	1

	тель. Алгоритм Евклида. Расширенный алгоритм Евклида. Алгоритм Евклида для многочленов»					
Защита лабораторной работы №2	Исследование алгоритма Евклида.	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	6 неделя	5
Отчет по СРС	Углубление знаний по теме «Теория сравнений»	[1], [2], [3], [5], [6],[10]	2 недели	текущий	6 неделя	1
Письменный опрос	Проверка теоретических знаний и практических навыков	[1-20] конспекты лекций	1 контактный час	рубежный	7 неделя	10
Отчет по СРС	Углубление знаний по теме «Первообразные корни»	[1], [2], [3], [5], [6],[10]	2 недели	текущий	7 неделя	1
Защита лабораторной работы №3	Китайская теорема об остатках	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	7 неделя	4
Отчет по СРС	Углубление знаний по теме «Дискретное логарифмирование.»	[1], [2], [3], [10], [14],	2 недели	текущий	9 неделя	1
Отчет по СРС	Углубление знаний по теме «Китайская теорема об остатках.»	[1], [2], [3], [10],	2 недели	текущий	10 неделя	1
Защита лабораторной работы №4	Кольцо целых чисел	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	11 неделя	4
Отчет по СРС	Углубление знаний по теме «Кольцо целых чисел»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	12 неделя	1
Защита лабораторной работы №5	Генерация псевдослучайных последовательностей	[1], [2], [8]	1 неделя	текущий	12 неделя	5
Отчет по СРС	Углубление знаний по теме «Вычислительные алгоритмы, алгоритмы получения псевдослучайные последователь-	[1], [2], [3], [5], [12],[11]	2 недели	текущий	13 неделя	1

	ностей»					
Отчет по СРС	Углубление знаний по теме «Эллиптические кривые»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	14 неделя	1
Письменный опрос	Проверка теоретических знаний и практических навыков	[1-20] конспекты лекций	1 контактный час	рубежный	14 неделя	10
Защита лабораторной работы №6	Тестирование чисел на простоту и построение больших простых чисел.	[1], [2], [3], [5], [7],[14]	1 неделя	текущий	15 неделя	5
Отчет по СРС	Углубление знаний по теме «Арифметические операции над большими числами»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	15 неделя	1
Итого по рубежным контролям						60
Экзамен	Проверка усвоения дисциплины	[1-20] конспекты лекций	3 часа	Итоговый	В период сессии	40
Итого						100

Список основной литературы

1. Ященко В.В. Введение в криптографию. Новые математические дисциплины. - М.: МЦНМО Питер, 2001. - 287 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: ТРИУМФ, 2003. - 400 с.

3. Кнут, Д.Э. Искусство программирования, т.2. Получисленные алгоритмы / Д.Э. Кнут - М.: Издательский дом «Вильямс», 2000. – 832 с.

4. Фергюсон Н., Шнайер Б. Практическая криптография – М.: Издательский дом Вильямс, 2005. – 424 с.

5. Коробейников А.Г. Математические основы криптологии : учебное пособие / А.Г. Коробейников, Ю.А. Гатчин. – СПб : СПб ГУ ИТМО, 2004. – 106 с.

6. Фомичев, В.М. Дискретная математика и криптология / В.М. Фомичев. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.

Список дополнительной литературы

7. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. - М.: Кудиц-образ, 2001.- 363 с

8. . Бабаш, А.В. Криптография. Под. ред. В.П. Шерстюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин – М.: СОЛОН-ПРЕСС, 2007. – 512 с.Декстер М. Joomla!: программирование. – М. : Вильямс, 2013. – 592 с.

9. Яковлев, А.В. Криптографическая защита информации : учебное пособие / А.В. Яковлев [и др.]. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.

10. Жданов О. Н. Криптоанализ классических шифров : лабораторный практикум / Жданов О. Н., Куденкова И. А. – Красноярск, 2008. – 107 с.

11. Аграновский, Александр Владимирович. Практическая криптография : Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.

12. Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.

13. Душин В.К. Теоретические основы информационных процессов и систем. Дашков и К, 2014. -348 с.

14. Лебедько Е.Г., Математические основы передачи информации. .-СПб: СПбГУ ИТМО, 2010. -93 с.

15. Кудряшов Б.Д. Теория информации. СПб: 2009, - 320 с.

16. Духин А.А. Теория информации. – М.: Гелиос АРВ. 2007.

17. Смарт Н. Криптография. – М.: Техносфера, 2005., - 528 с.

18. Алаферов А.П., Зубов А.Ю., Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002., - 480 с.

19. Василенко О.Н., Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко –Москва: Изд-во МЦНМО, 2003. – 326 с.

20. Смарт Н., Криптография/ Н. Смарт- Москва: Изд-во ТЕХНОСФЕРА, 2005. - 525 с.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

по дисциплине MOSZI 3214 «Математическое обеспечение систем защиты информации»

модуль МО 19 «Математическое обеспечение»

Гос. изд. лиц. №50 от 31.03.04

Подписано к печати _____ 20__г. Формат 90x60/16 Тираж ____ экз.

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

100027 Издательство КарГТУ Караганда, Бульвар Мира, 56