Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

«Утверждаю»
Председатель Ученого совета,
ректор, академик НАН РК
Газалиев А.М.

_____
«____» _____ 2015 г.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ МАГИСТРАНТА (SYLLABUS)

Дисциплина **K 5308** «Криптология»

Модуль **STZI 5** «Современные технологии защиты информации»

Специальность 6M070400– Вычислительная техника и программное обеспечение

Факультет «Информационных технологий»

Кафедра «Информационные технологии и безопасность»

2015

Предисловие

Программа обучения по дисциплине для магистранта – syllabus разработана: доцентом кафедры ИТБ к.т.н. Исагуловым С.Т.

Обсуждена на заседании кафедры «Информационные технологии и безопасность» (ИТБ)
Протокол № _____ от «____»_____2015г.
Зав. кафедрой_____Коккоз М.М. «____»_____2015г.

Одобрена учебно-методическим советом факультетом информационной технологии

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

Сведения о преподавателе и контактная информация

Исагулов С.Т., кафедры ИТБ, к.т.н., доцент.

Кафедра «Информационных технологий и безопасности» находится в главном корпусе КарГТУ (Караганда, Б.Мира 56), аудитория 429, контактный телефон 56-54-44, 56-75-98 (1028).

Трудоемкость дисциплины

Семестр	Количество кредитов/ECTS	Вид занятий					Количество часов СРМ	Общее количество часов	Форма контроля
		количество контактных часов			количество часов СРМП	аудит. часов			
		лекции	практические занятия	лабораторные занятия					
1	4/6	15	15	30	60	120	60	180	Экзамен

Характеристика дисциплины

Дисциплина «Криптология» входит в компонент по выбору цикла профилирующих дисциплин.

Данная дисциплина позволит магистрантам изучить теоретические основы построения и практического использования систем защиты информации в информационных системах, обучить магистрантов систематизированным представлениям о принципах, методах и средствах реализации защиты данных, приобретению практических навыков по защите информации в информационных системах необходимых для проектирования и эксплуатации.

Цель дисциплины

Дисциплина «Криптология» необходима как связующее звено между фундаментальными теоретическими знаниями, полученными магистрантами в ходе образовательного процесса и их эффективным использованием в практической деятельности.

Развивающая цель изучения направлена на формирование творческой личности, на развитие памяти, мышления, воображения, мотива, то есть на формирование профессиональной деятельности.

Практическая цель направлена на изучение теоретических основ построения и практического использования систем защиты информации в информационных системах. Обучение магистрантов систематизированным представлениям о принципах, методах и средствах реализации защиты данных, приобретению практических навыков по защите информации в информационных системах, необходимых для их проектирования и эксплуатации.

Воспитательная цель предполагает соответствие содержания предмета информационной безопасности и защиты информации современным требованиям воспитания подрастающего поколения, которые направлены на формирование у обучаемых гражданственности, мировоззрения, нравственности и высокой морали.

Задачи дисциплины

Задачи дисциплины следующие: формирование у магистрантов умения и навыков, необходимых для их дальнейшей профессиональной деятельности. Изучить ба-

зовые понятия криптографии и криптологии, основные определения, содержание, обзор возможностей, и практические сведения.

В результате изучения данной дисциплины магистранты должны:

иметь представление:

- о методах и средствах защиты информации при реализации информационных процессов ввода, вывода, передачи, обработки и хранения информации.

знать:

- особенности объектов защиты информации и их классификацию;
- ПЭВМ как объект защиты.

уметь:

- ставить и решать конкретные задачи по применению средств защиты информации для оптимизации функционирования информационных систем (ИС);
- применять системы защиты от вирусов и несанкционированного доступа в ПЭВМ.

приобрести практические навыки:

- оценки уровня безопасности в ИС.

быть компетентным:

- в вопросах разработки программного обеспечения защиты информации.

Пререквизиты

Для изучения данной дисциплины необходимо усвоение следующих дисциплин: «Дискретная математика», «Теория информация».

Постреквизиты

Знания, полученные при изучении дисциплины «Криптология», используются при освоении следующих дисциплин: «Технологии высокоскоростных вычислений», «Технология проектирования программных систем», «Моделирование систем и комплексов»

Тематический план дисциплины

Наименование раздела, (темы)	Трудоемкость по видам занятий, ч.				
	лекции	практические	лабораторторные	СРМП	СРМ
1 Введение. Классификация угроз компьютерным системам и сетям.	1	-	2	4	4
2 Симметричные криптосистемы.	1	2	4	4	4
3 Выработка гаммы с помощью генераторов псевдослучайных чисел.	1	2	4	4	4
4 Стандарты криптографирования.	1	2	4	4	4
5 Стандарт шифрования ГОСТ 28147-89.	1	-	-	4	4

6 Шифрование в режиме гаммирования.	1	2	4	4	4
7 Асимметричные криптосистемы.	1	-	-	4	4
8 Асимметричная криптосистема шифрования.	1	2	4	4	4
9 Необратимые контрольные последовательности.	1	-	-	4	4
10 Электронная цифровая подпись.	1	-	-	4	4
11 Получение ЭЦП на основе алгоритма ГОСТ Р 34.11-2001.	1	2	4	4	4
12 Виды аутентификации.	1	-	-	4	4
13 Протоколы аутентификации.	1	2	4	4	4
14 Генерация ключей.	1	-	-	4	4
15 Методы и средства защиты от удаленных атак через сеть.	1	1	-	4	4
ИТОГО:	15	15	30	60	60

Перечень практических занятий

1 Принципы защиты хранимого пароля от взлома.

2. Возможные варианты написания программы защиты хранимого пароля.

3. Модели шифрования по Диффи-Хеллману.

4. Работа генератора случайных чисел на линейном конгруэнтгом генераторе.

5. Методика написания программы генератора ПСЧ на регистрах сдвига произвольной длины.

6. Методика шифрования табличным методом.

7. Модели хэширования произвольного текста при разных хэш-функциях.

8. Аутентификация на симметричной системе в режиме полного доверия.

9. Аутентификация на симметричной системе в режиме не полного доверия.

10. Протоколы строгой аутентификации.

Перечень лабораторных занятий

1 Защита хранимого пароля от исследования методом эксперимента.

2 Исследование моделей шифрования по Диффи-Хеллману.

3 Разработка программы линейного конгруэнтного генератора случайных чисел.

4 Разработка программ, моделирующих генераторы случайных чисел на регистрах сдвига.

5 Разработка программы для шифрования файлов методом простой табличной замены.

6 Разработка программы для выработки Hash методом циклического гаммирования с введением нелинейности и постановки его на файлы.

Темы контрольных заданий для СРМ

1. 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.
11. Работа с большими целыми числами для целочисленной арифметики. Сложение целых чисел большой длины (например, длиной 20 байт)
12. Работа с большими целыми числами для целочисленной арифметики. Вычитание целых чисел большой длины (например, длиной 20 байт)
13. Модели умножения и деления больших чисел
14. Методика определения числа на простоту. Составить модель
15. Рассмотреть модель для реализации ЭЦП по алгоритму Эль Гамаля.

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%.

График выполнения и сдачи заданий по дисциплине

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи	Баллы
Лабораторная	Лабораторная работа №1 «Реализация простейших метод защиты программного обеспечения от несанкционированного доступа»	[1], [2], [3] [5]	3 недели	текущий	3 неделя	3
СРМП	Подготовка к лабораторной работе 1 «Защита программного обеспечения паролем»	[1], [2], [3] [5]	3 недели	текущий	3 неделя	2
СРМП	Защита лабораторной работы 1	[1], [2], [3], [5], [6],[10]	1 неделя	текущий	3 неделя	2
Лабораторная	Лабораторная работа №2 «Реализация алгоритма шифрования методами прямой замены»	[1], [2], [3], [5], [6],[10]	2 недели	текущий	5 неделя	3
СРМП	Подготовка к лабораторной работе 2 «Методы прямой замены (Цезаря, Еврейскйи)»	Вся рекомендуемая литература, конспекты лекций	3 недели	текущий	5 неделя	2
СРМП	Оформление и защита лабораторной работы №2 Рубежный контроль	Вся рекомендуемая литература, конспекты лекций	1 неделя	текущий	5 неделя	2
Лабораторная	Лабораторная работа №3 «Реализация алгоритма шифрования методами перестановок»	[1], [2], [3], [10], [14],[15]	2 неделя	текущий	7 неделя	3
СРМП	Подготовка к лабораторной работе 3 «Реализация метода Магический квадрат»	[1], [2], [3], [5], [12],[11]	3 неделя	текущий	7 неделя	2
СРМП	Оформление и защита лабораторной роботы 3	[1], [2], [3], [5], [12],[11]	1 неделя	текущий	7 неделя	2
Лабораторная	Лабораторная работа №4 «Реализация блочных алгоритмов шифрова-	Вся рекомендуемая литература, конспекты	2 неделя	текущий	9 неделя	3

	ния»	лекций				
СРМП	Подготовка к лабораторной работе 4 «Реализация метода Биграмм»	Вся рекомендуемая литература, конспекты лекций	3 неделя	текущий	9 неделя	2
СРМП	Оформление и защита лабораторной работы №4	[1], [2], [3], [5], [6],[10]	1 неделя	текущий	9 неделя	2
Лабораторная	Лабораторная работа №5 «Реализация много петлевого алгоритма шифрования»	Вся рекомендуемая литература, конспекты лекций	2 недели	текущий	11 неделя	3
СРМП	Подготовка к лабораторной работе 5 «Реализация метода Виженера»	Вся рекомендуемая литература, конспекты лекций	3 недели	текущий	11 неделя	2
СРМП	Рубежный контроль	[1], [2], [3], [10], [14],[15]	1 недели	текущий	10 неделя	2
СРМП	Оформление и защита лабораторной работы №5	[1], [2], [3], [10], [14],[15]	1 недели	текущий	11 неделя	2
Лабораторная	Лабораторная работа №6 «Реализация датчика псевдослучайных чисел (ДПЧ)»	[1], [2], [3], [5], [12],[11]	2 недели	текущий	13 неделя	3
СРМП	Подготовка к лабораторной работе 6 «Моделирование дискретной случайной величины»	Вся рекомендуемая литература, конспекты лекций	3 недели	текущий	13 неделя	2
СРМП	Подготовка к лабораторной работе 7 «Графическая оценка ДПЧ»	Вся рекомендуемая литература, конспекты лекций	3 неделя	текущий	14 неделя	2
Лабораторная	Лабораторная работа №7 «Оценка качества ДПЧ»	[1], [2], [3] [5]	3 неделя	текущий	15 неделя	3
СРМП	Оформление и защита лабораторной работы 7	[1], [2], [3], [5], [6],[10]	1 неделя	текущий	15 неделя	2
СРМП	Рубежный контроль	[1], [2], [3], [5], [6],[10]	1 неделя	текущий	14 неделя	2
Коллоквиум №1	Закрепление теоретических знаний и практических навыков по шифрованию информа-	Вся рекомендуемая литература, конспекты лекций	1 контактный час	рубежный	7 неделя	4,5

	ции					
Коллоквиум №2	Закрепление теоретических знаний и практических навыков по реалиизации алгоритмов шифрования информации	Вся рекомендуемая литература, конспекты лекций	1 контактный час	рубежный	14 неделя	4,5
Экзамен	Проверка усвоения материала дисциплины	Весь перечень основной и дополнительной литературы	3 контактных часов	Итоговый	В период сессии	40
Итого						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 прошу предоставлять справку, в других случаях – объяснительную записку.
3. Отрабатывать пропущенные занятия независимо от причины пропусков.
4. Активно участвовать в учебном процессе.
5. Своевременно выполнять и сдавать индивидуальные задания.
6. Быть терпимыми, открытыми, откровенными и доброжелательными к сокурсникам и преподавателям.

Список основной литературы

1. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком. 2007. -452с.
2. Герасименко В.А. – Защита информации в автоматизированных системах обработки информации. Книга 1,2 – М.: Энергоатомиздат, 2012. -176с.
3. Салома А. Криптография с открытым ключом.
4. Хоффман Л. Дж. Современные методы защиты информации / Пер. с англ. — М.: Сов. радио, 2008.-264с.
5. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. Издательство агентства Яхтсмен М.- 2006 -71с.
6. Мельников В. В. Защита информации в компьютерных системах Москва «Финансы и статистика» «Электроинформ» 2007. -368с. 161
7. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях Издательство агентства «Яхтсмен» М.-, 2008. - 368с

Список дополнительной литературы

8. Анин Б. Защита компьютерной информации. - СП6.: БХВ-СанкПетербург, 2000.-384с.
9. Милославская Н.Г. Толстой А.И. Интрасети: доступ в Интернет, защита: Учебное пособие для вузов. - М.: ЮКИТИ-ДАНА, 2007.-527 с.

10. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях /Под ред. В.Ф. Шаньгина,- М.: Радио и связь, 2009.- 328 с.
11. Домашев А.В., Попов В.О., Правиков Д.И., Прокофьев И.В., Щербаков А.Ю. Программированием алгоритмов защиты информации. Учебное пособие -М.: «Нолидж», 2008,-288с.
12. Гульев И.А. Компьютерные вирусы взгляд изнутри - М.: ДМК,2008-304с.
13. Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 2011.-216с.
14. Гостехкомиссия РФ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. — М.: Воениздат, 2002.
15. Пшенин Е.С. Теоретические основы защиты информации: Учебное пособие, Алматы: КазНТУ, 2010-125с. ISB 9965-487-З 6-7 162.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ МАГИСТРАНТА (SYLLABUS)

Дисциплина **K 5308** «Криптология»

Модуль **STZI 5** «Современные технологии защиты информации»

Гос. изд. лиц. № 50 от 31.03.2004.

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

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

_____

100027. Издательство КарГТУ, Караганда, Бульвар Мира, 56