АННОТАЦИЯ ДИСЦИПЛИНЫ

«Криптография»

Дисциплина «Криптография» является частью программы магистратуры «Математическая кибернетика» по направлению «01.04.02 Прикладная математика и информатика».

Цели и задачи дисциплины

Цель дисциплины:овладение основным математическим аппаратом исследования формализованных структур, формирование логического и системного мышления студентов. Целью преподавания дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике. Задачи дисциплины: - формирование знаний системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; - формирование умений принципов синтеза и анализа шифров; - приобретение навыков математических методов, используемых в криптоанализе..

Изучаемые объекты дисциплины

- алгоритмы поточного шифрования; - алгоритмы блочного шифрования; - алгоритмы вероятностного шифрования; - криптографические протоколы..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		3
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	18	18
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	34	34
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	90	90
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	144	144

Краткое содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
3-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Раздел 1. Шифрование	6	0	10	30
Тема 1. Основные понятия, термины, определения. Предмет и задачи дисциплины. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Тема 2. ШИФРЫ ПЕРЕСТАНОВКИ. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. ШИФРЫ ЗАМЕНЫ. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). ПОТОЧНЫЕ ШИФРЫ. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены. Тема 3. ТЕОРИЯ К.ШЕННОНА. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Раздел 3. Криптографические протоколы	8	0	16	32
Тема 6. ВОПРОСЫ СИНТЕЗА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ. Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Проверка построенной последовательности на случайность. Методы усложнения последовательностей псевдослучайных чисел. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнений последовательности. Различные способы задания дискретных функций. Тема 7. Методы анализа криптографических алгоритмов. Понятие криптоатаки. Виды криптоатак. Классификация криптоатак. Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уравнений шифрования, бесключевые методы. Особенности криптоанализа блочных шифров. Криптографические параметры узлов и блоков шифраторов. Основные принципы построения криптоалгоритмов (выбор группы шифра, параметров ПСП, параметров функции усложнения) СИСТЕМЫ ШИФРОВАНИЯ С ОТКРЫТЫМИ КЛЮЧАМИ. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Секретные характеристики в системах с открытым ключом. Преимущества ассиметричных систем шифрования. Вероятностное шифрование. Тема 8. МОДЕЛИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ. Сложность криптографических алгоритмов (теорема Кука, NP-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
криптографических протоколов. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения. Тема 9. Протоколы установления подлинности. Парольные системы разграничения доступа и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и ЭЦП. Протоколы управления ключами. Протоколы сертификации ключей. Протоколы распределения ключей. Открытое распределение ключей Диффи-Хэлмана и его модификация. Протоколы Oakley, ISAKMP. Проблемы и перспективы исследований в области современной криптографии. Квантовая криптография. Стеганография.				
Раздел 2. Проблемы реализации криптографических алгоритмов	4	0	8	28
Тема 4. ИМИТОСТОЙКОСТЬ ШИФРОВ. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования. ПОМЕХОУСТОЙЧИВОСТЬ ШИФРОВ. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв. Тема 5. РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ. Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров.				
ИТОГО по 3-му семестру	18	0	34	90
ИТОГО по дисциплине	18	0	34	90