АННОТАЦИЯ ДИСЦИПЛИНЫ

«Методы и средства криптографической защиты информации»

Дисциплина «Методы и средства криптографической защиты информации» является частью программы бакалавриата «Информационная безопасность (общий профиль, СУОС)» по направлению «10.03.01 Информационная безопасность».

Цели и задачи дисциплины

Изучение дисциплины «Криптографические методы защиты информации» имеет целью овладение основным математическим аппаратом исследования формализованных структур, формирование логического и системного мышления студентов. Целью преподавания дис-циплины является изложение основополагающих принципов защиты информации с помо-щью криптографических методов и примеров реализации этих методов на практике. В прогрессе изучения дисциплины студент осваивает следующие заданные дисциплинарные компетенции по направлениям подготовки 090900.62 и 090303.65: 1) способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21); 2) способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27); 3) способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-28). Задачи дисциплины – дать основы: 1) системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; 2) принципов синтеза и анализа шифров; 3) математических методов, используемых в криптоанализе..

Изучаемые объекты дисциплины

1) алгоритмы поточного шифрования; 2) алгоритмы блочного шифрования; 3) алгоритмы вероятностного шифрования; 4) криптографические протоколы..

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	64	64
- лекции (Л)	28	28
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	32	32
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	116	116
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	216	216

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
6-й семестр				
Заключение	2	0	2	3
ЗАКЛЮЧЕНИЕ. Проблемы и перспективы исследований в области современной криптографии. Квантовая криптография. Стеганография. Нерешенные задачи. Итоги изучения курса.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Введение в криптографию	4	0	4	10
Тема 1. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Тема 2. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Тема 3. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.				
Принципы построения криптографических алгоритмов	10	0	10	35
Тема 10. 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. Тема 11. 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. Тема 12. Методы усложнения последовательностей псевдослучайных чисел. Связь между качеством				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнений последовательности. Различные способы задания дискретных функций. Тема 13. 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) Тема 14. 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.				
Основные классы шифров и их свойства	4	0	4	15
Тема 4. ШИФРЫ ПЕРЕСТАНОВКИ. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Тема 5. ШИФРЫ ЗАМЕНЫ. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). Тема 6. ПОТОЧНЫЕ ШИФРЫ. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.				
Надежность шифров	3	0	4	18
Тема 7. 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. Тема 8. ИМИТОСТОЙКОСТЬ ШИФРОВ. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования. Тема 9. ПОМЕХОУСТОЙЧИВОСТЬ ШИФРОВ. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.				
Криптографические протоколы	5	0	8	35
Тема 15. 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 криптографических протоколов. Тема 16 ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения. Тема 17. Протоколы установления подлинности. Парольные системы разграничения доступа и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и ЭЦП. Тема 18. Протоколы управления ключами. Протоколы сертификации ключей. Протоколы распределения ключей. Открытое распределение ключей Диффи-Хэлмана и его				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
модификация. Протоколы Oakley, ISAKMP.				
ИТОГО по 6-му семестру	28	0	32	116
ИТОГО по дисциплине	28	0	32	116