Аннотация к рабочей программе
дисциплины «Криптографические методы защиты информации»
специальность 100503 Информационная безопасность АС
(специализация «Информационная безопасность АС на транспорте»).

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа)
Форма контроля: экзамен, курсовая работа на 6 семестре
Предполагаемые семестры: 6

Целями освоения учебной дисциплины являются: изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Учебная дисциплина «Криптографические методы защиты информации» обеспечивает приобретение знаний и умений в соответствии с Федеральным Государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Задачи дисциплины «Криптографические методы защиты информации» - 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.

Учебная дисциплина относится к циклу Б1. Изучение дисциплины «Криптографические методы защиты информации» базируется на дисциплинах: «Математика», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов».

Дисциплина «Криптографические методы защиты информации» обеспечивает изучение дисциплин:

– «Разработка и эксплуатация защищенных автоматизированных систем»;

– «Управление информационной безопасностью»;

– «Информационная безопасность автоматизированных транспортных систем»;

– «Защита электронного технологического документооборота»;

– «Информационная безопасность информационно-управляющих и информационно-логистических систем транспорта»;

– «Организация работы администратора автоматизированных систем»;

– Основы информационного противоборства и др.

Знания и практические навыки, полученные из дисциплины «Криптографические методы защиты информации», используются обучаемыми при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:
Исторический обзор. Открытые сообщения и их характеристики
Основные задачи и понятия криптографии. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Поточные шифры замены. Шифры простой замены и их анализ.

Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89. Криптоалгоритм AES. Надёжность шифров. Методы синтеза и анализа симметричных шифрсистем. Хеш-функции и их криптографические приложения.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

ПК-4: способностью проводить анализ защищенности автоматизированных систем;

ПК-27: способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;

ПК-28: способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы;

ПК-29: способностью администрировать подсистему информационной безопасности автоматизированной системы;

ПК-30: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;

ПК-31: способностью управлять информационной безопасностью автоматизированной системы;

ПК-32: способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

В результате изучения дисциплины «Криптографические методы защиты информации» студенты должны:

знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;

уметь:

- использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- уметь пользоваться научно-технической литературой в области криптографии;

владеть:

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ПЭВМ в анализе простейших шифров;
- навыками математического моделирования в криптографии.