Аннотация рабочей программы дисциплины

Основы криптографии

Направление подготовки: 11.03.02 - Инфокоммуникационные технологии и системы связи

Профиль подготовки: Защищенные системы и сети связи

Квалификация (степень) выпускника: Бакалавр

Общая трудоемкость дисциплины, изучаемой 6 семестре, составляет 4 зачетные единицы. По дисциплине предусмотрены: защита курсовой работы и зачет.

Цели и задачи освоения дисциплины

Целью преподавания дисциплины «Основы криптографии» является формирование у студентов теоретических знаний в области методов криптографической защиты информации в современных инфокоммуникационных системах.

Задачей дисциплины является выработка ясного представления у студентов об основных теоретических аспектах криптографии, а также способах шифрования и расшифрования сообщений, применяемых в различных симметричных и асимметричных криптосистемах с целью защиты информации от несанкционированного доступа

Требования к результатам освоения содержания дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-2);
- способность иметь навыки самостоятельной работы на компьютере и в компьютерных сетях, осуществлять компьютерное моделирование устройств, систем и процессов с использованием универсальных пакетов прикладных компьютерных программ (ОПК-4);
- способность применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики (ПК-17).

Основные разделы дисциплины

1. Основные понятия теории чисел и дискретной математики.
2. Основные понятия и терминология криптографии.
3. Требования, предъявляемые к современным криптосистемам для защиты информации.
4. Основные математические алгоритмы шифрования и расшифрования информации.

5. Построение симметричных и асимметричных криптосистем защиты информации и используемые в них стандарты шифрования.
6. Методы криптозащиты документов с использованием электронной подписи.