

ФТД.03 Криптографические протоколы

Объем дисциплины (модуля) 1 ЗЕТ (36 час)

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основной целью дисциплины «Криптографические протоколы» является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ

ПК-2: Способен администрировать средства защиты информации прикладного и системного программного обеспечения

ПК-2.2: Знает принципы функционирования программных средств криптографической и стеганографической защиты информации

В результате освоения дисциплины обучающийся должен

Знать: основные задачи и понятия криптографии; требования к криптографическим протоколам и основные характеристики криптографических протоколов;

Уметь: использовать криптографические протоколы для проектирования и разработки компьютерных систем; пользоваться научно-технической литературой в области криптографии.

Владеть: криптографической терминологией; навыками использования типовых криптографических протоколов; навыками использования ПЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Элементы криптографических протоколов

Раздел 2. Основные криптографические протоколы