

ФТД.В.02 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

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач

:

:

:

:

:

:

:

:

:

ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

:

:

:

:

:

:

:

:

:

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств 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

