

# Б1.Б.16 Криптографические методы защиты информации

Объем дисциплины (модуля) 3 ЗЕТ (108 час)

## ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

:  
:  
:  
:  
:  
:  
:  
:  
:  
:

**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 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; 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.

## СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Введение в криптографию

Раздел 2. Симметричные криптосистемы

Раздел 3. Асимметричные криптосистемы

Раздел 4. Средства криптографической защиты информации