Б1.Б.19 Методы и средства криптографической защиты информации

Объем дисциплины (модуля) **5 ЗЕТ (180 час)**

ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
Цель дисциплины: приобретение знаний и умений в области криптографической защиты информации; формирование мировоззрения и системного мышления. Задачи дисциплины: Изложение основополагающих принципов защиты информации с помощью криптографических методов; применение на практике криптоглафических методов и средств защиты информации.

ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ
ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-2.3: Осуществляет меры противодействия нарушениям информационной безопасности с использованием различных программных и аппаратных средств защиты информации
ОПК-2.1: Знает аппаратные средства вычислительной техники, принципы построения информационных систем и сетей, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;
ОПК-9.2: Применяет отечественные и зарубежные стандартизированные алгоритмы в области методов криптографической защиты информации
ОПК-9.1: Знает основные задачи и понятия криптографии, принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах
ОПК-9.3: Применяет программные и программно-аппаратные средства криптографической защиты информации для решения задач профессиональной деятельности
ОПК-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.3: Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объектов защиты различных видов

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