

## Аннотация дисциплины С.1.1.31 Дисциплина. Методы и средства криптографической защиты информации

Дисциплина "Методы и средства криптографической защиты информации" изучается обучающимися по основной профессиональной образовательной программе "Анализ безопасности информационных систем" направления подготовки "10.05.03 Информационная безопасность автоматизированных систем".

Дисциплина изучается в 7 семестре. Общая трудоемкость дисциплины составляет 144/4 часов/з.ед. Самостоятельная работа заключается в выполнении работ, указанных в разделе 4.

В ходе изучения дисциплины осуществляется текущий контроль в форме технологии рейтингового контроля в соответствии с технологической карты дисциплины, размещенной на электронном курсе, а также промежуточный контроль в форме экзамен.

Целью изучения дисциплины является формирование следующих компетенций:

1. ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

В ходе изучения дисциплины последовательно рассматриваются темы:

1. КЗИ. основные задачи и принципы КЗИ
2. Обзор классической и современной криптографии: от древних греков до 21 века
3. Симметричные и ассиметричные алгоритмы и схемы шифрования. Основные варианты использования
4. Теоретическая и практическая криптография. Методы шифров
5. Режим шифрования. Модели шифров. Формальные модели шифров. Алгебраическая модель шифра. Модель шифра простой замены
6. Симметричные системы шифрования и расшифрования
7. Принципы блочного шифрования. Шифр Файстеля
8. Реализация КЗИ в сетях общего пользования
9. Протоколы современных криптографических систем. Основные классы протоколов

Основными стратегическими образовательными технологиями являются: лекционные занятия, практические и лабораторные занятия.

В рамках указанных технологий применяются тактические образовательные технологии: классическая лекция.