

АННОТАЦИЯ

рабочей программы дисциплины

Криптографические методы защиты информации

1. Цель и задачи дисциплины

Целью изучения дисциплины является: ознакомление студентов с математическими основами современной криптографии, принципами защиты информации с помощью криптографических методов и способов реализации этих методов на практике. Знакомит обучающегося с ролью криптографии в современном мире, мировой культуре и истории.

Задачи дисциплины состоят в том, чтобы освоить студентом основ системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе.

2. Структура дисциплины

2.1 Общая трудоемкость дисциплины составляет 144 часа, 4 зачетные единицы

2.2 Основные разделы дисциплины:

- 1 - Введение в криптографию. Математические операции в криптографии
- 2 - Системы шифрования
- 3 - Хеш-функции

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-2 – способность понимать, совершенствовать и применять математический аппарат;

ПК-3 – способность критически переосмысливать накопленный опыт, изменять при необходимости вид и характер своей профессиональной деятельности;

ПК-4 – способность работать в составе научно-исследовательского и производственного коллектива и решать задачи профессиональной деятельности.

4. Виды промежуточной аттестации: экзамен