

АННОТАЦИЯ рабочей программы дисциплины ФТД.02 СОВРЕМЕННАЯ КРИПТОГРАФИЯ

Направление подготовки 09.04.02 Информационные системы и технологии

Объем трудоемкости: 2

Цель дисциплины – освоение студентами основных принципов современной криптографии и умение практического применения знаний для защиты информации.

Задачи дисциплины:

1. дать представления о классических системах шифрования;
2. дать представление о современных симметричных блочных шифрах и о методах их взлома;
3. дать представление о современных потоковых шифрах;
4. познакомить с современной асимметричной криптографией.

Место дисциплины в структуре ООП ВО

Дисциплина «Современная криптография» относится к вариативной части факультативного блока учебного плана.

Дисциплина «Современная криптография» учитывает накопленный опыт практической работы магистрантов в образовательных учреждениях, расширяет рамки представлений о сущности образования через освоение подходов к современной классификации наук и месте образования в этой классификации, раскрывает философские проблемы становления человека, методы получения современного научного знания в области образования, а также образовательные инновации, проекты, критерии оценки их эффективности. Изучение дисциплины является основой для последующего изучения дисциплин профессионально-педагогического цикла. Дисциплина базируется на знаниях, полученных при изучении дисциплин «Методы исследования и моделирования информационных процессов и технологий», «Логика и методология науки».

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций: ПК-2

Основные разделы дисциплины:

Основы теории чисел

Числовые сравнения

Симметричные и асимметричные шифры

Методы взлома шифров

Современные симметричные криптосистемы

Отечественный стандарт шифрования данных ГОСТ

Цифровая подпись

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет во 2 семестре

Автор Е.Н.Тумаев