АННОТАЦИЯ рабочей программы дисциплины
ФТД.02 СОВРЕМЕННАЯ КРИПТОГРАФИЯ

Направление подготовки 09.04.02 Информационные системы и технологии

Объем трудоемкости: 1

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

Задачи дисциплины:
1. дать представления о классических системах шифрование;
2. дать представление о современных симметричных блочных шифров и о методах их взлома;
3. дать представление о современных потоковых шифрах;
4. познакомить с современной ассиметричной 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

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-2	способность анализировать системные проблемы обработки информации и содержания в современной криптографии	логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных их разных областей науки и техники	проводить разработку и исследование теоретических и экспериментальных моделей, объектов профессиональной деятельности в различных областях; сбор, анализ научно-технической информации, отечественного	навыками профессиональной эксплуатации современного оборудования и приборов

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
				и зарубежного опыта по тематике исследования; выносить суждения на основании неполных данных	

Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в А семестре

№	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Внеаудиторная работа
			Л	ЛР	СРС
1	2	3	4	5	6
1.	Тема 1. Актуальность информационной безопасности, понятия и определения	5,8	1	1	3,8
2.	Тема 2. Угрозы информации	5	1	1	2
3.	Тема 3. Вредоносные программы	5	1	2	2
4.	Тема 4. Защита от компьютерных вирусов	5	2	2	1
5.	Тема 5. Методы и средства защиты компьютерной информации	5	2	2	1
6.	Тема 6. Криптографические методы информационной безопасности	5	2	2	1
7.	Тема 7. Лицензирование и сертификация в области защиты информации	5	1	2	2
	Итого по дисциплине:	35,8	10	12	13,8

Основные разделы дисциплины:

Основы теории чисел
Числовые сравнения
Симметричные и ассиметричные шифры
Методы взлома шифров
Современные симметричные криптосистемы
Отечественный стандарт шифрования данных ГОСТ
Цифровая подпись

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет в 10 семестре

Автор Е.Н.Тумаев