

**Аннотация к рабочей программы дисциплины**  
**«ФТД.02. Криптографические протоколы»**  
(код и наименование дисциплины)

**Объем трудоемкости:** 2 зачетных единицы

**Цель дисциплины:** задачи информатизации и защиты информации методами криптографии. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

**Задачи дисциплины:** получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

**Место дисциплины в структуре образовательной программы**

Дисциплина «криптографические протоколы» относится к факультативной части учебного плана. ФТД.02.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

**Требования к уровню освоения дисциплины**

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

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
<b>ПК-4</b> Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	
ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах	Знать: об основных задачах и понятиях криптографии; об этапах развития криптографии; о видах информации, подлежащей шифрованию; о классификации шифров; о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о методах криптозащиты компьютерных систем и сетей; Уметь использовать: типовые шифры замены и перестановки; частотные характеристики языков и их использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем: типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; постановки задач криптоанализа и подходы к их решению; Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты.
ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках	
ПК-4.3 Демонстрирует умение отбора среди существующих методов наиболее подходящие для решения конкретной прикладной задачи	

**Содержание дисциплины:**

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1.	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	18	2	4		12

2.	Поточные шифры. Синронизированные и самосинхронизирующиеся. Надежность шифров.	20	4	4		12
3.	Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами	16	2	2		12
4.	Системы шифрования с открытыми ключами	17,8	4	4		9,8
5.	<b>Итого по дисциплине:</b>		<b>12</b>	<b>14</b>		<b>45,8</b>
	Контроль самостоятельной работы (КСР)	-				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	12,8				
	Общая трудоемкость по дисциплине	72				

**Курсовые работы:** не предусмотрены

**Форма проведения аттестации по дисциплине:** зачет

Автор            А.В. Рожков, профессор, д.ф.-м.н., профессор