АННОТАЦИЯ
дисциплины Б1.О.32.02 «Теоретико-числовые методы криптографии»
для специальности 01.05.01 Фундаментальные математика и механика

Объем трудоемкости: составляет 3 зачетные единицы (108 часов, из них – 79,2 часа контактной работы (34 лекций, 34 часов лабораторных занятий, 11 часов КСР, 0,2 часов ИКР); 28,8 часа самостоятельной работы).

Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины.

Задачи освоения дисциплины «Теоретико-числовые методы криптографии»: 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 «Теоретико-числовые методы криптографии» относится к относится к обязательной части Блока 1 "Дисциплины (модули)" учебного плана и является одной из основных дисциплин в освоении математических знаний. Дисциплина «Теоретико-числовые методы криптографии» читается в 6 семестре.

Знания, полученные в этом курсе, могут быть использованы в ходе практик, в других компьютерных дисциплинах. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Математический анализ».

Требования к уровню освоения дисциплины

Изучение данной дисциплины направлено на получение необходимого объёма теоретических знаний, отвечающих требованиям ФГОС ВО и необходимых для дальнейшего успешного изучения всех дисциплин высшей математики, с формированием следующих общепрофессиональных компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-1	Способен находить, формулировать и решать актуальные и значимые проблемы фундаментальной математики и механики	об основных задачах и понятиях криптографии; об этапах развития криптографии; о видах информации, подлежащей шифрованию: о классификации шифров	использовать: типовые шифры замены и перестановки; частотные характеристики языков и их использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных	криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров

				шифрсистем	
2.	ОПК-3	Способен самостоятельно создавать и грамотно использовать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов	О методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о методах криптозащиты компьютерных систем и сетей	Использовать типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; постановки задач криптоанализа и подходы к их решению; основные математические методы, используемые в анализе типовых криптографических алгоритмов	навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты

Основные разделы дисциплины:

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Самостоятельная работа
			Л	ЛЗ	
1	**2**	**3**	**4**	**5**	**6**
1	Модели шифров.	24	8	10	6
2	Мультипликативные функции.	22	8	8	6
3	Табличное и модульное гаммирование.	26	10	8	8
4	Построение больших простых чисел.	24.8	8	8	8,8
	Итого:		**34**	**34**	**28,8**

Курсовые работы: *предусмотрена*

Форма проведения аттестации по дисциплине: *зачет*

Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: https://e.lanbook.com/reader/book/5193/#1
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: https://e.lanbook.com/reader/book/68466/#1

Автор РПД доктор физ.-мат.наук, профессор Рожков А.В.