АННОТАЦИЯ
дисциплины «Б1.В.10 ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ»

Объем трудоемкости: 4 зачетные единицы (144 часа, из них – 32,3 часа контактной работы (16 часов лекций, 16 практических занятий, 0,3 часа ИКР); 85 часов самостоятельной работы, 26,7 часов контроль).

Цель дисциплины:

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

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.

Изучение теоретических основ предмета: Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел.

Системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;

Алгебраических и теоретико-числовых принципов синтеза и анализа шифров;

Математических методов, используемых в криптоанализе и криптографии.

Место дисциплины в структуре ООП ВО

Дисциплина «Теоретико-числовые методы криптографии» относится к вариативной части блока Б1 Дисциплины и модули и является обязательной дисциплиной.

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

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-4	Способностью к применению методов математического и алгоритмического моделирования при решении теоретических и прикладных задач	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины: Разделы дисциплины, изучаемые в 1 семестре

№ раздела	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Самостоятельная работа
			Л	ЛЗ	
1	2	3	4	5	6
1	Модели шифров.	32	4	4	28
2	Мультипликативные функции.	32	4	4	28
3	Табличное и модульное гаммирование.	19	4	4	11
4	Построение больших простых чисел.	26	4	4	18
	Итого:		16	16	85

Курсовые работы: не предусмотрены.
Форма проведения аттестации по дисциплине: экзамен

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/book/5193
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/book/68466

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