

АННОТАЦИЯ
дисциплины «Б1.В.ДВ.04.02 Алгоритмы теории чисел»

Объем трудоемкости: 3 зачетные единицы (108 часа, из них – 48,2 часа контактной работы (16 часов лекций, 32 лабораторных занятий, 0,2 часа ИКР); 59,8 часов самостоятельной работы).

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 теории чисел. 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 «Алгоритмы теории чисел» относится к части, формируемой участниками образовательных отношений блока Б1 Дисциплины (модули) и является дисциплиной по выбору.

Данная дисциплина, как математическая основа криптографии, криптоанализа, 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-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	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.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
2	ПК-3	Способен публично представлять собственные и известные научные результаты	Способы подачи и демонстрации научно-информационного материала	Представить материал перед публикой, уметь руководить аудиторией	Навыками проведения лекционных и практических занятий, навыками полемики.

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Модели шифров.		4		8	14
2	Мультипликативные функции.		4		8	14
3	Табличное и модульное гаммирование.		4		8	15,8
4	Построение больших простых чисел.		4		8	16
	Итого по дисциплине:		16		32	59,8

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Виноградов И.М. Основы теории чисел. 13-е изд. [Электронный ресурс]. - СПб.: Лань, 2019. - URL: <https://e.lanbook.com/reader/book/115195/>
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>

Дополнительная литература:

1. Бухштаб А.А. Теория чисел, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: <https://e.lanbook.com/book/65053>
2. Манин Ю.И., Панчишкин А.А. Введение в современную теорию чисел [Электронный ресурс]. - М.: МЦНМО, 2009. - URL: <http://e.lanbook.com/view/book/9368/>

Интернет-ресурсы:

1. Пакет компьютерной алгебры Sage 8.9. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r10p2. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры PARI/GP 2.11. Официальный сайт <http://pari.math.u-bordeaux.fr/>

Автор РПД, д.ф.-м.н., профессор

Рожков А.В.