АННОТАЦИЯ

дисциплины Б1.В.ДВ.02.02 «Криптография и основы защиты информации»

Объем трудоемкости: 4 зачетные единицы (144 ч., из них 70,3 контактных – 68 ч. аудиторной нагрузки: лекционных 34 ч., лабораторные занятия 34 ч., 2 ч. КСР, 0,3 ИКР) 38 ч. самостоятельной работы, 35,7 ч. 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 систем кодирования и криптосистем. 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: коды исправляющие ошибки, коды сжатия информации как текстовой так и мультимедийной. Математические и теоретико-числовые основы теории кодирования и криптологии.

Обучение системному подходу к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения кодирующих и криптографических средств.

Место дисциплины в структуре ООП ВО

Дисциплина «Теория кодирования и защита информации» относится к части, формируемой участниками образовательных отношений блока Б1 и является дисциплиной по выбору. Курс «Теория кодирования и защита информации» продолжает начатое ранее обучение студентов по направлению математика и компьютерные науки. Знания, полученные в этом курсе, могут быть использованы в курсах защита операционных систем и баз данных, криптография, организационно-правовые методы защиты информации и др. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика», «Математический анализ».

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 решать актуальные и важные задачи фундаментальной и прикладной математики	О компьютерной реализации информационных объектов. Связи компью-	Определять структуры данных в компьютерной алгебре.	навыками использования основных типов шифров и криптографических

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
2.	ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	терной алгебры и численного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии	использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифр-систем.	алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты..

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	28	8		8	12
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	30	10		10	10
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	22	7		7	8
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	26	9		9	8
	Итого по дисциплине:		34		34	38

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. – URL. https://e.lanbook.com/reader/book/103908/#1
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: https://e.lanbook.com/reader/book/70724/#1

Автор РПД Рожков А.В.