АННОТАЦИЯ

дисциплины Б1.В.ДВ.14.02 «ТЕОРИЯ КОДИРОВАНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ»

Объем трудоемкости: 2 зачетные единицы (72 часа, из них – 50,2 часа контактной работы (24 часа лекций, 24 часа лабораторных занятий, 2 часа КСР, 0,2 часа ИКР); 21,8 часа 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 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 вариативной части профессионального цикла дисциплин по выбору студента (Б1.В.ДВ.14.02) 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.	ОПК-2	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информа-	содержание основных понятий по правовому обеспечению информационной безопасности; правовые способы защиты государственной тайны	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой ин-	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научнотехнической 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	ционной безопасности. Способность строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата		формации	

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Основные понятия и определения теории кодирования.	18	6		6	6
2	Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом.	18	6		6	6
3	Алгебраические методы в теории кодов.	18	6		6	6
4	Теория кодов и криптография.	15.8	6		6	3.8
	<i>Итого по дисциплине:</i>		24		24	21.8

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Бирюков А.А. Информационная безопасность: защита и нападение, 2-е изд. [Электронный ресурс]. – М.: ДМК Пресс, 2017. – URL: <http://e.lanbook.com/view/book/93278/>
2. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2017 https://e.lanbook.com/book/92914?category_pk=1537.

Дополнительная литература:

1. Нестеров С.А. Основы информационной безопасности, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2017. - https://e.lanbook.com/book/90153?category_pk=1537.
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: <http://e.lanbook.com/view/book/70724/>
3. Столов Е.Л. Цифровая обработка сигналов. Водяные знаки в аудиофайлах [Электронный ресурс]. - СПб.: Лань, 2018. - URL: <http://e.lanbook.com/view/book/106736/>

Интернет-ресурсы:

1. Пакет компьютерной алгебры Sage 8.2. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r9p1. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры Maple 2018. <http://www.maplesoft.com>
4. <http://www.pravo.gov.ru> – официальный портал правовой информации
5. <http://www.government.ru> - интернет-портал Правительства РФ
6. <http://graph.document.kremlin.ru> - раздел «Документы» портала Президента России
7. <http://minsvyaz.ru/ru> - сайт Минкомсвязи РФ
8. <http://www.rsoc.ru> - сайт Федеральной службы Роскомнадзор
9. <http://www.scrf.gov.ru> – сайт Совета безопасности РФ
10. <http://base.consultant.ru> – сайт правовой информации «Консультант+»
11. <http://www.fstec.ru> – официальный сайт ФСТЭК России
12. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)
13. Электронная библиотека <http://gen.lib.rus.ec/>

Автор РПД

Рожков А.В.