

**Министерство образования и науки Российской Федерации**  
**федеральное государственное бюджетное образовательное учреждение**  
**высшего образования**  
**«Казанский национальный исследовательский технический университет**  
**им. А.Н. Туполева-КАИ»**  
Институт Радиоэлектроники и телекоммуникаций  
Кафедра Радиофотоники и микроволновых технологий

**АННОТАЦИЯ**  
**к рабочей программе**  
**ТЕОРИЯ КОДИРОВАНИЯ И КРИПТОГРАФИЯ**

Индекс по учебному плану: **Б1.В.ДВ.06.01**

Направление подготовки: **11.04.01 Радиотехника**

Квалификация: **магистр**

Магистерская программа:

**Радиотехнические средства передачи, приема и обработки сигналов**

Виды профессиональной деятельности: **научно-исследовательская,**  
**научно-педагогическая.**

Разработчик: к.т.н., доцент кафедры РЭКУ Д.П. Данилаев

Казань 2017 г.

## **РАЗДЕЛ 1. ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

### **1.1 Цель изучения дисциплины**

Изучение принципов криптографической защиты информации, помехоустойчивого кодирования и механизмов их реализации при проектировании и эксплуатации радиотехнических систем и средств передачи и приема информации на фоне действия шумов и помех.

### **1.2 Задачи дисциплины**

Основными задачами дисциплины являются:

- изучить теоретические основы помехоустойчивого кодирования и криптографической защиты информации в современных радиотехнических системах;
- изучить методы, отечественные и международные стандарты кодирования информации для организации ее передачи по каналам связи;
- овладеть средствами и алгоритмами помехоустойчивого и криптографического кодирования информации;
- углубление и закрепление теоретических знаний, и формирование практических навыков при выполнении лабораторных занятий в учебных аудиториях кафедры, а также в период производственной практики.

### **1.3 Место дисциплины в структуре ОП ВО**

Дисциплина «Теория кодирования и криптография» входит в состав вариативной части магистерской программы по направлению подготовки 11.04.01 «Радиотехника», магистерская программа «Радиотехнические средства передачи, приема и обработки сигналов».

### **1.4 Перечень компетенций, которые должны быть реализованы в ходе освоения дисциплины**

ПК-1 – способностью самостоятельно осуществлять постановку задачи исследования, формирование плана его реализации, выбор методов исследования и обработку результатов, ПК-2 – способностью выполнять моделирование объектов и процессов с целью анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ, ПК-3 – способностью разрабатывать и обеспечивать программную реализацию эффективных алгоритмов решения сформулированных задач с использованием современных языков программирования.

## РАЗДЕЛ 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ТЕХНОЛОГИЯ ЕЕ ОСВОЕНИЯ

### 2.1 Структура дисциплины, ее трудоемкость и применяемые образовательные технологии

Таблица 2 Распределение фонда времени по видам занятий

Наименование раздела и темы	Всего часов	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах/интерактивные часы)				Коды составляющих компетенций	Формы и вид контроля освоения составляющих компетенций (из фонда оценочных средств)
		лекции	лаб. раб.	пр. зан.	сам. раб.		
<i>Раздел 1. Основные положения теории кодирования и шифрования</i>							<i>ФОС ТК-1 тесты</i>
Тема 1.1. Введение в теорию криптографического закрытия информации	9	1			8	ПК-1.з, ПК-3.з	Контрольные вопросы по теме теоретического курса
Тема 1.2. Основные понятия в теории криптографического закрытия информации	9	1			8	ПК-1.з, ПК-3.з	Контрольные вопросы по теме теоретического курса
Тема 1.3. Классификация методов преобразования информации	22/2	2/1	4/1		16	ПК-1з, ПК-1.у, ПК-1.в, ПК-2.з, ПК-3.з, ПК-3.у, ПК-3.в	Тестирование качества освоения теоретического материала. Защита результатов лабораторных занятий.
<i>Раздел 2. Основные методы защиты информации</i>							<i>ФОС ТК-2 тесты</i>
Тема 2.1. Основные методы защиты информации	30/3	2/1	8/2		20	ПК-1з, ПК-1.у, ПК-1.в, ПК-2.з, ПК-2.у, ПК-2.в, ПК-3.з, ПК-3.у, ПК-3.в	Контрольные вопросы по теме теоретического курса
Тема 2.2. Шифрование с помощью генератора псевдослучайных чисел	22/1	2	4/1		16	ПК-1з, ПК-1.у, ПК-1.в, ПК-2.з, ПК-2.у, ПК-2.в, ПК-3.з, ПК-3.у, ПК-3.в	Контрольные вопросы по теме теоретического курса
Тема 2.3. Стандарты шифрования. Системы шифрования	16	2			14	ПК-1з, ПК-1.у, ПК-1.в, ПК-3.з, ПК-3.у, ПК-3.в	Выполнение учебных, проектных заданий. Защита результатов лабораторных и практических занятий
Экзамен	36				36	ПК-1з, ПК-1.у, ПК-1.в, ПК-2.з, ПК-2.у, ПК-2.в, ПК-3.з, ПК-3.у, ПК-3.в	<i>ФОС ПА</i>
ИТОГО:	144/ 7	10/2	16/4		118		

## **РАЗДЕЛ 3 ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **3.1 Учебно-методическое обеспечение дисциплины**

#### **3.1.1 Основная литература**

1. Осмоловский, С.А. Стохастическая информатика: инновации в информационных системах / С.А. Осмоловский. - М.: Горячая линия-Телеком, 2011. - 320с.

2. Крухмалев, В.В. Цифровые системы передачи : учеб. пособие для студ. вузов / В. В. Крухмалев, В. Н. Гордиенко, А. Д. Моченов ; под ред. А. Д. Моченова. - 2-е изд., перераб. и доп. - М. : Горячая линия - Телеком, 2014. – 372 с.

3. Золотарев, В. В. Многопороговые декодеры и оптимизационная теория кодирования / В. В. Золотарев, Ю. Б. Зубарев, Г. В. Овечкин ; под ред. В. К. Левина. - М. : Горячая линия-Телеком, 2013. - 239 с.

#### **3.1.2 Дополнительная литература**

1. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение : учеб. пособие / Р. Морелос-Сарагоса; пер. с англ. В.Б. Афанасьева. - М. : Техносфера, 2005. - 320 с.

2. Вернер, М. Основы кодирования : учебник для вузов / М. Вернер ; пер. с нем. Д.К.Зигангирова. - М. : Техносфера, 2004. - 288 с.

3. Золотарев, В. В. Помехоустойчивое кодирование. Методы и алгоритмы : справочник / В.В. Золотарев, Г.В. Овечкин; под ред. Ю.Б. Зубарева. - М. : Горячая Линия - Телеком, 2004. - 126 с.

4. Ризаев, И.С. Элементы теории информации и кодирования сообщений: практич. пособие / И.С. Ризаев, Ф.И. Эминов. - Казань : Медицина, 1996. - 30с.

5. Зяблов, Виктор Васильевич. Обобщенные каскадные помехоустойчивые конструкции на базесверточных кодах / В. В. Зяблов, С. А. Шавгулидзе. - М. : Наука, 1991. - 206 с.

6. Чисар,И. Теория информации: теоремы кодирования для дискретных систем без памяти / И. Чисар, Я. Кернер ; пер. с англ. С. И. Гельфанда и Л. Е. Филипповой, под ред. Р.Л. Дробушина. - М. : Мир, 1985. - 397 с.

7. Витерби, Э. Принципы цифровой связи и кодирования / Э. Витерби, Дж. Омура; пер. с англ. под ред. К.Ш. Зигангирова. - М. : Радио и связь, 1982. - 536 с.

8. Млечин, В В. Теория радиоэлектронного преодоления. Анализ воздействия помех на радиотехнические системы и устройства / В. В. Млечин. - М. : Радиотехника, 2009. - 976 с.

9. Лебедько, Е Г. Теоретические основы передачи информации: учеб. пособие для студ. вузов / Е. Г. Лебедько. - СПб. ; М. ; Краснодар : Лань, 2011. - 352 с.

10. В. И. Дмитриев Прикладная теория информации Москва: Высш.Школа, 1989 -384с.

11. Введение в криптографию / Под общ. Ред. В.В.Ященко. – 4-е изд., доп. – М.: МЦНМО, 2012. – 348 с.

12. Зубов, А Ю. Криптографические методы защиты информации. Совершенные шифры : учеб. пособие для вузов / А.Ю. Зубов. - М. : Гелиос АРВ, 2005. - 192 с.

13. Аграновский, А. В. Практическая криптография : алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади. - М. : СОЛОН-Пресс, 2002. - 256 с.

14. Левин, М. Криптография: Руководство пользователя : учебник / М. Левин. - М. : Познавательная книга плюс, 2001. - 320 с.

15. Молдовян, Н А. Введение в криптосистемы с открытым ключом : учеб. пособие / Н.А. Молдовян, А.А. Молдовян. - СПб. : БХВ-Петербург, 2005. - 288 с.

16. Молдовян, Н А. Криптография. От примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. - СПб. : БХВ-Петербург, 2004. – 448с.

## **3.2 Информационное обеспечение дисциплины (модуля)**

### **3.2.1 Основное информационное обеспечение**

1. Данилаев Д.П. «Теория кодирования и криптография» [Электронный ресурс]: курс дистанц. обучения по направлению подготовки магистров 11.04.01 «Радиотехника», 2015. – Доступ по логину и паролю. URL: [https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content\\_id=184366\\_1&course\\_id=11763\\_1&mode=reset](https://bb.kai.ru:8443/webapps/blackboard/execute/content/blankPage?cmd=view&content_id=184366_1&course_id=11763_1&mode=reset).

## **3.3 Кадровое обеспечение**

### **3.3.1 Базовое образование**

Высшее образование в предметной области радиотехники и /или наличие ученой степени и/или ученого звания в указанной области и /или наличие дополнительного профессионального образования– профессиональной переподготовки в области радиотехники и/или наличие заключения экспертной комиссии о соответствии квалификации преподавателя профилю преподаваемой дисциплины.