



МИНОБРНАУКИ РОССИИ  
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Утверждено:  
на заседании кафедры  
протокол № 11 от «17» июня 2019 г.  
Зав. кафедрой  / Р.С. Юлмухаметов

Согласовано:  
Председатель УМК факультета математики и  
информационных технологий  
 / Ефимов А.М.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

дисциплина Теория кодирования, защита информации

Часть, формируемая участниками образовательных отношений


**программа бакалавриата**

Направление подготовки (специальность)

02.03.03 Математическое обеспечение и администрирование информационных систем

Направленность (профиль) подготовки  
Системное и интернет-программирование

Квалификация  
бакалавр

Разработчики (составители) доцент, к.ф.-м.н., доцент	<u></u> / Луценко В.И.
---	--

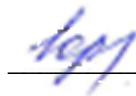
Для приема: 2019

Уфа 2019 г.

Составитель: Доцент кафедры ПиЭИ, к.ф.-м.н. Луценко В.И.

Рабочая программа дисциплины утверждена на заседании кафедры программирования и экономической протокол информатики от «17» июня 2019 г. № 11.

Заведующий кафедрой



\_\_\_\_\_ / Юлмухаметов Р.С./

### Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине
4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания
4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций
4.3. Рейтинг-план дисциплины
5. Учебно-методическое и информационное обеспечение дисциплины
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине
Приложение №1
Приложение №2
Приложение №3
Приложение №4

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

(с ориентацией на карты компетенций)

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

<b>Категория (группа) компетенций</b>	<b>Формируемая компетенция (с указанием кода)</b>	<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по дисциплине (модулю)</b>
Теоретические и практические основы профессиональной деятельности	ПК-1. Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий.	ПК-1.1. Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Должен обладать фундаментальными знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.
		ПК-1.2. Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий.	Уметь находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий.
		ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области программирования и информационных технологий	Приобретен практический опыт научно-исследовательской деятельности в области программирования и информационных технологий в области информационной

			безопасности.
<p>Математические и алгоритмические модели, программы, программные системы и комплексы, методы их проектирования и реализации, способы производства, сопровождения, эксплуатации и администрирования в различных областях цифровой экономики.</p>	<p>ПК-7. Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемноориентированных программных систем и комплексов в профессиональной деятельности.</p>	<p>ПК-7.1. Владеет знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Владеет тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;</p>	<p>Владеть знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Владеть тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;</p>
		<p>ПК-7.2. Умеет программировать для компьютеров с различной современной архитектурой;</p>	<p>Уметь программировать для компьютеров с различной современной архитектурой для обеспечения системной защиты;</p>

		ПК-7.3. Имеет практический опыт выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования.	Владеть навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования для обеспечения информационной безопасности.
--	--	---	--

## 2. Цель и место дисциплины в структуре образовательной программы

. Дисциплина (модуль) «Теория кодирования, защита информации» относится к вариативной части, дисциплины по выбору.

Дисциплина (модуль) изучается на 3 курсе в 5 семестре.

Цель изучения дисциплины – формирование у обучающихся фундаментальных теоретических знаний в области применения наиболее эффективных методов кодирования, позволяющих осуществлять передачу определенного количества информации по каналу связи с помощью минимального количества символов, как при отсутствии, так и при наличии помех.

Для изучения данной дисциплины студент должен получить необходимые знания, умения и компетенции, которые формируются в результате изучения перечисленных ниже дисциплин.

Перечень дисциплин, изучение которых должно предшествовать изучению данной дисциплины:

- Иностранный (английский) язык;
- Математический анализ (функции одной переменной);
- Алгебра и геометрия;
- Вычислительные методы;
- Языки и методы программирования;

Знания и умения, полученные в результате освоения данной дисциплины, будут использоваться при прохождении обучающийся предквалификационной практики, подготовке им выпускной квалификационной работы, а также в научной и практической деятельности после окончания университета.

## 3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

#### **4. Фонд оценочных средств по дисциплине**

**4.1. Перечень индикаторов достижения компетенций с указанием планируемых результатов обучения по дисциплине (модулю), соотнесенных с установленными в образовательной программе индикаторами достижения компетенций.. Описание показателей и критериев оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания**

Код и формулировка компетенции: . ПК-1. Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий.



Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
ПК-1.1. Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Должен обладать фундаментальными знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Отсутствие умений или (фрагментарные ) умение применять фундаментальные знания, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Сформированное (возможно несистематическое) умение применять фундаментальные знания, полученными в области математических и (или) естественных наук, программирования и информационных технологий.
ПК-1.2. Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий..	Уметь находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий.	Отсутствие умений или (фрагментарные ) умение применять находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирован	Сформированное (возможно несистематическое) умение применять находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирован
ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области программирования и информационных технологий	Владеть опытом научно-исследовательской деятельности в области программирования и информационных технологий	Отсутствие владения или фрагментарное владение опытом научно-исследовательской деятельности в области программирования и информационных технологий	Успешное и систематическое (возможно содержащее незначительные пробелы) владение опытом научно-исследовательской деятельности в области программирования и

			информационных технологий
ПК-7.1. Владеет знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Владеет тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;	Владеть знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Владеть тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;	Отсутствие владения или (фрагментарные ) владения знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Отсутствие владения или (фрагментарные ) владения тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;	Сформированное владения (возможно несистематическое) владения знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Сформированное владения (возможно несистематическое) владения знаниями по направлениям тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;
ПК-7.2. Умеет программировать для компьютеров с различной современной архитектурой;	Уметь программировать для компьютеров с различной современной архитектурой для обеспечения системной защиты;	Отсутствие умений или (фрагментарные ) умение программировать для компьютеров с различной современной архитектурой для обеспечения системной	Сформированное (возможно несистематическое) умение применять находить программировать для компьютеров с различной

		защиты;	современной архитектурой для обеспечения системной защиты;
ПК-7.3. Имеет практический опыт выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования.	Владеть навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования для обеспечения информационной безопасности.	Отсутствие владения или фрагментарное владение навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования для обеспечения информационной безопасности.	Успешное и систематическое (возможно содержащее незначительные пробелы) навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования для обеспечения информационной безопасности.

**4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине (модулю), соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)**

<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по дисциплине (модулю)</b>	<b>Контролируемые действия по проверке знаний, умений и владений (Оценочные средства)</b>
ПК-1.1. Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	Знать основные понятия, определения и свойства объектов дискретной математики, формулировки и доказательства	Лабораторные работы, зачет
ПК-1.2. Умеет находить, формулировать и	Должен обладать фундаментальными	Лабораторные работы, зачет

решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий..	знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий.	
ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области программирования и информационных технологий	Уметь находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий.	Лабораторные работы, зачет
ПК-7.1. Владеет знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Владеет тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;	Владеть знаниями по направлениям развития: компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств, операционных систем, операционных и сетевых оболочек, сервисных программ. Владеть тенденциями развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности;	Лабораторные работы, зачет
ПК-7.2. Умеет программировать для компьютеров с различной современной архитектурой;	Уметь программировать для компьютеров с различной современной архитектурой для обеспечения системной защиты;	Лабораторные работы, зачет
ПК-7.3. Имеет практический опыт выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования.	Владеть навыками выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования для обеспечения информационной безопасности.	Лабораторные работы, зачет

#### 4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

## 5. Учебно-методическое и информационное обеспечение дисциплины

### 5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

#### Основная литература:

1. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: <https://e.lanbook.com/book/68466>.
2. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : Лань, 2019. — 324 с. — Режим доступа: <https://e.lanbook.com/book/114688>.
3. Березкин, Е.Ф. Основы теории информации и кодирования [Электронный ресурс] : учебное пособие / Е.Ф. Березкин. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 320 с. — Режим доступа: <https://e.lanbook.com/book/108326>.

#### Дополнительная литература:

4. Мытник, К.Я. Смарт-карты и информационная безопасность [Электронный ресурс] / К.Я. Мытник, С.П. Панасенко ; под ред. В.Ф. Шаньгина. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 516 с. — Режим доступа: <https://e.lanbook.com/book/116128>.

### 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1	Электронно- библиотечная система «ЭБ БашГУ»	Собственная электронная библиотека учебных и научных электронных изданий, которая включает издания преподавателей БашГУ	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация в Библиотеке БашГУ, дальнейший доступ из любой точки сети Интернет	<a href="https://elib.bashedu.ru/">https://elib.bashedu.ru/</a>
2	Электронно-библиотечная система «Университетская	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой	Регистрация из сети БашГУ,	<a href="http://www.biblioclub.ru/">http://www.biblioclub.ru/</a>

библиотека online»		точки сети Интернет	дальнейший доступ из любой точки сети Интернет	
3 Электронно-библиотечная система издательства «Лань»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	<a href="http://e.lanbook.com/">http://e.lanbook.com/</a>

2018/2019	Договор на ЭБС между БашГУ и издательством «Лань» № 848 от 03.09.2018	С 01.10.2018 по 30.09.2019
	Соглашение на бесплатные коллекции в ЭБС между БашГУ и издательством «Лань» № 961 от 01.10.2018	С 01.10.2018 по 30.09.2019
	Договор на доступ к электронным научным периодическим изданиям между БашГУ и РУНЭБ № 1262 от 11.12.2018	С 11.12.2018 по 31.12.2019
	Договор на БД диссертаций между БашГУ и РГБ №095040040 от 27.02.2019	С 27.02.2019 по 26.02.2020

## 6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

<p><b>1. учебная аудитория для проведения занятий лекционного типа:</b> аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное)</p> <p><b>2. учебная аудитория для проведения занятий семинарского типа:</b> аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория №</p>	<p><b>Аудитория №426</b></p> <p>Учебная мебель, доска, персональные компьютеры LenovoThinkCentreA70zIntelPentiumE 5800, 320 Gb, 19" – 13 шт., шкаф TLKTWP-065442-G-GY</p>
	<p><b>Аудитория №520а</b></p> <p>Учебная мебель, доска, монитор LG 19 L1942S SF 1280 x 1024,5ms,8000:1,black (3,4 кг,VGA,19"(48,3см)5mc, мониторы LG 19" L1942SBF 1280x1024,5ms,8000:1,black 10 шт., системный блок HP Pavilion Slimline S3500 FAMD Athlon 64 X2 5400+/2.8GHz, 4Gb, 500Gb 12шт., доска аудитор. ДА36.</p>

<p>522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное)</p> <p><b>3. учебная аудитория для курсового проектирования (выполнения курсовых работ):</b> аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное)</p> <p><b>4. учебная аудитория для проведения групповых и индивидуальных консультаций:</b> аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное)</p> <p><b>5. учебная аудитория для текущего контроля и промежуточной аттестации:</b> аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное)</p> <p><b>6. помещения для самостоятельной работы:</b></p> <p>аудитория № 426 (Физмат корпус - учебное), читальный зал №2 (Физмат корпус - учебное)</p> <p><b>7. помещение для хранения и профилактического обслуживания учебного оборудования:</b> аудитория № 522 (Физмат корпус - учебное)</p>	<p style="text-align: center;"><b>Аудитория № 521</b></p> <p>Учебная мебель, доска, коммутатор HP V1905-24 Switch 24*10/100+2*10/100/1000, персональные компьютеры в комплекте DEPO Neos 460MDi5 2300/4GDDR1333/T500G/DVD W – 12 шт., проектор Optoma EX542i.DLP3D.XGA(1024*768).2700 ANSI Lm.3000 1.Lamp5000+/-40 ver, шкаф TLKTWP-065442-G-GY, экран на штативе DraperDiplomat (1:1) 84/84* 213*213 MW, доска аудитор. ДА36.</p> <p style="text-align: center;"><b>Аудитория №522</b></p> <p>Учебная мебель, доска, персональный компьютер LenovoThinkCentre A70z IntelPentium E 5800, 320 Gb, 19" – 13 шт., кондиционер LessarLS/LU-H24KB2.</p> <p style="text-align: center;"><b>Аудитория № 524</b></p> <p>Учебная мебель, доска настенная меловая, коммутатор HP V1905-24 Switch 24*10/100+2*10/100/1000, персональный компьютер в комплекте HP AiO 20"CQ 100 eu – 27 шт., экран ScreeMediaGolgview 274*206 NW 4:3, универсальное потолочное крепление ScreeMedia для проектора, регулировка высоты , шкаф TLKTWP-065442-G-GY,</p> <p>патч-корд (1296), доска аудитор. ДА32.</p> <p style="text-align: center;"><b>Аудитория № 525</b></p> <p>Учебная мебель, доска, персональные компьютеры в комплекте DEPO Neos 460MDi5 2300/4GDDR1333/T500G/DVDW/ - 13 шт., доска аудитор. ДА32.</p> <p style="text-align: center;"><b>Читальный зал №2</b></p> <p>Учебная мебель, учебно-наглядные пособия, стенд по пожарной безопасности, моноблоки стационарные – 8 шт, принтер – 1 шт., сканер – 1 шт.</p>
--	---

МИНОБРНАУКИ РОССИИ  
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ**

дисциплины «Теория кодирования, защита информации» на 6 семестр

очная

форма обучения

Рабочую программу осуществляет:

Лекции: доцент каф. ПиЭИ, к.ф.-м.н. Луценко В.И.

Практические занятия: доцент каф. ПиЭИ, к.ф.-м.н. Луценко В.И.

<b>Вид работы</b>	<b>Объем дисциплины</b>
Общая трудоемкость дисциплины (ЗЕТ / часов)	2/72
Учебных часов на контактную работу с преподавателем:	36,2
Лекций	12
практических/ семинарских	
Лабораторных	24
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР) включая подготовку к экзамену/зачету	35.8

Форма контроля:

Зачет 5 семестр



№п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		Всего	ЛК	ПР/СЕ М	ЛР	СР			
1	2	3	4	5	6	7	8	9	10
	5- й семестр	72	12		24	35.8			
1	Модуль 1. Теория информации. Базовые понятия теории информации. 1.1. Теория информации рассматривается как существенная часть кибернетики. Характеристики непрерывной и дискретной информации. 1.2. Принципы хранения, измерения, обработки и передачи информации. Схема передачи информации. Сущность работы ЦВМ и АВМ и их применение на практике. 1.3. Базовые понятия: информация, канал связи, шум, кодирование.		1		3	4	1-2	Отчет по лабораторной работе №1	отчеты по лабораторным работам
2	Модуль 2. Энтропия Шеннона. 2.1 Энтропия дискретной случайной величины. Понятие префиксного кодирования. 2.2 Сжатие информации. Основная теорема о кодировании при отсутствии помех. 2.3 Метод блокирования.		1		3	4	1-2	Отчет по лабораторной работе №2	отчеты по лабораторным работам

3	<p>Модуль 3. Математическая модель системы связи.</p> <p>3.1 Коды с исправлением ошибок. Коды с обнаружением ошибок.</p> <p>3.2 Понятие сигнала и его модели. Различные формы представления детерминированных сигналов.</p>		1		3	4	1-2	Отчет лабораторной работе №3	по	отчеты по лабораторным работам
4	<p>Модуль 4. Кодирование информации.</p> <p>4.1 Основные задачи кодирования.</p> <p>4.2 Эффективное и помехоустойчивое кодирование. Основные теоремы Шеннона о кодировании.</p> <p>4.3 Эффективные коды: код Шеннона - Фано, код Хаффмана, и их характеристики.</p>		1		3	4	1-2	Отчет лабораторной работе №4	по	отчеты по лабораторным работам
5	<p>Модуль 5. Методики построения помехоустойчивых кодов.</p> <p>5.1 Код с проверкой четности.</p> <p>5.2 Код с тройным повторением.</p> <p>5.3 Код Хэмминга..</p>		1		3	4	1,2	Отчет лабораторной работе №5	по	отчеты по лабораторным работам
6	<p>Модуль 6. Математические основы шифрования с открытым ключом.</p> <p>6.1 Сравнения.</p> <p>6.2. Функция Эйлера</p> <p>6.3 Теорема Эйлера.</p>		3		3	4	1-2	Отчет лабораторной работе №6	по	отчеты по лабораторным работам
7	<p>Модуль 7. Математические основы шифрования с открытым ключом.</p>		3		3	4.8	1-2	Отчет лабораторной работе №7	по	отчеты по лабораторным работам

	7.1 Теорема малая Ферма. 7.2. Алгоритм генерации длинных простых чисел.								
8	Модуль 8. Моделирование цифровой подписи.		1		3	7	1-2	Отчет по лабораторной работе №8	отчеты по лабораторным работам
	Всего часов:	72	12		24	35.8			0.2

Приложение № 2

**Рейтинг – план дисциплины**

Теория кодирования, защита информации

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	баллы	
			минимальный	максимальный
<b>Текущий контроль</b>				<b>80</b>
Отчеты по лабораторным работам	6	8	0	48
<b>Рубежный контроль</b>				<b>32</b>
Защита отчетов	4	8	0	32
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных занятий			0	-10
<b>Итоговый контроль</b>				<b>20</b>
1. Зачет	10	2	0	20
<b>ИТОГО</b>				<b>100</b>

Вопросы для самостоятельной проработки  
Раздел 1 Информация и ее свойства

При изучении раздела 1 необходимо:

1. Читать лекции, содержащие основы образовательной программы по дисциплине «теория информации и кодирования».

Акцентировать внимание на следующих понятиях:

- данные, информация;
- свойства информации;
- формы адекватности информации.

Определить основные особенности информационных коммуникаций.

Уяснить основные особенности и сферы применения синтаксической, семантической, прагматической адекватности.

2. Для самооценки по разделу 1 необходимо ответить на следующие вопросы:

1. Каким образом измеряется объем данных в сообщении, привести пример;
2. Дайте определение понятию «количество информации».
3. Напишите и разъясните формулу Шеннона, Хартли, приведите пример;
4. Что такое тезаурусная мера, тезаурус;
5. Как можно определить ценность информации;
6. Перечислите качества информации;
7. Перечислите единицы измерения информации и приведите примеры;
8. Характеристики для оценки качества информации.

Раздел 2. Классификация и кодирование информации

При изучении раздела 2 необходимо:

**1. Читать лекции, содержащие основы образовательной программы по дисциплине «теория информации и кодирование».**

Акцентировать внимание на следующих понятиях:

- иерархическая система классификации информации;
- фасетная система классификации информации;
- дескрипторная система классификации информации.

Определить основные особенности системы кодирования.

36

Уяснить основные особенности и сферы применения последовательного кодирования, параллельного кодирования, регистрационного кодирования

(порядковая система кодирования, серийно-порядковая система кодирования).

**2. Для самооценки по разделу 2 необходимо ответить на следующие вопросы:**

1. Иерархическая система кодирования.
2. Фасетная система кодирования.
3. Дескрипторная система кодирования.
4. Назначение системы кодирования.
5. Основные идеи классификационного и регистрационного кодирования.
6. Классификация информации, циркулирующей в организации.

**Раздел 3. Информационно-логические основы построения**

**При изучении раздела 3 необходимо:**

**1. Читать лекции, содержащие основы образовательной программы по дисциплине**

***«Теория кодирования, защита информации».***

Акцентировать внимание на следующих понятиях:

- позиционные системы счисления;
- законы алгебры-логики;
- представление информации в ПК.

Определить основные особенности процесса логического синтеза вычислительных схем.

Уяснить основные особенности и сферы применения алгоритмов решения задач.

**2. Для самооценки по разделу 3 необходимо ответить на следующие вопросы:**

1. Непозиционные системы счисления
2. Позиционные системы счисления
3. Охарактеризуйте перевод числа из десятичной системы счисления в любую другую систему счисления
4. Охарактеризуйте перевод дробного числа из любой системы счисления в десятичную систему счисления
5. Определите поля постоянной длины
6. Упакованный формат двоично-кодированного десятичного числа
7. Распакованный формат двоично-кодированного десятичного числа
8. ASCII-код для представления символьной информации
9. Определение алгебры логики
10. Простейшие операции алгебры-логики

37

11. Перечислите законы алгебры-логики. Приведите примеры

12. Рассмотрите логический синтез вычислительных систем на примере одноразрядного двоичного сумматора

13. Определите логическую схему сумматора

14. Поясните логические блоки сумматора

**Для самостоятельной проверки знаний необходимо ответить на следующие вопросы:**

1. Формы представления информации в персональном компьютере

2. Основные понятия алгебры логики

3. Отличие информации от данных

4. Формы адекватности информации и их особенности

5. Меры информации

6. Характеристики для оценки качества информации

7. Виды классификации информации

8. Иерархическую систему классификации

9. Фасетную систему классификации

10. Дескрипторную систему классификации

11. Назначение системы кодирования информации

12. Основные идеи классификационного и регистрационного кодирования

13. Классификацию информации, циркулирующей в организации

## Дополнительные вопросы к отчетам по лабораторным работам

1. Понятие информации.
2. Системы передачи информации.
3. Различные подходы к измерению информации и их применение.
4. Структурные меры информации.
5. Статистический подход к измерению информации.
6. Энтропия и ее свойства.
7. Понятие сигнала и его модели.
8. Основные преобразования сигналов.
9. Информационные характеристики источника сообщений.
10. Основные задачи кодирования.
11. Эффективное кодирование. Теорема Шеннона о кодировании для канала без шума.
12. Код Шеннона-Фано.
13. Код Хаффмана.
14. Помехоустойчивое кодирование. Теорема Шеннона о кодировании для канала с шумом.
15. Код с проверкой четности. Код с тройными повторениями.
16. Код Хэмминга.
17. Информационные характеристики канала связи.
18. Принципы построения криптосистем
19. Уровни криптосистем
20. Компоненты Криптосистем
21. Функции Криптосистем
22. Методы получения “случайности”
23. Архивация. Алгоритмы архивации
24. Генерация ключей. Распределение ключей. Главный ключ.
25. Восстановление системы при компрометации ключей
26. Классификация криптоалгоритмов
27. Симметричные криптоалгоритмы
28. Асимметричные криптоалгоритмы
29. Технология Хэш-функций

**Критерии оценки (в баллах):**

- **25-30 баллов** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов. Студент без затруднений ответил на все дополнительные вопросы.

- **17-24 баллов** выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

- **10-16 баллов** выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- **1-10 баллов** выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос.



## Лабораторные работы

### Примерные варианты лабораторных работ

№	Наименование	Кол-во часов
1	Методы контроля доступа к файлу	3
2	Методы использования аппаратных средств защиты	3
3	Использование средств ограничения доступа	3
4	Методы защиты программ	3
5	Методы работы с большими числами	3
6	Методы генерации больших простых чисел	3
7	Методы работы с RSA	3
8	Моделирование работы с цифровой подписью	3
	<b>Итого</b>	<b>24</b>

#### Описание методики оценивания:

#### Критерии оценки (в баллах):

За отчёт по лабораторной работе

- 7 баллов выставляется студенту, если нет замечаний;
- 5 баллов выставляется студенту, если имеются несущественные замечания;
- 3 баллов выставляется студенту, если в целом получены верные результаты, но имеются существенные замечания.

Приложение № 4

#### Примеры тестовых заданий

##### Тест 1

Тема: «Измерение информации»

1. Какое количество информации по Хартли может содержать система, информационная емкость которой определяется десятичным числом 1250.
2. Найти среднее количество информации по Шеннону в системе со следующим вероятностным распределением  
 $p(1/2; 1/4; 1/4)$
3. Какое максимальное количество информации по Шеннону содержит система со следующим вероятностным распределением  
 $p(0,2; 0,8)$

##### Тест 2

Тема: «Модели сигналов. Преобразование сигналов»

1. Выберите наиболее реальную модель сигнала.

Варианты ответов:

- a) случайный процесс;
- b) детерминированный сигнал;
- c) случайный сигнал.

2. Сколько видов модуляции гармонического сигнала существует?

Варианты ответов:

- a) два;
- b) бесконечно много;
- c) три.

3. Какой спектр имеет периодический сигнал?

Варианты ответов:

- a) сплошной;
- b) линейчатый.

Тест 3

Тема: «Кодирование информации»

1. Что происходит с длиной сообщения при эффективном кодировании?

Варианты ответов:

- c) увеличивается;
- d) остается прежней;
- e) уменьшается.

2. Как изменяется эффективность кода при увеличении длины блока при блоковом кодировании?

Варианты ответов:

- a) не убывает;
- b) не изменяется;
- c) не возрастает.

3. Закодировать сообщение 100110 кодом с проверкой четности.

43

Варианты ответов:

- a) 1001100;
- b) 10011011;
- c) 1001101.

Тест 4

Тема: «Передача информации»

1. Какое устройство системы передачи информации обеспечивает эффективность ее передачи?

Варианты ответов:

- a) модулятор;
- b) кодер источника;
- c) кодер канала.

2. Какое устройство системы передачи информации обеспечивает достоверность ее передачи?

Варианты ответов:

- a) кодер канала;
- b) кодер источника;
- c) модулятор.

3. Что является информационной характеристикой только канала связи?

- a) скорость передачи информации;
- b) пропускная способность.

Тест 5

Тема: «Классификация и кодирование информации»

Вопрос 1.

Система распределения объектов по классам в соответствии с определенным признаком называется . . . .

- a. Кодирование;
- б. Классификация;

в. Классификатор;

г. Реквизит.

Вопрос 2.

Основные методы классификации объектов:

а. Иерархический;

б. Двоичный;

в. Дескрипторный;

г. Фасетный.

Вопрос 3.

Стандарт кодировки, позволяющий закодировать больше символов:

а. КОИ-8;

б. ASCII;

в. ISO;

г. Unicode.

Вопрос 4.

Самая распространённая позиционная система счисления:

а. Римская;

б. Двоичная;

в. Десятичная;

г. Арабская.

Вопрос 5.

Совокупность средств, методов и условий, позволяющих использовать информационные ресурсы, называется ...

а. Информационный рынок;

б. Информационный потенциал;

в. Информационная услуга;

г. Информационный продукт.