

**МИНОБРНАУКИ РОССИИ**

**Ярославский государственный университет им. П.Г. Демидова**

Кафедра интеллектуальных информационных радиофизических систем

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

20 июня 2023 г.

**Рабочая программа дисциплины**

**Теория информации**

Направление подготовки (специальности)

10.05.01 Компьютерная безопасность

Направленность (профиль)

«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена

на заседании кафедры

от 17 апреля 2023 г., протокол № 8

Программа одобрена НМК

физического факультета

протокол № 5 от 25 апреля 2023 г.

## 1. Цели освоения дисциплины

Целью освоения дисциплины «Теория информации» является освоение основных понятий и методов теории информации, от информационного описания сигналов и каналов до физического уровня и требований к аппаратуре для передачи и приёма информации, а также обеспечение понимания у студентов значения информации в современном обществе и формирование навыков поиска и обработки информации по профилю.

## 2. Место дисциплины в структуре ОП специалитета

Дисциплина относится к обязательной части.

Требует знаний, полученных при изучении дисциплин "Математический анализ", "Теория вероятностей и математическая статистика", «Электроника и схемотехника». Знания и навыки, полученные при изучении дисциплины "Электроника и схемотехника", используются обучаемыми при изучении общепрофессиональных и специальных дисциплин.

## 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП специалитета

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
<b>Профессиональные компетенции</b>		
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	ИД_ОПК-3.3 Применяет математический аппарат для решения прикладных и теоретических задач	<b>Знать:</b> – информационные и физические характеристики источников информации и каналов её передачи; – математические модели источников информации и модели каналов передачи информации;  <b>Уметь:</b> – рассчитывать информационные характеристики источников;  <b>Владеть навыками:</b> – численного анализа информационных характеристик дискретных каналов связи.

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости  Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.	Общие сведения о системах передачи информации	6	5	3		1		14	Тестирование, тест- диктант, задания для самостоятельной работы
2.	Математические модели сообщений, сигналов и помех	6	5	2		1		9	Тестирование, тест- диктант, задания для самостоятельной работы
3.	Информационные характеристики источников	6	5	3		1		6	Тестирование, тест- диктант, задания для самостоятельной работы
4.	Математические модели каналов передачи информации	6	5	2		1		7	Тестирование, тест- диктант, задания для самостоятельной работы
5.	Количество информации и пропускная способность	6	6	4		0,5		9	Тестирование, тест- диктант, задания для самостоятельной работы
6.	Основы теории кодирования	6	6	2		0,5		9,7	Тестирование, тест- диктант, задания для самостоятельной работы
		6					0,3		Зачет
	Всего		32	16		5	0,3	54,7	

Содержание разделов дисциплины

##### Тема №1. Общие сведения о системах передачи информации

Сообщения, их источники и получатели. Сигнал как носитель сообщения. Сообщение и информация. Основные параметры сигналов: длительность, ширина спектра и динамический диапазон. Система связи и канал связи. Структурная схема системы связи.

Дискретные и непрерывные каналы, их основные характеристики. Физические принципы передачи и приёма информации. Дискретизация и квантование непрерывных сообщений. Теорема Котельникова. Условия восстановления аналогового сигнала по дискретизированному. Кодирование. Модуляция. Структурная схема системы передачи дискретных сообщений, модем и кодек. Передача непрерывных сообщений. Демодуляция и декодирование. Решающее устройство.

## **Тема №2. Математические модели сообщений, сигналов и помех**

Классификация сигналов и сообщений. Детерминированные и случайные процессы. Математические модели детерминированных сигналов. Помехи и искажения в каналах. Аддитивные и мультипликативные помехи. Классификация помех по физическим свойствам и происхождению. Характеристики случайных процессов (СП). Стационарные и нестационарные СП. Эргодическое свойство стационарных СП. Особенности нестационарных процессов. Функции корреляции и их свойства. Процесс с равномерной функцией плотности вероятности. Гауссовский СП. Спектр плотности мощности и его связь с функцией корреляции (теорема Винера–Хинчина). Понятие белого шума. Квазигладкий шум, его функция корреляции. Эффективная ширина спектра.

## **Тема № 3. Информационные характеристики источников**

Количественная мера информации дискретного источника. Энтропия как мера неопределенности сообщений, основные свойства энтропии. Собственная информация источника. Энтропия источника без памяти при равновероятном и неравновероятном выборе символов. Избыточность и производительность источника. Условная энтропия и её свойства. Количественная мера информации непрерывного источника. Дифференциальная энтропия. Дифференциальная энтропия равномерного и гауссовского источника. Аддитивный белый гауссовский шум (АБГШ) как наилучший тестовый помеховый сигнал. Измерительная информация. Определение энтальпии непрерывного сигнала. Энтальпия-производительность непрерывного источника. Кодирование в непрерывных каналах. Теоремы оптимального кодирования для канала с помехами.

## **Тема №4. Математические модели каналов передачи информации**

Классификация каналов передачи информации. Стационарные, нестационарные, с памятью и без. Модели непрерывных каналов. Идеальный канал без помех, канал с аддитивным гауссовым шумом. Канал с неопределенной фазой сигнала, однолучевый канал с замираниями. Канал с межсимвольной интерференцией и аддитивным шумом. Многолучевое распространение. Модель многолучевого распространения. Случайные линейные каналы и их характеристики, особенности проводных и радиоканалов, замирания сигналов. Модели дискретного канала. Симметричный и несимметричный каналы без памяти, канал со стиранием. Дискретные каналы с памятью. Марковский канал. Канал Гильберта. Модели формирования вероятности ошибки при передаче 1 символа сообщения для каналов с памятью и без памяти. Биномиальная модель. Модель Пуассона. Причины наличия памяти у канала.

## **Тема № 5. Количество информации и пропускная способность**

Взаимная информация – количество информации на выходе дискретного канала относительно его входа. Свойства взаимной информации. Скорость передачи информации по дискретному каналу. Информационная ёмкость и пропускная способность дискретного канала связи. Пропускная способность двоичных каналов. Зависимость пропускной способности канала от алфавита канальных символов. Теорема Шеннона о передаче по каналу без помех. Теорема о свойстве асимптотической равновероятности. Типичные последовательности. Основная теорема Шеннона. Минимальная длина кода.

Максимальная скорость передачи. Обмен между верностью, задержкой и эффективностью системы. Количество информации в непрерывном канале. Информационная ёмкость непрерывного канала, её зависимость от частоты. Формула Шеннона. Возможность обмена полосы пропускания на мощность сигнала. Сравнение пропускной способности дискретных и непрерывных каналов.

#### **Тема № 6. Основы теории кодирования**

Классификация методов кодирования. Избыточность и относительная скорость кода. Проблема согласования источника сообщений с каналом. Примитивное (безыбыточное) кодирование. Принципы статистического кодирования. Код Фано-Шеннона. Принципы помехоустойчивого кодирования. Кодовое расстояние. Систематические линейные коды. Декодирование линейных кодов. Проверочные матрицы. Коды Хемминга. Блочные корректирующие коды. Обнаружение и исправление ошибок. Циклические коды. Коды БЧХ, коды Рида-Соломона. Сверточные (решетчатые) коды (СК). Кодирование в каналах с памятью. Декорреляция ошибок методом перемежения символов, применение циклических и сверточных кодов. Понятие об итеративных и каскадных кодах. Граница Симмонса. Неравенство Крафта. Предельные возможности помехоустойчивого кодирования. Эффективное кодирование дискретных сообщений. Сжатие сообщений. Метод Лемпела-Зива. Укрупнение алфавита и неравномерное кодирование.

### **5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине**

В процессе обучения проводятся лекции, практические и лабораторные занятия, в ходе которых используются следующие типы занятий и образовательные технологии.

**Вводная лекция** - ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция** (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

**Консультации** – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

**Электронный учебный курс «Теория информации» в LMS Электронный университет Moodle ЯрГУ**, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;

- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- представлены тексты/видеозаписи лекций по отдельным темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

#### **6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса по дисциплине используются:

– для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

– Microsoft Office (Microsoft Office Std 2013 OfficeSTD 2013 RUS OLP NL Acdmc 021-10232 Microsoft Open License №0005279522 Лицензионный договор №Л - 1703 от 10/12/2013; акт №1647 от 26/12/2013);

- Adobe Acrobat Reader.

#### **7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT»  
[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)

#### **8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины**

##### **а) основная литература**

1. Зверева Е.Н. Сборник примеров и задач по основам теории информации и кодирования сообщений [Электронный ресурс] / Е.Н. Зверева, Е.Г. Лебедько. -СПб. : Университет ИТМО, 2014. - 76 с. - 2227-8397. - Режим доступа: <http://www.iprbookshop.ru/68114.html>
1. Белов В.М., Новиков С.Н., Солонска О.И. Теория информации. Курс лекций: учебное пособие для вузов. – М.: Горячая линия - Телеком, 2012. – 143с. URL: <https://www.studentlibrary.ru/book/ISBN9785991202374.html>
2. Санников В.Г. Теория информации и кодирования [Электронный ресурс] : учебное пособие / В.Г. Санников. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 95 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/61558.html>

##### **б) дополнительная литература**

1. Кудряшов Б.Д. Теория информации. – С.-Пб.: Питер, 2009. – 320 с.

- URL: [http://lib.uniyar.ac.ru/opac/bk\\_cat\\_card.php?rec\\_id=1219156&cat\\_cd=YARSU](http://lib.uniyar.ac.ru/opac/bk_cat_card.php?rec_id=1219156&cat_cd=YARSU)
2. Галлагер Р. Теория информации и надежная связь. – М.: Советское радио, 1974. – 719 с.  
URL: [http://lib.uniyar.ac.ru/opac/bk\\_cat\\_card.php?rec\\_id=331003&cat\\_cd=YARSU](http://lib.uniyar.ac.ru/opac/bk_cat_card.php?rec_id=331003&cat_cd=YARSU)
3. Котоусов А.С. Теория информации. – М.: Радио и связь, 2003. – 80 с.  
URL: [http://lib.uniyar.ac.ru/opac/bk\\_cat\\_card.php?rec\\_id=318174&cat\\_cd=YARSU](http://lib.uniyar.ac.ru/opac/bk_cat_card.php?rec_id=318174&cat_cd=YARSU)

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

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);
- учебные аудитории для проведения лабораторных работ;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочим программам дисциплин.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся. группа обучающихся делится на две подгруппы).

Учебно-методическое обеспечение, необходимое для осуществления образовательного процесса по дисциплине включает в свой состав:

Авторы:

Доцент кафедры инфокоммуникаций и радиофизики, к.ф.-м.н. \_Т.К. Артёмова

Доцент кафедры инфокоммуникаций и радиофизики, к.ф.-м.н. А.С. Гвоздарёв

**Приложение №1 к рабочей программе дисциплины  
«Теория информации»**

**Фонд оценочных средств  
для проведения текущей и промежуточной аттестации студентов  
по дисциплине**

**1. Типовые контрольные задания или иные материалы,  
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,  
характеризующих этапы формирования компетенций**

**1.1 Контрольные задания и иные материалы,  
используемые в процессе текущей аттестации**

**Задания для самостоятельной работы**

**Задание по теме №1 «Общие сведения о системах передачи информации» –  
Домашнее задание №1**

1) Подготовить аргументированное 3-х-минутное выступление со ссылками на источники (например, наименование статьи, её авторы и выходные данные) и агрегаторы (база данных, электронная библиотека, отделение университетской библиотеки) информации на тему «Значение информации в развитии современного общества».

Возможные направления развития темы:

- объёмы информации, наработанной человечеством, к настоящему времени;
- информационные потребности современного общества – общая характеристика;
- информационные потребности в образовании;
- информационные потребности в науке;
- информационные потребности промышленности;
- информационные потребности социума;
- информационные потребности современного члена общества;
- механизмы распространения информации разными субъектами информационного обмена;
- технологии хранения информации;
- технологии обработки информации;
- современные потребности в скоростях передачи информации;
- современные потребности в объёмах передаваемой информации;
- современные требования к качеству информации;
- охрана информации в современном обществе;
- регуляция потоков информации со стороны государства;
- регуляция потоков информации со стороны основных участников информационного обмена.

2) Выступить на семинаре и ответить на вопросы товарищей.

**Задание по теме №2 «Математические модели сообщений, сигналов и помех» –  
Домашнее задание №2**

Решить задачи №1, 3, 4, 7 со стр. 39 сборника задач «Сборник примеров и задач по основам теории информации и кодирования сообщений» / Зверева Е.Н., Лебедько Е.Г.; СПб: НИУ ИТМО, 2014. – 76 с., рекомендованного в списке литературы.



**Задания по теме № 3 «Информационные характеристики источников» – Домашнее задание №3**

Решить задачи №2, 6, 7 со стр. 21 сборника задач «Сборник примеров и задач по основам теории информации и кодирования сообщений» / Зверева Е.Н., Лебедько Е.Г.; СПб: НИУ ИТМО, 2014. – 76 с., рекомендованного в списке литературы.

**Задания по темам № 4 «Математические модели каналов передачи информации» и №5 «Количество информации и пропускная способность» – Домашнее задание №4**

Решить задачи №2, 3 со стр. 15 и №2, 5, 7 со стр. 31 сборника задач «Сборник примеров и задач по основам теории информации и кодирования сообщений» / Зверева Е.Н., Лебедько Е.Г.; СПб: НИУ ИТМО, 2014. – 76 с., рекомендованного в списке литературы.

**Задания по теме № 6 «Основы теории кодирования» – Домашнее задание №5**

Решить задачи №1, 3, 5 со стр. 48; №1, 3 со стр. 57; №1-3 со стр. 63 сборника задач «Сборник примеров и задач по основам теории информации и кодирования сообщений» / Зверева Е.Н., Лебедько Е.Г.; СПб: НИУ ИТМО, 2014. – 76 с., рекомендованного в списке литературы.

**Задания по теме №7 «Принципы многоканальной связи и распределения информации» – Домашнее задание №6**

1) Подготовить аргументированное 3-х-минутное выступление со ссылками на источники и агрегаторы информации на тему «Современные информационные и информационно-коммуникационные системы».

Возможные направления развития темы:

- мировые информационные системы;
- международные агрегаторы научных публикаций;
- российские агрегаторы научных публикаций;
- электронные библиотечные системы издательств, университетов, библиотек;
- сети беспроводной передачи речи (радиотелефония);
- сети беспроводной передачи мультимедийной информации;
- сети теле- и радиовещания;
- сети проводной телефонии;
- телеграфные сети;
- сети спутниковой связи с геостационарными спутниками;
- сети спутниковой связи с негеостационарными спутниками;
- самоорганизующиеся сети;
- коммуникационные мини-сети предприятий;
- компьютерные сети предприятий.

В ходе выступления требуется отразить следующие аспекты темы:

- одноканальная это система или многоканальная;
- как обеспечивается доступ абонентов в сеть;
- в каком из режимов работает сеть;
- если режим дуплексный, то как он технически обеспечивается;
- как обеспечивается одновременность доступа нескольких абонентов в сеть;
- открытый или закрытый канал используется;
- какая из моделей каналов наиболее пригодна для описания линии передачи информации;
- каковы параметры задействованных физических сигналов;
- какова структура сети;
- есть ли особые узлы и какие они имеют особенности;
- как организовано управление сетью;
- базы данных сосредоточенные или распределённые;

- каковы на сегодняшний день технические возможности такой сети (пропускная способность, объём хранимой информации, задержки при передаче информации;
- есть ли разница в технических возможностях связи между направлениями передачи информации.

2) Выступить на семинаре (практически это 3 слайда с перечнем фактов и цифр, являющихся очень краткими ответами на вышеизложенные вопросы) и ответить на вопросы товарищей.

### Примерные материалы для тест-диктантов

#### Тест-диктант №1

№ задания	Задание
1	Напишите формулу для тригонометрической формы ряда Фурье
2	Напишите формулу для прямого преобразования Фурье
3	Какова размерность спектральной плотности тока?
4	Какова размерность спектра периодического напряжения?
5	Прямоугольный импульс длительности 1 мс и амплитуды 1 В. Определите ширину спектра по первым нулям.
6	Прямоугольный импульс длительности 1 мс и амплитуды 1 В. Определите величину постоянной составляющей в спектре сигнала.
7	Дайте определение стационарного случайного процесса
8	Дайте определение эргодического случайного процесса

#### Тест-диктант №2

№ задания	Задание
1	Символы алфавита $z_1, z_2, z_3, z_4, z_5, z_6$ имеют вероятности 0,3 0,25 0,2 0,15 0,06 0,04 соответственно. Построить алфавит кода методом Шеннона-Фано
2	Каково максимальное значение энтропии двоичного источника?
3	Запишите формулу для количества информации, передаваемого по каналу связи
4	Канал имеет полосу пропускания 100 кГц, динамический диапазон около 30 дБ. Определите его пропускную способность
5	Назовите 2 причины уменьшения энтропии у источника
6	Приведите пример двоичного канала со стиранием
7	У каких каналов пропускная способность выше при прочих равных условиях – у дискретных или у непрерывных каналов?
8	Какова функция корреляции белого шума?

#### Тест-диктант №3

№ задания	Задание
1	Источник работает со скоростью 10 Мбит/с. Какова должна быть пропускная способность канала без помех, чтобы удовлетворить условиям теоремы Шеннона?
2	Как влияет повышение разрядности АЦП на качество восстановления сигнала без шума?
3	Вещательный источник распределяет нагрузку между двумя каналами. С какой скоростью работает источник, если пропускная способность каналов 1 Мбит/с и 10 Мбит/с?
4	Как влияет повышение разрядности АЦП на качество восстановления сигнала при фиксированном уровне шума?

## **1.2 Список вопросов и (или) заданий по разделу №1 теме для проведения промежуточной аттестации**

### **Список вопросов к зачёту**

1. Сообщения, сигналы, информация. Основные параметры сигналов: длительность, ширина спектра и динамический диапазон.
4. Система связи и канал связи. Структурная схема системы связи. Физические принципы передачи и приёма информации.
5. Дискретизация и квантование непрерывных сообщений. Теорема Котельникова. Условия восстановления аналогового сигнала по дискретизированному.
6. Модуляция. Принцип импульсно-кодовой модуляции. Методы формирования и детектирования сигналов амплитудной, частотной, фазовой, импульсной модуляции.
7. Понятие синхронизации и принципы ее обеспечения в системах электросвязи. Симплексный, полудуплексный и дуплексный режимы связи. Основные характеристики систем передачи информации: помехоустойчивость и скорость передачи. Пропускная способность системы передачи информации.
8. Классификация сигналов и сообщений. Детерминированные и случайные процессы. Математические модели детерминированных сигналов.
9. Помехи и искажения в каналах. Аддитивные и мультипликативные помехи. Классификация помех по физическим свойствам и происхождению.
10. Характеристики случайных процессов (СП). Стационарные и нестационарные СП. Эргодическое свойство стационарных СП. Особенности нестационарных процессов. Функции корреляции и их свойства.
11. Процесс с равномерной функцией плотности вероятности. Гауссовский СП.
12. Спектр плотности мощности и его связь с функцией корреляции (теорема Винера–Хинчина). Понятие белого шума. Квазيبелый шум, его функция корреляции. Эффективная ширина спектра. Дискретизация случайных процессов. Разложение Карунева-Лозва.
13. Случайные последовательности. Марковские сигналы. Цепь Маркова. Гауссовские марковские процессы.
14. Модели речевых, телевизионных, телеграфных и факсимильных сообщений.
15. Энтропия дискретного источника, основные свойства энтропии. Энтропия источника без памяти при равновероятном и неравновероятном выборе символов. Избыточность и производительность источника.
16. Условная энтропия и её свойства. Энтропия объединения источников. Примеры.
17. Количественная мера информации непрерывного источника. Дифференциальная энтропия. Дифференциальная энтропия равномерного и гауссовского источника. Аддитивный белый гауссовский шум (АБГШ) как наилучший тестовый помеховый сигнал.
18. Измерительная информация. Определение эpsilon-энтропии непрерывного сигнала. Эpsilon-производительность непрерывного источника.
19. Кодирование в непрерывных каналах. Теоремы оптимального кодирования для канала с помехами.
20. Классификация каналов связи. Стационарные, нестационарные, с памятью и без. Модели непрерывных каналов. Идеальный канал без помех, канал с аддитивным гауссовым шумом. Канал с неопределенной фазой сигнала, однолучевый канал с замираниями. Канал с межсимвольной интерференцией и аддитивным шумом.
21. Многолучевое распространение. Модель многолучевого распространения. Случайные линейные каналы и их характеристики, особенности проводных и радиоканалов, замирания сигналов.

22. Флуктуационные, сосредоточенные и импульсные помехи, их вероятностные характеристики.
23. Модели дискретного канала. Симметричный и несимметричный каналы без памяти, канал со стиранием.
24. Дискретные каналы с памятью. Марковский канал. Канал Гильберта.
25. Модели формирования вероятности ошибки при передаче 1 символа сообщения для каналов с памятью и без памяти. Биномиальная модель. Модель Пуассона. Причины наличия памяти у канала.
26. Модели волоконно-оптических каналов связи. Квантовый шум. Распределение фонового излучения на выходе фотодетектора и смеси сигнала с фоновым излучением. Пуассоновский процесс для описания потока событий. Экспоненциальная модель для интервала между событиями в телекоммуникационной системе.
27. Взаимная информация – количество информации на выходе дискретного канала относительно его входа. Свойства взаимной информации. Скорость передачи информации по дискретному каналу.
28. Информационная ёмкость и пропускная способность дискретного канала связи. Пропускная способность двоичных каналов. Зависимость пропускной способности канала от алфавита канальных символов.
29. Теорема Шеннона о передаче по каналу без помех. Теорема о свойстве асимптотической равновероятности. Типичные последовательности. Основная теорема Шеннона. Минимальная длина кода. Максимальная скорость передачи. Обмен между верностью, задержкой и эффективностью системы.
30. Количество информации в непрерывном канале. Информационная ёмкость непрерывного канала, её зависимость от частоты. Формула Шеннона. Возможность обмена полосы пропускания на мощность сигнала. Сравнение пропускной способности дискретных и непрерывных каналов.
31. Классификация методов кодирования. Избыточность и относительная скорость кода. Проблема согласования источника сообщений с каналом. Прimitивное (безыбыточное) кодирование.
32. Принципы статистического кодирования. Код Фано-Шеннона.
33. Принципы помехоустойчивого кодирования. Кодовое расстояние. Систематические линейные коды. Декодирование линейных кодов. Проверочные матрицы.
34. Коды Хемминга. Блочные корректирующие коды. Обнаружение и исправление ошибок. Циклические коды. Коды БЧХ, коды Рида-Соломона. Сверточные (решетчатые) коды (СК).
35. Кодирование в каналах с памятью. Декорреляция ошибок методом перемежения символов, применение циклических и сверточных кодов.
36. Понятие об итеративных и каскадных кодах. Граница Симмонса. Неравенство Крафта. Предельные возможности помехоустойчивого кодирования.
37. Эффективное кодирование дискретных сообщений. Сжатие сообщений. Метод Лемпела-Зива. Укрупнение алфавита и неравномерное кодирование.

### Задание для тестового контроля

*Впишите в правом столбце под номером букву, соответствующую верному из ответов*

<b>1. Источник, у которого удельная энтропия максимальна</b> а) двоичный с равновероятными независимыми символами б) непрерывный в) 4-ичный с неравновероятными символами г) 4-ичный в равновероятными независимыми символами	1.
<b>2. Формула для энтропии дискретного источника символов естественного языка</b> а) $H = I(Y) - I(Y X)$ б) $H = n \log_2 m$ в) $H = -\sum_i p(x_i) \log_2 p(x_i)$ г) $H = I(X,Y)/T$	2.

<b>3. Энтропия дискретного источника с равновероятными независимыми символами при размере алфавита 32</b> а) 2 бит/симв                      б) 5 бит/симв                      в) 10 бит/симв                      г) 4 бит/симв	3.
<b>4. Причины уменьшения энтропии источника по сравнению с максимально возможным значением</b> а) уменьшение мощности                      в) искажения б) нелинейность источника                      г) разная вероятность символов	4.
<b>5. Источник выдаёт 600 симв/мин. Техническая скорость источника</b> а) 60 Бод                      б) 100 Бод                      в) 10 Бод                      г) 600 Бод	5.
<b>6. Техническая скорость источника 50 Бод, удельная энтропия 3 бит/симв. Какое количество информации выдаёт источник за время 3 с?</b> а) 50 бит                      б) 450 бит                      в) 150 бит                      г) 750 бит	6.
<b>7. Ширина спектра сигнала при длительности кодовых символов 1 мкс равна</b> а) 2 кГц                      б) 1 кГц                      в) 1 МГц                      г) 2 МГц	7.
<b>8. Какой ширины полосы требуется канал передачи информации, если длительность символов источника 1 мс и используется 8-символьный код?</b> а) 8 кГц                      б) 2 кГц                      в) 16 кГц                      г) 4 кГц	8.
<b>9. Рекомендации по частоте дискретизации для сигнала с верхней частотой в спектре 10 кГц</b> а) не ниже 20 кГц                      б) не выше 10 кГц                      в) не ниже 10 кГц                      г) не выше 20 кГц	9.
<b>10. Рекомендуемое число уровней квантования для сигнала с максимальной мощностью 1 мВт принимаемого на фоне шумов 1 мкВт</b> а) от 1000                      б) от 1001                      в) не более 1000                      г) не более 1001	10.
<b>11. Какова производительность источника, имеющего в составе 8-ми-разрядный АЦП с частотой дискретизации 40 кГц?</b> а) 5 кбит/с                      б) 320 кбит/с                      в) 312,5 кбит/с                      г) 4,88 кбит/с	11.
<b>12. Энтропия двоичного источника с символами, имеющими вероятности 0,1 и 0,9</b> а) -1,454 бит                      б) -0,469 бит                      в) 0,469 бит                      г) 1,454 бит	12.
<b>13. Двоичные источники X, Y, Z имеют вероятности появления символов: X(0,5 0,5), Y(0,3 0,7) Z(0,2 0,8). Их энтропии соотносятся</b> а) $H(X) > H(Y) > H(Z)$ б) $H(X) < H(Y) < H(Z)$ в) $H(Z) > H(X) > H(Y)$ г) $H(Y) > H(Z) > H(X)$	13.
<b>14. Канал, вход которого – вход АЦП, а выход – выход ЦАП, -</b> а) непрерывно-дискретный                      в) дискретно-непрерывный б) цифровой                      г) аналоговый (непрерывный)	14.
<b>15. Если в секунду энтропия принятого сигнала 128 бит, а помехи 28 бит, то пропускная способность канала</b> а) 100 бит/с                      б) 156 бит/с                      в) 128 бит/с                      г) 4,57 бит/с	15.
<b>16. Провайдер протянул канал на 600 Мбит/с в подъезд. Максимальная гарантированная скорость в трёх пользующихся Интернетом одновременно квартирах</b> а) 600 Мбит/с                      б) 199,99 Мбит/с                      в) 200 Мбит/с                      г) 599,99 Мбит/с	16.
<b>17. Восстановите матрицу условных вероятностей двоичного канала</b> а) $\begin{pmatrix} 0,1 & 0,8 \\ 0,9 & 0,2 \end{pmatrix}$ б) $\begin{pmatrix} 0,1 & 0,9 \\ 0,8 & 0,2 \end{pmatrix}$ в) $\begin{pmatrix} 0,1 & 0,5 \\ 0,5 & 0,2 \end{pmatrix}$ г) $\begin{pmatrix} 0,1 & 0 \\ 0 & 0,2 \end{pmatrix}$	17.
<b>18. Канал в задании №17</b> а) двоичный симметричный со стиранием                      в) двоичный несимметричный без помех б) двоичный Гильберта                      г) двоичный несимметричный	18.
<b>19. Проводные цифровые линии связи чаще всего описываются моделью канала</b> а) двоичный симметричный со стиранием                      в) двоичный несимметричный без помех б) двоичный Гильберта                      г) двоичный несимметричный без памяти	19.
<b>20. Сотовая связь или Wi-Fi чаще всего описываются моделью канала</b> а) двоичный симметричный со стиранием                      в) двоичный несимметричный без помех б) двоичный Гильберта                      г) двоичный несимметричный без памяти	20.
<b>21. Наиболее болезненная в общем случае помеха</b> а) «соль»                      б) АБГШ                      в) «перец»                      г) шум Пуассона	21.

<b>22. Спектральная плотность мощности помехи 2 нВт/Гц. Её мощность в приёмнике с эффективной шумовой полосой 20 кГц</b> а) 40 мкВт                      б) 20 мкВт                      в) 2000 мкВт                      г) 80 мкВт	22.
<b>23. Как проявится широкополосная помеха 1 мкВт с полосой 1МГц в узкополосном приёмнике с полосой пропускания 10 кГц?</b> а) 0,1 мкВт                      б) 0,2 мкВт                      в) 10 нВт                      г) 5 нВт	23.
<b>24. Сравните ёмкости трёх каналов: а – двоичный, б – 16-ричный, с - непрерывный</b> а) $C(c) < C(b) < C(a)$ б) $C(c) > C(b) > C(a)$ в) $C(b) > C(c) > C(a)$ г) $C(a) > C(c) > C(b)$	24.
<b>25. Интервал между поступлениями спама в почтовый ящик описывается распределением</b> а) равномерным                      б) гауссовским                      в) экспоненциальным                      г) Пуассона	25.
<b>26. Ошибка округления напряжения цифрового вольтметра имеет равномерное распределение от <math>-c/2</math> до <math>c/2</math>, где цена деления <math>c=1</math> мкВ. Математическое ожидание и дисперсия ошибки:</b> а) 0,5 мкВ; 1 мкВ <sup>2</sup> б) 0 мкВ; 0,25 мкВ <sup>2</sup> в) 0 мкВ; 1/12 мкВ <sup>2</sup> г) 0,5 мкВ; 12 мкВ <sup>2</sup>	26.
<b>27. Вероятность того, что ошибка округления не превзойдёт четверти цены деления по модулю для вольтметра из №26</b> а) 0,25                      б) 0,5                      в) 0,75                      г) 1	27.
<b>28. Значение автокорреляционной функции некоторого случайного процесса при нулевом сдвиге равно 10. Средняя мощность процесса (в Вт)</b> а) 20                      б) 5                      в) 10                      г) 100	28.
<b>29. Расстояние Хэмминга между кодами (1 1 1 -1 -1 -1) и (1 -1 1 -1 1 -1)</b> а) 1                      б) 0                      в) 3                      г) 2	29.
<b>30. Число атак на сервер в единицу времени описывается распределением</b> а) равномерным                      б) гауссовским                      в) экспоненциальным                      г) Пуассона	30.

### Правила выставления оценки на зачете.

Изучение дисциплины заканчивается зачетом. Во время подготовки к зачету предусмотрена групповая консультация.

Билет для зачета состоит из двух теоретических вопросов по материалам курса.

1. Теоретический вопрос в билете оценивается в 3 балла:

- 3 балла, если вопрос раскрыт более чем на 90% от требуемого объема. При этом студент демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом; осуществляет межпредметные связи; умеет связывать теорию с практикой. Дает развернутые, полные и четкие ответы на вопрос билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.
- 2 балла, если вопрос раскрыт более чем на 70%, но менее, чем на 90% от требуемого объема. При этом ответ в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.
- 1 балл, если вопрос раскрыт более чем на 50%, но менее чем на 70% от требуемого объема. При этом студент демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагается в терминологически корректно, но допускаются ошибки в определениях и раскрытии некоторых основных понятий, формулировке положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Итоговая оценка высчитывается исходя из суммарного балла за оба вопроса билета.

В результате для получения оценки «зачтено» необходимо, чтобы суммарный балл был не ниже 4.

## **Приложение №2 к рабочей программе дисциплины «Теория информации»**

### **Методические указания для студентов по освоению дисциплины**

Основной формой занятий по дисциплине «Защита информации в беспроводных сетях» являются лекции и практические занятия. На лекциях излагается необходимый минимум теоретических сведений, ставятся вопросы, на которые надо найти ответ самостоятельно, даются рекомендации по подбору литературы, даются отсылки к нормативной базе. Теоретический материал представляет собой компиляцию из огромного количества источников, поэтому материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и дополнять информацией, полученной из учебной и научной литературы.

На практических занятиях отрабатываются полученные знания, разбираются практические ситуации, приобретаются практические знания по работе с реальным оборудованием.

Для успешного освоения дисциплины обязательно выполнение всех домашних заданий, они являются формой текущей аттестации. В качестве заданий для самостоятельной работы дома предлагаются задания, аналогичные разобранным на практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых заданий. Некоторые задания относятся к категории заданий повышенной сложности, они подразумевают применение вычислительной техники с математическими пакетами, например, Matematica, MathCad, MATLAB, R, Stetistica или их бесплатных, свободно распространяемых аналогов, например, Octave, SciLAB, FreeMat и других или онлайн-вычислений (пользуйтесь любым удобным Вам способом). По окончании практического курса проводится контрольная работа, включающая в себя задания, интегрирующие множество мелких освоенных задач в один расчётный проект.