**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# Теория информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **2**
Семестр: **3**
Учебный план набора 2013 года

Распределение рабочего времени

| № | Виды учебной деятельности | 3 семестр | Всего | Единицы |
|---|---|---|---|---|
| 1 | Лекции | 16 | 16 | часов |
| 2 | Практические занятия | 24 | 24 | часов |
| 3 | Всего аудиторных занятий | 40 | 40 | часов |
| 4 | Из них в интерактивной форме | 20 | 20 | часов |
| 5 | Самостоятельная работа | 32 | 32 | часов |
| 6 | Всего (без экзамена) | 72 | 72 | часов |
| 7 | Общая трудоемкость | 72 | 72 | часов |
| | | 2.0 | 2.0 | З.Е |

Зачет: 3 семестр

Томск 2017

Согласована на портале № 17385

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «16» 2 2017 г.

# ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент каф. РТС _____ В. А. Бутько

Заведующий обеспечивающей каф.
РТС _____ С. В. Мелихов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. С. Задорин

Эксперты:

старший преподаватель каф. РТС _____ Д. О. Ноздреватых

Согласована на портале № 17385

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов знаний, умений и навыков, позволяющих самостоятельно проводить математическое моделирование процессов хранения, преобразования и передачи информации, оценивать предельные и реальные возможности пропускной способности и помехоустойчивости информационных систем.

### 1.2. Задачи дисциплины

– освоение основных понятий теории информации и математических методов количественного описания информации;

– овладение методами оптимального и помехоустойчивого кодирования в системах хранения, передачи и обработки информации;

– изучение принципов и основных методов защиты информации от несанкционированного доступа.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Теория информации» (Б1.Б.13) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Алгебра и геометрия, Информатика, Математический анализ.

Последующими дисциплинами являются: Криптографические методы защиты информации, Математические основы криптологии, Основы информационной безопасности, Сети и системы передачи информации.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

В результате изучения дисциплины студент должен:

– **знать** основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды; математические методы количественного описания информации; математические модели и информационные характеристики источников сообщений и каналов передачи информации; основные понятия и методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи; принципы и основные методы защиты информации от несанкционированного доступа;

– **уметь** строить математические модели информационных систем и процессов; вычислять теоретико-информационные характеристики источников сообщений и каналов передачи информации; применять на практике методы эффективного и помехоустойчивого кодирования;

– **владеть** основами построения математических моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры |
|---|---|---|
| | | 3 семестр |
| Аудиторные занятия (всего) | 40 | 40 |
| Лекции | 16 | 16 |
| Практические занятия | 24 | 24 |
| Из них в интерактивной форме | 20 | 20 |
| Самостоятельная работа (всего) | 32 | 32 |

Согласована на портале № 17385

| | | |
|---|---|---|
| Подготовка к контрольным работам | 3 | 3 |
| Проработка лекционного материала | 7 | 7 |
| Подготовка к практическим занятиям, семинарам | 22 | 22 |
| Всего (без экзамена) | 72 | 72 |
| Общая трудоемкость ч | 72 | 72 |
| Зачетные Единицы | 2.0 | 2.0 |

## 5. Содержание дисциплины

### 5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лекции | Практические занятия | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|
| 3 семестр | | | | | |
| 1 Основные понятия теории информации | 4 | 4 | 4 | 12 | ОПК-4 |
| 2 Кодирование источника | 3 | 6 | 9 | 18 | ОПК-4 |
| 3 Помехоустойчивое кодирование | 7 | 12 | 16 | 35 | ОПК-4 |
| 4 Основы теории защиты информации | 2 | 2 | 3 | 7 | ОПК-4 |
| Итого за семестр | 16 | 24 | 32 | 72 | |
| Итого | 16 | 24 | 32 | 72 | |

### 5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины по лекциям | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 3 семестр | | | |
| 1 Основные понятия теории информации | Информация, сообщения, сигналы. Системы передачи, хранения и распределения информации. Математические модели дискретных сообщений. Количественная мера информации. Собственная информация. Условная собственная информация. Энтропия. Условная энтропия и взаимная информация. Модели каналов. Скорость передачи информации. Пропускная способность дискретных каналов. | 4 | ОПК-4 |

Согласована на портале № 17385

| | | | |
|---|---|---|---|
| | Итого | 4 | |
| 2 Кодирование источника | Основные понятия теории кодирования информации. Избыточность, её роль при передаче информации. Теоремы Шеннона о кодировании в дискретном канале без помех. Оптимальное эффективное кодирование. Коды Шеннона-Фано и Хаффмана. Блоковое кодирование. Коды Лемпела-Зива. | 3 | ОПК-4 |
| | Итого | 3 | |
| 3 Помехоустойчивое кодирование | Модель канала передачи информации с помехами. Принципы помехоустойчивого кодирования. Теоремы Шеннона о кодировании в дискретном канале с помехами. Корректирующие свойства кодов. Кодовое расстояние. Обнаружение и исправление ошибок. Классификация кодов. Линейные блочные коды. Матричное описание кодов. Систематические линейные коды. Кодирование и декодирование линейных кодов. Коды Хэмминга. Циклические коды: порождающий полином, способы кодирования и декодирования. Коды БЧХ и Рида-Соломона. Сверточное кодирование. | 7 | ОПК-4 |
| | Итого | 7 | |
| 4 Основы теории защиты информации | Обобщенная модель системы передачи и хранения информации. Цели шифрования. Элементы криптографии. Симметричные и несимметричные системы шифрования. Основные способы шифрования. Электронная подпись. | 2 | ОПК-4 |
| | Итого | 2 | |
| Итого за семестр | | 16 | |

**5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами**

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Предшествующие дисциплины | | | | |
| 1 Алгебра и геометрия | + | + | + | + |
| 2 Информатика | + | + | | |
| 3 Математический анализ | + | + | + | + |

Согласована на портале № 17385

| Последующие дисциплины | | | | |
|---|---|---|---|---|
| 1 Криптографические методы защиты информации | + | + | + | + |
| 2 Математические основы криптологии | + | + | + | + |
| 3 Основы информационной безопасности | + | + | + | + |
| 4 Сети и системы передачи информации | + | + | + | + |

**5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий**

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

| Компетенции | Виды занятий | | | Формы контроля |
|---|---|---|---|---|
| | Лекции | Практические занятия | Самостоятельная работа | |
| ОПК-4 | + | + | + | Контрольная работа, Домашнее задание, Опрос на занятиях, Зачет, Выступление (доклад) на занятии |

## 6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

| Методы | Интерактивные практические занятия | Интерактивные лекции | Всего |
|---|---|---|---|
| 3 семестр | | | |
| Работа в команде | 12 | | 12 |
| Презентации с использованием слайдов с обсуждением | | 8 | 8 |
| Итого за семестр: | 12 | 8 | 20 |
| Итого | 12 | 8 | 20 |

## 7. Лабораторные работы

Не предусмотрено РУП

## 8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Согласована на портале № 17385

Таблица 8. 1 – Наименование практических занятий (семинаров)

| Названия разделов | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 3 семестр | | | |
| 1 Основные понятия теории информации | Определения информации. Элементы теории вероятностей. Модель дискретного источника сообщений. Количественные меры информация. Энтропия источника дискретных сообщений. Избыточность источника. Производительность источника. Скорость передачи информации. Пропускная способность дискретных каналов. | 4 | ОПК-4 |
| | Итого | 4 | |
| 2 Кодирование источника | Теоремы Шеннона о кодировании в дискретном канале без помех. Избыточность и эффективность кода. Равномерное кодирование. Кодирование и декодирование источников сообщений кодами Шеннона-Фано и Хаффмана. Кодирование блоками. Количественная оценка эффективности кода. Кодирование и декодирование кодом Лемпела-Зива. | 6 | ОПК-4 |
| | Итого | 6 | |
| 3 Помехоустойчивое кодирование | Теоремы Шеннона о кодировании в дискретном канале с помехами. Линейные блочные коды. Порождающая и проверочная матрицы. Кодирование сообщения блочным кодом с заданными корректирующими свойствами. Декодирование методами минимума кодового расстояния и вычисления синдрома. Коды Хэмминга. Циклические коды. Полиномиальное описание кодовых векторов. Кодирование и декодирование с использованием циклических кодов. Обнаружение и исправление ошибок. | 12 | ОПК-4 |
| | Итого | 12 | |
| 4 Основы теории защиты информации | Шифрование методами замены, перестановок, подстановок и скремблирования. Шифрование методом RSA. | 2 | ОПК-4 |
| | Итого | 2 | |
| Итого за семестр | | 24 | |

Согласована на портале № 17385

## 9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| 3 семестр | | | | |
| 1 Основные понятия теории информации | Подготовка к практическим занятиям, семинарам | 2 | ОПК-4 | Домашнее задание, Зачет, Конспект самоподготовки, Контрольная работа, Опрос на занятиях |
| | Проработка лекционного материала | 1 | | |
| | Подготовка к контрольным работам | 1 | | |
| | Итого | 4 | | |
| 2 Кодирование источника | Подготовка к практическим занятиям, семинарам | 6 | ОПК-4 | Выступление (доклад) на занятии, Домашнее задание, Зачет, Конспект самоподготовки, Контрольная работа, Опрос на занятиях |
| | Проработка лекционного материала | 2 | | |
| | Подготовка к контрольным работам | 1 | | |
| | Итого | 9 | | |
| 3 Помехоустойчивое кодирование | Подготовка к практическим занятиям, семинарам | 12 | ОПК-4 | Выступление (доклад) на занятии, Домашнее задание, Зачет, Конспект самоподготовки, Контрольная работа, Опрос на занятиях |
| | Проработка лекционного материала | 3 | | |
| | Подготовка к контрольным работам | 1 | | |
| | Итого | 16 | | |
| 4 Основы теории защиты информации | Подготовка к практическим занятиям, семинарам | 2 | ОПК-4 | Выступление (доклад) на занятии, Домашнее задание, Зачет, Опрос на занятиях |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| Итого за семестр | | 32 | | |
| Итого | | 32 | | |

Согласована на портале № 17385

## 10. Курсовая работа (проект)

Не предусмотрено РУП

## 11. Рейтинговая система для оценки успеваемости студентов

### 11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

| Элементы учебной деятельности | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|---|---|---|---|---|
| 3 семестр | | | | |
| Выступление (доклад) на занятии | 4 | 4 | 4 | 12 |
| Домашнее задание | 6 | 6 | 6 | 18 |
| Зачет | | | 30 | 30 |
| Конспект самоподготовки | 3 | 3 | 2 | 8 |
| Контрольная работа | 8 | 8 | 8 | 24 |
| Опрос на занятиях | 2 | 3 | 3 | 8 |
| Итого максимум за период | 23 | 24 | 53 | 100 |
| Нарастающим итогом | 23 | 47 | 100 | 100 |

### 11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

| Баллы на дату контрольной точки | Оценка |
|---|---|
| ≥ 90% от максимальной суммы баллов на дату КТ | 5 |
| От 70% до 89% от максимальной суммы баллов на дату КТ | 4 |
| От 60% до 69% от максимальной суммы баллов на дату КТ | 3 |
| < 60% от максимальной суммы баллов на дату КТ | 2 |

### 11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|---|---|---|
| 5 (отлично) (зачтено) | 90 - 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 - 89 | B (очень хорошо) |
| | 75 - 84 | C (хорошо) |
| | 70 - 74 | D (удовлетворительно) |
| 3 (удовлетворительно) (зачтено) | 65 - 69 | |
| | 60 - 64 | E (посредственно) |
| 2 (неудовлетворительно) (не | Ниже 60 баллов | F (неудовлетворительно) |

Согласована на портале № 17385

| | | |
|---|---|---|
| зачтено) | | |

## 12. Учебно-методическое и информационное обеспечение дисциплины

### 12.1. Основная литература

1. Теория и техника передачи информации: Учебное пособие / Акулиничев Ю. П., Бернгардт А. С. - 2012. 210 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1750, дата обращения: 19.03.2017.
2. Теория информации : Учебное пособие для вузов / А. С. Котоусов. - М. : Радио и связь, 2003. - 77[3] с. : ил, табл. - Библиогр.: с. 78. (наличие в библиотеке ТУСУР - 38 экз.)

### 12.2. Дополнительная литература

1. Теория информации и кодирование : Учебное пособие для вузов / Б. Б. Самсонов [и др.]. - Ростов н/Д : Феникс, 2002. - 288 с. : ил. (наличие в библиотеке ТУСУР - 20 экз.)

### 12.3 Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Теория информации: Учебно - методическое пособие для проведения практических занятий и самостоятельной работы студентов / Акулиничев Ю. П. - 2012. 170 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1744, дата обращения: 19.03.2017.

#### 12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

### 12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Научно-образовательный портал ТУСУРа - https://edu.tusur.ru/
2. Библиотека ТУСУРа - https://lib.tusur.ru/
3. Поисковые системы сети Интернет.

## 13. Материально-техническое обеспечение дисциплины

### 13.1. Общие требования к материально-техническому обеспечению дисциплины

#### 13.1.1. Материально-техническое обеспечение для лекционных занятий

Лекционная аудитория, оборудованная средствами демонстрации слайдов и презентаций. Аудитория для практических занятий.

#### 13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебная аудитория с количеством посадочных мест не менее 25, оборудованная доской и стандартной учебной мебелью.

#### 13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

Согласована на портале № 17385

### 13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

## 14. Фонд оценочных средств

### 14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

### 14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

**Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью**

| Категории студентов | Виды дополнительных оценочных средств | Формы контроля и оценки результатов обучения |
|---|---|---|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки |

### 14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Согласована на портале № 17385

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 17385

**Приложение 1**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

# Теория информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **2**
Семестр: **3**

Учебный план набора 2013 года

Разработчики:
- доцент каф. РТС В. А. Бутько

Зачет: 3 семестр

Томск 2017

Согласована на портале № 17385

## 1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

| Код | Формулировка компетенции | Этапы формирования компетенций |
|---|---|---|
| ОПК-4 | способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации | Должен знать основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды; математические методы количественного описания информации; математические модели и информационные характеристики источников сообщений и каналов передачи информации; основные понятия и методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи; принципы и основные методы защиты информации от несанкционированного доступа;;<br>Должен уметь строить математические модели информационных систем и процессов; вычислять теоретико-информационные характеристики источников сообщений и каналов передачи информации; применять на практике методы эффективного и помехоустойчивого кодирования;;<br>Должен владеть основами построения математических моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач.; |

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

| Показатели и критерии | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости | Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем | Контролирует работу, проводит оценку, совершенствует действия работы |
| Хорошо (базовый уровень) | Знает факты, принципы, процессы, общие понятия в пределах изучаемой области | Обладает диапазоном практических умений, требуемых для решения определенных проблем в | Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к |

Согласована на портале № 17385

| | | | |
|---|---|---|---|
| | | области исследования | обстоятельствам в решении проблем |
| Удовлетворительно (пороговый уровень) | Обладает базовыми общими знаниями | Обладает основными умениями, требуемыми для выполнения простых задач | Работает при прямом наблюдении |

## 2 Реализация компетенций

### 2.1 Компетенция ОПК-4

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание этапов | основные понятия теории информации и кодирования; математические методы количественного описания информации; математические модели и информационные характеристики источников сообщений и каналов передачи информации; основные понятия и методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи | строить математические модели информационных систем и процессов; вычислять теоретико-информационные характеристики источников сообщений и каналов передачи информации; применять на практике методы эффективного и помехоустойчивого кодирования | основами построения математических моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач |
| Виды занятий | • Интерактивные практические занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Интерактивные лекции;<br>• Практические занятия;<br>• Лекции;<br>• Самостоятельная работа; | • Интерактивные практические занятия;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Контрольная работа;<br>• Домашнее задание;<br>• Опрос на занятиях;<br>• Выступление (доклад) на занятии;<br>• Зачет; | • Контрольная работа;<br>• Домашнее задание;<br>• Опрос на занятиях;<br>• Выступление (доклад) на занятии;<br>• Зачет; | • Домашнее задание;<br>• Выступление (доклад) на занятии;<br>• Зачет; |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|

Согласована на портале № 17385

| | | | |
|---|---|---|---|
| Отлично (высокий уровень) | • Обладает фактическими и теоретическими знаниями методов математического описания информации, эффективного помехоустойчивого кодирования, принципы и основные методы защиты информации; | • Умеет строить математические модели информационных процессов, вычислять информационные характеристики источников сообщений и каналов передачи информации, применять на практике методы эффективного и помехоустойчивого кодирования; | • Владеет пониманием значения информации в развитии общества, навыками применения математического аппарата для решения прикладных теоретико-информационных задач; |
| Хорошо (базовый уровень) | • Знает методы математического описания информации, эффективного и помехоустойчивого кодирования, принципы защиты информации; | • Умеет строить вычислять информационные характеристики источников сообщений и каналов передачи информации, применять на практике методы эффективного и помехоустойчивого кодирования; | • Понимает значение информации в развитии общества, владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач; |
| Удовлетворительно (пороговый уровень) | • Обладает базовыми общими знаниями количественного описания информации, принципов кодирования и защиты информации; | • Обладает основными умениями, требуемыми для решения простых задач кодирования информации; | • Владеет некоторыми навыками применения математического аппарата для решения прикладных теоретико-информационных задач; |

## 3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

### 3.1 Вопросы на самоподготовку

– Что такое вероятностный подход к измерению количества информации? Для каких источников дискретных сообщений применимы формулы Хартли, Шеннона? Объясните логарифмическую меру в определении количества информации. Какие единицы служат для измерения количества информации? то такое собственная информация и энтропия дискретной случайной величины? Какой вид дискретных сообщений обладает наибольшей энтропией? Каким образом описывается статистическая зависимость между соседними символами в дискретных сообщениях? При каких условиях энтропия источника дискретных сообщений с фиксированным числом состояний принимает максимальное значение? При каких условиях максимальна энтропия совокупности двух символов и чему она равна? В чем состоит правило сложения энтропий для независимых источников? Как определяется избыточность источника сообщений? Что такое пропускная способность канала связи, как ее рассчитать?

– Какой смысл вкладывают в понятие «кодирование источника»? Что такое сжатие информации? Какие выводы дают нам теоремы Шеннона для канала без шумов? На каких принципах основано построение эффективных кодов при неравновероятном появлении символов сообщения? Каково значение минимально-возможной средней длины кодовой комбинации? В чем состоит принцип построения эффективного кода по алгоритму Шеннона-Фано? В чем состоит принцип построения эффективного кода по алгоритму Хаффмана? Когда полезно кодировать блоки букв, а не отдельные буквы? В чем заключается главный недостаток кодов Хаффмана и Шеннона-Фано? Ка-

Согласована на портале № 17385

кие идеи лежат в основе словарных методов сжатия информации?

– Дайте определение взаимной информации переданного и принятого символов. Как влияет на ее величину интенсивность помех в канале связи? Какой смысл вкладывают в понятие «канальное кодирование»? Какие выводы следуют из теорем Шеннона для дискретного канала с помехами? Какие коды называются корректирующими? Может ли помехоустойчивый код быть безызбыточным? Что такое кодовое расстояние? Чем определяется корректирующая способность кода? Что значит «обнаружить ошибки» при декодировании кодовой комбинации? Что значит «исправить ошибки» при декодировании кодовой комбинации? Каковы возможности кода с кодовым расстоянием 5 в обнаружении и исправлении ошибок? Каков характерный признак, позволяющий отличить кодовую таблицу линейного блочного кода от кодовых таблиц других кодов? Чему равно количество комбинаций в кодовой таблице линейного блочного кода? Что такое проверочная матрица линейного блочного кода? Как она используется при обнаружении ошибок в принятой комбинации? Почему в проверочной матрице не может быть нулевых столбцов, строк? Почему декодирование по минимуму расстояния применяется редко? Что такое синдром? В чем заключается фундаментальное свойство комбинаций циклического кода? В чем состоят преимущества циклических кодов? Являются ли сверточные коды блочными и чем обусловлена их популярность? Каковы основные параметры сверточных кодов?

### 3.2 Зачёт

– 1) Вычислить энтропию и избыточность источника сообщения с распределением вероятностей символов: p1=0,03; p2=0,26; p3=0,09; p4=0,05; p5=0,16; p6=0,1; p7=0,09; p8=0,22. 2) При каких условиях энтропия источника дискретных сообщений с фиксированным числом состояний принимает максимальное значение? Докажите. 3) Стационарный источник выдает за T=10000 с двоичными посылками длительности t=1 мс один миллион бит информации. За какое время и с каким количеством двоичных посылок можно передать тот же объем информации, если соответствующей обработкой полностью устранить избыточность источника? 4) Докажите, что значение условной энтропии H(Y/X) в симметричном канале без памяти совпадает с величиной безусловной энтропии H(Y) только в случае статистической независимости символов на входе и выходе. 5) Показать, что в симметричном m-ичном канале без памяти условная энтропия сообщений на выходе канала при заданном ансамбле на входе определяется выражением H(Y/X) = -plog[p/(m - 1)] - (1 - p)log(1 - p), где p - вероятность ошибки символа. 6) Сообщения источника с производительностью 850 бит/с поступают на вход двоичного симметричного канала с вероятностью искажения p = 0,05. Длительность символов сигнала в канале 1 мс. Достаточна ли пропускная способность канала для передачи всей информации, поступающей от источника?

– 6) Построить оптимальный код сообщения, состоящего из: a) пяти равновероятных букв; b) шести равновероятных букв; c) семи равновероятных букв; d) восьми равновероятных букв. Дать оценку эффективности построенных кодов. В каких случаях код, построенный для первичного алфавита с равновероятным появление букв, окажется самым эффективным? 7) Статистические свойства троичного источника без памяти определяются вероятностями 0,48, 0,42 и 0,1. Определить энтропию источника и его избыточность. Произвести кодирование источника двоичными кодами Хаффмана, Шеннона-Фано и равномерным кодом. Произвести блоковое кодирование источника блоками по два символа двоичными кодами Хаффмана, Шеннона-Фано и равномерным кодом. Сравнить полученные коды по избыточности.

– 8) Двоичный код, предназначенный для кодирования восьми сообщений, содержит кодовые комбинации: 10011, 01010, 11001, 00101, 10110, 00000, 01111, 11100. Является ли код линейным? Найти избыточность кода и минимальное расстояние Хемминга. 9) Дана проверочная матрица систематического (7,4)-кода. Представить правило определения порождающей матрицы кода. Определить кодовое расстояние, число обнаруживаемых и исправляемых ошибок. Составить таблицу синдромов одиночных ошибок для (7,4)-кода и показать, каким ошибочным разрядам они соответствуют. 10) Можно ли найти 32 двоичных кодовых слова длиной 8 таких, что каждое кодовое слово отличается от других не менее, чем тремя компонентами? 11) Определить положение одиночной ошибки в искаженном слове 1100011 кода Хемминга длины 10. 12) Закодировать кодом Хэмминга слово a=1001. Вычислить синдром этого слова. Декодировать принятое кодовое слово для векторов ошибки e1=(0100000) и e2=(1001000). 13) Закодировать циклическим кодом Хэмминга (7,4) информационную последовательность 0101 (младший разряд слева). Проверить правиль-

Согласована на портале № 17385

ность кодирования путем декодирования полученного кодового слова. 14) Обнаружить, какая из трех принятых комбинаций 0011010, 0110100, 1010011 циклического кода Хэмминга (7,4) содержит ошибку. Исправить обнаруженную ошибку.

– 15) Защита информации от несанкционированного доступа. Принципы и цели шифрования. 16) Симметричные системы шифрования. Шифрование методами замены, перестановок, подстановок и скремблирования. 17) Шифрование методом RSA.

### 3.3 Темы домашних заданий

– Вероятностное описание дискретных источников информации. Мера количества информации. Собственная информация, энтропия, избыточность. Математическая модель канала передачи информации. Двоичный симметричный канал. Условная энтропия и взаимная информация. Информационные характеристики источников и каналов информации. Скорость создания и скорость передачи информации. Пропускная способность дискретных каналов.

– Кодирование источника дискретных сообщений. Равномерное кодирование. Кодирование и декодирование кодами Шеннона-Фано и Хаффмана. Блоковое кодирование. Количественная оценка эффективности кода. Алгоритм кодирования Лемпела-Зива.

– Помехоустойчивое кодирование. Кодовое расстояние и корректирующие свойства кода. Линейные блочные коды. Порождающая и проверочная матрицы. Коды Хемминга. Декодирование методами минимума кодового расстояния и вычисления синдрома. Кодирование и декодирование с использованием циклических кодов. Сверточное кодирование.

– Защита информации. Шифрование методами замены, перестановок, подстановок и скремблирования. Шифрование методом RSA.

### 3.4 Темы опросов на занятиях

– Информация, сообщения, сигналы. Математические модели дискретных сообщений. Количественные мера информации. Собственная информация. Условная собственная информация. Энтропия. Условная энтропия и взаимная информация. Скорость создания и скорость передачи информации. Пропускная способность дискретных каналов.

– Основные понятия теории кодирования информации. Избыточность, её роль при передаче информации. Теоремы Шеннона о кодировании в дискретном канале без помех. Коды Шеннона-Фано и Хаффмана. Блоковое кодирование.

– Принципы помехоустойчивого кодирования. Теоремы Шеннона о кодировании в дискретном канале с помехами. Корректирующие свойства кодов. Кодовое расстояние. Обнаружение и исправление ошибок. Классификация кодов. Линейные блочные коды. Матричное описание кодов. Порождающая и проверочная матрицы. Кодирование и декодирование линейных кодов. Коды Хэмминга. Циклические коды: порождающий полином, способы кодирования и декодирования. Коды БЧХ и Рида-Соломона. Сверточное кодирование.

– Обобщенная модель системы передачи и хранения информации. Цели шифрования. Симметричные и несимметричные системы шифрования. Симметричные и несимметричные системы шифрования. Шифрование методами замены, перестановок, подстановок и скремблирования.

### 3.5 Темы докладов

– Сжатие информации. Алгоритм кодирования Лемпела-Зива.
– Коды БЧХ.
– Цифровая подпись.

### 3.6 Темы контрольных работ

– Вероятностное описание сообщений. Собственная информация, энтропия, избыточность. Условная информация, условная энтропия, взаимная информация.

– Кодирование источника равномерным кодом, кодами Шеннона-Фано и Хаффмана. Сравнение кодов по избыточности.

– Помехоустойчивое кодирование. Коды Хэмминга. Циклические коды.

## 4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие

Согласована на портале № 17385

материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

### 4.1. Основная литература

1. Теория и техника передачи информации: Учебное пособие / Акулиничев Ю. П., Бернгардт А. С. - 2012. 210 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1750, свободный.
2. Теория информации : Учебное пособие для вузов / А. С. Котоусов. - М. : Радио и связь, 2003. - 77[3] с. : ил, табл. - Библиогр.: с. 78. (наличие в библиотеке ТУСУР - 38 экз.)

### 4.2. Дополнительная литература

1. Теория информации и кодирование : Учебное пособие для вузов / Б. Б. Самсонов [и др.]. - Ростов н/Д : Феникс, 2002. - 288 с. : ил. (наличие в библиотеке ТУСУР - 20 экз.)

### 4.3. Обязательные учебно-методические пособия

1. Теория информации: Учебно - методическое пособие для проведения практических занятий и самостоятельной работы студентов / Акулиничев Ю. П. - 2012. 170 с. [Электронный ресурс] - Режим доступа: http://edu.tusur.ru/publications/1744, свободный.

### 4.4. Базы данных, информационно справочные и поисковые системы

1. Научно-образовательный портал ТУСУРа - https://edu.tusur.ru/
2. Библиотека ТУСУРа - https://lib.tusur.ru/
3. Поисковые системы сети Интернет.

Согласована на портале № 17385