

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
Ярославский государственный университет им. П.Г.Демидова

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

ТЕОРИЯ ИНФОРМАЦИИ

Направление подготовки (специальность):
02.04.02 Фундаментальная информатика и информационные технологии

Образовательная программа
Искусственный интеллект и компьютерные науки

очная форма обучения

Составитель:
ТИМОФЕЕВ ЕВГЕНИЙ АЛЕКСАНДРОВИЧ,
Д.Ф.-М.Н., ПРОФЕССОР
Ф-ТА ИВТ ЯРГУ ИМ. П.Г. ДЕМИДОВА

г. Ярославль

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Кудряшов Б. Теория информации: учебник для ВУЗов. СПб: Питер, 2009 – 314 с.
2. Свирид Ю.В. Основы теории информации: курс лекций. Мн.: БГУ, 2003 – 139 с.
3. Лидовских В.В. Теория информации: учебное пособие. М.: МАТИ, 2002 – 120с.

Дополнительная литература:

1. Введение в криптографию: Учебник / Под общ. ред. В.В. Яценко. - СПб.: Питер, 2001.-288с
2. Тимофеев Е.А. Защита информации в распределенных сетях: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2001.-60с
3. Краснов М.В. Теория информации: методические указания. - Ярославль.: ЯрГУ, 2004.-27с.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие. - М.: Логос, 2001.-263с.
5. Ярочкин В.И. Информационная безопасность: Учебное пособие для студентов непрофильных вузов. - М.: Международные отноше, 2000.-400с.
6. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. - М.: Гелиос АРВ, 2001.-480с.
7. Петраков А.В. Основы практической защиты информации: Учебное пособие для вузов - 3-е изд. - М.: Радио и связь, 2001.-368с.
8. Теория кодирования : метод. указания / сост. М. В. Краснов ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2006, 47с
9. Теория кодирования [Электронный ресурс] : метод. указания / сост. М. В. Краснов ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2006, 47с

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю)

Для самостоятельного подбора литературы в библиотеке ЯрГУ рекомендуется использовать:

1. Личный кабинет (http://lib.uniylar.ac.ru/opac/bk_login.php) дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.

2. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniylar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/пароллю.

3. Электронная картотека «Книгообеспеченность» (http://www.lib.uniylar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла

дисциплин и специальностей. Электронная картотека [«Книгообеспеченность»](#) доступна в сети университета и через Личный кабинет.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая перечень информационных справочных систем (при необходимости)

1. www.wikipedia.org

Перечень информационных технологий, используемых при изучении дисциплины, включая программное обеспечение

В процессе осуществления образовательного процесса используются:

- для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система LaTeX;
- для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next");

**Учебно-методические указания и рекомендации
к изучению тем лекционных и практических занятий, самостоятельной
работе студентов**

Наименование раздела дисциплины	Название темы с кратким содержанием
Основные задачи теории информации	1. Основные задачи теории информации История возникновения, развития и современному состоянию теории информации. Понятие информации. Проблемы количественного измерения информации. Подходы к введению количественной меры информации.
Основные понятия теории информации	2. Основные понятия теории информации Различные подходы к измерению информации. Определение понятий сигнала, информационного канала и помех. Понятие кодирования информации. Три подхода к измерению информации. Вероятностная мера Шеннона.
Эффективное кодирование	3. Эффективное кодирование Понятие избыточности информации и методы ее устранения. Статистические и корреляционные методы эффективного кодирования. Методы Шеннона-Фано, Хаффмана, арифметическое кодирование, методы Лемпеля-Зива.

Наименование раздела	Название темы с кратким содержанием
Помехозащищенное кодирование	<p>4. Помехозащищенное кодирование</p> <p>Модели информационного канала с помехами. Двоичный симметричный канал. Емкость канала связи. Максимальные скорости передачи по каналу с помехами. Обнаружение и исправление ошибок при передаче через канал с помехами. Общие свойства помехозащищенного кодирования. Блочные коды. Групповые коды. Табличное, матричное и полиномиальное кодирование. Совершенные и квазисовершенные коды. Совершенные коды Хэмминга и коды Голея. Квазисовершенные коды БХЧ. Другие методы помехозащищенного кодирования.</p>

Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Текущий контроль успеваемости производится по выполнению домашних заданий практики и индивидуальных заданий. При регулярном выполнении домашних заданий и досрочной сдаче всех индивидуальных заданий студент получает досрочную отличную оценку по экзамену. При сдаче индивидуальных работ в срок студент может получить досрочную оценку по экзамену. Оценка по результатам выполнения коллоквиума (контрольной работы). До начала экзамена студент обязан сдать все индивидуальные задания. При несданных заданиях их сдача производится дополнительно к экзаменационному заданию за счет времени, отводимому на экзамен.

Пример индивидуального задания и (или) задания на контрольной работе (коллоквиуме)
Задача для индивидуальных заданий, коллоквиума и экзамена.

Задача: *Порт перегрузки определяется динамически меняющимися списками грузов (на складах порта и на кораблях груз определяется именем, портом назначения, количеством) и кораблей (имя, список грузов, свободная грузоподъемность: сколько можно еще погрузить, состояние погрузки или разгрузки). В состоянии разгрузки корабля разгружаются грузы (из списка корабля в список складов порта), порт назначения которых не соответствует порту назначения корабля. В состоянии погрузки – погружаются грузы (из списка складов порта в список корабля), порт назначения которых соответствует порту назначения корабля.*

Задание : *Определить список грузов, которые везут наиболее нагруженные корабли и при этом в минимальное число портов.*

На экзамене или коллоквиуме надо для задачи определить схему БД, разложение логической формулы запроса на составные части входящих подзапросов, проектирование подзапроса оптимального по трудоемкости с пошаговым определением максимальной и минимальной трудоемкости.

Результаты решения задачи обсуждаются на консультациях.

Варианты контрольной работы.

1. Взломать аффинную криптосистему если известно, что 12 переходит в 15, а 11 переходит в 10 модуль равен 31
2. Построить систему Хилла $d=2$

Вопросы для подготовки к экзамену.

1. История возникновения, развития и современному состоянию теории информации.
2. Понятие информации. Проблемы количественного измерения информации.
3. Подходы к введению количественной меры информации.
4. Различные подходы к измерению информации.
5. Определение понятий сигнала, информационного канала и помех.

6. Понятие кодирования информации. Три подхода к измерению информации.
7. Вероятностная мера Шеннона.
8. Понятие избыточности информации и методы ее устранения.
9. Статистические и корреляционные методы эффективного кодирования.
10. Методы Шеннона-Фано, Хаффмана
11. Арифметическое кодирование
12. Методы Лемпеля-Зива.
13. Модели информационного канала с помехами.
14. Двоичный симметричный канал.
15. Емкость канала связи. Максимальные скорости передачи по каналу с помехами.
16. Обнаружение и исправление ошибок при передаче через канал с помехами.
17. Примеры кодов обнаружения и исправления.
18. Общие свойства помехозащищенного кодирования.
19. Блочные коды. Групповые коды.
20. Табличное, матричное и полиномиальное кодирование.
21. Совершенные и квазисовершенные коды.
22. Совершенные коды Хэмминга и коды Голея.
23. Квазисовершенные коды БХЧ.
24. Защита информации от несанкционированного доступа.
25. Причины возникновения и история криптографии.
26. Современные симметричные криптопреобразования.
27. Примеры стандартов.
28. Преимущества и недостатки симметричных алгоритмов.
29. Несимметричные криптопреобразования.
30. Примеры систем без передачи ключей и систем с несимметричным ключом.
31. Современные стандарты несимметричных алгоритмов.
32. Преимущества и недостатки симметричных алгоритмов.
33. Понятие криптостойкости алгоритма и задачи криптоанализа.