Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет информатики и радиоэлектроники

«Утверждаю»
Первый проректор
_____ М.В. Давыдов
«31» 10 2024 г.

ПРОГРАММА

вступительного экзамена в магистратуру по специальностям
7-06-0611-06 Системы и сети инфокоммуникаций,
7-06-0611-02 Информационная безопасность
факультета информационной безопасности
по дисциплине «Основы теории информации»

2024

1 МОДЕЛЬ КАНАЛА ПЕРЕДАЧИ, ХРАНЕНИЯ ОБРАБОТКИ И РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИИ

1.1 Роль и место теории информации в современных инфокоммуникационных системах и сетях.

1.2 Обобщенная модель канала передачи, хранения обработки и распределения информации.

1.3 Эталонная модель взаимосвязи открытых систем.

1.4 Информационные методы в коммуникационных системах и сетях для повышения достоверности передаваемой, обрабатываемой, хранимой и распределяемой информации.

1.5 Первичное кодирование информации. Рефлексные коды. Код Грея, код FOMOT.

2 КАЧЕСТВЕННАЯ И КОЛИЧЕСТВЕННАЯ ОЦЕНКИ ИНФОРМАЦИИ

2.1 Понятие источника информации. Блоковый источник информации.

2.2 Источники сообщений и их свойства.

2.3 Понятие избыточности информации. Количественная оценка информации.

2.4 Энтропия, ее свойства. Энтропия как мера неопределенности выбора.

2.5 Количество информации как мера снятой информации. Относительная избыточность.

3 КОДИРОВАНИЕ ДЛЯ ДИСКРЕТНОГО ИСТОЧНИКА БЕЗ ПАМЯТИ

3.1 Задача кодирования источников информации.

3.2 Дискретный источник информации без памяти.

3.3 Условия взаимной однозначности алфавитного кодирования.

4 ЭФФЕКТИВНОЕ КОДИРОВАНИЕ

4.1 Сокращение избыточности информации.

4.2 Параметры кодов.

4.3 Моментальные коды.

4.4 Кодовые деревья и префиксные коды.

4.5 Неравенство Крафта. Средняя длина кодового слова и энтропия.

5 ТЕОРЕМА ШЕННОНА О КОДИРОВАНИИ ДЛЯ КАНАЛА БЕЗ ШУМА

5.1 Условная энтропия.

5.2 Первая теорема Шеннона.

5.3 Энтропия блокового источника.

5.4 Код Шеннона-Фано.

5.5 Код Хаффмана.

5.6 Код Лемпеля-Зива.

6 КАНАЛЫ БЕЗ ПАМЯТИ И ПЕРЕДАЧА ИНФОРМАЦИИ

6.1 Двоично-симметричный канал без памяти. Передача информации. Пропускная способность двоично-симметричного канала.

6.2 Теорема кодирования для дискретных каналов без памяти (Теорема Шеннона).

6.3 Дифференциальная энтропия.

6.4 Пропускная способность непрерывного канала.

6.5 Формула Шеннона.

7 ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

7.1 Основная теорема Шеннона о кодировании для канала с помехами.

7.2 Возможности исправления ошибок линейными кодами.

7.3 Блоковые коды.

7.4 Ошибки, их разновидности.

7.5 Кодовое расстояние Хэмминга и его связь с корректирующей способностью. Границы для минимального расстояния кодов.

8 АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

8.1 Группы. Подгруппы. Разложение групп на смежные классы.

8.2 Кольца. Кольцо полиномов.

8.3 Конечные поля. Представление элементов конечного поля.

8.4 Арифметика полей Галуа.

8.5 Векторные пространства и подпространства. Линейно зависимые и независимые векторы.

9 ЛИНЕЙНЫЕ КОДЫ

9.1 Линейные коды, исправляющие ошибки: построение и основные свойства. Вектор ошибок.

9.2 Порождающая и проверочная матрица систематического линейного кода. Каноническая форма порождающей матрицы.

9.3 Линейные коды Хэмминга.

9.4 Линейные коды Рида-Маллера.

9.5 Совершенные и квазисовершенные коды.

9.6 Смежные классы линейных кодов.

9.7 Вычисление минимального веса линейного кода по порождающей матрице этого кода.

10 МЕТОДЫ ДЕКОДИРОВАНИЯ ЛИНЕЙНЫХ КОДОВ

10.1 Декодирование по минимуму расстояния и синдрому.

10.2 Декодеры максимального правдоподобия.

10.3 Вычисление синдрома.

10.4 Табличное синдромное декодирование.

10.5 Вычисление вероятности ошибки декодирования.

11 ВВЕДЕНИЕ В ЗАЩИТУ ИНФОРМАЦИИ

11.1 Информационные угрозы и атаки.

11.2 Алгоритмы блочного шифрования.

11.3 Ассиметричные алгоритмы шифрования.

11.4 Криптографические протоколы.

11.5 Модели разграничения доступа к информации в инфокоммуникационных системах.

11.6 Методы разграничения доступа и способы их реализации.

11.7 Обеспечение целостности данных в инфокоммуникационных системах и сетях.

ЛИТЕРАТУРА

1. Умняшкин С.В. Теоретические основы цифровой обработки и представления сигналов: учебн. пособие: – ИД. «Форум»: ИНФРА-М, 2011.

2. Королев А.И. Помехоустойчивое кодирование информации / А.И. Королев, Аль-Ахмед Саид, В.К. Конопелько. – Мн.: Бестпринт, 2013.

3. Луенвергер Д. Дж. Информатика. – М.: Техносфера, 2008.

4. Смарт Н. Криптография. – М.: Техносфера, 2006.

5. Методы и средства защиты информации. В 2-х т. С.В. Ленков, Д. А. Перегудов, В.А. Хорошко. Под ред. В.А. Хорошко. – К.: Арий, 2008.

6. Вернер М. Основы кодирования. Учебник для ВУЗов. – М.: Техносфера, 2006.

7. Морелос–Сарагоса Р. Искусство помехоустойчивого кодирования. Методы алгоритмы, применение. Учеб. пособие. – М.: Техносфера, 2005.

8. Миано Дж. Форматы и алгоритмы сжатия изображений в действии: учеб. пособие. – М.: Триумф, 2003.

9. Сэломон Д. Практическое руководство по методам сжатия данных. – М.: Техносфера, 2003.

10. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации.- М.: Издательский центр «Академия», 2006.

11. Лосев В.В. Помехоустойчивое кодирование в радиотехнических системах передачи информации. Ч.2. Циклические коды, МРТИ , 1984.

12. Муттер В.М. Основы помехоустойчивой телепередачи информации. Л.: Энергоатомиздат. Ленингр. отд-ние, 1990.

13. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации.- М.: Издательский центр «Академия», 2006.

14. Киселев В.Д., Евсиков О.В., Кислицын А.С. Защита информации в современных системах передачи информации. М.: Солид, 2002.

15. Закон Республики Беларусь «Об информации, информатизации и защите информации», 2008.