

Предисловие

Учебное пособие «Помехоустойчивое кодирование в цифровых системах связи» предназначено для первоначального знакомства студентов радиотехнических специальностей с основными положениями теории и практического применения помехоустойчивого кодирования для защиты информации от искажений в канале связи с шумом. Основное внимание было уделено вопросам изложения материала в доступной для понимания форме. Предлагаемый материал позволит приобрести знания о параметрах и способах представления канальных помехоустойчивых кодов, нашедших наибольшее распространение в современных цифровых системах связи, овладеть навыком кодирования и декодирования, ознакомиться с потенциальными оценками качества декодирования помехоустойчивых кодов, способами декодирования и алгоритмами, их реализующими.

Учебное пособие подготовлено в соответствии с примерной образовательной программой высшего образования по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Усвоение материала учебного пособия будет способствовать формированию общепрофессиональной компетенции ОПК-11 — способности применять положения теории в области электрических цепей, радиотехнических сигналов, распространения радиоволн, кодирования, электрической связи, цифровой обработки сигналов для решения задач профессиональной деятельности, знаний об основных понятиях теории информации, основных кодах источников информации и помехоустойчивых кодах, основных параметрах и способах представления помехоустойчивых кодов, умений рассчитывать параметры помехоустойчивых кодов и применять базовые способы кодирования и декодирования типовых помехоустойчивых кодов и кодов источников информации.

Учебное пособие состоит из трех разделов, включающих 14 глав.

В первом разделе «Введение в теорию информации», который включает четыре главы, приведены основные положения теории информации, предложенные Клодом Шенноном. В главах раздела рассмотрены ансамбли и источники дискретных сообщений, математическая модель канала связи с шумом, предложенная К. Шенноном, вопросы определения пропускной способности канала связи и приведено обоснование принципа построения помехоустойчивых кодов для защиты информации от искажений в канале связи с шумом. Кроме того, во второй главе рассмотрены различные способы кодирования источников сообщения (сжатие информации) для устранения избыточности в передаваемых сообщениях.

Во втором разделе «Помехоустойчивое кодирование», который включает три главы, приведены основные параметры, способы представления, кодирования и декодирования двух классов помехоустойчивых кодов: линейных блочных кодов и сверточных кодов как подкласса древовидных кодов, а также кодовые конструкции (каскадные коды), в которых линейные блочные и сверточные коды выступают в качестве компонентных кодов.

В третьем разделе «Помехоустойчивые коды в цифровых системах связи», который состоит из семи глав, рассмотрены помехоустойчивые коды, нашедшие наибольшее распространение в цифровых системах связи. К ним относятся: циклические коды, несистематические сверточные коды, каскадные коды с последовательным соединением через перемежитель компонентных циклических кодов (турбо-блочные коды), каскадные коды с параллельным соединением через перемежитель компонентных рекурсивных систематических сверточных кодов (турбо-сверточные коды), каскадные коды волоконно-оптических систем связи, мажоритарно декодируемые коды, включая коды с малой плотностью проверок на четность. В заключении раздела показано применение циклических линейных блочных кодов в каналах связи с переспросом, которые используются для верификации передаваемых пакетов информации. В каждой из глав изложены основные способы представления, параметры и характеристики помехоустойчивых кодов, рассмотрены способы их кодирования и декодирования, приведены качественные характеристики помехоустойчивых кодов.

В каждой главе основные положения проиллюстрированы примерами. Главы завершаются вопросами и задачами для самопроверки, ответы к которым приведены в приложении.

В приложении приведены параметры наиболее распространенных помехоустойчивых кодов.

Учебное пособие предназначено для обучающихся по специальностям 10.05.02 «Информационная безопасность телекоммуникационных систем» и 10.05.03 «Информационная безопасность автоматизированных систем».

Учебное пособие может быть также полезно аспирантам, инженерам, специалистам и научным работникам, занимающимся проектированием и эксплуатацией модемов и кодеков цифровых систем связи.

Введение

Первые упоминания о применении человечеством помехоустойчивого кодирования относятся ко II веку до н.э. В X томе «Всеобщей истории» древнегреческого историка Полибия описан способ передачи информации на расстоянии с использованием эмпирически разработанного помехоустойчивого кода с помощью факелов (факельный телеграф), изобретенный александрийскими учеными Клеоксеном и Демоклитом.

Как научная теория помехоустойчивое кодирование начало формироваться в 40-х годах XX века. Она неразрывно связана с развитием теории цифровой связи как одного из разделов теории электрической связи. В основе теории цифровой связи лежат три фундаментальных положения, которые предопределили бурное развитие цифровых систем связи и теории помехоустойчивого кодирования в частности.

Во-первых, это теорема В.А. Котельникова (теорема отсчетов), сформулированная им в 1933 году [1], которая обосновывает возможность преобразования сигнала с ограниченным спектром из аналоговой формы в цифровую и обратно без искажений. Благодаря теореме Котельникова [2] цифровой способ передачи информации становится таким же универсальным, как и аналоговый способ передачи информации.

Во-вторых, это теория оптимального приема сигналов [2, 3], разработанная В.А. Котельниковым и представленная им в 1947 году. Он сформулировал и решил задачу оптимального статистического синтеза приемных устройств цифровых систем связи в линейном канале с аддитивным белым гауссовским шумом.

И, в-третьих, это основы теории цифровой связи, которые были опубликованы в фундаментальной работе К. Шеннона [4] в 1948 году. К. Шеннон изложил созданную им теорию информации, которая позволила ему дать количественную оценку эффективности применения как уже разработанных, так и проектируемых *цифровых систем связи* (ЦСС). Главным выводом теории информации является то, что построение «хороших» ка-

налов не всегда оказывается целесообразным. Гораздо проще и экономически выгоднее использовать помехоустойчивое кодирование. Теорема кодирования, сформулированная и доказанная К. Шенноном, гласит, что информация в цифровом виде может передаваться по каналу связи с шумом со сколь угодно высоким качеством, если скорость передачи информации не превышает пропускную способность канала связи и если применить помехоустойчивое кодирование. Теоретические результаты, полученные К. Шенноном, опровергли бытующее в то время утверждение, что высокое качество передачи информации по каналу связи с шумом может быть достигнуто лишь за счет уменьшения скорости ее передачи (т.е. только за счет многократной передачи по каналу связи сообщения до тех пор, пока оно не будет принято без искажений).

В 1950 году практически одновременно с работой К. Шеннона появилась классическая работа Р. Хемминга [5], посвященная построению линейного блочного кода, исправляющего однократные ошибки. Работы К. Шеннона и Р. Хемминга стимулировали дальнейшее интенсивное развитие теории помехоустойчивого кодирования, поиск и открытие ряда мощных кодов, разработку эффективных методов декодирования.

Теоретические пределы, полученные В.А. Котельниковым, К. Шенноном и другими исследователями способствовали развитию теории цифровой связи и одного из ее базовых разделов: теории помехоустойчивого кодирования. За ранними работами К. Шеннона и Р. Хемминга появилось много новых и важных достижений в области теории помехоустойчивого кодирования. Наиболее существенные из них перечислены ниже [6].

- 1949 год. Создание М.Дж. Голеем (США) совершенного линейного блочного кода, корректирующего ошибки кратности 3 и меньше.
- 1950 год. Создание Р. Хэммингом (США) совершенных линейных блочных кодов, корректирующих одиночные ошибки.
- 1954 год. Создание кодов с мажоритарным декодированием (США — И.С. Рид и Д.Е. Маллер).
- 1954 год. Исследование помехоустойчивости приема с «мягким» решением для кода Р.А. Вагнера (США — Сильверман и М. Болсер).
- 1955 год. Разработка сверточных кодов (США — П. Элайс; СССР — Л.М. Финк и В.И. Шляпоберский).

- 1956 год. Применение математического аппарата теории групп к построению линейных кодов, корректирующих ошибки (США — Д. Слепьян).
- 1956 год. Исследование линейных переключающих схем для получения кодов, исправляющих ошибки (США — Д.А. Хаффмен).
- 1957 год. Первые исследования циклических кодов (США — Е. Прейндж).
- 1957 год. Разработка метода последовательного декодирования сверточных кодов (США — Дж. Возенкрафт).
- 1959 год. Создание циклических линейных блочных кодов (США — Р.К. Воуз и Д.К. Рой-Чоудхури (1960 г.), Франция — А. Хоквингем (1959 г.)).
- 1960 год. Исследование помехоустойчивости приема сигналов в канале с группированием ошибок при использовании метода перемежения информационных символов (СССР — А.А. Харкевич и Э.Л. Влох (1960 г.), США — Дж.Л. Рамсей (1970 г.)).
- 1960 год. Создание эффективных циклических линейных блочных кодов (США — И.С. Рид и Г. Соломон).
- 1961 год. Исследование эффективности метода последовательного декодирования сверточных кодов (США — Дж. Возенкрафт и В. Рейффен).
- 1963 год. Исследование методов мажоритарного декодирования блочных кодов как при «жестком», так и при «мягком» решении демодулятора (США — Дж.Л. Месси).
- 1963 год. Разработка модифицированного алгоритма последовательного декодирования сверточных кодов (США — Р.М. Фано).
- 1963 год. Разработка линейных блочных кодов с малой плотностью проверок на четность (США — Р.Дж. Галлагер).
- 1965 год. Исследование циклических кодов с мажоритарным декодированием (СССР — В.Д. Колесников и Е.Т. Мирончиков).
- 1966 год. Разработка стэк-алгоритма последовательного декодирования сверточных кодов (СССР — К.Ш. Зигангиров, США — Ф. Джелинек (1969 г.)).
- 1967 год. Разработка алгоритма декодирования сверточных кодов по максимуму правдоподобия (США — А.Дж. Витерби).
- 1968 год. Разработка алгебраического алгоритма декодирования циклических кодов: ПГЦ-алгоритм декодирования (США — У. Питерсон, Д.Ц. Горнштейн, Н. Цирлер).

- 1968 год. Модификация алгоритма декодирования циклических кодов (США — Э.Р. Берлекемп, Дж.Л. Месси);
- 1970 год. Циклические линейные блочные коды Д. Гоппа (США).
- 1970 год. Исследование каскадных кодов (США — Г. Форни. СССР — Э.Л. Блох и В.В. Зяблов (1976 г.)).
- 1971–1972 годы. Алгоритмы «мягкого» декодирования блочных кодов (США — Е. Велдон и Д. Чейз).
- 1976–1977 годы. Алгоритмы многопорогового декодирования (СССР — В.В. Золотарев).
- 1982 год. Исследования решетчатой кодовой модуляции (США — Г. Унгербок).
- 1982–1991 годы. Исследование помехоустойчивости различных методов приема сигнально-кодовых конструкций в канале связи с аддитивным белым гауссовским шумом (СССР — С.Л. Портной, В.В. Зяблов, В.Л. Банкет, В.В. Гинзбург).
- 1993 год. Разработка и исследование турбо-сверточных кодов (Франция — К. Берру).
- 1997 год. Фирма АНА изготовила кодек кодов-произведения.
- 1997–1999 год. Применение турбо-сверточных кодов с компонентными рекурсивными систематическими сверточными кодами в CCC «Инмарсат» (стандарт M4) и CCSDS.
- 2000–2003 год. Применение турбо-сверточных кодов в стандарте DVB-RCS, CCC VSAT.
- 2004–2005 год. Применение кодеков с каскадными кодами (LDPC-БЧХ) фирмы TurboConcept в стандарте DVB-S2, CCC VSAT.
- 2008–2009 год. Использование кодеков с кодами с малой плотностью проверок на четность фирмами Китая и Японии в стандарте DVB.
- 2008 год. Применение в волоконно-оптических системах связи каскадных кодов с компонентными БЧХ-кодами и кодами Рида-Соломона по стандартам ITU-T G.709 и G.975.1.

В текущем двадцатилетии основные усилия и успехи в области помехоустойчивого кодирования были направлены и достигнуты не в разработке новых классов кодов, а в создании, развитии и внедрении быстродействующих алгоритмов их декодирования.

Основные положения теории помехоустойчивого кодирования можно найти в прекрасных фундаментальных работах зарубежных [7–14] и отечественных [15–19] авторов.