

УДК 621.391.15

## ЭФФЕКТИВНЫЕ АЛГОРИТМЫ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ДЛЯ ЦИФРОВЫХ СИСТЕМ СВЯЗИ

В.В. Золотарёв, ведущий научный сотрудник НИИР, д.т.н.

Г.В. Овечкин, ассистент кафедры Рязанской государственной радиотехнической академии, к.т.н.

Передача информации по каналам связи существенно усложняется из-за помех и искажений в канале. Эффективным средством повышения достоверности передаваемой информации является помехоустойчивое кодирование. В статье производится сравнение основных алгоритмов декодирования помехоустойчивых кодов, сделанное по материалам научно-технических конференций и публикациям по теории кодирования.

**Критерии эффективности кодирования.** За 12 лет, прошедшие с момента публикации обзорной статьи [1], теория помехоустойчивого кодирования продвинулась далеко вперед. Появились мощные коды и методы их декодирования, обеспечивающие работу систем связи вблизи пропускной способности канала. Наиболее общим показателем качественной оценки методов декодирования является энергетический выигрыш кодирования (ЭВК), показывающий снижение энергии, необходимой для передачи одного бита данных (при некоторой выбранной средней вероятности ошибки на бит  $P_b(e)$ ) в случае использования тех или иных алгоритмов кодирования и декодирования, по сравнению со случаем, когда кодирования нет.

Зарубежные специалисты более 20 лет назад оценивали каждый 1 дБ ЭВК в миллионы долларов [2]. Сейчас ценность ЭВК возросла еще больше, поскольку появилась возможность уменьшать размеры очень дорогих антенн или повышать дальность связи, увеличивать скорость передачи или снижать необходимую мощность передатчика, улучшать другие важные свойства современных систем связи. Заметим, что их стоимость растет все быстрее и уже совершенно несопоставима с теми затратами, которые были необходимы несколько десятилетий назад. Кроме того, существенно возрастают взаимные помехи приема между различными системами, появляется все больше экологических ограничений на мощность передатчиков, растет потребность в резком увеличении скоростей обмена данными между сетями, а также в значительном росте их достоверности.

И в дальнейшем, в условиях глобализации экономики и взрывной информатизации общества эти тенденции будут только усиливаться. Отсюда можно сделать вывод о том, что возрастание на несколько порядков (!) экономической (как и экологической и, вообще, системной) ценности ЭВК на базе методов помехоустойчивого кодирования становится чрезвычайно актуальным и требует внедрения теоретических достижений в области помехоустойчивого кодирования при создании компьютерных систем связи.

**Характеристики декодеров.** На рис. 1 представлена зависимость вероятности ошибки на бит  $P_b(e)$  на выходе декодера от уровня шума  $E_b/N_0$  в двоичном симметричном канале без

памяти (ДСК). Ошибки возникают при работе жесткого модема с двоичной фазовой модуляцией в канале с аддитивным белым гауссовским шумом, когда в декодере не используются оценки достоверности принятых символов. Такая модель канала достаточно точно описывает реальные спутниковые и некоторые другие типы каналов.

Кривые 1, 2, 3 соответствуют широко используемому алгоритму Витерби (АВ) [3, 4] для кодовой скорости  $R = 1/2$  и длины кодирующего регистра  $k = 7, 11$  и 15. Данный метод является оптимальным, однако его сложность растет экспоненциально с ростом  $k$  и поэтому на практике декодеры с  $k > 9$  не используются. В результате возникает необходимость поиска более простых (с точки зрения практической реализации) декодеров, обеспечивающих в то же время близкое к оптимальному декодирование.

**Многopороговые алгоритмы.** Один из простейших алгоритмов коррекции ошибок – пороговый декодер (ПД) Мессис [5], принимающий решение о значении каждого декодируемого символа на основе обычного "голосования" проверок. Схема порогового декодера сверточного самоортогонального кода (СОК) с кодовым расстоянием  $d = 5$ , кодовой скоростью  $R = 1/2$  и длиной кодового ограничения  $n_A = 14$  представлена на рис. 2. Он состоит из двух двоичных регистров, нескольких полусумматоров (сумматоров по mod 2) и порогового элемента  $T$ , который просто суммирует двоичные проверки декодируемого символа и сравнивает их с порогом, изменяя этот символ и все относящиеся к нему проверки, если сумма проверок превысила некоторое пороговое значение. Но данный метод имеет невысокую корректирующую способность, из-за чего редко применяется в системах передачи данных.

Значительно лучшими характеристиками обладают многopороговые декодеры (МПД) [6], являющиеся модификацией представленного выше ПД. МПД в процессе контроля принятых кодовых последовательностей многократно исправляют информационные символы пришедшего из канала сообщения. Эти декодеры обладают важнейшим строго доказанным свойством – сходимостью к решению оптимального декодера (ОД), сохраняя линейную от длины кода сложность реализации.

Схема МПД сверточного СОК с  $d = 5$ ,  $n_A = 14$  и двумя итерациями декодирования представлена на рис. 3. При большем числе итераций, обычно необходимом для работы в области больших шумов канала, последующие итерации полностью аналогичны второй. Как видно из представленной схемы, каждая итерация МПД отличается от обычного ПД только наличием "разностного" регистра, в котором отмечаются измененные пороговым элементом (ПЭ) информацион-

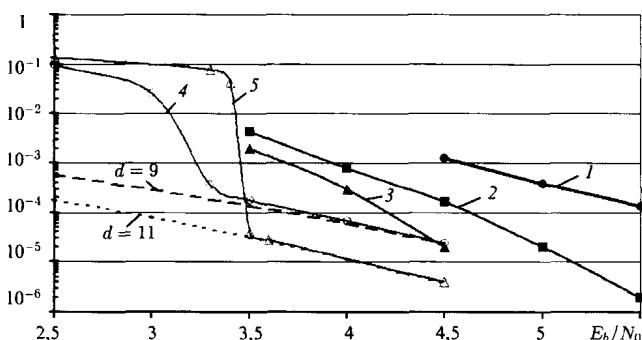


Рис. 1

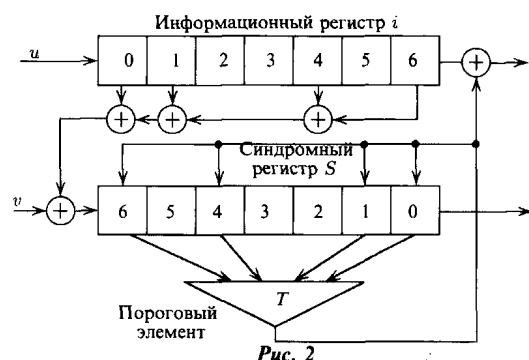


Рис. 2

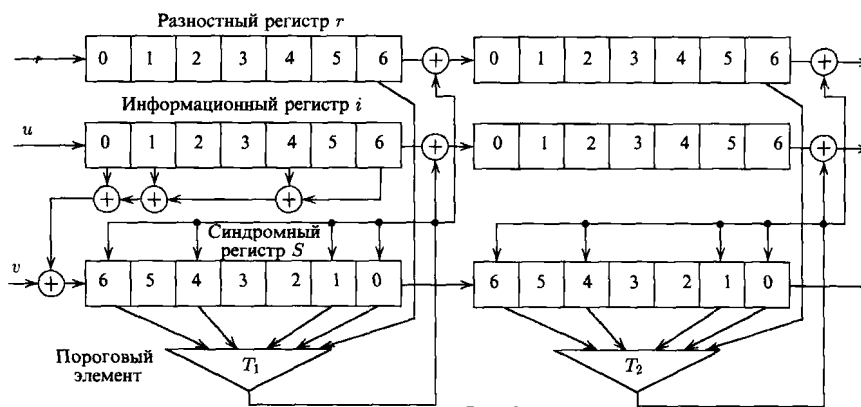


Рис. 3

ные символы. Существенно, что решения ПЭ из разностного регистра затем используются другим ПЭ на следующей итерации декодирования. На каждой итерации МПД при декодировании информационного символа  $i_k$  на ПЭ – единственном активном элементе декодера (при использовании жесткого модема в ДСК) выполняются следующие операции.

1. Вычисляется сумма проверок (каждая из которых для случая ДСК равна 0 или 1), т. е. функция

$$L_i = \sum_{m=1}^J S_{g_m} + r_i,$$

где  $J = d - 1$  – количество проверок (ненулевых элементов  $g_m$  порождающего полинома кода  $G$ );  $r_i$  – символ разностного регистра, относящийся к декодируемому символу  $i_k$ , также равный 0 или 1;  $S_m$  –  $m$ -й элемент синдромного регистра, входящий в множество проверок относительно декодируемого символа  $i_k$ .

2. Если  $L_i > T$ , где  $T \geq (d - 1)/2$  – значение порога порогового элемента, то информационный символ  $i_k$ , все связанные с ним проверки  $\{S_{g_m}\}_{m=1, J}$  и символ  $r_i$  инвертируются.

3. Переход к декодированию следующего символа (п. 1).

Заметим, что при применении мягкого модема, когда в гауссовском канале оценивается надежность приема каждого двоичного символа, в МПД выполняются те же операции, но проверки суммируются уже с весами, определяющими надежность оценок принятых из канала битов. Пороги  $T$  для декодируемых символов будут переменными, а не фиксированными, как в случае ДСК.

Анализ характеристик МПД. Кривая 4 на рис. 1 соответствует работе МПД сверточного СОК с  $R = 1/2$ , минимальным кодовым расстоянием  $d = 9$ , длиной кодового ограничения  $n_A = 4168$  бит и  $I = 15$  итерациях декодирования [6]. Возможности МПД с  $R = 1/2$ ,  $d = 11$  и  $I = 20$  представлены на рис. 1 кривой 5. Пунктиром на рисунке показаны вероятности ошибочного декодирования кода с  $d = 9$  и  $d = 11$  оптимальным декодером. Как следует из графиков, МПД (для достаточно длинных кодов) оказывается лучше даже заведомо нереализуемого оптимального АВ с  $k = 15$  и более. Отметим, что с ростом длины кодового ограничения  $n_A$  и увеличением числа итераций характеристики МПД быстрее сходятся к характеристикам оптимального декодера.

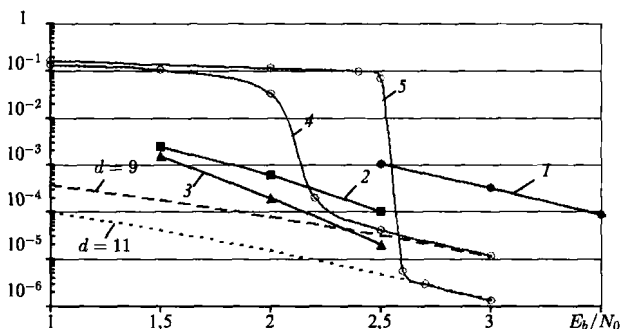


Рис. 4

На рис. 4 показаны характеристики тех же алгоритмов декодирования при использовании мягкого модема, оценивающего достоверность принимаемых двоичных символов с квантованием выхода на  $Q = 16$  уровней для вышеперечисленных кодов. Из сопоставления рис. 1 и 4 видно, что переход к мягкому модему при использовании АВ позволяет получить дополнительный ЭВК порядка 2 дБ, а при использовании МПД – 1,4...1,7 дБ. Но и в этом случае МПД, сохраняя простоту обычного ПД, существенно превосходит АВ по эффективности. Основные соотношения между этими алгоритмами имеют место и при других кодовых скоростях.

Приведенные выше данные показывают, что доступные для реализации оптимальные АВ уступают МПД, в котором могут легко декодироваться длинные коды, в широком диапазоне кодовых скоростей при использовании как жесткого, так и мягкого модемов. При этом МПД выполняет только простейшие операции сложения и сравнения небольших целых чисел, что обуславливает его крайнюю простоту при всех вариантах программной или аппаратной реализации.

Существенное улучшение характеристик декодирования обеспечивают каскадные методы кодирования [7] при меньшей сложности реализации по сравнению с некаскадными. При этом исходные данные кодируются двумя и более кодами, которые затем определенным образом декодируются соответствующими этим кодам методами.

Эффективность турбокодов. Рассмотрим открытые в 1993 г. турбокоды [8–10] – коды с параллельным каскадированием. Они создаются с помощью двух и более систематических кодеров, связанных между собой перемежителями. Название "турбо" отражает свойства используемого при декодировании итеративного алгоритма: информация с выхода одной итерации декодирования является входной для следующей итерации. В декодерах составляющих кодов обычно применяются оптимальный алгоритм декодирования по максимуму апостериорной вероятности (MAP-алгоритм) или его упрощенный вариант – max-log-MAP (MLM).

На рис. 5 показаны характеристики турбокодов: кривая 1 –  $R = 1/2$ ,  $K = 65536$ , MAP; кривая 2 –  $R = 1/2$ ,  $K = 1000$ , MAP; кривая 3 –  $R = 1/2$ ,  $K = 1000$ , MLM. Здесь  $K$  – длина информационного блока. При получении графиков выполнялось до 20 итераций декодирования. Коды показывают очень хорошие характеристики при большом шуме в канале связи. С их помощью достигается  $P_b(e) = 10^{-5}$  при  $E_b/N_0 = 0,7$  дБ, что всего лишь на 0,5 дБ выше теоретически достижимой границы. Однако при снижении уровня шума наблюдается эффект "насыщения" вероятности ошибки, возникающий из-за небольшого кодового расстояния приведенных кодов.

Сложность декодеров турбокодов очень велика. Например, турбокод, основанный на MAP-декодере, выполняет порядка  $12N$  FLOP/IB/Iтер, а на MLM –  $30N$  АЕО/IB/Iтер. Здесь  $N$  – число возможных состояний кодера, FLOP/IB/Iтер – количество операций с вещественными числами (включая умножение и сложение), приходящихся на один информационный бит на каждой итерации, а АЕО/IB/Iтер – количество сложений, вычитаний и сравнений целых чисел.

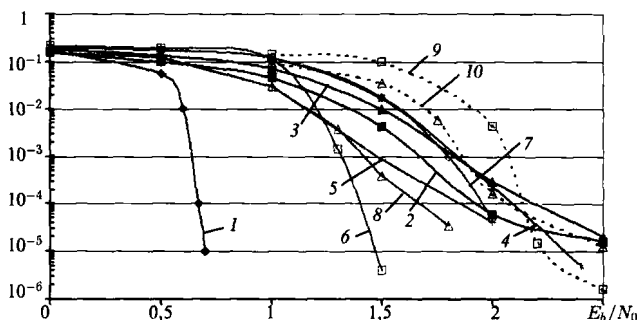


Рис. 5

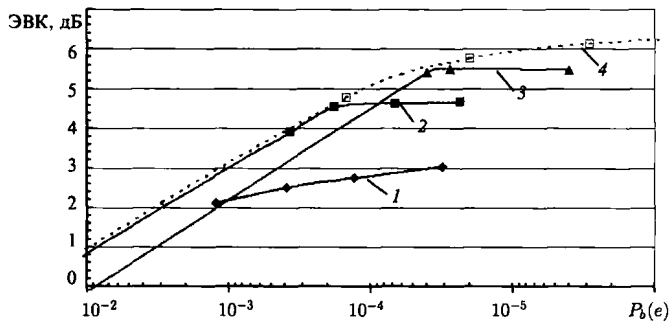


Рис. 6

Другим видом каскадных кодов являются *последовательные каскадные коды* [11], для декодирования которых также применяется итеративная схема. Их возможности также показаны на рис. 5: кривая 4 –  $R = 1/2$ ,  $K = 1000$ , MLM; кривая 5 –  $R = 1/2$ ,  $K = 1000$ , MAP. Коды обладают большим кодовым расстоянием и поэтому показывают лучшие характеристики при среднем и низком уровне шума.

*Плетеные коды* [12–15] также являются последовательными каскадными кодами. В кодере данного кода ряд внешних кодеров и внутренний как бы переплетаются. На рис. 5 представлены возможности плетеных кодов: кривая 6 –  $R = 1/2$ ,  $K = 10000$ , MLM; кривая 7 –  $R = 1/2$ ,  $K = 1000$ , MLM; кривая 8 –  $R = 1/2$ ,  $K = 1000$ , MAP. Коды оказываются хуже турбо при большом уровне шума и лучше – при среднем и низком.

Из рис. 5 видно, что в случае работы при умеренных шумах МПД, характеризующийся высоким быстродействием и простотой (МПД с  $d = 9$  выполняет порядка 12 АЕО/IV/Iter), свойственной всем мажоритарным алгоритмам, ничем не уступает рассмотренным каскадным схемам. Кроме того, при таком уровне ошибки на выходе МПД в основном одиночные [6], что позволяет успешно применять его в очень простых каскадных кодах даже без использования дополнительных перемежителей. Кривые 9 и 10 на рис. 5 отражают возможности каскадных схем на основе МПД и кода с контролем четности (ККЧ): 9 – МПД с  $R = 1/2$ ,  $d = 9$ ,  $n_A = 4168$  и ККЧ с  $n = 50$ ; 10 – МПД с  $R = 1/2$ ,  $d = 7$ ,  $n_A = 3052$  и ККЧ с  $n = 50$ . Использование данной каскадной схемы позволяет уменьшить вероятность ошибки декодирования в 10–100 раз по сравнению с простым МПД.

Заметим, что число операций в МПД (и без того очень небольшое) можно еще сократить – в некоторых случаях примерно в 4 раза без потери эффективности декодирования, что значительно увеличивает скорость работы алгоритма.

**Сравнение алгоритмов декодирования.** Завершим сопоставление алгоритмов рассмотрением обеспечиваемого ими ЭВК. На рис. 6 отражена энергетическая эффективность алгоритмов декодирования при работе с жестким модемом: кривая 1 – АВ с  $k = 7$ ,  $R = 1/2$ ; кривая 2 – МПД с  $R = 1/2$ ,  $d = 9$ ; кривая 3 – МПД с  $R = 1/2$ ,  $d = 11$ ; кривая 4 – каскадный: ККЧ с  $n = 50$  и МПД с  $R = 1/2$ ,  $d = 9$ . Рис. 7 показывает ЭВК алгоритмов декодирования при работе с мягким модемом: кривая 1 – АВ с  $k = 7$ ,  $R = 1/2$ ; кривая 2 – турбо с  $R = 1/2$ ,  $K = 65536$ , MAP; кривая 3 – турбо с  $R = 1/2$ ,  $K = 1000$ , MLM; кривая 4 – МПД с  $R = 1/2$ ,  $d = 9$ . Каскадные схемы на основе МПД с  $d = 9$  и  $d = 7$  представлены кривыми 5 и 6. Из рисунков видно, что МПД и каскадные схемы на его основе при малых  $P_b(e)$  незначительно уступают турбокодам.

Приведенные результаты относились к двоичным кодам и системам с двоичной фазовой модуляцией. На основе важнейшего свойства сходимости решения МПД к оптимальному при всех изменениях декодируемых символов [6] реализованы недвоичные МПД, обеспечивающие характеристики, близкие или несколько более высокие, чем у кодов Рида-Соломона. Аналогично, высокие характеристики МПД, обеспечиваемые ими в каналах со стираниями и в системах с многопозиционной модуляцией, делают их универсальным средством простого достижения высокого уровня помехозащищенности сообщений

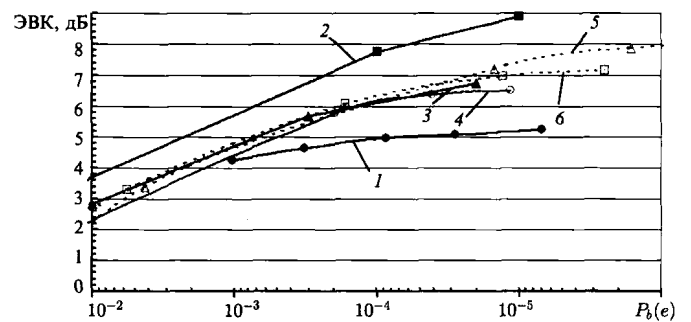


Рис. 7

в системах широкого спектра применения. При этом сохраняется такая же сложность реализации, как и в простейшем пороговом декодере.

**З а к л ю ч е н и е.** В настоящее время возможности технологии позволяют даже для высокоскоростных каналов создавать аппаратно-программные версии декодеров, которые будут успевать выполнять достаточно большое число операций с каждым декодируемым символом. Это дает возможность строить все более сложные кодовые конструкции. Однако алгоритмы, нерационально использующие вычислительные ресурсы, все же значительно проигрывают гораздо более простым, но решающим задачу декодирования более эффективно.

Несомненно, что проблемы сложности реализации кодирования сохранятся в обозримом будущем, а в связи с ростом скоростей обмена информацией требования более простой реализации декодеров будут все актуальнее. Самыми дешевыми при всех вариантах реализации окажутся те алгоритмы, которые выполняются только очень простые, однородные и быстрые операции. Наиболее полно этим требованиям удовлетворяют МПД. А соответствие его возможностей характеристикам самых сложных алгоритмов делает МПД еще более привлекательным.

Конечно, при необходимости достижения уровней энергетического выигрыша, сравнимого с лучшими турбокодами, размеры памяти МПД и число выполняемых им операций сложения заметно возрастают. Но даже в этом случае сложность их реализации останется, видимо, существенно меньшей. Однако необходимость реализации декодеров для аппаратуры связи с энергетикой всего на несколько десятых децибелл, т.е. на 2–4% меньшей предельно возможных значений, требует более глубокой технологической проработки и обоснования. Видимо, эти вопросы станут действительно актуальными не ранее, чем через несколько лет.

Таким образом, в истекший после публикации [1] период были созданы условия для достижения уровней энергетики, весьма близких к теоретическим пределам для каналов космической и спутниковой связи. Высокие характеристики могут обеспечить несколько методов. Однако их сложность при сопоставимых уровнях ЭВК показывает, что алгоритмы на базе МПД близки по числу операций к простейшему декодеру порогового типа. Поэтому в большинстве случаев МПД являются наиболее предпочтительным алгоритмом декодирования в высокоскоростных системах связи.

#### ЛИТЕРАТУРА

1. Золотарев В.В. Использование помехоустойчивого кодирования в технике связи // Электросвязь. – 1990. – № 7. – С. 7–10.
2. Берлекэмп Э.Р. Техника кодирования с исправлением ошибок // ТИИЭР. – 1980. – Т. 68, № 5. – С. 24–58.
3. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. под ред. Б.С. Цыбакова. – М.: Радио и связь, 1987. – 392 с.
4. Золотарев В.В. Реальный энергетический выигрыш кодирования для спутниковых каналов // В кн.: 4-я Международная конференция "Спутниковая связь – ICSC-2000". – М.: МЦНТИ, 2000. – Т. 2. – С. 20–25.
5. Мессис Дж. Пороговое декодирование: Пер. с англ. под ред. Ю.Л. Сагаливича. – М.: Мир, 1966. – 208 с.

6. Самойленко С.И., Давыдов А.А., Золотарев В.В., Третьякова Е.И. Вычислительные сети. – М.: Наука, 1981.
7. Форти Д. Каскадные коды: Пер. с англ. под ред. С.И. Самойленко. – М.: Мир, 1970. – 208 с.
8. Berrou C., Glavieux A., Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes // Proceeding of ICC'93, Geneva, Switzerland, May 1993. – P. 1064–1070.
9. Barbulescu S.A. Iterative decoding of turbo codes and other concatenated codes. Ph.D. dissertation. – Feb. 1996.
10. Andrews K., Berner J., Chen V. et al. Turbo-decoder implementation for the deep space network // IPN Progress Report 42–148. – Feb. 15, 2002.
11. Benedetto S., Montorsi G., Divsalar D., Pollara F. Serial concatenation of interleaved codes: Performance analysis, design and iterative decoding // JPL TDA Progress Report. – August 1996. – V. 42–126.
12. Host S., Johannesson R., Zyablov V. A first encounter with binary woven convolutional codes // In: Proc. International Symposium on Communication Theory and Applications, Lake District, UK. – July 1997. – P. 13–18.
13. Freudenberger J. Untersuchung von woven-codes. Ph.D. dissertation. – Jan. 1999.
14. Зяблов В.В., Йоханнессон Р., Скопинцев О.Д., Хёст С. Асимптотические дистанционные свойства двоичных плетеных сверточных кодов // Проблемы передачи информации. – 1999. – Т. 35, вып. 4. – С. 29–46.
15. Freudenberger J, Shavgulidze S., Zyablov V., Bossert M. Woven codes with outer warp: variations, design and distance properties // Journal on Selected Areas in Communications issue on The Turbo Principle: From Theory to Practice, 2001.

*Получено 07.04.03*

## **ВНИМАНИЮ СПЕЦИАЛИСТОВ!**

**С 18 октября 2003 г. в Москве  
в малом зале Политехнического музея  
д.т.н. В.В. Золотарёв читает  
курс научно-популярных лекций на тему:  
"Современные методы помехоустойчивого  
кодирования как проблема поиска  
глобального экстремума"**

В цикле из четырех лекций изложены общие подходы и конкретные алгоритмы многопорогового декодирования (МПД) блочных и сверточных кодов в каналах с большим уровнем шума. Демонстрируется мультфильм, иллюстрирующий возможное декодирование длинных кодов при линейной сложности реализации. На простых примерах будет показано, что МПД выполняет примерно на два порядка меньше операций, чем турбодекодеры с сопоставимой эффективностью. Особое внимание будет уделено перспективам применения декодеров корректирующих кодов в системах связи.

Начало лекций в 18 часов. Билеты – в кассе музея.

Дополнительную информацию о МПД можно найти на сайтах [www.mtdbest.iki.rssi.ru](http://www.mtdbest.iki.rssi.ru) и [www.iki.rssi.ru](http://www.iki.rssi.ru) в разделе семинаров по информатике и механике за 27.11.2002 г., а также в НТЦ АСС ФГУП НИИРадио по тел: (095)-261-03-27, (095)-261-54-44 или по e-mail: [zolotasd@yandex.ru](mailto:zolotasd@yandex.ru) у докладчика.

НТЦ АСС принимает заказы на разработку высокоскоростных МПД на новейшей элементной базе и программные варианты реализации алгоритма для широкого диапазона значений избыточности кодов и энергетического выигрыша.