Результаты работы целесообразно использовать при разработке перспективных ККС в специальных информационно-телекоммуникационных системах.

*Литература: 1. Bennett C. H., Bessette F., Brassard G., Savalle L. and SmolinJ., Experimental Quantum Cryptography, Proceedings of Eurocrypt '90, also in Journal of Cryptology, Vol. 5, No. 1 (1992).-P. 3-28. 2. Huges R. G., Buttler W. T., Kwiat P. G., Luiher G. G., Morgan G. I., Nordholt J. E., Peterson C. G., Simmsons C. M. Secure communications using quantum cryptography. – Los Alamos National Laboratory. LA-UR-97-1099.3. Townsend P., 1997b, Quantum cryptography on multiuser optical fiber networks, Nature (London) 385.-P. 47–49. 4. Shannon C. A mathematical theory of communication // Bell Syst.Tech. J. – 1948. – Vol. 27. – P. 379–423. 5. Maurer U. "Secret Key Agreement by Public Discussion Based on Common Information" // IEEE Trans. on IT., Vol. 39, May 1993, pp. 733 – 742. 6. Седельников В. М. Алгоритм выработки общего ключа с использованием квантового канала // Проблемы передачи информации Т.35, №1, 1999.–С.100-109. 7. В. Н. Вервейко, А. И. Пушкарев, Т. В. Цепурит. Функции хэширования: классификация, характеристика и сравнительный анализ//Радиотехника: Всеукр.межвед.науч.-техн.. сб. 2002. Вып. 126 С172-179. 8. Berrou C., Glavieux A. Near optimum error correcting coding and decoding: turbo-codes // IEEE Trans. on Commun. – 1996. – Vol.44, №10. – P. 1261-1271. 9. Банкет В. Л., Прокопов С. Д. Эффективность применения турбо-кодов в телекоммуникационных системах // Наукові праці УДАЗ ім. О. С. Попова. – 2000. – №3. – с. 36-41.*

**УДК 681.3**

# ПРИМЕНЕНИЕ ТУРБОКОДОВ В СПЕЦИАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

***Сергей Зайцев, Сергей Ливенцев, Дмитрий Алексеев***
*Специальный факультет СБ Украины ВИТИ НТУУ «КПИ»*

*Аннотация:* **Рассмотрены вопросы применения турбокодов в специальных телекоммуникационных системах. Указаны основные принципы построения турбокодов и их характеристики.**
*Summery:* **There are considered problems of turbocode using in special telecommunication systems in the article. There are showed basic principles of turbocode building and they characteristics.**
*Ключевые слова:* **Помехоустойчивое кодирование, турбокоды, итеративное декодирование.**

## I Введение

Одним из перспективных направлений совершенствования характеристик специальных телекоммуникационных систем является применение корректирующих кодов. В настоящее время широкое распространение в телекоммуникационных системах получил класс помехоустойчивых кодов – турбокоды. Однако в существующей литературе описанию характеристик и способов построения составных кодов уделено не достаточно внимания. ***Целью работы*** является рассмотрение структуры построения турбокодов и их основных характеристик.

Турбокоды используются в качестве метода канального кодирования [1, 2] в системах передачи телеметрической информации с космических аппаратов по рекомендации *CCSDS (Consultative Committee for Space Data Systems),* системах подвижной радиосвязи третьего поколения *UMTS* (*Universal Mobile Telecommunications System*) и *cdma*2000, системах цифрового телевизионного вещания стандарта *DVB-RCS* (*Digital Video Broadcasting Return Channel for Satellite*), спутниковых модемах с повышенной энергетической эффективностью *SDM*-300a, *CDM*-550.

## II Постановка задачи

Задачей, решаемой в работе, является описание характеристик составных элементов турбокодов. Для решения поставленной задачи рассмотрим основы теории построения компонентных кодов. Турбокод образуется при параллельном каскадировании двух или более свёрточных кодов, называемых компонентными, разделённых перемежителем. В связи с этим турбокоды иногда называют параллельными каскадными свёрточными кодами. Если в роли компонентных кодов используются стандартные блоковые коды – коды Хэмминга, БЧХ либо Рида-Соломона – то такие коды называют параллельными каскадными блоковыми кодами [2, 3, 4].

В турбокодах используются следующие положения теории кодирования [1 – 3]:

1 длинные коды с шумоподобной структурой обеспечивают предельно достижимую пропускную

способность канала;

2 эффективное применение алгоритмов вероятностного декодирования с использованием априорных вероятностей декодируемых символов на входе декодера и формированием решений о каждом декодированном символе с оценкой степени надежности этого решения (декодирование с "мягким выходом");

3 каскадная структура кода позволяет существенно упростить процедуру кодирования и декодирования;

4 конструктивный путь построения декодера длинного кода – итеративное декодирование (многократное использование одного декодера).

## III Кодер турбокода

Структурная схема кодера обобщённого турбокода приведена на рис. 1. В процессе кодирования информационная последовательность $U$ разбивается на блоки символов длины $N$. После этого сформированная последовательность поступает на систематический выход кодера $y^1$, а также параллельно на $k$ ветвей, состоящих из последовательного соединения устройства перемежения и компонентного кодера [1].

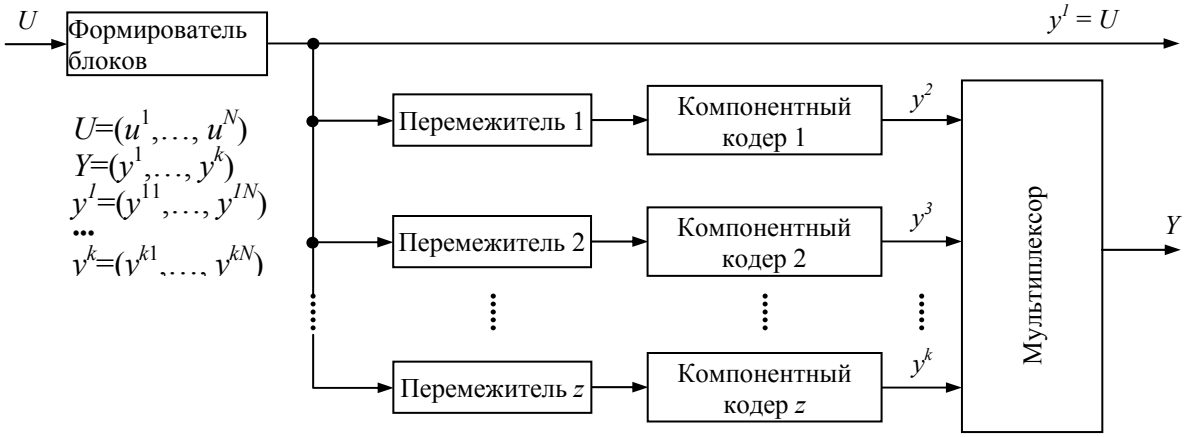


**Рисунок 1 – Структурная схема кодера обобщённого турбокода**

Кроме рассмотренной структуры существует последовательная и гибридная (последовательно-параллельная) структура построения турбокода [4]**.**

На рис. 2 показан пример кодера турбокода [3 – 5]. Этот турбокод включает два рекурсивных систематических сверточных кода (*RSC*). Первый составной кодер работает непосредственно с информационной последовательностью бит $U=(u^1,\ldots,u^N)$ длиной $N$, производя две выходные последовательности $y^1$ и $y^2$. Второй составной кодер оперирует с переставленной последовательностью информационных бит $y^3$, произведенную перемежителем длиной $N$. Переключатель делает скорость кодирования всего кода равной 1/2. Без переключателя скорость кодирования будет равна 1/3 (1/($k$+1)).

***Перемежитель*** – устройство, обеспечивающее перестановку позиций информационных бит исходной последовательности.

Перемежитель должен выполнять следующие задачи [6]:

1 чередование бит сообщения перед передачей и обратную операцию после приема, что приводит к рассеиванию пакета ошибок во времени: в результате они становятся для декодера случайно распределенными, поэтому турбокод с большим размером блока можно характеризовать как длинный случайный код;

2 преобразование входной информационной последовательности таким образом, чтобы комбинации, приводящие к кодовым словам с низким весом на выходе первого компонентного кодера, были преобразованы в комбинации, порождающие кодовые слова с высоким весом на выходе остальных кодеров, тем самым, обеспечивая небольшое число кодовых слов малого веса результирующего турбохода;

3 минимизирует корреляцию между внешними входами декодера.

Существует две категории устройств перемежения (рис. 3) – регулярные и псевдослучайные [6 – 8].

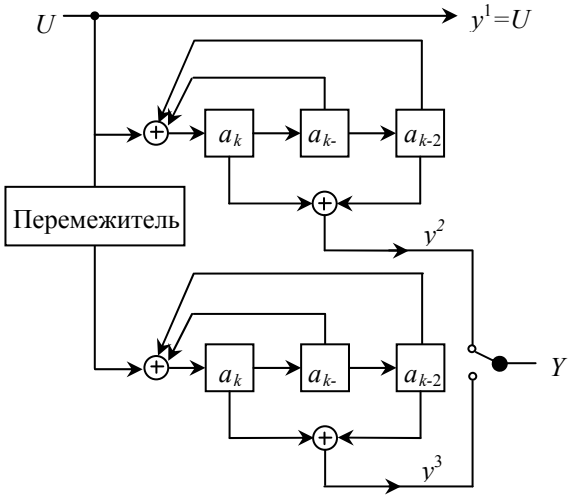


**Рисунок 2 – Схема параллельного соединения двух *RSC*-кодеров**


**Рисунок 3 – Классификация устройств перемежения**

К регулярным относятся такие устройства перемежения, метод формирования которых можно описать формулой либо строгой закономерностью.

Псевдослучайный перемежитель – это устройство, которое осуществляет перестановку символов внутри блока по псевдослучайному закону и формируется с помощью датчика псевдослучайных чисел. Обычно таблица перемежения такого устройства целиком сохраняется в памяти кодера и декодера.

## IV Декодирование турбокодов

Одной из главных особенностей декодирования турбокодов является использование принципа итеративного декодирования. Структурная схема декодера турбокода со скоростью $R$=1/3, который состоит из двух элементарных декодеров, двух перемежителей и двух деперемежителей, приведена на рис. 4, где $X^{C1}$, $X^{П2}$, $X^{П3}$ соответственно систематические и проверочные символы [2].

После выполнения определенного числа итераций декодер 2 выносит решение (с учетом операций деперемежения) о декодированных символах. Важная особенность заключается в том, что информация о каждом декодированном символе, который производится декодером и поступает на вход следующего

декодера, поддается перестановке. Поэтому она оказывается некореллированной с «мягкими канальными символами» на входе декодера и может быть использована в качестве априорной.

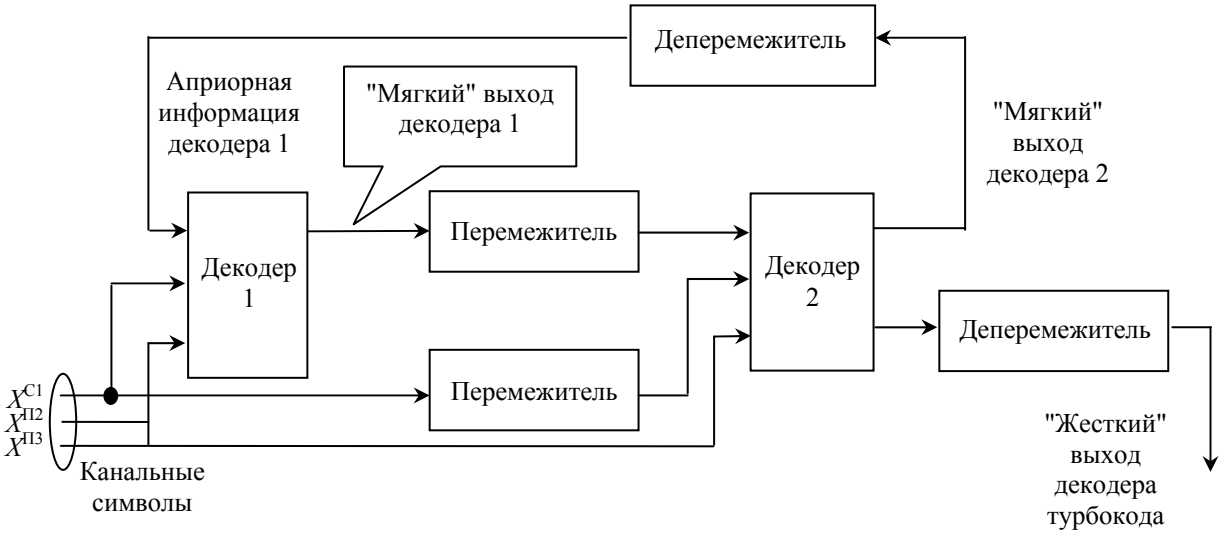


**Рисунок 4 – Структурная схема декодера турбокода со скоростью *R*=1/3**

## V Алгоритмы декодирования турбокодов

Высокая исправляющая способность турбокодов обусловлена разработанными для них эффективными алгоритмами декодирования. При декодировании турбокодов используются алгоритмы с "мягким" входом и "мягким" выходом (*SISO* алгоритмы). Данные алгоритмы можно разделить на два типа: первые происходят от оптимального алгоритма по максимуму апостериорной вероятности *MAP* (*max-log-MAP*, *log-MAP*), которые минимизируют вероятность ошибочного символа, вторые – от алгоритма Витерби, который минимизирует вероятность ошибочной последовательности символов (*SOVA* алгоритм).

Основным преобразованием над алгоритмом *MAP* является логарифмирование, поэтому алгоритм *MAP* более сложен в вычислении, чем алгоритм Витерби.

*Max-log-MAP* алгоритм основан на некоторых преобразованиях над оптимальным алгоритмом *MAP* и использовании аппроксимации. Основными преобразованиями над алгоритмом *MAP* является логарифмирование и аппроксимация.

Аппроксимация существенно ухудшает помехоустойчивость декодера *max-log-MAP* по сравнению с декодером *MAP*. Для улучшения алгоритма *max-log-MAP* предложено использовать логарифм Якобиана для более точного вычисления, т. е. максимизация дополнена корректирующим термином. Это значит, что *log-MAP* алгоритм немного сложнее, чем *max-log-MAP,* но дает точно такие значения, как *MAP* алгоритм. Поэтому данный алгоритм является более привлекательным при использовании в итеративном турбо декодере.

Основной задачей разработчиков алгоритма *SOVA* была модификация классического алгоритма Витерби таким образом, чтобы кроме жёстких (двухуровневых) решений о декодированных символах он позволял определять надёжности этих решений, а также использовать априорную “информацию” при поиске выжившего пути.

**Характеристики помехоустойчивости турбокода** [9 – 11].

Основные характеристики помехоустойчивости турбокодов определяются компьютерным моделированием с использованием основных алгоритмов декодирования, так как в настоящее время адекватного математического аппарата, описывающего характеристики турбокодов, в достаточной мере не разработано.

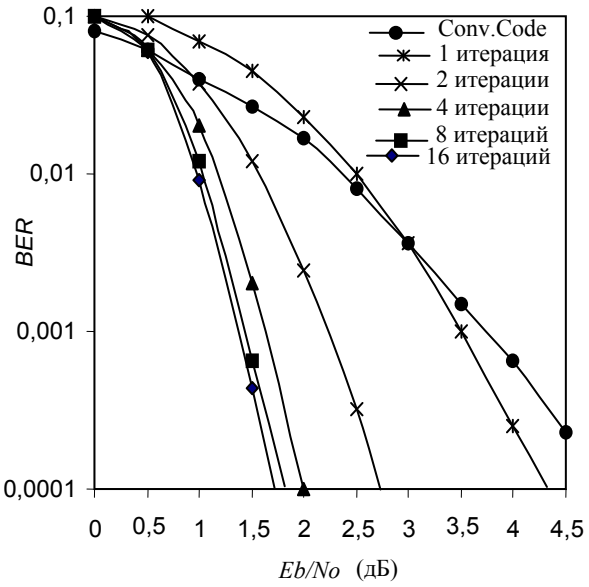


**Рисунок 5 – Зависимость характеристик турбокода от количества итераций**

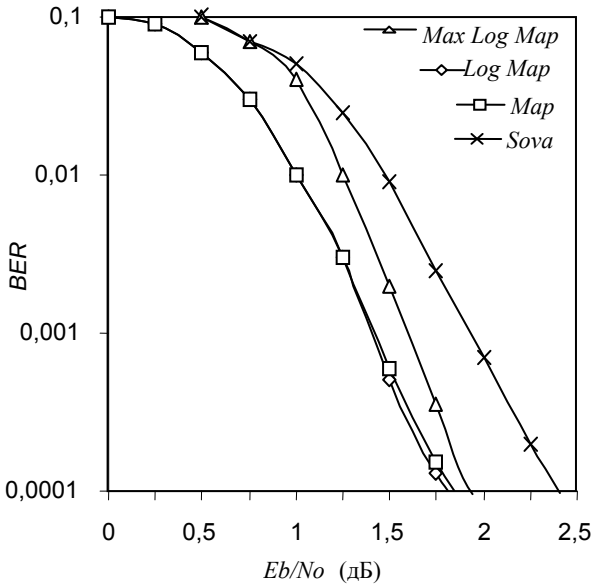


**Рисунок 6 – Зависимость характеристик турбокода от алгоритма декодирования**

На рис. 5 показано влияние количества итераций на характеристики турбокода, то есть зависимость частоты ошибки бита (*BER*) как функции соотношения энергии сигнала к спектральной плотности мощности шума ($E_b/N_0$), при использовании алгоритма декодирования *MAP* по сравнению с нерекурсивным сверточным кодом (conv. code – 2, 1, 3). Анализ показывает (табл. 1), что после первой итерации, при малых значениях $E_b/N_0$, характеристики турбокода и сверточного кода одинаковы. При увеличении количества итераций $L$ характеристики турбокода улучшаются, однако при $L > 8$ улучшение незначительное ($S < 0{,}1$ дБ), где $S$ – разность значений $E_b/N_0$ при $BER=10^{-4}$ между турбокодом и сверточным кодом.

Таблица 1 – Характеристики декодирования корректирующих кодов

| Количество итераций | $E_b/N_0$ при $BER = 10^{-4}$ | $E_b/N_0$ при $BER = 10^{-3}$ | $E_b/N_0$ при $BER = 10^{-2}$ | $E_b/N_0$ при $BER = 5 \times 10^{-2}$ | $S$ (*conv*) при $BER = 10^{-4}$ |
|---|---|---|---|---|---|
| 1 итерация | 4,25 | 3,5 | 2,55 | 0,35 | 0,4 |
| 2 итерации | 2,75 | 2,25 | 1,65 | 0,0 | 1,9 |
| 4 итерации | 2,0 | 1,65 | 1,15 | 0,0 | 2,6 |
| 8 итераций | 1,85 | 1,45 | 1,025 | 0,0 | 2,75 |
| 16 итераций | 1,75 | 1,4 | 1,0 | 0,0 | 2,85 |

На рис. 6 представлены характеристики турбокода при различных алгоритмах декодирования и использовании в его составе случайного перемежителя размером 1000 бит. Анализ показывает, что характеристики *Max Log MAP* и *Sova* алгоритмов несколько хуже алгоритмов *MAP* и *Log MAP* – при $BER = 10^{-4}$ приблизительно на 0,1 дБ и 0,6 дБ соответственно.

## VI Выводы

Рассмотренные характеристики показывают некоторое преимущество турбокодов перед известными блочными и сверточными корректирующими кодами и, поэтому, являются более предпочтительными при проектировании перспективных специальных телекоммуникационных систем.

*Литература:* ***1.*** *Варгаузин В., Протопопов Л. Турбокоды и итеративное декодирование: принципы, свойства, применение // TeleMultiMedia № 4(4), 2000. – С. 7-10.* ***2.*** *Банкет В. Л., Прокопов С. Д., Постовой А. Г., Топорков Ф. В. Алгоритм кодирования / декодирования турбокодов // Зв'язок.. – 2004. – № 4. – С. 45 - 46.* ***3.*** *Pyndian R., Glavieux A., Picart A., Jacq S. Near optimum decoding of product codes // in Proc. IEEE*

*Conf. Globecom-94. – 1994. – San Francisco. – CA. – November. – P. 339-343.* ***4.*** *Barbulescu A., Pietrobon S. Turbo Codes: a tutorial on a new class of powerful error correcting coding schemes. Part I: Code Structures and Interleaver Design // University of South Australia, 1998. – October. – P. 1 –22.* ***5.*** *Berrou C., Glavieux A.,Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes // Proc. Int. Conf. On Commun., ICC-93. – Geneva, 1993. – May. – P. 1064 – 1070.* ***6.*** *Hokfelt J., Edfors O., Maseng T. Interleaver Design for turbo codes based on the perfomance of iterative decoding // P. 1 – 5.* ***7.*** *Банкет В. Л., Прокопов С. Д., Постовой А. Г., Топорков Ф. В. Экспериментальное исследование процедур кодирования / декодирования турбокодов // Зв'язок. – 2004. – № 6. – С. 57-58.* ***8.*** *Ливенцев С. П., Алексеев Д. А., Зайцев С. В. Анализ характеристик перемежителей, используемых в турбокодах // Зв'язок. – 2005. – № 3. – С. 57-61.* ***9.*** *Qi J. Turbo code in IS-2000 code division multiple access communications under fading // Wichita State University. – 1999. P. 9-16.* ***10.*** *Woodard J., Hanzo L. Comparative Study of Turbo Decoding Techniques: An Overview // IEEE Transactions on Vehicular Technoligy, Vol. 49, No. 6, 2000. - November. P. 2208 – 2232.* ***11.*** *Robertson P., Villebrun E., Hoeher P. A comparison of optimal and sub-optimal MAP decoding algorithms operating in the log domain // in Proc. Int. Conf. on Commun., ICC-95. – 1995. – June. – P. 1009-1013.*

**УДК 681.3.06**

# ВЫСОКОСКОРОСТНОЙ UMAC АЛГОРИТМ

***Геннадий Халимов***
*Харковский национальний университет радиоэлектроники*

*Анотація:* **Розглядається високошвидкісний UMAC алгоритм, характеристики, параметри та оцінка таємності.**
*Suumary:* **The high-speed UMAC algorithm, characteristics, parameters and an estimation of privacy are considered.**
*Ключевые слова:* **UMAC алгоритм, универсальные хеш-функции.**

## I Введение

UMAC алгоритм, известный в модификациях UMAC (1999) [1] и UMAC (2000) [2], представлен проекту NESSIE как программно ориентированный для реализации на современных операционных платформах и обеспечивает чрезвычайно высокую скорость вычислений. Разработчики UMAC преследовали две главные цели:

- ✓ высокую скорость вычислений;
- ✓ доказуемую секретность.

Решение этих задач оказалось возможным на основе применения композиционной схемы с многократным универсальным хешированием и криптографическим вычислением тега аутентификации.

Задачей данной статьи является анализ основных характеристик UMAC кодов, изложение алгоритма построения и оценка секретности. С этой целью в разделе 2 приводятся основные определения универсальных хеш-функций UMAC реализации. В разделе 3 рассматриваются версии алгоритма UMAC (1999) и UMAC (2000). В разделе 4 оценена секретность UMAC схемы.

## II Определения универсальных хеш-функций UMAC реализации

Алгоритм UMAC является композиционной схемой универсального хеширования. Коды подлинности сообщений, основанные на универсальном хешировании, используют определение семейства хеш-функций [3].

**Определение 1.** $H=\{h: D\to R\}$ есть семейство хэш-функций с общей областью определения $D$ и конечным диапазоном значений $R$.

MAC коды являются отображением $H: K\times D\to R$, где $h = H_K: D\to R$ – функция, определенная для каждого $K \in K$ с заданным распределением на H. Основные универсальные семейства хэш-функций имеют следующие представления.

1. H является универсальным семейством хэш-функций $(\varepsilon\text{-}U)$, если для всех $x\neq y\in D$,

$$Pr_{h\in H}[h(x)=h(y)]=\varepsilon,\ \varepsilon=1/|R|.$$

2. H является $\Delta$-универсальным семейством хэш-функций $(\varepsilon\text{-}\Delta U)$, если для всех $x\neq y\in D$ и всех $a\in R$,

$$Pr_{h\in H}[h(x)-h(y)=a]=\varepsilon,\ \varepsilon=1/|R|.$$