*А. Г. Солтанов*

# СХЕМЫ ДЕКОДИРОВАНИЯ И ОЦЕНКА ЭФФЕКТИВНОСТИ LDPC-КОДОВ. ПРИМЕНЕНИЕ, ПРЕИМУЩЕСТВА И ПЕРСПЕКТИВЫ РАЗВИТИЯ

## Введение

Коды с малой плотностью проверок на четность (LDPC-код от англ. Low-density parity-check code, LDPC-code, низкоплотностный код) были впервые предложены Р. Галлагером и позднее исследовались во многих научных работах. Несмотря на то что в течение долгого времени LDPC-коды были практически исключены из рассмотрения, в последние годы наблюдается увеличение количества исследований в этой области. Это связано с тем, что, обладая плохим минимальным расстоянием, коды с малой плотностью, тем не менее, обеспечивают высокую степень исправления ошибок при весьма малой сложности их декодирования. Было показано, что с ростом длины некоторые LDPC-коды могут превосходить турбокоды и приближаться к пропускной способности канала с аддитивным белым гауссовским шумом (АБГШ). Вместе с тем многие предложенные конструкции LDPC-кодов являются циклическими или квазициклическими, что позволяет производить не только быстрое декодирование, но и эффективные процедуры кодирования. Кроме того, даже для LDPC-кодов, не обладающих свойством цикличности, были предложены эффективные процедуры кодирования.

Появление новых эффективных алгоритмов декодирования стимулировало и повышение интереса к методам построения недвоичных LDPC-кодов. Первоначально построение недвоичных LDPC кодов осуществлялось путем замены ненулевых элементов в проверочной матрице двоичных LDPC-кодов на случайные элементы конечного поля. Позднее Лиин (Lin) предложил методы алгебраического построения квазициклических недвоичных LDPC-кодов (QC NB-LDPC).

LDPC-коды становятся востребованными в системах передачи информации, требующих максимальной скорости передачи при ограниченной полосе частот. Основным конкурентом LDPC-кодов на данный момент являются турбокоды, которые нашли свое применение в системах спутниковой связи, ряде стандартов цифрового телевидения и мобильных системах связи третьего поколения. Однако LDPC-коды по сравнению с турбокодами имеют ряд преимуществ.

Во-первых, LDPC-коды обгоняют турбокоды по скорости декодирования.

Во-вторых, LDPC-коды более предпочтительны в каналах с меньшими вероятностями ошибок. С развитием методов передачи информации каналы передачи улучшаются, что дает хорошую перспективу для развития LDPC-кодов.

Имеет место также и правовой аспект применения LDPC-кодов и турбокодов. Компании France Telecom и Telediffusion de France запатентовали широкий класс турбокодов, что ограничивает возможность их свободного применения и в то же время стимулирует развитие и использование других методов кодирования, таких как LDPC.

## 1. Кодирование и декодирование LDPC-кодов

Кодирование в LDPC осуществляется путем умножения кодовых слов **c** на проверочную матрицу **H** и получения векторов **y**. При реализации кодера в нем может храниться сама проверочная матрица **H** (например, для коротких кодов), однако чаще встречаются другие аппаратные реализации. Наибольший интерес для исследователей представляет процедура декодирования, ввиду того что она является более времязатратной и ресурсоемкой.

Декодирование — это процедура поиска и исправления ошибки, наложенной каналом на кодовое слово, по принятому из канала вектору или собственно поиск кодового слова по вектору, принятому из канала.

Декодирование по максимуму правдоподобия кода **C** обозначает нахождение по заданному принятому вектору **y** такого кодового слова **c** из **C** (множества всех кодовых слов), которое максимизирует вероятность того, что передавалось слово с при условии принятия вектора **y**. Задача декодирования по максимуму правдоподобия является NP-полной.

Для оценки качества работы различных декодеров используется оценка вероятности ошибки декодирования (BER) на информационный бит, вычисляемая как отношение количества ошибочных информационных бит после декодирования к общему количеству переданных информационных бит. Итеративные схемы декодирования кодов с низкой плотностью проверок на четность не являются декодерами по максимуму правдоподобия, но позволяют получить разумный баланс по сложности и вероятности ошибки декодирования по сравнению с декодированием по максимуму правдоподобия. Итеративное декодирование подразумевает, что нахождение кодового слова будет производиться не за один проход, а за несколько, с последовательным уточнением результата на каждом шаге. Применяются следующие основные схемы декодирования.

### «Жесткое» декодирование

«Жесткое» декодирование — это схема декодирования для двоичного симметричного канала при небольшом количестве ошибок в канале. «Жесткое» декодирование инвертированием битов — самая простая схема декодирования кодов с низкой плотностью проверок на четность.

Под проверкой понимается любая строка $\mathbf{h} = \{h_0, ..., h_{N-1}\}$ из проверочной матрицы кода с низкой плотностью проверок на четность. Будем говорить, что проверка для некоего вектора $\mathbf{y} = \{y_0, ..., y_{N-1}\}$ выполняется тогда, когда скалярное произведение вектора **y** на проверку дает ноль. Будем говорить, что элемент $y_i$ принятого вектора **y** участвует в проверке $\mathbf{h} = \{h_0, ..., h_{N-1}\}$ тогда, когда соответствующий элемент проверки $h_i$ не равен нулю.

Одна итерация «жесткого» декодирования инвертированием битов производится следующим образом.

1. Для принятого вектора вычисляются все проверки.

2. Если некоторый бит принятого вектора участвовал более чем в половине невыполнившихся проверок, бит инвертируется.

3. После такого анализа всех символов принятого вектора вектор проверяется на принадлежность коду. Если вектор является кодовым словом, декодирование заканчивается, в противном случае выполняется следующая итерация алгоритма.

Такая процедура декодирования применима для кодов с низкой плотностью проверок на четность потому, что большинство проверок в таком случае будут содержать одну ошибку или не будут содержать ошибок вообще и тогда невыполнение большого количества проверок для символа принятого слова будет обозначать наличие в нем ошибки.

Сложность одной итерации «жесткого» декодирования инвертированием бит является линейной, количество итераций декодирования обычно выбирается около $\log_2(N)$, где $N$ — длина кодового слова.

### Декодирование по вероятностям

Декодирование по вероятностям является «мягким» декодированием, т. е. декодированием на основе вектора, состоящего не из дискретных значений (0 и 1), а из вещественных величин, полученных на выходе канала путем пересчета вероятностей (англ. belief propagation decoding).

На основе принятого из канала вектора формируются два (для двоичного случая) вектора вероятностей того, что в принятом векторе на данной позиции находился заданный символ.

Каждому ненулевому элементу проверочной матрицы кода с низкой плотностью проверок на четность приписываются две величины: $q^x_{i,j}$ и $r^x_{i,j}$. Величина $q^x_{i,j}$ является вероятностью того, что $j$-й символ принятого вектора имеет значение $x$ по информации, полученной из всех

проверок, кроме *i*-й. Величина $r^x_{i,j}$ является вероятностью того, что проверка *i* выполняется, если *j*-й символ принятого вектора равен *x*, а все остальные символы проверок имеют распределение вероятностей, заданное величинами $\{q^x_{i,j} : j \text{ из } N(i)\backslash j\}$, где N(i) — множество символов, входящих в i-ю проверку.

Перед началом работы алгоритму требуется инициализация, далее алгоритм работает по принципу пересчета вероятностей символов принятого вектора (belief propagation), используя для пересчета вероятностей правило Байеса для апостериорной вероятности события. Одна итерация алгоритма представляет собой следующую последовательность действий.

1. Для всех проверок вычисляются величины $\Delta r_{i,j}$ и пересчитываются вероятности $r^x_{i,j}$ для $x = \{0, 1\}$.

2. Для всех символов принятого вектора пересчитываются вероятности $q^x_{i,j}$.

3. Формируются векторы псевдоапостериорной вероятности $q^0_j$ и $q^1_j$.

4. Формируется вектор решения **c'** по следующему правилу: $c'_j = 1$, если $q^1_j > S$, иначе 0.

Если вектор **c'** является кодовым словом, декодирование заканчивается, в противном случае выполняется следующая итерация алгоритма.

Сложность данного алгоритма выше, чем сложность «жесткого» декодирования инвертированием битов, но качество декодирования повышается за счет использования дополнительной информации на выходе канала. Однако точность работы такого алгоритма зависит от инициализации: чем точнее она произведена, тем точнее будет конечный результат. Для канала с гауссовским шумом инициализация может быть произведена при помощи информации о дисперсии шума в канале. Для других распределений шума в канале или при неизвестных характеристиках шума точная инициализация алгоритма может оказаться сложной задачей.

### Быстрое декодирование LDPC

Несмотря на то что декодирование пересчетом вероятностей является эффективным методом для каналов с непрерывным выходом, тот факт, что сложность его значительно выше, чем сложность «жесткого» декодирования, создает предпосылки для поиска более быстрых алгоритмов декодирования, обладающих приемлемым качеством.

Среди известных алгоритмов быстрого декодирования кодов с низкой плотностью проверок на четность для каналов с непрерывным выходом наиболее известен алгоритм «min-sum», являющийся упрощением декодера «belief propagation», а также алгоритм UMP (Uniformly Most Powerful).

Сложность декодера UMP (быстрого декодирования по надежностям) значительно ниже, чем сложность декодера, пересчитывающего вероятности, за счет того, что пересчет надежностей выполняется по упрощенной схеме (схеме «взвешенного» мажоритарного голосования, в качестве «весов» используется надежность проверок), а также за счет возможности использования исключительно целочисленных операций сложения и сложения по модулю два. Также к достоинствам быстрого декодера по надежностям можно отнести то, что декодеру не требуется знать характеристики шума в канале (дисперсию и т. д.), следовательно, такой декодер может работать в любом симметричном канале с двоичным входом.

Недостатком быстрого декодера по надежностям является оценка вероятности ошибки декодирования, которая для канала с аддитивным гауссовским шумом оказывается на 0,5 дБ хуже, чем вероятность ошибки декодирования вероятностного декодера.

### Многопороговое декодирование

Основная идея многопорогового декодирования по надежностям состоит в том, чтобы изменять значения порогов инвертирования символов от одной итерации к другой следующим образом: на первых итерациях порог инвертирования символов выбирается так, чтобы количество инвертированных символов было минимальным (вплоть до инвертирования только одного

символа на первой итерации); на последующих итерациях пороги инвертирования постепенно повышаются.

При многопороговом декодировании, если на первой итерации была исправлена хотя бы одна ошибка, декодирование на последующих итерациях становится значительно проще и общее качество декодирования улучшается. По-прежнему для работы декодеру не требуется информация о шуме в канале, достаточно лишь задать надежности.

Декодер, работающий по многопороговой схеме, позволяет получить вероятность ошибки декодирования на 0,1–0,4 дБ лучше, чем обеспечивает быстрый декодер по надежностям UMP, практически приближаясь к вероятности ошибки, получаемой при вероятностном декодировании кодов с низкой плотностью проверок на четность. Помимо независимости от характеристик канала многопороговый декодер обладает свойством декодеров кодов с низкой плотностью проверок на четность, а именно универсальностью и применимостью для любой конструкции таких кодов.

Следует отметить, что эффективность нерегулярных LDPC-кодов оказывается выше эффективности регулярных кодов. Это объясняется тем, что в нерегулярных кодах из-за различного числа единиц в строках и столбцах информационные символы защищены по-разному. В результате при декодировании проявляется так называемый эффект волны, когда более защищенные биты декодируются быстрее и затем как бы помогают при декодировании менее защищенных бит.

## 2. Оценка эффективности недвоичных LDPC-кодов

Схема модели приведена на рис. 1. Для моделирования модема, канала связи и кодека Рида–Соломона использовались стандартные объекты и функции Matlab. Декодирование недвоичных LDPC-кодов производилось с помощью алгоритма FFTQSPA с максимальным количеством итераций декодирования, равным 20. Было проведено сравнение коротких ($N \approx 120$), средних ($N \approx 250$) и длинных ($N \approx 500$) кодов.

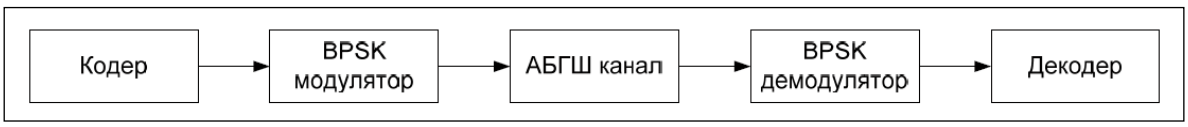


*Рис. 1. Схема модели*

При анализе коротких кодов сравнивались недвоичные LDPC-коды $N = 120$, $K = 71$, $R = 0{,}5917$, символы кода принадлежат GF(16), и коды Рида–Соломона $N = 127$, $K = 77$, $R = 0{,}6062$, символы кода принадлежат GF(128). Результаты моделирования этих кодов приведены на рис. 2. Как видно из рисунка, недвоичные LDPC-коды существенно превосходят коды Рида–Соломона. При вероятности ошибки на бит $10^{-5}$ это преимущество составляет 1,6 дБ.

При анализе кодов, имеющих среднюю длину блока, сравнивались недвоичные LDPC-коды $N = 248$, $K = 137$, $R = 0{,}5524$, символы кода принадлежат GF(32), и коды Рида–Соломона $N = 255$, $K = 141$, $R = 0{,}5529$, символы кода принадлежат GF(256). Результаты моделирования этих кодов приведены на рис. 3. При данной длине блока при вероятности ошибки на бит $10^{-5}$ преимущество NB-LDPC составляет 2 дБ.

При анализе длинных кодов сравнивались недвоичные LDPC-коды $N = 504$, $K = 267$, $R = 0{,}5297$, символы кода принадлежат GF(64), и коды Рида–Соломона $N = 511$, $K = 271$, $R = 0{,}5303$, символы кода принадлежат GF(512). Результаты моделирования этих кодов приведены на рис. 4. При вероятности ошибки на бит $10^{-5}$ преимущество NB-LDPC составляет 2,4 дБ.

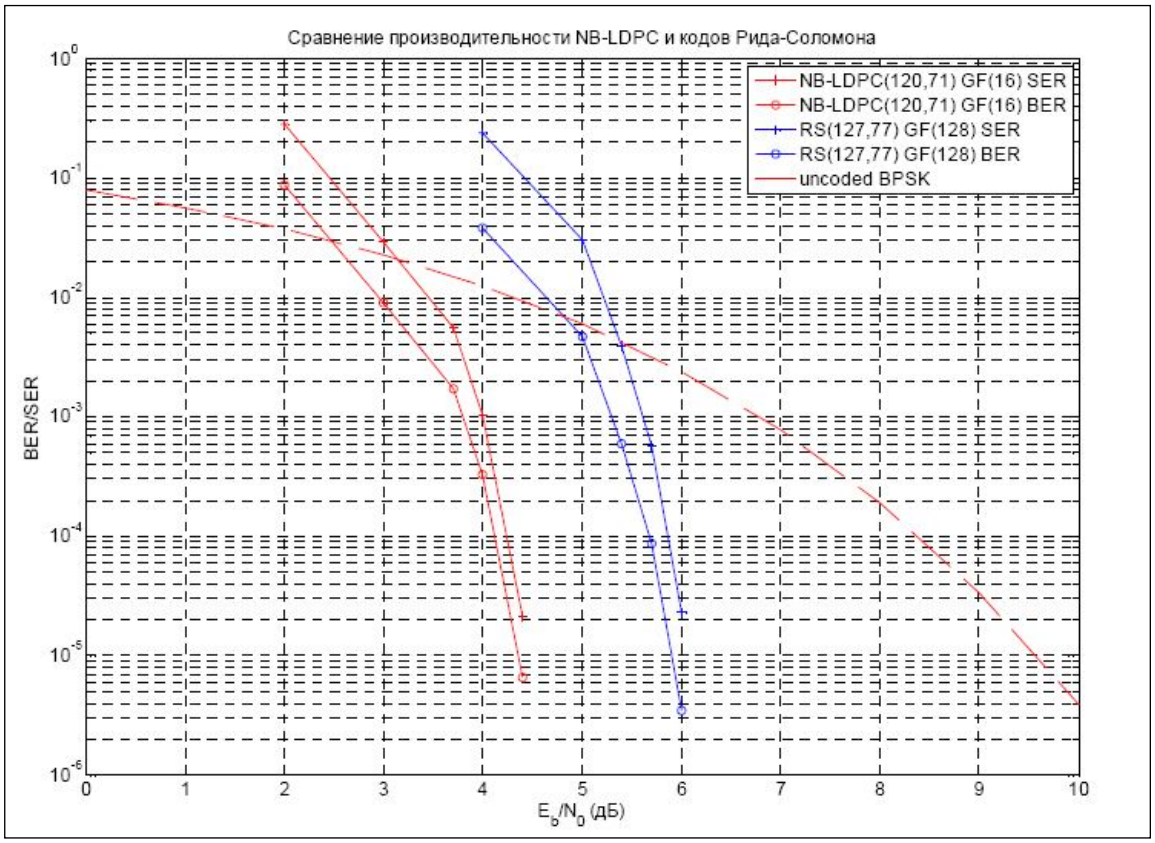


*Рис. 2. Сравнение производительности NB-LDPC и кодов Рида–Соломона при небольшой длине блока*

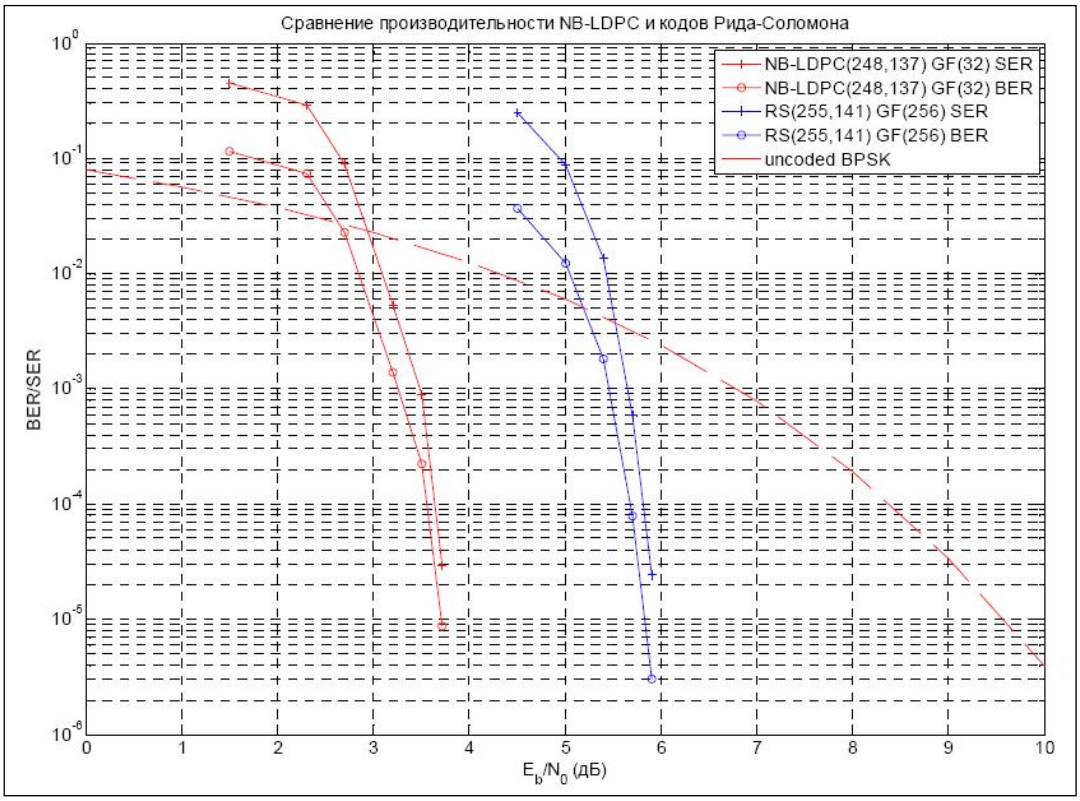


*Рис. 3. Сравнение производительности NB-LDPC и кодов Рида–Соломона при средней длине блока*

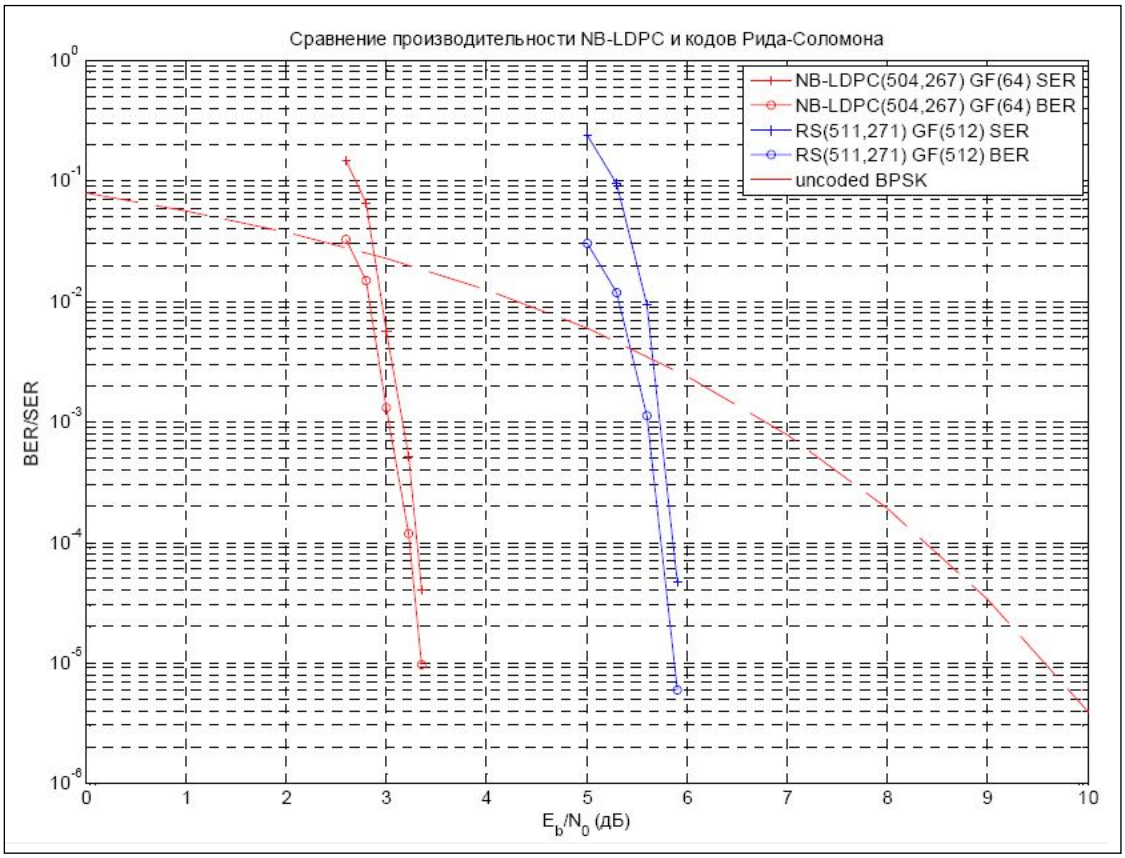


*Рис. 4. Сравнение производительности NB-LDPC и кодов Рида—Соломона при большой длине блока*

### 3. Преимущества LDPC-кодов, их применение и перспективы развития

LDPC-коды в современных системах передачи информации занимают нишу, аналогичную турбокодам. Оба эти класса кодов используются в системах, где требуются повышенные скорости передачи данных при ограниченной полосе пропускания канала. К числу таких систем можно отнести, например, спутниковую связь, цифровое телевидение (в том числе высокой четкости), а также каналы передачи в электронно-вычислительных машинах и их сетях. LDPC-кодеры могут обеспечивать поистине колоссальную скорость передачи данных (до 40 Гб/с), что обусловлено простотой их реализации. Наиболее быстрыми декодерами разумно было бы считать многопороговые декодеры (МПД), декодирующие по одноименному алгоритму, о котором говорилось выше. В МПД 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. Например, МПД может быть реализован с использованием линейных сдвиговых регистров — самых быстрых аппаратных элементов.

Следует отметить, что LDPC-кодирование не является сугубо теоретической разработкой, а уже активно используется и введено в некоторые стандарты. Например, в 2003 г. LDPC-код вместо турбокода стал частью стандарта DVB-S2 спутниковой передачи данных для цифрового телевидения. Аналогичная замена произошла и в стандарте DVB-T2 для цифрового наземного телевизионного вещания. Также LDPC-коды вошли в стандарт IEEE 802.3an сети Ethernet 10G и другие.

По результатам исследования среди кодов для включения в стандарт DVB-S2 были отмечены следующие преимущества:

- отставание от границы Шеннона всего на 0,6—0,8 дБ;
- преимущество на 0,3 дБ по сравнению с лучшим из представленных турбокодов;
- преимущество на 2,5—3,0 дБ, т. е. 30-процентный прирост в мощности, по сравнению со стандартом DVB-S.

**Заключение**

Вышеизложенный материал позволяет сделать вывод, что развитие каналов связи, влекущее за собой уменьшение количества ошибок, а также все увеличивающиеся объемы передаваемой информации открывают широкие перспективы для дальнейшего внедрения и использования LDPC-кодов.

Были проведены моделирование работы недвоичных LDPC-кодов и сравнение их производительности с производительностью кодов Рида—Соломона. Результаты моделирования показали, что недвоичные LDPC-коды имеют существенное преимущество над кодами Рида—Соломона. Это преимущество увеличивается по мере увеличения длины кода и разрядности символа.

Современные исследования в основном сосредоточены на создании LDPC-кодов с улучшенными характеристиками, а также методов их декодирования. Например, кодов на базе евклидовых геометрий. Для таких кодов также создаются и развиваются специальные методы декодирования и ускоренного декодирования с приемлемыми потерями в вероятности декодирования, и они показывают неплохие результаты. Дальнейшее развитие в рамках данной проблематики заключается в отработке современных алгоритмических решений в области кодирования и декодирования LDPC-кодов, а также в эмпирической проверке результатов современных теоретических исследований в этой области.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Овчинников А.* К вопросу о построении LDCP-кодов на основе евклидовых геометрий // Вопросы передачи и защиты информации: Сборник статей под ред. А. Крука. СПбГУАП. СПб., 2006. — 226 с.
2. *Белоголовый А. В., Крук Е. А.* Многопороговое декодирование кодов с низкой плотностью проверок на четность // Вопросы передачи и защиты информации: Сборник статей под ред. А. Крука. СПбГУАП. СПб., 2006. — 226 с.
3. *Золотарев В. В., Овечкин Г. В.* Обзор исследований и разработок методов помехоустойчивого кодирования (по состоянию на 2005 год). URL: http://www.mtdbest.ru/articles/obzor_po_kodir2.pdf.
4. LDPC Codes, Application to Next Generation Communication Systems - Dr. Lin-Nan Lee Vice President. - Hughes Network Systems, Germantown, Maryland 20854, October 8, 2003.
5. *Воробьев К. А.* Методы построения и декодирования недвоичных низкоплотностных кодов // Теория и практика системного анализа. 2010. Т. II. С. 96—102.
6. *Gallager R. G.* Low density parity check codes // IRE Trans. Inform. Theory. Jan. 1962. Vol. IT-8. P. 21—28.