УДК 621.391

МЕТОД КОМБИНИРОВАННОГО ДЕКОДИРОВАНИЯ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

Н.А. ШТОМПЕЛЬ
Украинский государственный университет железнодорожного транспорта

Abstract *– The error-correcting codes have been widely used in telecommunication systems. Currently low-density parity check codes became widespread. These codes have some advantages over turbo-codes and other code constructions. The iterative hard and soft decoding methods of low-density parity check codes are used. The soft belief propagation decoding allows increasing correcting capabilities such codes. Belief propagation decoding is suboptimal decoding and has reasonable error probability only for long low-density parity check codes. The maximum likelihood decoding can not be achieved even for medium-length codes in practice. The features of several decoding methods of block codes and low-density parity check codes are presented. The parity-check matrix and graphical representation of binary and bipolar low-density parity check codes are described. The joint approach for decoding low-density parity check codes with using population-based procedures is proposed. On the first stage of joint decoding hard decoding is performed on the basis on syndrome. Further soft belief propagation decoding is applied. After that decoding with using reliability information about received symbols and population-based procedures are performed. The implementation features of main decoding stages are given. The research results of performance joint decoding method for codes with different parameters are presented. Analysis of the obtained results showed that joint decoding method can be used for relatively long low-density parity check codes. The performance joint decoding method decreases with growth of the code length.*

Анотація *– Запропоновано комбінований підхід до декодування кодів з малою щільністю перевірок на парність з використанням популяційних процедур. Приведено особливості реалізації основних етапів декодування. Представлено результати дослідження ефективності методу комбінованого декодування для кодів з різними параметрами.*

Аннотация *– Предложен комбинированный подход к декодированию кодов с малой плотностью проверок на четность с использованием популяционных процедур. Приведены особенности реализации основных этапов декодирования. Представлены результаты исследования эффективности метода комбинированного декодирования для кодов с разными параметрами.*

Введение

Для повышения достоверности передачи информации в телекоммуникационных системах широко используются различные методы помехоустойчивого кодирования. В настоящее время распространение получили коды с малой плотностью проверок на четность, которые обладают рядом преимуществ по сравнению с турбокодами и другими кодовыми конструкциями. Одним из ключевых достоинств данных кодов является возможность применения итеративных методов мягкого и жесткого декодирования с относительно низкой вычислительной сложностью. Стандартный метод жесткого декодирования кодов с малой плотностью проверок на четность основывается на инвертировании наименее надежного бита в принятой последовательности и находит применение в высокоскоростных телекоммуникационных системах. Для улучшения корректирующей способности кодов данного класса часто используется метод мягкого декодирования на основе распространения доверия. Хотя данный метод не обеспечивает достижения границы декодирования по максиму-

му правдоподобия, его применение позволяет приблизиться к пропускной способности канала с аддитивным белым гауссовым шумом для некоторых видов кодов с малой плотностью проверок на четность [1-2].

Следует отметить, что представленные методы итеративного декодирования данных кодов являются субоптимальными и обеспечивают приемлемую вероятность ошибки декодирования только для длинных кодов (длиной более нескольких тысяч бит). С другой стороны, декодирование по максимуму правдоподобия (оптимальное декодирование) кодов с малой плотностью проверок на четность даже средней длины (длиной порядка сотен бит) невозможно реализовать на практике [3].

В [4] предложен метод декодирования линейных блоковых кодов, который основан на использовании информации о надежности принятых символов и процедуре упорядочивания статистик. Из-за высокой вычислительной сложности последней процедуры данный метод декодирования может быть использован только для кодов с малой плотностью проверок на четность малой размерности (длиной до нескольких десятков бит).

Идея декодирования блоковых кодов по упорядоченным статистикам легла в основу метода декодирования [5], особенностью которого является совместное использование популяционных процедур поисковой оптимизации и наиболее надежного базиса.

В [6] предложен подход к мягкому декодированию кодов с малой плотностью проверок на четность с последовательным применением идей декодирования на основе распространения доверия и декодирования по упорядоченным статистикам, который имеет характеристики близкие к декодированию максимуму правдоподобия и обеспечивает возможность варьирования между вычислительной сложностью и энергетическим выигрышем от кодирования. В значительной степени вычислительная сложность данного метода декодирования определяется особенностями процедуры упорядочивания статистик, что ограничивает область его применения в высокоскоростных телекоммуникационных системах.

Таким образом, актуальной задачей является обеспечение заданной достоверности передачи информации в современных телекоммуникационных системах путем разработки метода декодирования относительно длинных кодов с малой плотностью проверок на четность с приемлемой вычислительной сложностью.

Целью статьи является повышение эффективности мягкого декодирования кодов с малой плотностью проверок на четность для обеспечения заданной достоверности передачи информации в телекоммуникационных системах.

Основная часть

Пусть задан двоичный код с малой плотностью проверок на четность C' с длиной N и размерностью K, который полностью определяется проверочной матрицей H и порождающей матрицей G.

Тогда двоичный вектор $c' = (c'_1, c'_2, ..., c'_N)$ является кодовым словом данного кода, только если $c'H^T = 0$, что в развернутом виде соответствует вычислению i-ых составляющих синдрома (проверочных условий):

$$s'_i = \sum_{j=1}^{N} h_{i,j} c'_i = 0 \,(\mathbf{mod} 2),\ i = 1, 2, ..., N - K, \qquad (1)$$

где $h_{i,j}$ – элемент проверочной матрицы, $h_{i,j} \in \{0, 1\}$;

c'_i – элемент двоичного вектора, $c'_i \in \{0, 1\}$.

Применим отображение двоичных символов в символы поля действительных чисел R вида $c_j \to (-1)^{c'_j}$, что соответствует отображению двоичного кода C' в биполярный код C (т.е. осуществим отображение вида $C' \to C$).

При этом вектор $c = (c_1, c_2, ..., c_N)$ с элементами $c_j \in \{1, -1\}$ по аналогии с (1) является кодовым словом биполярного кода C, только если

$$s_i = \prod_{j=1}^{N} c_j^{h_{i,j}} = 1,\ i = 1, 2, ..., N - K. \qquad (2)$$

В таком случае задача мягкого декодирования кодов с малой плотностью проверок на четность «по ближайшему соседу» для канала с аддитивным белым гауссовым шумом состоит в поиске кодового слова $c \in C$, которое для заданного принятого вектора $r = (r_1, r_2, ..., r_N)$ с элементами $r_j \in R$ минимизирует евклидово расстояние $\sum_{j=1}^{N} (r_j - c_j)^2$, что, в свою очередь, соответствует максимизации $\sum_{j=1}^{N} r_j c_j$. При замене принятого вектора r на вектор правдоподобия $\phi = (\phi_1, \phi_2, ..., \phi_N)$, где $\phi_j = \mathbf{ln}\left(\frac{P(r_j \mid 1)}{P(r_j \mid 0)}\right)$, декодирование «по ближайшему соседу» соответствует декодированию по максимуму правдоподобия для любого дискретного канала без памяти. Однако при этом вычислительная сложность декодирования растет экспоненциально с увеличением длины кода N, что ограничивает область применения данного подхода только кодами малой длины.

Для повышения эффективности декодирования относительно длинных кодов с малой плотностью проверок на четность в данной работе предлагается реализовать совместное использование идей декодирования на основе распространения доверия и декодирования на основе популяционных процедур поисковой оптимизации с использованием информации о надежности принятых символов. Суть предлагаемого метода декодирования заключается в том, что результат, получаемый после каждой итерации декодирования на основе распространения доверия, используется в качестве исходных данных для декодирования на основе популяционных процедур поисковой оптимизации.

Для описания основных шагов декодирования на основе распространения доверия целесообразно использовать представление кодов с малой плотностью проверок на четность в виде графов Таннера, которые содержат битовые и проверочные

вершины, соединенные ребрами. Структура графа Таннера полностью определяется проверочной матрицей кода, которая фактически является матрицей инцидентности данного графа. Связь между матричным и графовым представлением кодов с малой плотностью проверок на четность может быть представлена такими двумя множествами. Множество $V(i) \equiv \{j \in [1, N] : h_{i,j} = 1\}$ включает битовые вершины, которые связаны с i-ой проверочной вершиной, т.е. определяет принятые символы, входящие в i-ое проверочное условие (1). Множество $P(j) \equiv \{i \in [1, N - K] : h_{i,j} = 1\}$ включает проверочные вершины, которые связаны с j-ой битовой вершиной, т.е. определяет проверочные условия (1), в которых задействован j-ый принятый символ. Декодирование на основе распространения доверия основано на последовательном уточнении элементов предполагаемого кодового слова и проверке условия (1), что соответствует итеративному обмену сообщениями между битовыми и проверочными вершинами графа Таннера.

С другой стороны, декодирование на основе популяционных процедур поисковой оптимизации с учетом информации о надежности принятых символов использует структуру модифицированной порождающей матрицы кодов с малой плотностью проверок на четность и целевую функцию, получаемую из (2) путем определения K наиболее надежных принятых символов (независимых элементов предполагаемого кодового слова) – вектора $\tilde{c} = (c_1, c_2, ..., c_K)$.

Используемая в данном методе декодирования целевая функция имеет следующий вид:

$$f(\tilde{c}) = \sum_{j=1}^{N} r_j c_j = r_1 c_1 + r_2 c_2 + ... + r_K c_K + r_{K+1} \pi_{K+1}(\tilde{c}) + ... + r_N \pi_N(\tilde{c}), \qquad (3)$$

где $c_i = \pi_i(\tilde{c}) = \prod_{j=1}^{N} c_j^{p_{i,j}}$, $i = K+1, K+2, ..., N$ – зависимые элементы предполагаемого кодового слова; $p_{i,j} \in \{0, 1\}$ – элементы, определяемые из $N-K$ проверочных условий (2) на основании K наиболее надежных независимых принятых символов.

Основные этапы предлагаемого метода комбинированного декодирования кодов с малой плотностью проверок на четность представлены ниже.

Стадия 1. Жесткое декодирование на основе синдрома (проверочных условий).

Шаг 1. Пусть $c'_j = sign(r_j)$, где $c'_j = 0$, если $r_j \geq 0$, и $c'_j = 1$ – в противном случае; для $j = 1, 2, ..., N$. В результате получаем вектор $c' = (c'_1, c'_2, ..., c'_N)$.

Шаг 2. Если проверочное условие (1) выполняется для всех $i = 1, 2, ..., N-K$, то вектор c' является двоичным кодовым словом и процесс декодирования завершается, в противном случае осуществляется переход к стадии 2.

Стадия 2. Мягкое декодирование на основе распространения доверия.

Этап 1. Инициализация.

Установка для j-ой битовой вершины, которая соединена ребром с i-ой проверочной вершиной, следующих значений вероятностей:

$$p_j^1 = \frac{1}{1+e^{\frac{2r_j}{\sigma^2}}}, \qquad p_j^0 = 1 - p_j^1, \tag{4}$$

$$P_{ij}^1 = p_j^1, \qquad P_{ij}^0 = 1 - P_{ij}^1, \tag{5}$$

где p_j^1, p_j^0 – вероятности того, что j-й элемент принятого вектора $c'_j = 1$ или $c'_j = 0$ соответственно;

σ^2 – дисперсия канала с аддитивным белым гауссовым шумом;

P_{ij}^1, P_{ij}^0 – вероятности того, что j-й элемент принятого вектора $c'_j = 1$ или $c'_j = 0$, которые определяются на основе информации, полученной из всех проверочных условий, кроме условия s'_i, соответственно.

Этап 2. Передача сообщений от проверочных вершин к битовым вершинам.

Шаг 1. Вычисление для каждой i-ой проверочной вершины, связанной ребром с j-ой битовой вершиной, разницы между значениями вероятностей (5) и вспомогательной величины:

$$\Delta P_{ij} = P_{ij}^0 - P_{ij}^1,$$

$$\Delta Q_{ij} = \prod_{j'} \Delta P_{ij'},$$

где $j' \in V(i) \setminus \{N\}$.

Шаг 2. Определение вероятности того, что проверочное условие s'_i выполняется, если j-ый элемент принятого вектора $c'_j = 1$ или $c'_j = 0$ соответственно:

$$Q_{ij}^1 = \frac{1}{2}(1 - \Delta Q_{ij}), \qquad Q_{ij}^0 = \frac{1}{2}(1 + \Delta Q_{ij}). \tag{6}$$

Этап 3. Передача сообщений от битовых вершин к проверочным вершинам.

Шаг 1. Вычисление вероятностей (5) для каждой j-ой битовой вершины, соединенной ребром с i-ой проверочной вершиной, с учетом условия нормировки $P_{ij}^0 + P_{ij}^1 = 1$:

$$P_{ij}^1 = p_j^1 \prod_{i'} Q_{i'j}^1, \qquad P_{ij}^0 = p_j^0 \prod_{i'} Q_{i'j}^0,$$

где $i' \in P(j) \setminus \{N - K\}$.

Шаг 2. Определение апостериорных вероятностей, уточняющих значения вероятностей (4), с учетом (6) и условия нормировки $P_j^0 + P_j^1 = 1$:

$$P_j^1 = p_j^1 \prod_i Q_{ij}^1, \qquad P_j^0 = p_j^0 \prod_i Q_{ij}^0. \tag{7}$$

Этап 4. Проверка условия окончания декодирования.

Шаг 1. Определение значения j-ого элемента предполагаемого двоичного кодового слова $\hat{c}'$ на основе значений вероятностей, полученных с помощью (7):

$$\hat{c}'_j = \begin{cases} 0, при\, \phi_j = \ln(P_j^1 / P_j^0) \geq 0, \\ 1, при\, \phi_j = \ln(P_j^1 / P_j^0) < 0, \end{cases} \quad (8)$$

где ϕ_j – элемент вектора правдоподобия.

Шаг 2. Если для предполагаемого двоичного кодового слова $\hat{c}'$ выполняются проверочные условия (1), то процесс декодирования завершается, в противном случае – переход к стадии 3.

Стадия 3. Декодирование на основе популяционных процедур поисковой оптимизации.

Этап 1. Нахождение наиболее надежного базиса с использованием вероятностей (7), который вычисляется с помощью двух перестановок порождающей матрицы G.

Шаг 1. Размещение элементов вектора правдоподобия ϕ_j в порядке уменьшения их надежности $|\phi_j|$, что определяет перестановку столбцов π_1 матрицы G.

Шаг 2. Упорядочивание столбцов матрицы G в соответствии с перестановкой π_1, т.е. получение матрицы $G' = \pi_1(G)$.

Шаг 3. Формирование матрицы G'' таким образом, чтобы ее первые K столбцов были первыми K независимыми столбцами матрицы G', что определяет перестановку столбцов π_2 матрицы G'.

Шаг 4. Упорядочивание столбцов матрицы G' в соответствии с перестановкой π_2, т.е. получение матрицы $G'' = \pi_2(G')$, которая в систематической форме задает наиболее надежный базис G_s.

Этап 2. Поиск с использованием популяционных процедур поисковой оптимизации вектора $\tilde{c}$, который обеспечивает максимальное значение функции (3).

Шаг 1. Инициализация популяции. В области поиска создается заданное число пробных векторов путем формирования биполярного вектора $\tilde{c}$, в соответствии с K «наиболее надежными» независимыми позициями в векторе правдоподобия ϕ, и случайных биполярных векторов длиной K.

Шаг 2. Миграция агентов популяции. С помощью некоторого набора миграционных операторов, специфичных для каждой из популяционных процедур, агенты перемещаются в области поиска таким образом, чтобы в итоге приблизиться к искомому экстремуму целевой функции $f(\tilde{c})$.

Шаг 3. Окончание поиска. Если число итераций меньше максимального числа итераций L_{max}, то возвращаемся к шагу 2, в противном случае – текущий вектор $\tilde{c}$ является наиболее вероятной информационной частью кодового слова c_s, которое можно сформировать с использованием надежного базиса G_s.

Этап 3. Проверка условия окончания декодирования.

Шаг 1. Формирование оценки предполагаемого биполярного кодового слова с помощью обратного отображения $\hat{c} = \pi_1^{-1}[\pi_2^{-1}(c_s)]$.

Шаг 2. Если для предполагаемого биполярного кодового слова $\hat{c}$ выполняются проверочные условия (2), то процесс декодирования завершается; в противном случае, если не достигнуто максимальное число итераций, – переход к стадии 2 с использованием в качестве начальных значений полученных вероятностей (7).

Таким образом, в процессе декодирования согласно предложенного метода сначала осуществляется жесткое решение на основании принятого вектора r, в результате которого формируется двоичный вектор c'. Если проверочное условие выполняется для каждого элемента данного вектора, то принимается решение, что данный вектор является переданным кодовым словом и процесс декодирования завершается. В противном случае выполняется одна итерация декодирования на основе распространения доверия и по результатам проверки условия окончания декодирования выносится решение о переданном кодовом слове $\hat{c}'$ или осуществляется переход к декодированию на основе популяционных процедур поисковой оптимизации. При достижении максимального числа итераций формируется наиболее вероятное биполярное кодовое слово $\hat{c}$ и процесс декодирования завершается.

Предложенный метод декодирования предполагает возможность применения различных популяционных процедур поисковой оптимизации, особенности и характеристики которых представлены в [7]. Для оценки эффективности разработанного метода декодирования кодов с малой плотностью проверок на четность используем процедуру роя частиц, которая часто применяется в качестве поискового механизма при решении различных оптимизационных задач.

Экспериментальные исследования проводились путем компьютерного моделирования процесса передачи информации через канал с аддитивным белым гауссовым шумом при использовании различных кодов с малой плотностью проверок на четность, для декодирования которых применялись разработанный метод комбинированного декодирования и классический метод декодирования на основе распространения доверия. При проведении моделирования ограничивалось максимальное число итераций декодирования: для стандартного метода – 50 итераций, для предлагаемого метода – 20 итераций.

Результаты моделирования (в логарифмическом масштабе) для кода с малой плотностью проверок на четность с длиной 504 и размерностью 252 бита представлены на рис. 1.

Из рис. 1 следует, что предложенный метод декодирования позволяет повысить достоверность передачи информации по сравнению со стандартным методом декодирования кодов с малой плотностью проверок на четность, в частности, при отношении сигнал/шум 2 дБ выигрыш составляет более одного порядка.

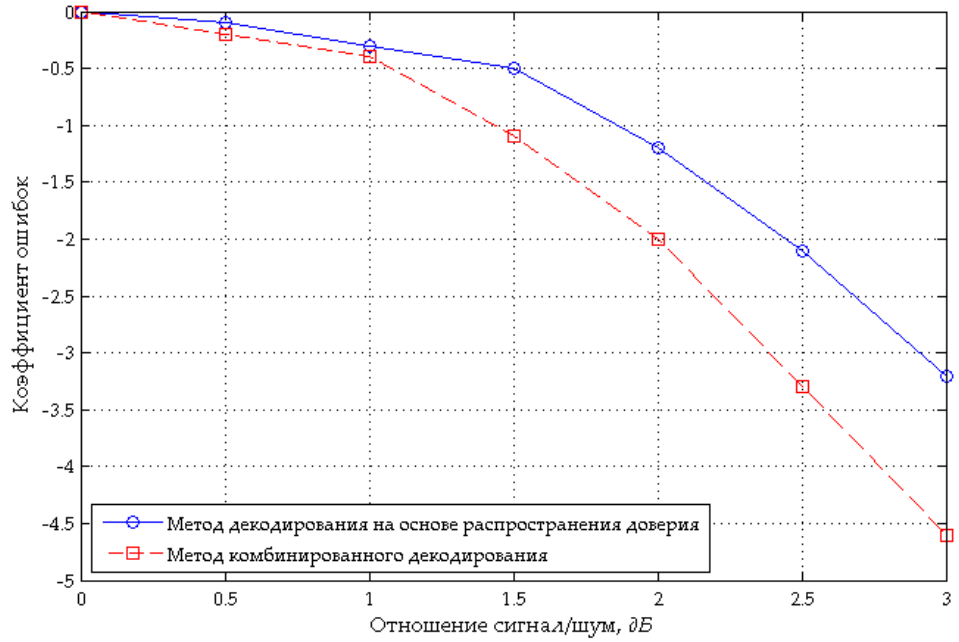

Рис. 1. Зависимость коэффициента ошибок от отношения сигнал/шум для кода с малой плотностью проверок на четность с длиной 504 и размерностью 252 бита

Результаты моделирования (в логарифмическом масштабе) для кода с малой плотностью проверок на четность с длиной 1008 и размерностью 504 бита представлены на рис. 2.

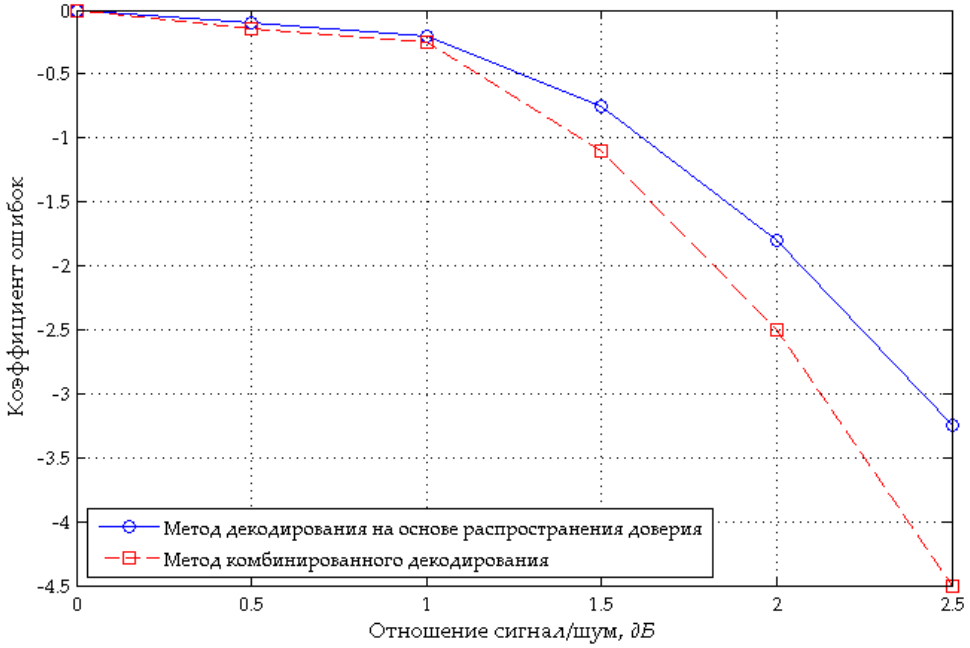

Рис. 2. Зависимость коэффициента ошибок от отношения сигнал/шум для кода с малой плотностью проверок на четность с длиной 1008 и размерностью 504 бита

Из рис. 2 следует, что при увеличении длины кода происходит снижение эффективности разработанного метода декодирования кодов с малой плотностью проверок на четность, например, при отношении сигнал/шум 2 дБ выигрыш составляет менее одного порядка.

Выводы

Предложен подход к декодированию кодов с малой плотностью проверок на четность, который основан на совместном использовании идей декодирования на основе распространения доверия и декодирования на основе популяционных процедур поисковой оптимизации. Из проведенных исследований следует, что разработанный метод декодирования можно использовать для относительно длинных кодов с малой плотностью проверок на четность, однако его эффективность снижается при увеличении длины кода.

Список литературы:

1. *Штомпель Н.А.* Методы мягкого декодирования кодов с малой плотностью проверок на четность // Вісник Національного технічного університету «Харківський політехнічний інститут»: збірник наукових праць. – 2013. – № 27 (1000). – С. 163 – 168.

2. *Штомпель Н.А.* Вычислительная сложность методов декодирования кодов с малой плотностью проверок на четность // Системи обробки інформації: збірник наукових праць. – 2013. – Вип. 6 (113). – С. 177 – 180.

3. *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение: пер. с англ. – Москва: Техносфера, 2005. – 320 с.

4. *Fossorier M.P.C., Lin S.* Soft-decision decoding of linear block codes based on ordered statistics // IEEE Transactions on Information Theory. – 1995. – Vol. 41, № 5. – P. 1379 – 1396.

5. Метод декодирования линейных блоковых кодов на основе популяционных процедур поисковой оптимизации / А.С. Жученко, Н.Г. Панченко, С.В. Панченко [и др.] // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – 2016. – Вип. 2 (117). – С. 25 – 29.

6. *Fossorier M.P.C.* Iterative reliability-based decoding of low-density parity check codes // IEEE Journal on Selected Areas in Communications. – 2001. – Vol. 19, № 5. – P. 908 – 917.

7. *Карпенко А. П.* Современные алгоритмы поисковой оптимизации. Алгоритмы, вдохновленные природой: учебное пособие. – Москва: Издательство МГТУ им. Н. Э. Баумана, 2014. – 446 с.