На правах рукописи

УСАТЮК ВАСИЛИЙ СТАНИСЛАВОВИЧ

МЕТОД, АППАРАТНО-ОРИЕНТИРОВАННЫЙ АЛГОРИТМ И СПЕЦИАЛИЗИРОВАННОЕ УСТРОЙСТВО ДЛЯ ПОСТРОЕНИЯ НИЗКОПЛОТНОСТНЫХ КОДОВ АРХИВНОЙ ГОЛОГРАФИЧЕСКОЙ ПАМЯТИ

Специальность 05.13.05 – Элементы и устройства
вычислительной техники и систем управления

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

КУРСК – 2022

Работа выполнена в Юго-Западном государственном университете

Научный руководитель:	доктор технических наук, доцент **Егоров Сергей Иванович**
Официальные оппоненты:	**Назаров Лев Евгеньевич** доктор физико-математических наук, старший научный сотрудник, Фрязинский филиал Федерального государственного бюджетного учреждения науки «Институт радиотехники и электроники им В.А. Котельникова» Российской академии наук, лаборатория инструментальных и информационных методов исследования окружающей среды средствами дистанционного зондирования, главный научный сотрудник **Мартышкин Алексей Иванович** Кандидат технических наук, доцент, Пензенский государственный технологический университет, заведующий кафедрой «Программирование», г. Пенза
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Рязанский государственный радиотехнический университет им. В.Ф. Уткина»

Защита диссертации состоится «05» июля 2022 г. в 11 часов на заседании диссертационного совета Д 212.105.02 при Юго-Западном государственном университете по адресу: г. Курск, ул. 50 лет Октября, 94.

С диссертацией можно ознакомиться в библиотеке Юго-Западного государственного университета и на сайте Юго-Западного государственного университета, **https://swsu.ru/upload/iblock/d61/agit7hperlg6bmubbn4owvw6m2ou5013/dissertatsiya_Usatyuk_final.pdf**

Автореферат разослан «___» _____ 2022 г.

Ученый секретарь
диссертационного совета Титенко Евгений Анатольевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

В связи с интенсивным увеличением объема информации, хранимой в электронном виде, в настоящее время актуальными являются вопросы развития систем голографического архивного хранения данных, в которых запись данных сопровождается процессами кодирования, а считывание данных – процессами их декодирования. Особенностью канала считывания информации голографического носителя является группирование ошибок и высокий уровень вероятности ошибки на бит – до $5 \cdot 10^{-2}$. Тогда как современные требования к надежности считывания архивной голографической памяти определяют вероятности ошибки на бит в диапазоне $10^{-8} - 10^{-10}$. Для достижения этого показателя надежности, ошибки, возникающие при хранении и считывании данных в голографической памяти, исправляют с помощью кодов с низкой плотностью проверок по четности (низкоплотных кодов).

Низкоплотностные коды были предложены Галлагером Р. в 60-х годах прошлого века и исследовались Таннером Р., Зябловым В.В. и Маргулисом Г.А. Всплеск интереса к применению этих кодов на практике возник в связи с появлением в 1997 году работы Маккея Д., посвященной декодированию с мягкими решениями этих кодов. В дальнейшем низкоплотностные коды исследовались Назаровым Л.Е., Габидулиным Э.М., Кудряшевым Б.Д., Трифоновым П.В., Фроловым А.А., Рыбиным П.С., Фоссорье М., Васичем Б. и другими. Тем не менее, в исследованиях этих ученых при построении кодов не уделялось достаточного внимания учету их дистантных свойств и спектров связности, что усложняет построение низкоплотностных кодов средней длины с высокой корректирующей способностью, требуемых в системах голографической памяти.

Приложениями этих кодов для голографической памяти занимаются компании AT&T (Alcatel-Lucent /NOKIA), Hitachi Maxell, Sony, Panasonic, Mitsubishi, Nichia, Alps Electric, Bayer Material Science, Sanyo, Lite-on, TrellisWare. Корректирующая способность низкоплотностного кода F-LDPC, предложенного компанией TrellisWare, для голографической памяти, далека от границы Полянского, что определяется ограниченной длиной кода (32000 бит) со скоростью кода 0.5, вызванной секторной организацией данных, и применением недостаточно совершенных методов построения этих кодов. Используемые в настоящее время программные реализации методов и алгоритмов построения низкоплотностных кодов имеют большую вычислительную сложность и недостаточную производительность, в них слабо учитываются комбинаторно-алгебраические свойства Таннер-графа и дистантные свойства кода, что приводит к появлению треппин-сетов и кодовых слов малого веса, отрицательно влияющих на корректирующую способность кодов.

Таким образом, объективно сложилось **противоречие** между необходимостью повышения надежности чтения в накопителях голографической памяти данных, за счет понижения вероятности ошибки на бит в области рабочих значений диапазона отношений сигнал-шум, устройствами коррекции ошибок низкоплотными кодами, и отсутствием методов построения низкоплотностных кодов, обеспечивающих повышенную надежность, с использованием аппаратно-ориентированных алгоритмов и специализированных устройств для редукции числа циклов и определения дистантных свойств низкоплотностных кодов.

В связи с этим, **актуальной научно-технической задачей** является разработка методов, аппаратно-ориентированного алгоритма и специализированного устройства для построения низкоплотностных кодов для декодеров, обеспечивающих повышение надежности чтения в архивной голографической памяти.

Целью диссертационной работы является повышение надежности воспроизведения информации в накопителях архивной голографической памяти за счет понижения вероятности ошибки на бит в области рабочих значений диапазона отношений сигнал-шум, устройствами коррекции ошибок низкоплотными кодами.

В соответствии с поставленной целью в диссертации решаются следующие **задачи**:

1. Анализ существующих методов построения низкоплотностных кодов, используемых в накопителях архивной голографической памяти, выбор и обоснование цели исследования.

2. Создание метода построения низкоплотностных кодов для накопителей архивной голографической памяти.

3. В рамках метода построения низкоплотностных кодов созданы частный метод оценки кодового расстояния и аппаратно-ориентированный алгоритм оценки кодового расстояния с использованием геометрии чисел.

4. Разработка специализированного устройства, осуществляющего поиск кодового расстояния в подрешетке m-размерности для построения низкоплотностных кодов, и экспериментальная оценка надежности считывания данных из голографической памяти.

Объект исследований – вычислительные процессы, методы и аппаратно-ориентированный алгоритм в задаче кодирования-декодирования данных, считываемых из голографической памяти.

Предмет исследований - специализированное устройство для построения низкоплотностных кодов архивной голографической памяти.

Методы исследования. Для решения поставленных задач применялись методы: помехоустойчивого кодирования, геометрии чисел, абстрактной алгебры, теории графов, теории вероятностей, теории сложности вычислений, имитационного моделирования, параллельного программирования, теории проектирования ЭВМ.

Научная новизна и положения, выносимые на защиту:

1. Метод построения низкоплотностных кодов, состоящий из двух фаз построения и расширения протографа, отличающийся комбинированием жадного алгоритма запрещенных коэффициентов и стохастического алгоритма отжига, позволяющих улучшить дистантные свойства кодов и их спектры связности для фильтрации кодов кандидатов, обеспечивающий повышение надежности считывания информации в голографической памяти.

2. Метод оценки кодового расстояния, основанный на вложение кода в решетку, отличающийся применением для поиска кратчайших векторов параллельным перебором линейных комбинаций базисных векторов решётки, а также применением на этапе ортогонализации параллельных методов QR-разложения матриц, применением метода ветвей и границ в скользящем окне по подрешеткам *m*-размерности, позволяющий ускорить нахождение кодового расстояния.

3. Аппаратно-ориентированный алгоритм поиска кратчайшего вектора в решетке, отличающийся этапом распараллеливания вычисления координатных компонент с использованием зигзагообразного обхода Шнора элементов решетки, позволяющий оперативно получить необходимые индексы и кратчайший вектор нахождения кодового расстояния.

4. Специализированное устройство поиска кратчайшего вектора в решетке, включающее операции модификации координатных компонентов вектора и блоков вычисления частичных сумм совместно с блоком модификации/вычисления приращений координат и его границ, отличающееся использованием регистровых стеков и параллельным выполнением мультипликативных операции в одном временном интервале, позволяющее в подрешетки *m*-размерности сократить количество DSP процессоров в устройстве.

Практическая ценность работы состоит в следующем:

1. Комбинация метода построения низкоплотностных кодов для архивной голографической памяти, аппаратно-ориентированного алгоритма и специализированного устройства поиска кратчайшего вектора в решетке позволила построить новый низкоплотностный код для архивной голографической памяти, декодер которого обеспечивает повышение надежности воспроизведения информации от 8,9 раз при отношении значения сигнал-шум 1,1 дБ по сравнению с F-LDPC кодом, предложенным компанией TrellisWare для голографической архивной памяти.
2. Созданный метод оценки кодового расстояния линейных блочных кодов, позволил дать оценки расстояний для низкоплотностных кодов длиной 32000 бит, используемых в голографической памяти.
3. Разработанное специализированное устройство поиска кратчайшего вектора в решетке обеспечивает выигрыш по быстродействию в сравнении с программной реализацией в 33.93 раза для подрешетки 512-размерности для низкоплотных кодов.

Реализация и внедрение.

Основные научные результаты и выводы диссертационной работы внедрены в ООО «Техкомпания Хуавей». Используемые результаты защищены компанией Huawei Technologies Co. тремя международными патентами. Также результаты диссертационной работы используются на кафедре вычислительной техники ЮЗГУ при преподавании дисциплин: «Защита информации» по направлению подготовки 09.03.01, «Схемотехника (элементная база перспективных ЭВМ)» по направлению подготовки 09.04.01. Внедрение подтверждается соответствующими актами.

Достоверность результатов диссертации обеспечивается обоснованным и корректным применением положений и методов математического аппарата алгебры и комбинаторики, теории вероятности, теории графов, теории помехоустойчивого кодирования, теории проектирования ЭВМ, а также подтверждается совпадением теоретических выводов с результатами имитационного моделирования.

Соответствие диссертации паспорту научной специальности.

Согласно паспорту специальности 05.13.05 – «Элементы и устройства вычислительной техники и систем управления» проблематика, рассмотренная в диссертации, соответствует пунктам 3, 4 паспорта специальности. 3. Разработка принципиально новых методов анализа и синтеза элементов и устройств вычислительной техники и систем управления с целью улучшения их технических характеристик, в части синтеза специализированного устройства поиска кратчайшего пути, необходимого для построения низкоплотностного кода, позволяющего в подрешетке m-размерности сократить количество DSP процессоров в устройстве. 4. Разработка научных подходов, методов, алгоритмов и программ, обеспечивающих надежность, контроль и диагностику функционирования элементов и устройств вычислительной техники и систем управления, в части создания метода и аппаратно-ориентированного алгоритма построения низкоплотностного кода, позволяющего повысить надежность воспроизведения данных голографической памяти ЭВМ.

Апробация работы. Основные теоретические положения и научные результаты диссертационной работы докладывались и обсуждались на следующих всероссийских и международных научных конференциях: 4-ой и 5-ой региональных научно-практических конференциях «Платоновские чтения» (г. Иркутск 2012, 2013), Всероссийской научной конференции «Наука. Технологии. Инновации» (г. Новосибирск, 2012), Всероссийских конференциях «Компьютерная безопасность и криптография» – «SIBECRYPT'12» в Институте динамики систем и теории управления СО РАН (г. Иркутск, 2012), «SIBECRYPT'13» (г. Томск, 2013), «XVI Всероссийском Симпозиуме по прикладной и

промышленной математике» (г. Челябинск, 2015), 18-й Международной научно-технической конференции «Проблемы передачи в сетях и системах телекоммуникаций» (г. Рязань, 2015), II и III Международных конференциях «Инжиниринг & Телекоммуникации –En&T» (г. Москва/Долгопрудный, г. 2015, 2016), XIII Международной научно-технической конференции «Новые информационные технологии и системы» (г. Пенза, 2016), XIII Международной научно-технической конференции Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений «Распознавание 2017», (г. Курск, 2017), XII Международной научной конференции «Перспективные технологии в средствах передачи информации - ПТСПИ-2017» (г. Владимир-Суздаль, 2017), 15-й Международной конференции IEEE East-West Design & Test Symposium (г. Нови-Сад, Сербия, 2017), конференции «Applied Mathematics Day» в МИАН РАН (г. Москва, 22 сентября 2017), конференции «Машинное обучение и анализ алгоритмов» в ПОМИ РАН (г. Санкт-Петербург, 18-20 декабря 2017 г.), 41-й Международной конференции «Telecommunications and Signal Processing» (г. Афины, Греция, 4-6 июля 2018 г.), 5-й Международной конференции по матричным методам в математике и приложениях, «The 5th International Conference on Matrix Methods in Mathematics and Applications (MMA 2019)»(19-23 Августа 2019 г. г. Москва), 43-й Международной конференции «Telecommunications and Signal Processing» (г. Милан, Италия, 2020 г.).

Публикации. По теме диссертации опубликовано 29 научных работ, в их числе 5 статей в научных рецензируемых изданиях, входящих в перечень ВАК Минобрнауки России, 8 работ проиндексированы в международной базе Scopus. Оригинальность технических решений, предложенных автором, подтверждена тремя Международными патентами на изобретения.

Личный вклад соискателя. Все выносимые на защиту научные результаты получены соискателем лично. В опубликованных в соавторстве работах по теме диссертации лично соискателем предложено: в [1, 2] метод поиска кратчайшего вектора в решетке, в [4, 11] методы оценки кодового расстояния на основе геометрии чисел, в [6-10, 14, 16, 29] методы построения низкоплотностных кодов, в [5] быстродействующее устройство поиска кратчайшего вектора в решетке.

Объем и структура работы. Диссертационная работа состоит из введения, четырех разделов, заключения, списка литературы и приложений. Работа содержит 160 страниц текста (с учетом приложений) и иллюстрируется 60 рисунками и 12 таблицами; список литературы включает 147 наименований.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертационный работы, определяется область исследований, цель и задачи, научная новизна и практическая значимость работы. Изложены основные положения, выносимые на защиту, приводится информация об апробации и общей структуре диссертации.

В первом разделе выполнен анализ существующих методов и алгоритмов построения низкоплотностных кодов применительно к архивной голографической памяти ЭВМ**.**

Код с малой плотностью проверок на чётность (LDPC-код от англ. Low-density parity-check code, LDPC-code, низкоплотностный код) – это блочный линейный код размерностью K и длиной кодового слова N, задаваемый проверочной матрицей H размерности $(N\text{-}K)\times N$, имеющей небольшую плотность отличных от нуля символов.

Достоинством низкоплотностных кодов является возможность применения субоптимального алгоритма декодирования с мягкими решениями методом распространения

доверия (BP, belief-propagation), обладающего значительно большей помехоустойчивостью по сравнению с алгоритмами декодирования с жесткими решениями, сложность которого растет линейно относительно длины кода.

Алгоритм BP предусматривает представление LDPC-кода в виде двудольного графа Таннера (пример графа Таннера приведен на рис. 1).

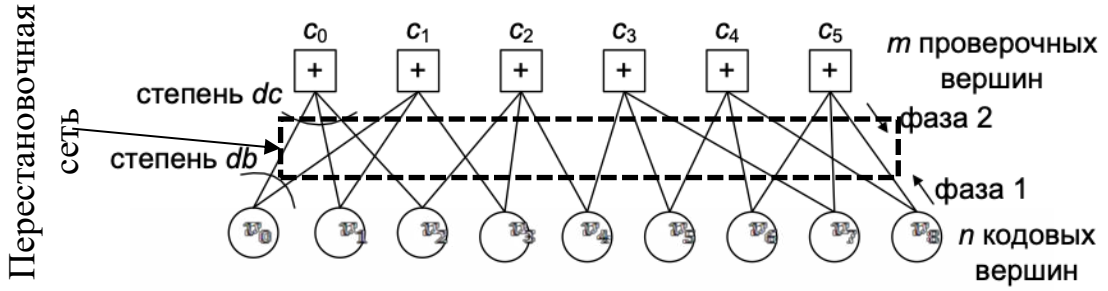

Рисунок 1. Двудольный граф Таннера двоичного регулярного LDPC кода длины 9.

Граф Таннера *G={C,V,E}* имеет два множества вершин – *C,V*. Одно множество состоит из *m'=N-K* проверочных вершин $\{c_0, c_1, \dots, c_{m'-1}\}$, соответствующих m' строкам матрицы *H*, второе - из $n = N$ кодовых вершин $\{v_0, v_1, \dots, v_{n-1}\}$, соответствующих *n* столбцам матрицы *H*. Кодовая вершина v_j соединяется ребром с проверочной вершиной c_i в том случае, если элемент проверочной матрицы на *j*-столбце и *i*-й строке $H_{i,j} \neq 0$.

В соответствии с итеративным алгоритмом декодирования BP получение верных значений бит кодового слова осуществляется в результате многократного обмена сообщениями между вершинами графа Таннера. Каждая итерация алгоритма содержит две фазы. В фазе 1 обновляются сообщения проверочных вершин на основе анализа сообщений кодовых вершин; в фазе 2 – обновляются сообщения кодовых вершин на основе анализа сообщений проверочных вершин.

На эффективность BP-декодирования отрицательно влияет наличие циклов в графе Таннера, образующих треппин-сеты (Trapping set, TS,) или (*a*,*b*)-подграфы (подграфы в графе Таннера, состоящие из *a* кодовых вершин, *b* из которых инцидентны проверочным вершинам с нечетнымий степенями). Эти подграфы обусловливают ошибку BP-декодирования. В случае, если сообщения проверочных вершин изменят значения кодовых вершин, инцидентных нечетному числу проверок, то, вследствие неправильного подсчета условных вероятностей, обусловленного циклами графа Таннера, на кодовых вершинах подграфа ошибка не будет скорректирована, даже если она является корректируемой в соответствие с дистантными свойствами кода.

Структура графа Таннера и распределение строчных и столбчатых весов квазициклического LDPC-кода определяется базовой проверочной матрицей (граф Таннера которой называется протографом). Проверочная матрица квазициклического LDPC-кода получается путем расширения базовой матрицы подматрицами циклических перестановок. Использование циркулянтов позволяет получать компактное представление квазициклического LDPC-кода и осуществлять параллельное кодирование и декодирование с глубиной параллелизма, равной размеру циркулянта.

Повышение надежности голографической памяти осуществляется за счет уменьшения вероятности ошибки на бит P_{BER} в области рабочих значений отношений сигнал-шум.

Процедура построения квазициклических LDPC-кодов предусматривает выполнение 2-х этапов:

1) выбор протографа (базовой матрицы);

2) расширение базовой проверочной матрицы.

Расширение базовой проверочной матрицы заключается в замене единичных символов базовой матрицы на циркулянты размера z. На этом этапе определяются значения циклических сдвигов всех циркулянт. Для реализации этапов построения LDPC-кодов используются комбинаторно-алгебраические методы и методы статистической физики. Сравнение методов представлено в Табл. 1.

Таблица 1 – Классификация методов построения низкоплотностных кодов

Классы методов построения кодов	Методы	Недостатки методов
Комбинаторно-алгебраические методы:	конечные геометрии, блочные дизайны, числовые сетки, слова малого веса кодов Рида-Соломона, метод Саливана (O'Sullivan2006)	Строит коды с фиксированными параметрами (длина, скорость). Затруднено построение нерегулярных кодов.
Методы статистической физики	Density Evolution (Эволюция плотностей), Covariance Evolution (Эволюция ковариации), PEXIT-chart	Игнорирование комбинаторно-алгебраических свойств Таннер-графа и дистантных свойств кода

Недостатки перечисленных методов для построения низкоплотностных кодов средней длины (32000 бит), которые используются в голографической памяти, делают актуальной задачу построения кодов с повышенной корректирующей способностью для голографической памяти.

Второй раздел посвящен созданию метода построения низкоплотностных кодов для архивной голографической памяти.

Входными данными метода построения низкоплотностного кода являются: требуемая длина кода $\boldsymbol{N}$, минимальный размер циркулянта $\boldsymbol{z_{min}}$, $\boldsymbol{z}$ – текущий размер циркулянта, параметры алгоритма декодирования, вероятность ошибки на бит на выходе декодера $\boldsymbol{P_{BER}}$ при требуемом отношении сигнал-шум **SNR,** размерность начальной базовой проверочной матрицы (протографа) $\boldsymbol{J \times L}$; битовая маска M размером $\boldsymbol{J \times L}$**,** определяющая подлежащие инвертированию значения базовой матрицы; число кодов кандидатов card и число итераций $\boldsymbol{iteration}$ процедуры построения низкоплотностного кода.

Выходные данные метода построения низкоплотностных кодов: **массив кодов кандидатов** $\{C'\}$. В результате работы метода определяется множество аппаратно-ориентированных кодов кандидатов с длиной $N = L \times z$ и скоростью $R = 1 - dv_{avg} / dc_{avg}$, где dv_{avg}, dc_{avg} средний вес столбца (число единиц в столбце) и строки в проверочной матрице, соответственно.

Метод построения низкоплотностного кода предусматривает выполнение следующих этапов:

1. На основе вычисленного распределения весов строк и столбцов при помощи метода Эволюции плотностей (Density Evolution) осуществляется инициализация базовой матрицы. Выполняется инициализация множества кодов кандидатов пустым множеством $\{C'\} = \emptyset$.

Фаза оптимизации протографа:

2. Случайным образом в позициях битовой маски $M_{j,l} = rand(0,1)$ инвертируются значения базовой матрицы, и вычисляется порог итеративного декодирования $Threshold = Eb/No\ (\sigma)$: $I_{A,V}^{(n)} \approx 1, \sigma = \frac{1}{\sqrt{4R}} * 10^{-\frac{Eb/No}{20}}$, получаемый при помощи метода статистической физики PEXIT-chart. Метод PEXIT-chart предусматривает обмен взаимной информацией между символьными и проверочными вершинами графа Таннера: $I_{E,V}$ и

$I_{E,C}$. Апостериорная информация (внешняя) $I_{E,V}$ символьных узлов вычисляется в соответствие с уравнениями:

$$I_{E,V} = J(\sigma) = J\left(\sqrt{(d_v - 1)\sigma_A^2 + \sigma_{ch}^2}\right), \quad (1)$$

$$J(\sigma) = 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-(l-\frac{\sigma^2}{2})^2/2\sigma^2} \log(1 + e^{-l}) dl, \quad (2)$$

где $J(\sigma) -$ функция взаимной информации, σ_A^2 и σ_{ch}^2-априорная дисперсия и дисперсия шума. Априорная информация $I_{A,V}$ символьных узлов вычисляется в соотвествие с уравнением:

$$I_{A,V} = J(\sigma_A), I_{E,V} = J(\sigma) = J\left(\sqrt{(d_v - 1)\left[J^{-1}(I_{A,V})\right]^2 + \sigma_{ch}^2}\right). \quad (3)$$

Апостериорная информация (внешняя) $I_{E,C}$ проверочных узлов (факторов) вычисляется в соответствие с уравнением:

$$I_{E,C} = 1 - J\left(\sqrt{(d_c - 1)\left[J^{-1}(1 - I_{A,C})\right]^2}\right). \quad (4)$$

Веса символьных и проверочных узлов графа Таннера задаются в виде полиномов распределения весов $\lambda(z) = \sum_{d=1}^{d_v} \lambda_d z^{d-1}$ и $\rho(z) = \sum_{d=1}^{d_c} \rho_d z^{d-1}$, где λ_d доля проверок веса d в столбце проверочной матрицы, и ρ_d доля проверок веса d в строке, d_v и $d_c -$ максимальный вес столбца и строки, соответственно.

Для нерегулярных кодов

$$I_{E,V} = \sum_{d=1}^{d_v} \lambda_d I_{E,V}(d, I_{A,V}), I_{E,C} = \sum_{d=1}^{d_v} \rho_d I_{E,C}(d, I_{A,C}). \quad (5)$$

Вычисление функции взаимной информации $J(\cdot)$ реализуется путем вычисления значений аппроксимирующего полинома, либо путем выбора из таблицы предварительно вычисленных значений функции (LUT).

При помощи вычисления функций $I_{E,V}(d, I_{A,V})$ и $I_{E,C}(d, I_{A,C})$ выполняется итеративный процесс эволюции взаимной информации начиная с нулевого значения $I_{A,V}^{(0)}$:

$$I_{A,V}^{(0)} = 0, I_{A,V}^{(n+1)} = I_{E,C}(d, I_{E,V}(d, I_{A,V}^{(n)})). \quad (6)$$

Процесс останавливается, когда априорная информация $I_{A,V}^{(n)}$ на некоторой итерации принимает значение близкое к 1.

3. Вычисляется кодовое расстояние и на его основе – вероятность ошибочного декодирования P_{UB} (верхняя оценка ошибки):

$$P_{UB} \approx \frac{\omega_{d_{min}{}^K}}{N} Q\left(\sqrt{\frac{d_{min}{}^K}{N} 2E_b/N_0}\right), \quad (7)$$

где $d_{\min}$ -кодовое расстояние, $\omega_{d_{\min}}$ - кратность слов минимального веса, $Q(x)$ - Q-функция $Q(x) = (\pi N_0)^{-1/2} \int_x^{\infty} e^{-n^2/N_0} dn$, K- информационная длина кода, N – кодовая длина кода, E_b/N_0 –отношение сигнал-шум, $E_b/N_0 = SNR - 10log_{10}(R)$, R – скорость кода.

4. Шаг проверки полученной вероятности ошибочного декодирования

4.1 Если $P_{UB} \leq P_{BER}$ & $Treshold \leq SNR$ **,** переход к п.5.

4.2 Если ($P_{UB} > P_{BER}$) & $Treshold > SNR$ & ($z > z_{min}$), увеличивается размер протографа $\boldsymbol{J} \times \boldsymbol{L}$, уменьшается значение z, переход к п.2.

4.3 Если ($P_{UB} > P_{BER}$) & $Treshold > SNR$ & ($z < z_{min}$), останов.

5. Расширяется протограф жадным методом запрещённых коэффициентов, накапливается требуемое число кодов кандидатов в множестве {C'}.

6. Вычисляется уточненное кодовое расстояние кодов кандидатов, применяя метод оценки кодового расстояния, подробно рассмотренный в следующем разделе. В множестве {C'} остаются коды с достаточным кодовым расстоянием $P_{UB} \leq P_{BER}$:

$$P_{UB} \approx \sum_{i=d_{min}}^{N} \omega_i / KQ\left(\sqrt{\frac{iK}{N} 2E_b/N_0}\right), \quad (8)$$

где ω_i- кратность слов веса i, i -вес кодового слова, $Q(x)$ - Q-функция, K- информационная длина кода, N – кодовая длина кода, E_b/N_0- отношение сигнал-шум.

7. Для оставшихся в множестве {C′} кодах осуществляется поиск пересечения коротких циклов, которые потенциально содержат малое число невыполненных проверок – треппин сетов. Поиск треппин-сетов осуществляется методом выборки по значимости Коула (Cole's Importance Sampling). Вероятность ошибки на бит в символьных узлах треппин-сета вычисляется по формуле:

$$P_{TS_{BER}} = Q\left(\frac{2m_\lambda + 2\sum_{j=1}^{iter} \frac{m_{\lambda^{ext}}^{(j)} + m_\lambda}{\mu_{max}^{j}}}{\sqrt{\left(1+\sum_{j=1}^{iter} \frac{1}{\mu_{max}^{j}}\right) m_\lambda + \sum_{j=1}^{iter} \frac{m_{\lambda^{ext}}^{(j)}}{\mu_{max}^{j}}}}\right), \quad (9)$$

где μ_{max}^{j}- спектральный параметр роста логарифмов коэффициэнтов правдоподобия на j итерации алгоритма распространения доверия, показывает, насколько логарифмы правдоподобия λ растут быстрее в треппин-сете по отношению к оставшемуся графу; $Q(x)$ - Q −функция; m_λ начальное значение логарифмов правдоподобия в символьных узлах, полученных из канала, $m_{\lambda^{ext}}^{(j)}$ - сообщение в методе распространения доверия на j итерации, вычисляемое при помощи Эволюции плотностей или ее аппроксимаций, например $m_{\lambda^{ext}}^{(j)} = \phi^{-1}\left(1 - \left[1 - \phi\left(m_\lambda + (d_v - 1)m_{\lambda^{ext}}^{(j-1)}\right)\right]^{d_c - 1}\right)$, $\lambda(\lambda^{ext})$- логарифмы правдоподобия в символьных узлах из канала (внешние логарифмы правдоподобия из декодера на $j-1$ итерации, extrinsic information), d_c-вес проверочного узла, d_v-вес символьного узла, ϕ - функция проверочного узла в Эволюции плотностей или ее приближении (Reciprocal Channel Approximation, RCA Gaussian Approximation). Например, для аппроксимации Гауссианами получим:

$$\phi(x) = \begin{cases} \exp\left(-0.4527x^{0.86} + 0.0218\right), \text{ для } 0 \leq x < 10 \\ \sqrt{\frac{\pi}{x}} \exp(-0.25x)\left(1 - \frac{10}{7x}\right), \text{для } x \geq 10 \end{cases}. \quad (10)$$

8. Для каждого кода кандидата $c \in \{C'\}$ вычисляется значение штрафа $Penalte$ от $Treshold$ порога итеративного декодирования (PEXIT chart). Штраф обусловлен конечной длиной LDPC-кода и рассчитывается по формуле: $Penalte = Treshold - P_{watterfall}$,

$$P_{waterfall}(N,\sigma) \cong Q\left(\frac{\sqrt{N}\left(C(\sigma) - C(\sigma^*) - \beta N^{-\frac{2}{3}}\right)}{\alpha}\right) + O\left(N^{-\frac{1}{3}}\right), \quad (11)$$

где N - длина кода, α - масштабирующий коэффициент, β - коэффициент сдвига, σ^* -порог итеративного декодирования (среднеквадратичное отклонение), σ -среднеквадратичное отклонение в АБГШ-канале, $C(\sigma)$ - пропускная способность канала, соответствующая мощности шума σ , $Q(x)$ - Q −функция. Коэффициэнты α и β вычисляются путем решения системы дифференциальных уравнений в методе Эволюции Ковариации (Covariance Evolution). По соотношению штрафа $Penalte$ и порога $Treshold$ упорядочиваются коды кандидаты согласно выражению, $\mathrm{C} \subset \{\mathrm{C}'\}$:

$$c_1 \prec c_2 : c_1(Threshold + Penalte)_{P_{BER}} < c_2(Threshold + Penalte)_{P_{BER}}, c_1, c_2 \in C . \qquad (12)$$

В случае, одинаковых штрафов, упорядочивание происходит по дополнительным параметрам, сложность аппаратной имплементации. При полной эквивалентности один из кодов выбирается случайно.

9. При помощи метода имитации отжига модифицируются коды кандидаты из множества $\{\mathrm{C}'\}$ для улучшения спектра связности графа Таннера, [8].

10. Если число итераций процедуры не превысило требуемую величину и число кодов кандидатов меньше заданной величины $|\{\mathrm{C}'\}| < \mathrm{card}$: осуществляется переход к шагу 2, иначе завершается работа алгоритма.

Введенная фаза расширения протографа позволяет получить проверочные матрицы квазициклических низкоплотностных кодов, ориентированные на аппаратную реализации перестановочной сети при помощи сдвигового регистра. Шаги 5 и 9 направлены на получение уточнённой оценки порога итеративного декодирования с учетом особенностей расширения протографа и реализуются оригинальными алгоритмами А и Б, соответственно.

Алгоритм А (расширения протографа с использованием жадного метода запрещенных коэффициентов) представлен ниже.

На вход Алгоритма А подаются: требуемый обхват графа g , базовая матрица в форме списка проверочных уравнений $h_{j,l}$ (единиц в базовой проверочной матрице, заданных номерами строки j и столбца l). В алгоритме используется массив флагов запрещенных циклических сдвигов циркулянтов $noshift$ (циклических сдвигов, формирующих циклы длиной меньше g) размерности $J \times L \times z$.

1. Инициализируется массив флагов запрещенных циклических сдвигов циркулянт: $noshift_{J \times L \times z} = 0$,$0 \le j \le J-1$, $0 \le l \le L-1$, $0 \le s \le z-1$.

2. В цикле по $0 \le j \le J-1$, $0 \le l \le L-1$, для всех ненулевых элементов базовой проверочной матрицы:

2.1. Задается случайный сдвиг циркулянта $p_{j,l} = rand(0, z-1)$ с нулевым значением флага запрещенных циклических сдвигов.

2.2. Выполняется модификация массива флагов запрещенных сдвигов для элементов базовой матрицы с неопределенным до сих пор сдвигом циркулянта. Для всех потенциально возможных циклов глубиной до g , в которых участвует элемент базовой матрицы $\mathrm{h_{j,l}}$, проверяется выполнение условия наличия циклов, формула 4 в [10]. Если условия выполняются, то соответствующий флаг запрещенного циклического сдвига устанавливается в единицу $noshift_{j,l,z} = 0$.

2.3. Если все флаги запрещенных сдвигов равны 1, запускается работа алгоритма заново. В случае превышения заданного числа запусков работа алгоритма завершается с фиксацией неудачи построения квазициклического кода.

Алгоритм Б (расширения протографа с использованием имитации отжига) представлен ниже

1. Инициируется счетчик шагов алгоритма Nstep=0.
2. Выбирается случайно не нулевой элемент в базовой матрице $h_{j,l}$;
3. Перечисляются все циклы, проходящие через этот циркулянт $h_{j,l}$, используемые в формуле расчета штрафной функции *Penalte;*
4. Вычисляется число циклов Θ для всевозможных циклических сдвигов $a_{j,l} \in \{0 \dots L-1\}$ циркулянта $a_{j,l}$, при помощи формулы 4 в [10];
5. Выбирается случайно одно из значений $a_{j,l}$ с вероятностью, зависящей от числа циклов и температуры Temp, (величины, зависящая от числа циклов в графе и количество шагов алгоритма Б). Если Nstep=0, то Temp=$max_{a_{j,l}}\Theta$. Вероятность выбора сдвига циркулянта $a_{j,l}$, задана функцией:

$$P\left(a_{jl}\right) = w(a_{jl}) / \sum_{i=0}^{L-1} w(i), \tag{13}$$

где функция плотности вероятности $w\left(a_{jl}\right)$ возрастает с уменьшением числа циклов Θ и падает с уменьшением температуры:

$$w\left(a_{jl}\right) = e^{\frac{-\Theta\left(a_{jl}\right)}{Temp}}; \tag{14}$$

6. Инкрементируется переменная Nstep, вычисляется новое значение температуры:

$$Temp = \eta \frac{\Phi}{Nstep^2}, \tag{15}$$

где η - константа, Φ -общее число циклов в расширенной матрице H.

7. Останавливается работа алгоритма, если через заданное число шагов Φ не изменилось, иначе алгоритм перезапускается.

На выходе Алгоритмы А и Б выдают проверочные матрицы H квазициклических кодов. Алгоритм А быстро вычисляет начальное приближение расширенной проверочной матрицы. Оригинальность Алгоритма Б в предлагаемом методе построения квазициклических низкоплотностных кодов заключается в пропуске значительного числа локальных минимумов числа треппин-сетов, что позволяет получить квазициклические коды с дистантными свойствами и спектром связности, не достижимые предложенными ранее методами, а также на порядок более высокую вероятность успешного расширения протографов.

Вычислительная сложность расчета кодового расстояния известными методами на 6 этапе растет экспоненциально от информационной длины кода $O(2^k)$, что может быть реализовано только на суперЭВМ. В связи с этим в диссертации разработан более быстродействующий метод вычисления кодового расстояния, использующий верхние и нижние оценки кодового расстояния и позволяющий по ним ранжировать коды кандидаты.

Третий раздел посвящен методу оценки кодового расстояния линейных блочных кодов.

Чаще всего для оценки кодового расстояния применяют метод Брауэра-Зиммермана. Ключевой особенностью метода Брауэра-Зиммермана является перебор кодовых

слов на основе информационных совокупностей в сочетании с одновременным вычислением верхних и нижних границ кодового расстояния. Метод Брауэра-Зиммермана применим к произвольным линейным блочным кодам, позволяет получить верхнюю оценку временных затрат. К сожалению, его производительность недостаточна для оценки кодового расстояния низкоплотностных кодов средней длины.

В разделе предложен более быстродействующий метод оценки кодового расстояния, основанный на поиске кратчайшего вектора в решетке. В соответствии с этим методом выполняется следующая последовательность действий:

1. *Вложение кода в решетку.* Базис решетки B_c масштабируется некоторой константой N, такой, чтобы в результате приведения базиса решетки получился базис размера $n \times n$:

$$B_c^T = \begin{pmatrix} N \cdot G & I_k \\ N \cdot q \cdot I_n & 0^{n \times k} \end{pmatrix}, \tag{16}$$

где $G \in F_q^{k \times n}$ - порождающая матрица кода, I_k - единичная матрица, B_c^T -транспонированный базис решетки.

В случае систематического кода $G = (I_k \mid P), P \in F_q^{k \times (n-k)}$, масштабирующий коэффициент N равен 1.

2. *Приведение базиса решетки*. Выполняется поиск короткого базиса решетки методом Коркина-Золотарева, дающий в результате некоторый набор векторов малого веса.

3. *Ортогонализация базиса решетки* B_c с целью получения ортогонального базиса решетки и коэффициентов Грама-Шмидта.

Ортогонализация базиса по Граму-Шмидту выполняется следующим образом:

$$b_1^{\perp} = b_1,\ b^{\perp}{}_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^{\perp}, i = 2,3,...,n, \tag{17}$$

где $\mu_{i,j}$ -коэффициенты Грама-Шмидта вычисляемые по формуле

$$\mu_{i,j} = \frac{\langle b_i, b_j^{\perp} \rangle}{\langle b_j^{\perp}, b_j^{\perp} \rangle} = \frac{\langle b_i, b_j^{\perp} \rangle}{\left\| b_j^{\perp} \right\|^2}. \tag{18}$$

Коэффициенты Грама-Шмидта образуют верхнюю треугольную матрицу с $n \times (n-1)/2$ ненулевыми элементами.

4. *Поиск кратчайшего вектора в решетке*. После чего в решетке ищется вектор с минимальным числом отличных от нуля координатных компонент. Количество отличных от нуля компонент найденного вектора равняется искомому кодовому расстоянию.

Задача поиска кратчайшего вектора x в решетке сводится к целочисленному решению системы неравенств:

$$\begin{cases} x_n^2 \left\| b_n^{\perp} \right\|^2 \le A^2, \\ (x_{n-1} + \mu_{n,n-1} x_n) \left\| b_{n-1}^{\perp} \right\|^2 \le A^2 - x_n^2 \left\| b_n^{\perp} \right\|^2 \\ \cdots \\ (x_1 + \sum_{i=2}^{n} x_i \mu_{i,j})^2 \left\| b_1^{\perp} \right\|^2 \le A^2 - \sum_{j=2}^{n} l_j \end{cases}, \tag{19}$$

где A-верхняя оценка кодового расстояния, x_i- координатная компонента искомого вектора $l_j = \left(x_j \sum_{i=j+1}^{n} x_i \mu_{i,j}\right)^2 \left\|b_j^{\perp}\right\|^2$ -частичная сумма.

Для этой цели используется метод Каннана-Финке-Поста (КФП).

Метод КФП представляет собой вариант метода ветвей и границ и заключается в переборе линейных комбинаций базисных векторов решётки, дающих вектор с нормой, ограниченной сверху оценкой A, которая может уменьшаться в процессе поиска.

Поиск кратчайшего вектора в решетке является самой вычислительно сложной частью предложенного метода оценки минимального кодового расстояния. Для повышения быстродействия процедуры оценки минимального кодового расстояния в диссертации предлагается параллельная процедура поиска кратчайшего вектора в решетке, основанного на КФП.

Сущность параллельного поиска заключается в предварительном вычислении значений координатных компонент дерева перебора, разбиение дерева и параллельный перебор на многоядерных процессорах общего назначения или процессорах видеокарт.

Для ускорения ортогонализации базиса решетки (этап 3 метода оценки кодового расстояния), предложено применять вместо модифицированного метода Грама-Шмидта, параллельные методы QR-разложения матриц: блочный метод Хаусхолдера при использовании многоядерных процессоров и метод поворота Гивенса при использовании видеокарт.

Предложенные методы оценки кодового расстояния позволяют значительно увеличить длину оцениваемого низкоплотностного кода, а также произвольного линейного блочного кода, для которого возможно определение кодового расстояния, Табл. 2.

Параллельный поиск обеспечивает уменьшение времени оценки кодового расстояния примерно на порядок. Например, для оценки кодового расстояния тернарного кода [128, 64] реализованному в пакете MAGMA 2.2-09 алгоритму Брауэра-Зиммермана потребуется порядка 134 дней, для аналогичной оценки предложенным методом потребуется около 15 дней. Для верхней оценки кодового расстояния CCSDS AR4JA-кода со скоростью 4/5 пакету Magma (без знания автоморфизмов) потребуется 344 дня, с использованием предложенного метода на это требуется около 27 дней.

Таблица 2 - Время поиска кодового слова минимального веса, сек

Параметры кода, $[n, k, d]$ / Метод оценки	[384,192, 15]	[1008,504, $12 \leq d \leq 20$]	[2016, 1008, $12 \leq d \leq 62$]	[32000, 16000, $14 \leq d \leq 82$]
Брауэр-Циммерман	59717	10^{13}	10^{66}	-
Предложенный метод с параллельным КФП	9432	4×10^6	10^7	6×10^8

Дальнейшее ускорение поиска кодового слова минимального веса возможно с использованием аппаратного акселератора, реализующего поиск кратчайшего вектора в подрешетке (решетке). При этом поиск слова минимального веса сводится к многократному поиску кратчайшего вектора в подрешетке.

Четвертый раздел посвящен разработке аппаратно-ориентированного алгоритма и специализированного устройства поиска кратчайшего вектора в решетке (подрешетке).

Наибольшие вычислительные затраты предложенного метода оценки кодового расстояния линейного кода занимает поиск кратчайшего вектора в решетке, заключающийся в решении системы (19). Именно он ограничивает применение анализа дистантных свойств кода при построении низкоплотностных кодов для голографической памяти. По-

этому для реализации поиска кратчайшего вектора в коде разработано специализированное устройство, реализуемое на программируемых логических интегральных схемах (ПЛИС).

Со схемотехнической точки зрения поиск кратчайшего вектора сводится к итерационно-вычислительной процедуре определения значений координатных компонент дерева перебора и использовании этих компонент для вычисления векторов решетки на основе множества операций умножения, сложения 32- битных чисел, сдвига, их сравнения и перезаписи в процессе перебора элементов решетки.

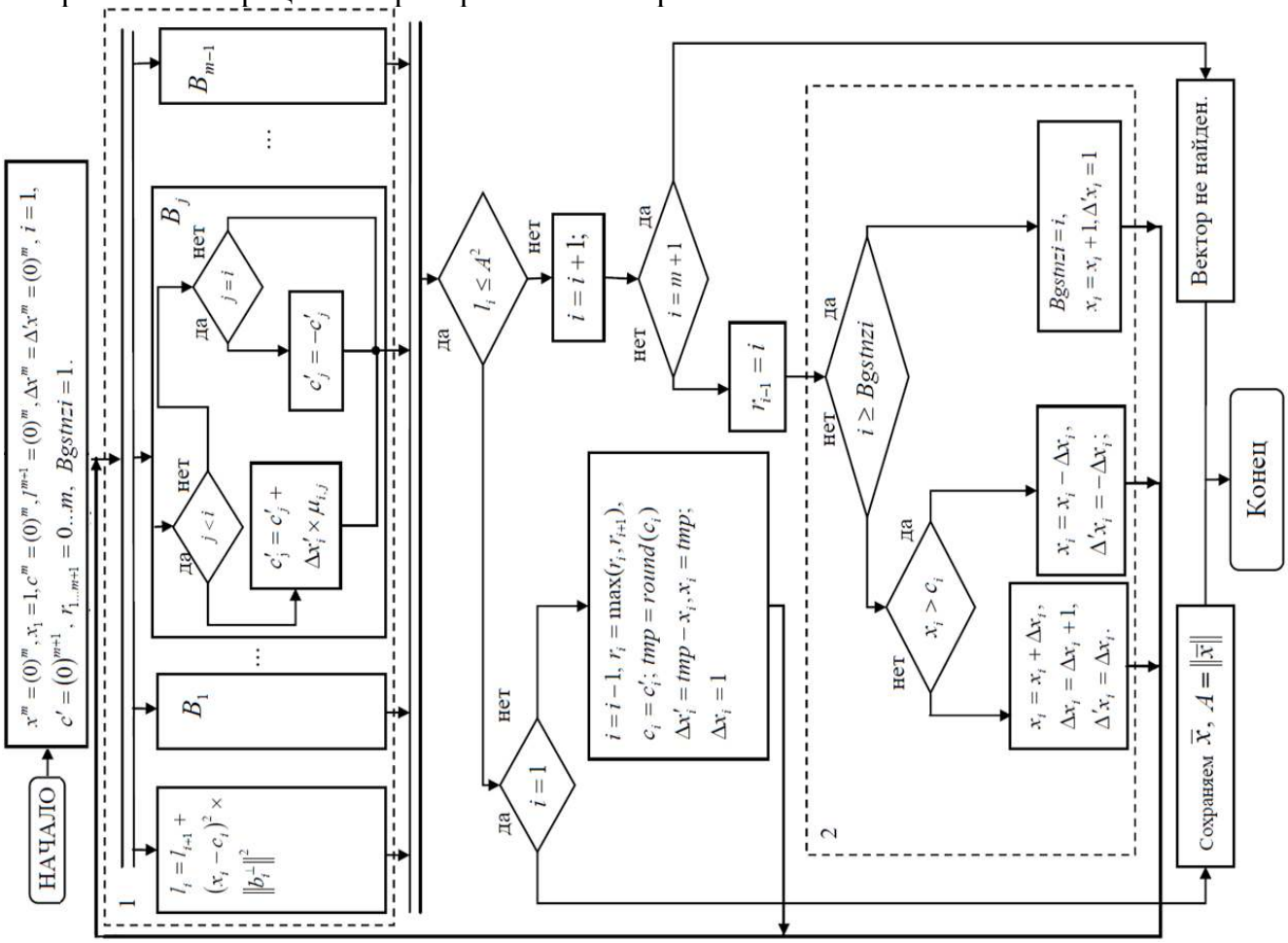

Рисунок 2. Аппаратно-ориентированный алгоритм поиска кратчайшего вектора в решетке

Перебор координатных компонент вектора (x_1, x_2,…, x_m) осуществляется при помощи зигзагообразного обхода Шнора (блок 2 на рис. 2).

Структурная схема специализированного устройства поиска кратчайшего вектора, реализующая предложенный алгоритм, приведена на рисунке 3.

Устройство содержит: интерфейс с шиной PCI-E хост – компьютера, блок модификации c'_i и x'_i, блок модификации x_i, блок вычисления l_i и блок управления.

Быстродействие устройства в основном определяется временем умножения многоразрядных чисел. В предлагаемом специализированном устройстве удалось совместить во времени вычисления $c'_j = c'_j + \Delta x'_i \times \mu_{i,j}$ и $l_i = l_{i+1} + (x_i - c_i)^2 \times \left\| b_i^{\perp} \right\|^2$, требующие умножений. Это позволило повысить быстродействие устройства не менее, чем в 1,5 раза.

Интерфейсный блок предназначен для загрузки исходных данных и возвращает в хост компьютер найденный кратчайший вектор

Представленный алгоритм находит решение системы (19) в виде вектора (x_1, x_2,…,x_m). Особенностью алгоритма является одновременное (параллельное) выполнение

всех мультипликативных операций (умножений), требующих наибольших временных затрат при аппаратной реализации (блок 1 на рис. 2). Умножения используются при расчете частичных сумм

$$l_i = l_{i+1} + (x_i - c_i)^2 \times \left\| b_i^{\perp} \right\|^2 \tag{20}$$

и величин изменения c_j во время перебора координатных компонент:

$$c'_j = c'_j + \Delta x'_i \times \mu_{i,j}\,. \tag{21}$$

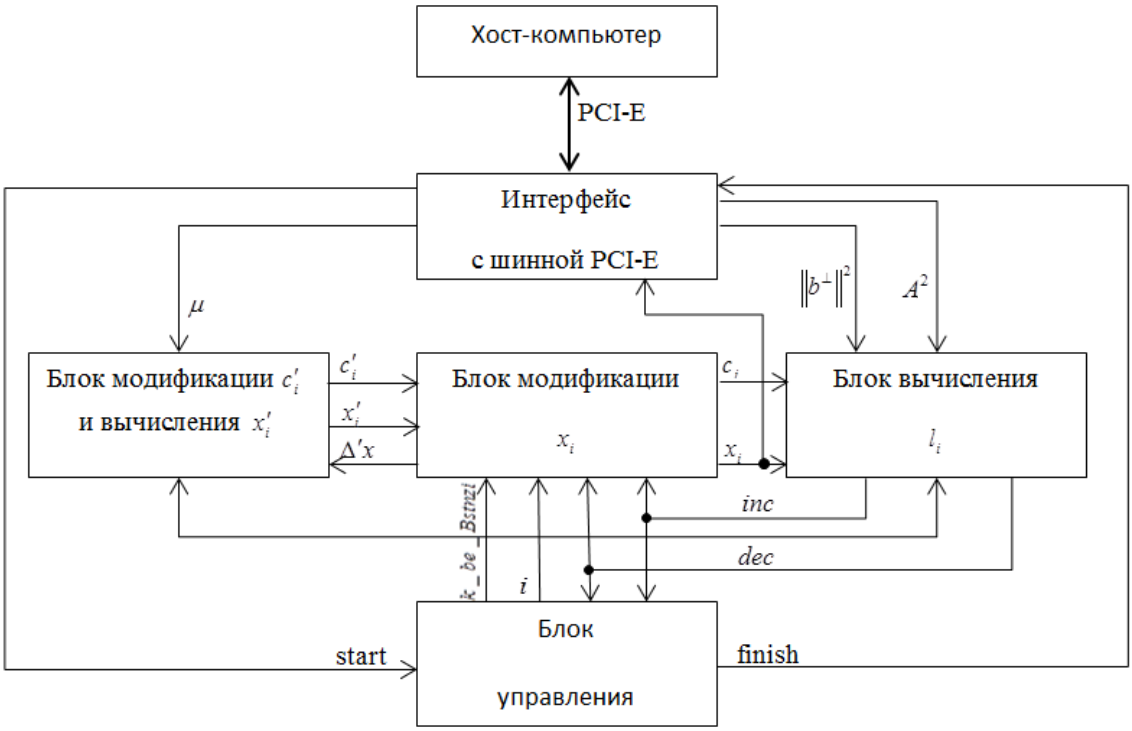

Рисунок 3. Специализированное устройство поиска кратчайшего вектора

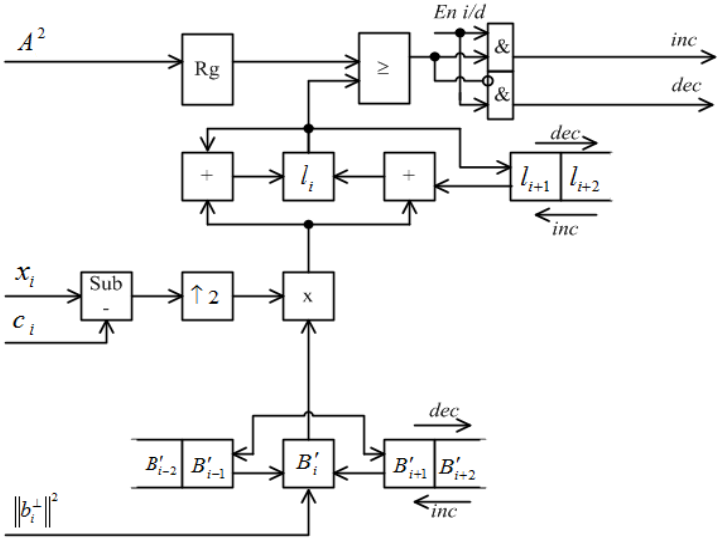

Рисунок 4. Структурная схема блока вычисления l_i специализированного устройства

Блок вычисления частичных сумм l_i (рис. 4) содержит входной регистр, умножитель, квадратор, два сумматора, вычитатель, компаратор и три стековых регистра. Блок вычисляет значение l_i, сравнивает его с оценкой нормы A и в зависимости от результата сравнения формирует один из управляющих сигналов inc или dec. Сигналы inc и dec соответствуют увеличению (inc) или уменьшению (dec) индекса текущей координатной

компоненты i. Они определяют направления сдвига регистров, хранящих l_i, $\left\|b_i^{\perp}\right\|^2$, c_i, x_i, обеспечивая тем самым правильный выбор элементов из последовательности.

Блок модификации c'_i и вычисления x'_i, приведенный на рисунке 5, содержит память RAM, умножители, регистры, мультиплексоры, дешифратор, блоки изменения знака и округления. Он реализует вычисления, описанные в блоках B_1 - $B_{m\text{-}1}$ алгоритма. RAM имеет распределенную структуру при реализации на ПЛИС и хранит коэффициенты Грама-Шмидта $\mu_{i,j}$ разрядностью - 32 бита. Значения c'_j (j=1, …, m-1) хранятся в 8-разрядных регистрах Rg и меняются на величину произведения $c'_j = c'_j + \Delta x'_i \times \mu_{i,j}$.

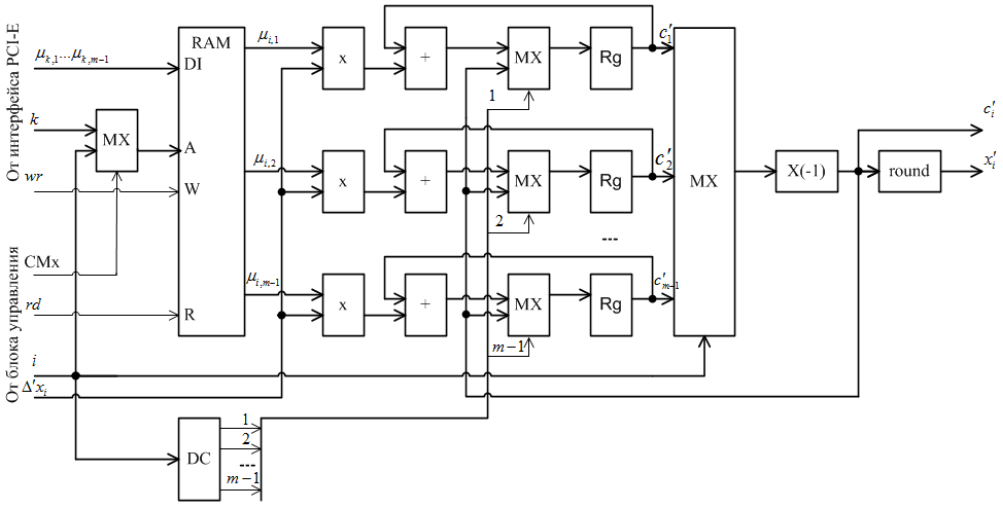

Рисунок 5. Структурная схема блока модификации c'_i и вычисления x'_i

Блок модификации x_i (рис. 6) содержит сумматоры, вычитатель, компаратор, блок изменения знака, мультиплексоры и три стековых регистра. Блок осуществляет изменение координатных компонент искомого вектора в процессе зигзагообразный обхода, а также возвращает непосредственно координаты искомого кратчайшего вектора в решетке.

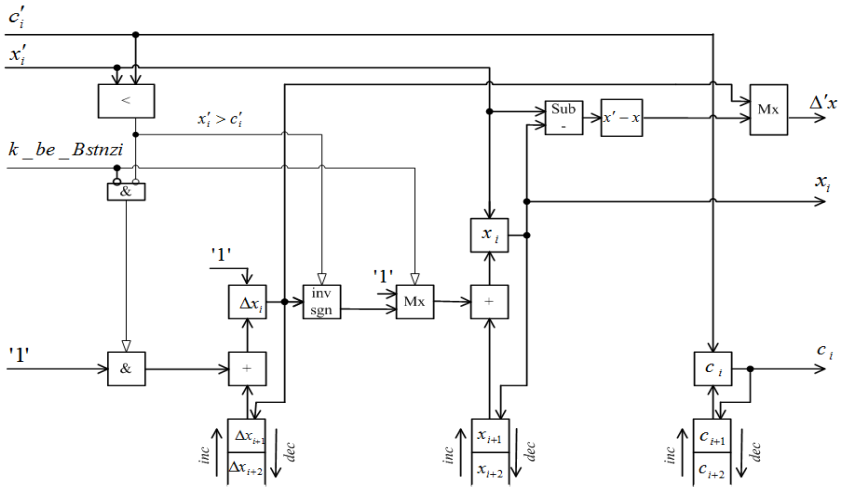

Рисунок 6. Структурная схема блока модификации x_i специализированного устройства

В предложенной аппаратной реализации специализированного устройства используется 32 бита для коэффициентов и ортогонализованного базиса решетки $\|b_i^{\perp}\|^2$, а также 8 бит для c' и $\Delta x'$;

Синтез блоков устройства осуществлялся в САПР Vivado v2016.3 (64-bit) на ПЛИС Virtex UltraScale, тактовая частота 213 МГц. В табл. 3 приведены оценки аппаратной сложности операционной части устройства для различных размеров подрешетки m.

В табл. 4 приведено сравнение по быстродействию предлагаемого устройства и программной реализации поиска по методу КФП на AMD Phenom 965/8 Gb DDR2-800.

В результате применения предложенных методов, аппаратно-ориентированного алгоритма и специализированного устройства был построен низкоплотностный квазициклический код со скоростью 0.5, длиной N=32000 (КОД А), позволивший значительно повысить надежность воспроизведения информации по сравнению с низкоплотностным квазициклическим кодом (КОД Б), предложенным компанией TrellisWare для голографической архивной памяти, (рис. 7, табл. 5).

Таблица 3 – Аппаратная сложность операционной части устройства в зависимости от размера подрешетки *m*

m	64	128	256	512
Количество LUT	690	1301	2803	6154
Количество FF	322	832	1120	2242
Количество DSP	28	46	92	184
Объём памяти, КБ	8,125	32,25	128,5	513

Таблица 4 – Время поиска слов минимального веса предлагаемым устройством и программной реализацией

m / Параметры	64	128	256	512
Сложность аппаратной реализации, вентилях	286716	474462	945778	1894860
Число циклов работы устройства	$0{,}49\cdot10^9$	$236\cdot10^9$	$486\cdot10^9$	$1005\cdot10^9$
Время T_1 поиска слов предлагаемым устройством, с.	9,84	4720	9720	20100
Время T_2 поиска слов программной реализацией, с.	333,68	156011	329925	681946
T_2/ T_1	33,91	33,05	33,94	33,93

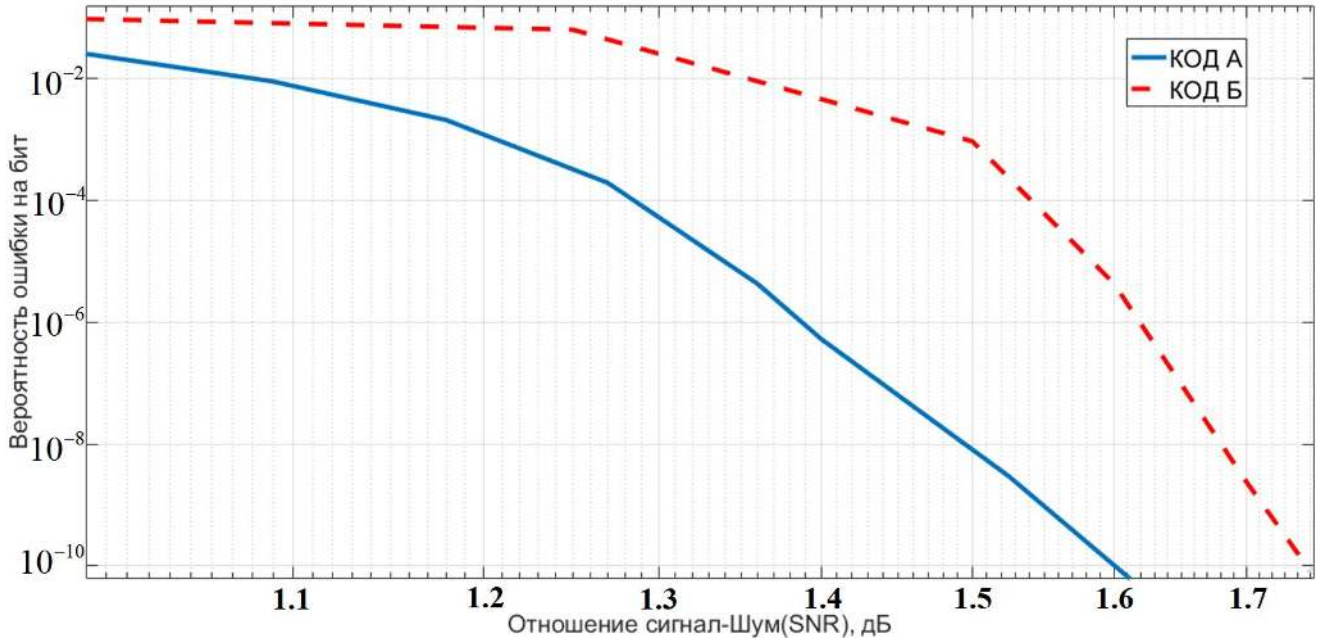

Рисунок 7 – Корректирующая способность построенного низкоплотностного кода в сравнении с F-LDPC низкоплотностным кодом компании TrellisWare

Таблица 5 –Надежность воспроизведения информации в накопителях архивной голографической памяти

SNR, отношение сигнал-шум, дБ	TrellisWare код Б	Предложенный код А	Выигрыш по надежности
	P_{BER}	P_{BER}	$(P_{BER})_Б / (P_{BER})_A$
1,1	8×10^{-2}	9×10^{-3}	8,9
1,45	3×10^{-3}	$7{,}2 \times 10^{-8}$	41670
1,6	5×10^{-6}	$1{,}1 \times 10^{-10}$	45455

В заключении сформулированы основные результаты диссертационной работы.

В приложениях приводятся данные, полученные в ходе имитационного моделирования, акты внедрения.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе в рамках решения научно-технической задачи разработки методов, аппаратно-ориентированного алгоритма и специализированного устройства для построения квазициклических низкоплотностных кодов для декодеров, повышающих надежность воспроизведения информации в накопителях архивной голографической памяти, достигнуты следующие основные результаты:

1. Создан метод построения низкоплотностных кодов, отличающийся использованием в фазе расширения протографа жадного метода запрещенных коэффициентов и метода имитации отжига, обеспечивающий дистантные свойства кодов и их спектры связности для фильтрации кодов кандидатов, позволивший построить низкоплотностный код со скоростью 0.5 длины N=32000 для архивной голографической памяти, применение которого в декодере обеспечило повышение надежности воспроизведения информации от 8,9 раз при отношении сигнал-шум 1.1 дб в сравнение с F-LDPC кодом, рекомендованным стандартом HVD.

2. Разработан метод оценки кодового расстояния, основанный на вложение кода в решетку, отличающийся применением для поиска кратчайших векторов параллельным перебором линейных комбинаций базисных векторов решётки, а также применением на этапе ортогонализации параллельных методов QR-разложения матриц, применением метода ветвей и границ в скользящем окне по подрешетке 512-размерности, позволяющий ускорить нахождение кодового расстояния в 33,93 раза.

3. Разработан аппаратно-ориентированный алгоритм поиска кратчайшего вектора в решетке, отличающийся этапом распараллеливания вычисления координатных компонент с использованием зигзагообразного обхода Шнора элементов решетки, позволяющий оперативно получить необходимые индексы и ускоряющий поиск не менее чем в полтора раза.

4. Создано специализированное устройство поиска кратчайшего вектора в решетке, включающее операции модификации координатных компонентов вектора и блоков вычисления частичных сумм совместно с блоком модификации/вычисления приращений координат и его границ, отличающееся использованием регистровых стеков и параллельным выполнением мультипликативных операции в одном временном интервале, позволяющееся в подрешетки 512-размерности сократить количество DSP процессоров в 4 раза.

Рекомендации. Результаты работы могут быть использованы при создании новых контроллеров архивной голографической памяти с повышенной надежностью хранения информации. Предложенные технические решения также могут быть использованы при

разработке новых систем помехоустойчивого кодирования телекоммуникационных систем, например, для беспроводной связи (WI-FI, 6G) и оптических каналов передачи данных.

Перспективы дальнейшей разработки темы. Оценка влияния использования внешнего кода Рида-Соломона с мягкими решениями на повышение надежности считывания информации голографической памяти. Анализ повышения надежности при $P_{BER} < 10^{-10}$.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых научных журналах и изданиях, рекомендуемых ВАК:

1. Кузьмин, О.В. Программный комплекс приведения базиса целочисленных решеток. [Текст] / О.В. Кузьмин, **В.С. Усатюк** // Программные продукты и системы. – 2012. – №4(100). – С. 180-183.
2. Кузьмин, О.В. Параллельные алгоритмы вычисления локальных минимумов целочисленных решеток / О.В. Кузьмин, **В.С. Усатюк** // Программные продукты и системы. – 2015. – №1(109). – С. 55-62.
3. Усатюк, В.С. Определение кодового расстояния недвоичного LDPC-кода блочным методом Коркина-Золотарева. [Текст] // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. - 2015. - № 3 (16). - С. 76-85.
4. Усатюк, В.С. Построение квазициклических недвоичных низкоплотностных кодов на основе совместной оценки их дистантных свойств и спектров связности. [Текст] **/ В.С. Усатюк,** С. И. Егоров // Телекоммуникации. – 2016. - №8. - С. 32-40
5. Усатюк, В.С. Устройство для оценки кодового расстояния линейного блочного кода методом геометрии чисел. [Текст]/ **В.С. Усатюк,** С. И. Егоров // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. - 2017. - № 4 (25). - С. 24-33.

В научных изданиях, индексируемых в SCOPUS:

6. **Usatyuk V.**, Egorov S., "Generalization of floor lifting for QC-LDPC codes" 2017 IEEE East-West Design &Test Symposium (EWDTS), Novi Sad, 2017, pp.1-6.
7. Vorobyev I., N. Polyanskii, G. Svistunov, S. Egorov and **V.Usatyuk**, "Generalization of Floor Lifting for QC-LDPC Codes: Theoretical Properties and Applications," IEEE East-West Design &Test Symposium (EWDTS), Kazan, 2018, pp. 1-6
8. **Usatyuk V**., I. Vorobyev, "Simulated Annealing Method for Construction of High-Girth QC-LDPC Codes," Intern. Conf. on Telecom. and Signal Proc. (TSP), 2018, pp. 1-5.
9. Svistunov G., **Usatyuk V.**, "Interleaved Cyclic Group Decomposition Length Adaptive MET QC-LDPC Codes," 2019 IEEE BlackSeaCom, Sochi, Russia, 2019, pp. 1-3
10. **Usatyuk V.**, Vorobyev I., "Construction of High Performance Block and Convolutional Multi-Edge Type QC-LDPC codes," (TSP), 2019, pp. 158-163,
11. **Usatyuk V.**, Egorov S., G. Svistunov, "Construction of Length and Rate Adaptive MET QC-LDPC Codes by Cyclic Group Decomposition," (EWDTS), 2019, pp. 1-5
12. **Usatyuk V.**, Egorov S. "Hyper Neural Network as the Diffeomorphic Domain for Short Code Soft Decision Beyond Belief Propagation Decoding Problem," 2020 IEEE East-West Design & Test Symposium (EWDTS), Varna, Bulgaria, 2020, pp. 1-6
13. **Usatyuk V.** "Wireless Channels Topology Invariant as Mathematical Foundation of Neural Network Channel Estimation Transfer Learning Properties," 2020 43rd Intern. Conf. on Telecom. and Signal Processing (TSP), Milan, Italy, 2020, pp. 105-111

Патенты на изобретение:

14. Пат. No.WO/2017/105270 МПК H03M 13/1142 Determination of a quasi-cyclic low-density parity-check, qc-ldpc, code for channel coding in digital communication systems **/ Usatyuk V.S.**, Gaev V.A., Shatilov S. V.,Khodunin A. V. - PCT/RU2015/000886; заявл. 15.12.2015. опубл. 22.06.2017

15. Пат. No. EP3533145 МПК H03M 13/11 Generation of spatially-coupled quasi-cyclic ldpc codes **/ Usatyuk V.S.** –заявл. 21.11.2016.опубл. 04.09.2019

16. Пат. No.US 10,944,425B2 МПК H03M 13/036 Devices and methods for generating a low density parity check code for a incremental redundancy harq communication apparatuses **/ Usatyuk V.S**., Polyanskii N. A., Vorobyev I. V. – заявл. 13.07.2019 опубл. 03.2021

В других изданиях:

17. Усатюк, В.С. Оценка эффективности библиотек вычислений произвольнойточности. [Текст] / М.У. Изимов, **Усатюк В.С.** Современные проблемы естествознания образования и информатики: Материалы VII(I) Межвузовской научной конференции. Братск, 3 декабря 2008. – Братск: ГОУ ВПО «БрГУ», 2008. - С. 97-100.

18. Усатюк, В.С. Задачи теории решеток и их взаимные редукции. [Текст] / **Усатюк В.С.** // Молодежь. Наука. Инновация (Youth. Science. Innovation): Труды II международной научно-практической Интернет-конференции / Под ред. Г.К.Сафаралиева, А.Н. Андреева, В.А. Казакова – Пенза: Издательство Пензенского филиала РГУИТП, 2010-2011. – С. 362-367.

19. Усатюк, В.С. Реализация параллельных алгоритмов ортогонализации в задаче поиска кратчайшего базиса целочисленной решетки. [Текст] / **Усатюк В.С.** // Прикладная дискретная математика. Приложение. –2012. – № 5. – С. 120-122.

20. Усатюк, В.С. Обзор методов приведения базиса решеток и некоторых их приложений. [Текст] / **Усатюк В.С.** // Наука. Технологии. Инновации // Материалы всероссийской научной конференции молодых ученых в 7-и частях. – Новосибирск: Изд-во НГТУ, 2012. Часть 2 – С. 147-151

21. Усатюк, В.С. Экспериментальная оценка точности представления плавающихчисел и времени выполнения блочного метода Коркина-Золотарева для приведения базиса целочисленных решеток сложных по Гольдштейну-Майеру. [Текст] / **Усатюк В.С.** //Наука. Технологии. Инновации // Материалы всероссийской научной конференции молодых ученых в 7-и частях. – Новосибирск: Изд-во НГТУ, 2012. Часть 2 – С. 151-155

22. Усатюк, В.С. Реализация параллельного алгоритма поиска кратчайшего вектора в блочном методе Коркина–Золотарева [Текст] / **Усатюк В.С.** // Прикладная дискретная математика. Приложение. –2013. – № 6. – С. 130-131.

23. Усатюк, В.С. Приложение блочного метода Коркина-Золотарева для демодуляции сигналов MIMO. [Текст] / **Усатюк В.С.** // Обозрение прикладной и промышленной математики. – 2015. - №5. Том 22. – С. 600-602.

24. Усатюк, В.С. Построение двоичных низкоплотностных квазициклических кодов методом назначения случайных разрешенных сдвигов циркулянта. [Текст] / **Усатюк В.С.** // Проблемы передачи в сетях и системах телекоммуникаций// Материалы 18-й Международной научно-технической конференции. 2015 Рязань, 26-28 октября 2015 г. Москва-Научно-техническое издательство "Горячая линия-Телеком", -С. 35-39

25. Усатюк, В.С. Определение кодового расстояния линейного блочного кода методом Коркина-Золотарева. [Текст] **/ Усатюк В.С.** // II International Conference «Engineering & Telecommunication En&T 2015». November18-19, 2015. Book of Abstracts. – Moscow – Dolgoprudny: MIPT, 2015. p. 51-53

26. Усатюк, В.С. Вероятностный метод определения кодового расстояния линейного блочного кода. [Текст] **/ Усатюк В.С.** // III International Conference «Engineering & Telecommunication En&T 2016». November 29-30, 2016. Book of Abstracts. – Moscow – Dolgoprudny: MIPT, 2016. p. 43-46

27. Усатюк, В.С. Вероятностный метод определения кодового расстояния линейного блочного двоичного и тернарного кодов [Текст] / **Усатюк В.С.** // Новые информационные технологии и системы. Сборник научных статей XIII Международной научно-технической конференции. 2016, Пензенский государственный университет. - Пенза, 2016. - С. 171-173.

28. **Усатюк, В.С.** Length adaption methods for QC-LDPC codes. Конференция Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2017: сб. материалов XIII Междунар. науч.-техн. конф. 2017. Юго-Западный государственный университет (Курск) – С. 27-29.

29. Усатюк, В.С. Повышение надежности применения LDPC-кодов путем увеличения кодового расстояния, спектра связности и метода выборки по значимости. [Текст] / **В.С. Усатюк,** С. И. Егоров // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сб. науч. ст. по материалам VI Всерос. науч.-практ. конф. / редкол.: В. Г. Андронов (отв. ред.) [и др.]; Юго-Зап. гос. ун-т. – Курск, 2022 – С. 10-14.

Соискатель В.С. Усатюк

Подписано в печать _____. Формат 60×84 1/16 .
Печ. л. 1.0. Тираж ___ экз. Заказ ___
Юго-Западный государственный университет.
Издательско-полиграфический центр
Юго-Западный государственный университет
305040, Курск, ул. 50 лет Октября, 94.