На правах рукописи

Пчелин Никита Александрович

ИССЛЕДОВАНИЕ КОГНИТИВНЫХ МЕТОДОВ ОБРАБОТКИ ИЗБЫТОЧНЫХ КОДОВ В СИСТЕМЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ КОМПЛЕКСОВ

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Ульяновск – 2019

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Ульяновский государственный технический университет»

Научный руководитель: **Гладких Анатолий Афанасьевич,** доктор технических наук, профессор, г. Ульяновск.

Официальные оппоненты: **Комашинский Владимир Ильич**, доктор технических наук, доцент, заместитель директора по научной работе федерального государственного бюджетного образовательного учреждения науки «Институт проблем транспорта им. Н.С. Соломенко» Российской академии наук, г. Санкт-Петербург.

Чилихин Николай Юрьевич, кандидат технических наук, начальник отдела в Филиале ПАО «МТС» в Ульяновской области, г. Ульяновск.

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Рязанский государственный радиотехнический университет», г. Рязань.

Защита состоится 14 июня 2019 г. в 14:00 на заседании диссертационного совета Д219.003.02 при Федеральном государственном образовательном бюджетном учреждении высшего образования «Поволжском государственном университете телекоммуникаций и информатики» (ФГОБУ ВО ПГУТИ) по адресу: 443010, г. Самара, ул. Льва Толстого д. 23, конференц-зал.

С диссертацией можно ознакомиться в библиотеке Федерального государственного образовательного бюджетного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» на сайте www.psuti.ru/science/diss-ob.

Автореферат разослан «30» апреля 2019 г.

Отзывы и замечания по автореферату в двух экземплярах, заверенных печатью учреждения, просим направлять по вышеуказанному адресу на имя ученого секретаря диссертационного совета.

Ученый секретарь
диссертационного совета Д219.003.02,
доктор технических наук, профессор А.И. Тяжев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Перспективное развитие сенсорных сетей, систем дистанционного управления робототехникой и управления беспилотными средствами связывается с активным применением в них радиоканалов. Объективно такие каналы требуют защиты передаваемых по ним данных не только от ошибок, но и от влияния деструктивных факторов, начиная с попыток перехвата управления беспилотными средствами (фактор спуфинга) вплоть до полного срыва процедуры управления.

Для защиты радиоканалов и передаваемой по ним информации от помех, своевременного обнаружения факторов спуфинга и попыток подавления радиосвязи системы управления целесообразно использование хорошо изученных свойств избыточных кодов. В ряде исследований показано, что наиболее подходящими для такой цели являются короткие блоковые двоичные или недвоичные коды при их мягком декодировании в системе эквивалентных кодов. Этот подход потенциально обеспечивает декодирование принятых данных за пределами метрики Хэмминга даже в условиях применения двоичных кодов, для которых ограничение по составу перестановок надежных символов может составлять до 20% от множества допустимых перестановок.

Актуальность темы исследования обусловлена наличием следующих нерешенных задач:

– отсутствует математически обоснованный механизм формирования порождающих матриц эквивалентных кодов для полного множества допустимых перестановок символов кодовых векторов по ограниченному подмножеству эталонных образцов таких матриц без применения аппарата классических матричных преобразований;

– практически отсутствует подход к использованию в системе перестановочного декодирования аппарата когнитивной обработки данных в системе формирования перестановок мягких решений символов (МРС) и последующего использования их в процедуре поиска требуемой эталонной матрицы;

– отсутствует методика создания когнитивной карты декодера (ККД) и оценка сложности ее реализации.

Степень разработанности темы

Теоретические основы построения эквивалентных систематических кодов и методы их применения в реальных системах обмена данными заложены в работах F. J. MacWilliams, W. Wesley Peterson, E.J. Weldon, Р.Л. Добрушина, С.И. Самойленко, Р.Р. Варшамова, В.В. Зяблова, К.Ш. Зигангирова.

Впервые перестановочное декодирование рассматривалось в работах P. G. Neumann и E. Prange. Особое внимание уделялось кодам, имеющим симметрию алфавита. Под симметрией алфавита понималась перестановка позиций, относительно которой алфавит являлся инвариантным в целом. Дальнейшее исследование перестановочного декодирования проводилось F. J. MacWilliams. Она исследовала возможности перестановочного декодирования

применительно к систематическим и циклическим кодам. Мягкие решения в ее исследованиях не применялись.

Классический метод перестановочного декодирования заключается в перестановке наиболее надежных символов принятой кодовой комбинации на позиции информационных разрядов и кодирование этих надежных символов с использованием эквивалентных кодов. Поскольку указанная операция выполняется на приемной стороне, полученный вектор эквивалентного кода не поражается помехами. Последующее сравнение принятого из канала связи (КС) переставленного вектора и вектора эквивалентного кода позволяет указать в принятом векторе на пораженные помехой символы.

Сложность состоит в том, что для этого необходимо вычислить порождающую матрицу эквивалентного кода. Процесс расчета указанной матрицы необходимо проводить для каждого принятого вектора помехоустойчивого кода, в том числе вычислять определитель переставленной порождающей матрицы кода и осуществлять поиск обратной матрицы для дальнейшего её использования при нахождении порождающей матрицы эквивалентного кода, приведенной в систематическую форму. Естественно, что выполнение матричных операций процессором приемника приводит к резкому повышению сложности вычислений, что отрицательно сказывается на временных параметрах системы управления. Принципиально декодер в состоянии запомнить полученный таким образом результат и использовать его в случае повторения перестановки, но применение когнитивных методов обработки указанного класса помехоустойчивых кодов в системах передачи данных и в системах передачи команд информационно-управляющих комплексов (ИУК) в указанных работах не рассматривается.

Цели и задачи исследования

Целью работы является повышение скорости обработки данных в системе перестановочного декодирования двоичных избыточных кодов путем применения когнитивной концепции к процедуре декодирования.

Для достижения указанной цели в диссертационной работе были поставлены следующие задачи:

1. Исследовать существующие способы мягкой обработки избыточных помехоустойчивых кодов методом перестановочного декодирования и выявить характерные недостатки таких подходов применительно к организации циклов управления систем реального времени.
2. Осуществить анализ методов когнитивной обработки информации в современных технических системах и обосновать способы использования принципов когнитивной обработки данных в системах мягкого декодирования двоичных блоковых помехоустойчивых кодов.
3. Разработать алгоритм обработки данных с использованием когнитивных принципов на канальном уровне и реализовать на этой основе принцип перестановочного декодирования.
4. Провести унификацию математической модели стирающего КС с элементами мягкой когнитивной обработки данных и использовать её для

исследования системы перестановочного декодирования групповых помехоустойчивых кодов.

5. Выработать практические рекомендации по использованию когнитивных принципов в системе защиты данных от влияния мешающих факторов.

Методы исследования

Для решения поставленных задач и достижения обозначенной цели применены методы системного анализа, элементы алгебры теории групп, колец и полей, методы математического моделирования, теории вероятности и теории управления, численные методы.

Объект исследования

Объектом настоящего диссертационного исследования является когнитивная система перестановочного декодирования, используемая для защиты информации от влияния мешающих факторов при ее передаче в ИУК реального времени.

Предмет исследования.

Предметом исследования являются алгоритмы когнитивной мягкой обработки двоичных избыточных кодов.

Соответствие рассматриваемой специальности

Содержание диссертационной работы соответствует пунктам 2, 3, 8, 14 паспорта специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Научная новизна

1. Впервые доказано уникальное соответствие метода перестановочного декодирования принципам когнитивной обработки данных, отличающееся наличием процедуры обучения декодера по вычисленным или известным образцам перестановок номеров символов кодового вектора.
2. На основе всестороннего исследования свойств перестановок символов кодовых векторов развит метод быстрых матричных преобразований (БМП) эталонных матриц в порождающие матрицы эквивалентного кода, отличающийся полным отсутствием арифметических операций в таком преобразовании.
3. Раскрыта общая структура совместной системы обработки данных на канальном уровне, отличающаяся унификацией процедуры формирования мягких решений.
4. Получен патент на конструкцию декодера избыточного кода, отличающуюся наличием режима обучения для формирования когнитивной карты декодера в ходе его функционирования.

Практическая ценность работы

Практическая значимость работы заключается в предложенном алгоритме когнитивного декодирования двоичных кодов оптимальном в смысле минимизации числа арифметических операций, выполняемых в двоичных

полях Галуа. Разработанный алгоритм перестановочного декодирования избыточных помехоустойчивых групповых кодов имеет улучшенные характеристики по вычислительной сложности и скорости работы по сравнению с классическими алгоритмами. ККД и механизм формирования проверочной матрицы позволяют уменьшить объем используемой памяти за счет организации БМП эталонных матриц эквивалентных кодов.

Основные положения, выносимые на защиту

1. Принцип формирования когнитивной карты перестановочного декодера, позволяющий полностью исключить матричные вычисления в системе формирования порождающих матриц эквивалентных кодов.
2. Система лексикографического хранения и поиска эталонных матриц эквивалентных кодов из состава когнитивной карты, позволяющая снизить требования к объему памяти когнитивной карты.
3. Система БМП, использующая процедуру адресной перестановки строк и столбцов эталонных матриц в зависимости от размещения номеров надежных символов принятого кодового вектора.
4. Унифицированное правило формирования мягких решений, позволяющее минимизировать появление ошибочных символов с высоким значением мягких решений, при использовании различных видов модуляции.

Степень достоверности результатов

Результаты работы базируются на использовании общепринятой методологии исследований в области общей теории связи, аргументированным применением известных научных положений теории построения помехоустойчивых кодов, корректным привлечением методов математической статистики, теории вероятностей и исследования операций апробации созданного программно-аппаратного комплекса и подтверждаются соответствием результатов теоретических и экспериментальных исследований.

Степень апробации результатов

Основные результаты диссертационной работы докладывались и обсуждались на Международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» REDS, (г. Москва, 2015 г.), XXI, XXII, XXIII, XXIV международных научно-технических конференциях «Радиолокация. Навигация. Связь» RNLS (г. Воронеж, 2015 г., 2016 г., 2017 г., 2018 г.), IV Всероссийской научно-технической конференции молодых конструкторов и инженеров «Минцевские чтения» (г. Москва, 2017 г.), 20-й Международной конференции «Цифровая обработка сигналов и её применение» DSPA (г. Москва, 2018 г.), II Научном форуме Телекоммуникации: теория и технологии ТТТ-2017. Проблемы техники и технологий телекоммуникаций ПТиТТ-2017 (г. Казань, 2017 г.).

Результаты работы опубликованы в 18 печатных трудах, в числе которых 7 статей в журналах, входящих в перечень ВАК, 1 патент РФ на изобретение, 10 трудов и тезисов докладов на Международных и Всероссийских научно-технических и научно-практических конференциях.

Реализация результатов работы

Материалы диссертации были использованы:

1. При выполнении НИР «Разработка методов кодирования радиолинии передачи команд комплекса взаимного обмена информацией и взаимного ориентирования» (шифр «РТК-3 УлГТУ» 2017 г.). Результаты работы используются в разработках ФНПЦ АО «НПО «Марс» при создании и совершенствовании широкополосного помехоустойчивого КС.

2. Включены в учебный материал для обучения бакалавров по направлению 11.03.02 в УлГТУ на кафедре «Телекоммуникации» в учебных дисциплинах «Общая теория связи 2» и «Теория кодирования и защиты информации» при выполнении индивидуальных заданий по курсовому проектированию и расчетно-графических работ.

Личный вклад автора

Автору работы принадлежит разработка улучшенного алгоритма перестановочного декодирования, процедуры БМП и формирования ККД. Диссертант участвовал в проведении математического моделирования и в испытаниях разработанного алгоритма. В совместных публикациях автор участвовал в обсуждениях, выводе аналитических соотношений, проведении расчетов, разработке и составлении математических моделей, проведении испытаний имитационных моделей и выполнении анализа полученных результатов. Персоналии, выполнявшие совместные исследования и имеющие отношение к теме диссертационной работы, представлены поименно в качестве соавторов конкретных совместных публикаций.

Структура и объем работы

Диссертация состоит из введения, четырех глав, заключения, списка сокращений, списка литературы и одного приложения, содержит 125 страниц машинописного текста, в том числе 29 рисунков и 10 таблиц. Список литературы включает в себя 109 наименований. В приложениях к диссертации представлены перечень образцов эталонных матриц для кода Хэмминга (7,4,3), патент на изобретение, а также акт внедрения результатов работы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении дано обоснование актуальности темы диссертационного исследования, сформулированы цели и задачи работы, ее научная новизна и практическая значимость, представлены научные положения, выносимые на защиту.

В первой главе осуществляется анализ современных взглядов на построение ИУК и использование в них методов повышения спектральной и энергетической эффективности телекоммуникационной составляющей. Показывается, что в общем случае акт управления в техногенной среде осуществляется на базе целевой функции, задаваемой в формате функционала $F\langle X,Y,T,P,C\rangle$, где X – в общем случае множество объектов составляющих материальную основу системы управления (СУ); Y – условия их

функционирования; T – требования к временным параметрам, накладываемые на процедуру управления; P – требования по достоверности, обрабатываемых в СУ команд и сигналов управления, параметр C определяет совокупность условий по организации криптографической защиты информационной составляющей СУ и обеспечению скрытности управления в случае такой необходимости. Исходя из цели диссертационной работы, в ходе исследований главное внимание уделено обеспечению требований к СУ по параметрам T и P.

Основным критерием эффективности применения избыточного кода в системе связи является показатель, получивший название энергетический выигрыш кода (ЭВК). В канале с гауссовским шумом для выявления асимптотических границ показателя ЭВК предполагается, что отношение $E_b / N_0 \to \infty$, в котором значение E_b – энергия сигнала, приходящаяся на бит, N_0 – спектральная плотность гауссовского шума, в случае жестких решений и реализации алгоритма исправления $t = (d_{\min} - 1)/2$ ошибок ЭВК оценивается выражением

$$D_h = 10\lg(R(t+1)) = 10\lg(R(d_{\min} + 1)/2)\ \text{дБ}, \qquad (1)$$

здесь $d_{\min}$ – минимальное расстояние кода, $R = k/n$ – относительная скорость кода, k – число информационных символов в кодовом векторе длины n.

При использовании алгоритмов исправления стираний ЭВК оценивается выражением

$$D_s = 10\lg(Rd_{\min})\ \text{дБ}. \qquad (2)$$

Сравнения выражений (1) и (2) показывает, что в условиях $E_b / N_0 \to \infty$ ЭВК при исправлении стираний оказывается в два раза выше, чем при исправлении ошибок.

Известны методы декодирования помехоустойчивых кодов, которые реализуют максимальное использование введенной в код избыточности и обеспечивают более высокий показатель ЭВК. В этом случае асимптотической оценкой энергетического выигрыша от применения блокового двоичного кода может служить выражение

$$D_m = 10\lg\left(k\left(1 - R + 1/n\right)\right)\ \text{дБ}. \qquad (3)$$

Показано, что только два метода декодирования двоичных кодов способны обеспечить ЭВК в соответствии с выражением (3). К ним относятся метод списочного декодирования на основе вычисления кластера и метод перестановочного декодирования. Декодирование по спискам имеет недостаток, выражающийся в необходимости точного вычисления номера кластера. Кроме того, такой метод не может использовать режим обучения для оптимизации в смысле минимизации параметра T в СУ. На рисунке 1 показаны результаты аналитического моделирования системы связи при различных подходах к декодированию.

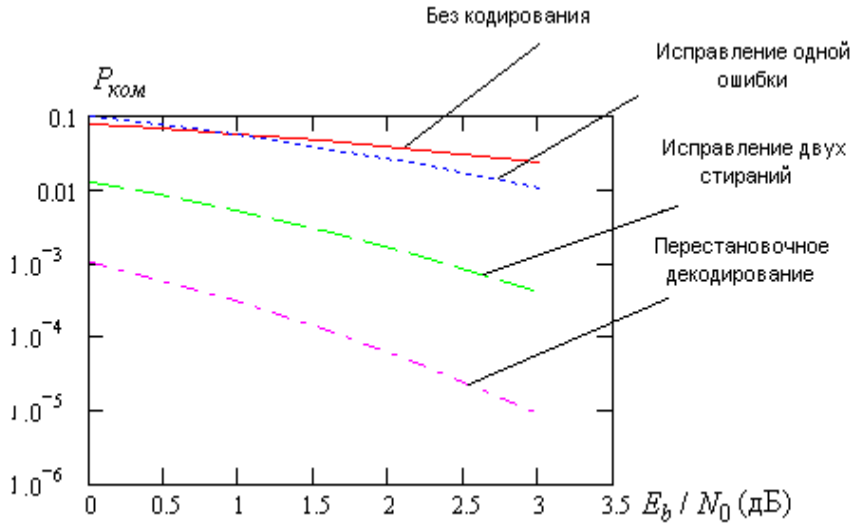

Рисунок 1 – Вероятность ошибки восстановления комбинации кода Хэмминга (7,4,3)

В работе главное внимание было уделено методу перестановочного декодирования двоичных систематических блоковых кодов, потому что он обеспечивает наибольший ЭВК и дает возможность реализовать в СУ когнитивный подход к организации процедуры декодирования, позволяющей рационально организовать эффективную процедуру перестановочного декодирования, минимизируя параметр T с одновременным снижением сложности вычислительного процесса.

Показано, что для организации перестановочного декодирования декодер должен получать мягкие решения символов (МРС) вместе с жесткими оценками в виде вещественных чисел λ_i, где i является порядковым нумератором символа в кортеже жестких решений принятой кодовой комбинации $V_{пр}$ при этом $V_{пр} = V_{пер} \oplus V_e$, где $V_{пер}$ – переданный передатчиком вектор, V_e – вектор ошибок, действовавший в КС при передаче по нему вектора $V_{пер}$. Задачей приемника является вычисление вектора V_e.

Для этого принятые символы вектора $V_{пр}$ ранжируются в порядке убывания значений λ_i, образуя переставленный вектор приема $V_{перест}$. Из полученной последовательности извлекаются левые наиболее надежные символы, которые формируют информационный вектор $V_{перест}^{инф}$. Далее с его получаем $V_{перест}^{инф}$. Он кодируется приемником с образованием вектора эквивалентного кода $V_{эк}$. По понятным причинам в таком векторе влияние мешающих факторов минимально и составляющая помехи декодера $E_{дек} \approx 0$. Сравнивая значения $V_{перест} \oplus V_{эк} = V_e^{пер}$, получают переставленный вектор ошибок, который легко преобразовать в истинный вектор ошибок V_e.

Когнитивный подход к организации работы декодера заключается в том, чтобы не повторять ранее выполненные вычисления, а просто запомнить их и

использовать по мере необходимости. Рационально весь класс допустимых перестановок $\binom{n}{k}$ нумераторов символов вычислить заранее и связать с каждой перестановкой единственный образец некоторой матрицы $G'_{сис}$. Если этого не выполнять, то сложность декодера за счет матричных вычислений будет оцениваться как $O\left(n^3\right)$.

Для решения последующих задач исследования предлагается структурная схема искусственной когнитивной системы (ИКС), которая представлена на рисунке 2.

Рисунок 2 – Структурная схема искусственной когнитивной системы

В предложенной схеме выделяются два контура. Во-первых, заметен внутренний контур когнитивной адаптации, в основе которой лежит когнитивная карта. В этой карте фиксируются удачные и неудачные исходы адаптивного регулирования. Во-вторых, имеется внешний контур когнитивной адаптации, который включает в себя блок целевого функционала.

К ИКС (небиологическим системам) принято относить технические структуры большей или меньшей сложности, обладающие группой специфических функций. К таким функциям целесообразно отнести:

– наличие целевой функции – обмен данными между выраженными частями технической структуры средствами цифровых или аналоговых форматов для быстрого и эффективного решения практических задач;

– функция регулирования – сравнение данных реального времени с данными диагностики и реализации процедуры когнитивного регулирования и когнитивной адаптации;

– функция моделирования – система взаимоувязанных семантических моделей для усваивания новых связей между актуальными событиями внешней среды;

– функция адаптации – для реализации процедуры когнитивной адаптации.

Архитектура ИКС находится в полной зависимости от среды ее функционирования и связывается с этой средой через сенсорную плоскость, при этом результат обработки данных этой плоскости отражается в когнитивной карте ИКС, являющейся неотъемлемой частью когнитивной модели. В данном случае знания следует трактовать как связь между событиями.

Во второй главе рассматриваются принципы формирования МРС в системе мягкого декодирования двоичных помехоустойчивых кодов. МРС могут иметь целочисленные значения или формироваться с бесконечным числом действительных чисел. Целочисленные МРС значительно быстрее обрабатываются декодером и проигрывают нецелочисленным значениям оценок по ЭВК всего 0,2 дБ. При формировании МРС в каналах с неизвестными параметрами целесообразно использовать свойства стирающего КС с широким интервалом стирания φ:

$$\lambda_i(z) = \left\lfloor \left| \frac{\lambda_{\max}}{\varphi\sqrt{E_b}} \times z_i \right| \right\rfloor, \; при \; 0 \le z_i \le \varphi\sqrt{E_b}, \qquad (4)$$

где $\lambda_{\max}$ – максимальное значение МРС принятое в системе, $\sqrt{E_b}$ – математическое ожидание принимаемых сигналов. Обычно $0 \le \varphi < 1$, а z_i – текущее значение реализации сигнала.

В результате исследования было сформировано обобщенное правило формирования МРС, показанное на рисунке 3

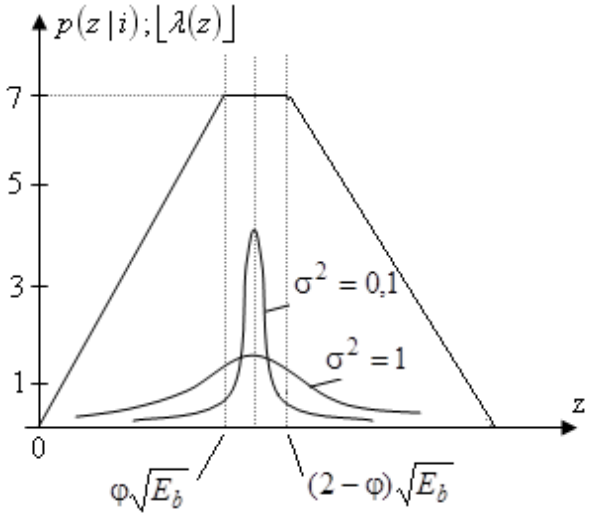

Рисунок 3 – Обобщенное правило формирования МРС для амплитудной и фазовой модуляции

В гауссовском КС целочисленные МРС, выработанные по принципу (4), представляют случайный процесс с математическим ожиданием $M_\lambda(h)$ и дисперсией $\sigma^2_\lambda(h)$, где $h = E_b/N_0$ - отношение сигнал/шум. В ходе испытаний статистических моделей с характеристикой (4) оценивались свойства и возможности использования указанных характеристик $M_\lambda(h)$ и $\sigma^2_\lambda(h)$ в роли сенсоров переключающих функций когнитивной адаптации.

Установлено, что наиболее информативной характеристикой являются значения $M_\lambda(h)$, которые имеют минимальный разброс при различных кортежах данных, как показано на рисунке 4.

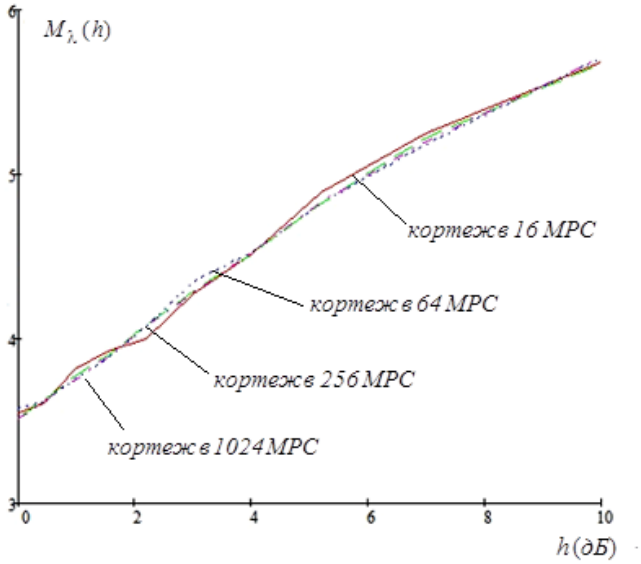

Рисунок 4 – Результаты обобщенной оценки $M_\lambda(h)$

Включение статистических откликов КС в виде конфигурации метаматематического ожидания значений МРС на зачетных отрезках в ККД является перспективной задачей разработки алгоритмов когнитивной адаптации на уровне полунепрерывного КС.

В третьей главе на основе положений алгебраической теории групп и колец раскрывается закономерность изменения структуры проверочной матрицы эквивалентного кода относительно аналогичной матрицы исходного основного кода. Делается вывод о строгом соответствии выполненных перестановок нумераторов кодового вектора линейным преобразованиям вычисленных заранее эталонных проверочных матриц, которые входят в структуру порождающих матриц эквивалентных кодов. Возможность предварительного вычисления требуемых проверочных частей порождающих матриц эквивалентных кодов в систематической форме составляет базис для организации когнитивной процедуры поиска таких матриц. Доказывается, что перестановочное декодирование за счет этого нового свойства является единственным представителем среди многочисленных и разнообразных алгоритмов декодирования помехоустойчивых кодов, который способен реализовать процедуру когнитивной обработки оперативной информации.

В общем случае количество перестановок определяется выражением C_n^k. Например, для кода Хэмминга (7,4,3) может быть сгенерировано $C_7^4 = 35$ последовательностей. В соответствии с каждой полученной последовательностью Z_i из основной порождающей матрицы кода Хэмминга (7,4,3) G извлекаются номера (столбцы), которые образуют матрицу $Q_{k\times k}$. Осуществляется поиск определителя матрицы $Q_{k\times k}$. Если $\Delta \neq 0$, данная

последовательность Z_i записывается как положительное решение в соответствующую базу. По классическому алгоритму перестановочного декодирования вычисляется матрица G_{nep}^{cuc}. Данная матрица заносится в базу матриц положительных решений и в дальнейшем ей присваивается жесткое однозначное соответствие конкретной последовательности Z_i. В ходе повторения последовательности Z_i при работе декодера в оперативном режиме матрица G_{nep}^{cuc}, которая однозначно соответствует данной последовательности Z_i, не вычисляется, а извлекается из базы матриц положительных решений. Если в результате поиска определителя получен результат $\Delta = 0$, такая последовательность Z_i заносится как отрицательное решение в соответствующую базу. Для рассматриваемого кода Хэмминга (7,4,3) имеем 35 различных последовательностей Z_i. 28 последовательностей (80%) при вычислении определителя матрицы $Q_{k\times k}$ дают в результате $\Delta \neq 0$. Для 7 комбинаций (20%) получается $\Delta = 0$. Последовательности Z_i, которые имеют положительные решения ($\Delta \neq 0$) приведены в таблице 1.

Таблица 1 – База номеров последовательностей положительных решений в каноническом виде

1234	1236	1237	1245	1246	1256	1257
1267	1345	1346	1347	1356	1357	1457
1467	1567	2345	2347	2356	2357	2367
2456	2457	2467	3456	3467	3567	4567

Последовательности Z_i, когда $\Delta = 0$, представлены в таблице 2.

Таблица 2 – База номеров последовательностей отрицательных решений в каноническом виде

1235	1247	1367	1456	2346	2567	3457

Общее количество образцов матриц эквивалентного кода G_{nep}^{cuc} определяется выражением $N = C_n^k \times k! \times (n-k)!$. Для кода Хэмминга (7,4,3) необходимо около 141 тысячи бит памяти. Для более длинных кодов, например, для кода БЧХ (15,5,7) требуется существенно больший объем памяти для хранения всех матриц G_{nep}^{cuc} в размере около 11,15 терабайт. Такой объем памяти недопустимо увеличивает требования к декодеру, его сложности и стоимости.

В работе предложен алгоритм, позволяющий уменьшить объем памяти, требуемый для хранения ККД. Он не требует классических матричных вычислений и получил название БМП. Механизм БМП имеет несложную программно-аппаратную реализацию и позволяет получить эквивалентные коды из эталонных образцов. Рассмотрим действие механизма БМП на примере последовательности $Z_i' = 4752613$. Последовательность $Z_i = 2457$ состоит в базе положительных решений (таблица 1). Элементы с низким значением МРС

переставленной в каноническом виде порождающей матрицы $G_{пер}$ располагаются на позициях 136. В ККД декодера находится образец эталонной матрицы G_{Z_i}

$$G_{2457136} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \quad (5)$$

В эталонном образце матрицы (5) пятый столбец соответствует позиции 1, шестой столбец соответствует позиции 3 и последний столбец соответствует позиции 6. Общая нумерация позиций столбцов и строк эталонной матрицы показана на рисунке 5.

$$G_{2457136} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{matrix} 2 \\ 4 \\ 5 \\ 7 \end{matrix}$$

$$1 \quad 3 \quad 6$$

Рисунок 5 – Эталонная матрица с позициями номеров 2457 136

Для формирования порождающей матрицы $G_{4752613}$ в последовательности 4752 613 необходимо поменять строки пятого, шестого и седьмого столбцов эталонной матрицы в порядке 4752. Столбцы, которые получились в результате перестановки строк, имеют порядок 136. Их необходимо перестроить в последовательности 613.

$$G_{4752613} \Rightarrow \begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 3 & 6 \end{matrix} \Rightarrow \begin{matrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 6 & 1 & 3 \end{matrix} \Rightarrow G^{cuc}_{4752613} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

В результате выполненные перестановки строк и столбцов соответствуют матричным вычислениям

$$G_{4752613} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} = G^{cuc}_{4752613} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

В случае применения механизма БМП, ресурсоемкие матричные вычисления классического перестановочного декодирования исключаются, и вместо них производится простая перестановка столбцов и строк эталонных матриц G_{Z_i}. При использовании БМП в ККД для кода Хэмминга (7,4,3) необходима память всего для 28 эталонов порождающих матриц эквивалентных кодов и объем

памяти, требуемый для хранения ККД, всего 784 бита. Для кода БЧХ (15,5,7) для хранения ККД необходимо около 0,3 Мбита памяти.

Для ускоренного поиска произвольной перестановки столбцов матрицы G нумераторы в ККД имеют лексикографическое распределение. Каждому нумератору из числа линейно независимых перестановок соответствует порождающая матрица эквивалентного кода, проверочная часть которой хранится в отдельной базе данных декодера. Для рационального хранения данных в ходе исследований была вскрыта циклическая структура нумераторов, приведенная в таблице 3.

Таблица 3 – Циклические группы нумераторов когнитивной карты

Z_1	Z_2	Z_3	Z_4	Z_5
1234 567	1236 714	1245 673	1246 735	1235
2345 671	2347 125	2356 714	2357 146	2346
3456 712	3451 236	3467 125	3461 257	3457
4567 123	4562 347	4571 236	4572 361	4561
5671 234	5673 451	5612 347	5613 472	5672
6712 345	6714 562	6723 451	6724 513	6713
7123 456	7125 673	7134 562	7135 624	7124

Было установлено, что каждой циклической группе Z_j нумераторов, однозначно соответствует единая проверочная матрица H_{Z_j}.

Формирующие комбинации нумераторов циклических групп Z_j показаны в первой строке таблицы 3, а проверочные части порождающих матриц для этих групп имеют вид

$$H_{z_1}=\begin{matrix}1&0&1\\1&1&1\\1&1&0\\0&1&1\end{matrix};\quad H_{z_2}=\begin{matrix}1&0&1\\0&1&1\\1&1&1\\1&1&0\end{matrix};\quad H_{z_3}=\begin{matrix}1&1&1\\0&1&1\\1&1&0\\1&0&1\end{matrix};\quad H_{z_4}=\begin{matrix}1&0&1\\1&1&0\\1&1&1\\0&1&1\end{matrix}.$$

Справедливость данного положения основана на трех, доказанных в работе теоремах.

Теорема 1. Обратная матрица Q^{-1}, полученная из линейно независимой ключевой матрицы Q, формирует систему линейных перемещений строк переставленной матрицы G' для приведения матрицы $G'_{сист}$ к систематической форме.

Доказательство. Поскольку произведение матриц $Q\times Q^{-1}=E$, то содержание строк матрицы Q^{-1} позволяет однозначно сформировать последовательность операций со строками G' для ее преобразования к матрице

$G'_{сист}$. Не вызывает сомнения, что ключевая матрица Q' для матрицы $G'_{сист}$ является единичной матрицей E.

Теорема 2. Сдвиг по циклу столбцов порождающей матрицы G исходного блокового кода при рассмотрении ключевой матрицы Q приводит к тому, что определитель ее не равен нулю и верно тождество $G'_{сист} = G$.

*Доказательство***.** Так как столбцы матрицы исходного кода G являются линейно независимыми, то их циклический сдвиг в любую сторону обеспечивает линейную независимость ключевой матрицы Q. Это в свою очередь подтверждает возможность приведения переставленной матрицы G' к ее аналогу в систематической форме $G'_{сист}$ и верность тождества $G'_{сист} = G$.

Теорема 3. При перестановке номеров q_i и h_j в любом порядке матрица $G'_{сист}$ может быть получена из эталонной матрицы $G'_{сист}$, представленной в канонической форме, путем перестановок пронумерованных строк и столбцов.

Доказательство. Любая матрица G', обладающая свойством линейной независимости, у которой расположение номеров строк q_i и столбцов h_j имеет произвольный порядок, имеет всегда ключевую матрицу Q, которая позволяет преобразовать матрицу G' к виду $G'_{сист}$. Данный процесс представляется эквивалентным перестановке столбцов и строк проверочной части матрицы G'.

Таким образом, объем памяти, необходимой для хранения в базе данных проверочных частей порождающих матриц эквивалентных кодов в систематической форме, уменьшается в k раз. Для осуществления эффективного поиска порождающей матрицы эквивалентного кода необходимо объединение данных из таблиц 1 и 3 в рамках единой лексикографически упорядоченной ККД, формат которой представлен в таблице 4. На базе этой карты декодер может реализовать унифицированный алгоритм обработки данных, используя сокращенное число порождающих матриц.

Таблица 4 – Единая лексикографически упорядоченная ККД

1234 567 – 1 1234 567	1236 457 – 2 1236 745	1237 456 – 1 7123 456	1245 367 – 3 1245 673	1235
1246 357 – 4 1246 735	1256 347 – 3 5612 347	1257 346 – 2 7125 634	1267 345 – 1 6712 345	1247
1345 267 – 2 3451 267	1346 257 – 4 3461 257	1347 256 – 3 7134 562	1356 247 – 4 5613 472	1367
1357 246 – 4 7135 624	1457 236 – 3 4571 236	1467 235 – 2 6714 523	1567 234 – 1 5671 234	1456

Продолжение таблицы 4

2345 167 – 1 2345 671	2347 156 – 2 2347 156	2356 147 – 3 2356 714	2357 146 – 4 2357 146	2346
2367 145 – 3 6723 451	2456 137 – 2 4562 371	2457 136 – 4 4572 361	2467 135 – 4 6724 513	2567
3456 127 – 1 3456 712	3467 125 – 3 3467 125	3567 124 – 2 5673 412	4567 123 – 1 4567 123	3457

Пусть принят вектор V, для которого в результате преобразования в вектор V' нумераторы значений надежных 7415 и ненадежных символов 623. Отсюда упорядоченная перестановка надежных символов равна 1457 и значения нумераторов надежных символов приняли лексикографически упорядоченную конфигурацию вида **1457.** Проверка принадлежности полученной конфигурации перестановки 1457 к категории линейно зависимых дает отрицательный результат. Следовательно, декодер осуществляет лексикографический поиск значения 1457 в группе линейно независимых перестановок, получая значение когнитивной карты в виде ярлыка:

1457 236 – 3 **4571 236**

.

Из него следует, что образцом дальнейших матричных преобразований является матрица с номером 3. Извлекая эту матрицу из базы данных, декодер выполняет над ней в соответствии с шаблоном обычные перестановки строк и столбцов, как показано ниже.

$$H_{z_3} = \begin{matrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{matrix}.$$

И с нумераторами

$$H_{z_3} = \begin{matrix} 1 & 1 & 1 & 4 \\ 0 & 1 & 1 & 5 \\ 1 & 1 & 0 & 7 \\ 1 & 0 & 1 & 1 \\ 2 & 3 & 6 & \end{matrix}.$$

Последовательность дальнейших преобразований в соответствии верхней строкой шаблона имеет вид:

$$H_{z_3} = \begin{matrix} 1 & 1 & 1 & 4 \\ 0 & 1 & 1 & 5 \\ 1 & 1 & 0 & 7 \\ 1 & 0 & 1 & 1 \\ 2 & 3 & 6 & \end{matrix} \Rightarrow \begin{matrix} 1 & 1 & 0 & 7 \\ 1 & 1 & 1 & 4 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 5 \\ 2 & 3 & 6 & \end{matrix} \Rightarrow \begin{matrix} 0 & 1 & 1 & 7 \\ 1 & 1 & 1 & 4 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 5 \\ 6 & 2 & 3 & \end{matrix}.$$

Подстановка единичной матрицы слева обеспечивает получение требуемой матрицы эквивалентного кода G'_s.

$$G'_S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Матричные преобразования классического типа приводят к аналогичному результату, но требуют значительных вычислительных затрат. Сравнительные характеристики требуемых объемов памяти ККД при различных подходах к ее организации для некоторых двоичных кодов приведены в таблице 5. Учитывая свойства групповых кодов, рассматриваемых над двоичными полями Галуа заданной степени расширения, становится очевидным преимущество предлагаемого способа, поскольку нет необходимости выполнять арифметические действия над элементами матриц с соблюдением соответствующих правил сложения и умножения обрабатываемых матриц.

Таблица 5 – Сравнительные данные требуемого объема памяти ККД

Параметры кода	Полный набор матриц	Набор эталонных матриц	Предлагаемый способ
(7,4)	7 кбайт	52,5 байта	7,5 байта
(15,5)	152 Гбайта	14 кбайт	3,7 кбайта
(15,7)	8525 Гбайт	43 кбайта	6 кбайтов

В четвертой главе дано описание алгоритма работы перестановочного декодера с процедурой обучения. Для введения когнитивных процедур в алгоритм декодирования помехоустойчивых кодов с использованием мягких решений предложено ввести блоки отвечающие за режим обучения. Эти блоки позволяют обеспечить функционирование декодера при обработке оперативной информации или в специальном режиме обучения при отсутствии оперативной работы. Технический результат применения алгоритма заключается в резком повышение производительности декодера, обеспечивающего снижение времени цикла управления.

В заключении приведены основные результаты проведенных исследований:

1. Разработан эффективный алгоритм перестановочного декодирования, использующий когнитивную обработку данных и позволяющий, например, для кода Хэмминга (7,4,3) исключить 1072 арифметических операции при классическом поиске эквивалентного кода, что сокращает цикл обработки подобных данных при использовании ПЛИС на 21 микросекунду.

2. Разработана система рационального хранения эталонных матриц, позволяющая снизить требования к объему памяти когнитивной карты декодера. Для кода Хэмминга (7,4,3) объем сократился в 144 раза, для более длинного кода БЧХ (15,5,7) в $4{,}35 \times 10^8$ раз.

3. Разработан механизм БМП, который позволил заменить арифметические операции системой преобразования эталонных матриц путем адресной перестановки строк и столбцов. Для кода Хэмминга (7,4,3) этот метод

позволяет заменить 1072 элементарных операции на семь операций копирования и переноса при рациональном использовании памяти декодера.

4. Обоснован унифицированный метод формирования мягких решений двоичных символов, позволяющий использовать единую формирующую функцию для всех видов двоичной модуляции.

5. Показана возможность существенного сокращения числа эталонных матриц за счет учета вскрытых в ходе исследований циклических свойств переставленных матриц. Дана количественная оценка получаемого выигрыша за счет введения системы навигации когнитивной карты.

6. Выработаны практические рекомендации по использованию когнитивных принципов в системе защиты данных от влияния деструктивных факторов, закрепленные патентом РФ на изобретение.

Направление дальнейших исследований

В целях дальнейшего развития когнитивного подхода при декодировании избыточных помехоустойчивых кодов целесообразно на базе имитационных моделей изучить возможность введения когнитивной процедуры при формировании мягких решений символов.

В перспективе предлагается исследовать сочетание перестановочного декодирования в системе каскадного кода для когерентных сетей, а также использовать результаты обработки данных внутренним кодом для формирования МРС внешнего недвоичного кода.

Не вызывает сомнений разработка опытного образца декодера с когнитивными функциями для проведения натурных испытаний и углубленного изучения полученных результатов.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ:

Публикации в изданиях, рекомендованных ВАК

1. Пчелин Н.А. Синтез адаптивных систем обмена данными интегрированных информационно-управляющих комплексов // Автоматизация процессов управления. – 2016. – № 2 (44). – С.18-23.

2. Гладких А.А., Наместников С.М., Пчелин Н.А., Шагарова А.А. Статистические свойства и особенности формирования мягких решений недвоичных символов избыточных кодов // Автоматизация процессов управления. – 2016. – № 3 (45). – С.44-51.

3. Гладких А.А., Пчелин Н.А. Моделирование алгоритмов адаптивной обработки данных в системе с мягким декодером // Радиотехника. – 2016. – № 9. – С.40-43.

4. Ганин Д.В., Гладких А.А., Пчелин Н.А., Сорокин И.А. Адаптивная обработка данных в системе мягкого декодирования // Вестник НГИЭИ. – 2016. – №10 (65). – С.15-22.

5. Гладких А.А., Наместников С.М., Пчелин Н.А. Эффективное перестановочное декодирование двоичных блоковых избыточных кодов // Автоматизация процессов управления. – 2017. – № 1(47). – С.67-74.

6. Гладких А.А., Наместников С.М., Пчелин Н.А. Повышение достоверности данных в системе беспроводных сенсорных сетей // Автоматизация процессов управления. – 2017. – № 4 (50). – С.101-107.

7. Гладких А.А., Пчелин Н.А., Шахтанов С.В. Минимизация объема памяти когнитивной карты декодера в системе поиска эквивалентных кодов // Радиотехника. – 2018. – № 6. – С.38-41.

Список патентов

8. Гладких, А.А., Маслов, А.А., Пчелин Н.А., Тамразян, Г.М., Баскакова Е.С. Перестановочный декодер с режимом обучения. Патент РФ. – № 2644507, дата государственной регистрации 12.02.2018.

Публикации в других изданиях

9. Климов Р.В., Пчелин Н.А., Тамразян Г.М. Применение дополненного аппарата регенерационного кодирования для оптимизации внутрисетевого трафика // Сборник докладов Международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» REDS-2015. – Москва, 2015. – С.119-122.

10. Полосин М.В., Пчелин Н.А., Тамразян Г.М. Применение мягких методов декодирования кодов БЧХ в адаптивных системах помехоустойчивого кодирования // Сборник докладов XXI Международной научно-технической конференции «Радиолокация, навигация, связь». – Воронеж, 2015. – Т.3. – С.1613-1618.

11. Пчелин Н.А. Многоконтурная адаптация систем обмена данными в условиях действия деструктивных факторов // Сборник докладов XXII Международной научно-технической конференции «Радиолокация, навигация, связь». – Воронеж, 2016. – Т.1. – С.508-517.

12. Пчелин Н.А. Синтез телекоммуникационных систем информационно-управляющих комплексов / Н.А. Пчелин // Сборник научных трудов «Современные проблемы проектирования, производства и эксплуатации радиотехнических систем». – 2016. – Ульяновск: УлГТУ. – С.180-184.

13. Гладких А.А., Масленникова Т.Н., Муракаев А.И., Пчелин Н.А. Повышение эффективности перестановочных декодеров на базе когнитивных принципов // Труды Четвертой Всероссийской научно-технической конференции молодых конструкторов и инженеров «Минцевские чтения». – 2017. – Москва, 2017. – С.301-312.

14. Гладких А.А., Пчелин Н.А. Повышение эффективности декодирования двоичных блоковых избыточных кодов // Сборник докладов XXIII Международной научно-технической конференции «Радиолокация, навигация, связь». – Воронеж, 2017. – Т.1. – С.370-380.

15. Пчелин Н.А. Быстрые матричные преобразования двоичных блоковых кодов // Сборник научных трудов X Юбилейной Всероссийской научно-практической конференции (с участием стран СНГ), посвященный 60-летию

УлГТУ «Современные проблемы проектирования, производства и эксплуатации радиотехнических систем». – 2017. – Ульяновск: УлГТУ. – С.143-146.

16. Пчелин Н.А. Перестановочный декодер с когнитивной процедурой обработки данных // Сборник научных трудов II Научного форума Телекоммуникации: теория и технологии ТТТ-2017. Проблемы техники и технологий телекоммуникаций ПТиТТ-2017 XVIII международной научно-технической конференции. – Казань: КНИТУ-КАИ, 2017. – Т.1 – С.114-117.

17. Пчелин Н.А. Оптимизация классического алгоритма перестановочного декодирования // Труды 20-й Международной конференции «Цифровая обработка сигналов и ее применение» DSPA-2018. – Москва, 2018. – С.334-337.

18. Пчелин Н.А. Эффективное использование двоичных блоковых кодов в системе беспроводных сенсорных сетей / Н.А. Пчелин // Сборник докладов XXIV Международной научно-технической конференции «Радиолокация, навигация, связь». – Воронеж, 2018. – Т.1. – С.368-373.

Пчелин Никита Александрович
ИССЛЕДОВАНИЕ КОГНИТИВНЫХ МЕТОДОВ ОБРАБОТКИ ИЗБЫТОЧНЫХ КОДОВ В СИСТЕМЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ КОМПЛЕКСОВ

Подписано в печать 9.01.2019. Формат 60×84/16.
Усл. печ. л. 1,00. Тираж 100 экз. Заказ.
ИПК «Венец» УлГТУ, 432027, г. Ульяновск, Северный Венец, 32