

ОБРАБОТКА И ПЕРЕДАЧА ИНФОРМАЦИИ PROCESSING AND TRANSMISSION OF INFORMATION

УДК 004.56

А. А. Хартанович

Белорусский государственный технологический университет

ИСПОЛЬЗОВАНИЕ НИЗКОПЛОТНОСТНЫХ КОДОВ И КОДОВ РИДА – СОЛОМОНА В СИСТЕМАХ ИЗБЫТОЧНОГО КОДИРОВАНИЯ ИНФОРМАЦИИ

Обеспечение надежного хранения и передачи данных представляет собой серьезную проблему в современном информационном обществе. Кодирование информации является одним из направлений исследований и разработок, которое позволяет достаточно эффективно решать проблему достоверности информации. В рамках такого подхода известны методы, основанные на комбинации двух различных кодов, которые позволяют исправлять различные типы ошибок. В статье предлагается ранее не исследованная комбинация, состоящая из кодов LDPC и Рида – Соломона для коррекции случайных и пакетных ошибок соответственно. Исследуются и анализируются производительность исправления ошибок и вычислительная эффективность упомянутой комбинации кодов. Моделирование Монте-Карло показывает, что данный подход обеспечивает более низкий коэффициент битовых ошибок. При этом скорость кодирования и декодирования предлагаемой комбинации достаточна для обработки различных объемов данных. Описаны методы повышения производительности и направления использования комбинирования низкоплотностных кодов и кодов Рида – Соломона в системах защиты информации и стеганографических системах. Результаты показывают, что сильные стороны обоих методов кодирования в комбинации значительно повышают целостность данных в зашумленных каналах связи, сохраняя при этом разумные скорости кодирования и декодирования.

Ключевые слова: кодирование, избыточные коды, коды Рида – Соломона, коды LDPC, комбинированный подход.

Для цитирования: Хартанович А. А. Использование низкоплотностных кодов и кодов Рида – Соломона в системах избыточного кодирования информации // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2025. № 1 (290). С. 47–55.

DOI: 10.52065/2520-6141-2025-290-8.

A. A. Khartanovich

Belarusian State Technological University

USING LOW-DENSITY CODES AND REED – SOLOMON CODES IN REDUNDANT INFORMATION CODING SYSTEMS

Ensuring reliable storage and transmission of data is a serious problem in the modern information society. Information coding is one of the areas of research and development that allows solving the problem of information reliability quite effectively. Within the framework of this approach, methods are known based on a combination of two different codes that allow correcting various types of errors. The article proposes a previously unexplored combination consisting of LDPC and Reed – Solomon codes for correcting random and burst errors, respectively. The error correction performance and computational efficiency of the mentioned code combination are investigated and analyzed. Monte Carlo simulation shows that this approach provides a lower bit error rate. At the same time, the encoding and decoding speed of the proposed combination is sufficient to process various data volumes. The methods for increasing the performance and directions of using a combination of low-density codes and Reed – Solomon codes in information security systems and steganographic systems are described. The results show that the strengths of both coding methods in combination significantly improve data integrity in noisy communication channels while maintaining reasonable encoding and decoding rates.

Keywords: coding, redundant codes, Reed – Solomon codes, LDPC codes, combined approach.

For citation: Khartanovich A. A. Using low-density codes and Reed – Solomon codes in redundant information coding systems. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2025, no. 1 (290), pp. 47–55 (In Russian).

DOI: 10.52065/2520-6141-2025-290-8.

Введение. В современном мире информация играет важную роль, так как она влияет на все аспекты жизни и развития общества. Обеспечение безопасности и достоверности при обмене информацией является одной из главных задач. Информация, передаваемая или хранимая различными способами, должна удовлетворять условию целостности данных, что помогает удостовериться в том, что она не была изменена или повреждена. В связи с этим возникает проблема, связанная с защитой информации от искажения при передаче и хранении, например, из-за действия шумов в каналах связи или при несанкционированном доступе к данным с целью их изменения и впоследствии к утрате корректных данных [1].

Наиболее популярным решением данной проблемы является применение избыточного кодирования [2], которое использует дополнительные данные с целью обнаружения и исправления ошибок, возникающих в процессе передачи или хранения информации в различных системах, структурах или каналах. Особенность данного кодирования представляется в виде добавления к исходному сообщению (исходной информации) избыточных данных, которые не влияют на смысл передаваемого сообщения, а лишь используются для того, чтобы при получении сообщения проверить его корректность. В случае, если сообщение оказывается некорректным, то можно использовать избыточные данные для исправления ошибок и получения достоверного сообщения.

В каналах связи возникают случаи, когда из-за действия шумов в сообщении возникают случайные одиночные и (или) множественные и (или) пакетные ошибки (ошибки в нескольких последовательных битах) [3–4]. В зависимости от выбираемого алгоритма кодирования избыточные коды способны исправлять оба типа ошибок. Однако нередко возникает проблема, когда полученное сообщение содержит одновременно и пакетные, и случайные ошибки. К таким сообщениям необходимо последовательно применять два избыточных кода, что снизит пропускную способность канала: первым может быть код, который исправит пакетные ошибки, а вторым – код, исправляющий случайные ошибки.

В настоящее время заслуживающим внимание решением данной проблемы является метод комбинирования известных избыточных кодов с целью исправления большего числа ошибок и приближения к оптимальной пропускной способности канала [5]. Для этого необходимы коды, исправляющие различные виды ошибок с высо-

кими корректирующими способностями, а также эффективные конструкции декодирования сообщения.

Для исправления пакетных ошибок наиболее известными и эффективными являются коды Фейра, Рида – Соломона (РС), БЧХ, турбокоды и операции перемежения/деперемежения совместно с традиционными кодами. Среди избыточных кодов, исправляющих одиночные ошибки, эффективными являются циклические и фонтанные коды, коды Хэмминга и LDPC.

В данной статье рассматривается новый подход в использовании комбинации различных кодов для коррекции пакетных и случайных ошибок на основе РС и LDPC соответственно, а также описывается оценка эффективности упомянутого комбинирования.

Основная часть. Коды LDPC (low-density parity-check) характеризуются их определением как low-density, то есть матрицы проверки на четность должны быть разреженными, что означает то, что они должны содержать в основном нули и небольшое количество единиц [6, 7]. За счет данного свойства значительно упрощается процесс кодирования и декодирования. Коды LDPC способны корректировать большое количество случайных ошибок с относительно низкой вычислительной сложностью и могут достигать производительности, близкой к пределу Шеннона [8]. Данные коды не имеют строгого предела по количеству исправляемых ошибок, так как оно зависит главным образом от скорости кода и длины кодового слова: более низкая скорость приводит к лучшему исправлению ошибок. Однако недостатком LDPC является их слабая способность исправления пакетных ошибок. Поэтому в качестве второго кода для комбинированного подхода предлагается использовать РС [9].

Коды РС особенно эффективны для исправления пакетных ошибок и стираний. Если код добавляет к исходному сообщению $2t$ избыточных символов, то он может исправить до t ошибок в блоке.

Исходя из свойств кодов LDPC и РС можно сделать вывод о том, что они взаимодополняемы, что делает возможным их совместное применение в схеме на основе использования комбинирования двух кодов. Данное кодирование способно исправлять оба типа ошибок и работать более эффективно, уменьшая количество избыточных битов, минимизируя при этом время обработки.

Система на основе комбинированного подхода предполагает использование внутреннего

кода для исправления пакетных ошибок, чтобы не нарушать последовательность бит, и внешнего кода для исправления оставшихся случайных ошибок (рис. 1).

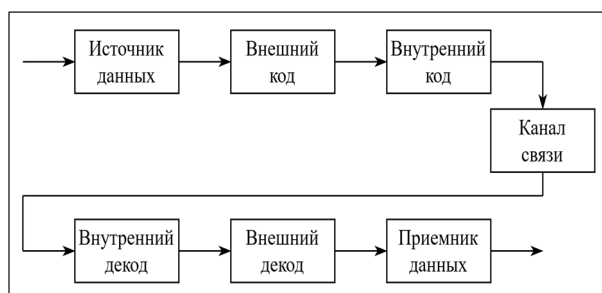


Рис. 1. Структурная схема информационной системы на основе комбинирования двух кодов

В качестве внутреннего предлагается использование кода PC, а в качестве внешнего – LDPC. Чтобы оценить эффективность комбинирования двух кодов, необходимо учитывать такие показатели, как частота ошибок по битам (BER – Bit Error Rate) после декодирования, равная количеству битовых ошибок, деленных на общее количество бит, скорость кода и отношение сигнал/шум (SNR – Signal-to-noise Ratio), равное мощности полезного сигнала к мощности шума.

После проведенного анализа эффективных кодов [10, 11] был построен график зависимости BER от SNR среди турбокода, кодов LDPC, PC, сверточного и БЧХ. Для построения кривой графика комбинации LDPC и PC используется моделирование Монте-Карло [12] с помощью библиотек языка Python, которое основывается на первоначальном кодировании информации с помощью LDPC, после – кодом PC, далее на передаче сообщения по шумному каналу и последующем декодировании (рис. 2). При моделировании приме-

няются различные длины блоков, скорость кодов, количество ошибок и уровень SNR.

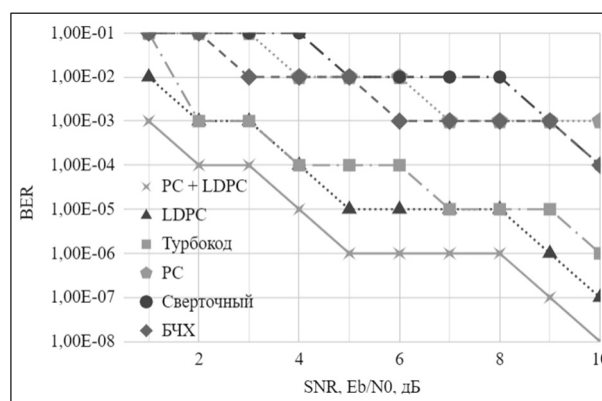


Рис. 2. График зависимости BER от SNR

Возможность комбинированного кода с исправлением пакетных и случайных ошибок обеспечивает самый низкий BER на всех уровнях SNR, что особенно эффективно в смешанных шумовых средах. В этом заключается рациональное использование предлагаемой комбинации.

Исходя из анализа можно сделать некоторые выводы, которые для наглядности представлены в виде табл. 1.

LDPC, турбокоды, БЧХ и сверточные коды способны исправлять случайные ошибки, коды PC – пакетные. LDPC обеспечивает самый низкий BER для случайных ошибок и хорошо работает в средах с высоким SNR, но ухудшается сильнее при низком SNR без дополнительных слоев коррекции ошибок. Турбокод эффективен в средах с низким SNR, особенно для случайных ошибок, но менее эффективен, чем LDPC в условиях с высоким SNR. PC лучше всего подходит для пакетной коррекции, но менее эффективен для случайного шума, особенно при низком SNR.

Таблица 1

Сравнение производительности комбинированного и одиночных кодов

Код	Тип исправляемых ошибок	Производительность
LDPC + PC	Случайные и пакетные	Достаточно хорошая производительность как для пакетных, так и для случайных ошибок. Производительность, близкая к пределу Шеннона для комбинированных систем
Турбокод	Случайные	Производительность близка к пределу Шеннона. Чувствительность к пакетным ошибкам по сравнению с PC + LDPC
LDPC	Случайные	Производительность вблизи предела Шеннона. Менее эффективна против пакетных ошибок
PC	Пакетные	Отлично подходит для пакетных ошибок. Слабее для случайных ошибок. Повышенная вычислительная сложность для длинных блоков
Сверточный	Случайные	Умеренная производительность. Обычно более низкая способность исправления ошибок по сравнению с LDPC и турбокодами
БЧХ	Случайные	Более сильная коррекция ошибок, чем у сверточных кодов. Недостаточно эффективная производительность, как у LDPC или турбокодов для высоких скоростей передачи данных

БЧХ код является достаточно хорошим для коррекции случайных ошибок, но менее эффективен, чем код LDPC и турбокод. Сверточный код в целом уступает коду LDPC и турбокоду, особенно в средах с высоким SNR. Комбинированный подход на основе данного анализа обеспечивает наилучшую производительность как для случайной, так и для пакетной коррекции ошибок, что делает его наиболее надежным вариантом для всех уровней SNR.

В связи с уменьшением коэффициента BER уменьшается и скорость кода. На основе работ [13–17] выяснено, что самая высокая скорость наблюдается у кодов LDPC, БЧХ и сверточного, которая напрямую зависит от размера блока, количества ошибок для исправления, длины ограничения и алгоритма Витерби соответственно, но они не способны исправлять по-отдельности все типы ошибок. Другие коды имеют умеренную скорость, зависящую в основном от размера блока данных. С учетом индивидуальных скоростей кодирования и декодирования LDPC и PC совокупная скорость комбинированной системы в большей степени будет зависеть от более медленного из двух кодов, поэтому предполагать скорость работы комбинации нужно исходя из скорости PC. В силу того, что код LDPC имеет высокую скорость за счет итеративных вычислений и разреженной матрицы проверки на четность, а код PC может быть интенсивно вычислительным из-за того, что использует алгебраический метод (синдромы, полиномы) кодирования и декодирования блоков данных, комбинированный подход обеспечивает достойное исправление ошибок, но его следует рассматривать для данных относительно небольших размеров для достижения наилучших показателей скорости работы, а также не следует использовать в системах, где требуется быстрое действие передачи больших объемов данных.

Комбинированный подход для малых объемов эффективен, так как скорость кодирования LDPC показывает отличные результаты на всех объемах данных, а PC лучше всего работает с данными размеров до 1 килобайта (Кб), что обеспечивает в совокупности комбинированное кодирование с максимальной скоростью

до 200 мегабит в секунду (Мб/с). Декодирование также эффективно из-за скорости кода PC и того, что LDPC коду для небольших блоков данных потребуется всего несколько итераций для исправления. Такая комбинация приведет к низкому коэффициенту битовых ошибок даже в шумных условиях.

Данные о скорости работы кодов представлены в виде табл. 2, где М – кодируемое сообщение объемом до 1 Кб, 100 Кб и 10 Мб. Предполагаемая скорость комбинации основывается на максимальной скорости кодирования и декодирования PC, так как он имеет значительное влияние из-за более медленной работы по сравнению с LDPC.

По мере увеличения размера данных увеличиваются и размеры блоков, обрабатываемых кодами PC и LDPC, что приводит к более медленному процессу кодирования. Скорость декодирования общей схемы замедляется из-за необходимости увеличения количества итераций у кода LDPC, в то же время PC по-прежнему хорошо обрабатывает пакетные ошибки, но значительно уступает в скорости. BER остается низким, поскольку декодирование LDPC обеспечивает исправление большинства случайных ошибок после того, как код PC справится с пакетными ошибками. Однако производительность может ухудшиться, особенно если SNR очень низкое. Для больших объемов данных сложность кодирования PC и LDPC становится значительной, так как скорость LDPC на больших блоках замедляется, а время на кодирование PC, особенно с большой длиной кода, становится слабым местом. Декодирование PC должно обрабатывать большие блоки, а итеративное декодирование LDPC становится ограниченным в производительности, которое особенно медленно при работе с большими наборами данных в шумных средах, так как для точности требуется больше итераций. Комбинированный подход по-прежнему обеспечивает достаточно высокое качество исправления ошибок для больших объемов, особенно в средах, подверженных пакетным ошибкам, однако компромиссом является скорость, поскольку время декодирования резко увеличивается, что является особенно существенным для приложений, работающих в реальном времени.

Таблица 2

Сравнение максимальной скорости работы кодов

Код	Скорость кодирования, Мб/с			Скорость декодирования, Мб/с		
	М < 1 Кб	М < 100 Кб	М < 10 Мб	М < 1 Кб	М < 100 Кб	М < 1 Мб
Турбокод	200	100	20	100	70	15
LDPC	800	400	200	700	400	150
PC	200	100	50	150	80	30
Сверточный	300	150	100	200	100	70
БЧХ	250	150	80	200	100	50
PC + LDPC	200 (максимальная PC)	100 (максимальная PC)	50 (максимальная PC)	150 (максимальная PC)	80 (максимальная PC)	30 (максимальная PC)

В итоге скорость кодирования и декодирования комбинированного подхода выполняется относительно быстро для небольших объемов данных, но уменьшается для средних и больших. В то же время комбинация обеспечивает отличную производительность исправления ошибок для всех размеров данных, гарантируя низкий BER в большинстве сред. Комбинация кодов PC и LDPC на основе анализа хорошо подходит для приложений реального времени, таких как телекоммуникации или потоковая передача, где необходимо быстро обрабатывать небольшие сообщения. Подходит для систем со средней пропускной способностью, например, спутниковая связь, хранение данных с умеренными требованиями к задержке, где их целостность имеет решающее значение, а пакетные ошибки являются обычным явлением. А также подходит для автономных или приложений не в реальном времени, требующих высокой эффективности исправления ошибок, таких как, например, архивное хранение или передача больших объемов данных по шумным каналам. Как итог, данный подход имеет преимущество в использовании для систем, где целостность данных важнее скорости работы.

Несколько комбинированных подходов к кодированию с исправлением ошибок используются в современном мире в различных системах передачи и хранения. Сравнительные выводы о характеристиках известных комбинаций с рассматриваемым LDPC и PC были сделаны на основе нескольких работ [18–22]. Эти коды часто объединяют различные типы исправления ошибок, используемых в промышленности. Их основные преимущества и недостатки представлены в виде табл. 3.

Производительность PC и LDPC максимальная среди всех рассматриваемых кодов на небольших объемах данных размером до 1 Кб, что свидетельствует о том, что данная комбинация является целесообразной и практичной для реализации и использования.

Подводя итог, необходимо подчеркнуть, PC и LDPC обеспечивает сильную сбалансированную производительность, но лучше всего подходит для приложений, где исправление имеет приоритет над задержкой, особенно когда необходимо устранить как пакетные, так и случайные ошибки.

Существуют методы, позволяющие улучшить производительность предлагаемого комбинированного подхода путем распараллеливания работы кода LDPC, что существенно снизит задержки при передаче данных и ускорит работу кодирования. Для этого могут использоваться оптимизация матрицы проверки на четность, многоуровневое декодирование, метод уменьшения количества итераций при кодировании и декодировании сообщения, в том числе механизм раннего завершения для уменьшения количества итераций в зависимости от условий канала, а также параллельный метод использования нескольких субдекодеров [23, 24]. Для улучшения производительности кода PC возможны случаи применения как систематических кодов, так и алгоритмов Берлекэмп – Мессе, Форни или параллельной обработки [25].

Преимуществом использования подхода комбинирования кодов PC и LDPC является надежная возможность исправления двух видов ошибок, что значительно снижает возникновение некорректности, требующей повторной передачи данных, из-за чего повышается эффективность пропускной способности канала.

Таблица 3

Сравнение известных комбинированных кодов с кодом PC + LDPC

Комбинированный код	Преимущества	Недостатки	Сравнение с PC + LDPC
Коды турбопродуктов	Близкий к пределу Шеннона, хорошая коррекция случайных ошибок	Низкая скорость декодирования, слабая коррекция пакетных ошибок	PC + LDPC эффективнее для пакетных ошибок, но скорость работы ниже
PC + Сверточный	Хорошая коррекция пакетных ошибок	Слабая коррекция случайных ошибок	PC + LDPC эффективнее для исправления случайных ошибок
Полярный + CRC	Высокая производительность, эффективен для небольших данных	Высокая задержка для больших данных, слабая коррекция пакетных ошибок	PC + LDPC скорость работы выше для больших данных, эффективнее для пакетных ошибок
LDPC + БЧХ	Высокая пропускная способность, низкая задержка	Слабая коррекция пакетных ошибок	PC + LDPC эффективнее для пакетных ошибок, но скорость работы ниже
Турбокод + PC	Низкое значение BER, хорошая коррекция случайных ошибок	Низкая скорость декодирования	PC + LDPC скорость работы выше для больших данных

Система на основе комбинирования кодов, обеспечивая надежное исправление ошибок скрытых данных при внедрении, может улучшить стеганографию [26].

Когда сообщение встраивается в определенные области контейнера, искажения могут повлиять на последовательные биты, вызывая при этом пакетные ошибки – коды РС способны восстановить исходную информацию, даже если сегмент данных поврежден. Случайные ошибки могут возникнуть в стеганографических системах из-за шума в каналах или искажений в процессе сжатия – коды LDPC исправят это, что сделает скрытые данные более устойчивыми к различным типам атак.

Подход комбинирования на основе избыточных кодов, позволяя внедрять меньше данных, сохраняя при этом высокую надежность, обеспечивает эффективное исправление ошибок [27]. Это сводит к минимуму изменения в контейнере-носителе, тем самым снижает вероятность обнаружения методами стеганоанализа.

На основе анализа выявлено, что особым преимуществом пользуется встраивание информации в контейнер-изображение методом дискретного вейвлет-преобразования (ДВП), который обеспечивает некоторую устойчивость к сжатию, обрезке, вращению и масштабированию, сохраняя при этом незаметность, так как данные внедряются в коэффициенты преобразования [28]. ДВП раскладывает изображение на поддиапазоны (LL, LH, HL, HH) различных частотных значений, где высокочастотные поддиапазоны (LH, HL, HH) используются для встраивания сообщения. В силу

того, что внедрение происходит в частотные характеристики изображения, данные меньше подвержены изменениям и потере в случае модификации контейнера.

Применение комбинации РС и LDPC с методом ДВП может позволить восстановить исходное сообщение даже при значительных изменениях в силу преимуществ обоих.

Заключение. Предложенный и проанализированный подход комбинированного кодирования информации основан на двух избыточных кодах: РС как внутреннего и LDPC как внешнего. Данная комбинация способна исправить множественные ошибки, включая пакетные и случайные, что значительно повышает корректирующую способность. На основе проведенных анализов рассмотрены характеристики комбинированного РС и LDPC, а также некоторых одиночных и комбинированных кодов, в ходе чего выявлены основные преимущества и недостатки. Особым достоинством предлагаемого подхода является низкий коэффициент битовых ошибок после декодирования и достаточно эффективная скорость работы для небольших объемов данных.

Научный и практический интерес представляет дальнейшее развитие исследований в данной предметной области, связанное с оценкой пропускной способности канала, корректирующими способностями комбинации на основе кодов РС и LDPC для повышения надежности и эффективности системы избыточного кодирования, а также метод использования комбинации в стеганографических приложениях.

Список литературы

1. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.
2. Hamming R. W. Error detecting and error correcting codes // The Bell System Technical Journal. 1950. Vol. 29, no. 2. P. 147–160. DOI: 10.1002/j.1538-7305.1950.tb00463.x.
3. Meggitt J. E. Error-correcting codes for correcting bursts of errors // Transactions of the American Institute of Electrical Engineers. Part I. Communication and Electronics. 1961. Vol. 79, no. 6. P. 708–711. DOI: 10.1109/TCE.1961.6373036.
4. Nguyen H., Shwedyk E. Probability theory, random variables and random processes // A First Course in Digital Communications. Cambridge University Press. 2009. P. 77–134. DOI: <https://doi.org/10.1017/CBO9780511841583.004>.
5. Compiled Code Study of Joint Parity and Cyclic Redundancy Check / G. Xiaoqing [et al.] // IEEE 5th International Conference on Electronic Information and Communication Technology (ICEICT). 2022. P. 77–80. DOI: 10.1109/ICEICT55736.2022.9909046.
6. Gallager R. Low-density parity-check codes // IRE Transactions on Information Theory. 1962. Vol. 8, no. 1. P. 21–28. DOI: 10.1109/TIT.1962.1057683.
7. Хартанович А. А. Сравнительный анализ современных избыточных кодов и их применение в стеганографии // Информационные технологии: материалы 88-й науч.-техн. конф. проф.-препод. состава, науч. сотрудников и аспирантов, Минск, 29 января – 16 февраля 2024 г. Минск, 2024. С. 19–22.
8. Computational complexities and relative performance of LDPC codes and turbo codes / J. Zuo [et al.] // IEEE 4th International Conference on Software Engineering and Service Science. 2013. P. 251–254. DOI: 10.1109/ICSESS.2013.6615299.

9. Burst-error-correcting algorithm for Reed-Solomon codes and its performance over a bursty channel / L. Yin [et al.] // IEEE 2002 International Conference on Communications, Circuits and Systems and West Sino Expositions. 2002. Vol. 1. P. 77–81. DOI: <https://doi.org/10.1109/ICCCAS.2002.1180576>.
10. Bingrui W., Qingli Z. Study of performance comparison of satellite error correction codes for correcting big burst data errors // IEEE 3rd International Conference on Big Data Analysis (ICBDA). 2018. P. 254–258. DOI: <https://doi.org/10.1109/icbda.2018.8367687>.
11. Performance comparison of turbo codes with LDPC codes and with BCH codes for forward error correcting codes / M. Alwan [et al.] // IEEE Student Conference on Research and Development (SCORED). 2015. P. 556–560. DOI: <https://doi.org/10.1109/SCORED.2015.7449398>.
12. Monte Carlo simulation of the binary communications system based on Matlab / J. Liu [et al.] // International Conference on Electrical and Control Engineering. 2011. P. 2368–2370. DOI: [10.1109/ICECENG.2011.6057010](https://doi.org/10.1109/ICECENG.2011.6057010).
13. Воробьев Э. И., Преображенский Ю. П. Исследование помехоустойчивого кодирования различных файлов // Моделирование, оптимизация и информационные технологии. 2018. Т. 6, № 4: Системы безопасности. С. 535–544. DOI: [10.26102/2310-6018/2018.23.4.040](https://doi.org/10.26102/2310-6018/2018.23.4.040).
14. Li J. The efficient implementation of Reed-Solomon high rate erasure resilient codes // IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP). 2005. Vol. 3. P. 1097–1100. DOI: [10.1109/ICASSP.2005.1415905](https://doi.org/10.1109/ICASSP.2005.1415905).
15. New architectures for fast convolutional encoders and threshold decoders / D. Haccoun [et al.] // IEEE Journal on Selected Areas in Communications. 1988. Vol. 6, no. 3. P. 457. DOI: [10.1109/49.1923](https://doi.org/10.1109/49.1923).
16. Ma X., Yang, E. Low-Density Parity-Check Code with Fast Decoding Speed // IEEE Transactions on Information Theory. 2006. 44 p. DOI: <https://doi.org/10.48550/arXiv.cs/0602081>.
17. Abbasfar A. Turbo-like Codes: Design for High Speed Decoding. 2007. 84 p.
18. Turbo Product Codes: Applications, Challenges, and Future Directions / H. Mukhtar [et al.] // IEEE Communications Surveys And Tutorials. 2016. Vol. 18, no. 4. P. 3052–3069. DOI: <https://doi.org/10.1109/COMST.2016.2587863>.
19. Mergu K. Performance Analysis of Reed-Solomon Codes Concatenated with Convolutional Codes Over AWGN Channel // APTIKOM Journal on Computer Science and Information Technologies. 2016. Vol. 1, no. 1. P. 27–32. DOI: <https://doi.org/10.11591/APTIKOM.J.CSIT.100>.
20. Performance Analysis of CRC-Polar Concatenated Codes / L. Sari [et al.] // Jurnal infotel. 2020. Vol. 12, no. 4. P. 123–128. DOI: <https://doi.org/10.20895/INFOTEL.V12I4.494>.
21. Design and Simulation of Parallel BCH Code with LDPC Code For Flash Memories / A. Mahdy [et al.] // 12th International Conference on Electrical Engineering (ICEENG). 2020. P. 196–199. DOI: <https://doi.org/10.1109/ICEENG45378.2020.9171743>.
22. On the concatenation of turbo codes and Reed-Solomon codes / G. Zhou [et al.] // IEEE International Conference on Communications. 2003. Vol. 3. P. 2134–2138. DOI: <https://doi.org/10.1109/ICC.2003.1204021>.
23. Романенко Д. М., Пацей Н. В. Защита информации методами избыточного кодирования на основе каскадных схем // Эпоха науки. 2019. № 20. С. 194–200. DOI: [10.24411/2409-3203-2019-12034](https://doi.org/10.24411/2409-3203-2019-12034).
24. Пацей Н. В. Параллельное каскадное вероятностное декодирование кодов низкой плотности проверок на четность // Труды БГТУ. Физико-математические науки и информатика. 2015. № 6. С. 157–161.
25. Das A., Toubia N. A. Systematic b-adjacent symbol error correcting reed-solomon codes with parallel decoding // IEEE 36th VLSI Test Symposium (VTS). 2018. P. 1–6. DOI: [10.1109/VTS.2018.8368650](https://doi.org/10.1109/VTS.2018.8368650).
26. Урбанович П. П. Особенности использования методов избыточного кодирования в стеганографических приложениях // Информационные технологии и системы 2022: материалы Междунар. науч. конф., Минск, 23 ноября 2022 г. Минск: БГУИР, 2022. С. 173–174.
27. Урбанович П. П. Коррекция одиночных и двойных парных ошибок в стенографических каналах передачи информации // Информационные системы и технологии: материалы Междунар. науч. конгр. по информатике, Минск, 27–28 октября 2022 г. Минск, 2022. С. 113–119.
28. Хартанович А. А. Сравнение эффективности стеганографических методов для различных форматов изображений // 75-я науч.-техн. конф. учащихся, студентов и магистрантов: сб. науч. работ, Минск, 22–27 апреля 2024 г. Минск: БГТУ, 2022. С. 789–790.

References

1. Urbanovich P. P. *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii* [Information protection by cryptography, steganography and obfuscation methods]. Minsk, BGTU Publ., 2016. 220 p. (In Russian).
2. Hamming R. W. Error detecting and error correcting codes. *The Bell System Technical Journal*, 1950, vol. 29, no. 2, pp. 147–160. DOI: [10.1002/j.1538-7305.1950.tb00463.x](https://doi.org/10.1002/j.1538-7305.1950.tb00463.x).

3. Meggitt J. E. Error-correcting codes for correcting bursts of errors. *Transactions of the American Institute of Electrical Engineers. Part I. Communication and Electronics*, 1961, vol. 79, no. 6, pp. 708–711. DOI: 10.1109/TCE.1961.6373036.
4. Nguyen H., Shwedyk E. Probability theory, random variables and random processes. *A First Course in Digital Communications. Cambridge University Press*, 2009, pp. 77–134. DOI: <https://doi.org/10.1017/CBO9780511841583.004>.
5. Xiaoqing G., Guangzu L., Linlin S., Jun Z. Compiled Code Study of Joint Parity and Cyclic Redundancy Check. *IEEE 5th International Conference on Electronic Information and Communication Technology (ICEICT)*, 2022, pp. 77–80. DOI: 10.1109/ICEICT55736.2022.9909046.
6. Gallager R. Low-density parity-check codes. *IRE Transactions on Information Theory*, 1962, vol. 8, no. 1, pp. 21–28. DOI: 10.1109/TIT.1962.1057683.
7. Khartanovich A. A. Comparative analysis of modern redundant codes and their application in steganography. *Informatsionnyye tekhnologii: materialy 88-y nauchno-tekhnicheskoy konferentsii professorsko-prepodavatel'skogo sostava, nauchnykh sotrudnikov i aspirantov* [Information technologies: materials of the 88th Scientific and Technical Conference of the teaching staff, researchers and postgraduates]. Minsk, 2024, pp. 19–22 (In Russian).
8. Zuo J., Sun Q., Zhao F. Computational complexities and relative performance of LDPC codes and turbo codes. *IEEE 4th International Conference on Software Engineering and Service Science*, 2013, pp. 251–254. DOI: 10.1109/ICSESS.2013.6615299.
9. Yin L., Lu J., Letaief K. B., Wu Y. Burst-error-correcting algorithm for Reed-Solomon codes and its performance over a bursty channel. *IEEE 2002 International Conference on Communications. Circuits and Systems and West Sino Expositions*, 2002, vol. 1, pp. 77–81. DOI: <https://doi.org/10.1109/ICCCAS.2002.1180576>.
10. Bingrui W., Qingli Z. Study of performance comparison of satellite error correction codes for correcting big burst data errors. *IEEE 3rd International Conference on Big Data Analysis (ICBDA)*, 2018, pp. 254–258. DOI: <https://doi.org/10.1109/icbda.2018.8367687>.
11. Alwan M. H., Singh M., Mahdi H. F. Performance comparison of turbo codes with LDPC codes and with BCH codes for forward error correcting codes. *IEEE Student Conference on Research and Development (SCoReD)*, 2015, pp. 556–560. DOI: <https://doi.org/10.1109/SCoRED.2015.7449398>.
12. Liu J., Wu S., Chen C., Xiong G. Monte Carlo simulation of the binary communications system based on Matlab. *International Conference on Electrical and Control Engineering*, 2011, pp. 2368–2370. DOI: 10.1109/ICECENG.2011.6057010.
13. Vorobyov E. I., Preobrazhensky Y. P. Study of noise-resistant coding of various files. *Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii; Sistemy bezopasnosti* [Modeling, optimization and information technology: Security systems]. 2018, vol. 6, no. 4, pp. 535–544. DOI: 10.26102/2310-6018/2018.23.4.040 (In Russian).
14. Li J. The efficient implementation of Reed-Solomon high rate erasure resilient codes. *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2005, vol. 3, pp. 1097–1100. DOI: 10.1109/ICASSP.2005.1415905.
15. Haccoun D., Lavoie P., Savaria Y. New architectures for fast convolutional encoders and threshold decoders. *IEEE Journal on Selected Areas in Communications*, 1988, vol. 6, no. 3, p. 457. DOI: 10.1109/49.1923.
16. Ma X., Yang, E. Low-Density Parity-Check Code with Fast Decoding Speed. *IEEE Transactions on Information Theory*, 2006. 44 p. DOI: <https://doi.org/10.48550/arXiv.cs/0602081>.
17. Abbasfar A. Turbo-like Codes: Design for High Speed Decoding, 2007. 84 p.
18. Mukhtar H., Al-Dweik A., Shami A. Turbo Product Codes: Applications, Challenges, and Future Directions. *IEEE Communications Surveys And Tutorials*, 2016, vol. 18, no. 4, pp. 3052–3069. DOI: <https://doi.org/10.1109/COMST.2016.2587863>.
19. Mergu K. Performance Analysis of Reed-Solomon Codes Concatenated with Convolutional Codes Over AWGN Channel. *APTIKOM Journal on Computer Science and Information Technologies*, 2016, vol. 1, no. 1, pp. 27–32. DOI: <https://doi.org/10.11591/APTIKOM.J.CSIT.100>.
20. Sari L., Assiddiq U. P., Alam S., Surjati I. Performance Analysis of CRC-Polar Concatenated Codes. *Jurnal infotel*, 2020, vol. 12, no. 4, pp. 123–128. DOI: <https://doi.org/10.20895/INFOTEL.V12I4.494>.
21. Mahdy A., Abdelaziz M., El-azeem M. Design and Simulation of Parallel BCH Code with LDPC Code For Flash Memories. *12th International Conference on Electrical Engineering (ICEENG)*, 2020, pp. 196–199. DOI: <https://doi.org/10.1109/ICEENG45378.2020.9171743>.
22. Zhou G., Lin T., Wang W., Lindseyn W. On the concatenation of turbo codes and Reed-Solomon codes. *IEEE International Conference on Communications*, 2003, vol. 3, pp. 2134–2138. DOI: <https://doi.org/10.1109/ICC.2003.1204021>.

23. Romanenko D. M., Patsey N. V. Information protection by methods of redundant coding based on cascade schemes. *Epokha nauki* [The Age of Science], 2019, no. 20, pp. 194–200 (In Russian). DOI: 10.24411/2409-3203-2019-12034.
24. Patsey N. V. Parallel cascade probabilistic decoding of low-density parity-check codes. *Trudy BGTU* [Proceedings of BSTU], 2015, no 6: Physics and Mathematics. Informatics, pp. 157–161 (In Russian).
25. Das A., Touba N. A. Systematic b-adjacent symbol error correcting reed-solomon codes with parallel decoding. *IEEE 36th VLSI Test Symposium (VTS)*, 2018, pp. 1–6. DOI: <https://doi.org/10.1109/VTS.2018.8368650>.
26. Urbanovich P. P. Features of using redundant coding methods in steganographic applications. *Informatsionnyye tekhnologii i sistemy 2022: materialy Mezhdunarodnoy nauchnoy konferentsii* [Information technologies and systems 2022: materials of the international scientific conference]. Minsk, 2022, pp. 173–174 (In Russian).
27. Urbanovich P. P. Correction of single and double paired errors in stenographic information transmission channels. *Informatsionnyye sistemy i tekhnologii: materialy Mezhdunarodnogo nauchnogo kongressa po informatike* [Information systems and technologies: materials of the international scientific congress on informatics]. Minsk, 2022, pp. 113–119 (In Russian).
28. Khartanovich A. A. Comparison of the effectiveness of steganographic methods for different image formats. *75-ya nauchno-tekhnicheskaya konferentsiya uchashchikhsya, studentov i magistrantov: sbornik nauchnykh rabot* [75rd Scientific and Technical Conference of students, undergraduates and undergraduates: collection of scientific papers]. Minsk, 2024, pp. 789–790 (In Russian).

Информация об авторе

Хартанович Алина Александровна – магистрант кафедры информационных систем и технологий. Белорусский государственный технологический университет (ул. Свердлова, 13а, 220006, г. Минск, Республика Беларусь). E-mail: alinakhartanovichlo@gmail.com

Information about the author

Khartanovich Alina Aleksandrovna – Master's degree student, the Department of Information Systems and Technologies. Belarusian State Technological University (13a Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: alinakhartanovichlo@gmail.com

Поступила 31.10.2024