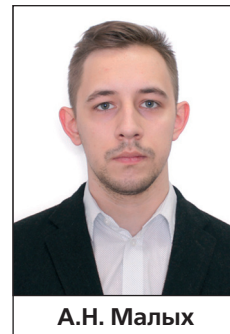


СОВЕРШЕНСТВОВАНИЕ АЛГОРИТМА ОЦЕНКИ СВОЙСТВ ЦИКЛИЧЕСКОГО КОДА В СИСТЕМАХ ДИСПЕТЧЕРСКОЙ ЦЕНТРАЛИЗАЦИИ

В статье предложен алгоритм сокращенного перебора, позволяющий кратно уменьшить ресурсоемкость и время расчета количества необнаруженных трансформаций циклического кода по сравнению с алгоритмом полного перебора.

Ключевые слова: железнодорожная автоматика и телемеханика, диспетчерская централизация, циклические коды

EDN: ENZQPE



А.Н. Малых



А.Н. Малых

Одним из основополагающих требований, предъявляемых к современным системам железнодорожной автоматики и телемеханики, является их соответствие нормативным значениям показателей надежности и функциональной безопасности.

В документе [1] установлены следующие требования к реализации функций телеуправления (ТУ) и телесигнализации (ТС) системами диспетчерской централизации (ДЦ):

- вероятность трансформации сигнала ТС не более 10^{-10} ;
- вероятность потери сигнала ТС не более 10^{-8} ;

- вероятность возникновения ложного сигнала ТС при отсутствии передачи не более 10^{-12} ;
- вероятность трансформации сигнала ТУ не более 10^{-14} ;
- вероятность потери сигнала ТУ не более 10^{-10} ;
- вероятность генерации ложной команды ТУ при отсутствии передачи не более 10^{-12} ;
- интенсивность опасных отказов технических средств передачи и реализации ответственных команд должна быть не более $3 \cdot 10^{-11}$ 1/ч на одну команду.

При реализации неотчетливых команд ТУ, непосредственно не связанных с обеспечением безопасно-

Малых Александр Николаевич, старший преподаватель кафедры «Системы управления транспортной инфраструктурой» Российского университета транспорта (РУТ (МИИТ)). Область научных интересов: влияние надежности и эффективности систем железнодорожной автоматики и телемеханики на перевозочный процесс. Автор 23 научных работ.

Малых Алексей Николаевич, ассистент кафедры «Системы управления транспортной инфраструктурой» Российского университета транспорта (РУТ (МИИТ)). Область научных интересов: имитационное моделирование технологических процессов на железнодорожном транспорте. Автор 12 научных работ.

Орлов Александр Валерьевич, кандидат технических наук, доцент, доцент кафедры «Системы управления транспортной инфраструктурой» Российского университета транспорта (РУТ (МИИТ)). Область научных интересов: эффективность технических систем. Автор 95 научных работ.

Смыслов Алексей Владимирович, аспирант кафедры «Системы управления транспортной инфраструктурой» Российского университета транспорта (РУТ (МИИТ)). Область научных интересов: анализ надежности, безопасности и эффективности систем телеуправления на железнодорожном транспорте. Автор пяти научных работ.

Тарадин Николай Александрович, кандидат технических наук, доцент, доцент кафедры «Системы управления транспортной инфраструктурой» Российского университета транспорта (РУТ (МИИТ)). Область научных интересов: надежность и безопасность функционирования инфраструктуры на железнодорожном транспорте. Автор 60 научных работ.

сти движения поездов, к системам ДЦ предъявляются требования по достоверности передачи информации. При определении достоверности используются следующие методы: экспертные, расчетные, испытания на машинных моделях, а также испытания системы в условиях эксплуатации [2]. Расчетные методы могут быть использованы для определения передачи информации аппаратурой ДЦ и достоверности передачи информации в каналах ТУ и ТС.

Сложная структура аппаратного обеспечения системы и использование при передаче длинных сообщений, к которым относятся сигналы ТУ и ТС, приводят к тому, что точный расчет вероятностных характеристик практически невозможен. Поэтому при расчетах используется верхняя оценка вероятности искажения сигналов ТУ и ТС при известном классе кода, длины кодовой комбинации n , числе контрольных разрядов r и числе информационных разрядов k .

Рассмотрим алгоритм сокращенного перебора, позволяющий многократно снизить вычислительные ресурсы при расчете количества необнаруженных трансформаций циклического кода с целью доказательства безопасности передачи данных в системах ДЦ.

Для обеспечения требуемого уровня надежности и безопасности передачи данных в системах телеуправления на железнодорожном транспорте широко применяются помехозащищенные коды [3]. Одним из наиболее часто используемых видов таких кодов являются циклические коды [4].

В частности, в ГОСТ Р 59263-2020 [5] среди прочих рекомендуется применение стандартных интерфейсов CAN и Ethernet, в которых в качестве проверки целостности кадров (frame check sequence) обычно применяется CRC (cyclic redundancy check), например, CRC-16 и CRC-16-CCITT. Для генерации кода CRC-16 и CRC-16-CCITT используется полином шестнадцатой степени, соответственно, контрольная часть такого кода состоит из шестнадцати разрядов. Для этих видов кодов установлено, что минимальное кодовое расстояние $d_{\min} = 4$ и код способен гарантированно обнаруживать все ошибки нечетной кратности.

Для расчета количества необнаруженных трансформаций кода CRC-16-CCITT авторами предложены математическая модель и алгоритм, которые позволяют с помощью перебора рассчитать количество необнаруженных трансформаций $N_{\text{нт}}$ для сообщения заданной длины n и заданного значения кратности ошибки k . Кратность ошибки k указывает на то, сколько бит в принятом сообщении изменило свое значение на противоположное («1» в исходном

сообщении трансформируется в «0» в принятом, а «0» трансформируется в «1»). Предполагается, что появление ошибок равновероятно по всей длине сообщения, вероятность их появления характеризуется коэффициентом битовых ошибок BER (bit error gate).

Для имитации воздействия помех на отправленное сообщение реализован алгоритм полного перебора возможных вариантов сочетаний трансформированных битов. Исходное сообщение заданной длины поразрядно суммируется по модулю два (исключающее «ИЛИ» или XOR) со сформированными неповторяющимися шаблонами ошибок, которые представляют собой вектор, равный длине исходного сообщения n , состоящего из k единиц и $(n-k)$ нулей.

Число шаблонов ошибок $N_{\text{ш}}(n, k)$, равное количеству проводимых проверок, можно вычислить по формуле

$$N_{\text{ш}}(n, k) = C_n^k,$$

где n — длина исходного сообщения; k — кратность ошибки.

При реализации алгоритма при каждой проверке искаженное сообщение делится на образующий полином и в случае, если результат деления равен нулю, считается, что произошла необнаруженная трансформация. В этом случае, переменная-счетчик, которая отвечает за подсчет количества необнаруженных трансформаций, увеличивает свое значение на 1. Блок-схема данного алгоритма представлена на рис. 1.

Анализ данного алгоритма показывает, что количество необнаруженных трансформаций $N_{\text{нт}}$ и количество шаблонов ошибок $N_{\text{ш}}$ для сообщений с заданной длиной n и кратностью ошибки k не зависят от содержания исходного сообщения.

При определении количества необнаруженных трансформаций $N_{\text{нт}}$ для относительно коротких сообщений ($n=152$ бит) и кратности ошибки $k=4$, расчет происходит сравнительно быстро: около двух минут. При этом количество сформированных шаблонов ошибок равно:

$$N_{\text{ш}}(152, 4) = C_{152}^4 = 21\,374\,050 \text{ шаблонов.}$$

Однако, увеличение длины отправляемого сообщения n и/или увеличение кратности ошибки k приводит к существенному росту количества возможных шаблонов ошибок $N_{\text{ш}}$. Например, расчет количества необнаруженных трансформаций $N_{\text{нт}}$ для сообщений длиной $n=1000$ бит и кратностью ошибки $k=4$ будет проводиться в течение нескольких суток (количество шаблонов ошибок: $N_{\text{ш}}(1000, 4) = C_{1000}^4 = 41\,417\,124\,750$). При

большей длине сообщения n или кратностях ошибок k расчет становится еще более ресурсоемким.

В задачах, связанных с комбинаторикой, описанная выше проблема получила соответствующее название — «проклятие размерности»: с ростом размера исходных данных происходит быстрый рост сложности переборных алгоритмов [6].

Для решения вышеописанной проблемы авторами был разработан метод, позволяющий проводить перебор не всех возможных шаблонов ошибок $N_{\text{ш}} = C_n^k$, а лишь некоторой части — $N'_{\text{ш}}$, что значительно снижает

продолжительность расчетов при полном совпадении результатов вычислений. Количество действий в сокращенном алгоритме по сравнению с алгоритмом полного перебора будет равно:

$$N'_{\text{ш}} = \frac{k}{n} \cdot N_{\text{ш}} = \frac{k}{n} \cdot C_n^k.$$

Сравнительная оценка объемов вычислений количества необнаруженных трансформаций в сообщении длиной n и кратностью ошибки k при использовании алгоритма с полным перебором шаблонов ошибок и

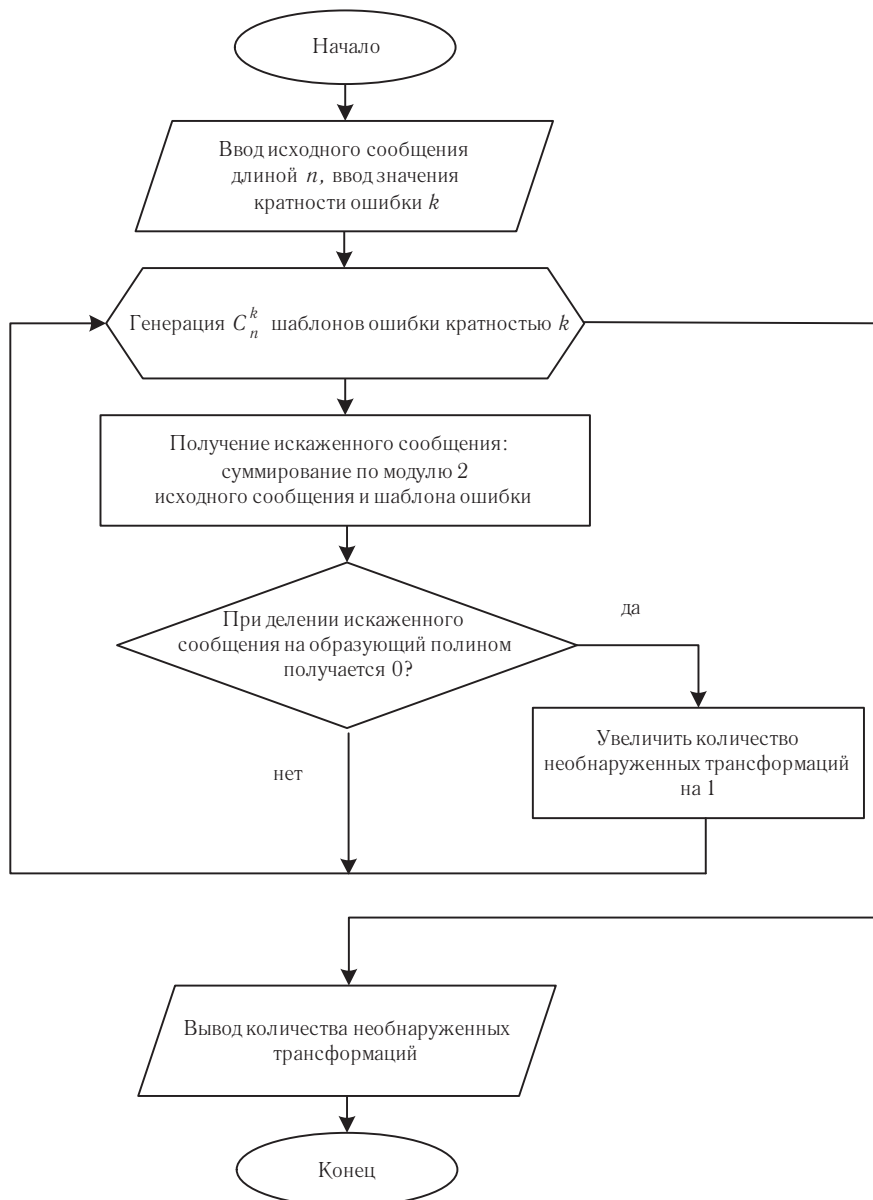


Рис. 1. Блок-схема алгоритма для поиска количества необнаруженных трансформаций, основанного на полном переборе всех возможных шаблонов ошибок

Таблица 1

**Сравнительная оценка алгоритмов расчета количества
необнаруженных трансформаций**

Длина сообщения в битах, n	Кратность ошибки, k	Количество действий при полном переборе всех шаблонов ошибки, $N_{\text{ш}} = C_n^k$	Количество действий при сокращенном алгоритме перебора	Отношение количества действий при полном переборе к количеству действий при сокращенном алгоритме
48	4	194 580	16 215	$\frac{194580}{16215} = \frac{n}{k} = \frac{48}{4} = 12$
48	6	12 271 512	1 533 939	$\frac{12271512}{1533939} = \frac{n}{k} = \frac{48}{6} = 8$
152	4	21 374 050	562 475	$\frac{21374050}{562475} = \frac{n}{k} = \frac{152}{4} = 38$
152	6	15 500 461 060	407 906 870	$\frac{15500461060}{407906870} = \frac{n}{k} = \frac{152}{6} = 25,33$

предложенного сокращенного алгоритма перебора показана в табл. 1.

Разработанный метод основан на свойствах циклического кода: в списке шаблонов ошибок, приводящих к необнаруженным трансформациям, зафиксированы паттерны, анализ которых дал возможность рассчитать количество необнаруженных трансформаций без проведения полного перебора. Блок-схема алгоритма для нахождения количества необнаруженных трансформаций с помощью сокращенного перебора шаблонов ошибок представлена на рис. 2.

Для сравнения двух рассмотренных выше алгоритмов на рис. 3 представлен полный список шаблонов ошибок, приводящих к необнаруженным трансформациям для сообщения длиной $n=48$ бит. На рис. 4 представлен список шаблонов ошибок, приводящих к необнаруженным трансформациям, но полученный с помощью алгоритма сокращенного перебора. Список на рис. 3 содержит 48 шаблонов ошибок, приводящих к необнаруженным трансформациям ($N_{\text{шт}}=48$ по количеству строк), а список на рис. 4 содержит всего две строки.

При анализе списка шаблонов на рис. 3, полученного с помощью полного перебора, можно обнаружить, что в нем есть повторяющиеся комбинации

нулей и единиц — «паттерны». Таких паттернов всего два: они представлены в списке на рис. 4.

Паттернами в данном случае будем называть наборы из «1» и «0», которые содержат в себе четыре «1» (так как кратность ошибок $k=4$), т.е.:

Pattern 1: 10001000000100001

Pattern 2: 100000001000000000000010000000001

Для того, чтобы определить количество необнаруженных трансформаций $N_{\text{шт}}$ с помощью предлагаемого метода сокращенного перебора в строках, содержащих паттерны, подсчитывается количество символов «0» справа от самих паттернов. Это обусловлено тем, что в полном списке шаблонов, приводящих к необнаруженным трансформациям, паттерн «циклически сдвигается вправо» — количество таких сдвигов как раз определяется количеством символов «0» справа от паттернов.

Очевидно, что для рассмотренного случая в полученном списке шаблонов, приводящих к необнаруженным трансформациям, чаще будет повторяться Pattern 1, так как его длина меньше, чем длина Pattern 2. Так, на рис. 5 видно: в строке 32 Pattern 2 «полностью сдвинулся вправо» и не может больше повторяться, далее со строки 33 повторяется только более короткий Pattern 1.

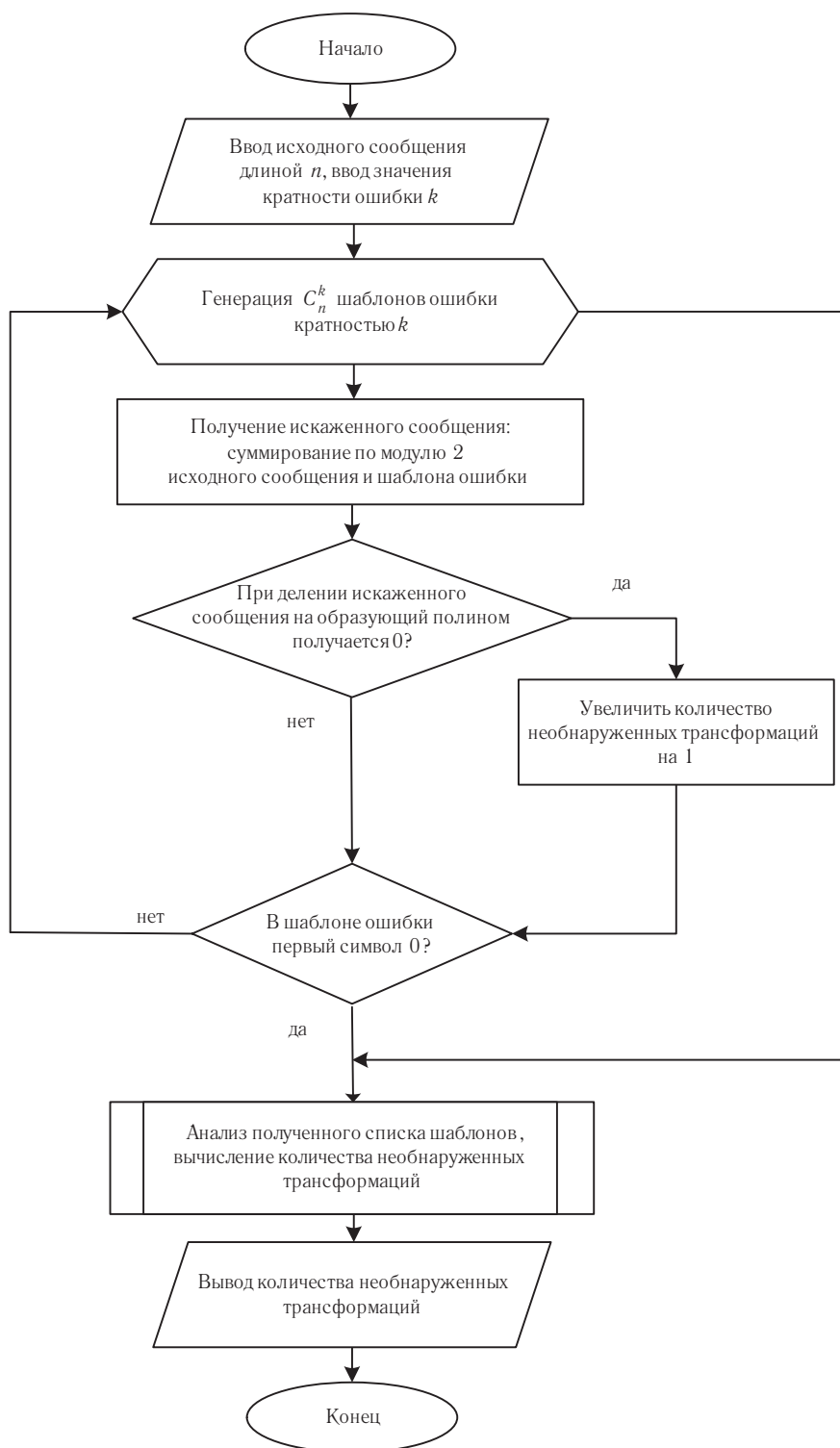


Рис. 2. Блок-схема разработанного алгоритма для нахождения количества необнаруженных трансформаций, основанного на сокращенном переборе шаблонов ошибок

[illegible]

Рис. 4. Список шаблонов ошибок, приводящих к необнаруженным трансформациям, полученный с помощью сокращенного перебора

Количество необнаруженных трансформаций, определяемых предлагаемым методом сокращенного перебора, можно рассчитать по формуле

$$N_{\text{нт}} = N_{\text{пат}} + \sum_{i=1}^{N_{\text{пат}}} (n - l_{\text{пат } i}),$$

где n — длина сообщения;

$l_{\text{пат } i}$ — длина i -го паттерна;

$N_{\text{пат}}$ — количество паттернов в списке шаблонов, приводящих к необнаруженным трансформациям.

Для рассмотренного на рис. 5 случая количество необнаруженных трансформаций определяется суммой количества паттернов (2) и количества символов «0» справа от паттернов 1 и 2 (31 и 15), т.е.

$$N_{\text{нт}} = 2 + 31 + 15 = 48.$$

Таким образом, предложенный алгоритм сокращенного перебора позволяет кратно уменьшить ресурсоемкость и время расчета количества необнаруженных трансформаций циклического кода по сравнению с алгоритмом полного перебора. 

Литература

1. ГОСТ 33896-2016. Системы диспетчерской централизации и диспетчерского контроля движения поездов. Требования безопасности и методы контроля = centralized traffic and dispatching control systems of trains movement. Safety requirements and methods of checking : национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 31 марта 2017 г. № 235-ст.: введен впервые : дата введения 2017-11-01. - Москва : Стандартинформ, 2019. - 11 с. - Текст : непосредственный.
2. Горелик, А. В. Технологическая эффективность процесса проектирования систем железнодорожной автоматики и телемеханики : специальность 05.22.08. «Управление процессами перевозок» : диссертация на соискание ученой степени доктора технических наук / Горелик Александр Владимирович. - Москва, 2005. - 384 с. - Текст : непосредственный.
3. Системы диспетчерской централизации : учебник / Д. В. Гавзов, О. К. Дрейман, В. А. Кононов, А. Б. Никитин. - Москва : Издательство «Маршрут», 2002. - 407 с. - 5-89035-074-9. - Текст : электронный // УМЦ ЖДТ: электронная библиотека. - URL: <https://umczdt.ru/books/1196/225875/> (дата обращения: 18.12.2024). - Режим доступа: по подписке.
4. Шубинский, И. Б. Функциональная надежность информационных систем: методы анализа / И. Б. Шубинский. - Москва : Журнал «Надежность», 2012. - 295 с. - Текст : непосредственный.
5. ГОСТ Р 59263-2020. Системы и устройства железнодорожной автоматики и телемеханики микропроцессорные. Требования к интерфейсам и протоколам обмена информацией = Microprocessor systems and devices of railway automatics and telemechanics. Requirements for interfaces and information exchange protocols: национальный стандарт Российской Федерации : издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2020 г. № 1317-ст.: введен впервые: дата введения 2021-06-01. - Москва : Стандартинформ, 2020. - 11 с. - Текст : непосредственный.
6. Richard Ernest Bellman; Rand Corporation. Dynamic programming. - Princeton University Press, 1957. - ISBN 978-0-691-07951-6.