УДК 004.052.42

Самофалов К. Г., чл.-кор. НАН Украины,
Али Тауфик Окла Аль-Хавальди,
Лазученков Д. В.

ОПТИМИЗАЦИЯ КОДИРОВАНИЯ КОНТРОЛЬНЫХ СУММ ПРИ ПЕРЕДАЧЕ И ХРАНЕНИИ ЦИФРОВОЙ ИНФОРМАЦИИ

Национальный технический университет Украины «КПИ»

В статье предложен новый подход к повышению эффективности обнаружения ошибок передачи данных с использованием контрольной суммы путем оптимизации ее кодирования на основе специальных дифференциальных булевых преобразований. Разработаны два способа получения таких преобразований, приведены примеры функций кодирования контрольной суммы.

Введение

Современный этап развития компьютерных и сетевых технологий неразрывно связан с проблемой обеспечения надежности передачи и хранения данных. Динамичное расширение использования потенциально подверженным помехам эфирных каналов связи и сложных методов уплотнения передаваемой информации сопряжено с увеличением числа возникающих ошибок передачи данных. Сходная ситуация имеет место и при хранении данных на магнитных носителях: постоянный рост продольной и поперечной плотности хранения информации на таких носителях также сопряжен с увеличением числа возникающих ошибок [2].

Вместе с тем, расширяющееся использование информационных технологий во всех областях человеческой деятельности, в том числе и сферах, сопряженных с техногенным риском, требуют адекватного повышения надежности всех составляющих компьютерных систем, в том числе, надежности передачи и хранения информации [3].

Непрерывный рост скоростей передачи цифровых данных в современных телекоммутационных системах диктует жесткие требования к производительности средств контроля ошибок: она должна быть соизмеримой с пропускной способностью канала. Это обстоятельство определяет необходимость радикального повышения надежности средств контроля ошибок, обладающих повышенным быстродействием и допускающих распараллеливание при реализации аппаратными средствами.

Таким образом, особенности современного этапа развития и использования компьютерных технологий обуславливают актуальность и практическую важность разработки новых и совершенствования известных средств обеспечения надежности передачи и хранения данных в компьютерных системах и сетях.

Анализ современного состояния проблем обнаружения ошибок передачи и хранения цифровой информации

Для обеспечения надежной передачи данных по каналам связи компьютерных сетей используется широкий спектр средств, важное место среди которых занимает избыточное кодирование передаваемой информации. В большинстве систем, передача и хранение информации выполняется блоками: соответственно отдельно контролируется правильность передачи или хранения каждого блока.

При использовании специального кодирования можно выделить два подхода к исправлению возникающих ошибок:

- обнаружение ошибок специальными кодами и их исправление за счет повторной передачи блока, запрос на которую выдается автоматически при обна-

ружении ошибки (*ARQ – Automatic Repeat Request*);

- исправление возникающих ошибок за счет применения корректирующих кодов без повторной передачи (*FEC – forward error correction*).

Очевидно, что первый из упомянутых подходов неприменим для исправления ошибок хранения данных. Главное преимущество *ARQ* перед схемами прямого исправления ошибки *FEC* заключается в том, что обнаружение ошибок требует более простого декодирующего оборудования и меньшей избыточности, чем коррекция ошибок. Реализация обнаружения ошибок обладает существенно меньшей вычислительной сложностью, что позволяет выполнять функции контроля ошибок значительно быстрее. Кроме того, эффективность *ARQ* меньше зависит от кратности возникающих ошибок.

Выбор того или иного подхода к устранению возникающих ошибок зависит от интенсивности и характера возникающих ошибок. Основными источниками ошибок в цифровых каналах передачи данных являются межбитовая интерференция, внешние помехи и тепловой шум проводящей среды [2]. Характер возникающих ошибок зависит не только от источника, но также и от типа проводящей среды и метода модуляции сигналов. Так, в эфирных каналах связи доминирующим источником ошибок передачи являются внешние помехи, при этом интенсивность возникающих ошибок достаточно высока, так, что применение технологий *FEC* оказывается более предпочтительным. В проводных системах цифровой передачи данных, в которых интенсивность ошибок на несколько порядков ниже по сравнению с эфирными, более эффективным является использование ARQ [5]. В проводных каналах с последовательной передачей без использования модуляции, ошибки передачи носят одиночный характер, а сами каналы достаточно хорошо соответствуют модели двоичного симметричного канала. Такая модель предполагает появление ошибочной передачи нуля или единицы равновероятными, причем вероятность p_j, того, что при передаче n-разрядного кода произойдет j ошибок определяется для двоичного симметричного канала выражением:

$$p_m = \binom{n}{j} \cdot p^j \cdot (1-p)^{n-j}, \qquad (1)$$

где p – вероятность ошибочной передачи одного бита.

Для обнаружения ошибок при поблочной передаче данных наиболее часто используются циклические избыточные коды (*CRC – Cyclic Redundancy Codes*) и контрольные суммы (*CS – Check sums*) [2]. Последние по сравнению с *CRC* существенно проще и обеспечивает наибольшую скорость контроля ошибок, что является весомым фактором в условиях постоянного роста пропускной способности каналов передачи данных. В отличие от CRC, структура операций, выполняемых при вычислении контрольной суммы допускает широкое распараллеливание, что позволяет эффективно реализовать такой контроль аппаратными средствами, так, что время, затрачиваемое на выполнение контроля ошибок, практически не будет сказываться на производительности передачи данных.

Обозначим через $D_1,D_2,\ldots,D_k$ k n-разрядных кодов, составляющих передаваемый блок, а через $D_1',D_2',\ldots,D_k'$ – блок на приемнике. Контрольные суммы на приемнике и передатчике вычисляются одинаково: $S_S = D_1 \oplus D_2 \oplus \ldots \oplus D_k$ и $S_R = D_1' \oplus D_2' \oplus \ldots \oplus D_k'$.

Обычная контрольная сумма предполагает, что передача данных выполняется в виде блока, организованного в виде k n-разрядных кодов: $D_1,D_2,\ldots,D_k$. Разрядность n кода при этом определяется структурной организацией контроля, ее значение может совпадать с числом одновременно передаваемых бит, а может и отличаться от нее. По окончании пересылки блока данных, передатчик пересылает приемнику контрольную сумму S_S,

которая суммируется по модулю 2 с контрольной суммой, вычисленной на приемнике S_R, с получением n-разрядного кода дифференциала $\Delta=S_S \oplus S_R$. Если $\Delta=0$, то считается, что ошибка не возникла. Для симметричного двоичного канала и, при имеющем месте на практике соотношении $k >> n$, можно считать, что при передаче одного кода может возникнуть только одна ошибка.

Основным недостатком контрольной суммы является относительно низкая надежность обнаружения ошибок четной кратности. Действительно, при возникновении наиболее вероятной из них, двукратной ошибки, код Δ может принимать только n^2 различных значений из 2^n возможных, то есть, для рассматриваемой модели канала, обычная контрольная сумма неэффективно их кодирует. Вероятность P_2 необнаружения двукратной ошибки определяется формулой [2]:

$$P_2 = \frac{1}{n}. \qquad (2)$$

Таким образом, уровень надежности обнаружения ошибок при использовании контрольной суммы может быть повышен за счет оптимизации кодирования, то есть вычисления контрольных сумм на передатчике и приемнике в виде:
$S_S = F(D_1) \oplus F(D_2) \oplus \ldots \oplus F(D_k)$ и $S_R = F(D_1') \oplus F(D_2') \oplus \ldots \oplus F(D_k')$, где F – функция кодирования, задаваемая в виде системы булевых функций. В работе [1] в качестве функции кодирования было предложено использовать ортогональную систему булевых функций, удовлетворяющих критерию строго лавинного эффекта. При этом, при возникновении двукратной ошибки, код Δ принимает $n!/((n/2)!)^2$ различных значений и, соответственно, вероятность необнаружения двукратной ошибки существенно уменьшается в сравнении с обычной контрольной суммой. Однако при этом число вариантов – $n!/((n/2)!)^2$ кодирования двукратной ошибки существенно меньше возможного числа кодов Δ – 2^n, а значит, и в этом случае, не достигается оптимизации кодирования. Следовательно, повышение надежности обнаружения ошибок доминирующего типа контрольной суммой может быть достигнуто за счет дальнейшей оптимизации ее кодирования путем выбора соответствующего функционального преобразования.

Целью работы является повышение надежности контроля ошибок с использованием контрольной суммы за счет разработки функциональных преобразований, оптимизирующих ее кодирование для доминирующих видов ошибок в двоичном симметричном канале.

Оптимизация кодирования контрольной суммы

В качестве способа практической реализации оптимизации кодирования контрольной суммы с учетом доминирующего типа возникающих ошибок предлагается вычисление модифицированной контрольной суммы, подобно тому, как это выполнено в работе [1]. При этом в качестве слагаемых предлагается использовать коды, полученные в результате булевых преобразований над контролируемыми кодами, которые представляют собой систему m булевых функций от n переменных:

$$F(D) = \{f_1(D), f_2(D), \ldots, f_m(D)\}, \qquad (3)$$

где D – n-разрядный код: $D=\{d_1,d_2,\ldots,d_n\}$, $\forall j \in \{1,\ldots,n\}$: $d_j \in \{0,1\}$. При возникновении однократной ошибки в j-том разряде кода D_i, последний трансформируется в $D_i'=\{d_1,\ldots,d_j \oplus 1,\ldots,d_n\}$ и дифференциал Δ контрольной суммы может быть представлен в виде набора значений дифференциалов функций $f_1,f_2,\ldots,f_m$ по переменной d_j на двоичном наборе $\{d_1,d_2,\ldots,d_{j-1}, d_{j+1},\ldots,d_n\}$:

$$\Delta = F(D_i) \oplus F(D_i') =$$
$$\{f_1(D_i) \oplus f_1(D_i'), \ldots, f_m(D_i) \oplus f_m(D_i')\} = \qquad (4)$$
$$= \{\frac{\partial f_1}{\partial d_j}, \frac{\partial f_2}{\partial d_j}, \ldots, \frac{\partial f_m}{\partial d_j}\}.$$

Оптимизация кодирования одиночной ошибки в модифицированной m-раз-

рядной контрольной суммы может быть достигнута, если число возможных значений кода Δ составит 2^m. Поскольку число вариантов локализации одиночной ошибки в коде D равно n, то для того, чтобы одиночная ошибка могла быть однозначно кодирована контрольной суммой достаточно, чтобы $m = \lceil \log_2 n \rceil$. При этом, двоичный код, образованный изменением функций при возникновении ошибки в j–м разряде кода D, то есть при изменении переменной d_j равен j-1:

$$\forall j \in \{1,...,n\}: \sum_{t=0}^{\lceil \log_2 n \rceil - 1} \frac{\partial f_t}{\partial d_j} \cdot 2^t = j-1. \quad (5)$$

Очевидно, что условие (5) выполняется, если каждая из функций $f_1,f_2,\ldots,f_m$ линейна и q–тая функция f_q включает переменную d_j тогда, когда q–тая цифра двоичного представления числа j-1 равна единице. Например, если n=8, то m=3 и система функций, удовлетворяющих (5) может иметь такой вид:

$$\begin{aligned} f_1 &= d_2 \oplus d_4 \oplus d_6 \oplus d_8, \\ f_2 &= d_3 \oplus d_4 \oplus d_7 \oplus d_8, \\ f_3 &= d_5 \oplus d_6 \oplus d_7 \oplus d_8. \end{aligned} \quad (6)$$

Число разрядов контрольной суммы в рассмотренном варианте ее кодирования существенно меньше разрядности кода D: $m<n$, однако вероятность, того, что ошибка любой кратности, большей единицы (однократные ошибки обнаруживаются всегда) соответствует выражению (2). Например, двукратная ошибка не обнаруживается только в том случае, если обе ошибки произошли в одном и том же разряде.

Для того, чтобы уменьшить вероятность того, что многократная ошибка не будет обнаружена, необходимо, в дополнение к системе функций (5), образующих множество Ξ_1 использовать систему из u функций, составляющих множество Ξ_2, так, что $F=\{\Xi_1, \Xi_2\}$.

Для того, чтобы с высокой надежностью обнаруживать двукратную ошибку, необходимо выполнение ряда условий. Поскольку две ошибки, локализованные в разных разрядах передаваемых кодов всегда обнаруживается с использованием функций множества Ξ_1, то для того, чтобы обнаруживались ошибки, происходящие в одном и том же разряде разных кодов блока, необходимо, чтобы вероятность совпадения значений дифференциалов функций, составляющих множество Ξ_2 при изменении одной переменной была возможно меньшей или даже сводилась к нулю. Для этого дифференциалы функций этого множества не должны быть равны константе, то есть функции должны быть нелинейными, причем дифференциалы функций $f_{m+1},f_{m+2},\ldots,f_{m+u}$, по любой из переменных должны представлять собой ортогональную систему функций.

Для реализации этого условия предлагается два способа выбора функций множества Ξ_2.

В соответствии с первым из них, функции $f_{m+1},f_{m+2},\ldots,f_{m+u}$ определены на множестве n переменных, совпадающих со значениями разрядов передаваемых кодов, множество их возможных значений образует множество Z. В этом случае, число функций множества Ξ_2 равно n-1, то есть $u=n$-1, а сами функции $f_{m+1},f_{m+2},\ldots,f_{m+u}$ должны удовлетворять условию:

$$\forall j \in \{1,..., n\}, a_t \in \{0,1\}:$$
$$\sum_{D \in Z} \bigoplus_{t=1}^{u} a_t \cdot \frac{\partial f_{m+t}}{\partial d_j} = 2^{u-1}. \quad (7)$$

Ниже приведен пример системы из 7-ми булевых функций от 8-ми переменных (n=8), составляющих множество Ξ_2 и удовлетворяющих условию (7):

$$\begin{aligned} f_4 &= d_1 \cdot d_2 \oplus d_3 \cdot d_4 \oplus d_5 \cdot d_7 \oplus d_6 \cdot d_8, \\ f_5 &= d_1 \cdot d_3 \oplus d_2 \cdot d_4 \oplus d_5 \cdot d_8 \oplus d_6 \cdot d_7, \\ f_6 &= d_1 \cdot d_4 \oplus d_2 \cdot d_5 \oplus d_3 \cdot d_6 \oplus d_7 \cdot d_8, \\ f_7 &= d_1 \cdot d_5 \oplus d_2 \cdot d_6 \oplus d_3 \cdot d_7 \oplus d_4 \cdot d_8, \\ f_8 &= d_1 \cdot d_6 \oplus d_2 \cdot d_7 \oplus d_3 \cdot d_8 \oplus d_4 \cdot d_5, \\ f_9 &= d_1 \cdot d_7 \oplus d_2 \cdot d_8 \oplus d_3 \cdot d_5 \oplus d_4 \cdot d_6, \\ f_{10} &= d_1 \cdot d_8 \oplus d_2 \cdot d_3 \oplus d_4 \cdot d_7 \oplus d_5 \cdot d_6. \end{aligned} \quad (8)$$

Дифференциалы по любой из 8-ми переменных приведенных 7-ми функций,

составляющих множество Ξ_2, образуют систему ортогональных булевых функций. Например, дифференциалы по 4-й переменной d_4 образуют систему линейных функций, свойство ортогональности которой вполне очевидно:

$$\frac{\partial f_4}{\partial d_4} = d_3; \frac{\partial f_5}{\partial d_4} = d_2; \frac{\partial f_6}{\partial d_4} = d_1; \frac{\partial f_7}{\partial d_4} = d_8;$$

$$\frac{\partial f_8}{\partial d_4} = d_5; \frac{\partial f_9}{\partial d_4} = d_6; \frac{\partial f_{10}}{\partial d_4} = d_7.$$

Дифференциалы функций f_1, f_2, f_3 по переменной d_4 равны $\frac{\partial f_1}{\partial d_4} = 1; \frac{\partial f_2}{\partial d_4} = 1;$ $\frac{\partial f_3}{\partial d_4} = 0$ и соответствуют номеру переменной x_4: j–$1=011_2=3$

Выполнение условия (7) обеспечивает обнаружение двух ошибок, если они происходят в одинаковых разрядах различных кодов. То есть двукратная ошибка не будет обнаружена только в том случае, если обе ошибки произойдут в одном и том же разряде j при передаче двух кодов D_i и D_e, $i,e \in \{1,\ldots,k\}$, которые либо равны между собой, либо отличаются только j-тым разрядом. Вероятность этого определяется формулой:

$$p_2 = \frac{1}{2^{n-1} \cdot n}. \qquad (9)$$

Очевидно, что формула (9) определяет вероятность необнаружения не только двукратной, но и ошибки любой кратности, большей единицы. Сравнение с выражением (2) показывает, что надежность обнаружения двукратной ошибки существенно увеличена по сравнению с обычной контрольной суммой.

Таким образом, сущность первого из предложенных способов оптимизации кодирования контрольной суммы состоит в том, что функции преобразования компонент суммы множества Ξ_2 выбираются таким образом, чтобы их дифференциалы по любой из переменных зависели от кода D. Двукратная ошибка не будет обнаружена только в том случае, если обе ошибки произойдут в одном и том же разряде пары одинаковых кодов, либо пары кодов, отличных только в этом разряде. Если считать, появление каждого из n–разрядных кодов в блоке равновероятным, то вероятность двукратной ошибки, для которой выполняются эти условия определяется формулой (9). Однако на практике весьма частой является ситуация, когда некоторые коды в блоке повторяются достаточно часто. Такая ситуация характерна для текстовых документов и для изображений. Соответственно, в этом случае, эффективность предложенного способа кодирования компонент контрольной суммы уменьшается.

Второй способ кодирования компонент контрольной суммы лишен этого недостатка и состоит в том, что функции $f_{m+1}, f_{m+2}, \ldots, f_{m+u}$ множества Ξ_2 выбираются таким образом, чтобы их дифференциалы по любой из переменных зависели от номера H кода в блоке. Если контролируемый блок включает в себя k кодов, то число w двоичных разрядов H составляет $w = \lceil \log_2 k \rceil$, соответственно, u=w. В этом случае, функции $f_{m+1}, f_{m+2}, \ldots, f_{m+w}$ определены на множестве $n+w$ переменных, которое включает n разрядов передаваемых кодов $d_1, d_2, \ldots, d_n$ и w разрядов номера передаваемых кодов в блоке $h_1, h_2, \ldots, h_w$. Для оптимального, с точки зрения обнаружения ошибок, кодирования компонент контрольной суммы, булевы функции $f_{m+1}, f_{m+2}, \ldots, f_{m+u}$ должны выбираться таким образом, чтобы их дифференциалы по любой из переменных $d_1, d_2, \ldots, d_n$ образовывали ортогональную систему функций от переменных $h_1, h_2, \ldots, h_w$, которые могут принимать 2^w значений, образующих множество Q. В частном случае, дифференциалы системы булевых функций $f_{m+1}, f_{m+2}, \ldots, f_{m+u}$ по любой из переменных $d_1, d_2, \ldots, d_n$ могут представлять собой ортогональные линейные системы от переменных $h_1, h_2, \ldots, h_w$. В этом случае должно выполняться следующее условие:

$$\forall j \in \{1,..., n\}, a_t \in \{0,1\}:$$

$$\sum_{H \in Q} \bigoplus_{t=1}^{w} a_t \cdot \frac{\partial f_{m+t}}{\partial d_j} = 2^{u-1}. \quad (10)$$

Пусть, например, число k кодов в контролируемом блоке равно 64, а разрядность кода равна 8-ми (n=8). Тогда w=u=6, соответственно, номер H кода в блоке состоит из 6-ти двоичных разрядов H={h_1,h_2,…,h_6}. Система булевых функций, составляющих множество Ξ_2 включающая 6 функций, удовлетворяющая условию (10) имеет следующий вид:

$$\begin{aligned} f_4 &= h_1 \cdot (d_1 \oplus d_2 \oplus ... \oplus d_8), \\ f_5 &= h_2 \cdot (d_1 \oplus d_2 \oplus ... \oplus d_8), \\ f_6 &= h_3 \cdot (d_1 \oplus d_2 \oplus ... \oplus d_8\}, \\ f_7 &= h_4 \cdot (d_1 \oplus d_2 \oplus ... \oplus d_8\}, \\ f_8 &= h_6 \cdot (d_1 \oplus d_2 \oplus ... \oplus d_8), \\ f_9 &= h_6 \cdot (d_1 \oplus d_2 \oplus ... \oplus d_8). \end{aligned} \quad (11)$$

Дифференциалы по любой из 8-ми переменных приведенных 6-ти функций, составляющих множество Ξ_2, образуют систему ортогональных булевых функций. Например, дифференциалы по 4-й переменной d_4 образуют систему линейных функций, свойство ортогональности которой вполне очевидно:

$$\frac{\partial f_4}{\partial d_4} = h_1; \frac{\partial f_5}{\partial d_4} = h_2; \frac{\partial f_6}{\partial d_4} = h_3;$$

$$\frac{\partial f_7}{\partial d_4} = h_4; \frac{\partial f_8}{\partial d_4} = h_5; \frac{\partial f_9}{\partial d_4} = h_6.$$

Это обеспечивает оптимальность кодирования ошибки при каждом фиксированном разряде, в котором она произошла, то есть однозначную зависимость кода ошибки от номера передаваемого кода в блоке.

При возникновении двукратной ошибки в различных кодах, дифференциалы функций f_{m+1},f_{m+2},…,f_{m+u} будут различны, а следовательно $\Delta \neq 0$. При возникновении двукратной ошибки в одном коде, дифференциалы функций f_1,f_2,…,f_m будут различными, а значит, $\Delta \neq 0$. Таким образом, второй из предложенных способов оптимизации кодирования контрольной суммы обеспечивает выявление всех одно и двукратных ошибок, то есть доминирующих ошибок для симметричных двоичных каналов. Вероятность P_3 того, что ошибки большей кратности не будут обнаружены при предлагаемом способе кодирования определяется формулой:

$$P_3 = \frac{1}{k \cdot n}. \quad (12)$$

Сравнение выражений (9) и (12) показывает, что использование второго способа кодирования контрольной суммы предпочтительнее при большом количестве кодов в блоках. По сравнению с обычной контрольной суммой, повышение надежности обнаружения ошибок четной кратности при использовании предлагаемого способа кодирования, составляет несколько порядков. По сравнению с использованием лавинных преобразователей [2], надежность обнаружения многократных ошибок увеличивается в t_1 раз при использовании первого из предложенных способов и в t_2 раз – при использовании второго. При этом численные значения и определяются выражениями:

$$\begin{aligned} t_1 &= \frac{2^{n-1} \cdot ((n/2)!)^2}{(n-1)!}, \\ t_2 &= \frac{k \cdot ((n/2)!)^2}{(n-1)!}. \end{aligned} \quad (13)$$

Анализ значений формул (13) для наиболее часто встречаемых на практике значений k и n показывает, что надежность обнаружения многократных ошибок увеличивается в десятки раз по сравнению с использованием лавинных преобразований [1].

Вычисления, реализующие функциональные преобразования (6), (8), (11) намного проще операций деления полиномов, выполняемых в *CRC*, и допускают многоуровневое распараллеливание. Так, при аппаратной реализации, одновременно могут вычисляться логические произведения функций (8), сами функции систем (6) и (8), (11) также могут вычисляться параллельно. Это позволяет обес-

печить высокую скорость реализации операций контроля, недостижимую при использовании *CRC*, и эффективно реализовать функции обнаружения ошибок без задержки в работе перспективных высокоскоростных каналов передачи цифровой информации.

Выводы

Предложен подход к повышению эффективности обнаружению ошибок при передаче и хранении данных с использованием контрольных сумм, который основан на оптимизации ее кодирования. Это позволяет существенно снизить вероятность взаимного маскирования ошибок при их четной кратности как по сравнению с обычной контрольной суммой, так и по сравнению с использованием лавинных преобразований для кодирования ее компонент [1].

Разработано два способа получения специальных дифференциальных булевых функциональных преобразований, оптимизирующих кодирование контрольной суммы блока кодов с точки зрения критерия обнаружения ошибок, доминирующих в двоичном симметричном канале. Приведены примеры преобразований, оптимизирующих кодирование контрольной суммы для обоих предложенных способов. Теоретически обоснованы оценки вероятности обнаружения ошибок различной кратности. Доказано, что при кодировании компонент контрольной суммы с использованием функций, зависящих как от передаваемых кодов, так и от номера кода в блоке, будут обнаружены все ошибки кратности меньше 3-х.

Проведенный анализ показал, что использование предложенного подхода позволяет снизить вероятность необнаружения многократных ошибок на несколько порядков по сравнению с известными схемами вычисления контрольной суммы.

Структура функциональный преобразований значительно проще, по сравнению с преобразованиями CRC, допускает многоуровневое распараллеливание при аппаратной реализации, что позволяет обеспечивать высокую производительность контроля ошибок без внесения задержек в процесс передачи данных.

Разработанный подход может быть использован для реализации эффективного контроля ошибок в перспективных высокоскоростных каналах передачи цифровой информации компьютерных сетей.

Список литературы

1. *Троян О. С.* Применение лавинных преобразований для повышения надежности обнаружения ошибок с использованием контрольных сумм. // Вісник Національного технічного університету «КПІ». Інформатика, управління та обчислювальна техніка. – К.: ВЕК+, 2004. – №41. – С. 141-154.

2. *Klove T., Korzhik V.* Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems. Norwell, MA: Kluwer, 1995. – 433 p.

3. *Saxena N. R., McCluskey E. J.* Extended precision checksums. // Proc.17-th Intern. Symp. Fault-Tolerant Comput. : FCTS-17, – Pittsburgrh (USA), 1987. – P. 142-147.