УДК 004.9:623+004.056.53](083.73)
ББК 32.973
Ф 91

Фролов Александр Дмитриевич
Соискатель Краснодарского высшего военного училища им. генерала армии С.М. Штеменко, Краснодар, e-mail: idfrolov@yandex.ru

Методика выбора циклического кода для резервирования параллельных каналов связи

(Рецензирована)

Аннотация. *Показано, что для критически важных информационных систем эффективными являются системы с решающей обратной связью. В таких системах, наряду с высокой достоверностью, выбранный код должен обеспечить и высокую скорость передачи информации, что является необходимым условием оптимальности выбранного кода. Высокую достоверность обеспечивают коды, обладающие хорошей обнаруживающей и исправляющей способностью. Данная работа посвящена выбору оптимального корректирующего кода для систем передачи информации по параллельным каналам связи с решающей обратной связью. Разработана методика выбора циклического кода для резервированных параллельных каналов связи, удовлетворяющих заданным требованиям по быстродействию и достоверности, отличавшаяся от известных сокращением расчетов. Приведены результаты численных исследований.*

Ключевые слова: *оперативность, достоверность, критически важные информационные системы, система с решающей обратной связью, циклические коды.*

Frolov Aleksandr Dmitrievich
Competitor of General S.M. Shtemenko Krasnodar Higher Military School, Krasnodar, e-mail: id-frolov@yandex.ru

Cyclic code selection method for reservation of parallel channels of communication

Abstract. *It is shown that for mission-critical information systems, effective are decision feedback systems. In such systems the selected code must provide both high reliability and high data transfer rate, which is a necessary condition for optimality of the selected code. Codes having a good ability to detect and correct are able to provide high reliability. This work is devoted to the choice of optimal correction code for systems relaying information over parallel communication channels with decision feedback. The paper develops the technique of cyclic code selection for redundant parallel communication channels that satisfy given requirements of speed and reliability, differing from the known ones in calculation reductions. The results of numerical studies are given.*

Keywords: *efficiency, reliability, mission-critical information systems, system with decision feedback, cyclic codes.*

Введение

Анализ современных войн, локальных конфликтов и контртеррористических операций со всей убедительностью демонстрирует повышение значимости информационной составляющей вооруженной борьбы. Именно стремление к информационному превосходству породило ведение военных действий в информационном пространстве на основе анализа и принятия решений в реальном масштабе времени. Критически важные информационные системы (КВИС) представляют особый интерес для массированных информационных атак. Кроме того, за последние годы наблюдается устойчивая тенденция роста потока криптограмм. Если в мирное время задержка прохождения конфиденциальной информации может привести к простой дестабилизации функционирования военных объектов, то в ходе боевых действий это будет связано со срывом выполнения стратегических или тактических боевых задач, что является недопустимым.

Таким образом, необходимость повышения надежности управления войсками и оружием и обеспечение его непрерывности, оперативности и достоверности в любых условиях обстановки обусловлены современными принципами ведения боевых действий и потребностями перехода к инновационным системам КВИС. При традиционных методах обработки криптограмм нормативную пропускную способность спецоргана можно сохранить при возрастании нагрузки только за счет привлечения дополнительных материальных и человеческих ресурсов. Однако такими методами можно решить лишь частную задачу обеспечения

командования ВС РФ оперативной связью на данном конкретном учении, а проблема обеспечения надежности, оперативности и достоверности системы КВИС оперативно-стратегического управления в информационном пространстве остается открытой.

Таким образом, традиционные методы обеспечения нормативной пропускной способности себя полностью исчерпали. Кроме того, в условиях радиоэлектронной борьбы при использовании системы с решающей обратной связью (РОС) следует ожидать снижения оперативности передачи криптограмм за счет увеличения простоя аппаратуры в режиме «запроса». Для снижения простоя аппаратуры в режиме «запроса» следует повышать достоверность передачи криптограмм, например, за счет эффективного использования циклических кодов. В известных работах вопросы повышения достоверности криптограмм с эффективным использованием циклических кодов не рассматривались, что является одним из недостатков известных сетевых методов передачи криптограмм с использованием РОС при работе по параллельным каналам с резервированием.

Известно [1], что вероятность ошибок в каналах передачи данных находится в пределах от 10^{-2} до 10^{-4} соответственно при группировании ошибок порядка: $\alpha = 0{,}35$; $\alpha = 0{,}4$; $\alpha = 0{,}55$, а достоверность передачи данных, передаваемых по таким каналам связи в критически важных информационных системах, должна быть не менее вероятности правильного приема. Такую достоверность можно обеспечить путем выбора корректирующего кода в системе передачи информации по параллельным каналам связи с РОС. Известно, что к таким кодам относятся циклические коды, аппаратурная сложность которых по сравнению с другими кодами имеет преимущества с точки зрения простоты реализации и стоимости. Известные методы выбора циклических кодов по заданному значению минимального кодового расстояния и длины кодовой комбинации не всегда обеспечивают оптимальность кода, под которым понимают гарантированное обеспечение выбранным кодом заданных значений достоверности скорости передачи криптограмм.

Целью работы является повышение оперативности и достоверности передачи информации путем разработки методики выбора циклического кода для резервированных параллельных каналов связи.

Основная часть

Известно [2], что эффективность систем с решающей обратной связью определяется заданной достоверностью и скоростью работы системы.

Достоверность обеспечивается допустимой вероятностью ошибочного приема кодовой комбинации из ξ элементов исходного первичного кода $P_{ош}(\geq 1, \xi)$ на выходе системы. Данная вероятность зависит от вероятности ошибки в канале связи P выбранного корректирующего кода и логики работы системы и может определяться соотношением [2]:

$$P_{ош}(\geq 1, \xi) = \frac{B_{ош}(\xi)}{B_{пр}(\xi) + B_{ош}(\xi)},$$

где $B_{ош}(\xi)$ – число ошибочных комбинаций, выданных потребителю, за достаточно большое время;

$B_{пр}(\xi)$ – число ξ элементных комбинаций, выданных потребителю без ошибок, за достаточно большое время работы.

Достоверность системы всегда указывается при проектировании в виде заданной вероятности ошибочного приема кодовой комбинации $P_{зад}(\geq 1, \xi)$, которая должна быть обеспечена при допустимых параметрах канала связи. Обеспечение заданной величины $P_{зад}(\geq 1, \xi)$ достигается выбором корректирующего кода.

Также важным параметром системы с РОС является скорость передачи информации, которая определяется как отношение числа двоичных символов, выданных приемником потребителю, к общему числу двоичных символов, переданных в канал связи. Скорость пере-

дачи информации зависит от коэффициента передачи кода $R=\frac{k}{n}$, качества канала связи и логики работы системы. Поэтому для скорости передачи информации в системах с РОС можем записать:

$$R'=\frac{k}{n}\cdot r. \quad (1)$$

То есть сомножитель $\frac{k}{n}$ определяется выбранными параметрами циклического кода, а второй сомножитель r зависит как от параметров кода, так и от характеристик канала связи. Он определяет избыточность, которая вводится системой за счет повторения принятых с ошибками комбинаций при $n\to\infty$, $r\to 0$.

Таким образом, скорость передачи R' при заданной вероятности ошибки в канале P и коэффициенте группирования ошибок в канале α будет иметь максимальное значение при определенной длине кодовой комбинации, которая будет равна $n=n_{опт}$. Оптимальную длину кодовой комбинации $n_{опт}$ можно найти, приравняв первую производную скорости по длине комбинации к нулю: $\frac{dR}{dn}=0$. Эффективность системы с РОС оценивается по критерию максимума скорости передачи при сохранении заданной достоверности передачи. Оптимальной считается такая система с РОС, которая при заданной вероятности ошибки $P_{зад}(\geq 1,\xi)$ обеспечивает максимальную скорость передачи информации по каналу связи [2]:

$$R'=R_{мах}, \qquad P_{ош}(\geq 1,\xi)\leq P_{зад}(\xi). \quad (2)$$

С другой стороны, для вероятности обнаружения ошибок циклическим кодом справедлива оценка:

$$P_{ош}(\geq 1,\xi)\leq P_{ош}(n)\approx\frac{1}{2^{n-k}}\left(\frac{n}{d}\right)^{1-\alpha}\cdot P. \quad (3)$$

Необходимо рассчитать параметры кода такие, как: скорость кода, скорость передачи по каналу при заданной емкости повторителя и условии, когда обратный канал идеальный и когда он имеет такие же параметры, как и прямой канал, для того, чтобы выбранный циклический код удовлетворял заданным требованиям. Затем следует оптимизировать параметры найденного кода. По найденным параметрам циклического кода из таблиц циклических кодов выбрать порождающий многочлен.

Таким образом, алгоритм метода выбора оптимального циклического кода, удовлетворяющего заданным требованиям, складывается из следующих шагов.

На первом шаге определяется максимальное значение скорости кода $\frac{k}{n}$, при котором обеспечивается заданная вероятность $P_{зад}(\geq 1,\xi)$. Для этого по формуле (3) рассчитываются значения вероятности ошибок $P_{ош}(\geq 1,\xi)$ для выбранных длин кодовых комбинаций $n=2^m-1$ с различными значениями показателя степени m. Результаты расчетов сводятся в таблицу и по данным таблицы строятся графики зависимости вероятности ошибок от скорости передачи кода $P(\geq 1,\xi)=f\left(\frac{k}{n}\right)$ для каждого из трех каналов. Одновременно на этих же графиках проводится линия заданного значения вероятности ошибок $P_{зад}(\geq 1,\xi)$. Точки пересечения линии заданных значений вероятности ошибки $P_{зад}(\geq 1,\xi)$ с расчетными кривыми вероятности ошибок $P(\geq 1,\xi)$ для каждого из выбранных кодов с длиной комбинации n определяют максимальные значения скорости передачи кода $\frac{k}{n}$, при которых обеспечива-

ется заданное значение вероятности ошибки $P_{зад}(\geq 1,\xi)$. Найденные таким образом значения скорости передачи кода $\frac{k}{n}$ для удобства сводятся в отдельную сводную таблицу.

На втором шаге производится расчет сомножителя, определяющего скорость передачи по каналу r_1 – в предположении, что обратный канал идеальный и r – в предположении, что обратный канал имеет такие же параметры по вероятности ошибки P и группированию ошибок α, как и прямой канал. Расчеты указанных сомножителей производятся по приведенным ниже формулам при заданной емкости повторителя h.

$$r_1 = (1-P)^{(nh)^{1-\alpha}}, \quad r = \frac{r_1}{2-r_1} \tag{4}$$

Результаты расчетов сводятся в таблицу. Конечные результаты расчета из данной таблицы для удобства опять переносятся в отдельную сводную таблицу. По данным сводной таблицы для каждого канала строятся графики зависимости скорости передачи кода от длины кодовой комбинации: $\frac{k}{n} = f(n)$, $r_1 = f(n)$, $r = f(n)$.

На третьем шаге осуществляется расчет непосредственно скорости передачи системы R_1 и R, соответственно для идеального канала обратной связи и когда параметры канала обратной связи идентичны параметрам прямого канала по формулам

$$R_1 = \frac{k}{n}\cdot r_1, \quad R = \frac{k}{n}\cdot r \tag{5}$$

для каждого из трех каналов, которые сводятся в сводную таблицу. По данным сводной таблицы строятся графики зависимости скорости передачи от длины кодовой комбинации.

На четвертом шаге по графикам зависимости скорости передачи от длины кодовой комбинации $R = f(n)$ находятся значения оптимальной длины кодовых комбинаций $n_{опт}$ и оптимальной скорости кода $\frac{k_{опт}}{n_{опт}}$. По найденным значениям $n_{опт}$ и $\frac{k_{опт}}{n_{опт}}$ из таблиц циклических кодов определяется длительность информационных символов $k_{опт}$ для каждого из каналов.

Наконец, ***на последнем пятом этапе*** для выбранного кода с оптимальными параметрами $n_{опт}$ и $k_{опт}$ из таблицы циклических кодов выбираются образующие полиномы и составляется порождающий многочлен $g(x)$.

По формуле (3) вероятность $P_{ош}(\geq 1,\xi)$ для различных параметров кода $n = 2^k - 1$ и заданной вероятности ошибок в канале связи, определяемых коэффициентом группирования α при следующих заданных начальных условиях: $n = 4,5,6,7,8,9,10,11$; $\zeta = 5$; $\alpha = 0{,}35$; $P = 10^{-3}$, $P_{зад}(\geq 1,\xi) \leq 10^{-7}$.

По результатам расчетов, путем построения на одном графике функции $P(\geq 1,\xi) = f\left(\frac{k}{n}\right)$ для заданной вероятности ошибки в канале и параметров кода n, а также прямой линии с заданной вероятностью ошибки $P_{зад}(\geq 1,\xi)$, по точкам пересечения находятся максимальные значения скорости передачи $\frac{k}{n}$. Найденные скорости гарантируют для соответствующих параметров кода заданную вероятность ошибки $P_{зад}(\geq 1,\xi)$. Кроме того, в предположении, что обратный канал – идеальный для емкости повторителя $h = 5$, по формуле $r_1 = (1-P)^{(nh)^{1-\alpha}}$ находится избыточность кода. Также по формуле $r = \frac{r_1}{2-r_1}$ находят избыточность для случая, когда канал обратной связи равноценен прямому. При аналогич-

ных предположениях по формуле (1) рассчитываются скорости передачи системы R_1', R'.

Результаты аналитических и графических расчетов сводятся в таблицу 1, по результатам которой строятся графики $\frac{k}{n} = f(n)$, $r_1 = f(n)$, $r = f(n)$, $R_1 = f(n)$, $R = f(n)$, которые приведены на рисунке 1.

Таблица 1

Результаты расчетов скорости передачи кода, избыточности и скорости передачи системы для различных длин кодовых комбинаций для идеального канала обратной связи и когда параметры канала обратной связи идентичны параметрам прямого канала

Вероятность ошибки в канале	Скорости кода и системы	n				
		15	31	63	127	255
$P_1 = 10^{-3}$ $\alpha = 0{,}35$	k/n	0,1	0,516	0,714	0,835	0,907
	r_1	0,984	0,973	0,959	0,935	0,894
	r	0,968	0,949	0,919	0,870	0,819
	R_1	0,0984	0,503	0,685	0,78	0,81
	R	0,0968	0,490	0,656	0,727	0,743

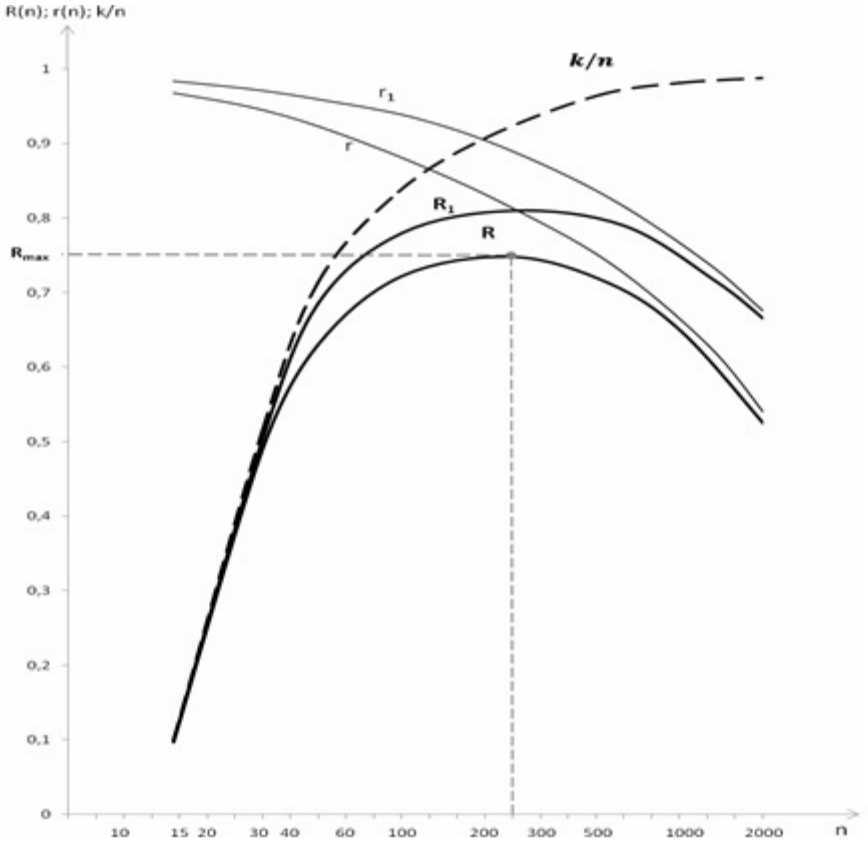

Рис. 1. Зависимость скорости передачи системы от параметров кода

По графикам $R = f(n)$ находится оптимальная длина и скорость передачи кода $n_{опт}$ и $\frac{k_{опт}}{n_{опт}}$. По найденным значениям определяется $k_{опт}$. Из графика рисунка 1 видно, что максимальная скорость $R_{\max} = 0{,}743$ обеспечивается при $n_{\max} = 255$. Для реализации найденных параметров кода на практике уменьшим значение длины кодовой комбинации до $n_{опт} = 127$, которой соответствует скорость передачи кода $\frac{k}{n} = 0{,}835$, тогда число информационных элементов кода будет равно $k = 106$. Учитывая, что длина первичного исходного

кода равна $\zeta = 5$, приводим длину информационных элементов кода кратной пяти, то есть $k = 105$. Таким образом, для найденных значений получаем оптимальный код с параметрами $n_{опт} = 126$, $k_{опт} = 127$, $d_{опт} = 7$. Скорость передачи найденного кода равна $R = 0{,}727$, то есть уменьшилась на незначительную величину $0{,}016$, хотя длина кодовой комбинации была уменьшена в два раза.

Определяем проверку первого условия оптимальности (максимальной скорости передачи) по формуле:

$$n - k \geq (1 - \alpha)\log_2 \xi + \log_2 P - \log_2 P_{зад}(\geq 1, \xi). \quad (6)$$

Подставив в формулу (6) оптимальные параметры кода и заданные значения, получаем:

$$126 - 105 > 0{,}65 \cdot \log_2 5 + \log_2 10^{-3} - \log_2 10^{-7}.$$

Упростив выражение, имеем $21>14{,}815$, следовательно, выбранный код обеспечивает максимальную скорость передачи.

Рассчитаем по формуле (3) вероятность ошибки при использовании найденного кода при заданных характеристиках канала связи и сравним ее с заданной вероятностью ошибки $P = 10^{-7}$:

$$P(\geq 1, \xi) = \frac{1}{2^{21}}\left(\frac{126}{7}\right)^{0{,}65} \cdot 10^{-3} = 6{,}2 \cdot 10^{-8}. \quad (7)$$

Расчеты показали, что вероятность ошибки при выбранных оптимальных параметрах кода не превосходит заданного значения, то есть $6{,}2 \cdot 10^{-8} \geq 10^{-7}$. Следовательно, данный код гарантированно обеспечивает второе условие оптимальности.

По значениям $n_{опт} = 126$ и $k_{опт} = 105$ из табулированных таблиц находятся образующие полиномы и определяется порождающий многочлен $g(x)$:

$$g(x) = \langle 235\rangle\langle 217\rangle\langle 211\rangle = \langle 010011101\rangle\langle 010001111\rangle\langle 010001001\rangle =$$
$$= (1 + x^2 + x^3 + x^4 + x^7)(1 + x^2 + x^3 + x^7)(1 + x^3 + x^7) =$$
$$= 1 + x + x^5 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{14} + x^{15} + x^{17} + x^{18} + x^{21}.$$

Вывод

В условиях применения помех естественной и организованной структуры разработанная методика в отличие от известных позволяет осуществлять выбор корректирующих кодов для системы с решающей обратной связью с оптимальными параметрами как для прямого, так и для обратного каналов связи, что обеспечит требуемую достоверность и оперативность прохождения информации в критически важных информационных системах.

Примечания:

1. Чернуха Ю.В. Разработка методов повышения помехозащищенности криптограмм, передаваемых по каналам низкого качества в условиях информационной борьбы // Отчет по НИР, шифр «Градация»-00009-И. Краснодар: КВИ, 2003. 89 с.
2. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. М.: Связь, 1975. 271 с.

References:

1. Chernukha Yu.V. Development of methods to increase the noise immunity of the cryptograms transmitted through the channels of low quality in terms of information warfare / Report on research work, code “Gradation”-00009-I. Krasnodar: KVI, 2003. 89 pp.
2. Korzhik V.I., Fink L.M. Noiseproof coding of discrete messages in random structure channels. M.: Svyaz, 1975. 271 pp.