УДК 621.391
doi:10.15217/issn1684-8853.2015.2.82

ПОМЕХОУСТОЙЧИВОСТЬ И СКРЫТНОСТЬ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО РАДИОКАНАЛАМ НА ОСНОВЕ КОМБИНИРОВАННОГО СЛУЧАЙНОГО КОДИРОВАНИЯ

Г. Н. Мальцев[a], *доктор техн. наук, профессор*
[a]*Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, РФ*

Цель: *в радиотехнических системах передачи информации методы канального кодирования, как правило, используются для повышения помехоустойчивости передачи информации по радиоканалам. Комбинированное случайное кодирование, являющееся сочетанием помехоустойчивого и стохастического кодирования, позволяет одновременно обеспечить помехоустойчивость и информационную скрытность передачи информации. Цель работы — исследование взаимосвязанных показателей достоверности и защищенности передачи информации по радиоканалам при использовании комбинированного случайного кодирования.* ***Методы:*** *качественный и количественный анализ потенциальной помехоустойчивости и информационной скрытности передачи информации по радиоканалам на основе комбинированного случайного кодирования при различных вариантах выбора параметров кода.* ***Результаты:*** *представлено описание разработанного метода комбинированного случайного кодирования и исследованы показатели достоверности и защищенности передачи информации по радиоканалам при различных сочетаниях числа информационных символов, проверочных символов и символов стохастического кода в кодовой комбинации комбинированного кода. Показана возможность выбора параметров комбинированного кода, одновременно удовлетворяющего требованиям к обоим анализируемым показателям, в том числе при обеспечении помехоустойчивости и информационной скрытности путем «обмена» на них скорости передачи информации.* ***Практическая значимость:*** *представлены рекомендации по выбору вариантов использования комбинированного случайного кодирования для передачи нескольких условно выделенных типов сообщений с различными приоритетами.*

Ключевые слова *— помехоустойчивое кодирование, стохастическое кодирование, достоверность и защищенность передачи сообщений по радиоканалам.*

Введение

В общем случае к системам радиосвязи и радиоуправления предъявляются требования по помехоустойчивости и скрытности передачи информации, являющимся составляющими помехозащищенности системы [1]. При этом скрытностью передачи информации одновременно обеспечивается информационная безопасность системы [2]. Поэтому в общем случае целесообразно использовать комплексный подход к обеспечению требуемого уровня взаимосвязанных показателей качества передачи информации по радиоканалам. В рамках данного подхода в настоящей статье рассматривается метод защищенной передачи информации на основе комбинированного случайного кодирования, который при соответствующем выборе параметров кода может быть использован для повышения как помехоустойчивости, так и информационной скрытности передачи информации.

Описание метода комбинированного случайного кодирования

В существующих радиотехнических системах передачи информации большинство методов повышения помехоустойчивости и информационной безопасности используются независимо друг от друга и не учитывают взаимосвязи помехозащищенности и информационной скрытности. Так, методы помехоустойчивого кодирования, получающие широкое применение в цифровых системах радиосвязи и радиоуправления, выбираются исходя из наихудших условий связи, в результате чего при низком уровне помех передача информации по радиоканалу осуществляется с большой избыточностью [3, 4]. При этом высокая корректирующая способность используемого корректирующего кода позволяет в широком диапазоне условий связи выделять передаваемые сообщения с высокой достоверностью, что объективно создает благоприятные условия для радиоперехвата и несанкционированного доступа к радиоканалу передачи информации и, следовательно, снижает скрытность и информационную безопасность системы.

Метод комбинированного случайного кодирования предполагает использование сочетания помехоустойчивого кодирования и псевдослучайной смены ансамбля используемых кодовых комбинаций — стохастического кодирования информации [5, 6]. При этом высокая достоверность передачи сообщений обеспечивается за счет помехоустойчивого кодирования при выборе параметров корректирующего кода, а информационная скрытность и защищенность от несанкционированного доступа — за счет стохастического кодирования, относящегося к некриптографическим методам защиты информации.

Близость комбинированного случайного кодирования к методам шифрования проявляется в структурных преобразованиях передаваемых и принимаемых сообщений на передающей и приемной сторонах [7]. Вместе с тем при комбинированном случайном кодировании не используются характерные для шифрования алгоритмы и ключи и обеспечивается теоретико-информационный уровень защиты информации, который определяется уровнем неопределенности выбора ансамбля кодовых комбинаций, соответствующих передаваемым сообщениям, для нарушителя, осуществляющего радиоперехват.

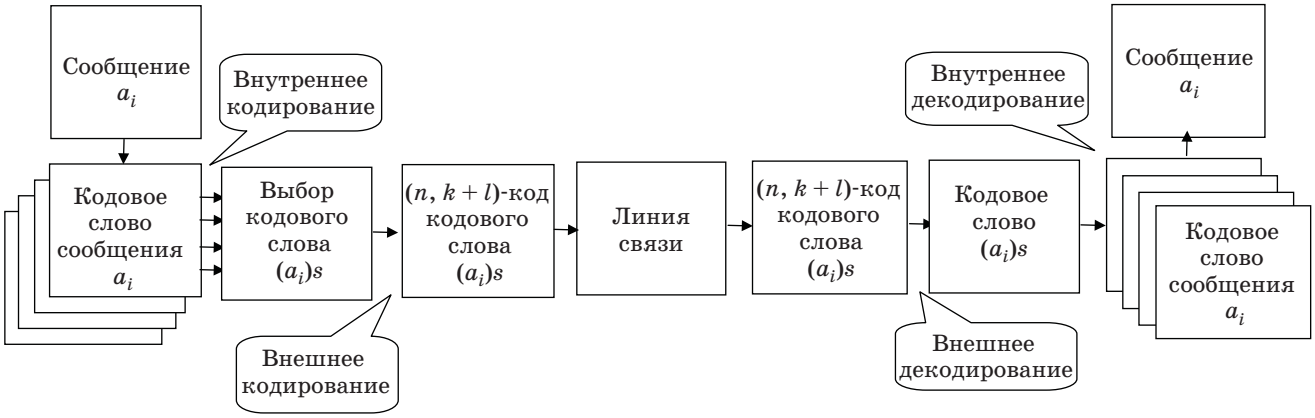
Схема преобразований сообщений при их передаче методом комбинированного случайного кодирования представлена на рис. 1.

В этой схеме стохастическое кодирование является внутренним кодированием, а помехоустойчивое кодирование — внешним кодированием. Соответственно, формирование кодового слова a_i, $i = 1, ..., N$, и его восстановление при приеме осуществляются в два этапа.

Первым этапом является стохастическое кодирование, которое может рассматриваться как кодирование источника. На этом этапе с использованием кодовой книги формируются M кодовых слов $(a_i)_s$, $s = 1, ..., M$, соответствующих передаваемому сообщению, и из них с помощью датчика случайных чисел выбирается некоторое s-е кодовое слово. В общем случае разрядность исходного сообщения a_i составляет $k = [\log_2 N]$, где $[\cdot]$ означает округление до ближайшего целого в сторону увеличения, а разрядность передаваемого кодового слова $(a_i)_s$ составляет $k + l$, где $l = [\log_2 M]$.

Вторым этапом формирования кодового слова является помехоустойчивое кодирование. На этом этапе осуществляется канальное кодирование кодового слова, выбранного из кодовой книги, блочным корректирующим $(n, k + l)$-кодом, который передается по линии связи. При приеме сообщения на первом этапе проводится декодирование принятого блочного $(n, k + l)$-кода с исправлением ошибок и выделение передаваемого кодового слова $(a_i)_s$. На втором этапе в кодовой книге выбирается сообщение a_i, соответствующее выделенному при декодировании кодовому слову. Для этого кодовые книги в пунктах приема и передачи должны быть полностью идентичны, а для нарушителя структура кодовой книги должна быть неизвестна.

Будем полагать, что при реализации комбинированного случайного кодирования внутреннее стохастическое кодирование используется в том виде, в котором оно описано в работах [5, 6]. Повышение информационной скрытности передачи информации при стохастическом кодировании достигается за счет использования кодовой книги, в которой каждому сообщению источника соответствует набор кодовых слов, из числа которых кодовое слово, передаваемое по радиоканалу передачи информации, выбирается случайным образом. Для получателя, имеющего такую же кодовую книгу, это не создает никакой неопределенности при декодировании сообщения, а для



Число передаваемых сообщений N ($i = 1, ..., N$). Разрядность сообщения $k = [\log_2 N]$	Число кодовых слов, соответствующих каждому сообщению, M ($s = 1, ..., M$). Разрядность кодового слова $k + l = [\log_2 N] + [\log_2 M]$	Помехоустойчивое кодирование передаваемого кодового слова $(n, k + l)$-кодом	Декодирование кодового слова, передаваемого $(n, k + l)$-кодом с обнаружением ошибок	Число необходимых для восстановления сообщения кодовых слов, соответствующих каждому сообщению, M ($s = 1, ..., M$). Разрядность кодового слова $k + l = [\log_2 N] + [\log_2 M]$	Число передаваемых сообщений N ($i = 1, ..., N$). Разрядность сообщения $k = [\log_2 N]$

■ ***Рис. 1.*** Схема преобразований сообщений при комбинированном случайном кодировании

нарушителя, не имеющего такой кодовой книги, это создает неопределенность и затрудняет несанкционированный доступ к передаваемой информации в случае радиоперехвата сигналов.

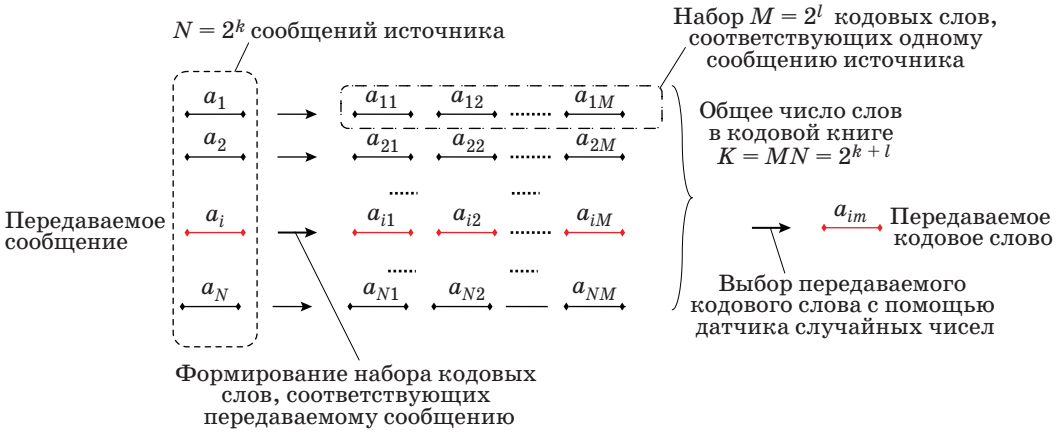
Принцип стохастического кодирования на основе кодовой книги поясняется на рис. 2.

Ансамбль передаваемых источником дискретных сообщений длины k образуют сообщения a_i, $i = 1, ..., N$. Общее число сообщений (объем ансамбля) $N = 2^k$. Каждому сообщению ставится в соответствие $M = 2^l$ кодовых слов, которые хранятся в определенной строке кодовой книги и случайным образом выбираются для передачи по каналу передачи информации. Общее число слов в кодовой книге $K = MN = 2^{k+l}$. Тогда стохастический код V может быть представлен как линейный код, образованный множеством двоичных последовательностей V_i, $i = 1, ..., N$, длины $(k + l)$, таких, что $V = \bigcup_{i=1}^{N} V_i$, $V_i \cap V_j = \varnothing$, $i \neq j$. Каждому k-разрядному сообщению a_i источника ставится в однозначное соответствие одно из подмножеств V_i, содержащее M $(k + l)$-разрядных кодовых слов a_{is}, $s = 1, ..., M$, и одно из них случайно и равновероятно выбирается для передачи по каналу. В дальнейшем в процессе внешнего помехоустойчивого кодирования выбранное для передачи кодовое слово кодируется блочным корректирующим кодом, при этом в него вводятся r проверочных символов, так что общее число разрядов передаваемых кодовых слов будет составлять $n = k + l + r$.

Внешнее помехоустойчивое кодирование используется в рассматриваемом методе комбинированного случайного кодирования в традиционном виде канального кодирования [3, 4]. Повышение помехоустойчивости передачи информации при помехоустойчивом кодировании достигается за счет использования корректирующих кодов, обнаруживающих и исправляющих ошибки при приеме. Строго говоря, из $(k + l)$ символов кодового слова, формируемого с помощью кодовой книги, информационными являются только k символов, но для этапа помехоустойчивого кодирования все $(k + l)$ символов входного кодового слова представляют собой информационное сообщение. В отсутствие обратного информационного канала используется помехоустойчивое кодирование с исправлением ошибок, что соответствует FEC-протоколам (*Forward Error Correction*) канального уровня. При приеме декодирование осуществляется путем обратного преобразования. Сначала декодируется корректирующий код с исправлением ошибок, а затем проводится оценка переданного сообщения $\tilde{a}_i$, соответствующего подмножеству V_i, содержащему выделенное (с учетом корректирующих способностей помехоустойчивого кода) кодовое слово $\tilde{a}_{is}$.

Используемое в данном случае понятие кодовой книги отличается от понятия электронной кодовой книги, используемого для описания одного из наиболее распространенных режимов блочного шифрования сообщений при криптографической защите информации (режим ECB — *Electronic Code Book*) [8]. При шифровании криптографическими методами электронная кодовая книга содержит набор ключей преобразования исходного сообщения в зашифрованное. Для синхронности использования ключей на передающем и приемном пунктах предварительно реализуются режимы согласования (синхронизации) или распространения ключей.

Принцип комбинированного случайного кодирования сохраняется и при использовании внешнего помехоустойчивого кодирования с обнаружением ошибок. При наличии обратного информационного канала это соответствует ARQ-протоколам (*Automatic Requester Quire*) канального уровня, при этом обнаружение ошибок при приеме приводит к переспросу и повторной передаче сообщения.



■ ***Рис. 2.*** Принцип стохастического кодирования с использованием кодовой книги

Помехоустойчивое кодирование с обнаружением ошибок также может использоваться и в отсутствие обратного информационного канала, если необходимо достижение компромисса между риском пропуска сообщения при обнаружении ошибки и прохождения ложного сообщения с необнаруженной ошибкой [9]. Во всех случаях внутренний стохастический код обеспечивает информационную скрытность, а внешний помехоустойчивый код — помехоустойчивость передачи сообщений.

Качественный анализ помехоустойчивости и скрытности передачи информации при комбинированном случайном кодировании

Рассмотренный принцип формирования кодовых комбинаций комбинированного кода эквивалентен передаче сообщений с помощью блокового кода, включающего k информационных символов, r проверочных символов помехоустойчивого кодирования и l псевдослучайных символов стохастического кодирования. Варианты распределения символов n-разрядного кода ($n = k + l + r$) между информационными символами, проверочными символами и символами стохастического кода приведены в табл. 1. Варианты 1 и 2 соответствуют помехоустойчивому кодированию, варианты 3 и 4 — стохастическому кодированию, вариант 6 — безызбыточному кодированию, а вариант 5, наиболее интересный с точки зрения совместного обеспечения помехоустойчивости и скрытности передачи информации, представляет собой общий случай комбинированного случайного кодирования. Такое представление позволяет качественно показать возможность одновременного повышения помехоустойчивости и скрытности передачи информации по радиоканалам с помехами и угрозами несанкционированного доступа при радиоперехвате.

При плохих условиях связи в радиоканале передачи информации используется только помехоустойчивое кодирование и n-разрядное кодовое слово включает только k информационных символов и r проверочных символов корректирующего кода (вариант 1). Тем самым обеспечивается требуемая помехоустойчивость передачи информации по радиоканалу. При средних условиях связи в радиоканале передачи информации n-разрядное кодовое слово включает k информационных символов и r проверочных символов корректирующего кода (вариант 2) или k информационных символов, r проверочных символов корректирующего кода и l символов стохастического кода (вариант 5). В обоих случаях требуемая помехоустойчивость передачи информации обеспечивается при меньшем числе проверочных символов корректирующего кода, при этом освободившиеся разряды могут заполняться символами стохастического кода для повышения информационной скрытности передаваемых сообщений. При хороших условиях связи в радиоканале передачи информации кодовое слово включает либо k информационных символов и l символов стохастического кода (варианты 3 и 4), либо только k информационных символов (вариант 6).

Число символов стохастического кода и размерность кодовой книги взаимосвязаны с инфор-

■ *Таблица 1*

Вариант формирования кодового слова	Тип кодирования	Структура кодового слова
1	Помехоустойчивое	k | r
2	Помехоустойчивое	k | r
3	Стохастическое	k | l
4	Стохастическое	k | l
5	Комбинированное случайное	k | l | r
6	Безызбыточное	k

■ *Таблица 2*

Вариант формирования кодового слова	Помехоустойчивость в условиях помех	Информационная скрытность в условиях радиоперехвата	Скорость передачи информации	Класс сообщений
1	Высокая	Низкая	Низкая	A
2	Средняя	Низкая	Средняя	B
3	Низкая	Высокая	Низкая	A
4	Низкая	Средняя	Средняя	B
5	Средняя	Средняя	Низкая	A
6	Низкая	Низкая	Высокая	C

мационной скрытностью передачи информации так же, как длина ключа при шифровании: чем больше l, тем выше информационная скрытность [7, 8]. В свою очередь скорость передачи информации во всех случаях определяется избыточностью кода и соотношением n и k, в результате повышение помехоустойчивости и информационной скрытности всегда достигается за счет уменьшения скорости передачи информации. В табл. 2 приведены ожидаемые результаты применения комбинированного случайного кодирования в системах радиосвязи и радиоуправления для рассмотренных вариантов формирования кодовых слов и рекомендации по их использованию для трех условно выделенных типов сообщений (А — высокоприоритетных, В — среднеприоритетных, С — низкоприоритетных).

Количественный анализ помехоустойчивости и скрытности передачи информации при комбинированном случайном кодировании

Количественный анализ помехоустойчивости и скрытности передачи информации при использовании комбинированного случайного кодирования может быть осуществлен с использованием показателей достоверности и защищенности передачи информации.

Достоверность передачи сообщений блочным помехоустойчивым (n, k)-кодом с исправлением ошибок характеризуется вероятностью ошибочного приема сообщения $P_{ош}$, которая при посимвольном приеме для стандартной биномиальной модели дискретного канала передачи информации определяется выражением

$$P_{ош} = \sum_{i=q_и+1}^{n} C_n^i p_0^i (1-p_0)^{n-i}, \qquad (1)$$

где p_0 — вероятность ошибочного приема информационного символа; $q_и$ — кратность исправляемых ошибок. Величина p_0 определяется условиями радиосвязи и связана с отношением сигнал/шум в радиоканале передачи информации [1, 4]. Величина $q_и$ определяется границей Хемминга

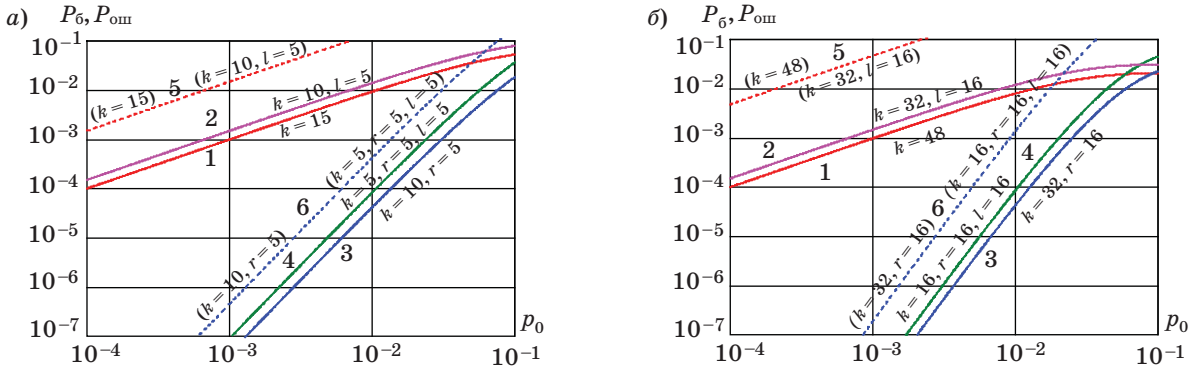
$$n - k \geq \log_2 \left(1 + \sum_{i=1}^{q_и} C_n^i\right), \qquad (2)$$

задающей минимальное число поверочных символов $r = n - k$, при котором существует корректирующий код, гарантированно исправляющий ошибки с кратностью $q_и$. При $r = 0$ код является безызбыточным и $q_и = 0$.

Величины p_0 и $P_{ош}$ являются общепринятыми показателями достоверности передачи дискретных сообщений с помехоустойчивым кодированием [2, 3]. При комбинированном случайном кодировании с учетом введенных обозначений число информационных символов k в неравенстве (2) заменяется на $(k + l)$, а кроме вероятности ошибочного приема сообщения $P_{ош}$, определяемой выражением (1), целесообразно использовать вероятность ошибки на бит $P_б = P_{ош}/k$, где $k = [\log_2 N]$. Тем самым показатель достоверности нормируется к количеству информации в передаваемом сообщении, которое определяется числом информационных символов в кодовом слове.

На рис. 3, *а* и *б* представлены результаты расчетов вероятностей $P_б$ и $P_{ош}$ в зависимости от p_0 при различных сочетаниях числа информационных символов k, проверочных символов r и символов стохастического кода l в n-разрядном кодовом слове $(n = k + l + r)$.

Выбранные при анализе (n, k)-коды соответствуют реальным помехоустойчивым циклическим кодам — коду (15,10), исправляющему



■ ***Рис. 3.*** Вероятности ошибочного приема сообщения и ошибки на бит при комбинированном случайном кодировании: *а* — $n = 15$; *б* — $n = 48$: *1* — $P_б$ при безызбыточном кодировании; *2* — $P_б$ при стохастическом кодировании; *3* — $P_б$ при помехоустойчивом кодировании; *4* — $P_б$ при комбинированном случайном кодировании; *5* — $P_{ош}$ при безызбыточном и стохастическом кодировании; *6* — $P_{ош}$ при помехоустойчивом и комбинированном случайном кодировании

$q_и = 2$ ошибки, и коду (48,32), исправляющему $q_и = 3$ ошибки [10]. При реализации комбинированного случайного кодирования эти коды позволяют поровну разделить кодовое слово между информационными символами, проверочными символами и символами стохастического кода. Анализ результатов расчетов показывает, что с точки зрения показателей достоверности $P_{ош}$ и $P_б$ принципиальное значение имеет использование помехоустойчивого кодирования, обеспечивающего существенное уменьшение $P_{ош}$ и $P_б$ при фиксированной величине p_0 за счет исправления ошибок. Выигрыш в помехоустойчивости, как и следовало ожидать, тем больше, чем выше кратность исправляемых помехоустойчивым кодом ошибок $q_и$ и чем меньше вероятность ошибочного приема информационного символа p_0. Введение статистического кодирования незначительно увеличивает величину $P_б$ и не влияет на величину $P_{ош}$, но приводит к снижению в $(n - r)/(n - r - l)$ раз скорости передачи информации. В рассмотренных случаях это снижение составляет 1,5–3 раза, однако при этом повышается информационная скрытность передачи сообщений. И если в случае помехоустойчивого кодирования происходит «обмен» скорости передачи информации на достоверность, то в случае стохастического кодирования происходит «обмен» скорости передачи информации на защищенность.

Количественная оценка защищенности передачи сообщений при стохастическом кодировании связана с определенными сложностями выбора показателя, поскольку при случайном выборе передаваемых кодовых слов из кодовой книги информационная скрытность определяется степенью неопределенности нарушителя об используемом ансамбле кодовых слов. По этой причине применительно к методу стохастического кодирования, являющемуся некриптографическим методом защиты информации, затруднено применение методов оценки информационной скрытности передачи сообщений с криптографической защитой, основанных на оценке вычислительной сложности и стойкости алгоритма шифрования к криптоанализу [2, 7].

В качестве количественных показателей защищенности передачи сообщений при стохастическом кодировании могут быть использованы объем кодовой книги и обобщенный показатель уровня информационной доступности. Объем кодовой книги, имеющей структуру, показанную на рис. 2, представляет собой общее число кодовых слов $K = MN$, которые могут быть с ее помощью сформированы. При отсутствии у нарушителя полной информации о кодовой книге для правильного выделения сообщения ему необходимо осуществлять перебор всех неизвестных ему кодовых слов. Их число определяет сложность перебора. В случае полностью неизвестной нарушителю кодовой книги сложность перебора определяется ее объемом $K = MN$.

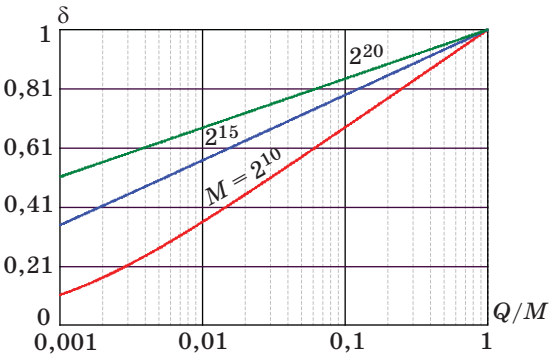
Уровень информационной доступности определяется соотношением между энтропией источника сообщений и условной энтропией нарушителя, осуществляющего радиоперехват. Он зависит от соотношения между общим числом кодовых комбинаций $K = MN$ кодовой книги, используемой источником и получателем, и числом кодовых комбинаций Q, верно выделяемых нарушителем, не знающим всей кодовой книги.

Вычисление величины Q требует учета свойств конкретных кодов и условий радиоперехвата, причем эти условия, как правило, таковы, что качество приема сигналов и достоверность выделения сообщений нарушителем ниже, чем получателем сообщений [11], и это приводит к снижению величины Q. Если в соответствии с представлением структуры кодового слова комбинированного случайного кода в табл. 1 полагать, что информационная скрытность передаваемого сообщения обеспечивается введением в кодовое слово l символов стохастического кода, то величину Q необходимо сопоставлять с числом кодовых слов в строке кодовой книги $M = 2^l$. Если использовать верхнее граничное значение $Q \le 2^t - 1$, где $0 \le t \le l$ — число позиций стохастического кода, верно выделяемых нарушителем при перехвате, то уровень информационной доступности δ передаваемых сообщений при комбинированном случайном кодировании может быть определен в следующем виде:

$$\delta = \frac{\log_2(Q+1)}{\log_2(M+1)}. \qquad (3)$$

Выражение (3) представляет собой информационный показатель защищенности передаваемой информации, определяемый как отношение энтропии, имеющей место для нарушителя, правильно выделяющего некоторое количество символов кодового слова, к максимально возможной энтропии источника, определяемой объемом кодовой книги. Нормировка в выражении (3) и добавление единицы к аргументу логарифма в числителе и знаменателе обеспечивают приведение величины δ к диапазону $0 \le \delta \le 1$. Минимальный уровень информационной доступности передаваемых сообщений имеет место при $t = 0$, в этом случае $\delta = 0$. Максимальный уровень информационной доступности передаваемых сообщений имеет место при $t = l$, в этом случае $\delta = 1$. В промежуточной ситуации при $0 < t < l$ имеет место ограниченный уровень информационной доступности передаваемых сообщений: $0 < \delta < 1$.

Практически информационная скрытность при стохастическом кодировании определяется



■ ***Рис. 4.*** Уровень информационной доступности передаваемых сообщений при комбинированном случайном кодировании

теоретико-информационным уровнем защищенности — вероятностью «угадывания» передаваемого сообщения или его идентификации в результате полного перебора всех (при $t = 0$) или части кодовых (при $t > 0$) слов соответствующей строки кодовой книги. Нормированный показатель δ характеризует близость защищенности передачи сообщений к ее теоретико-информационному уровню, соответствующему размерности используемой кодовой книги. Следует отметить, что возможен подход к определению уровня информационной доступности через энтропию всей кодовой книги $\log_2 K$, при этом величину Q необходимо сопоставлять с объемом кодовой книги $K = MN = 2^{n+l}$ [12].

Результаты расчетов величины δ от отношения Q/M при различных M представлены на рис. 4.

Диапазон значений и характер изменения показателя δ обусловлены его определением с использованием логарифмической меры энтропии и нормировкой в выражении (3). Результаты расчетов показывают, что с точки зрения показателя защищенности δ принципиальное значение имеют степень осведомленности нарушителя, характеризуемая величиной Q/M, и длина строки кодовой книги M. Величина δ тем выше, чем больше отношение Q/M, а при фиксированном отношении Q/M — чем больше длина строки кодовой книги M и соответственно чем больше объем кодовой книги $K = MN$. Влияние на величину δ параметра Q/M очевидно, а влияние на величину δ объема кодовой книги K связано со свойствами параметра δ как нормированной логарифмической меры информационной доступности, учитывающей информативность каждого символа, верно выделяемого нарушителем при радиоперехвате. При фиксированном отношении Q/M число позиций стохастического кода передаваемого сообщения $t = \log_2(Q + 1)$, верно выделяемых нарушителем при перехвате, тем выше, чем больше M.

Заключение

Метод комбинированного случайного кодирования обладает широкими возможностями по повышению помехозащищенности передачи информации и ее составляющих, в том числе при обеспечении заданной помехоустойчивости и информационной скрытности путем «обмена» на них скорости передачи информации. Представленные качественные и количественные оценки показателей достоверности и защищенности передачи информации позволяют выбрать параметры комбинированного кода, удовлетворяющего требованиям к анализируемым показателям. Рассмотренные показатели достоверности — вероятности ошибочного приема сообщения и ошибки на бит — являются общепринятыми вероятностными показателями при анализе помехоустойчивости систем радиосвязи и радиоуправления, при их проектировании и эксплуатации к этим показателям предъявляются конкретные технические требования. Рассмотренные показатели защищенности — объем кодовой книги и информационная доступность передаваемых сообщений для нарушителя — являются обобщенными и могут быть использованы в качестве исходных при переходе к частным показателям, учитывающим свойства используемых кодов, конкретные условия радиоперехвата и сложность перебора нарушителем кодовых слов из неизвестной ему кодовой книги.

Литература

1. **Борисов В. И., Зинчук В. М.** Помехозащищенность систем радиосвязи. Вероятностно-временной подход. — М.: Радиософт, 2008. — 260 с.
2. **Устинов Г. Н.** Основы информационной безопасности систем и сетей передачи данных. — М.: СИНТЕГ, 2000. — 248 с.
3. **Золотарев В. В., Овечкин Г. В.** Помехоустойчивое кодирование. Методы и алгоритмы: справочник. — М.: Горячая линия-Телеком, 2004. — 126 с.
4. **Вернер М.** Основы кодирования: пер с нем. — М.: Техносфера, 2008. — 288 с.
5. **Осмоловский С. А.** Стохастические методы передачи данных. — М.: Радио и связь, 1991. — 240 с.
6. **Осмоловский С. А.** Стохастические методы защиты информации. — М.: Радио и связь, 2003. — 320 с.
7. **Корниенко А. А., Еремеев М. А., Ададуров С. Е.** Средства защиты информации на железнодорожном транспорте: Криптографические методы и средства. — М.: Маршрут, 2006. — 256 с.

8. **Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001. — 376 с.
9. **Мальцев Г. Н., Чернявский Е. В.** Кодирование сообщений в системах радиоуправления без обратного информационного канала // Информационно-управляющие системы. 2011. № 4(53). С. 60–65.
10. **Блейхут Р.** Теория и практика кодов, контролирующих ошибки: пер. с англ. — М.: Мир, 1986. — 576 с.
11. **Мальцев Г. Н., Ададуров А. С.** Сценарный подход к организации защищенной передачи информации по радиоканалам системы управления и обеспечению безопасности движения на железнодорожном транспорте // Надежность. 2011. № 2. С. 30–39.
12. **Мальцев Г. Н., Ададуров А. С.** Снижение угроз информационной безопасности систем радиосвязи // Автоматика. Связь. Информатика. 2011. № 5. С. 22–24.

UDC 621.391
doi:10.15217/issn1684-8853.2015.2.82

Noise Stability and Information Security of Radio Transfer with Combined Random Coding

Maltsev G. N., Dr. Sc., Tech., Professor, georgy_maltsev@mail.ru
A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia St., 197198, Saint-Petersburg, Russian Federation

Purpose: In radio information transfer systems, methods of channel coding are usually used to increase the noise stability of the information transfer via radio channels. Combined random coding which is a combination of noiseproof and stochastic coding allows you to simultaneously provide the noise stability and information security of the transfer. The purpose of this work is studying the interconnected indicators of reliability and information transfer security when using the combined random coding. **Method:** Qualitative and quantitative analysis of potential noise stability and information security of radio transmission on the basis of combined random coding under various choice of the code parameters. **Results:** The developed method of combined random coding is described. The indicators of reliability and information security are studied under various combinations of the amount of the information symbols, checking symbols and stochastic code symbols in the coding combination of the combined code. It is shown how to select the combined code parameters which will simultaneously satisfy the demands to both the analyzed indicators. In particular, it will ensure the noise stability and information security by exchanging them for the information transfer speed. **Practical relevance:** Recommendations are given about choosing the options of using the combined random coding for the transfer of several conditionally selected types of messages with different priorities.

Keywords — Noiseproof Coding, Stochastic Coding, Reliability and Security of Message Transmission via Radio Channels.

References

1. Borisov V. I., Zinchuk V. M. *Pomekhozashchishchennost' sistem radiosviazi. Veroiatnostno-vremennoi podkhod* [Noiseimmunity of Systems of a Radiocommunication. Approach of Probable and Temporal]. Moscow, Radiosoft Publ., 2008. 260 p. (In Russian).
2. Ustinov G. N. *Osnovy informatsionnoi bezopasnosti sistem i setei peredachi dannykh* [Bases of Information Security of Systems and Networks of Data Transmission]. Moscow, SINTEG Publ., 2000. 248 p. (In Russian).
3. Zolotarev V. V., Ovechkin G. V. *Pomekhoustoichivoe kodirovanie. Metody i algoritmy* [Noisepro of Coding. Methods and Algorithms]. Moscow, Goriachaia liniia-Telekom Publ., 2004. 126 p. (In Russian).
4. Verner M. Information and Codiering. Braunschweig/Wiesbaden, Friedr. Vieweg & Sohn, 2002.
5. Osmolovskii S. A. *Stokhasticheskie metody peredachi dannykh* [Stochastic Methods of Data Transmission]. Moscow, Radio i sviaz' Publ., 1991. 240 p. (In Russian).
6. Osmolovskii S. A. *Stokhasticheskie metody zashchity informatsii* [Stochastic Methods of Information Security]. Moscow, Radio i sviaz' Publ., 2003. 320 p. (In Russian).
7. Kornienko A. A., Eremeev M. A., Adadurov S. E. *Sredstva zashchity infor-matsii na zheleznodorozhnom transporte: Kriptograficheskie metody i sredstva* [Information Means of Protection on Railway Transport: Cryptographic Methods and Means]. Moscow, Marshrut Publ., 2006. 256 p. (In Russian).
8. Romanets Iu. V., Timofeev P. A., Shan'gin V. F. *Zashchita informatsii v komp'iuternykh sistemakh i setiakh* [Information Security in Computer Systems and Networks]. Moscow, Radio i sviaz' Publ., 2001. 376 p. (In Russian).
9. Maltsev G. N., Chernyavskiy E. V. Coding of Messages in Radio Control Systems without Reverse Information Channel. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2011, no. 4(53), pp. 60–65 (In Russian).
10. Blahut R. E. Theory and Practice of Error Control Coding. Massachusetts, Addison-Wesley, 1983.
11. Maltsev G. N., Adadurov A. S. Scenario Approach to the Organization of the Protected Information Transfer for Radio Channels of a Control System and Safety of the Movement on Railway Transport. *Nadezhnost'*, 2011, no. 2, pp. 30–39 (In Russian).
12. Maltsev G. N., Adadurov A. S. Decrease in Threats of Information Safety Isty Radio Communications. *Avtomatika. Sviaz'. Informatika*, 2011, no. 5, pp. 22–24 (In Russian).