УДК 681.391

05.00.00 Технические науки

МЕТОДИКА ПРИМЕНЕНИЯ КОРРЕКТИРУЮЩИХ КОДОВ ДЛЯ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ КРИПТОГРАММ В СИСТЕМАХ СКРЫТОГО УПРАВЛЕНИЯ ВОЙСКАМИ С РЕШАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ

Фролов Александр Дмитриевич
соискатель
Войсковая часть 97692, Россия

В данной работе предлагается методика применения корректирующих кодов для повышения достоверности передачи криптограмм в системах скрытого управления войсками с РОС при наличии мощных помех естественной и организованной структуры

Ключевые слова: ОПЕРАТИВНОСТЬ, НАДЕЖНОСТЬ, СКРЫТОЕ УПРАВЛЕНИЕ, ЗАЩИЩЕННАЯ КОРПОРАТИВНАЯ СЕТЬ, СИСТЕМ С РЕШАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ, ЦИКЛИЧЕСКИЕ КОДЫ

Doi: 10.21515/1990-4665-134-113

UDC 681.391

Engineering

THE METHOD OF APPLICATION OF ERROR-CORRECTING CODES TO IMPROVE THE RELIABILITY OF TRANSMISSION OF CRYPTOGRAMS IN COVERT COMMAND AND CONTROL SYSTEMS WITH DECISION FEEDBACK

Frolov Aleksandr Dmitrievich
applicant
Military unit 97692, Russia

In this article, we propose a method to use error-correcting codes to improve the reliability of transmission of the cryptograms in systems of covert command and control with DF considering powerful jamming in a natural and organized structure

Keywords: EFFICIENCY, RELIABILITY, HIDDEN MANAGEMENT, SECURE CORPORATE NETWORK SYSTEMS WITH DECISION FEEDBACK, CYCLIC CODES

Анализ находящихся на вооружении стран НАТО сил и средств радиоэлектронной борьбы (РЭБ) позволяет сделать вывод о том, что США и государства, входящие в блок НАТО способны проводить массированные информационные атаки против систем управления ВС РФ, включая системы боевого управления и связи ракетных войск стратегического назначения (РВСН).

В условиях массированного применения средств РЭБ следует ожидать резкого снижения достоверности криптограмм, за счет возрастания потока местных и общих искажений, исправление которых традиционными методами будет весьма проблематичным. Снижение достоверности приведет к тому, что многие криптограммы будут запрашиваться и передаваться повторно, что неизбежно приведет к снижению оперативности спецсвязи в системе СУВ.

Если в мирное время задержка прохождения конфиденциальной информации может привести лишь к дестабилизации обстановки, то в ходе боевых действий - это будет связано со срывом выполнения стратегических или тактических боевых задач.

То есть, проблема обеспечения достоверности передачи криптограмм в условиях возрастания ошибок в каналах связи в современных условиях выдвигается в важную самостоятельную область исследования.

Значимость указанной проблемы усиливается при переходе к автоматизированным методам передачи конфиденциальной информации. Автоматизированные системы СУВ являются элементом автоматизированной системы управления войсками (АСУВ) и поэтому к ним предъявляются повышенные требования по достоверности передачи криптограмм, когда допустимая вероятность ошибки может составлять величину порядка $P_{доп} = 10^{-5} - 10^{-9}$.

Поэтому повышение достоверности и оперативности СУВ является одним из главных факторов укрепления дальнейшего повышения боевой готовности спецорганов. Одним из направлений решения этой задачи является внедрение современных информационных технологий, например, основанных на использовании корректирующих кодов для целей повышения достоверности передачи криптограмм [1].

В системах СУВ передача конфиденциальной информации осуществляется через системы передачи дискретной информации (СПДИ).

В современных системах передачи дискретной информации используются два основных принципа повышения достоверности:

а) без использования обратной связи;

б) с использованием обратной связи;

В первом случае борьба с ошибками производится с помощью корректирующих кодов с исправлением ошибок. Во втором случае

применяются корректирующие коды для обнаружения ошибок, затем передача запроса по обратному каналу связи и повторная передача информации, принятой с искажениями.

В настоящее время системы с обратной связью считаются практически более целесообразными, чем без обратной связи, так как позволяют обеспечить заданную вероятность искажений в каналах связи при массированных информационных атаках противника, за счет наличия обратного канала связи.

Решающая обратная связь позволяет строить адаптивные к помехам в канале алгоритмы работы системы СУВ. Например, с возможностью переключения основного канала на резервный, при ухудшении качества основного канала ниже заданной нормы. Поэтому при построении виртуальных сетей специальной связи в качестве опорных трактов целесообразно использовать высокоскоростные телекодовые каналы связи с решающей обратной связью (РОС).

Рассмотрим общие принципы и структуру построения высокоскоростного телекодового канала связи.

На рис. 1 приведена обобщенная схема системы передачи телекодовой информации. Источник информации (ИИ) выбирает некоторое сообщение из множества сообщений $m_1, m_2, m_3,..., m_i,..., m_N$ с вероятностями соответственно $P_{m_1}, P_{m_2}, P_{m_3},..., P_{m_i},..., P_{m_N}$. Индекс i в данном случае показывает номер сообщения, предназначенного для передачи через систему связи в ограниченное время T. Поскольку объем канала ограничен, то множество дискретных сообщений $\{M\}$ также будет ограничено.

Для коррекции ошибок на приеме осуществляется статистическое согласование ИИ с каналом связи путем введения в информацию избыточности.

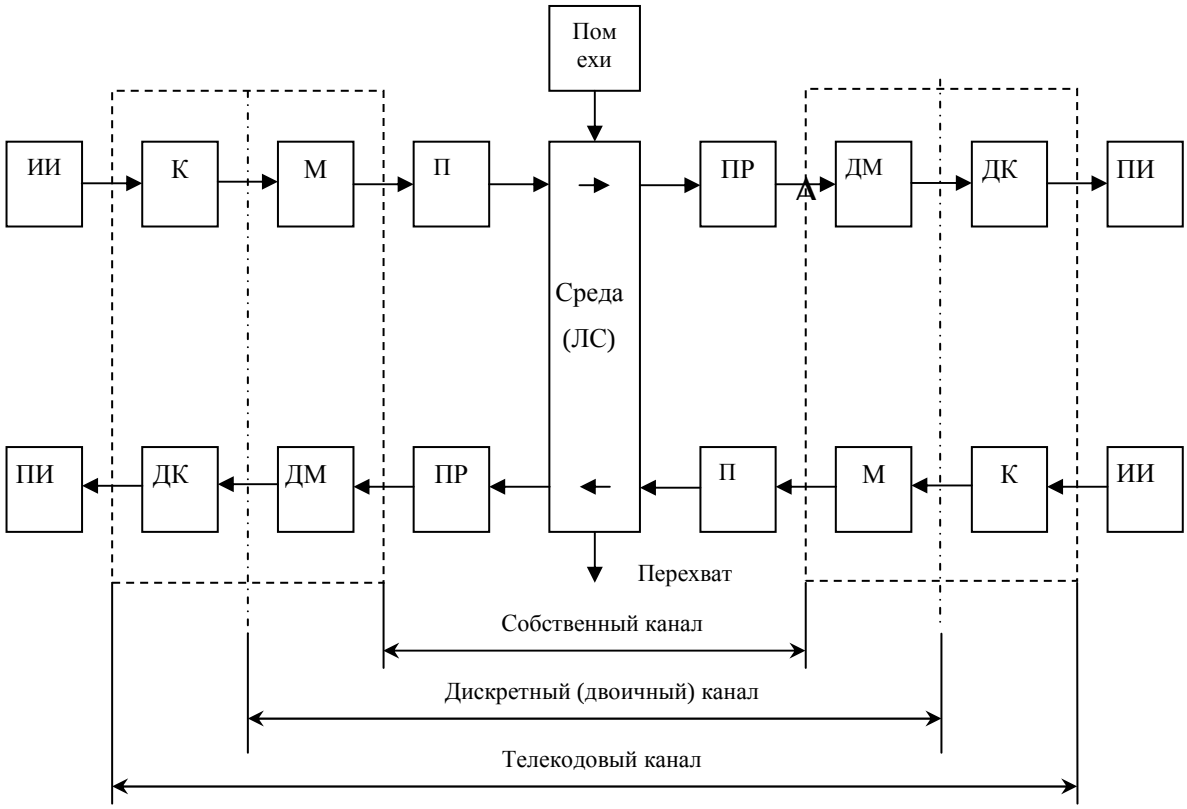

Рис. 1 Обобщенная схема системы передачи телекодовой информации

Избыточность вводится в специальном устройстве - кодере K, который выполняет однозначные преобразования элементов (знаков) равнодоступного кода в элементы (комбинации) X_i корректирующего кода. Закон преобразования множества $\{M\}$ в множество $\{X\}$ определяется алгоритмом работы кодера и зависит от конструкции примененного корректирующего кода.

Передающий модем M приводит множество сообщений к виду, удобному для управления передатчиком канала связи, путем, преобразования их в множество $\{S\}$. Под воздействием $\{S\}$ на выходе

передатчика $П$ происходит изменение одного из параметров электрического сигнала C (амплитуды, частоты или фазы).

Таким образом, в тракте передачи осуществляется следующий процесс преобразования информации:

$$\{M\} \rightarrow \{X\} \rightarrow \{S\} \rightarrow \{C\}$$

На приемной стороне связи осуществляются обратные функциональные преобразования вида:

$$\{C'\} \rightarrow \{S'\} \rightarrow \{X'\} \rightarrow \{M'\}$$

В результате из принятого сигнала выделяется конкретное сообщение m_i.

Воздействие помех в канале связи в аппаратуре формально можно учесть изменением индексов при сообщениях множества $\{M'\}$. Если на приеме $m_i' = \overline{m}_i$, то сообщение декодировано правильно и соответствует переданному. При $\overline{m}_i' = \overline{m}_j$ имеет место ошибка.

Таким образом, приемное устройство определяет, какому конкретному сообщению из множества $\{M'\}$ соответствует принятый сигнал C'. Здесь не исключена многоальтернативность принятия решения [1].

Было бы ошибочным полагать, что все помехи, воздействующие на передачу сообщения, образуется лишь в среде распространения. Помехи возникают во всех элементах канала связи, как в среде, используемой для передачи сигнала от передатчика к приемнику, так и в технических устройствах, выполняющих необходимые преобразования сигнала. В первом случае помехи называются внешними, во втором - внутренними.

Внутренние (или собственные) шумы, обязанные своим возникновением дискретной природе заряженных частиц, образуются из-за теплового движения этих частиц в элементах электрических цепей, из-за дробового эффекта в электронных приборах и ряда других явлений,

имеющих место при работе электротехнических устройств. Так, например, в оконечных каскадах усиления, где амплитуда колебаний достигает единиц вольта, приходится считаться с нелинейными искажениями, которые оцениваются коэффициентом нелинейных искажений.

В условиях информационной войны в качестве внешних помех выступают преднамеренно организованные помехи, направленные на подавление систем связи.

Для подавления передачи в системе с РОС достаточно в один из каналов дуплексной связи циклично вводить помеху, искажающую хотя бы один импульс с периодом:

$$T = n(M+1)t_0, \quad (1)$$

где:

n - длина кодовой комбинации;

$M+1$ - количество кодовых комбинаций, попавших под блокировку;

t_0 - длина элементарного импульса.

Для прогнозирования канала связи в оптимальных режимах работы необходимым условием является оценка состояния отдельных участков и всего канала в целом, то есть оценка непрерывного, дискретного и телекодового канала. Чаще всего анализ на приеме выполняется в два этапа: сначала принимается решение относительно каждого из элементов кодовой комбинации, а затем - относительно всей комбинации. Устройства, выполняющие эти операции, носят названия соответственно первой и второй решающих схем.

Декодирование может допускать утверждение (как одну из возможных альтернатив), что обнаружена ошибка, без каких-либо дополнительных гипотез относительно принятой комбинации. При этом выделяется лишь сигнал "ошибка" ("стирания") и не производится

попыток исправления. Возможно также сочетание обнаружения и исправления ошибки.

В некоторых специальных системах передачи телекодовой информации требуется очень высокая достоверность. При этом, кроме коррекции ошибок в первой и второй решающих схемах, можно прибегнуть к обработке результатов анализа информации по канальным критериям [2].

Под канальными критериями $I_{кап}$ понимаются первичные параметры собственно канала связи, получаемые на входе приемного модема $ДМ$. Среди них наиболее существенными являются:

- уровень сигнала (абсолютный, относительный и т.д.);
- соотношение уровней сигнала и помех;
- флюктуации группового времени запаздывания;
- характеристики замирания сигнала (в радиоканалах КВ диапазона);
- интенсивность и распределение интервалов прерываний в канале.

Для оценки коэффициентов правдоподобия в первой решающей схеме удобно использование импульсных критериев $I_{имп}$, например, распределение краевых искажений или интенсивности и распределение дроблений импульсов на выходе приемного модема $ДМ$.

Результаты анализа кодовых комбинаций во второй решающей схеме называют информационным критерием $I_{инф}$.

В общем случае имеется возможность обобщать результаты анализа критериев всех трех видов в блоке логической обработки, вырабатывая сигналы управления алгоритмом работы системы передачи дискретной информации [2].

В системах передачи дискретной информации с обратной связью передатчик с приемником соединены прямым и обратным каналами связи. Передатчик при вводе избыточности использует информацию о состоянии

прямого канала, получаемую по каналу обратной связи. Системы передачи дискретной информации с обратной связью делятся на три типа:

1. Система с решающей обратной связью.

2. Системы с информационной обратной связью.

3. Системы с комбинированной обратной связью.

В зависимости от алгоритма работы системы с РОС делятся на:

1. Системы с РОС с ожиданием (РОС-ОЖ).

2. Системы с РОС с последовательной непрерывной передачей кодовой комбинации (РОС-ПП).

3. Системы с РОС с накоплением правильных комбинаций (РОС-НК).

4. Системы с РОС с адресным переспросом комбинаций (РОС-АП).

В системах РОС-ПП наиболее активная роль принадлежит приемнику, а передатчик лишь управляет приемником с помощью сигналов передаваемых по каналу обратной связи. Приемник по принимаемой комбинации (n,k) кода принимает решение о выдаче этой комбинации получателю информации или о ее браковке. По каналу обратной связи передается сигнал обратной связи, зависящий от принятого решения. Могут быть два сигнала: сигнал подтверждение или запрос. В зависимости от этих сигналов передатчик осуществляет следующее:

при получении подтверждения передатчик передает очередную комбинацию;

при запросе осуществляет повторение ранее переданной комбинации.

При этом информация от источника сообщений через входное устройство поступает на накопитель и на кодирующее устройство. Далее информация считывается на выходное устройство и в канал связи.

В приемной части информация через входное устройство, регистрирующее устройство, декодирующее устройство и накопитель поступает к потребителю информации.

Если информация принята без ошибок, то с приемника распределительного устройства выдаются импульсы на считывание информации с накопителя к потребителю сообщений и посылается сигнал подтверждения приема информации и передатчик системы начинает передачу следующей комбинации.

Таким образом, СПДИ с РОС целесообразно:

применять циклические коды для исправления ошибок;

обратный канал использовать для передачи служебных и информационных сигналов или только служебных сигналов;

система может быть однократной или многократной.

Кроме того, передатчик и приемник одной и той же станции должны быть связаны определенными фазовыми соотношениями.

Рассмотрим основные свойства циклических кодов. Циклическим (n,k) кодом называется код, множество кодовых комбинаций которого представляется совокупностью многочленов степени (n-1) и менее, делящихся на некоторый многочлен $(g(x))$ степени $(n-1)$, являющийся сомножителем бинома x^n+1.

Циклические коды обладают следующими свойствами:

1. Порождающий многочлен есть делитель бинома $1+x^n \quad (n=2^m-1)$, где m-любое натуральное число.

2. Степень порождающего многочлена $g(x)$ равна числу избыточных разрядов в коде: $r=n-k$. k-число информационных элементов; n-общее число элементов для циклических кодов $r \geq 1$.

3. Минимальное кодовое расстояние $d_{\min} \geq 2$.

4. Коэффициент передачи $R=\frac{k}{n}$.

5. Минимальное кодовое расстояние связано определенными соотношениями с корректирующими свойствами кода:

$d_{\min} = S + 1, \qquad d_{\min} = 2t + 1,$

где S -число гарантированно обнаруживаемых ошибок;

t -число гарантированно исправляемых ошибок.

Разработка параметров циклического кода для автоматизированных систем СУВ должна осуществляться из условия обеспечения заданной достоверности передачи криптограмм на уровне $P_{доп} = 10^{-5} - 10^{-9}$.

Выводы: При ведении современных боевых действий в условиях мощных помех естественной и организованной структуры применение циклических кодов в режиме не только обнаружения, но и исправления ошибок в системах с решающей обратной связью позволит повысить достоверность передачи криптограмм и тем самым обеспечит оперативность управления войсками и оружием.

Библиографический список

1. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой - М.: Связь, 1975.

2. Хисамов Ф.Г. Крупенин А.В. Способ апостериорного преобразования информации в автоматизированных системах с решающей обратной связью критически важных объектов. / Ф.Г. Хисамов , А.В. Крупенин // Сборник трудов X международной конференция «Кибернетика и высокие технологии XXI века», Воронеж, 2009 г. С. 365-370

References

1. Korzhik V.I., Fink L.M. Pomehoustojchivoe kodirovanie diskretnyh soobshhenij v kanalah so sluchajnoj strukturoj - M.: Svjaz', 1975.

2. Hisamov F.G. Krupenin A.V. Sposob aposteriornogo preobrazovanija informacii v avtomatizirovannyh sistemah s reshajushhej obratnoj svjaz'ju kriticheski vazhnyh ob#ektov. / F.G. Hisamov , A.V. Krupenin // Sbornik trudov X mezhdunarodnoj konferencija «Kibernetika i vysokie tehnologii XXI veka», Voronezh, 2009 g. S. 365-370