УДК 621.396

МЕТОД ШИФРОВАНИЯ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ ПО СЛУЧАЙНОМУ ЗАКОНУ

А. Х. Абед

Кафедра «Конструирование радиоэлектронных и микропроцессорных систем»
ФГБУ ВПО «ТГТУ»; crems@crems.jesby.tstu.ru

Ключевые слова и фразы: защищенный канал связи; ключ; помехоустойчивость; радиостанция; ретранслированные помехи; шифрование.

Аннотация: Определив шифрование передаваемой между объектами информации как перспективное направление повышения помехоустойчивости каналов, в статье рассматривается необходимость организации дополнительного защищенного канала между объектами связи. Определяется круг возможных затруднений в этом направлении (создание специального канала, ключей) и предложены пути их устранения. Предложены к рассмотрению некоторые особенности передачи информации в случае действия ретранслированной помехи. Разработан метод шифрования, затрудняющий работу криптоаналитиков.

Перспективным направлением повышения помехоустойчивости каналов связи может стать шифрование передаваемой между объектами информации. Особенностью радиостанции (РС) при использовании известных методов шифрования является необходимость в защищенном канале для периодической передачи ключа на приемную сторону. Процедура передачи изменяющегося ключа на приемную сторону необходима в связи с тем, что рано или поздно криптоаналитик будет обладать достаточными сведениями о структуре и характере передаваемых между объектами сообщений.

Организация дополнительного защищенного канала между объектами вызывает значительные материальные затраты. Кроме того, необходимо определить максимально допустимый период смены ключа. Этого можно избежать, если ключ для расшифровки последующего сообщения передавать в составе предыдущего сообщения, причем сам ключ в передаваемом сообщении распределяется специальным образом. Известно [1], что ключ, основой формирования которого является истинно случайная последовательность, обладает абсолютной криптостойкостью, а «запускающим элементом» для генератора истинно случайной числовой последовательности может служить выходной сигнал любого прибора. Сформированные таким образом сообщения могут передаваться по общедоступному каналу. Схема той части цифрового канала передачи данных, входящего в состав РС, в которой осуществляется процедура шифрования, показана на рис. 1, где

приняты следующие обозначения: ГИСЧП – генератор истинно случайной числовой последовательности; ГК – генератор ключей; ЗУ – запоминающее устройство; ∑ – устройство расширения сообщения; БШ – блок шифрования; БДШ – блок дешифрования; СЧ – случайное число; С – сообщение; К – ключ; (К–1) – ключ для предыдущего сообщения; (С+К) – смешанное сообщение; ШС – шифрованное сообщение.

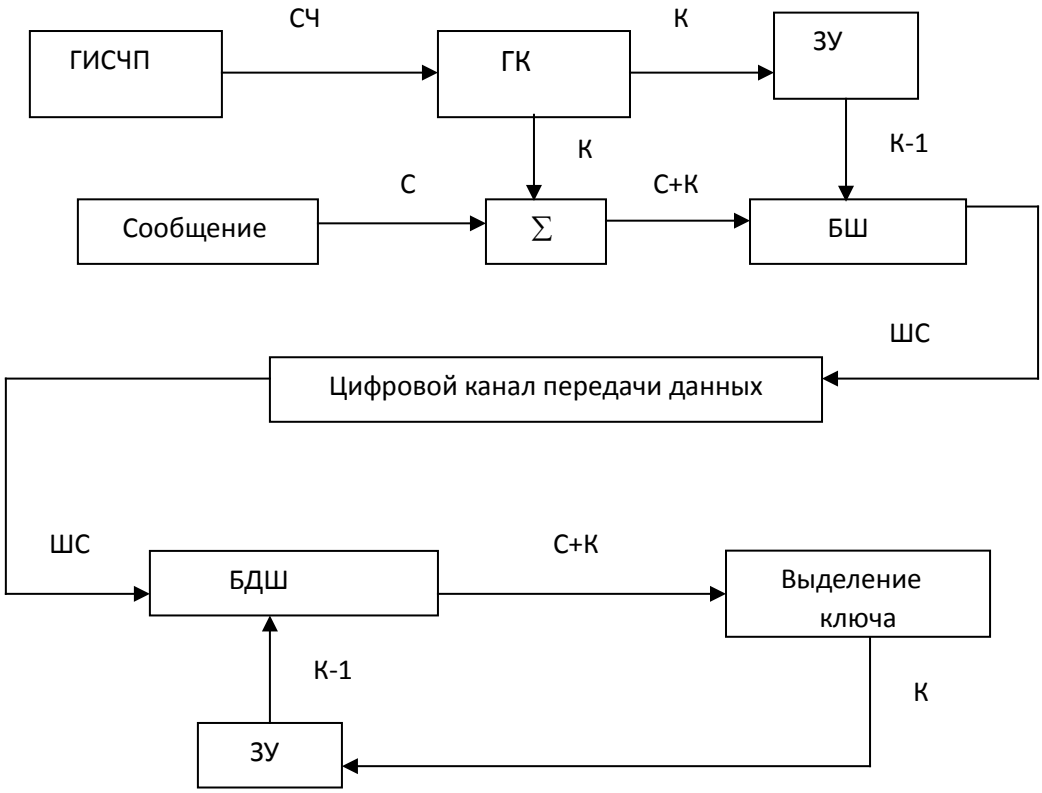

Рис. 1. Схема цифрового канала передачи данных с шифрованием сообщений по случайному закону

Рассмотрим особенности передачи сообщений предлагаемым способом в случае действия ретранслированной помехи. В процессе функционирования РС сумма очередного сообщения и ретранслированной помехи поступает на вход узкополосного демодулятора, который выносит решение об очередном двоичном сообщении. Качество работы РС оценивается вероятностью ошибки $P_{ОШ}$, являющейся функцией отношения мощностей помехи и сигнала $P_{П}/P_{c}$. В связи с тем, что сторона, организующая подавление радиосвязи, способна манипулировать отношением $P_{П}/P_{c}$ в РС необходимо использовать для передачи сообщений нормированные сигналы.

К числу представляющих интерес статистических характеристик относятся первые четыре центральных момента распределения значений корреляционной функции: математическое ожидание (МО) m; приведенная дисперсия (ПД) $\sigma^2 N$; коэффициент асимметрии (КА) α; коэффициент эксцесса (КЭ) γ.

Ансамбли кодовых последовательностей с целью повышения помехоустойчивости подбираются таким образом, чтобы, $m_c = 0,\ \sigma^2 N = 1,\ \alpha_c = 0,$ где нижний индекс «с» характеризует принадлежность статистической характеристики к сообщению.

Используя известные формулы [2], получим выражения для ПД и КЭ в общем виде:

$$\sigma^2 N = 1/L^2 \left[\sum_{i=1}^{NL^2} (\theta_i - m_c)^2 \right], \tag{1}$$

$$\gamma_c = \sigma^{-4} / NL^2 \left[\sum_{i=1}^{NL^2} (\theta_i - m_c)^4 \right], \tag{2}$$

где $\theta_i -$ значение выборки, N –длина кодовой последовательности, которой манипулируется сообщение; $L -$ количество кодовых последовательностей в ансамбле. Тогда с учетом специфики подбора кодовых последовательностей имеем

$$\sigma^2 N = 1/L^2 \left[\sum_{i=1}^{NL^2} \theta_i^2 \right], \tag{3}$$

$$\gamma_c = N/L^2 \left[\sum_{i=1}^{NL^2} \theta_i^4 \right]. \tag{4}$$

При использовании для формирования очередного сообщения разработанного метода шифрования криптоаналитик не будет иметь возможности «угадать» правило выбора кодовой последовательности. Тогда к числу наихудших для РС помех будут относиться ретранслированные помехи с введенной ложной информацией. Введение ложной информации осуществляется путем замены части элементарных сигналов на противоположные. Предполагается, что в ретранслированной помехе на противоположные заменены L последних символов сообщения (предположение не оказывает влияния на выводы при замене такого же количества символов, распределенных по всему сообщению).

Замена элементарных сигналов в ретранслированной помехе с целью обеспечения ее сходства с сообщением должна осуществляться криптоаналитиком таким образом, чтобы выполнялось условие:

$$m_{p.n.} = m_c = 0,\ \alpha_{p.n.} = \alpha_c = 0\,. \tag{5}$$

Тогда

$$\sigma^2_{p.n.}N = 1/L^2\left[\sum_{i=1}^{NL^2-L}\theta_i^2\right] + 1/L^2\left[\sum_{i=NL^2-L}^{NL^2}\theta_i^2\right]; \quad (6)$$

$$\gamma_{p.n.} = \left(\sigma_c^{-4}/NL^2\right)\left[\sum_{i=1}^{NL^2-L}\theta_i^4\right] + \left(\sigma_c^{-4}/NL^2\right)\left[\sum_{i=NL^2-L}^{NL^2}\theta_i^4\right]. \quad (7)$$

С учетом того, что $NL^2 >> L$, а также (1) и (2), сравнительные статистические характеристики ретранслированной помехи с введенной ложной информацией будут иметь вид:

$$\sigma^2_{p.n.}N = N\sigma_c^2 + 1/L, \quad (8)$$

$$\gamma_{p.n.} = \gamma_c + \sigma^{-4}_{p.n.}/NL = \gamma_c + NL/(L+1)^2. \quad (9)$$

Соотношения (8) и (9) наглядно показывают искажения статистических характеристик ретранслированной помехи с L измененными элементарными символами по отношению к копируемому сообщению.

График зависимости вероятности ошибки $P_{ош}$ от КЭ ретранслированной помехи, содержащей ложную информацию, показан на рис. 2.

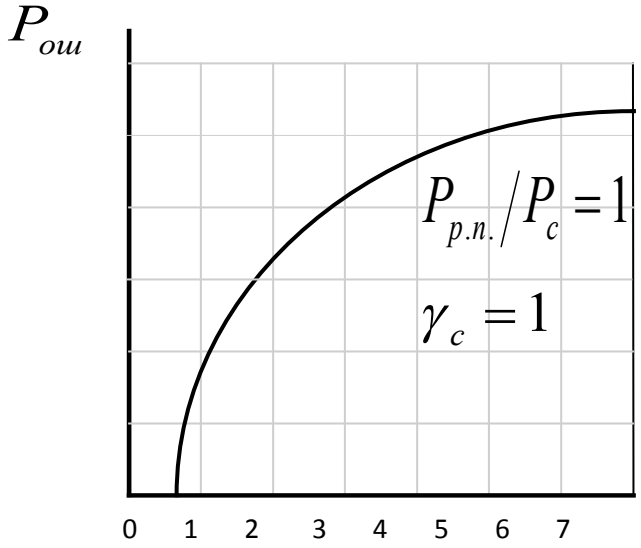

Рис. 2. Зависимость вероятности ошибки от коэффициента эксцесса

График построен для случая, когда мощности помехи и полезного сигнала равны, коэффициент эксцесса сообщения равен единице, а кодовая последовательность состоит из 127 знаков.

Анализ зависимостей (6–(9) и графика на рис.2 показывают, что вероятность ошибки при приеме сообщения совместно с ретранслированной помехой понижается при увеличении количества элементов кодовой последовательности, используемых при передаче сообщений, а также при уменьшении КЭ ретранслированной помехи. Это означает, что повышение помехоустойчивости РС можно осуществить не за счет безграничного увеличения N и L, а за счет понижения $\gamma_{p.n.}$ КЭ ретранслированной помехи.

Метод шифрования передаваемой информации по случайному закону открывает широкие возможности повышения помехоустойчивости РС на уровне узкополосных модулятора и демодулятора, так как передаваемый ключ может выполнять разные функции, в том числе быть опорным сигналом для приема следующего сообщения. Физический смысл полученных результатов заключается в учете статистических характеристик помех на входе узкополосного демодулятора от вероятности совпадения форм сообщения и преднамеренной помехи. Данные характеристики могут также использоваться для обнаружения «активного» противника в линиях радиосвязи.

Список литературы

1. Скляр, Б. Цифровая связь / Б. Скляр. – М.: Издат. дом Вильямс, 2003.–1104с.

2. Жуков, В.М. Особенности приема ортогональных многопозиционных сигналов в многолучевых каналах связи / В.М. Жуков, И.Г. Карпов, Г.Н. Нурутдинов // Радиотехника. –2006. – № 5. – С. 86-88.

Encryption Methods to Transmit Information at Random

A. H. Abed

Department "Designe of Radio and Microprocessor System" ,TSTU;
crems@crems.jesby.tstu.ru

Key words and phrases: encryption; key; Immunity; radio station; secure communications channel; the repeated interference.

Abstract: The encryption of data transferred between objects as a promising way to improve the noise immunity of the channel, the article examines the need to organize additional secure channel communications between objects. Determine the range of possible difficulties in this area (establishment of a special channel, keys) and the ways to address them. Proposed to consider some features of the transmission of information in the case of action relayed interference. A method of encryption, complicating the work of cryptanalysts.

Reference

1.Sklar, B. Digital Communications/ B. Sklar. – M.: Bublication Williams House, 2003. – 2003. – 1104p.

2. Zhukov, V.M. Features multi-position reception orthogonal signals in multipath channels of communication / V.M. Zhukov, I.G. Karpov, G.N. Nurutdinov // Radio engineering. –2006. – № 5. – P. 86-88.