УДК 621.396
DOI: 10.17277/vestnik.2016.02.pp.233-237

МЕТОД ШИФРОВАНИЯ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ ПО СЛУЧАЙНОМУ ЗАКОНУ

А. Х. Абед

Кафедра «Конструирование радиоэлектронных и микропроцессорных систем», ФГБОУ ВО «ТГТУ»; crems@crems.jesby.tstu.ru

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

Аннотация: Рассмотрена необходимость организации дополнительного защищенного канала между объектами связи, при шифровании передаваемой между объектами информации как перспективном направлении повышения помехоустойчивости каналов. Определен круг возможных затруднений (создание специального канала, ключей) и предложены пути их устранения. Представлены 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; $\sum$ – 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.

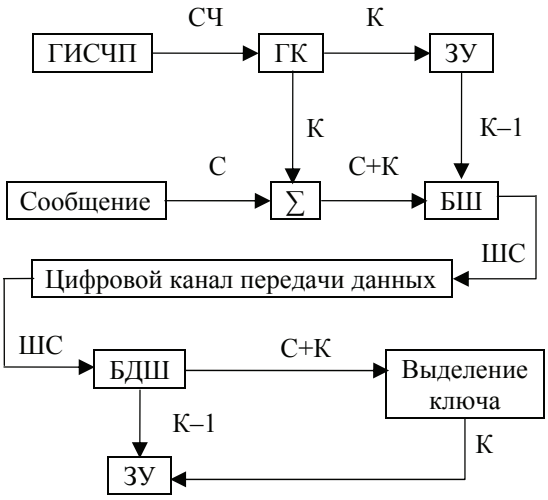

Рис. 1. Схема цифрового канала передачи данных с шифрованием сообщений по случайному закону

Рассмотрим особенности передачи сообщений предлагаемым способом в случае действия ретранслированной помехи. В процессе функционирования РС очередное сообщение и ретранслированная помеха одновременно поступают на вход узкополосного демодулятора, который выносит решение об очередном двоичном сообщении. Качество работы РС оценивается вероятностью ошибки $P_{\text{ош}}$, являющейся функцией отношения мощностей помехи и сигнала $P_{\text{п}}/P_{\text{сигн}}$. В связи с тем, что сторона, организующая подавление радиосвязи, способна манипулировать данным отношением, 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 в целях повышения помехоустойчивости подбираются таким образом, чтобы $m_{\text{c}} = 0;\ \sigma^2 N = 1;\ \alpha_{\text{c}} = 0,$ где нижний индекс «с» характеризует принадлежность статистической характеристики к сообщению.

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

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

$$\gamma_{\text{c}} = \frac{\sigma^{-4}}{NL^2}\left[\sum_{i=1}^{NL^2}(\theta_i - m_{\text{c}})^4\right], \tag{2}$$

где θ_i – значение выборки; N –длина кодовой последовательности, которой манипулируется сообщение; L – число кодовых последовательностей в ансамбле. Тогда с учетом специфики подбора кодовых последовательностей имеем:

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

$$\gamma_{\text{c}} = \frac{N}{L^2}\left[\sum_{i=1}^{NL^2}\theta_i^4\right]. \tag{4}$$

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 по-

мех 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 числа символов, распределенных по всему сообщению).

Замена элементарных сигналов в ретранслированной помехе в целях обеспечения ее сходства с сообщением должна осуществляться криптоаналитиком таким образом, чтобы выполнялись условия:

$$m_{\text{р.п}} = m_{\text{с}} = 0;\ \alpha_{\text{р.п}} = \alpha_{\text{с}} = 0,. \tag{5}$$

тогда

$$\sigma^2_{\text{р.п}} N = \frac{1}{L^2}\left[\sum_{i=1}^{NL^2-L} \theta_i^2\right] + \frac{1}{L^2}\left[\sum_{i=NL^2-L}^{NL^2} \theta_i^2\right]; \tag{6}$$

$$\gamma_{\text{р.п}} = \frac{\sigma_{\text{с}}^{-4}}{NL^2}\left[\sum_{i=1}^{NL^2-L} \theta_i^4\right] + \frac{\sigma_{\text{с}}^{-4}}{NL^2}\left[\sum_{i=NL^2-L}^{NL^2} \theta_i^4\right]. \tag{7}$$

Учитывая уравнения (1) и (2), а также, что $NL^2 >> L$, запишем сравнительные статистические характеристики ретранслированной помехи с введенной ложной информацией:

$$\sigma^2_{\text{р.п}} N = N\sigma_{\text{с}}^2 + 1/L; \tag{8}$$

$$\gamma_{\text{р.п}} = \gamma_{\text{с}} + \sigma_{\text{р.п}}^{-4} \big/ NL = \gamma_{\text{с}} + NL \big/ (L+1)^2. \tag{9}$$

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 $P_{\text{ош}}$ от КЭ ретранслированной помехи, содержащей ложную информацию, показан на рис. 2 и построен для случая, когда мощности помехи и полезного сигнала равны, $\gamma_{\text{с}} = 1$, а кодовая последовательность состоит из 127 знаков.

Анализ зависимостей (6) – (9) и графика на рис. 2 показывает, что вероятность ошибки при приеме сообщения совместно с ретранслированной помехой понижается при увеличении числа 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 $\gamma_{\text{р.п}}$ КЭ ретранслированной помехи. Метод шифрования передаваемой информации по случайному закону открывает ши-

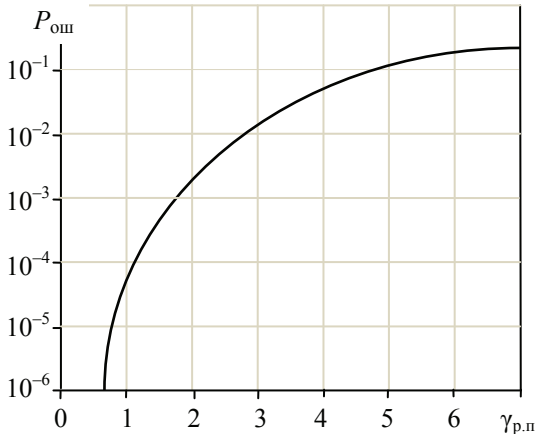

Рис. 2. Зависимость вероятности ошибки от коэффициента эксцесса:
$P_{\text{п}}/P_{\text{сигн}} = 1;\ \gamma_{\text{с}} = 1$

рокие 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. : Вильямс, 2003. – 1104 с.

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 Method to Transmit Information at Random

A. Kh. Abed

Department of Design of Radio and Microprocessor Systems, TSTU;
crems@crems.jesby.tstu.ru

Keywords: encryption; interference immunity; key; radio station; repeated interference; secure communications channel.

Abstract: The paper studies the need to create an additional security communication channel when encrypting the data transmitted between objects. It is as a promising method of improving the noise immunity of channels. The author defines the range of possible difficulties in this area (creating a special channel, keys) and the ways to address them. The author proposes to consider some features of data transmission in the case of action-relayed interference. The proposed encryption method is aimed at complicating the work of cryptanalysts.

References

1. Sklyar B. *Tsifrovaya svyaz'* [Digital Communication], Moscow: Vil'yams, 2003, 1104 p. (In Russ.)

2. Zhukov V.M., Karpov I.G., Nurutdinov G.N. [Features of Reception of Orthogonal Multiitem Signals in Multibeam Liaison Channels], *Radiotekhnika* [Radioengineering], 2006, no. 5, pp. 86-88. (In Russ., abstract in Eng.)

Methode der Chiffrierung der übergebenden Information nach dem Zufallsgesetz

Zusammenfassung: Es ist die Notwendigkeit der Organisierung des zusätzlichen geschützten Kanals zwischen den Objekten der Verbindung bei der Chiffrierung der zwischen den Objekten übergebenden Information wie die perspektivische Richtung der Erhöhung der Störunempfindlichkeit der Kanäle

betrachtet. Es ist der Kreis der möglichen Schwierigkeiten (die Bildung des speziellen Kanals, der Schlüssel) bestimmt und es sind die Wege ihrer Beseitigung angeboten. Es sind einige Besonderheiten der Sendung der Information im Falle der Handlung der weitergeleiteten Störung vorgelegt. Es ist die Methode der Chiffrierung, die die Arbeit der Kryptoanalytiker erschwert, entwickelt.

Méthode du cryptage des informations transmises par la loi de hasard

Résumé: Est considéré le besoin d'une organisation d'une voie protégée supplémentaire entre les objets de la communication lors du chiffrement de l'information transmise par les objets comme une orientation perspective de l'augmentation de la résistance aux interférences électroniques (création d'une voie spéciale, des clefs). Sont proposées les possibilitées des résolutions. Sont présentées quelques particularités de la transmission de l'information dans le cas des bruits. Est élaborée une méthode du chiffrement empêchant le travail des analystes de cryptage.

Автор: ***Абед Ахмед Хассан Абед*** **–** аспирант кафедры **«**Конструирование радиоэлектронных и микропроцессорных систем**»**, ФГБОУ ВО «ТГТУ».

Рецензент: ***Шамкин Валерий Николаевич*** **–** доктор технических наук, профессор кафедры **«**Конструирование радиоэлектронных и микропроцессорных систем», ФГБОУ ВО «ТГТУ».