УДК 621.396

А.А. Замула[1], Ю.В. Землянко[2], Е.А. Семенко[1], Д.А. Семченко[3]

[1]*Харьковский национальный университет имени В.Н. Каразина, Харьков*
[2]*Харьковский государственный университет питания и торговли, Харьков*
[3]*Харьковский национальный университет радиоэлектроники, Харьков*

УСЛОВИЯ РЕАЛИЗАЦИИ ДИНАМИЧЕСКОГО РЕЖИМА ФУНКЦИОНИРОВАНИЯ В СИСТЕМАХ СВЯЗИ

Рассмотрена возможность достижения требуемых показателей помехоустойчивости, скрытности систем связи на основе реализации динамического режима функционирования систем связи, при котором осуществляется смена соответствия бит сообщения – сложный сигнал по закону, предсказание которого возможно с вероятностью, не превышающей допустимую. Сформулированы необходимые и достаточные условия построения абсолютно стойкой системы на уровне источника сигналов.

Ключевые слова: *динамический режим, помехоустойчивость, скрытность, сложный сигнал.*

Введение

Комплексное решение проблемы обеспечения помехоустойчивости, скрытности функционирования системы связи может быть достигнуто, в том числе, на основе реализации динамического режима передачи информации, при котором осуществляется смена соответствия:

m бит сообщения – 2^m сложных сигналов.

Одним из путей достижения заданной помехоустойчивости и скрытности системы связи является реализация частотной избыточности в канале связи на основе использования дискретных кодовых сигналов (ДКС) с заданными корреляционными, ансамблевыми, структурными свойствами [1, 5]. Кроме того, достижение указанных характеристик функционирования системы связи при использовании динамического режима передачи данных возможно при реализации определенных условий (определенного закона) смены соответствия: бит сообщения – ДКС, и использования ансамбля сигналов (ДКС), соответствующего критериям оптимальности.

Определим условия смены соответствия m бит сообщения – 2^m сложных сигналов, при выполнении которых предсказание нарушителем правила смены соответствия возможно с вероятностью, не превышающей допустимой.

Очевидно, что смена соответствия должна осуществляться с применением некой управляющей функции. Примером такой функции может быть управляющая последовательность (УП) символов. И, если УП задается неким процессом, закон формирования выходной последовательности на выходе которого является непредсказуемым, то в этом случае можно говорить о скрытности функционирования системы передачи информации на уровне источника сложных сигналов.

Определим условия построения системы передачи информации, использующей динамические принципы передачи, при которых обеспечивается абсолютная скрытность системы на уровне источника сигналов. При этом под абсолютной скрытностью будем понимать невозможность злоумышленника определить закон, по которому производится смена соответствия: «бит сообщения – сложный сигнал.

Необходимые и достаточные условия реализации абсолютной скрытности на уровне источника сигналов

На рис. 1 представлена структурная схема реализации динамического режима функционирования радиоканала, состоящая из ИИ – источника информации, ДМ – динамического модулятора, УФУП – устройства формирования управляющей последовательности.

Пусть имеется некоторый источник информации, создающий в фиксированный момент времени одно из M возможных сообщений.

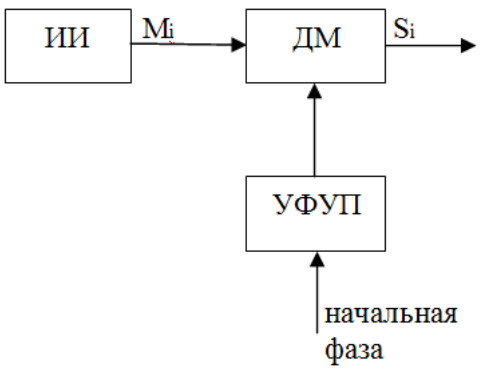

Рис. 1. Схема реализации динамического режима функционирования радиоканала

Каждое из M конкурирующих сообщений передается посредством сигнала:

$$S = \{S_i(t) : i = 1, 2, ... M\}.$$

На число сигналов M (или мощность множества S), не накладывается никаких ограничений и, если это необходимо, множество S может быть бесконечным.

Модулятор обеспечивает формирование сложных сигналов, а демодулятор (устройство обработки сложных сигналов) – их поиск, обнаружение и различение.

Символы сообщения от источника информации, представленные в виде m бит, поступают в динамический модулятор, в котором в соответствии с символами управляющей последовательности УФУП, осуществляется выбор 2^m из M сложных сигналов и таким образом устанавливается соответствие: m бит – 2^m сложных сигналов.

При появлении на входе динамического модулятора m бит сообщения в канал связи излучается сложный сигнал S_t, выбранный в зависимости от значения управляющей последовательности. По истечении времени T соответствие «m бит – 2^m сложных сигналов» изменяется по определенному закону (правилу).

Нарушитель, осуществляющий наблюдение за каналом связи, может реализовывать различные стратегии воздействия на систему связи: перехват переданных сигналов, их анализ, попытки распознавания сигналов и определения закона их излучения, формирование и постановка помех с целью навязывания ложных сообщений и др.

В демодуляторе на станции приема производится различение одного из 2^m разрешенных информационных сигналов. После демодуляции на выходе демодулятора формируются m бит сообщения, которые поступают получателю сообщений.

Естественным представляется постановка ряда вопросов, на которые необходимо дать ответы, если мы хотим построить систему связи, реализующую обсуждаемый метод передачи данных. Насколько устойчива система против раскрытия закона установления соответствия m бит сообщения – 2^m сложных сигналов, если нарушитель не ограничен временем и обладает всеми необходимыми средствами для анализа перехваченных сигналов. Имеет ли правило соответствия, которое использует нарушитель, единственное решение (j – вариант соответствия: m бит – сложный сигнал), и если нет, то сколько приемлемых решений возможно. Какой объем данных (число элементов физического носителя информации, сигнала) необходимо перехватить нарушителю, для того, чтобы решение стало единственно верным. Существуют ли системы, в которых вообще нельзя принять единственное правильное решение независимо от того, каков объем перехваченного в канале наблюдения.

Предположим, что имеется конечное число возможных дискретных сообщений $M_1, M_2, ..., M_N$ с априорными вероятностями

$$P(M_1), P(M_2), ..., P(M_N)$$

и что эти сообщения преобразуются в возможные сложные сигналы $S_1, S_2, ..., S_N$. После того как нарушитель перехватил некоторый сигнал, он имеет возможность вычислить апостериорные вероятности сообщений, содержащихся в принятом наблюдении.

Сформулируем необходимые и достаточные условия построения абсолютно стойкой системы на уровне источника сигналов.

Пусть каждые m бит источника сообщений в интервале T ставятся в соответствие 2^m сложных сигналов S, выбранных из пространства $\{S\}$ размерности $N \geq 2$, тогда необходимыми и достаточными условиями абсолютной стойкости на уровне источника сигналов являются условия:

$$P(M_i / S_i) = (M_i); \quad (1)$$

$$P(S_i / S_{i-1}, S_{i-2}, S_v, ..., S_1) = P(S_i). \quad (2)$$

Другими словами: вероятность появления сигнала в канале не должна зависеть от того, какое сообщение появилось на выходе источник S_i а и от того, какие сигналы до этого излучались. В этом случае перехват нарушителем сигнала не дает ему никакой информации, необходимой для определения содержания сообщения, содержащегося в полученных сигналах. С другой стороны, если эти условия равенства вероятностей не выполнены, то имеют место случаи, когда для определенного варианта соответствия m бит сообщения – 2^m сложных сигналов апостериорные вероятности, вычисленные нарушителя отличаются от априорных. А это, в свою очередь, может повлиять на выбор нарушителем своих действий и, таким образом, не обеспечит абсолютной стойкости системы.

Необходимое условие следует из теоремы Байеса, в соответствии с которой [2]:

$$P(M_i / S_i) = \frac{P(M_i) P(S_i / M_i)}{P(S_i)}, \quad (3)$$

где $P(M_i)$ – априорная вероятность (передачи сообщения M_i);

$P(M_i/S_i)$ – апостериорная вероятность сообщения M_i при условии, что перехвачен сигнал S_i;

$P(S_i/M_i)$ – условная вероятность сигнала S_i при условии, что выбрано сообщение M_i;

$P(S_i)$ – вероятность получения сигнала S_i.

Для обеспечения абсолютной стойкости системы должно быть выполнено одно из равенств: или

$$P(M_i) = 0,$$

или

$$P(S_i/M_i) = P(S_i),$$

тогда

$$P(M_i/S_i) = P(M_i) \quad [3]$$

и система обладает абсолютной стойкостью.

В этом случае количество информации, содержащейся у нарушителя $I(S/M)$ после перехвата сигнала:

$$\begin{aligned} I(S/M) &= H(M) - H(M/S) = \\ &= H(M) - H(M) = 0, \end{aligned} \tag{4}$$

где $H(M/S)$ – энтропия источника сообщения, при условиях, что перехвачен сигнал S;

$H(M)$ – энтропия источника открытого сообщения.

Условие (2) является достаточным условием абсолютной стойкости. В этом случае определение j – варианта соответствия может бить выполнено только методом статистического опробования всевозможных вариантов, т.е. методом перебора.

Как следует из (2), вероятность появления S_i сигнала не зависит от вероятности появления всех $i-1$ сигналов.

В этом случае количество информации в сигнале S_i после перехвата всех $i-1$ сигналов равно

$$\begin{aligned} I(S_i/S_v) &= H(S_i) - H(S_i/S_v) = \\ &= H(S_i) - H(S_v) = 0, \end{aligned} \tag{5}$$

где $v = \overline{1, i-1}$.

Из выражения (2) также следует равновероятность появление сигналов, (т.е. равновероятность отображение m бит – S_i сигнал), поэтому

$$H(S_i) = H(S_v). \tag{6}$$

Подставляя выражение (6) в выражение (5), получаем:

$$I(S_i/S_v) = 0.$$

Условие (2) является также и достаточным, так как независимость и равновероятность появления сигналов означает и равновероятность появления управляющей гаммы, символы которой статистически независимы и асимптотически равновероятны.

Сформулируем необходимое и достаточное условия абсолютной стойкости сигналов, формируемых источником сложных ФМ ШПС сигналов $\{S\}$. Под абсолютной стойкостью будем понимать их идеальную структурную скрытность.

Пусть $\{S\}$ – ансамбль ФМ ШПС сигналов объема N с числом разрядов L в каждом из них, тогда для обеспечения абсолютной стойкости каждого из $S_i \in \{S\}$ сложных ФМ ШПС необходимо и достаточно, чтобы

$$\begin{gathered} P(S_{j,i} / S_{v,R}) = P(S_{j,i}), \\ v = \overline{1,L}, R = \overline{1,N}, \end{gathered} \tag{7}$$

т.е. чтобы вероятность появления элемента $S_{j,i}$ сложного ФМ ШПС сигнала не зависела ни от элементов ранее переданных сигналов, ни от элементов $S_{j,i-1}, S_{j,i-2}, S_{j,v}, \ldots, S_{j,2}, S_{j,1}$ сигнала S_j.

Необходимость условия (7) следует непосредственно из критерия абсолютной структурной скрытности сигнала [7]:

$$S_c = 1/L, \tag{8}$$

где i – число символов сложного сигнала, которые необходимо знать для определения закона формирования оставшихся $L-i$ символов.

Если $i = L$, то

$$S_c = 1/L = L/L = 1.$$

Поэтому по любому числу перехваченных символов S_j сигнала нельзя предсказать последующие $L-1$ символов как сигнала, так и всех $S_v, v = \overline{1, i-1}, v \neq j$. Условие (7) является и достаточным.

Действительно, условная энтропия относительно закона формирования S_j сигнала после перехвата не менее R символов в v сигналах [6]

$$\begin{aligned} &H(S_{ji} / S_{v,k}) = \\ &= -\sum_{i=1}^{N} P(S_{j,i} / S_{v,k}) \log P(S_{j,i} / S_{v,k}), \end{aligned} \tag{9}$$

и среднее значение условной энтропии об источнике (законе формирования) сигналов [2, 5]

$$H\{S\}/\{S_v\} = -\sum_{j=1}^{v+1}\sum_{i=1}^{k} P\left(S_{j,i}/S_{v,k}\right)\times \times \log P\left(S_{j,i}/S_{v,k}\right); \quad (10)$$

вследствие справедливости (7) совпадает с априорной неопределенностью $H(\{S\})$ источника сигналов.

Поэтому количество информации, получаемое нарушителем при анализе (раскрытии закона формирования сигналов)

$$I(\{S\}/\{S_v\}) = H(\{S\}) - S(\{S\}/\{S_v\}) = H(\{S\}) - H(\{S\}) = 0.$$

Выводы

Анализ выражений (8) – (10) дает возможность сформулировать предложения по построению скрытной системы связи на основе использования сигналов с расширенным спектром и динамического режима передачи информации:

1. Закон формирования каждого из сигналов должен быть случайным, причем даже при перехвате $L-1$ из L символов сигнала не должно существовать единственного решения относительно закона его формирования.

2. Абсолютно стойким с точки зрения закона формирования является источник сигналов со случайным выбором сигналов из существующего ансамбля, так как только в этом случае у нарушителя отсутствует возможность принятия правильного решения относительно используемого в системе сигнала. Случайный выбор той или иной формы сигнала предполагает использование случайного закона формирования некой управляющей последовательности (УП), аналога ключевой последовательности для криптографических систем [4, 5].

Список литературы

1. Замула А.А. Предложения по построению широкополосных систем передачи со сложными сигналами / А.А. Замула // Радиотехника: всеукраинск. науч.-техн. сб. – 2012. – №171, вип. 4. – С. 177-185.

2. Борель Е. Вероятность и достоверность / Е. Борель. – 1969. – 126 с.

3. Shannon C.E. A mathematical theory of communication / C.E. Shannon // Bell System Technical Journal. – 1948. – № 27. – P. 379-423, 623-525.

4. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Видавництво «Форт», 2012. – 880 с.

5. Горбенко І.Д. Теоретичні основи побудови криптографічних систем абсолютної стійкості / І.Д. Горбенко, О.А. Замула // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 4 (111). – С. 101-105.

6. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон. – М.: Иностранная литература, 1963. – 830 с.

7. Горбенко И.Д. Защита ресурсов информационной системы на основе сложных сигналов. 4-й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития» / И.Д. Горбенко, А.А. Замула // Сб. науч. тр. Т. II. Междунар. конф. «Телекоммуникационные системы и технологи». – Х.: АНПРЭ, 2011. – С. 298-301.

Поступила в редколлегию 11.07.2014

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава.

УМОВИ РЕАЛІЗАЦІЇ ДИНАМІЧНОГО РЕЖИМУ ФУНКЦІОНУВАННЯ В СИСТЕМАХ ЗВ'ЯЗКУ

О.А Замула, Ю.В. Землянко, Є.О. Семенко, Д.О. Семченко

Розглянута можливість досягнення необхідних показників завадостійкості, скритності систем зв'язку на основі реалізації динамічного режиму функціонування системи зв'язку, при якому здійснюється зміна відповідності: біт повідомлення – складний сигнал відповідно до закону, передбачення якого можливо з ймовірністю, що не перевищує допустиму. Сформульовані необхідні та достатні умови побудови абсолютно стійкої системи на рівні джерела сигналів.

Ключові слова: *динамічний режим, завадостійкість, скритність, складний сигнал*

CONDITIONS OF DYNAMIC MODE FUNCTIONING REALIZATION IN COMMUNICATION SYSTEMS

A.A. Zamula, Y.V. Zemlianko, E.A. Semenko, D.A. Semchenko

The article focuses on the possibility to reach the required values of noise immunity, communication system security on the basis of realization of dynamic mode functioning in communication systems whereby change of message bit correspondence – complex signal by the law, the prediction of which is possible with a probability not exceeding the limits. Necessary and sufficient conditions of absolutely secure system construction on the level of signal source were formulated.

Keywords: *complex signal, dynamic mode, noise immunity, secrecy.*