УДК 621.391.7

Д. Г. ГАНШИН, А. А. ДУДКА, канд. техн. наук, А.Н. БИТЧЕНКО, канд. техн. наук, А. И. ЦОПА, д-р техн. наук

АНАЛИЗ СТРУКТУРНОЙ СКРЫТНОСТИ МНОГОЧАСТОТНЫХ СИГНАЛОВ ШИРОКОПОЛОСНЫХ СИСТЕМ СВЯЗИ

Введение

Обеспечение скрытности системы связи является одним из важнейших требований информационной безопасности ведомственных систем связи (ВСС). В данном случае под скрытностью понимается способность систем и средств радиосвязи противостоять радиотехнической разведке, которая предполагает последовательное выполнение трех основных задач: выявление факта работы системы связи (обнаружение сигнала); определение структуры обнаруженного сигнала и его основных параметров; раскрытие передаваемой информации. Противодействие этим задачам и определяет различные виды скрытности: энергетическую, пространственную, поляризационную, временную, структурную, информационную и др. При этом задачи по обеспечению скрытности ВСС ставятся, как правило, на сигнальном уровне, что предполагает выбор соответствующих характеристик и параметров сигнала, которые являются переносчиками информации [1 – 2].

При оценке скрытности сигналов используются два основных подхода. В первом (назовем его вероятностным) скрытность определяется как вероятность успешного выявления сигнала в заданное время. Однако это прежде всего мера успеха разведки, а не усилий, направленных на выявление состояния объекта. Кроме того, вероятностная мера скрытности неудобна численно, например, значения вероятностей успеха 0,94 и 0,99 близки, однако для их достижения могут потребоваться различные временные затраты [3].

Второй подход предполагает оценивать скрытность сигнала через затраты на выявление его состояния с заданной достоверностью (вероятностью правильного решения). Он точнее отражает существо термина «скрытность»; чем больше затраты, чем труднее выявить сигнал, тем лучше оно «спрятано» от радиотехнической разведки. В данной работе скрытность будем оценивать в рамках такого «затратного» подхода.

При раскрытии неопределенности состояния сигнала необходимо произвести соответствующие временные и аппаратные затраты. Очевидно, что при использовании для каждого состояния своего отдельного устройства обнаружения (параллельное одновременное измерение) результат будет получен наиболее быстро, но при максимальных аппаратных затратах. Если же использовать лишь один двоичный измеритель, то для выявления сигнала необходимо организовать поисковую процедуру, последовательно перебирая подмножества состояний сигнала. В этом случае аппаратные затраты минимальны, но поиск требует соответствующего времени. Теоретический анализ показывает [4], что параллельное и последовательное обнаружение сигнала имеет общие свойства и аппаратные затраты можно связать с временными, и наоборот.

Для обеспечения единообразия при оценке скрытности различных объектов (сигналов) целесообразно в качестве базового выбрать поисковый алгоритм обнаружения сигнала с одним двоичным измерителем (ДИ) и определить потенциальную структурную скрытность, которая не требует знания алгоритма обработки сигнала в приемнике-обнаружителе нарушителя [5, 6].

В беспроводном сегменте ВСС для передачи мультимедийной информации широко используются широкополосные системы связи с ортогональным частотным разделением каналов *OFDM* (*Orthogonal Frequency-Division Multiplexing*) [7 – 9]. Эти системы в основном зарубежного производства, со своими уровнем безопасности и алгоритмами взаимодействия.

Цель работы – оценка потенциальной структурной скрытности широкополосных многочастотных сигналов современных систем связи, определение путей ее увеличения при использовании таких сигналов в современных защищенных ВСС.

Основная часть

В ходе радиоэлектронной борьбы разведывательная система стремится выявить рабочие параметры системы радиосвязи, которая, в свою очередь, стремится затруднить разведку, управляя распределением вероятностей своих состояний. При этом можно установить распределение вероятностей рабочих параметров системы связи таким образом, что даже при оптимальных действиях противника его затраты на поиск будут максимально возможными.

Для решения этой задачи можно использовать понятие потенциальной скрытности. При выбранных параметрах системы связи определяется потенциальная скрытность и соответствующий оптимальный алгоритм поиска. Далее, изменяя параметры, определяют условия, при которых потенциальная скрытность максимальна.

Известно [3], что потенциальная скрытность *S*, численно равна минимально достижимому (минимум-миниморум по всем реализуемым алгоритмам поиска) среднему числу двоичных измерений, необходимому и достаточному для раскрытия всех возможных состояний объекта:

$$S = \min_{\sigma_K} R(\sigma_K), \tag{1}$$

где R – среднее число двоичных измерений, необходимых для выявления сигнала при заданном алгоритме поиска σ_K.

В данном случае идет речь о согласованном с объектом алгоритме поиска, обеспечивающем искомый минимум зависимости *R* от σ_K.

Потенциальная скрытность является характеристикой собственно объекта исследования (в нашем случае сигнала), его выраженным в числовой форме качеством, способностью противостоять выявлению текущего состояния. Потенциальная скрытность сигнала не зависит от действий системы выявления его состояний, так как предполагает использование оптимального алгоритма поиска. Фактически она является наиболее «*осторожной*» оценкой скрытности.

Потенциальная структурная скрытность зависит от ансамбля (арсенала) A реализаций сигнала и определяется числом двоичных измерений (диз), которые необходимо осуществить для раскрытия структуры широкополосного сигнала. Общее выражение для потенциальной структурной скрытности имеет вид [3]:

$$S_P = \log_2 A \text{ [диз]}, \tag{2}$$

где A – ансамбль (арсенал) реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала.

Такими параметрами сигнала могут быть несущая частота, амплитуда, вид модуляции, структура линейного кода, параметры формы и временные характеристики сигнала, а также другие специфические параметры, зависящие от физического уровня конкретной технологии передачи сигналов. Скрытность зависит от способа построения конкретного вида сигнала, используемого для переноса информации.

Так как в современных широкополосных системах связи используются составные сложные сигналы, то структурная скрытность будет суммой структурной скрытности отдельных элементов сигнала [1]:

$$S_\Sigma = S_1 + S_2 + .. + S_i = \log_2 A_1 + \log_2 A_2 + ... + \log_2 A_i \text{ [диз]}, \tag{3}$$

где A_1, A_2, . . ., A_i – количество (арсенал, ансамбль) всех возможных значений каждого из *i*-параметров составного сигнала. Для широкополосных сигналов арсенал возможных значений определяется базой сигнала $A_{ШПС} \approx B$.

Далее рассмотрим особенности формирования сигналов с ортогональным частотным разделением каналов *OFDM*, являющихся переносчиками информации в современных цифровых системах радиосвязи высокой пропускной способности и защищенности. Сигналы *OFDM* обладают следующими положительными свойствами: устойчивостью к многолучевому распространению, эффективным использованием частотного ресурса, возможностью адаптации под текущие условия передачи. Но наряду с преимуществами, *OFDM* сигнал обладает рядом недостатков: чувствительность к точности частотной синхронизации, связанная с близким расположением соседних поднесущих; большой пик-фактор сигнала, вызванный наличием большого количества поднесущих в сигнале; сложность аппаратной реализации, обусловленная наличием большого числа вычислений при обработке сигнала.

При формировании *OFDM*-сигнала последовательный цифровой поток данных делится в модуляторе на *N* подпотоков, из которых формируется один *OFDM* символ. Частотный разнос *f* между соседними несущими *f1, f2 ... f_N* в групповом радиоспектре *OFDM* выбирается из условия возможности выделения в демодуляторе индивидуальных несущих. Ортогональный метод демодуляции поднесущих группового спектра позволяет компенсировать помехи от соседних частот, несмотря на то, что их боковые полосы взаимно перекрываются. Кроме того, благодаря тому, что используется большое число параллельных потоков, длительность одного символа в параллельных потоках оказывается существенно большей, чем в последовательном потоке данных. При этом длительность канальных символов должна быть больше времени задержки сигнала в канале связи, что позволяет эффективно бороться с межсимвольной интерференцией (МСИ).

Для *OFDM* сигнала, сгенерированного *OFDM*-системой с *N* поднесущими $\{f_1, f_2, ..., f_N\}$, комплексная огибающая сигнала на интервале T описывается выражением [10]:

$$s(t) = A \cdot \sum_{n=1}^{N} x_n \cdot e^{\frac{j2\pi nt}{T}}, \qquad (4)$$

где A – амплитуда сигнала; x_n – символы данных; N – количество поднесущих частот.

Структура спектра одного *OFDM*-символа, представленная на рис. 1, содержит несколько групп поднесущих частот: центральная несущая (1), поднесущие передачи информации, пилот-тоны и поднесущие частоты защитного интервала.

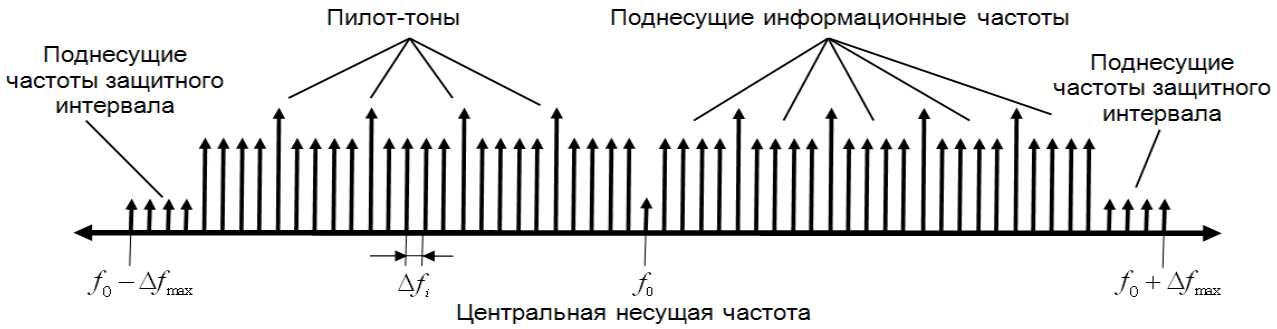

Рис.1. Структура спектра одного *OFDM*-символа

Передача *OFDM* символов по радиоканалу осуществляется кадрами *(frame)* t_{FR} определенной длительности, содержащими L отдельных *OFDM* символов (рис. 2).

Рассмотренная схема формирования *OFDM* сигналов позволяет оценить и его структурную скрытность с учетом возможного арсенала значений параметров данного сигнала.

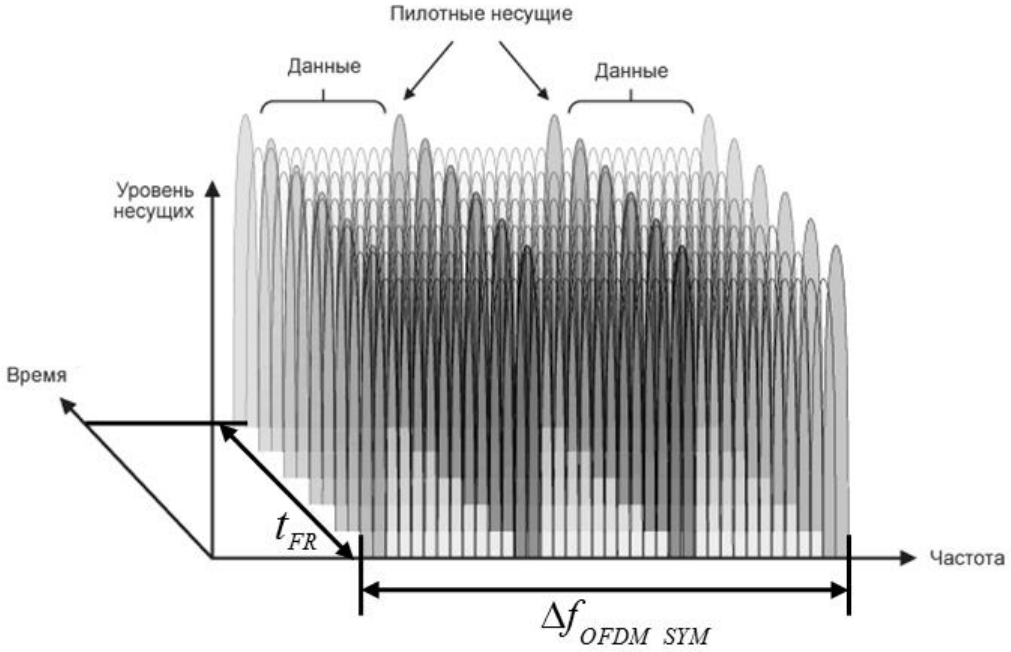

Рис. 2. Структура *OFDM* фрейма

Учитывая, что база сигнала *OFDM* приблизительно равна количеству поднесущих $B_C \approx N$, то потенциальная скрытность сигнала

$$S_{OFDM} = \log_2(N) \text{ [диз]}. \quad (5)$$

В зависимости от качества беспроводного канала связи каждая из N поднесущих частот использует *QAM* модуляцию со своим уровнем модуляции M_i, т.е. каждая поднесущая f_i несет n_i бит информации. Уровень *M* задает количество различных значений вектора модулированного сигнала, т.е. $M = 2^n$ – размерность ансамбля сигналов, где $n = 2,3,...8$. Тогда для сигнала *QAM-M* количество вариантов соответствия каждой точке сигнального ансамбля символа, который состоит из n бит, составляет M без учета ограничений кода Грея.

Соответственно, структурная скрытность сигнального созвездия *QAM-M*

$$S_{QAM} = \log_2(M) \text{ [диз]}. \quad (6)$$

Тогда потенциальная скрытность сигналов *OFDM* с модуляцией *QAM-M*

$$S_{OFDM\ QAM} = \log_2(N) + \log_2(M). \quad (7)$$

Как видно из выражения (7), скрытность сигналов *OFDM* повышается с увеличением числа N поднесущих частот f_i и существенно зависит от размерности M модуляции *QAM*.

Арсенал сигналов *OFDM* можно существенно повысить, если использовать методы псевдослучайного изменения нескольких параметров сигнала как по частоте, так и по времени.

На рис. 3 представлена структурная схема системы связи, позволяющая существенно повысить защищенность системы от перехвата информации при использовании *OFDM* сигналов.

Информацию, которую необходимо передать поступает в кодер *И*, в котором формируется помехоустойчивая последовательность за счет внесения определенной избыточности в передаваемую информацию. На выходе кодера получается последовательный поток данных.

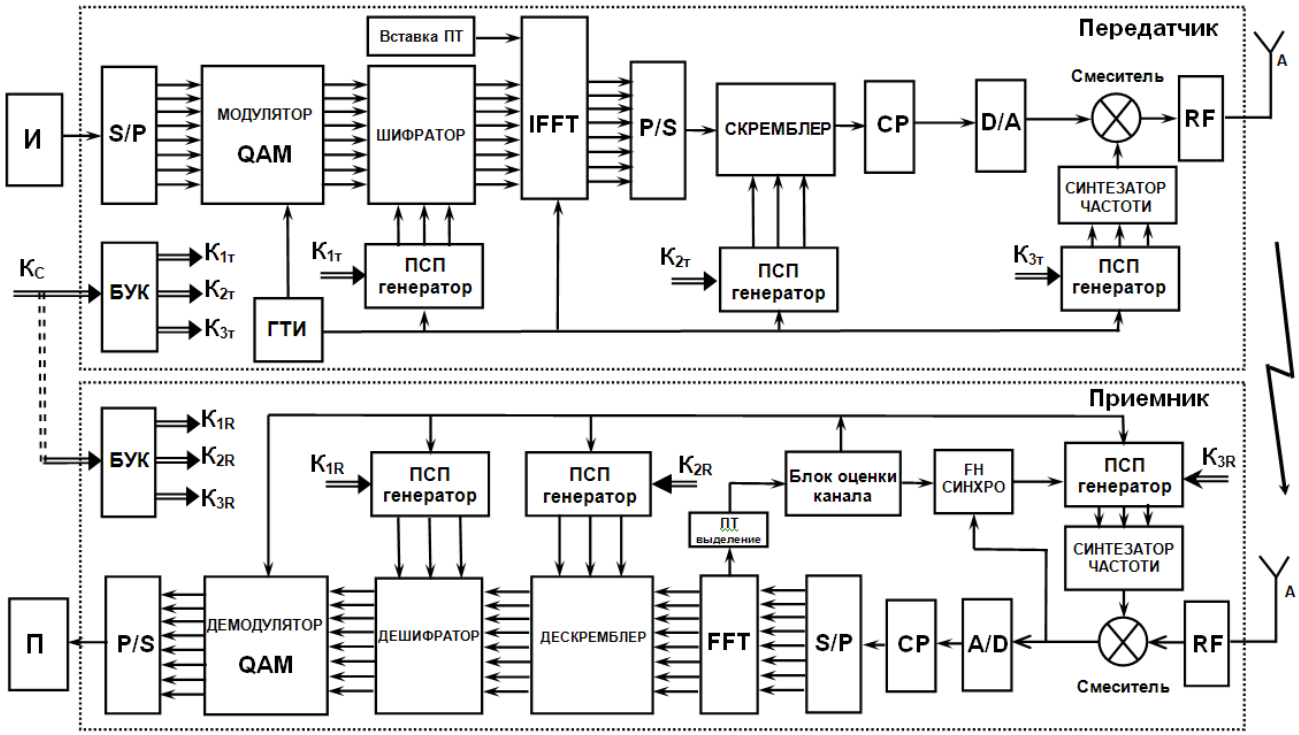

Рис. 3. Структурная схема системы связи с защитой от перехвата информации при использовании *OFDM* сигналов

Последовательный поток данных поступает в последовательно-параллельный блок (*S/P*), после которого формируются параллельные потоки данных. Параллельные потоки поступают в модулятор *QAM*, каждый поток модулируется разным уровнем *QAM* модуляции в зависимости от заданного соотношения сигнал/шум (*SNR*). Параллельные модулированные потоки поступают в шифратор, который выполняет шифрование параллельных потоков в псевдослучайную последовательность символов. Псевдослучайная последовательность формируется в блоке генератор псевдослучайной последовательности (*ПСП*), в свою очередь генератор *ПСП* управляется ключом K_{1T}. После шифратора параллельные потоки поступают в блок обратного преобразования Фурье (*IFFT*). К блоку *IFFT* подключен блок вставки пилот тона (*ПТ*) для получения пилот тона. На выходе *IFFT* формируются поднесущие, которые поступают в параллельно-последовательный (*P/S*) блок для получения последовательного потока символов. Последовательный поток поступает в скремблер, который формирует псевдослучайную последовательность символов. Псевдослучайная последовательность скремблера задается генератором *ПСП*, который управляется ключом K_{2T}. Блок (*СР*) добавляет защитный интервал. После добавления защитного интервала последовательный поток поступает в блок (*D/A*) цифро-аналоговый преобразователь, в котором формируется аналоговый сигнал определенного вида модуляции, в зависимости от типа системы связи. На выходе смесителя получаем сигнал с псевдослучайной перестройкой частоты, который поступает в радиочастотный процессор (*RF*) после чего на антенну (*А*). Синтезатор частоты управляется генератором *ПСП*, который управляется ключом K_{3T}. Ключи K_{1T}, K_{2T}, K_{3T}, формируются в блоке управление ключами (*БУК*) псевдослучайным образом.

Переданный передатчиком сигнал поступает на приемную антенну (*А*) далее сигнал поступает в блок радиочастотный процессор (*RF*) затем в смеситель. В смесителе поступает сигнал с псевдослучайной частотой, для восстановления сигнала на каждой несущей частоте

необходимо, чтобы генератор *ПСП* был синхронизирован с генератором *ПСП* передающей части, ключ K_{3R} соответствовал ключу K_{3T}, после чего синтезатор частоты приемной части будет синхронизирован с синтезатором передающей части. Блок (*FH*) отвечает за эту синхронизацию. После выделения сигнала на одной несущей частоте, сигнал поступает в блок (*A/D*) аналого-цифрового преобразователя, после которого формируется последовательный поток символов с защитным интервалом. Последовательный поток с защитным интервалом поступает в блок удаления защитного интервала (*CP*), после которого последовательный поток поступает в блок (*S/P*) последовательно-параллельного преобразования, на выходе которого получаем параллельные потоки, затем параллельные потоки поступают в блок (*FFT*) быстрого преобразования Фурье, где происходит выделение пилот тона. На выходе блока дескремблера получаем восстановленную последовательность символов. Для получения восстановленной символьной последовательности необходимо, чтобы ключ K_{2R} соответствовал ключу K_{2T}, ключ K_{2R} управляет генератором *ПСП*, который в свою очередь задает алгоритм дескремблера. После восстановления символьной последовательности ее необходимо дешифровать в блоке дешифратор. Дешифратор восстанавливает последовательность параллельных потоков. Дешифратор управляется генератором *ПСП*, ключ K_{1R} должен соответствовать ключу K_{1T}. Восстановленные параллельные потоки поступают в *QAM* демодулятор, на выходе которого получаем параллельные потоки данных. После чего параллельные потоки данных поступают в блок (*P/S*) параллельно последовательный преобразователь, на выходе которого получаем последовательный поток данных. Последовательный поток данных поступает в декодер (*П*), в котором убираем определенную избыточность, после чего на выходе получаем передаваемую информацию.

Псевдослучайная перестановка передаваемых символов между поднесущими частотами f_i, согласованная между передатчиком и приемником. В этом случае арсенал $A_{OFDM} = N!$ и потенциальная структурная скрытность увеличивается $S_{OFDM} = \log_2(N!)$.

Псевдослучайная перестановка времени (ПСПВ) появления отдельных символов *OFDM* в общем фрейме (кадре) *OFDM*, согласованная между передатчиком и приемником. Общее количество символов *OFDM* в одном фрейме L. Это дает возможность увеличить потенциальную скрытность сигналов *OFDM* $S_{ПСПВ} = \log_2(L!)$.

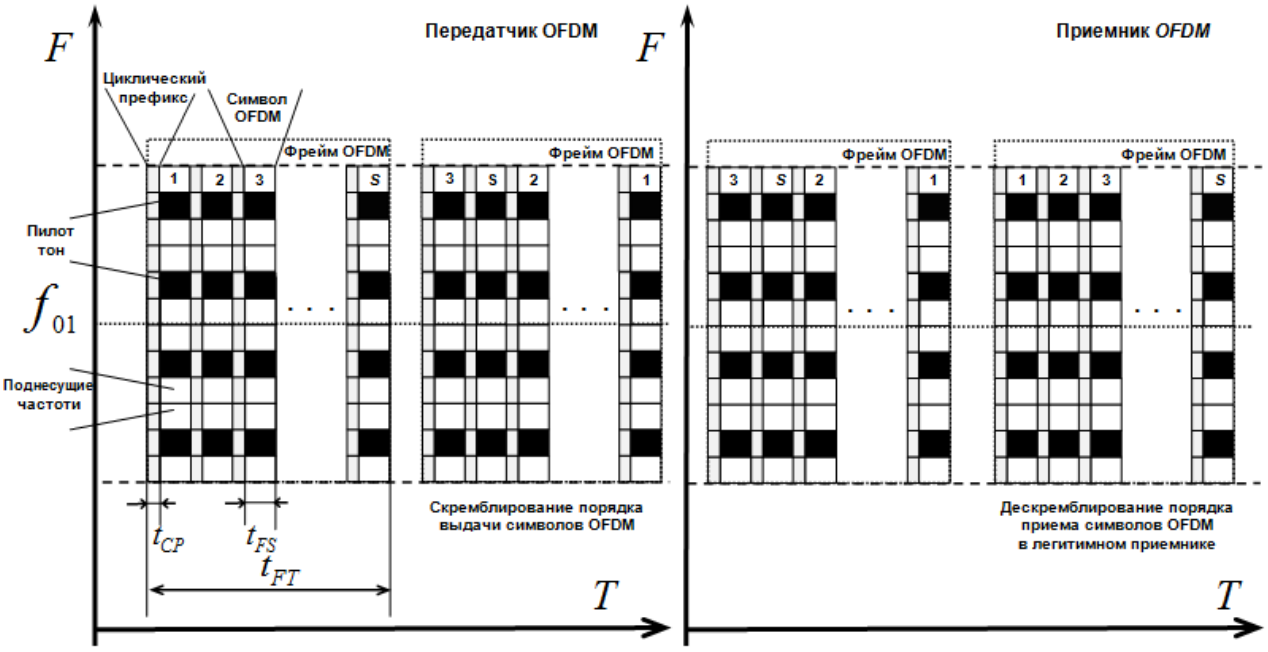

Рис. 4. Частотно-временная диаграмма псевдослучайной перестановки времени (ПСПВ) выдачи символов *OFDM* при скремблировании

Псевдослучайная перестройка частоты (ПСПЧ) поднесущих по согласованному закону между передатчиком и приемником. Это позволит значительно увеличить потенциальную скрытность сигналов *OFDM* $S_{ПСПЧ} = 0,697 \cdot B \cdot \log_2(B)$ [11].

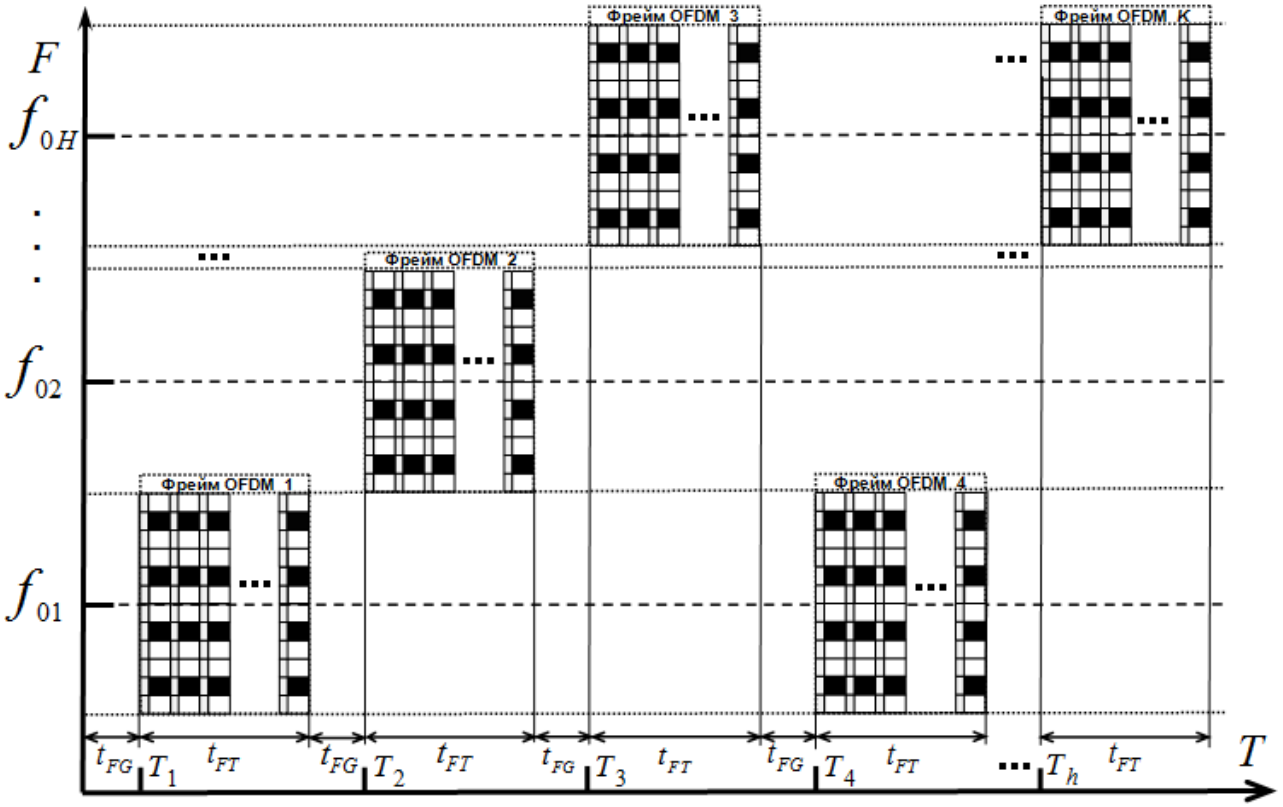

Рис. 5. Частотно-временная диаграмма передачи фреймов *OFDM* при использовании псевдослучайной перестройки частоты (ПСПЧ)

Используя приведенные выше выражения для потенциальной скрытности отдельных параметров *OFDM* сигналов, проведем общую оценку скрытности сигналов системы связи *FH-OFDM* с защитой от перехвата информации.

Потенциальная скрытность будет определяться арсеналом состояний всех составляющих сигнала

$$\begin{aligned} S_{FH\ OFDM} &= S_{OFDM} + S_{QAM} + S_{ПСПВ} + S_{ПСПЧ} = \\ &= \log_2(N!) + \log_2(M!) + \log_2(L!) + 0,697 \cdot B \cdot \log_2(B). \end{aligned} \quad (8)$$

В таблице приведены данные о потенциальной структурной скрытности сигналов современных беспроводных систем связи: *Wi-Fi*, *WiMAX*, *LTE*, *DBV* [11].

Полученные данные свидетельствуют о высокой потенциальной структурной скрытности сигналов современных цифровых технологий передачи информации по беспроводным каналам связи. Особенно это относится к технологии передачи цифрового телевизионного вещания *DBV*, использующей для передачи информации большое количество поднесущих частот и высокие уровни модуляции *QAM*.

Для увеличения структурной скрытности сигналов ВСС необходимо не только, по возможности, расширять ансамбли применяемых сигналов, но и использовать оригинальные методы формирования сигнального созвездия в системах связи собственной разработки, что позволит применять *OFDM* технологии в беспроводных сегментах ведомственных систем связи для доступа к специализированным базам данных и передачи служебной информации.

Вид технологии	Тип сигнала	Количество поднесущих частот *N*	Уровень модуляции *M-QAM*	Длина *L* фрейма *OFDM*	ПСПЧ *B*	Скрытность S, диз
Wi-Fi IEEE.802.11	*OFDM*	64	16	80	-	16
WiMAX IEEE.802.16d	*OFDM*	256	256	40	-	21
WiMAX IEEE.802.16e	*OFDM*	512	256	40	-	22
LTE	*OFDM*	1024	256	120	-	25
DBV-T	*OFDM*	6800	64	40	-	24
DBV-T2	*OFDM*	32000	256	40	-	25
Система FH-OFDM	*OFDM*	2048	256	120	100	22387

Заключение

1. На основе известной методики проведена оценка потенциальной структурной скрытности многочастотных сигналов беспроводных систем связи и получены новые данные о структурной скрытности сигналов современных *OFDM* технологий.

2. Для увеличения структурной скрытности сигналов, которые используются в *OFDM* технологиях, необходимо, по возможности, расширять ансамбль используемых сигналов, в том числе используя дополнительные возможности физического уровня этих технологий. Предложена структура системы связи с защитой от перехвата информации при использовании *OFDM* сигналов.

3. Для увеличения защищенности ВСС необходимо использовать отечественные системы связи, в которых могут быть реализованы оригинальные алгоритмы повышения структурной скрытности сигнала на основе псевдослучайного изменения временных и частотных параметров сигналов *OFDM* на основе общего системного ключа.

Список литературы: 1. *Методы* прогнозирования защищенности ведомственных систем связи, основанные на концепции отводного канала ; под ред. *А. И. Цопы и В. М. Шокало*. – Харьков : КП «Городская типография», 2011. – 502 с. 2. *Tsopa O. I.* Enthropian estimation of immunity in communication systems / Makarov L. B., Bitchenko A. M., Tsopa O. I., *Kuznetsov A. A.* // Telecommunication and Radio Engineering. – Begell House, 2014. – Vol. 73(17). – P. 1561-1573. 3. *Каневский З. М.* Теория скрытности / З. М. Каневский, В. П. Литвиненко. – Воронеж : ВГУ, 1991. – 144 с. 4. *Тузов Г. И.* и др. Помехозащищенность радиосистем со сложными сигналами. – М. : Радио и связь, 1985. – 264 с. 5. *Захарченко Н. В.* Структурная скрытность таймерных сигналов в системах с кодовым разделением сигналов / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-европейский журнал передовых технологий. – 2011. – №2/9(50). – С. 7-9. 6. *Кувшинов О. В., Вознюк Р. В.* Оцінка структурної скритності широкосмугових сигналів // Зб. наук. праць ВІТІ НТУ «КПІ». – 2011. – № 1. – С. 106-111. 7. *Григорьев В. А., Лагутенко О. И., Распаев Ю. А.* Сети и системы радиодоступа. – М. : Эко-Трендз, 2005. – 384 с. 8. *Сюваткин В. С., Есипенко В. И., Ковалев И. П., Сухоребров В. Г. WiMAX* – технология беспроводной связи: теоретические основы, стандарты, применение. – Сн.Пб. : БХВ-Петербург, 2005. – 268 с. 9. *Ганшин Д. Г.* Исследование защищенности системы связи с многочастотными сигналами / Д. Г. Ганшин, В. В. Маслий, А. И. Цопа // Радиотехника. – 2013. – Вып. № 173. – С. 195-203. 10. *IEEE 802.16-2009*. IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. 11. *Борисов В. И.* и др. Помехозащищенность систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты. – М. : Радио и связь, 2000. – 384 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 12.02.2016