

УДК 621.391.372.019

СИСТЕМА РАДИОСВЯЗИ С ПРИМЕНЕНИЕМ МЕТОДОВ РАСШИРЕНИЯ СПЕКТРА СИГНАЛОВ

Козленко Н.И., Мокроусов А.Н.

Методы передачи информации с применением расширения спектра сигналов

Обеспечение конфиденциальности связи с одновременным повышением её помехозащищённости является одним из основных направлений развития средств специальной связи. В подвижных системах радиосвязи и беспроводных локальных сетях находят применение методы расширения спектра с использованием ПСП или ППРЧ [1]. Потенциальные преимущества каждого из этих методов [2] предполагают необходимость их комплексного применения, что на сегодняшний день является практически реализуемым в связи с непрерывным развитием элементной базы.

Однако, главным недостатком существующих на сегодня методов помехозащиты (в дальнейшем – СП) с использованием ПСП и ППРЧ является то, что по каналу связи авторизованным пользователям передаётся само информационное сообщение, что позволяет неавторизованным пользователям при перехвате даже очень малого числа пакетов (составляющих небольшой процент от всего сообщения) с большой долей вероятности восстанавливать всё сообщение. Кроме того, при этом сообщение мало защищено от воздействия преднамеренных помех, а применение помехоустойчивого кодирования снижает скорость передачи информации. Таким образом, недостатком СП является отсутствие защиты передаваемого сообщения от несанкционированного прослушивания и низкая помехоустойчивость.

Идея предлагаемого метода (в дальнейшем обозначаемого как МП – метод передачи) в общем виде представляется следующим образом:

1) на передающем конце радиолинии со скачкообразной перестройкой рабочей частоты в пакетаторе происходит преобразование информационной последовательности в пакеты информации, представленной в двоичном виде (X бит)

2) полученное двоичное число Z пересчитывается в десятичное число $Y \in [0, 2^X - 1]$;

3) Y шифруется в другие десятичные числа $N_{ш1} = f_1(Y) \in [0, 2^X - 1]$ и $N_{ш2} = f_2(Y) \in [0, 2^X - 1]$, где f_1 и f_2 – известные на приёме и передаче алгоритмы;

4) $N_{ш1}$ и $N_{ш2}$ определяют десятичные числа $N_{ПСП} = g(N_{ш1}) \in [0, 2^M - 1]$, $M \geq X$, и $F_{ППРЧ} = h(N_{ш2}) \in [0, 2^K - 1]$, $K \geq X$, где g и h – известные на приёме и передаче алгоритмы;

5) по $N_{ПСП}$ и $F_{ППРЧ}$, согласно кодовым книгам определяются код ПСП и несущая частота;

6) полученная несущая частота передатчика модулируется полученным кодом ПСП с последующим излучением его в пространство;

Предлагается новый метод передачи информации с повышенной скрытностью и помехоустойчивостью в системах связи. Представлены функциональные схемы устройств, реализующих данный метод. Приводится описание системы радиосвязи с применением предложенного метода, расчетные выражения для оценки вероятности правильного приема и результаты моделирования.

7) на приёмном конце осуществляется приём сигнала одновременно на всех возможных частотах и для всех возможных кодов ПСП;

8) выбор того частотного канала, по которому производилась передача и выбор переданного ПСП;

9) на основе переданного ПСП определяется десятичное число $N_{ПСП}$ согласно кодовым книгам;

10) определяется десятичное число $N_{ш} = g^{-1}(N_{ПСП})$;

11) определяется десятичное число $Y = f^{-1}(N_{ш})$;

12) пересчитывается число Y из десятичного вида в двоичный Z ;

13) полученное значение Z представляется в виде блока информации;

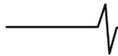
14) в депакетаторе происходит объединение полученных двоичных блоков в информационную последовательность и подача её на оконечное устройство.

Таким образом, представленный алгоритм МП исключает передачу самого информационного сообщения по каналу связи. Вместо этого передаётся ПСП, что при поэлементном накоплении на приёме значительно повышает помехоустойчивость.

Практическая реализация предложенного метода

Один из возможных вариантов функциональной схемы устройства для осуществления МП представлен на рис.1, где введены следующие обозначения:

- 1 – источник информации (ИИ);
- 2 – пакетатор-депакетатор (ПД);
- 3 – модулятор;
- 4 – первый антенно-фидерный блок (АФБ1);
- 5 – синхрогенератор;
- 6 – приёмник информации (ПИ);
- 7 – синтезатор частот (СЧ);
- 8 – первый блок памяти (БП1);
- 9 – генератор кода (ГК);
- 10 – микропроцессор;
- 11 – пороговый блок;
- 12 – второй блок памяти (БП2);
- 13₁-13_к – корреляторы;
- 14₁-14_к – частотные фильтры (ЧФ);
- 15 – второй антенно-фидерный блок (АФБ2).



Устройство работает следующим образом. На передающем конце входной сигнал поступает в ИИ, с выхода которого двоичная информационная последовательность поступает в ПД, где происходит её деление на двоичные блоки по X бит, составляющих двоичное число Z . С первого выхода ПД информационные блоки подаются на первый вход микропроцессора, в котором производятся следующие преобразования: двоичное Z пересчитывается в десятичное число Y , которое, в свою очередь, переводится в другие десятичные числа N_1 и N_2 , которые соответственно определяют десятичные числа $N_{ПСП}$ и $F_{ППРЧ}$.

По $N_{ПСП}$ в БП1 определяется код ПСП, а по $F_{ППРЧ}$ в БП2 - несущая частота. Определённый в БП1 код ПСП (M бит) генерируется в ГК и подаётся на информационный вход модулятора, где он модулируется частотой, синтезируемой СЧ на основе определённой в БП2 несущей частоты передатчика. Модулированная ПСП излучается в пространство с помощью АФБ1.

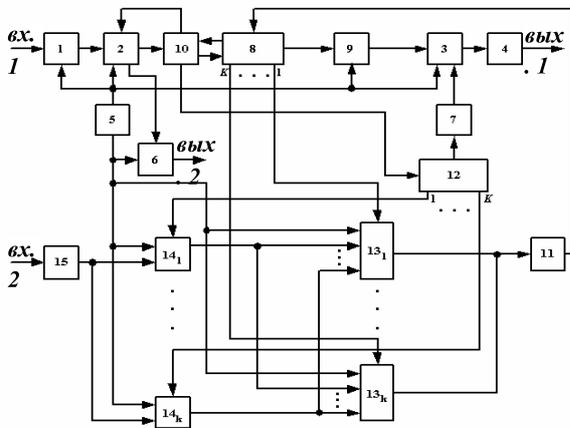


Рис. 1

На приёмном конце радиопередачи входной сигнал, принятый АФБ2, поступает на информационные входы ЧФ, где происходит выбор того частотного канала, по которому производилась передача. Каждый из ЧФ настроен на частоту ($F_{ППРЧ}$), значение которой хранится в БП2. При этом, коды с k параллельных выходов БП2 подаются на управляющие входы соответствующих ЧФ, на синхронизирующие входы которых подаётся синхросигнал со второго выхода синхрогенератора.

С выходов ЧФ принятый сигнал поступает на соответствующие параллельные входы корреляторов, где определяются корреляционные пики. Каждый коррелятор настроен на определённую опорную ПСП, значение которой хранится в БП1. С k параллельных выходов БП1 управляющие сигналы поступают на последовательные входы соответствующих корреляторов.

Значение пика АКФ на выходах корреляторов сравнивается с порогом в блоке 11. Номер коррелятора, имеющего максимальное значение АКФ, определяет вид ПСП, по которому в БП1 определяется $N_{ПСП}$, который со второго последовательного выхода БП1 подаётся на второй вход блока 10. В микропроцессоре на основе десятичного числа $N_{ПСП}$ сначала определяется десятичное число $N_{ин}$, а затем определяется десятичное число Y , которое переводится из десятичного вида в двоичный Z , который подаётся на третий вход ПД, где преобразуется в X бит двоичного блока. Полученные таким образом двоичные блоки объединяются в ПД в двоичную информационную последовательность, которая

со второго выхода ПД подаётся на информационный вход ПИ, где преобразуется в форму выходного сигнала и подаётся на второй выход устройства.

При этом работа ПИ синхронизируется сигналом со второго выхода синхрогенератора, а сигнал с первого выхода синхрогенератора синхронизирует работу ИИ, ПД, ГК и модулятора.

Использование в предлагаемом устройстве корреляторов позволяет поэлементно накапливать принятый сигнал, что обеспечивает защиту от воздействия преднамеренных помех. Использование блоков памяти позволяет идентифицировать код ПСП и рабочую частоту, а использование микропроцессора - проводить многократные преобразования передаваемого и принимаемого сигналов, что обеспечивает защиту от несанкционированного доступа.

Таким образом, устройство для реализации МП позволяет обеспечить высокую помехоустойчивость при соблюдении конфиденциальности.

Частными случаями МП могут быть случаи, когда с целью упрощения аппаратуры передачи и приёма на этапе 5 алгоритма МП принимаются или $N_{ПСП} = \text{const}$ (метод МП1), или $F_{ППРЧ} = \text{const}$ (метод МП2).

Схемы устройства для осуществления МП1 приведены на рис.2 и рис.3.

На рис.2 - схема передающего устройства, где:

- 1 - источник цифрового сигнала;
- 2 - блок формирования периодической последовательности видеопульсов, частота следования которых равна тактовой частоте передаваемого цифрового сигнала;
- 3 - блок формирования периодической последовательности видеопульсов, период повторения которых равен длительности кодовой комбинации;
- 4 - блок формирования кодовых комбинаций;
- 5 - блок шифрования кодовых комбинаций;
- 6 - перестраиваемый синтезатор частот;
- 7 - опорный генератор частоты;
- 8 - усилитель мощности.

На рис.3 - схема приемного устройства, где обозначено:

- 1 - блок усиления и преобразования входных сигналов в сигналы промежуточных частот;
- 2 - широкополосный фильтр промежуточной частоты;
- $3^1, 3^2, \dots, 3^k, \dots, 3^N$ - узкополосные полосовые фильтры рабочих частот;
- $4^1, 4^2, \dots, 4^k, \dots, 4^N$ - демодуляторы;
- 5 - устройство памяти зашифрованных кодовых комбинаций;
- 6 - дешифратор;
- 7 - сумматор.

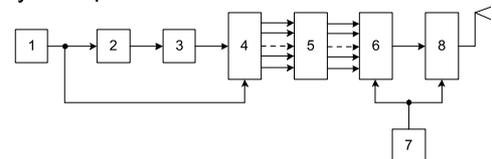


Рис. 2

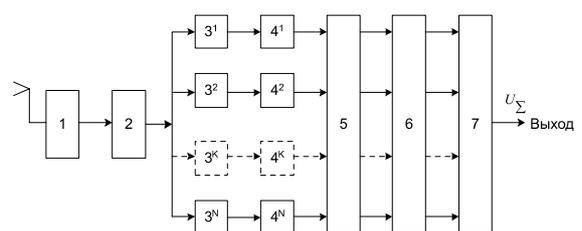


Рис. 3

Работа устройства происходит следующим образом. На передающей стороне (рис.2) с выхода источника цифровой сигнал поступает на вход блока 2, в котором из приходящего сигнала формируется периодическая последовательность видеоимпульсов, частота следования которых равна тактовой частоте (частота дискретизации) передаваемого цифрового сигнала $f_T = \frac{1}{T}$, где T – период повторения тактовых импульсов. Затем с выхода блока 2 полученная периодическая последовательность видеоимпульсов поступает на вход блока 3, в котором эта последовательность импульсов преобразуется в периодическую последовательность видеоимпульсов с периодом повторения равным длительности кодовой комбинации $T_K = nT$, где n – значность двоичного кода, то есть число импульсов кодовой комбинации. Полученная периодическая последовательность видеоимпульсов с выхода блока 3 поступает на вход блока 4, на другой вход которого подается цифровой сигнал с выхода блока 1. В блоке 4 осуществляется формирование двоичных кодовых комбинаций длительностью $T_K = nT$, которые с n выходов блока 4 подаются на соответствующие входы блока 5, в котором осуществляется шифрование поступающих кодовых комбинаций цифрового сигнала, то есть каждая поступающая двоичная кодовая комбинация сигнала заменяется на другую двоичную кодовую комбинацию в соответствии с заданным законом шифрования. Таким образом, полученные зашифрованные кодовые комбинации с выходов блока 5 поступают на соответствующие входы блока 6, на другой вход которого поступает сигнал опорной частоты с выхода блока 7. В блоке 6 каждой зашифрованной кодовой комбинации присваивается соответствующий номер промежуточной рабочей частоты, для этого двоичные значения зашифрованных кодовых комбинаций в блоке 6 преобразуются в десятичные значения, которым по заданному закону присваиваются соответствующие десятичные значения промежуточных рабочих частот, сигналы которых с выхода перестраиваемого синтезатора частот поступают на вход усилителя мощности, на опорный вход которого подается сигнал опорной частоты с выхода блока 7. В усилителе мощности сигналы промежуточных частот преобразуются в сигналы несущих частот, которые излучаются в пространство каждая в течение времени, равном длительности зашифрованных кодовых комбинаций $T_K = nT$.

Таким образом, осуществляется передача по радиоканалу только несущих частот вместо исходного цифрового сигнала, что практически полностью исключает возможность перехвата сигнала информации потенциальным разведприемником и обеспечивается структурная и информационная скрытность передаваемого цифрового сигнала.

На приемной стороне (рис.3) входные сигналы несущих частот в блоке 1 усиливаются и преобразуются в сигналы промежуточных частот, а затем поступают на вход блока 2 с выхода которого они поступают на входы соответствующих блоков $3^1, 3^2, \dots, 3^K, \dots, 3^N$, ширина полосы пропускания каждого из которых равна:

$$\Delta f = \frac{2}{T_K},$$

где T_K – длительность зашифрованных кодовых комбинаций. Затем с выходов блоков $3^1, 3^2, \dots, 3^K, \dots, 3^N$ сигналы поступают на соответствующие входы блоков

$4^1, 4^2, \dots, 4^K, \dots, 4^N$, в которых осуществляется демодуляция радиочастотных сигналов рабочих частот и формирование видеоимпульсов длительностью T_K , равной длительности зашифрованных кодовых комбинаций. Сформированные таким образом видеоимпульсы с выходов блоков $4^1, 4^2, \dots, 4^K, \dots, 4^N$ поступают на соответствующие входы блока 5, в котором заранее записан весь ансамбль зашифрованных кодовых комбинаций. Затем с помощью этих видеоимпульсов с устройства памяти осуществляется считывание соответствующих зашифрованных кодовых комбинаций, которые с выходов устройства памяти поступают на соответствующие входы дешифратора, где преобразуются в соответствующие кодовые комбинации исходного передаваемого цифрового сигнала. В результате полученные кодовые комбинации передаваемого цифрового сигнала с выходов дешифратора поступают на соответствующие входы сумматора, на выходе которого образуется передаваемый цифровой сигнал.

Таким образом, МП1 обеспечивает использование в приемном устройстве для демодуляции сигнала узкополосных фильтров с шириной полосы пропускания в n – раз меньшей (n – число импульсов кодовой комбинации) по сравнению со способом-прототипом, в котором кодовые комбинации передаются непосредственно по радиоканалу. Это позволяет в n – раз увеличить отношение сигнал/шум на входе демодулятора сигналов, что приводит к повышению помехоустойчивости передачи системы в целом.

Техническим результатом применения МП1 является повышение структурной, информационной скрытности и помехоустойчивости передаваемых цифровых сигналов, а также упрощение приемного устройства. Данный технический результат достигается тем, что сигналы двоичных кодовых комбинаций с помощью шифратора преобразуют в сигналы зашифрованных кодовых комбинаций, путем замены каждой двоичной кодовой комбинации на другую двоичную кодовую комбинацию в соответствии с заданным законом шифрования. Затем каждой зашифрованной кодовой комбинации присваивают соответствующий номер несущей частоты, которую излучают в пространство в течение времени, равном ее длительности T_K . Принимают сигналы несущих частот, усиливают и преобразуют в сигналы промежуточных частот, которые выделяют с помощью полосовых узкополосных фильтров, ширина полосы пропускания которых равна

$$\Delta f = \frac{2}{T_K},$$

где T_K – длительность зашифрованной кодовой комбинации, с последующей демодуляцией. В результате – получают видеоимпульсы, с помощью которых с устройства памяти считывают соответствующие зашифрованные кодовые комбинации, преобразуемые дешифратором в кодовые комбинации передаваемого цифрового сигнала, в результате суммирования которых принимают передаваемый цифровой сигнал.

Структурная схема радиолинии для осуществления МП2 представлена на рис.4 и рис.5.

На рис.4 – схема передающей стороны радиолинии, где обозначено:

- 1 – источник цифрового сигнала (ИЦС);
- 2 – блок формирования периодической последовательности видеоимпульсов (БФППВ);
- 3 – блок формирования кодовых комбинаций (БФКК);
- 4 – блок шифрования кодовых комбинаций (БШКК);
- 5 – генератор псевдослучайной последовательности (ГНПСП);
- 6 – генератор синхронизирующей ПСП (СПСП);
- 7 – опорный генератор частоты (ОГЧ);
- 8 – генератор тактовых импульсов (ГИ);
- 9 – формирователь сигнала несущей частоты (ФСНЧ);
- 10₁, 10₂ – первый и второй сумматоры;
- 11₁, 11₂ – первый и второй перемножители;
- 12 – фазовращатель на 90° (ФВ);
- 13 – усилитель мощности (УМ).

На рис.5 – схема приёмной стороны радиолинии, где обозначено:

- 1 – высокочастотный (ВЧ) блок;
- 2 – опорный генератор частоты (ОГЧ);
- 3 – генератор тактовых и синхронизирующих импульсов (ГТСИ);
- 4 – фазовращатель на 90° (ФВ);
- 5 – генератор псевдослучайной последовательности (ГНПСП);
- 6 – генератор синхронизирующей ПСП (СПСП);
- 7 – блок поиска СПСП;
- 8₁, 8₂, ..., 8_k, ..., 8_N – первый – N-ый корреляторы;
- 9 – блок принятия решения (решающий блок);
- 10 – устройство памяти зашифрованных кодовых комбинаций;
- 11 – дешифратор кодовых комбинаций;
- 12 – сумматор.

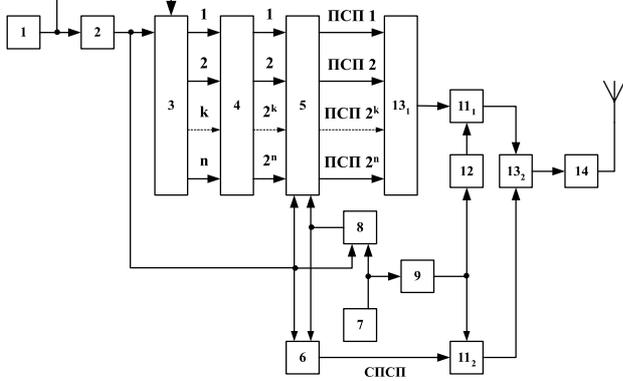


Рис.4

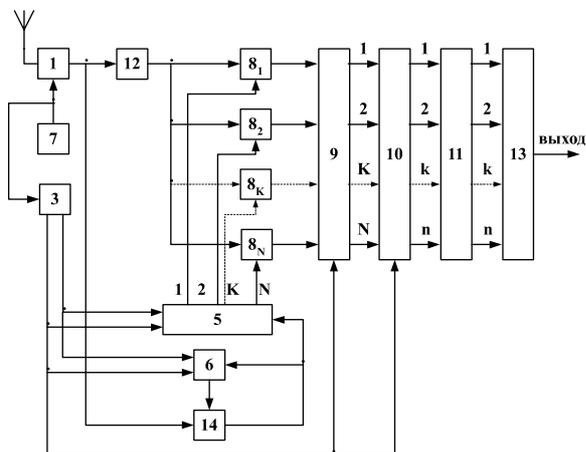


Рис.5

Работа устройства происходит следующим образом.

На передающей стороне с выхода ИЦС информационный сигнал поступает на вход блока 2, в котором из приходящего цифрового сигнала формируется периодическая последовательность видеоимпульсов, период повторения которых равен длительности кодовой комбинации $\tau_k = n / f_T$, где n – значность двоичного кода, то есть число импульсов кодовой комбинации, f_T – частота дискретизации передаваемого цифрового сигнала.

Полученная периодическая последовательность видеоимпульсов с выхода блока 2 поступает на первые входы ГТИ и генератора СПСП, и первый синхронизирующий вход ГНПСП для обеспечения их синфазности, а также – на первый вход БФКК, на второй вход которого подаётся цифровой сигнал с выхода ИЦС.

БФКК представляет собой n -разрядный сдвиговый регистр с последовательным входом и параллельным выходом, на вход которого поступает цифровой сигнал в последовательном коде, а затем в регистре происходит накопление n разрядов информационной последовательности, и она выставляется на выходную шину в параллельном виде. Так происходит со всей последовательностью информационных символов, поступающих от ИЦС. Таким образом, в блоке 3 происходит формирование двоичных кодовых комбинаций длительностью τ_k , которые с выходов 1, 2, ..., k, ..., n блока 3 подаются на соответствующие входы БШКК, в котором осуществляется шифрование поступающих кодовых комбинаций цифрового сигнала, то есть каждая поступающая двоичная кодовая комбинация сигнала заменяется на другую двоичную кодовую комбинацию в соответствии с заданным законом шифрования.

Затем в БШКК осуществляется преобразование зашифрованных двоичных кодовых комбинаций в десятичные числа, при этом на одном из 2^n выходов блока 4 появляется логическая единица в соответствии с десятичным числом, а на остальных выходах – логический ноль, которые затем поступают на соответствующие входы ГНПСП, где данному значению десятичного числа, в соответствии с используемым методом шифрования, присваивается номер ПСП, которая с одного из 2^n выходов ГНПСП подаётся на соответствующий вход первого сумматора, с выхода которого она поступает на первый вход первого перемножителя. В перемножителе сигналом ПСП осуществляется фазовая манипуляция на 180° сигнала несущей частоты, который с выхода ФСНЧ подаётся на один из входов второго перемножителя и на вход фазовращателя на 90°, с выхода которого сдвинутый по фазе на 90° сигнал несущей частоты подаётся на второй вход первого перемножителя.

На первый вход второго перемножителя подаётся сигнал СПСП с выхода блока 6, на второй вход которого поступают тактовые импульсы с выхода ГТИ, которые также поступают на один из входов ГНПСП. Для формирования тактовых импульсов и сигнала несущей частоты на другой вход ГТИ и на вход ФСНЧ подаётся сигнал с выхода ОГЧ. Во втором перемножителе сигналом СПСП осуществляется фазовая манипуляция на 180° сигнала несущей частоты, который затем поступает на один из входов второго сумматора.

ра, на первый вход которого подаётся сигнал с выхода первого перемножителя. Полученный суммарный фазоманипулированный широкополосный сигнал (ФМШПС) с выхода второго сумматора подаётся на вход усилителя мощности для его излучения в пространство. Таким образом осуществляется передача по радиолинии только псевдослучайных последовательностей (ПСП) вместо исходного цифрового сигнала, что практически полностью исключает возможность перехвата сигнала информации потенциальным разведприёмником и обеспечивается структурная и информационная скрытность передаваемого цифрового сигнала.

На приёмной стороне входной сигнал поступает на первый вход ВЧ блока 1, на второй вход которого подаётся сигнал с ОГЧ, поступающий также на вход ГТСИ. В блоке 1 осуществляется предварительная селекция входного ВЧ сигнала и его преобразование в сигнал промежуточной частоты, который затем подаётся на один из входов блока поиска СПСП и на вход фазовращателя на 90° , с выхода которого сигнал поступает на первые входы первого – N -го корреляторов ($N = 2^n$), на вторые 2^n входов которых подаются сигналы ПСП с $N = 2^n$ выходов ГНПСП, на первый и второй входы которого поступают соответственно тактовые и синхронизирующие импульсы с ГТСИ, которые также подаются на первый и второй входы генератора СПСП. При этом синхронизирующие импульсы, период повторения которых равен периоду повторения синхронизирующей ПСП, обеспечивают синфазность сигналов ПСП и СПСП и подаются также на один из входов решающего блока и блока 10.

В блоке поиска СПСП осуществляется поиск по времени задержки и обнаружение передаваемого сигнала СПСП, для этого на другой вход блока поиска СПСП подаётся видеосигнал СПСП с выхода генератора СПСП. Сигнал обнаружения СПСП с выхода блока поиска СПСП поступает на другие входы генератора ПСП и генератора СПСП для обеспечения их синхронизации. После обнаружения сигнала СПСП в каждом из $N = 2^n$ корреляторов осуществляется вычисление автокорреляционной функции входного сигнала ПСП с одной из 2^n ПСП, поступающих с ГНПСП. Затем сигналы с 2^n выходов корреляторов поступают на $N = 2^n$ входов решающей схемы, в которой в момент окончания сигнала ПСП принимается решение о его обнаружении и номере принятой ПСП и на каждый из 2^n выходов решающего блока выставляется сигнал логической единицы при приёме соответствующей ПСП. Затем сигнал с 2^n выходов решающего блока поступает на 2^n входов блока 10, в котором хранится весь набор зашифрованных кодовых комбинаций. В соответствии с кодом сигнала, поступающим на 2^n входов блока 10, происходит считывание соответствующей зашифрованной кодовой комбинации, которая с n выходов устройства памяти подаётся на n входов блока 11, в котором она преобразуется в кодовую комбинацию передаваемого цифрового сигнала.

Расшифрованные кодовые комбинации с n выходов блока 11 поступают на n входов сумматора, на выходе которого образуется передаваемый цифровой сигнал.

Таким образом, так как вычисление автокорреляционных функций входных сигналов ПСП осуществляется в течение времени, равном длительности кодовой комбинации T_k , то это приводит к повышению отношения сигнал/шум на выходе корреляторов в n раз, что позволяет значительно увеличить помехоустойчивость приёма цифрового сигнала.

Сигнал, передаваемый по радиолинии обладает большим числом степеней свободы, чем обычный двоичный информационный сигнал. В связи с этим значительно уменьшается вероятность раскрытия структуры сигнала при условии обнаружения этого сигнала, что улучшает структурную скрытность сигнала. Помимо этого, само информационное сообщение не передаётся по радиолинии, что улучшает информационную скрытность сигнала.

Расчётные соотношения

Рассмотрим двоичный симметричный канал с межбитовой ППРЧ.

Пусть E – отношение энергии сигнала к спектральной плотности мощности белого шума на приёме. Тогда вероятность ошибки на бит для МП определяются как [3]:

$$P_{МП} = \frac{1}{2} \cdot \left(1 - \Phi \left(\sqrt{E \cdot \frac{X}{N}} \right) \right), \quad (1)$$

где $\Phi(u) = \sqrt{\frac{2}{\pi}} \cdot \int_0^u \exp\left(-\frac{q^2}{2}\right) dq$ – функция Крампа,

а вероятности правильного приёма X битов, составляющих блок информации, для МП определяются как

$$W_{МП} = \sum_{i=0}^{t(N)} \frac{N!}{i! \cdot (N-i)!} \cdot P_{МП}^i \cdot (1-P_{МП})^{N-i}, \quad (2)$$

где N – объём ПСП, $t(N)$ – число ошибочных битов.

Формула (2) соответствует вероятности того, что в ПСП объёмом N $t(N)$ и менее битов будут ошибочными.

Для системы с ППРЧ и без какой-либо информационной избыточности значение вероятности ошибочного приёма на одной частоте [2]

$$W_{ППРЧ} = \frac{J}{2^X}, \quad (3)$$

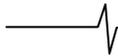
где J – число источников помехи, мощность которых не меньше мощности несущей полезного сигнала, 2^X – общее число имеющихся частот в системе.

Учитывая формулы (2), (3), вероятность правильного приёма одного блока информации в системе с ППРЧ для МП определяется как

$$V_{МП} = W_{МП} \cdot (1 - W_{ППРЧ}), \quad (4)$$

Если в (4) подставить формулы (1)-(3), то она примет вид

$$V_{МП} = \sum_{i=0}^{t(N)} \left[\frac{N!}{i! \cdot (N-i)!} \cdot \left(\frac{1}{2} - \frac{1}{\sqrt{2\pi}} \int_0^{\sqrt{\frac{E \cdot X}{N}}} \exp\left(-\frac{q^2}{2}\right) dq \right)^i \right] \times \left[\frac{1}{2} + \frac{1}{\sqrt{2\pi}} \int_0^{\sqrt{\frac{E \cdot X}{N}}} \exp\left(-\frac{q^2}{2}\right) dq \right]^{N-i} \quad (5)$$



Кроме того, если установить порог в виде минимально допустимой вероятности правильного приёма $V_{пор}$, то значение, полученное в (5), должно быть не меньше этого порога

$$V_{МП} \geq V_{пор} \quad (6)$$

На основании формул (5) и (6) функционирует предлагаемый способ передачи информации. Анализ результатов, полученных выше, позволяет определить набор входных параметров для расчётов по этим формулам, характеризующих ожидаемое качество радиосвязи. Такими входными параметрами являются:

- отношение энергии сигнала к спектральной плотности мощности белого шума на приёме E ;
- число информационных символов в пакете X ;
- объём ПСП, заменяющей информационный пакет, N ;
- число станций помех J .

Математическое моделирование

Для оценки эффективности рассмотренного способа передачи информации было проведено математическое моделирование на ЭВМ с помощью Mathcad 2000 Professional. В качестве ПСП были выбраны три M -последовательности с $N_1 = 31$, $N_2 = 63$ и $N_3 = 127$. Для данного типа ПСП $t(N) = \lfloor 0.25 \cdot N \rfloor$, где $\lfloor \cdot \rfloor$ означает наименьшее целое число [5].

Для данной модели в качестве параметров было выбрано $J = 2$. Результаты расчётов сравнительных оценок помехоустойчивости предложенного МП и метода, не использующего замену информационного блока на ПСП (обозначенного НМП), в зависимости от числа источников помехи и отношения энергии сигнала к спектральной плотности мощности белого шума, представлены на рис.6.

Анализ рис.6 показывает, что при фиксированных N и J необходимо иметь определённое сочетание E и X , чтобы обеспечить наибольшую помехоустойчивость при соблюдении конфиденциальности. Таким образом, идея способа состоит в том, чтобы в зависимости от конкретных условий помеховой обстановки (то есть, изменяя перечисленные выше входные параметры), обеспечить выполнение формул (5) и (6). Таким образом, выбор того или иного параметра (как, например, в нашем случае N_1 , N_2 или N_3) зависит от характера воздействующих помех и требует идентификации помеховой обстановки. Когда это выполнено, данный способ обеспечивает наиболь-

шую помехоустойчивость (за счёт поэлементного накопления) при соблюдении конфиденциальности (сама информация не передаётся по каналу связи). Кроме того, поскольку применение ПСП относится к организационно-техническим методам защиты от утечки информации [4], МП требует значительно меньших затрат, что для подавляющего большинства абонентов сетей связи является более чем приемлемым.

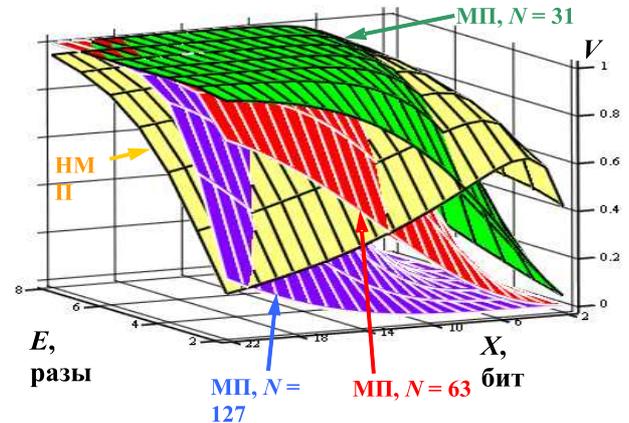


Рис.6

Заключение

Подводя общий итог вышеизложенному, можно сделать вывод: предложенный метод передачи информации и структурные схемы его реализации для рассмотренных модификаций позволяют обеспечить повышение скрытности и помехоустойчивости систем радиосвязи.

Литература

1. Борисов В.И. и др. Помехозащищённость систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2000.
2. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра: Пер. с англ. / Под ред. В.И. Журавлёва. – М.: Радио и связь, 2000.
3. Расчёт помехоустойчивости систем передачи дискретных сообщений: Справочник/Коржик В.И., Финк Л.М., Щелкунов К.Н.: Под ред. Л.М. Финка. – М.: Радио и связь, 1981.
4. Калинин Ю.К. Криптозащита сообщений в системах связи. Учебное пособие. – М.: МТУСИ, 2000.
5. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио