УДК 621.391.2

Г.Н. Розоринов

ПЕРЕДАЧА-ПРИЕМ ДИСКРЕТНОЙ ИНФОРМАЦИИ С ЗАЩИТОЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Предложена относительно простая и эффективная система передачи дискретной информации, основанная на использовании операции измерения многомерной функции распределения вероятностей модулированной несущей, то есть на выявлении признака зависимые – независимые отсчеты несущей, обеспечивающая конфиденциальность передачи и оптимальный прием широкополосных сигналов.

Приведены структурные схемы и результаты экспериментального исследования модема, подтверждающие его реализуемость и эффективность.

Ключевые слова: дискретная информация, конфиденциальная передача-прием, многомерная функция распределения вероятностей, оптимальный прием, широкополосные сигналы.

Введение

Для построения цифровых и аналоговых систем связи с защитой от несанкционированного доступа часто используются широкополосные сигналы [1]. Широкая полоса частот несущих сигналов используется как для повышения скорости передачи информации, так и для повышения устойчивости работы систем в условиях внешних помех. Известен класс широкополосных сигналов, называемых сигналами с расширением спектра, где полоса частот передаваемого сигнала может быть значительно шире полосы частот информационного сигнала. Достоинствами сигналов с расширением спектра являются:

- допустимость работы при малых отношениях сигнал-шум, как результат расширения информационного сигнала на большую полосу частот;
- устойчивость к селективному замиранию при многолучевом распространении сигнала;
- распределение сигнала по большой частотной полосе, вследствие чего передаваемая спектральная мощность сигнала мала и он слабо влияет на другие сигналы;
- расширение информационного сигнала на широкую передаваемую полосу и сжатие его в приемнике обеспечивает устойчивость приема при интерференции со стороны других сигналов [2].

Использование случайных сигналов в качестве расширяющих придает системам связи устойчивость по отношению к селективному замиранию и узкополосным скачкам, низкую вероятность перехвата, устраняет проблемы конфиденциальности и синхронизации. Потенциальные достоинства случайных сигналов не ограничиваются возможностью их применения в системах с расширением спектра. Они могут быть использованы также для маскировки передаваемой информации без расширения спектра, т.е. при совпадении полосы частот информационного и передаваемого сигналов, и для высокоскоростной передачи данных.

Целью настоящей работы является обоснование возможности существенного удешевления и упрощения системы передачи дискретной информации, при обеспечении оптимального ее приема по любому из известных статистических критериев обнаружения [3], а также обеспечение способности противостоять обнаружению и измерению параметров.

Основная часть

В работе [4] показано, что коэффициент независимости отсчетов случайного процесса

$$C^m(nT) = \frac{F^m\{x_1, nT-\tau_1;\, x_2, nT-2\tau\,;\ldots;\, x_m, nT-m\tau\,\}}{\prod_{i=1}^{m} F\{x_i, nT-i\tau\,\}}, \qquad (1)$$

где: $F^m\{x_1, nT-\tau_1; x_2, nT-2\tau; \ldots; x_m, nT-\tau_m\}$ - m-мерная функция распределения вероятностей случайного процесса; $F\{x_i, nT-i\tau\}$, $i=\overline{1,m}$ - одномерные функции распределения вероятностей, совпадает с оценкой отношения правдоподобия для случая проверки простой гипотезы, заключающейся в том, что наблюдаемые отсчеты случайного процесса ***зависимы*** против простой альтернативы, что эти отсчеты ***независимы.*** Там же приведены результаты измерений коэффициента независимости для произвольно распределенных случайных процессов. Из этих результатов следует, что изменяя коэффициент связи между отсчетами случайного процесса можно передавать информационные сигналы, обеспечивая их ***оптимальный*** прием путем измерения величины коэффициента независимости $C^m(nT)$.

По аналогии с предложенным в [4] алгоритмом формирования ***зависимых*** отсчетов для реализации модуляции может быть использован итерационный алгоритм вида

$$U(nT) = N(nT) + K \cdot S(nT) \cdot N\left[(n-1)T\right], \quad n = 0,1,2,\ldots, \qquad (2)$$

где: $N(nT)$, $n=0,1,2,\ldots$ - последовательность независимых отсчетов произвольно распределенного случайного процесса; $S(nT)$ - модулирующий сигнал; K - коэффициент связи между отсчетами; T - период следования отсчетов.

Структурная схема модулятора, реализующего алгоритм (2), показана на рис. 1.

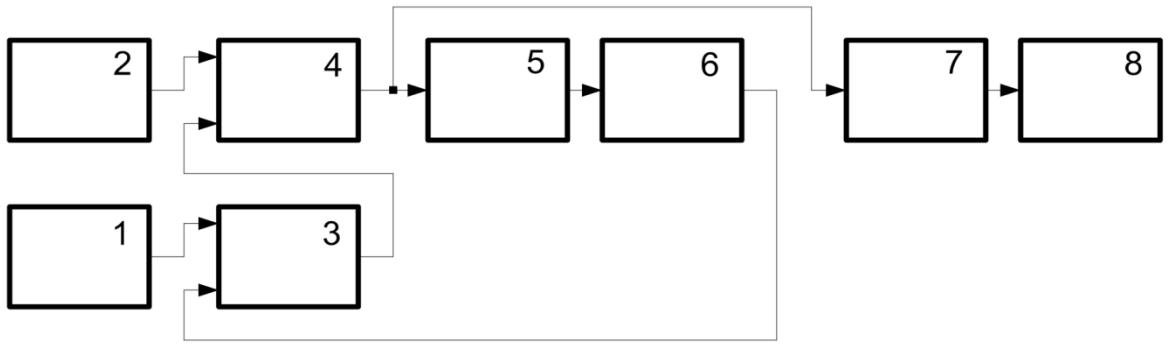

Рис. 1. Модулятор сигнала передачи

Входной информационный сигнал $S(nt)$, представляющий собой, например, последовательность прямоугольных импульсов подается от источника 1 информации на коммутатор 3 и разрешает прохождение через него сигнала с измененной функцией распределения вероятностей (с зависимыми отсчетами) в течение времени существования импульсов. В остальное время коммутатор 3 сигнал не пропускает. Сигнал, снимаемый с выхода коммутатора суммируется с помощью сумматора 4 с широкополосной несущей $N(nt)$, вырабатываемой формирователем 2. Несущая $N(nt)$, $n=1,2,...$ представляет собой дискретизированный случайный процесс с произвольной функцией распределения вероятностей (с независимыми отсчетами). Смесь сигналов, снимаемая с выхода сумматора 4 изменяется по амплитуде с помощью регулятора 5 уровня. При этом коэффициент K регулирования выбирается меньшим единицы ($K < 1$). Коэффициент K определяет степень связи между отсчетами и в итоге уровень конфиденциальности передаваемого сообщения. Далее сигнал $KN(nt)$ задерживается на время τ, кратное периоду дискретизации несущей (в простейшем случае равном периоду дискретизации) с помощью элемента 6 задержки.

Замкнутая цепь, состоящая из элементов 3-6 и представляет собой собственно модулятор. Выходом модулятора является выход сумматора 4, на котором формируются сигналы

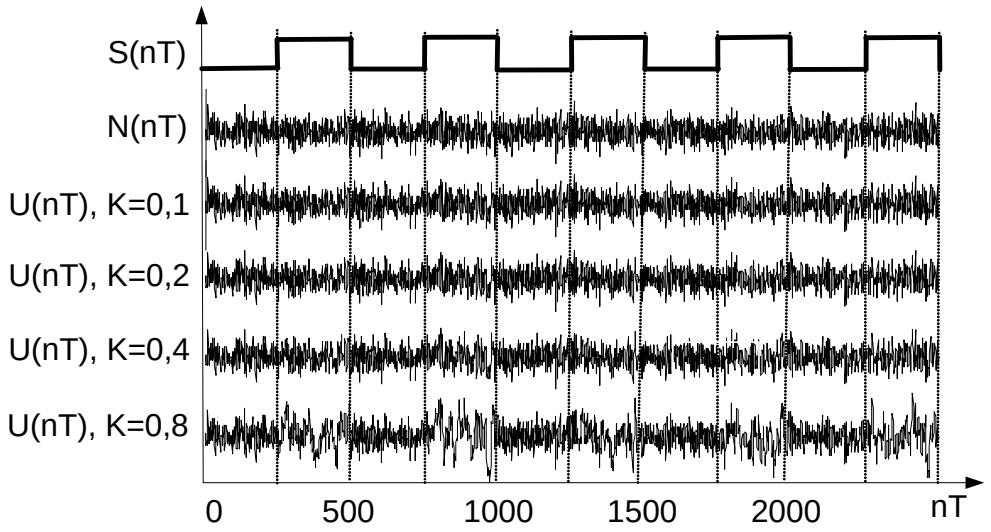

Рис. 2 Модуляция случайного процесса прямоугольными импульсами

$$U(nt)=\begin{cases} N(nt)+KN(nt-\tau)+K^2N(nt-2\tau)+...+K^mN(nt-m\tau), & при \quad S(nt)=1, \\ N(nt), & при \quad S(nt)=0. \end{cases} \tag{3}$$

Здесь $S(nt)=1$ означает наличие информационного импульса, а $S(nt)=0$- его отсутствие, $m=0,1,2,...$. Таким образом информационным параметром модуляции является признак зависимости или независимости отсчетов. На рис.2 показаны временные диаграммы модулированных меандром сигналов при разных значениях коэффициента K.

Из диаграмм видно, что при модуляции со значениями $K>0,4$ еще можно обнаружить информационный сигнал. Поэтому с выхода сумматора 4 сигнал подается на усилитель 7, где он нормируется по дисперсии. Так как отсчеты несущей $N(nt)$ независимы, имеют нулевое математическое ожидание и дисперсию σ^2, то на выходе модулятора (сумматора 4) получим такие математическое ожидание M_1 и дисперсию M_2:

$$\begin{aligned} &M_1\{U(nt)\}=0, \\ &M_2\{U(nt)\}=1+K^2+K^4+...+K^{2m}=\frac{1-K^{2(m+1)}}{1-K^2}. \end{aligned} \tag{4}$$

Это позволяет пронормировать модулированный сигнал по дисперсии на интервале времени действия информационных импульсов. Легко увидеть, что при $K<1$ и $m>10$ (что целесообразно выбирать) член $K^{2(m+1)} \approx 1$, поэтому нормирование по дисперсии заключается в умножении модулированного сигнала на величину $\sqrt{1-K^2}$ на интервале времени действия импульсов с помощью усилителя 7.

На временных диаграммах рис.3 показан результат модуляции случайного процесса последовательностью прямоугольных импульсов с последующим нормированием по дисперсии.

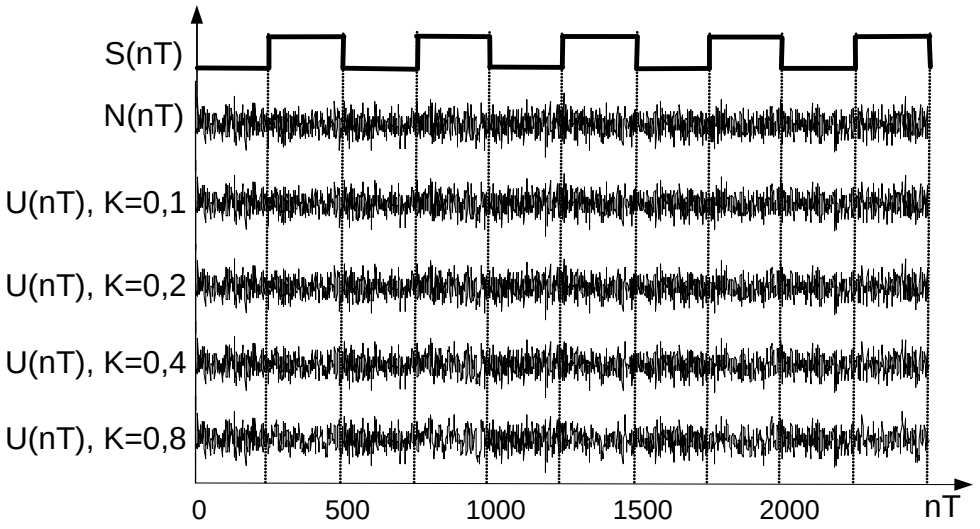

Рис. 3 Модуляция случайного процесса прямоугольными импульсами с нормированием по дисперсии

Видно, что нормирование по дисперсии выходного сигнала модулятора приводит к тому, что обнаружить модуляцию сигнала становится практически невозможно даже при больших значениях коэффициента связи K между отсчетами. Сформированный сигнал далее передается в канал передачи 8.

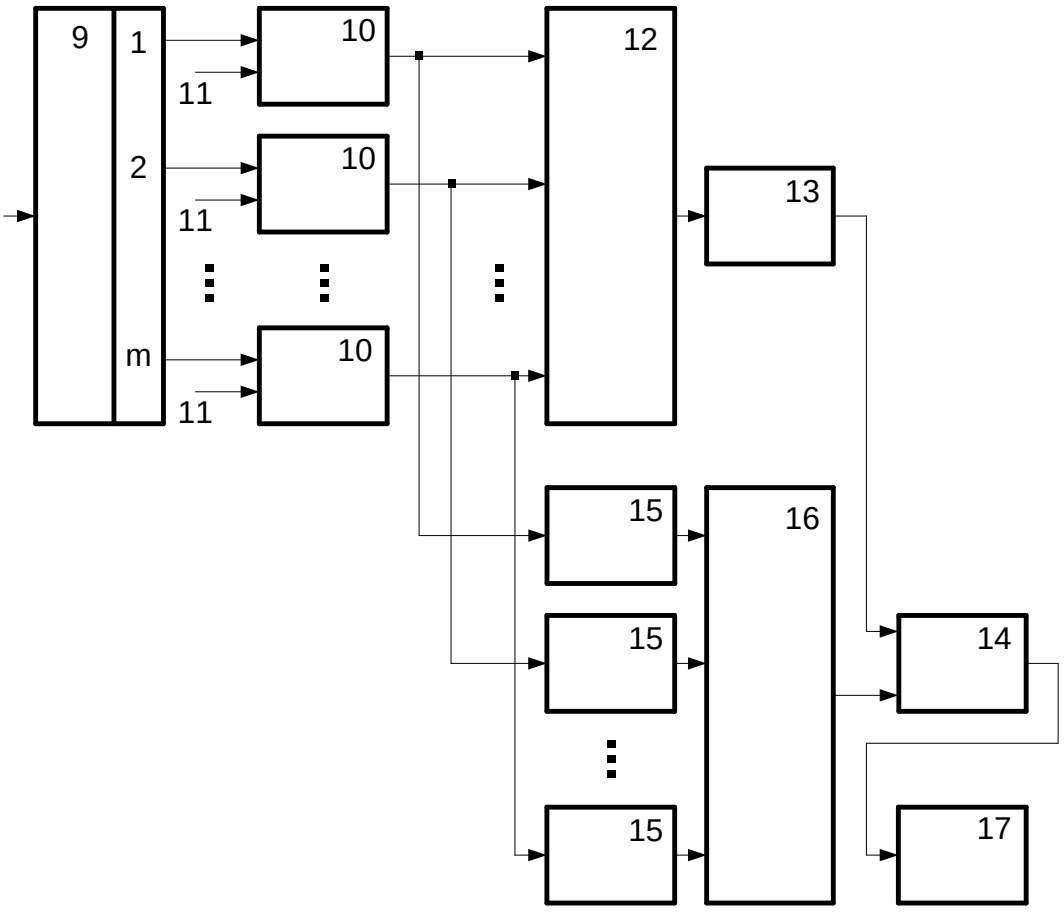

Рис. 4 Структурная схема демодулятора принятого сигнала

В качестве демодулятора модулированных сигналов может быть использовано устройство для измерения коэффициента независимости отсчетов случайного процесса [4]. Это устройство дает оценку отношения правдоподобия для случая проверки простой гипотезы о том, что наблюдаемые отсчеты случайного процесса ***зависимы*** против простой альтернативы, заключающейся в том, что эти отсчеты – ***независимы***. Структурная схема демодулятора модулированной описанным выше образом шумовой несущей показана на рис.4.

Прошедший по каналу 8 передачи информации модулированный сигнал $U^D\left(nt\right)$ поступает на вход элемента 9 задержки с m выходами. Задержанные на разное время сигналы $U^D\left(nT-m\tau\right),$ квантуются по уровню с помощью пороговых элементов 10 в соответствии с правилом

$$U^D(nT-m\tau)=\begin{cases}1 & при \quad U^D(nT-m\tau)\le x_m\\ 0 & при \quad U^D(nT-m\tau)>x_m\end{cases}. \qquad (5)$$

То есть, если мгновенные значения принятых задержанных сигналов меньше мгновенных значений пороговых напряжений, задаваемых с помощью шин 11, то на выходе пороговых элементов 10 вырабатывается высокий уровень сигнала, в противном случае – низкий уровень. Квантованные сигналы, снимаемые с выходов пороговых элементов 10 поступают на многовходовый элемент совпадения 12, который формирует сигнал

$$U^{Dm}(x_1,nT-\tau;\,x_2,nT-2\tau;\ldots;x_m,nT-m\tau)=\bigcap_{i=1}^{m}U^D(x_m,nT-i\tau). \qquad (6)$$

Этот сигнал поступает на t- текущий интегратор 13, с помощью которого формируется m- мерная оценка функции распределения вероятностей $F^{m*}\left(x_1,nT-\tau;\,x_2,nT-2\tau;\ldots;x_m,nT-m\tau\right)$ для задержанных сигналов $U^D(nT-m\tau)$ [5]. Принцип работы t- текущего интегратора описан, например, в [6].

Полученный сигнал оценки m-мерной функции распределения вероятностей подается на один из входов двухвходового делителя 14. Одновременно сигналы, снимаемые с выходов пороговых элементов 10 подаются на входы t- текущих интеграторов 15. Эти интеграторы формируют оценки $F^*(x_m,nT-m\tau)$ одномерных функций распределения вероятностей сигналов $U^D(nT-m\tau)$. Полученные сигналы оценок $F^*(x_m,nT-m\tau)$ перемножаются с помощью m-входового перемножителя 16, в результате чего вырабатывается произведение

$$\prod_{i=1}^{m}F^*(x_i,nT-i\tau)\ , \qquad (5)$$

которое поступает на другой вход делителя 14. На выходе этого делителя вырабатывается сигнал, величина которого отображает оценку коэффициента связи отсчетов $U^D(nT-m\tau)$ принятого сигнала, т.е.

$$C^{m*}(nT)=\frac{F^{m*}\left\{x_1,nT-\tau;\,x_2,nT-2\tau;\ldots;x_m,nT-m\tau\right\}}{\prod_{i=1}^{m}F^*\left\{x_i,nT-i\tau\right\}}. \qquad (6)$$

Этот сигнал и поступает в приемник информации 17.

На фиг.5 показаны временные диаграммы, поясняющие процесс демодуляции принятого сигнала.

При этом, несмотря на отсутствие каких-либо признаков информационного сигнала в широкополосной несущей, демодулятор уверенно его обнаруживает, реализуя алгоритм ***оптимального приема*** [3].

При проведении эксперимента постоянная накопления t - текущих интеграторов была выбрана равной 3000, а коэффициент связи между отсчетами $K = 0{,}6$.

Выводы

1. Предложена относительно простая и эффективная система передачи дискретной информации, основанная на использовании операции измерения многомерной функции распределения вероятностей модулированной несущей, т.е. выявлении признака зависимые – независимые отсчеты несущей, обеспечивающая конфиденциальность передачи и оптимальный прием широкополосных сигналов.

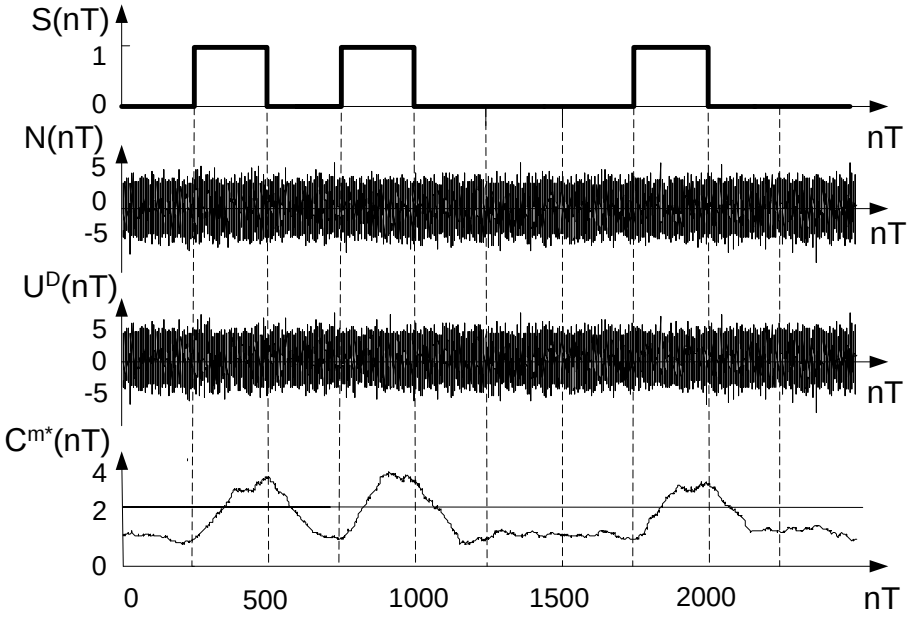

Рис. 5 Демодуляция принятого сигнала

2. Приведены результаты экспериментального исследования модема типа стохастический модулятор – оптимальный приемник, подтверждающие его практическую реализуемость, эффективность, и способность противостоять обнаружению.

Литература

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. - М.: Радио и связь, 1985.-384 с.

2. Дмитриев А.С., Панас А.И., Старков С.О. Динамический хаос как парадигма современных систем связи // Зарубежная радиоэлектроника, 1997, №10, с.4-26.

3. Левин Б.Р. Теоретические основы статистической радиотехники. Кн.2.- М.: Сов. радио.- 1968.- 552 с.

4. Брягин О.В., Егоров А.К., Розоринов Г.Н. Определение степени независимости отсчетов случайных процессов // Реєстрація, зберігання і оброб. даних.-2005.-Т.7.-№ 4.-С.

5. Брягин О.В., Егоров А.К., Розоринов Г.Н. Об оценке многомерных функций распределения вероятностей речевых сигналов // Реєстрація, зберігання і оброб. даних.-2004.-Т.6.-№ 3.-С.41-49.

6. Мирский Г.Я. Аппаратурное определение характеристик случайных процессов.- М.: Энергия, 1972. - 456 с.

Надійшла 19.11.2014 р. Рецензент: д.т.н., проф. Богданович В.Ю.