

УДК 004.056

## ОЦЕНКА РАЗБОРЧИВОСТИ РЕЧИ ВЗАИМНОЙ КОРРЕЛЯЦИЕЙ СИГНАЛА ЛИНЕЙНОЙ ЧАСТОТНОЙ МОДУЛЯЦИИ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

*д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, канд. техн. наук К.Я. РАХАНОВ, И.Б. БУРАЧЕНОК  
(Полоцкий государственный университет)*

*Обосновано использование взаимокорреляционной обработки сигнала линейной частотной модуляции (ЛЧМ) в пределах полос равной разборчивости между входом и выходом канала утечки информации. Показаны преимущества такой обработки для учета времени задержки измерительного ЛЧМ-сигнала. Представлены метод оценки разборчивости речи с помощью функции взаимной корреляции и имитационный эксперимент, который демонстрирует положительные свойства нового метода.*

**Введение.** Совершенствование методов оценки разборчивости речи определяется измерительным сигналом и методами их обработки на выходе каналов утечки информации. Значительная неравномерность амплитудно-частотной характеристики (АЧХ) каналов утечки обуславливает методическую погрешность при использовании гармонического сигнала в полосах равной разборчивости. Применение сигнала ЛЧМ, предложенного в работах [1, 2], позволяет решить эту научную задачу. К одним из наиболее эффективных методов оптимального приема детерминированного сигнала относятся методы, строящиеся на основе корреляционного приема. Непосредственная связь автокорреляционной функции с энергией сигнала определяет ее использование в процедурах энергетической оценки сигналов [3]. Однако в случае известной формы сигнала (ЛЧМ-сигнал в полосах равной разборчивости) более мощным средством обнаружения является функция взаимной корреляции [4].

**Преимущество функции взаимной корреляции** основано на том, что при оценке используется эталонный сигнал с нулевым шумом. Так как в эталонном сигнале отсутствует шум, в отличие от сигнала, используемого в функции автокорреляции, то на выходе получают большее отношение энергии сигнала к энергии шума при любых значениях отношения сигнал/шум на входе. Справедливость данного утверждения представим ниже.

Автокорреляционная и взаимокорреляционная функция в общем виде определяется общим интегралом:

$$R(\tau) = \int_{-\infty}^{\infty} S_1(t) \cdot S_2(t-\tau) dt, \quad (1)$$

где  $S_1$  – смесь измерительного ЛЧМ-сигнала и шума;

$S_2$  – в случае автокорреляционной функции – смещенная копия смеси измерительного ЛЧМ-сигнала и шума на время  $\tau$ ;

$S_2$  – в случае взаимокорреляционной функции – смещенный эталонный ЛЧМ-сигнал на время  $\tau$ .

Смесь ЛЧМ-сигнала и шума  $S(t)$  представим выражением

$$S(t) = s(t) + n(t), \quad (2)$$

где  $s(t)$  – ЛЧМ-сигнал;

$n(t)$  – шум.

Предположим, что  $s(t)$  и  $n(t)$  не коррелируют, тогда автокорреляционная функция  $R(\tau)$  будет представлена следующим образом:

$$\begin{aligned} R(\tau) &= \int_{-\infty}^{\infty} [s_1(t) + n_1(t)] \cdot [s_2(t-\tau) + n_2(t-\tau)] dt = \\ &= \int_{-\infty}^{\infty} (s_1(t)s_2(t-\tau) + s_1(t)n_2(t-\tau) + n_1(t)s_2(t-\tau) + n_1(t)n_2(t-\tau)) dt = \\ &= \int_{-\infty}^{\infty} s_1(t)s_2(t-\tau) dt + \int_{-\infty}^{\infty} s_1(t)n_2(t-\tau) dt + \int_{-\infty}^{\infty} n_1(t)s_2(t-\tau) dt + \int_{-\infty}^{\infty} n_1(t)n_2(t-\tau) dt = \\ &= R_{s_1 s_2}(\tau) + R_{s_1 n_2}(\tau) + R_{n_1 s_2}(\tau) + R_{n_1 n_2}(\tau). \end{aligned} \quad (3)$$

В случае взаимокорреляционной функции используется эталонный ЛЧМ-сигнал свободный от шума, следовательно функция (3) будет иметь вид

$$R(\tau) = R_{s_1 s_2}(\tau) + R_{n_1 n_2}(\tau). \quad (4)$$

В полученном уравнении (4) отсутствуют дополнительные случайные составляющие ( $R_{s_1 n_2}(\tau)$  и  $R_{n_1 s_2}(\tau)$ ), значимость которых возрастает при высоком уровне шумов отличных от белого, что отрицательно влияет на погрешность измерения.

**Мощность измерительного сигнала.** Для оценки мощности измерительного сигнала с помощью взаимокорреляционной функции между измерительным сигналом и эталонным сигналом при смещении  $\tau = 0$  рассмотрим функцию  $R(0)$ , которая соответствует энергии взаимодействия двух сигналов  $E_{12}$  [5]:

$$R(0) = \int_{-\infty}^{\infty} S_1(t) \cdot S_2(t) dt = E_{12}. \quad (5)$$

При прохождении через среду распространения измерительный сигнал  $S_1(t)$  искажается по отношению к эталонному  $S_2(t)$ . Такое искажение в общем виде можно представить как  $S_1(t) = \mu \cdot S_2(t)$ , где  $\mu$  – коэффициент искажения измерительного сигнала  $S_1(t)$  по отношению к эталонному  $S_2(t)$ .

Выполнив замену переменной  $S_1(t)$  в функции (5), получим

$$E_{12} = \int_{-\infty}^{\infty} \mu \cdot S_2(t) \cdot S_2(t) dt = \mu \int_{-\infty}^{\infty} S_2^2(t) dt = \mu \cdot E_{S_2}, \quad (6)$$

где  $E_{S_2}$  – энергия эталонного сигнала.

Из полученного уравнения выразим коэффициент искажения  $\mu$

$$\mu = \frac{E_{12}}{E_{S_2}}. \quad (7)$$

Аналогично выполнив замену  $S_2(t) = \frac{1}{\mu} S_1(t)$  в выражении (5), получим

$$E_{12} = \int_{-\infty}^{\infty} \frac{1}{\mu} \cdot S_1(t) \cdot S_1(t) dt = \frac{1}{\mu} \int_{-\infty}^{\infty} S_1^2(t) dt = \frac{1}{\mu} \cdot E_{S_1}, \quad (8)$$

где  $E_{S_1}$  – энергия измерительного сигнала.

Выразим энергию измерительного сигнала из полученного выражения (8):

$$E_{S_1} = \mu \cdot E_{12}. \quad (9)$$

Выполнив подстановку коэффициента искажения  $\mu$  из выражения (7), получим

$$E_{S_1} = \frac{E_{12}^2}{E_{S_2}}, \quad (10)$$

где  $E_{12}$  – энергия взаимодействия измерительного сигнала  $S_1(t)$  и эталонного  $S_2(t)$ , равная взаимной корреляции  $R(0)$  при смещении  $\tau = 0$ ;  $E_{S_2}$  – априорное значение энергии эталонного сигнала.

Из полученного выражения (10) получим мощность измерительного ЛЧМ-сигнала  $P_{S_1}$

$$P_{S_1} = \frac{E_{S_1}}{T} = \frac{E_{12}^2}{E_{S_2} T}, \quad (11)$$

где  $T$  – длительность измерительного ЛЧМ-сигнала.

Оценка мощности измерительного сигнала, представленная в выражении (11), позволяет перейти к энергетическому показателю защищенности объекта информатизации – отношению сигнал/шум. Расчет информационных показателей защищенности (парциальному коэффициенту разборчивости, коэффициент разборчивости речи, слоговой и словесной разборчивости) выполняется согласно работе [6].

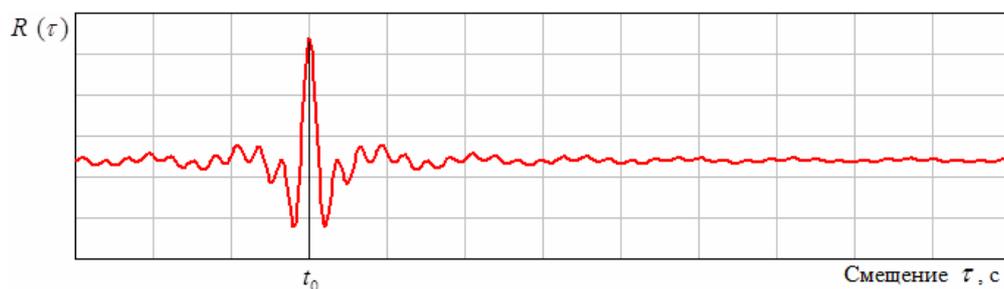
**Время задержки измерительного сигнала.** От момента запуска изменения до момента прихода сигнала в первичный измерительный преобразователь существует временная задержка (от 10 до 50 мс), которая вызвана прохождением сигнала через среду распространения, а также временем работы программного обеспечения, операционной системы. Данная временная задержка не является постоянной величиной и может меняться в зависимости от ряда внешних факторов. В таком случае классическая функция определения энергии сигнала будет представлена выражением

$$E = \int_{t_0}^{T+t_0} s^2(t) dt, \quad (12)$$

где  $t_0$  – время задержки ЛЧМ-сигнала.

Из выражения (12) следует, что время задержки является обязательной величиной, которую требуется учитывать при энергетической оценке сигнала. Определение времени задержки  $t_0$  выполняют за счет положительного свойства функции взаимной корреляции, отличающегося от свойства функции автокорреляции – сдвига максимума функции взаимной корреляции на время, равное времени задержки сигнала [4].

На рисунке 1 представлен график зависимости взаимной корреляционной функции от времени смещения  $\tau$ , наличие на котором острых пиков свидетельствует о существовании корреляционной связи между  $S_1$  и  $S_2$  при некоторых значениях  $\tau$ . В момент времени  $t_0$  наблюдается максимум взаимокорреляционной функции, который равен времени задержки ЛЧМ-сигнала.



**Рисунок 1 – График зависимости взаимокорреляционной функции  $R(\tau)$  от смещения  $\tau$**

Таким образом, перенос оценки величины взаимной корреляции  $R(\tau)$  на максимум функции в допустимом интервале времени учитывает время задержки сигнала  $t_0$ , при этом оценка мощности измерительного ЛЧМ-сигнала, определяемая из выражения (11), примет вид

$$P_{S_i} = \frac{R(t_0)^2}{E_{S_2} T}. \quad (13)$$

Оценка разборчивости речи заключается в следующем:

1) снижение порогового эффекта измерительного ЛЧМ-сигнала методом синхронного накопления с автоматическим принятием решения о достижении порога чувствительности по критерию максимального правдоподобия [7];

2) оценка мощности измерительного ЛЧМ-сигнала в каждой полосе равной разборчивости на входе первичного измерительного преобразователя  $P_{S_i}$  выполняется согласно выражению (13);

3) оценка мощности шума в каждой из полос равной разборчивости на входе первичного измерительного преобразователя  $P_{n_i}$  согласно выражению:

$$P_{n_i} = \frac{\int_0^T S_{i_i}^2(t) dt}{T - P_{S_{i_i}}};$$

4) расчет отношения сигнал/шум в каждой полосе равной разборчивости  $Q_i = \frac{P_{S_{i_i}}}{P_{n_i}}$ , где  $i$  – номер полосы равной разборчивости;

5) вычисление парциального коэффициента разборчивости речи для каждой полосы [6]:

$$Kp_i = \begin{cases} \frac{1}{3} \left( \frac{1}{1+10^{-0,1 \cdot Q_i}} + \frac{1}{1+10^{0,1(-Q_i+12)}} + \frac{1}{1+10^{0,1(-Q_i-12)}} \right), & Q < 0; \\ \frac{1}{3} \left( 1 - \frac{1}{1+10^{0,1 \cdot Q_i}} + 1 - \frac{1}{1+10^{0,1(Q_i+12)}} + 1 - \frac{1}{1+10^{0,1(Q_i-12)}} \right), & Q \geq 0; \end{cases}$$

6) расчет суммарного коэффициента разборчивости речи

$$K_s = \frac{1}{N} \sum_{i=1}^N K_{p_i},$$

где  $N$  – количество полос равной разборчивости.

7) вычисление информационных показателей защищенности – разборчивости речи<sup>1</sup> [6]:

**Имитационный эксперимент** выполнен с использованием классической для теории и практики локации модели сигнала с ЛЧМ [8]. Остановимся на примере анализа сигнала для первой полосы равной разборчивости, мгновенная частота которой меняется в пределах от 100 до 420 Гц [6]. Амплитуда сигнала  $A = 1$  В, длительность сигнала  $T = 4$  с, частота дискретизации  $f_d = 8192$  Гц. Интервал дискретизации  $\Delta t = 1/8192 = 122$  мкс. База сигнала  $B = \Delta\omega \cdot T = (420 - 100) \cdot 4 = 1280$ . Для демонстрации определения времени задержки ЛЧМ сигнала установим  $t_0 = 0,1$  с.

В этом случае математическая модель ЛЧМ-сигнала в дискретном виде представлена следующим выражением:

$$s(j) = 1 \cdot \sin \left( 2\pi \cdot \frac{j \cdot \text{ranc}(j / 8192)}{8192} \left( 100 + 1280 \frac{j \cdot \text{ranc}(j / 8192)}{8192 \cdot 2} \right) \right),$$

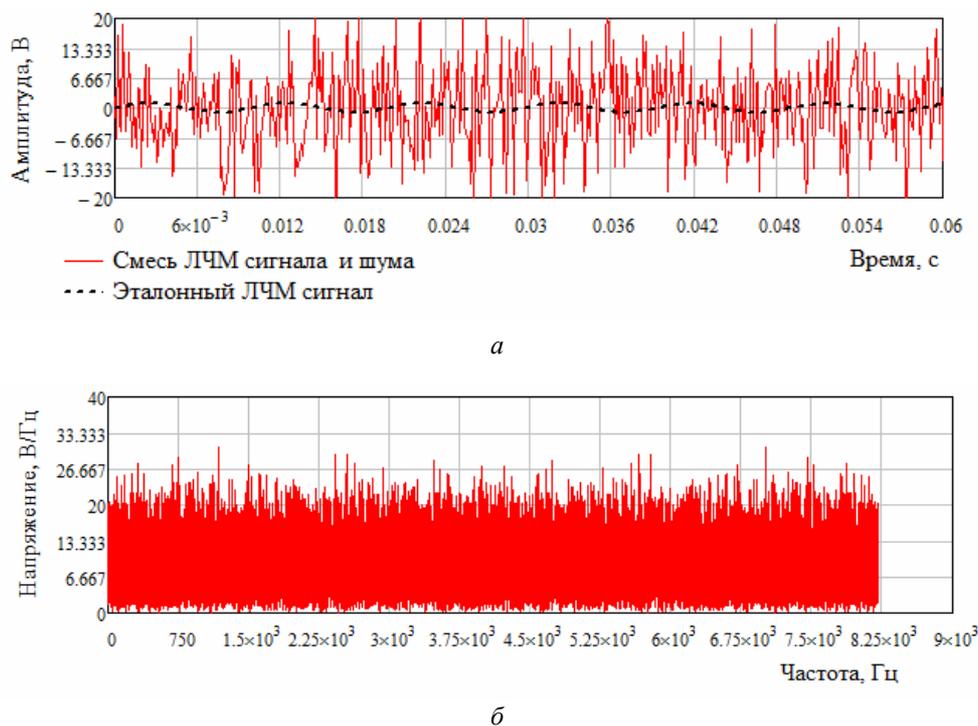
где  $j$  – индекс времени реализации сигнала;  $j \in 0 \dots 33588$ ;

*ranc* – функция выделения целой части от деления.

Математическая модель шума  $n(j)$  представлена генератором случайных значений, плотность вероятности которых подчинена нормальному закону. Математическое ожидание шума равно нулю, а среднеквадратическое отклонение шумового процесса  $\sigma = 10$  В, при этом отношение сигнал/шум на входе приемника равно минус 20 дБ.

Фрагмент реализации процесса смеси сигнала и шума  $S(n) = s(j) + n(j)$  представлен на рисунке 2, *а*, спектр – на рисунке 2, *б*. На данных графиках не наблюдается гармонических составляющих ЛЧМ сигнала, что подчеркивает сложность выделения ЛЧМ сигнала из шума.

<sup>1</sup> См. статью *д-р техн. наук, проф. В.К. Железняк, И.Б. Бураченко* «Оценка нормативного показателя защищенности речевого сигнала сложным сигналом с большой базой» на С. 10–14 настоящего номера.



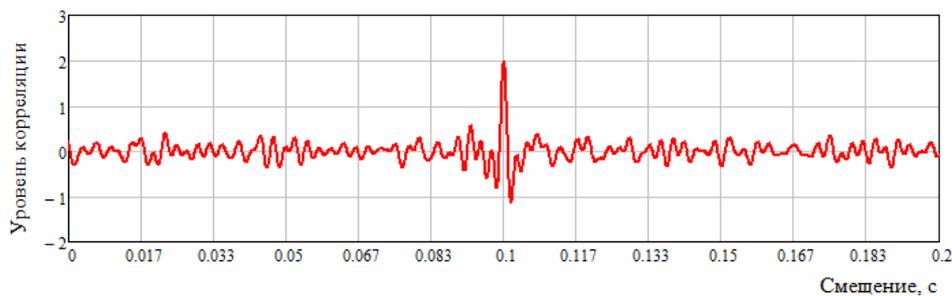
**Рисунок 2 – Реализация процесса смеси ЛЧМ сигнала и шума:  
 а – фрагмент реализации процесса смеси ЛЧМ сигнала и шума;  
 б – спектр реализации процесса ЛЧМ сигнала и шума**

Математическая модель расчета зависимости взаимной корреляции от смещения  $\tau$  представлено дискретным выражением:

$$R(k) = \sum_{j=0}^{33587} S(j) \cdot s\left(j - \frac{k}{8192}\right) \cdot \frac{1}{8912}, \quad (14)$$

где  $k$  – индекс времени смещения  $\tau$  ( $k \in 0 \dots 33588$ ).

На рисунке 3 представлена реализация взаимокорреляционной функции, на которой максимум приходится на смещение равное 0,1 с.



**Рисунок 3 – График зависимости взаимокорреляционной функции  $R(\tau)$  от смещения  $\tau$**

В массиве значений  $R(k)$ , полученном из выражения (14), максимальное значение равно  $R_{MAX} = 2,017$ , индекс времени смещения  $k$  которого равен 819, а время задержки  $t_0 = 819/8192 = 0,1$  с. Таким образом, экспериментально установленное время задержки измерительного сигнала  $t_0$  соответствует заданному времени задержки ЛЧМ-сигнала в параметрах эксперимента.

Мощность измерительного ЛЧМ сигнала в первой полосе равной разборчивости согласно выражению (13) равна  $P_{s_i} = \frac{2,017^2}{1^2 \cdot 4 / 2} = 0,504$  Вт. Мощность эталонного ЛЧМ сигнала в первой полосе равной разборчивости составила  $P_{s_i} = \frac{1^2 \cdot 4}{2} = 0,5$  Вт. Абсолютная погрешность оценки мощности  $\lambda = 0,004$ , а относительная погрешность  $\gamma = 0,8\%$ .

С помощью метода дисперсионной обработки результатов оценки мощности сигнала, представленного в работе [9], при доверительной вероятности 0,99 рассчитаны методические погрешности для отношений сигнал/шум минус 20 и минус 14 дБ и длительностях сигнала 2 и 4 с. Полученные значения относительных методических погрешностей представлены в таблице.

Таблица – Относительные методические погрешности

Отношение сигнал/шум, дБ	Длительность сигнала, с	Относительная погрешность, ±%
- 20	4	4,6
- 20	2	7,3
- 14	4	1,9
- 14	2	4,0

**Выводы.** В работе предложен метод оценки разборчивости речи с помощью функции взаимной корреляции, который:

- в оценке показателей учитывает время задержки измерительного ЛЧМ сигнала;
- позволяет одновременно оценивать мощность измерительного ЛЧМ сигнала и мощность шума;
- обладает низкой методической погрешностью и высокой чувствительностью;
- обладает высокой производительностью за счет использования простых вычислений.

#### ЛИТЕРАТУРА

1. Способ определения максимальной разборчивости речи : пат. 15204 Респ. Беларусь : МПК G 10L 15/00 / В.К. Железняк, К.Я. Раханов ; дата опубл.: 30.12.2011.
2. Устройство для определения разборчивости речи : пат. 15314 Респ. Беларусь : МПК G 10L 15/00, H 04R 29/00 / В.К. Железняк, К.Я. Раханов ; дата опубл.: 28.02.2012.
3. Дворников, С.В. Теоретические основы синтеза билинейных распределений / С.В. Дворников. – СПб. : Изд-во Политехн. ун-та, 2007. – 268 с.
4. Бендат, Дж.С. Измерение и анализ случайных процессов / Дж.С. Бендат, А. Пирсол ; пер. с англ. Г.В. Матушевского, В.Е. Привального ; под ред. И.Н. Коваленко. – М. : Наука, 1971. – 464 с.
5. Розенберг, В.Я. Радиотехнические методы измерения параметров процессов и систем / В.Я. Розенберг. – М. : Изд-во Комитета стандартов, мер и измерительных приборов при Совете министров СССР, 1970. – 308 с.
6. Железняк, В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – СПб. : ГУАП, 2006. – 188 с.
7. Обнаружение сигналов ВЧ-диапазона перемножением спектров фрагментов их реализаций / К.Я. Раханов [и др.] // Вестн. Полоц. гос. ун-та. Сер. С. Фундаментальные науки. – 2010. – № 9. – С. 29–34.
8. Баскаков, С.И. Радиотехнические цепи и сигналы : учебник для вузов по специальности «Радиотехника» / С.И. Баскаков. – 2-е изд., перераб. и доп. – М. : Высш. шк., 1988 – 448 с.
9. Синтез программно-аппаратной системы оценки разборчивости речи методом ЛЧМ-сигнала : результаты эксперимента // К.Я. Раханов // Вестн. Полоц. гос. ун-та. Сер. С. Фундаментальные науки. – 2012. – № 12. – С. 20–26.

Поступила 08.09.2015

#### ESTIMATION OF LEGIBILITY OF THE SPEECH BY MUTUAL SIGNAL CORRELATION OF LINEAR FREQUENCY MODULATION IN CHANNELS OF INFORMATION LEAKAGE

V. ZHELEZNYAK, K. RAKHANOV, I. BURACHENOK

*The article substantiates the use of the cross-correlation signal processing linear frequency modulation (LFM) within bands of equal intelligibility between input and output channels of information leakage. The advantages of such a treatment to take account of the delay time measuring chirp signal. A method for estimation of speech intelligibility using cross-correlation function and is a simulation experiment that demonstrates the positive qualities of the new method.*