

зованного сигнала составляющих  $F_{\text{вч}} \pm F_{\text{нч}} \pm 2F_{\text{нч}} \dots$ , для которых схемы подавления низкочастотных сигналов не являются препятствием, что позволяет принимать эти сигналы в линиях связи или по эфиру и извлекать из них речевую информацию.

В рамках государственной научно-технической программы нашим предприятием был разработан набор устройств, обеспечивающих защиту от утечки по аналоговым и цифровым линиям телефонной связи, охранной, пожарной сигнализации, а также сети электропитания, объединенных под товарным наименованием «Топаз».

Устройству маскируют на принципе маскирования защищаемого сигнала шумовым сигналом, значительно превышающим уровень защищаемого сигнала.

В настоящее время завершается процедура сертификации устройств, после чего они будут предложены для применения.

## **ОБРАБОТКА ШИРОКОПОЛОСНОГО ЛЧМ-СИГНАЛА МЕТОДОМ ВЗАИМНОЙ КОРРЕЛЯЦИИ ПО ВРЕМЕНИ И ЧАСТОТЕ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ**

**В. К. ЖЕЛЕЗНЯК, И. Б. БУРАЧЕНКО**

Задача оценки защищенности от утечки речевой информации в реальном масштабе времени в условиях воздействия шумов высокого уровня с достижением предельных значений методической погрешности, высокой чувствительности и высокой разрешающей способности по частоте актуальна. Наравне с гармоническим измерительным сигналом, обоснованным корреляционной теорией разборчивости речи [1] и регламентированным СТБ 34.101.29-2011, в работе [2] широкополосный ЛЧМ-сигнал предложен в качестве измерительного. Использование широкополосного ЛЧМ-сигнала для оценки защищенности речевой информации позволило снизить значения абсолютной и относительной погрешности при улучшении разборчивости речи. Однако достижение положительных результатов требует значительного увеличения времени обработки сигналов. Это обусловлено необходимостью снижения порогового эффекта широкополосного ЛЧМ-сигнала улучшением отношения сигнал/шум методом синхронного накопления спектральных составляющих ЛЧМ-сигнала и их частотно-временной обработкой путем преобразования Вигнера [2]. Использование широкополосного ЛЧМ-сигнала требует установления математического представления зависимости коэффициента разборчивости речи от параметров ЛЧМ-сигнала и уровня шумов в канале утечки (КУ) речевой информации.

**Целью работы** является разработка метода расчета коэффициента разборчивости речи с использованием функции взаимной корреляции по времени и частоте широкополосным ЛЧМ-сигналом, с высокой точностью и разрешающей способностью по частоте; обоснование численного значения критерия разборчивости речи и сравнение его с нормированным показателем защищенности в КУ речевой информации при минимизации времени обработки для получения численных значений параметров оценки.

Контроль утечки речевой информации осуществляется путем излучения широкополосных ЛЧМ-сигналов уровнем 74дБ в 20-ти полосах равной разборчивости (ППР) одинаковой длительностью  $T_c$  и различными значениями баз, определяемых выражением  $B = 2\Delta f T_c$ , где  $\Delta f$  – девиация частоты сигнала. Обоснование выбора исходных данных измерительных широкополосных ЛЧМ-сигналов представлено в работе авторов [3]. Для обработки на выходе КУ используется согласованный квадратурный приемник, нечувствительный к начальной фазе измерительного сигнала. Далее осуществляется оценка уровня сигнала после прохождения им преграды.

Коэффициент разборчивости речи рассчитываем на основании средних значений коэффициентов разборчивости в каждой отдельно взятой ППР по формуле [1]:

$$k_p = \frac{1}{n} \sum_{i=1}^n k_{pi}, \quad (1)$$

где  $k_{pi}$  – результат единичного измерения среднего значения разборчивости в  $i$ -й полосе КУ речевой информации;  $n$  – число единичных измерений ( $n=20$  количество ПРР).

Коэффициент разборчивости в  $i$ -й полосе КУ речевой информации определяем по формуле [3]:

$$k_{pi} = 2E_i / N_{oi}, \quad (2)$$

где  $E_i$  – энергия широкополосного ЛЧМ-сигнала в  $i$ -й полосе КУ;  $N_{oi}$  – спектральная плотность мощности шума в  $i$ -й полосе широкополосного ЛЧМ-сигнала.

Подставив в (1) значение коэффициента разборчивости в  $i$ -й полосе КУ (2), имеем формулу расчета коэффициента разборчивости речи:

$$k_p = \frac{1}{n} \sum_{i=1}^n \frac{2E_i}{N_{oi}}. \quad (3)$$

С целью повышения точности обнаружения измерительного широкополосного ЛЧМ-сигнала на фоне шумов высокого уровня и других воздействующих факторов при помощи частотно-временного преобразования Гильберта измерительные сигналы  $s_1(t)$  на входе и  $s_2(t)$  на выходе КУ представим в виде двух комплексных переменных:

$$\dot{s}_1(t) = s_1(t) \cdot e^{j\varphi_1(t)} \text{ и } \dot{s}_2(t) = s_2(t) \cdot e^{j\varphi_2(t)}, \quad (4)$$

где  $j = \sqrt{-1}$  – принятое в технических дисциплинах обозначение для мнимой единицы;  $\varphi_1(t)$  и  $\varphi_2(t)$  – полная фаза сигналов соответственно на входе и выходе КУ.

Такой вид представления сигналов позволяет получить обобщенную двумерную взаимно-корреляционную функцию (ВКФ) их комплексных огибающих по формуле [4]:

$$R_{1,2}(\tau, \Omega) = \int_{-\infty}^{\infty} s_1(t) s_2^*(t - \tau) e^{j\Omega t} dt. \quad (5)$$

где  $\tau$  и  $\Omega$  соответственно временное и частотное смещение сигнала;  $*$  – операция комплексного сопряжения.

Функция  $R_{1,2}(\tau, \Omega)$  может быть представлена и через спектральные плотности огибающих сигналов [4]:

$$R_{1,2}(\tau, \Omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F_1(\omega) F_2^*(\omega - \Omega) e^{j\omega\tau} d\omega, \quad (6)$$

где  $F_1(\omega)$ ,  $F_2^*(\omega - \Omega)$  – спектральные плотности исходного и принятого сигналов;  $\omega$  – значение частоты широкополосного ЛЧМ-сигнала.

Временная форма  $s(t)$  сигнала и его частотное представление  $F(\omega)$  позволяют проводить корреляционную оценку одновременно по времени и частоте, так как оба представления взаимосвязаны и модификация одного из них приводит к изменению другого. В частности, некоторый временной сдвиг эквивалентен частному фазовому сдвигу:  $s(t - \tau) \sim F(\omega) e^{-j\omega\tau}$ , а частотный сдвиг эквивалентен временному фазовому сдвигу:  $F(\omega - \Omega) \sim s(t) e^{-j\Omega t}$ .

Из (5) при условии, что  $s_1(t) = s_2(t)$ , имеем автокорреляционные функции (АКФ) входного или выходного сигналов. На рисунке 1 отображены совместно временная и частотная АКФ широкополосного ЛЧМ-сигнала в третьей ПРР.

Оценка энергии  $E_p$  широкополосного ЛЧМ-сигнала в  $i$ -й полосе на выходе КУ речевой информации на основе ВКФ одновременно по времени и частоте исходного измерительного и выходного широкополосных ЛЧМ-сигналов осуществляется с более высокой точностью в сравнении с другими методами. С целью повышения точности оценки учи-

тываются величины временного запаздывания и сдвига частоты, вычисляемые как разность между максимальным значением энергии, определяемой по АКФ в точке, соответственно  $\tau=0$  при оценке временного запаздывания и  $\Omega=0$  при оценке частотного сдвига входного измерительного сигнала и максимальным значением энергии, определяемой по ВКФ между входным и выходным измерительными сигналами.

Функцию  $R_{1,2}(\tau, \Omega)$  называют функцией неопределенности (ФН) [4]. Квадрат модуля ФН  $|R_{1,2}(\tau, \Omega)|^2$  образует тело неопределенности [4], представляющее собой трехмерную функцию двух переменных  $(\tau, \Omega)$ . Поучаем ФН Вудворда [5] и строим площадь сечения плоскостью, параллельной плоскости  $\tau, \Omega$  по уровню 0.5, которая служит мерой совместной разрешающей способности по времени и частоте. Эта площадь представляет собой основание цилиндра с высотой, равной главному максимуму, и объемом, равным объему, ограниченному всей поверхностью:

$$\Delta(\tau, \Omega) = \frac{1}{|R_{1,2}(0, 0)|^2} \int \int |R_{1,2}(\tau, \Omega)|^2 d\tau d\Omega. \quad (7)$$

Пример сечения по уровню 0.5 взаимной ФН широкополосного ЛЧМ-сигнала на выходе КУ в третьей ПРП показан на рисунке 2. Данное графическое представление позволяет с высокой точностью оценить временную задержку и частотный сдвиг, а также определить изменение угла наклона ФН после прохождения сигналом преграды. Благодаря существованию соотношения между частотно-временным представлением и ФН, данный вид анализа играет важную роль при исследовании сигналов сильно модулированных по фазе и частоте.

Впервые для оценки защищенности КУ речевой информации в условиях воздействия шумов высокого уровня предложен метод расчета коэффициента разборчивости речи на базе функций взаимной корреляции одновременно по времени и частоте. Расчет коэффициента разборчивости речи, с использованием ВКФ по времени и частоте, позволил при слабом измерительном сигнале в шумах высокого уровня понизить порог обнаружения сигнала на 6 дБ без дополнительных операций синхронного накопления и тем самым сократить время выделения сигнала из шумов. Предложенный метод расчета открывает новые возможности оценки степени защищенности КУ речевой информации с высокой точностью и разрешающей способностью по частоте за счет обработки широкополосного ЛЧМ сигнала ВКФ одновременно по времени и частоте.

#### Список использованных источников

1. Железняк, В. К. Защита информации от утечки по техническим каналам: учеб. пособие / В. К. Железняк. – СПб.: ГУАП. 2006. – 188 с.

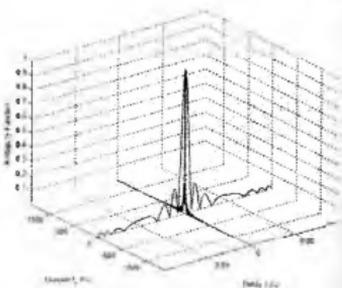


Рис. 1. Совместное отображение временной и частотной АКФ широкополосного ЛЧМ-сигнала в третьей ПРП

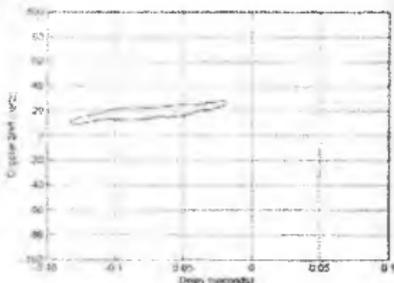


Рис. 2. Сечение по уровню 0.5 взаимной ФН широкополосного ЛЧМ-сигнала на выходе КУ в третьей ПРП

2. Раханов, К. Я. Широкополосная линейно-частотная модуляция сигнала для оценки разборчивости речи в каналах утечки информации / К. Я. Раханов, В. К. Железняк // Известия Нац. академии наук Беларуси / редкол.: П. А. Вицязь (гл. ред.) [и др.]. – Минск: Беларуская навука, 2014. – С. 88–95.

3. Железняк, В. К. Представление параметров широкополосного линейно-частотно-модулированного сигнала для оценки разборчивости речи в технических каналах утечки информации / В. К. Железняк, К. Я. Раханов, И. Б. Бураченко // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2014. – № 12. – С. 2–12.

4. Денисенко, А. Н. Статистическая теория радиотехнических систем / А. Н. Денисенко. – М.: АРИ, 2007. – 200 с.

5. Вудворд, Ф. М. Теория вероятностей и теория информации с применениями в радиолокации / Ф. М. Вудворд; пер. с англ.; под ред. Г. С. Горелика. – М.: Сов. радио, 1955.