

1Н//291111К(039)

IST '10

24-25 ноября
2010 года
Минск, Беларусь

Материалы VI Международной конференции

**Информационные
системы и технологии**

IST'2010

**Informational
systems and technologies**

INFOPARK



ИИ



МАТЕМАТИЧЕСКАЯ МОДЕЛЬ, ОСНОВАННАЯ НА НАУЧНОМ ЭКСПЕРИМЕНТЕ ПО ПОВЫШЕНИЮ ТОЧНОСТИ ОЦЕНКИ ЗАЩИЩЕННОСТИ КУ РЕЧЕВОЙ ИНФОРМАЦИИ

К.Я. Раханов, В.К. Железняк

Полоцкий государственный университет, НИОЭЛ ТЗИ
телефон: +375 (29) 516 09 89 e-mail: K.Rakhanau@gmail.com

Рассматривается метод оценки защищенности каналов утечки речевой информации (КУРИ) с использованием линейно-частотно-модулированного (ЛЧМ) сигнала со снижением порогового эффекта и частотно-временной обработкой измерительного сигнала. Метод анализируется с помощью регрессионной модели и программного компонента на основании входных параметров.

Введение. В работе [1] представлены сравнительные количественные и качественные показатели оценки защищенности КУРИ методом гармонического измерительного сигнала, основанного на корреляционной теории разборчивости речи. Метод обладает высокой достоверностью оценки параметров, на основании которых по установленному пороговому критерию принимается решение об обнаружении либо отсутствии КУРИ. Однако, методу присущи некоторые недостатки.

Целью является исследование метода оценки разборчивости речи в КУРИ, основанного на использовании в качестве измерительного линейно-частотно-модулированный (ЛЧМ) сигнал [2, 3].

Методика решения. Для повышения достоверности и точности оценки защищенности речи впервые предложен метод с использованием ЛЧМ-сигнала в качестве измерительного. Высокая помехоустойчивость достигнута оптимальной обработкой измерительного сигнала, которая позволяет исключить влияющие факторы КУРИ. Эксперименты показали, что заявленный метод позволяет:

- для учета неравномерности АЧХ выполнять измерения не на отдельных измерительных частотах, а во всем диапазоне частот полосы, на которые разбивается речевой диапазон частот;
- снизить влияние реверберации и резонансов замкнутых пространств;
- повысить чувствительность метода;
- измерять мощности сигнала и шума одновременно.

Однако, ЛЧМ-сигналу, так же как и другим ЧМ-сигналам, присущ недостаток – пороговый эффект. Для его снижения возможно применения синхронного накопления, но на практике синхронное накопление является непростой задачей, для решения которой

необходимо использовать сложные синхронизирующие последовательности или импульсы.

Воспользуемся центральной предельной теоремой теории вероятности, согласно которой

$$\sigma_{\bar{x}} = \frac{\sigma_x}{\sqrt{P}} \quad (1)$$

где σ_x – среднеквадратическое отклонение отдельных результатов измерения относительно среднего \bar{X} , $\sigma_{\bar{x}}$ – среднеквадратичное отклонение для P измерений, P – количество измерений.

Представим дискретную функцию, которая позволит найти усредненный спектр результатов измерений ЛЧМ-сигнала Sp^* :

$$Sp_j^* = \frac{1}{P} \sum_{i=1}^P FFT(S_i), \quad (2)$$

где j – номер спектральной составляющей измерительного сигнала $j \in [1..N]$, N – количество спектральных составляющих, Sp_j^* – усредненная спектральная составляющая с номером j , i – порядковый номер измерения $i \in [1..P]$, S_i – сигнал для i -го измерения, FFT – преобразование Фурье.

Измерительный сигнал со сниженным пороговым эффектом будет представлен $Sp = IFFT(Sp^*)$, где $IFFT$ – обратное преобразование Фурье.

В качестве оптимального частотно-временного преобразования ЛЧМ-сигнала выбрано распределение Вигнера, которое позволяет обеспечить максимальную концентрацию сигнальной энергии в континууме точек мгновенных частот в частотно-временном пространстве [4, 5]. Дискретная форма записи распределения Вигнера представлена выражением [6]:

$$Pw(k, n) = 2 \sum_{m=-N+1}^{N-1} Z_a^*(n-m) Z_a(n+m) e^{-j \frac{2\pi k m}{M}}, \quad (3)$$

где $M > 2N-1$, $k \in -N+1..N-1$, Z_a – аналитический сигнал измерительного ЛЧМ-сигнала, $*$ – знак комплексного сопряжения, N – количество дискретных точек. Из (3) следует, что для обработки аналогового сигнала он должен быть предварительно дискретизирован с тактовой частотой более чем вдвое превышающей частоту дискретизации по Котельникову.

Для качественного исследования метода оценки защищенности КУРИ с помощью ЛЧМ-сигнала воспользуемся регрессионной моделью, представляемой в общем виде функцией [7]:

$$y = f(x, z) + e, \quad (4)$$

где x – вектор контролируемых и управляемых факторов (параметров), z – вектор только контролирующих факторов, e – аддитивный Гауссов шум.

В функцию (4) введем параметры $\lambda = \lambda_1, \dots, \lambda_n$ из выражений (2) и (3) соответствующие уровню сигнала, уровню помехи, полосе разбиения речевого сигнала, частоте дискретизации, количеству интервалов измерения и их значениям, времени снижения порога ЛЧМ-сигнала, полосе пропускания входного тракта. При этом система дифференциальных уравнений первого порядка с переменными $y = y_1, \dots, y_i$ будет иметь вид [7]: $\dot{y}_i = F_i(y, \lambda)$, решение которой $y_i = y_i(\lambda)$, где $i = 1, \dots, n$.

Если чувствительность i -ой переменной по k -му параметру $s_{ik} = \partial y_i / \partial \lambda_k$, то обобщенное уравнение чувствительности [7]:

$$\dot{s}_{ik} = \sum_{j=1}^n \frac{\partial F_i}{\partial y_j} s_{jk} + \frac{\partial F_i}{\partial \lambda_k} \quad (5)$$

Для регрессионной модели $y_i = F_i(\lambda_1, \dots, \lambda_k)$ получим следующие уравнение чувствительности $s_{ik} = \Delta_k^{(i)} / \Delta$, где Δ – детерминант уравнения (5), $\Delta_k^{(i)}$ – детерминант, полученный из Δ заменой соответствующих столбцов векторами $(-\partial F_i / \partial \lambda_k)$.

Из условия $\Delta = 0$ следует, что $s_{ik} = \infty$ (т.е. неустойчивость системы). Данное условие определяет критическое значение параметра, вызывающее неустойчивость $\lambda_{кр}$.

Полученные результаты.

Разработан программный компонент (см. рис. 1), реализующий регрессионную модель метода оценки защищенности КУРИ с помощью ЛЧМ-сигнала. В программном компоненте контролируются следующие параметры: уровень сигнала, уровень помехи, полосы разбиения речевого сигнала, частота дискретизации, количество интервалов

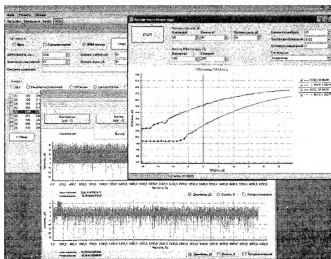


Рис. 1. Программный компонент

измерения и их значение, время снижения порога ЛЧМ-сигнала, полоса пропускания входного тракта.

Построены пороги обнаружения ЛЧМ-сигнала (см. рис. 2), определена кривая верности, аналитическое представление кривой верности в зависимости от входных параметров. Определены критические значения параметров, вызывающие неустойчивость метода. Рассчитано время измерения и обработки результатов. На основании полученных данных произведена оптимизация измерений и обработки.

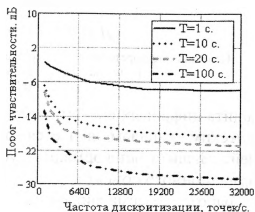


Рис. 2. Порог чувствительности в зависимости от времени обработки

Выводы

Метод оценки разборчивости речи в КУРИ с помощью ЛЧМ-сигнала обладает следующими преимуществами:

- высокой помехозащищенностью;
- весьма низким порогом чувствительности;
- исключением влияющих факторов на результаты измерений, в том числе неравномерность АЧХ КУРИ.

ЛИТЕРАТУРА

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие. ГУАП. –СПб., 2006. –188 с.
2. Железняк В.К., Раханов К.Я. Заявка на патент № а20100004 от 04.01.2010 г. Способ измерения максимальной разборчивости речи.
3. Железняк В.К., Раханов К.Я. Заявка на патент № а20100291 от 24.02.2010г. Устройство измерения максимальной разборчивости речи.
4. Дворников С.В. Теоретические основы синтеза билинейных распределений. – СПб.: Изд-во Политехн. ун-та, 2007. – 268 с.
5. Алексеев А.А., Кириллов А.Б. Технический анализ сигналов и распознавание радиоизлучений. – СПб.: ВАС, 1998. –368с.
6. Claasen T.A.C.M. and Mecklenbrauker W.F.G, The Wigner Distribution - A Tool for Time-Frequency Signal Analysis, part 1, 2, 3 // Phillips Journal of Research, vol. 35, pp. 217-250, 276-300, 372-389, 1980.
7. Горбунов С.С. Математическое моделирование и параметрическая неустойчивость динамических систем с детерминированными параметрами. – Томск: Изд-во ТПУ, 2002. – 231 с.