УДК 534; 621.391.16

СИНТЕЗ ПРОГРАММНО-АППАРАТНОЙ СИСТЕМЫ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ МЕТОДОМ ЛЧМ-СИГНАЛА: РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА

К.Я. РАХАНОВ
(Полоцкий государственный университет)

Представлены результаты сравнительной оценки теоретических и экспериментальных данных, полученных реализованной синтезированной программно-аппаратной системой оценки разборчивости речи. Новые теоретические данные, оценивающие каналы утечки речевой информации по единому критерию, подтверждены экспериментальным методом ЛЧМ-сигнала с высокой точностью. На новом принципе реализован в программно-аппаратной системе метод гармонического сигнала, что позволило наглядно подтвердить жизнеспособность метода ЛЧМ-сигнала. Методическая (теоретическая погрешность) на совпадающих частотах методов ЛЧМ и гармонического сигналов равны.

Обосновано и показано экспериментально, что тонкая структура ЛЧМ-сигнала значительно снижает методическую погрешность в сравнении с методом гармонического сигнала при воздействии влияющих факторов, основным из которых является неравномерность АЧХ.

Введение. Объективная оценка защищенности речевой информации на объекте информатизации является сложной задачей, обусловленной многообразием видов ее физического представления, что предопределяет наличие различных каналов утечки информации. Полнота оценки защищенности объекта информатизации обеспечивается оценкой всех каналов утечки информации с возможностью сравнения их информативности. Сравнение информативности каналов утечки основано на едином научно обоснованном нормативном показателе информационной ценности речевого сигнала – разборчивости речи [1].

Достоверная оценка разборчивости речи в каналах утечки информации обеспечивается корреляционной теорией [1], учитывающей отношение сигнал/шум, полосу речевого сигнала, усредненную спектральную плотность мощности речевого сигнала, спектральную плотность мощности фонового шума, частотно зависимую характеристику затухания контролируемой среды распространения, псофометрическую характеристику слуха.

Из существующих методов оценки защищенности информации метод шумового сигнала функционально ограничен, методически не совершенен [2, с. 3]. Метод гармонического сигнала обладает рядом преимуществ, но обладает некоторыми методическими погрешностями, основными из которых является невозможность учета значительной неравномерности АЧХ канала утечки [2, с. 3 – 4].

Анализ этих методов определил направление исследования, заключающееся в обосновании и разработке на новом принципе метода оценки защищенности присущих речевому сигналу каналов утечки информации [3, 4]. Новый метод базируется на преимуществах предложенного широкополосного ЛЧМ-сигнала в надпороговой области при устранении основного его недостатка – порогового эффекта. Частотно-временное представление сигнальной энергии функцией Вигнера позволило учесть тонкую структуру ЛЧМ-сигнала. Дополнение к корреляционной теории разборчивости речи, разработанной для метода гармонического сигнала, позволяет значительно снизить методические (теоретические) погрешности, обусловленные рядом факторов, искажающих акустический сигнал в замкнутом объеме.

В этой связи основным направлением исследований является разработка и внедрение в практику оценки разборчивости речи в каналах утечки информации методом ЛЧМ-сигнала, внедренной во вновь разработанную программно-аппаратную систему (ПАС). Выбранное направление исследований является ключевым, так как решает задачу оценки нормативных показателей в виде числовых значений разборчивости речи с новыми повышенными требованиями и высокой точностью программно-аппаратной системой. Цель работы – сравнительный анализ полученных теоретических и экспериментальных данных синтезированного ПАС, сравнительная оценка методов гармонического и ЛЧМ-сигналов, реализованных в опытном образце ПАС.

Рассматриваемая ПАС оценки разборчивости речи методом ЛЧМ-сигнала осуществляет оценивание интенсивности физических полей за пределами объекта информатизации в точке наблюдения (съема информации) при воздействии дестабилизирующих факторов высокого уровня. По результатам оценивания рассчитываются нормативные показатели разборчивости речи в образующихся каналах утечки речевой информации. Так как величина показателя непосредственно зависит от точности оценивания интенсивности (напряженности) полей рассеивания сигналов и уровня фоновых шумов, то интерес представляет исследование диапазона допустимый значений отношения сигнал/шум и погрешности оценки разборчивости речи.

Методика исследования

Параметрическая зависимость между влияющим фактором (отношением сигнал/шум на входе первичного преобразователя), контролируемыми параметрами (длительностью сигнала, временем накопления, частотой дискретизации) и вычисленным значением словесной разборчивости речи $W_{вых}$ на выходе измерителя может быть получена на основании исследований имитационной модели как функция многих переменных:

$$W = F_W(X), \tag{1}$$

где X – вектор контролируемых параметров и влияющих факторов.

Для этого в (1), сохраняя многофакторные условия, проводят многофакторные измерения W при различных входных факторах и контролируемых параметрах. По результатам измерений требуется установить F_W и описать ее количественно. Задача установления чувствительности решается методами дисперсионного анализа. Дисперсионный анализ при каждом фиксированном значении вектора X проводится на ограниченном числе (ряде) измерений величины Q. В результате формируется массив измеренных значений:

$$\begin{array}{ccccc} X_1 & \dots & X_i & \dots & X_N \\ W_{11} & \dots & W_{i1} & \dots & W_{N1} \\ \vdots & & \vdots & & \vdots \\ W_{1j} & \dots & W_{ij} & \dots & W_{Nj} \\ \vdots & & \vdots & & \vdots \\ W_{1M} & \dots & W_{iM} & \dots & W_{NM} \end{array}$$

Зависимость W от X устанавливается через попарное сравнение средних арифметических значений i-го ряда между собой по схеме независимых измерений [5].

Алгоритм проведения дисперсионной обработки:

1. Вычислить среднее арифметическое значение для каждого ряда измерений:

$$\overline{W_i} = \frac{1}{M}\sum_{j=1}^{M} W_{ij}, \tag{2}$$

где M – число измерений в i-м ряду.

2. Вычислить дисперсии средних арифметических значений для каждого ряда:

$$D_{W_i} = \frac{1}{M(M-1)}\sum_{j=1}^{M} W_{ij} - \overline{W_i}^{\,2}.$$

3. Вычислить попарные разности между W_i:

$$\Delta\overline{W}_{i-1,i} = \overline{W}_{i-1} - \overline{W}_i,$$

где $i \in [2...N]$.

4. Вычислить дисперсию попарных разностей:

$$D_{\Delta\overline{W}_{i-1,i}} = D_{\overline{W}_{i-1}} + D_{\overline{W}_i}.$$

5. Найти доверительные интервалы для всех попарных разностей:

$$\varepsilon_{i-1,i} = t(P_d, M)\sqrt{D_{\Delta\overline{W}_{i-1,i}}},$$

где $t(P_d, M)$ – коэффициент Стьюдента; M – количество измерений при фиксированном значении вектора X_i; P_d – доверительная вероятность.

6. Сравнить попарные разности $\Delta\overline{W}_{i-1,i}$ с соответствующим доверительным интервалом $\varepsilon_{i-1,i}$. Если $\Delta\overline{W}_{i-1,i} \geq \varepsilon_{i-1,i}$, имеет место зависимость W_i от X_i, в противном случае X_i не позволяет установить величину W_i.

7. Вычислить квантильную погрешность ΔW с заданной доверительной вероятностью P_d [6]:

$$\Delta W = t_n \frac{\sigma}{\sqrt{M}},$$

где t_n – нормированная квантиль нормального закона распределения для заданной доверительной вероятности P_d; σ – средне квадратичное отклонение значений W.

Так как исследование зависимости словесной разборчивости речи заключается в определении функциональной зависимости W от многих переменных (факторов), то усредненный результат – это искомая функция, а погрешность результата – область определения этой функции.Найденная усредненная оценка $\overline{W}$ выражением (2) имеет меньшую случайную погрешность, чем отдельные значения W_i, по которым она находится. Закон распределения $\overline{W}$ при $M \geq 30$ близок к нормальному при любом законе распределения исходных данных [6]. Таким образом, истинное значение измеряемой величины W принадлежит доверительному интервалу:

$$W - \Delta W \leq W \leq W + \Delta W.$$

Погрешность смещения экспериментальных значений X и W не могут быть разделены между собой. Поэтому общепринято условно разделять, что определение значений X производится без погрешности, а всю погрешность относят к координате W_i. Расстояние экспериментальных точек W_i вокруг некоторой детерминированной средней полосы $W = F_W(X)$ определяет полосу неопределенности (полосу погрешности) [6]. После определения полосы погрешности и окончательного вида искомой усредненной зависимости $W = F_W(X)$ частные значения погрешности представляются как $\Delta_i = W_i - W = f(W)$. В результате получим полосу погрешности для каждой экспериментальной точки.

На рисунках 1 и 2 приведены полосы погрешности, полученные на примере имитационного эксперимента для приемников гармонического и ЛЧМ-сигналов. Имитационный эксперимент выполнялся с помощью многофакторных измерений величины W при изменении отношения сигнал/шум от минус 28 дБ до 24 дБ на входе приемника. В качестве источника помехи использовался генератор белого гауссова шума в полосе 20 кГц, сигнал с которого напрямую подавался на вход приемников, исключая влияние внешних факторов (реверберации, резонансов, внешних шумов). Контролируемыми параметрами приемников установлены длительность сигнала (2 с) и частота дискретизации (20000 Гц).

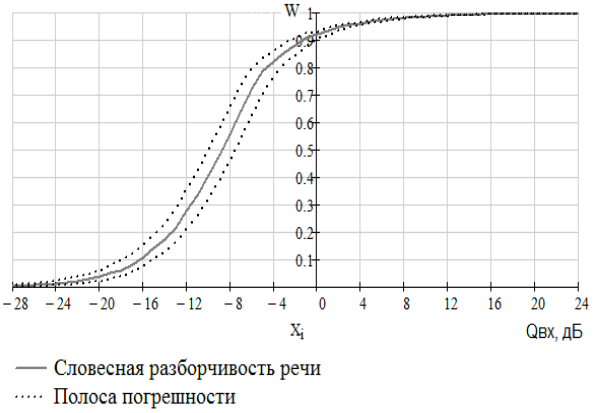


Рис. 1. Полоса погрешности разборчивости речи методом гармонического сигнала

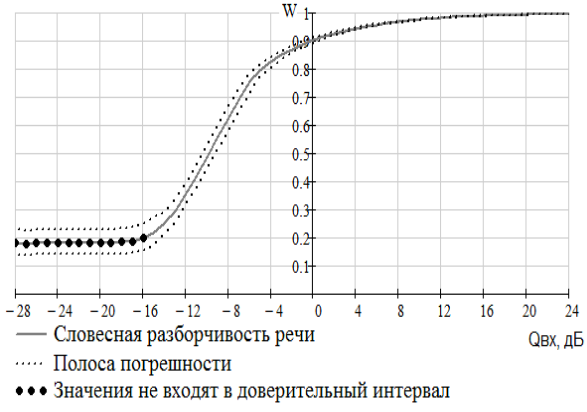


Рис. 2. Полоса погрешности разборчивости речи методом ЛЧМ-сигнала (без снижения порога)

Как видно из рисунка 2, полоса погрешности ЛЧМ-сигнала имеет трапецеидальную форму, что связано с наличием порогового эффекта ЛЧМ-сигнала. Для гармонического сигнала этот эффект не наблюдается (см. рис. 1). Сравнением попарных разностей $\Delta\overline{W}_{i-1,i}$ с доверительным интервалом $\varepsilon_{i-1,i}$ (п. 6) установлены значения словесной разборчивости речи, которые не входят в доверительный интервал. Согласно рисунку 2 при отношении сигнал/шум более чем минус 16 дБ значения словесной разборчивости входят в доверительный интервал, что определяет величину порога обнаружения ЛЧМ-сигнала.

На рисунках 1 и 2 полосам погрешности присущи как аддитивная, так и мультипликативная составляющие, следовательно, абсолютная погрешность $\Delta(W_{вх})$ представлена выражением:

$$\Delta(W_{вх}) = \Delta_0 + \gamma_s W_{вых}, \quad (3)$$

где Δ_0, $\gamma_s W_{вых}$ – аддитивная и мультипликативная составляющие абсолютной погрешности.

Относительная погрешность результата измерений, исходя из выражения (3), составляет:

$$\gamma(W_{вх}) = \frac{\Delta(W_{вх})}{W_{вх}} = \frac{\Delta_0}{W_{вх}} + \gamma_s.$$

На рисунке 3 приведена зависимость относительной погрешности метода гармонического сигнала от величины словесной разборчивости речи. Видно, что для данного имитационного эксперимента величина относительной погрешности не превышает ±1 % в начале диапазона и снижается по мере увеличения разборчивости речи. В отличие от гармонического сигнала, зависимость погрешности метода ЛЧМ-сигнала от словесной разборчивости речи (рис. 4) имеет ярко выраженный подъем в начале диапазона, обусловленный наличием порогового эффекта. Значение относительной погрешности выше порога чувствительности не превышает ±0,6 и спадает по мере увеличения разборчивости речи аналогично методу гармонического сигнала.

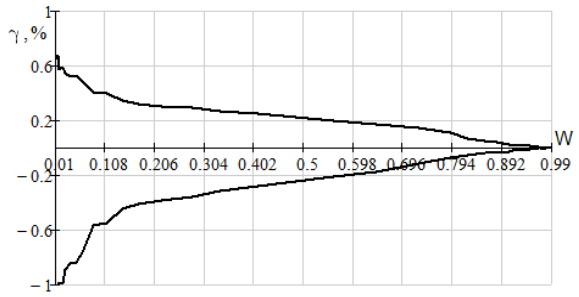


Рис. 3. Относительная погрешность результата расчета разборчивости речи методом гармонического сигнала

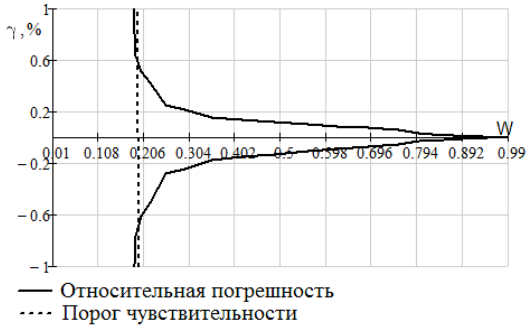


Рис. 4. Относительная погрешность результата расчета разборчивости речи методом ЛЧМ-сигнала (без снижения порога)

Снижение порогового эффекта метода ЛЧМ-сигнала для достоверной оценки нижних значений словесной разборчивости речи решается с помощью синхронного накопления спектральных составляющих ЛЧМ-сигнала, полученных быстрым преобразованием Фурье [2], результатом которого является снижение входного отношения сигнал/шум пропорционально количеству накоплений.

Полученные результаты

Результатом разработки явился опытный образец и комплект конструкторской документации программно-аппаратной системы «ЕРМАК», структурная схема которой представлена на рисунке 5. Принципиальное отличие разработанной ПАС от существующих заключается в использовании как гармонического, так и ЛЧМ-сигнала, тонкая структура которого анализируется частотно-временным представлением сигнальной энергии преобразованием Вигнера.

Программно-аппаратная система включает наряду с аппаратными средствами специальный программный комплекс. Основные функции специального программного комплекса: автоматизированное управление, генерация стимулирующих сигналов, адаптивная цифровая их обработка, вычисление и представление числовых результатов оценки защищенности каналов утечки информации, сравниваемых с нормативным показателем (критерием). Кроме того, программный комплекс обеспечивает замену ряда аппаратных средств (шумомера-анализатора, фильтров коррекции АЧХ). Такая реализация снижает стоимость ПАС, а также расширяет ее возможности в области генерации, анализа и оценки параметров стимулирующих сигналов, увеличивает масштабируемость.

Контроль защищенности речевой информации основан на измерении физических параметров каналов утечки информации с последующим расчетом разборчивости речи. Для расчета разборчивости речи диапазон речевых частот разбивается на двадцать полос равной разборчивости. В каждой полосе последовательно генерируется ЛЧМ-сигнал и подается на излучающее устройство, где сигнал усиливается и излучается через акустическую систему. Распространяясь в среде передачи и взаимодействуя с влияющими факторами (реверберацией, случайными помехами, маскирующими шумами, резонансными явлениями), первичные акустические сигналы вызывают вторичные виброакустические и электромагнитные излучения.

В точках приема регистрирующие устройства (микрофон, радиомикрофон, вибропреобразователь, преобразователи магнитной и электрической составляющих электромагнитного поля, измерительный трансформатор тока) преобразуют соответствующие сигналы в электрические, передают их на входные усилители приемопередающего устройства. Приемопередающим устройством производится предварительное подавление гармоник сети и обработка согласующим фильтром для речевого спектра в аналоговом виде. После чего сигнал передается на аналого-цифровой преобразователь для последующей обработки данных программным компонентом ПЭВМ.

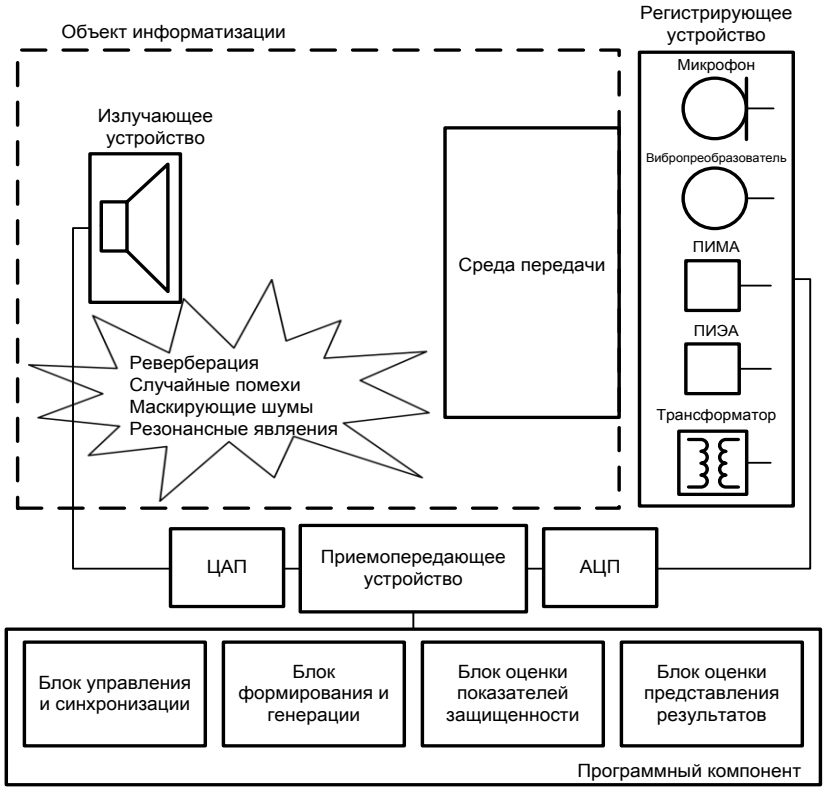


Рис. 5. Структура ПАС оценки разборчивости речи

На ПЭВМ в цифровом виде осуществляется разложение ЛЧМ-сигнала на частотно-временной плоскости и оценивается тонкая структура сигнальной энергии преобразованием Вигнера, вычисляются показатели защищенности и представляются результаты исследования в генерализированной форме. Время вычисления показателей защищенности методом ЛЧМ-сигнала типовым процессором (Intel® Core™ Duo U2400) составляет порядка 365 с, что является приемлемым для практического использования. Однако время расчета может быть снижено до 40 секунд благодаря уменьшению количества частотно-временных составляющих ЛЧМ-сигнала. Внешний вид ПАС «ЕРМАК» представлен на рисунке 6.



Рис. 6. Внешний вид программно-аппаратной системы «ЕРМАК»

Результаты оценки неравномерности АЧХ одного и того же объекта информатизации методом гармонического и ЛЧМ-сигнала представлены на рисунках 7 и 8. Сравнение показало, что оценка мощ-

ностей гармонического и ЛЧМ-сигналов совпадает на средних частотах равной разборчивости (частотах излучения гармонического сигнала). Однако во всей полосе явным преимуществом обладает ЛЧМ-сигнал, так как учитывает тонкую структуру неравномерности АЧХ. Данное свойство ЛЧМ-сигнала незаменимо при оценке защищенности каналов утечки со значительной неравномерностью АЧХ, например, электроакустического канала утечки информации.

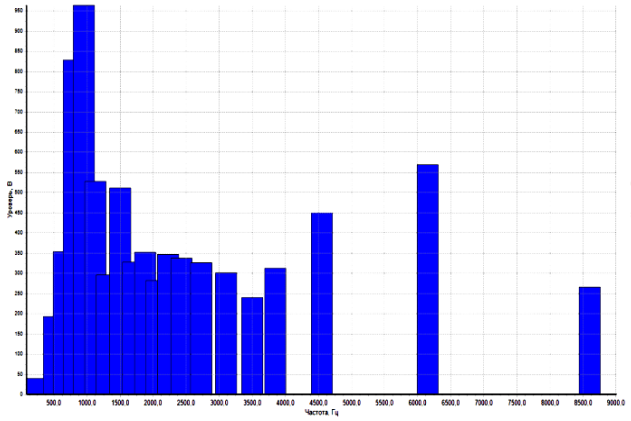


Рис. 7. Неравномерность АЧХ объекта информатизации, оцененная методом гармонического сигнала

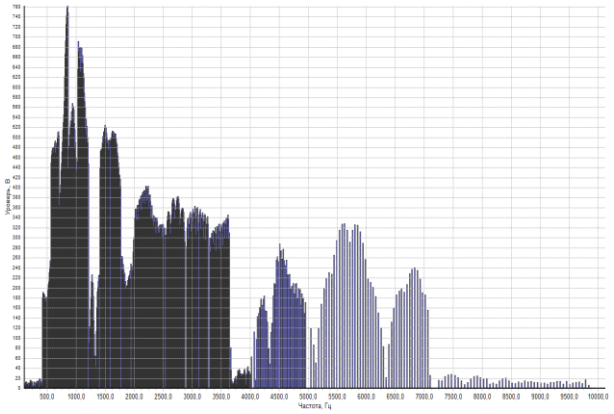


Рис. 8. Неравномерность АЧХ объекта информатизации, оцененная методом ЛЧМ-сигнала

На рисунке 9 показаны результаты экспериментальных полос погрешностей, полученных без накопления, а также с накоплением 10 и 100 раз.

Видно, что без накопления чувствительность ЛЧМ-сигнала только немного заходит в отрицательную область отношения сигнал/шум с уровнем минимальной допустимой словесной разборчивости речи не более 75 %, что несколько отличается от данных, полученных в результате имитационного эксперимента. Данный факт связан с проведением исследований в реальных условиях и обусловлен наличием влияющих факторов (реверберации, резонансов, фоновых, маскирующих шумов). При использовании накоплений в 10 и 100 раз порог чувствительности не смещался по отношению сигнал/шум, но изменил минимальное допустимое значение словесной разборчивости речи до 10 % (при накоплении в 10 раз) и 2 % (при накоплении в 100 раз).

На рисунке 10 представлены зависимости относительной погрешности оценки словесной разборчивости речи. Для всех случаев измерений погрешность не превышала ± 3 % в области допустимых значений, ограниченной снизу порогом чувствительности.

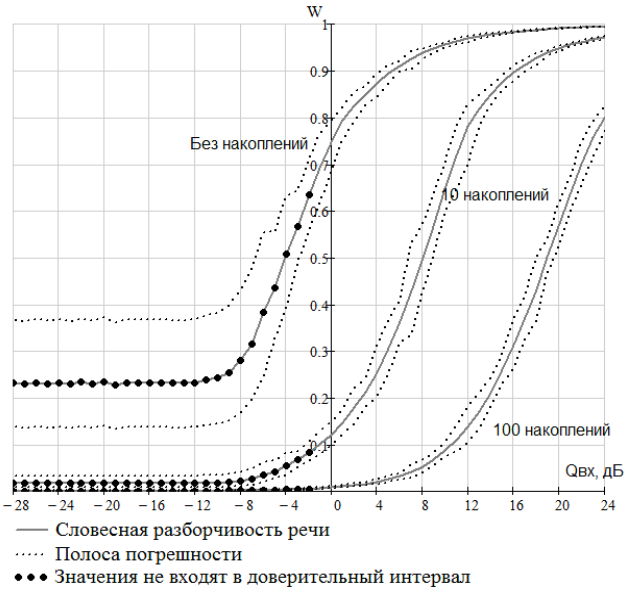


Рис. 9. Полоса погрешности разборчивости речи методом ЛЧМ-сигнала (без накопления, с накоплением 10 и 100 раз)

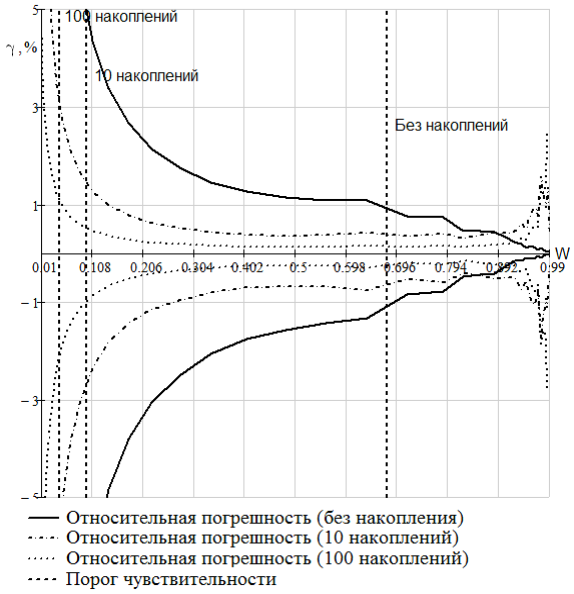


Рис. 10. Относительная погрешность результата расчета разборчивости речи методом ЛЧМ-сигнала (без накопления, с накоплением 10 и 100 раз)

Выводы

Сравнительные экспериментальные исследования обосновывают и подтверждают:

- контроль защищенности объекта информатизации осуществляется по всем каналам утечки речевой информации на базе единого информационного критерия – разборчивости речи;
- метод ЛЧМ-сигнала в отличие от гармонического метода оценки разборчивости речи учитывает в большей мере влияющие факторы (неравномерность АЧХ), что повышает методическую (теоретическую) точность на 50 % для самого неблагоприятного электроакустического канала утечки, обеспечивая полное совпадение результатов оценки разборчивости речи на средних частотах равной разборчивости;
- достижение требуемого порога чувствительности осуществляется путем накопления ЛЧМ-сигнала и может составлять менее чем минус 20 дБ;
- абсолютная погрешность не превышает ± 3 % на диапазоне допустимых значений, начало которого определено порогом чувствительности;
- практическое применение ПАС «ЕРМАК» не требует использования уровня ЛЧМ-сигнала более 84 дБ при исследованиях, что в отличие от метода шумового сигнала не нарушает экологические нормы;
- ПАС «ЕРМАК» обладает высокой производительностью, что позволяет наравне с КИПА «ФИЛИН-А» производить контроль защищенности объекта информатизации в реальном масштабе времени.

Автор выражает благодарность за полезные советы, ценные рекомендации и поддержку руководителю научной работы доктору технических наук, профессору Владимиру Кирилловичу Железняку.

ЛИТЕРАТУРА

1. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.
2. Железняк, В.К. Методы оценки защищенности речевой информации / В.К. Железняк, К.Я. Раханов // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12. – С. 2 – 8.
3. Способ определения максимальной разборчивости речи: пат. 15204 Респ. Беларусь, МПК G 10L 15/00 / В.К. Железняк, К.Я. Раханов; заявитель Полоц. гос. ун-т. – № a20100004; заявл. 04.01.2010; опубл. 30.12.2011 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2011. – № 6. – С. 164.
4. Устройство для определения разборчивости речи: пат. 15314 Респ. Беларусь, МПК G 10L 15/00, H 04R 29/00 / В.К. Железняк, К.Я. Раханов; заявитель Полоц. гос. ун-т. – № a20100291; заявл. 01.03.2010; опубл. 28.02.2012 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2012. – № 1. – С. 162.
5. Анцыферов, С.С. Общая теория измерений: учеб. пособие / С.С. Анцыферов, Б.И. Голубь; под ред. Н.Н. Евтихеева. – М.: Горячая линия – Телеком, 2007. – 176 с.
6. Новицкий, П.В. Оценка погрешностей результатов измерений / П.В. Новицкий, И.А. Зограф. – Л.: Энергоатомиздат, 1985. – 248 с.

Поступила 14.09.2012

SYNTHESIS OF SOFTWARE AND HARDWARE SYSTEMS SPEECH ESTIMATION BY LFM -SIGNAL: EXPERIMENTAL RESULTS

K. RAKHANOV

Results of comparative evaluation of theoretical and experimental data are presented, which are obtained by a realized synthesised software and hardware-based system of speech legibility evaluation. New theoretical data evaluating speech information leakage channels according to a uniform criterion are proven experimentally by LFM-signal method with high accuracy. A method of harmonic signal is realized on a new principle in software and hardware-based system, which allowed to visually confirm the viability of. Methodical (theoretical) inaccuracy on the same frequency of LFM-signal method and method of harmonic signal are equal. It is proven experimentally that the fine structure of LFM signal reduces methodical inaccuracy in comparison with the method of harmonic signal under the influence of some factors, the basic of which is irregularity of ARC.