

ческой конференции „Искусственный интеллект. Интеллектуальные и многопроцессорные системы – 2006». – Т.2. – Таганрог: Изд-во ТРТУ, 2006. – 404 с.

Надійшла 13.11.07

В статті розглянуте питання формалізації природної мови. Надана формальна модель словотворчої семантики, яка ураховує специфіку словотворчого значення в порів-

нянні з заданими граматичними та лексичними значеннями похідного слова.

In the article the formalization of semantics of natural language is considered. The formal model of semantics of creation of words is offered which takes into account word-formation specificity of meaning in comparison with the given grammatic and lexical meanings of a derivative word.

УДК 681.391

В. Н. Журавлев, Е. А. Архипова

АНАЛИЗ МЕТОДА РАСЧЕТА ПАРАМЕТРА ЭФФЕКТИВНОСТИ МАСКИРОВАНИЯ РЕЧИ В ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ

В статье проведен анализ метода цифровой корреляционной обработки контрольного фрагмента речи, который позволяет на основе расчета коэффициента корреляции обосновать аналитическую оценку параметра эффективности аддитивного маскирования речевых сигналов.

ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ

Среди разнообразных средств спецтехники в последние годы интенсивно развивается и совершенствуется рынок устройств, предназначенных для несанкционированного доступа (НСД) к конфиденциальной информации, содержащейся в речевом сигнале (РС), который является первичным общедоступным выражением результата мыслительного процесса человека.

При проектировании систем технической защиты речевой информации в выделенных помещениях (ВП) от утечки по каналам несанкционированного доступа (НСД) технической разведки противника (ТРП) основным параметром, определяющим, как показатель эффективности, так и категорию защиты, служит параметр словесной разборчивости $W(t)$. Данный параметр предлагается рассчитывать инструментально-расчетным методом [1–3], предполагающим следующие основные допущения.

1. Тестовый сигнал (модель РС) $si(\Delta\omega, t)$, маскирующий сигнал (МС) $sn(\Delta\omega, t)$ и сигнал канала утечки $su(\Delta\omega, t) = si(\Delta\omega, t) + sn(\Delta\omega, t)$ представляют собой случайные процессы с нормальным законом распределения плотности вероятности, при этом

$$\Delta\omega \times t \geq 10, \quad t \in [t_1, t_1 + T_a], \quad (1)$$

где $\Delta\omega$ – эффективная полоса частот РС, t_1 – время начала процесса анализа, T_a – интервал анализа эф-

фективности маскирования, который не превышает среднего интервала времени между ложными тревогами и выбирается из ряда фиксированных значений $T_a = (1, 5, 10, 30)$ секунд.

2. Тестовый и маскирующий сигналы представляют собой сигналы с равномерным распределением спектральной плотности мощности $N(\Delta\omega, t)$, т. е. со спектром «белого шума».

3. Точка канала НСД, в которой установлены средства ТРП, расположена на расстоянии 1 метр от источника тестового сигнала $si(\Delta\omega, t)$, при этом акустическое поле сигнала $su(\Delta\omega, t)$ полагается плоским с полностью активным акустическим сопротивлением среды распространения.

4. На основании предыдущего допущения, в части плоского акустического поля, а так же постоянства АЧХ рецептора средства ТРП на интервале времени T_a , отношение сигнал – помеха $SN(\Delta\omega, t)$ рассчитывается не как классическое [4] отношение эффективных энергий сигнала и помехи, поглощающихся рецептором средства ТРП за время интервала анализа:

$$SN(\Delta\omega, t) = 10 \lg \frac{\int_{t_1}^{T_a} p_{si}(\Delta\omega, t) dt}{\int_t^{T_a} p_{sn}(\Delta\omega, t) dt}, \quad t \in [t_1, t_1 + T_a], \quad (2)$$

где $p_{si}(\Delta\omega, t)$ и $p_{sn}(\Delta\omega, t)$ – мгновенные мощности сигнала и помехи, соответственно, а как логарифм отношения усредненных на интервале времени T_a акустических давлений, что возможно только для моногармонических анализируемых сигналов при активном входном сопротивлении рецептора давления.

В соответствии с отечественными руководящими документами [5], составляющими этого параметра для «белого» либо «розового» шумового сигнала, являются: с одной стороны – спектральная плотность мощности $N_{sn}(\Delta\omega, t)$ (для эталонного сигнала), с другой стороны – уровень звукового давления (акустические характеристики уровня выходного сигнала). Спектральную плотность мощности (СПМ) рекомендуется [6]

$$\text{рассчитывать по выражению: } N(\Delta\omega, t) = \frac{U_{\text{эфф}}^2}{1, 11\Pi_{\text{эфф}}},$$

где: $U_{\text{эфф}}$ – эффективное значение напряжения шумоподобного сигнала, $\Pi_{\text{эфф}}$ – значение эффективной полосы пропускания (терминология в соответствии с источником [6]). В рассматриваемом случае, сигналы $si(\Delta\omega, t)$ и $sn(\Delta\omega, t)$ содержат конечную сумму гармонических составляющих, рецептор звукового давления (микрофон либо слуховой аппарат человека) имеет комплексный характер входного сопротивления, а с учетом эффекта отоакустической эмиссии внутреннего уха, обладает существенной нестабильностью АЧХ на интервале времени T_a . На данном этапе можно акцентировать внимание на примере: квадрат амплитуды звукового давления идеального «белого» шума стремится к единице $p_{sn}^2(t) \rightarrow 1$, а его СПМ стремится к нулю:

$$N_{sn}(\Delta\omega, t) = \int_{t_1}^{t_1+T_a} sn(\Delta\omega, t)e^{-j\omega t} dt \rightarrow 0.$$

Инструментально-расчетный метод определения эффективности маскирования РС, изложенный в [1–3] трудоемок, содержит много эмпирических коэффициентов, которые не допускают его адаптации под РС конкретного диктора. Учитывая вышеизложенные основные допущения метода, можно констатировать, что его корректность вызывает сомнения, а исследование и анализ эффективности параметров маскирования РС в общем случае, представляет собой отдельную актуальную научно-техническую задачу, для которой объектом исследований является параметр информационной адекватности (разборчивости) сигнала $su(\Delta\omega, t)$ в точке НСД ТРП по отношению к тестовому сигналу $si(\Delta\omega, t)$.

1 ПРЕДЛАГАЕМЫЕ АЛГОРИТМЫ И РЕШЕНИЯ

Термины и определения. В связи с тем, что до настоящего времени в сфере активной защиты РС полностью не сформировался перечень терминов и определений, позволяющий углубленно анализировать объект исследований настоящей статьи, дополним, применив аксиоматический метод исследования, существующую

нормативную терминологию следующими терминами и определениями.

Шум – «беспорядочные звуковые колебания разной физической природы, характеризующиеся случайным изменением амплитуды, частоты и др.» [7]. В связи с тем, что на сигнал маскирования накладываются определенные ограничения [4], необходимо адаптировать данное определение к задачам СТЗИ.

Энергетическое маскирование – метод маскирования, при котором параметры МСП $sn(\Delta\omega, t)$ не адаптированы с параметрами РС $si(\Delta\omega, t)$, объем МСП $Qsn(t) = T_a\Delta\omega_{sn}(t)D_{sn}(t)$ равен объему канала утечки $Qku(t) = T_a\Delta\omega_{ku}(t)D_{ku}(t)$ и больше объема РС $Qsi(t) = T_a\Delta\omega_{si}(t)D_{si}(t)$ на всем интервале времени $t \in [t_1, t_1 + T_a)$ анализа $Qsn(t) = Qku(t) > Qsi(t)$, $t \in [t_1, t_1 + T_a)$, где $\Delta\omega_{sn}(t)$, $\Delta\omega_{si}(t)$, $\Delta\omega_{ku}(t)$ и $\Delta D_{sn}(t)$, $\Delta D_{si}(t)$, $\Delta D_{ku}(t)$ – эффективный диапазон частот сигналов $sn(\Delta\omega, t)$, $si(\Delta\omega, t)$ и канала утечки $su(\Delta\omega, t)$ и их динамические диапазоны, соответственно.

Параметрическое маскирование – метод маскирования, при котором параметры МСП $sn(\Delta\omega, t)$ адаптированы к параметрам РС $si(t)$ и объем МСП $Qsn(t)$ меньше объема канала утечки $Qku(t)$ и равен (либо больше) объема РС $Qsi(t)$ на интервале времени анализа $Qsn(t) < Qku(t) \geq Qsi(t)$, $t \in [t_1, t_1 + T_a)$.

Маскирующий сигнал помехи (МСП) – синтезированный СТЗИ сигнал $sn(\Delta\omega, t)$, который аддитивно воздействует на сигнал $si(\Delta\omega, t)$ в канале утечки.

$$N_{su}(\Delta\omega, t) = N_{sn}(\Delta\omega, t) + N_{si}(\Delta\omega, t), \quad (3)$$

где $N_{su}(\Delta\omega, t)$ – СПМ сигнала утечки в точке НСД ТРП. Данное воздействие вызывает эффект уменьшения объема $Qku(t)$ [8] канала утечки, который, в свою очередь, влияет на параметр информационной адекватности $W(t)$ в точке НСД ТРП.

Отношение сигнал – помеха (по МСП) – отношение спектральных плотностей мощности информационного сигнала и маскирующего сигнала помехи в полосе частот канала утечки, выраженное в децибелах (дБ).

$$SN(\Delta\omega, t) = 10 \lg \frac{\int_{\omega_1}^{\omega_2} N_{si}(\Delta\omega, t) d\omega}{\int_{\omega_1}^{\omega_2} N_{sn}(\Delta\omega, t) d\omega}, \quad \Delta\omega \in [\omega_1, \omega_2]. \quad (4)$$

Адекватность информации в точке НСД – вероятностный параметр $AD(t)$ соответствия, создаваемого ТРП, информативного смыслового образа $Oti(t)$, реальному информативному образу $Oi(t)$, который передается в выделенном помещении.

Прагматическая адекватность – логический параметр $PA(t)$, определяющий практическую ценность информации канала утечки для ТРП. В дальнейшем, по умолчанию, будем полагать, что данный параметр принимает значение «истина», $PA(t) = \text{true}$.

Синтаксическая адекватность – вероятностный параметр $SiA(t)$, формы представления сигнала РС $si(t)$ в канале утечки, не затрагивающий его смыслового содержания, например, язык общения.

Семантическая адекватность – вероятностный параметр $SeA(t)$ эффективности СТЗИ, который определяет соответствие передаваемых в выделенном помещении и получаемых ТРП смысловых образов. В случае определения семантической адекватности, как структурного параметра, то она будет характеризоваться изменением объема РС $Qsi(t)$ в точке НСД ТРП относительно объема канала утечки $Qku(t)$ на интервале времени анализа.

$$SeA(t) = \frac{\partial Qsi(t)}{\partial Qku(t)}, \quad t \in [t_1, t_1 + T_a]. \quad (5)$$

Системный параметр $SeA(t)$ на практике определяется в точке доступа ТРП к каналу НСД и измеряется в процентах разборчивости $W(t)$ счетного количества информационных элементов языка общения, которыми являются фонемы.

Для обеспечения логической последовательности анализа эффективности системных методов защиты РС произведем ранжирование предлагаемых параметров по эффективности их влияния на достоверность и надежность СТЗИ: 1) прагматическая адекватность; 2) семантическая адекватность; 3) синтаксическая адекватность.

Анализ волнового пакета акустического сигнала, распространяющегося в дисперсионной среде. В связи с тем, что, в общем случае, многолучевое и не плоское распространение сигналов $si(\Delta\omega, t)$ и $si(\Delta\omega, t)$ проявляется в их частотной и временной их дисперсии в объеме выделенного помещения, что искусственно повышает эффективность МСП. Худший случай минимальной эффективности маскирования будет наблюдаться для однолучевого распространения сферической звуковой волны сигнала $su(\Delta\omega, t)$, который должен являться мерой категорирования выделенного помещения. Для данного случая проведем анализ механизма распространения и взаимодействия акустических колебаний в воздушной среде.

Как известно, функция, описывающая гармоническую волну [9], распространяющуюся в бездисперсионной среде, записывается в виде:

$$u(x, t) = A \cos(kx - \omega t), \quad (6)$$

где $k = 2\pi/\lambda$ – волновой вектор, ω – круговая частота.

Анализ выражения (6) показывает, что можно ввести фазовую функцию $\phi(x, t)$ косинусоидальной бегущей волны, распространяющейся в положительном направлении оси OX , как аргумент волновой функции $\cos(\omega t - kx)$:

$$\phi(x, t) = \omega t - kx.$$

При анализе поведения гребня волны ($\cos\phi(x, t) \rightarrow \max$) или ее впадины ($\cos\phi(x, t) \rightarrow \min$), по мере увеличения времени необходимо переходить к большим значениям x так, чтобы фаза $\phi(x, t)$ была постоянной. Условие постоянства фазы с математической точки зрения означает, что полный дифференциал функции $\phi(x, t)$, имеющий вид

$$d\phi = \left(\frac{\partial\phi}{\partial t}\right)dt + \left(\frac{\partial\phi}{\partial x}\right)dx = \omega dt - kdx, \quad (7)$$

равен нулю. Приравнявая (7) нулю, находим условие постоянства фазы $\frac{dx}{dt} = v_f = \frac{\omega}{k}$, где v_f – фазовая скорость волны, которое дает связь между фазовой скоростью волны, частотой волны и волновым вектором. Условия распространения волны определяются свойствами среды. При этом ω , а, следовательно, и фазовая скорость, могут зависеть от волнового вектора k . Как указывалось, в общем случае рассматриваемые сигналы не являются плоскими волнами, их фазовая скорость v_f зависит от волнового вектора [10], поэтому их можно считать диспергирующими. Диспергирующая волна, представляющая собой суперпозицию бегущих волн с различными волновыми числами, будет менять свою форму по мере распространения в пространстве, так как составляющие с различными длинами волн распространяются с различными скоростями.

Рассмотрим задачу об описании движения волнового пакета, локализованного в момент времени $t = 0$ в пространстве. Данное условие означает, что огибающая волнового пакета является функцией достаточно быстро стремящейся к нулю при $x \rightarrow \pm\infty$. Введем обозначение $f(x) = u(x, 0)$. Условие «быстрого стремления функции к нулю» обеспечивает возможность ее разложения в ряд Фурье. Если функция $f(x)$ не периодическая функция по координате x , то ее суперпозиция составляющих ее функций непрерывна по переменной k , и выражается через интеграл Фурье $f(x) = \int_{-\infty}^{\infty} A(k)e^{ikx} dk$, где $A(k) = \int_{-\infty}^{\infty} f(x)e^{-ikx} dx$. Каждая гармоническая составляющая в данном выражении определяет собственную гармоническую волну с частотой $\omega = \omega(k)$, т. е. каждая частотная составляющая бегущей волны распространяется со своей собственной фа-

зовою швидкістю $v_f = \frac{\omega(k)}{k}$. Іскома функція $u(x, t)$, описуюча бегущую волну, являється суперпозицією гармонічних бегущих волн, образующих исследуемые сигналы. Это означает, что найти $u(x, t)$ можно заменой kx на $[kx - \omega(k)t]$ в каждой гармонической составляющей суперпозиции $u(x, t) = \int_{-\infty}^{\infty} A(k)e^{i[kx - \omega(k)t]} dt$.

Однако, для того, чтобы использовать алгоритмы цифровой обработки сигналов при нахождении численных значений функции $u(x, t)$ вычисление интеграла необходимо проводить на интервалах конечной длительности, т. е. проводить разложение функции не в интеграл, а в ряд Фурье. В данном случае, как известно [11], при расчете значений функции $f(x)$, следует использовать следующие выражения:

$$f(x) = \sum_{n=1}^N A(n)e^{iknx}, \quad k = \frac{2\pi}{x_{\max} - x_{\min}},$$

$$A(n) = \frac{1}{x_{\max} - x_{\min}} \int_{x_{\min}}^{x_{\max}} f(x)e^{-iknx} dx, \quad n = 0, 1, \dots, N,$$

$$u(x, t) = \sum_{n=1}^N A(n)e^{i(kn(x - x_{\min}) - \omega(kn))}, \quad (8)$$

где N – число значений функции $f(x)$.

Таким образом, можно сделать вывод, что в точке НСД ТРП происходит суммирование спектральных плотностей мощности гармонических составляющих сигналов в соответствии с (3). Исследование отношения $SN(\Delta\omega, t)$ необходимо производить на интервале времени T_a , в течение которого основные спектральные параметры сигналов не претерпевают существенных изменений, т. е. на интервале стационарности.

В работе исследуются случайные процессы $si(\Delta\omega, t)$, $sni(\Delta\omega, t)$ и $sn(\Delta\omega, t)$, которые на интервале времени T_a обладают свойством стационарности [12]. Основываясь на результатах ранее проведенных исследований, положим, что исследуемые случайные процессы распределены по нормальному закону, т. о. известна их главная статистическая характеристика – плотность распределения вероятности. Важной характеристикой случайных процессов является их автокорреляционные функции (АКФ), определяемые как

$$R_{ss}(\tau) = \frac{1}{T_a} \int_0^{T_a} s(\Delta\omega, t)s(\Delta\omega, t + \tau) dt, \quad (9)$$

где $s(\Delta\omega, t)$ – исследуемый процесс.

Анализ АКФ определяет: полную мощность исследуемого процесса, равную значению $R_{ss}(0)$, мощность постоянной составляющей на интервале времени T_a ,

определяемой как $R_{ss}(T_a)$, и интервал корреляции τ_0 случайного процесса, который определяет верхнюю частоту ω_2 исследуемой полосы частот $\Delta\omega$.

Детерминированной характеристикой случайного процесса является СПМ $N(\Delta\omega, t)$, показывающая, как распределена мощность сигнала в исследуемой полосе частот $\Delta\omega$. СПМ случайного процесса и его АКФ связаны преобразованием Фурье (теорема Винера-Хинчина):

$$N(\Delta\omega, t) = \int_0^{T_a} R_{ss}(\tau)e^{i\omega\tau} d\tau. \quad (10)$$

Анализ амплитудного спектра и СПМ сигналов помехи. Представим исследуемые сигналы $s(\Delta\omega, t)$ моделью в виде упорядоченного набора прилегающих друг к другу фрагментов длиной T_a :

$$s(\Delta\omega, t) = \sum_{i=1}^N s_i(\Delta\omega, t), \quad (11)$$

где $s_i(t) =$

$$= \begin{cases} s(t), & t \in [t_i, t_i + T_a), \quad t_i = t_0 + (i - 1)T_a, \quad i = \overline{1, N}, \\ 0, & t_i + T_a < t \leq t_i. \end{cases}$$

Для упрощения последующего анализа полагаем, что в пределах каждого отличного от 0 фрагмента значений сигнала $s_i(t)$ амплитуды центрированы и распределены по нормальному закону с дисперсией $D[s_i(t)]$.

Анализ спектрального коэффициента корреляции СПМ как параметра эффективности маскирования речи. В связи с тем, что зависимости речевого $si(\Delta\omega, t)$ и маскированного $su(\Delta\omega, t)$ сигналов не имеют функционального характера, т. е. равномерному изменению одного признака соответствует изменение другого признака в среднем, можно, для оценки тесноты связи между исследуемыми сигналами, применить методы корреляционного анализа СПМ, в частности коэффициент корреляционного отношения Пирсона [13]:

$$r = \frac{\sum_{i=1}^N (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^N (y_i - \bar{y})^2}}, \quad (12)$$

где x и y – исследуемые СПМ, \bar{x} и \bar{y} – выборочные средние значения, определяемые (в частности, для x)

$$\text{как } \bar{x} = \frac{1}{N} \sum_{i=1}^N x_i.$$

Таким образом, в качестве системного объективного параметра семантической адекватности (5) сигналов

в точке доступа ТРП к каналу НСД можно принять коэффициент корреляционного отношения Пирсона, определяемый в соответствии с (12), и рассчитываемый для функций СПМ $N(\Delta\omega, t)$ на т. н. «слоговых» временных интервалах T_a квазистационарного состояния речевых сигналов. Категорирование выделенных помещений можно производить в соответствии со шкалой Чеддока, которая позволяет укрупнено объединять коэффициенты корреляции в определенных интервалах тесноты связи между исследуемыми сигналами.

2 РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ

Методика эксперимента. Анализ сигналов проводился на персональном компьютере, который оснащен звуковой картой SB Audigy2, диапазоном квантования 16 бит и частотой дискретизации $f_s = 48$ кГц, отношением сигнал – шум порядка 80 dB. В качестве РС $si(\Delta\omega, t)$ анализировалось контрольное слово «лето», которое содержит гласные и согласные, а также вокализованные и невокализованные фонемы. Контрольное слово произносилось мужским голосом. Программирование алгоритма корреляционной обработки производилось в среде пакета программ MatLab 6.5. Параметр сегментации сигнала $si(\Delta\omega, t)$ на временные отрезки соответствовал слоговой постоянной времени $T_a = 23$ ms. Свойства центрированности реализации обеспечивается формой РС, симметричной относительно нуля. Интервал дискретизации $1/f_s = 20$ мкс значительно меньше максимального интервала корреляции $1/2\omega_2$ сигнала $si(\Delta\omega, t)$, что позволяет утверждать о состоятельности выборочных оценок математических ожиданий и дисперсий, рассчитываемых при анализе. Преобразования Фурье, корреляционные интегралы (10) и коэффициент корреляции (12) рассчитывались стандартными процедурами пакета MatLab.

В качестве сигналов маскирования $sn(\Delta\omega, t)$ исследовались два процесса: со спектральной плотностью мощности «белого» шума («HG»), который формировался массив значений стандартной процедурой пакета MatLab; и сигнал промышленного генератора типа «ANG2200» («Nang»). Перед проведением анализа задавалось интегральное значение отношения сигнал – помеха $SN(\Delta\omega, t)$, с постоянной интегрирования равной длительности контрольного слова, рассчитанное по общепринятой методике отношения среднеквадратических значений амплитуд сигнала и помехи. Маскировка сигнала $si(\Delta\omega, t)$ выполнялась на интервале длительности контрольного слова методом аддитивного маскирования СПМ в соответствии с выражением (3). Для проведения корреляционного анализа сигнал $N_{su}(\Delta\omega, t)$ сегментировался на N временных интервалов длительностью T_a в соответствии с (11). На каж-

дом интервале анализа T_a рассчитывались точечные оценки коэффициента корреляции $r(SN)$ (12).

Результаты экспериментов. На рис. 1 приведены результаты работы программы анализа амплитудного спектра и СПМ для двух сигналов маскирования – «HG» (левые рисунки) и «Nang» (правые рисунки). На верхних рисунках приведены временные диаграммы сигналов $sn(t)$, на средних – их амплитудные спектры, на нижних – СПМ.

Проведя анализ спектров (рис. 1) можно сделать выводы, что характеристики амплитудных спектров отличаются от СПМ как распределением амплитуд спектральных составляющих в исследуемом диапазоне частот, так и амплитудой спектральных составляющих, которая отличается более чем на 20 dB. Для сигнала «Nang» наблюдается изменение спектрального состава в высокочастотной области СПМ (>2 kHz), что говорит о корреляционной связи его высокочастотных составляющих, которые не участвуют в процессе маскирования РС.

На рис. 2 приведены результаты работы программы анализа точечных параметров эффективности маскирования контрольного слова «лето» для двух сигналов маскирования – «HG» (верхние рисунки) и «Nang» (нижние рисунки). На левых рисунках приведены зависимости коэффициента корреляции $r = f(T_a)$, на средних – зависимость амплитудного отношения сигнал – помеха от временного интервала анализа контрольного слова $SN[A(t)] = f(T_a)$, на правых – зависимость отношения сигнал – помеха СПМ от временного интервала анализа контрольного слова $SN[N(t)] = f(T_a)$.

Проведя анализ графиков (рис. 2), можно сделать выводы, что характеристики зависимости коэффициента корреляции $r = f(T_a)$ показывают большую эффективность сигнала «Nang» по сравнению с сигналом «белый шум», что подтверждается результатами ранее проведенных исследований [14]. Оценка параметра сигнал – помеха завышена, при расчете ее по методу [1–3], форма характеристик зависимостей $SN[A(t)] = f(T_a)$ и $SN[N(t)] = f(T_a)$ отличаются друг от друга, что говорит о различных соотношениях параметров суммируемых сигналов, что подтверждается предыдущим экспериментом настоящей статьи и сферичностью модели исследуемых акустических волн. Параметр сигнал – помеха является переменным на интервале длительности контрольного слова, его приблизительное соответствие интегральному (–10 dB) наблюдается только на временных интервалах вокализованных фонем.

На рис. 3 приведены результаты работы программы анализа точечных параметров зависимости коэффициента корреляции $r = f(SN, T_a)$ при маскировании контрольного слова «лето» двумя сигналами – «HG»

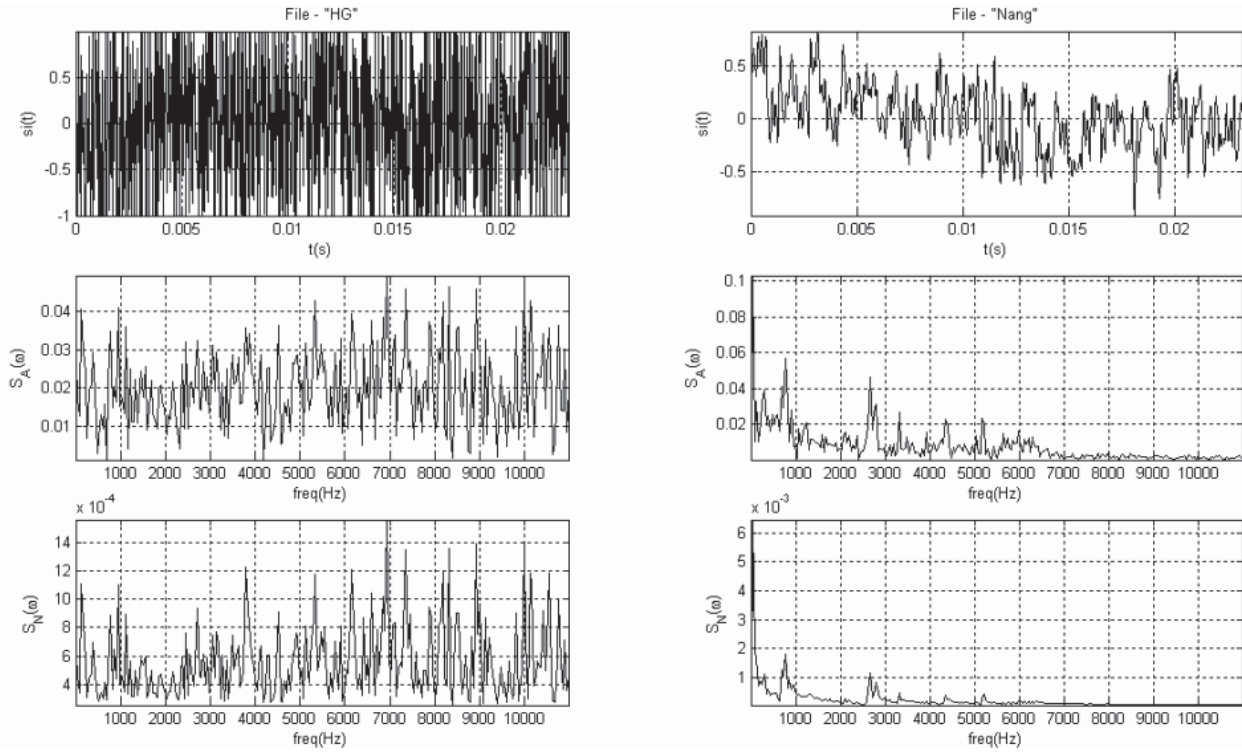


Рисунок 1 – Графики исследования амплитудных спектров и СПМ сигналов маскирования

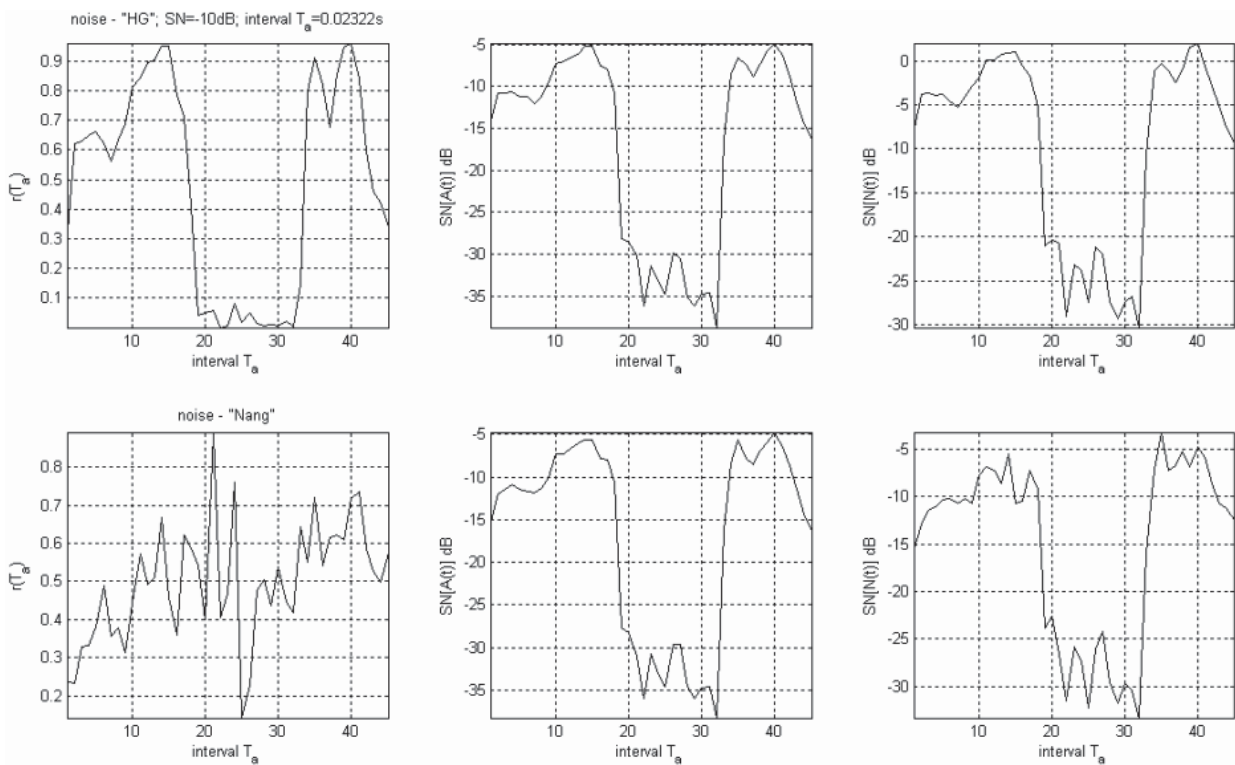


Рисунок 2 – Графики исследования зависимости коэффициента корреляции $r = f(T_a)$ и точечных отношений сигнал – помеха (амплитудного спектра и СПМ) аддитивного маскирования контрольного слова с интегральным отношением сигнал – помеха $SN = -10$ dB

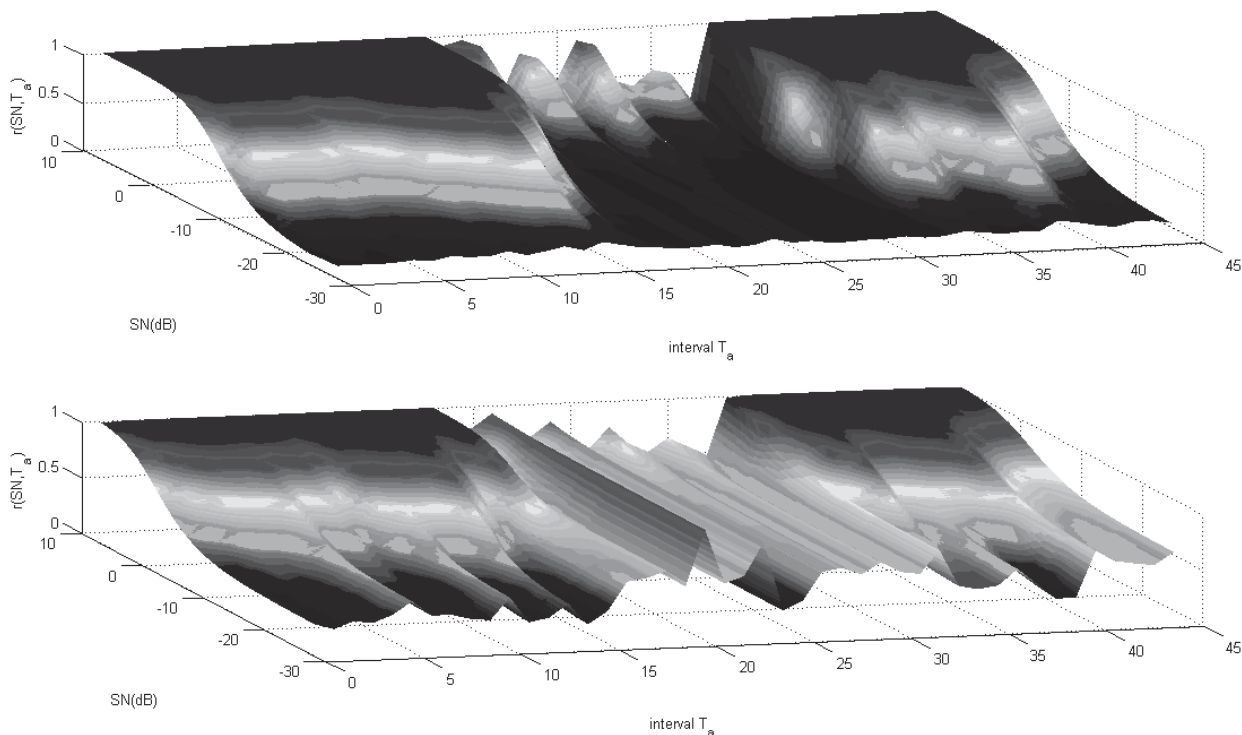


Рисунок 3 – Графики зависимостей значений точечных оценок коэффициента корреляции $r = f(SN, T_a)$ от интегрального значения отношения сигнал – помеха $SN[N(t)]$ от 10 до -30 dB

(верхний рисунок) и «Nang» (нижний рисунок) при изменении интегрального параметра сигнал – помеха $SN[N(t)]$ от 10 до -30 dB.

Проведя анализ графиков (рис. 3) можно сделать выводы, что характеристики зависимости коэффициента корреляции $r = f(SN, T_a)$ показывают большую эффективность сигнала «Nang» по сравнению с сигналом «белый шум» во всем диапазоне изменений интегрального параметра сигнал – помеха, что обобщает результаты предыдущего эксперимента. Характер изменения зависимости $r = f(SN, T_a)$ для сигнала «Nang» показывает внутренние корреляционные связи сигналов контрольного слова и маскирующего сигнала, особо это проявляется не интервале времени активности фонемы «т».

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

1. Предложенный и исследованный аналитический корреляционный параметр эффективности маскирования $r = f(T_a)$, определяемый в соответствии с выражением (13), является мерой оценки тесноты связи между исследуемыми сигналами $si(\Delta\omega, t)$ и $su(\Delta\omega, t)$, т. е. семантической адекватности в точке НСД ТРП $SeA(t) = r(t)$, $t \in [t_1, t_1 + T_a]$.

2. Приведенный анализ зависимости параметра отношения сигнал – помеха от вокализации фонем контрольного слова позволяет сделать вывод о том, что:

- в связи с тем, что РС на интервале длительности слова (или предложения) не стационарен по параметру постоянства дисперсии, при измерении и расчете $SN(t)$ необходимо учитывать только СПМ на стационарных интервалах времени вокализованных фонем, которые обладают природной помехозащищенностью;

- постоянная времени измерения СПМ должна укладываться в интервал стационарности, не может быть менее «слового интервала» $T_a \geq 15$ ms и не превосходить времени активности вокализованной фонемы, что при эффективной полосе частот $\Delta\omega = 3000$ Hz соответствует требованиям (1).

3. Предложенный метод позволяет применять в качестве тестовых сигналов ключевые слова конкретных дикторов, и, таким образом, адаптировать СПМ для проведения конфиденциальных переговоров ограниченного количества собеседников.

4. Корректность исследованных в проведенном эксперименте характеристик изменения параметра эффективности маскирования с общепринятыми параметрами разборчивости РС при наличии помех необходимо подтвердить проведением артикуляционных испытаний по стандартной методике [15].

В статье проведен критический анализ метода расчета параметра эффективности маскирования речи в технических каналах утечки информации. Предложен и подтвержден экспериментальными исследованиями метод цифровой корреляционной обработки контрольного фрагмента речи, который устраняет недостатки существующего метода и позволяет на основе расчета коэффициента корреляции АКФ сегментов сигнала контрольного слова и сигнала канала утечки рассчитать параметр эффективности аддитивного маскирования речевых сигналов.

ПЕРЕЧЕНЬ ССЫЛОК

1. Дворянкин С. В., Макаров Ю. К., Хорев А. А. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Защита информации. INSIDE. – 2007. – № 2. – С. 18–25.
2. Хорев А. А. Оценка эффективности защиты информации от утечки по техническим каналам // Специальная техника, 2006. – № 6. – С. 53–61.
3. Хорев А. А. Оценка эффективности защиты информации от утечки по техническим каналам // Специальная техника, 2007. – № 1. – С. 51–64.
4. Шеннон. Связь при наличии шума. В кн. Работы по теории информации и кибернетике. – М.: Издательство иностранной литературы, 1963. – 827 с.
5. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами впроміювання. Класифікація та загальні технічні вимоги. НД ТЗІ-Р-001-2000. ДСТСЗІ СБ України. – Київ.: – 2000. – 9 с.
6. НД ТЗІ 2.3-003-2001. Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методи-

- ка випробувань. ДСТСЗІ СБ України. – Київ.: – 2001. – 21 с.
7. Советский энциклопедический словарь. / Гл. ред. А. М. Прохоров. 4-е изд. – М.: Сов. энциклопедия, 1989. – 1632 с.
 8. Отт Г. Методы подавления шумов и помех в электронных системах. /пер с англ. – М.: Мир, 1978. – 317 с.
 9. Крауфорд Ф. Волны. – М.: Наука, 1974. – 358 с.
 10. Акустика: Справочник. Под ред. М.А. Сапожкова. – М.: Радио и связь, 1989. – 336 с.
 11. Цифровая обработка сигналов / А. Б. Сергиенко – СПб.: Питер, 2003. – 608 с.
 12. Цвикер Э., Фельдкеллер Р. Ухо как приемник информации. Пер. с нем. Под редакцией Б. Г. Белкина. – М.: Связь, 1971. – 255 с.
 13. Гайдышев И. Анализ и обработка данных: специальный справочник. – СПб: Питер, 2001. – 752 с.
 14. Журавлев В. Н., Прокофьев М. И. Анализ результатов артикуляционных и сегментальных испытаний сигнала маскирования речи. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2006. – № 13. – С. 36–48.
 15. ГОСТ Р 50840-95. Государственный стандарт Российской Федерации. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. Издание официальное. – М.: Госстандарт России, 1997. – 12 с.

Надійшла 3.10.07
Після доробки 17.10.07

В статті проведений аналіз методики цифрової кореляційної обробки контрольного фрагменту мови, що дозволяє на основі розрахунку коефіцієнта кореляції обґрунтувати аналітичну оцінку параметра якості передачі сигналу мови по каналам зв'язку та проводити аналіз ефективності адитивного маскування мовних сигналів.

The method of check utterance digital correlation processing, which allows to substantiate the communication path quality criteria analytic estimation on the base of correlation coefficient calculation and to analyze the speech signal additive masking effectiveness is under review.

УДК 004.75

М. Б. Ильяшенко

АЛГОРИТМ ОПТИМАЛЬНОГО РЕЗЕРВИРОВАНИЯ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ ПО КРИТЕРИЮ ЭФФЕКТИВНОГО ИСПОЛЬЗОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ УЗЛОВ

В работе предлагается алгоритм оптимального резервирования вычислительных ресурсов, способный осуществлять поиск областей резервирования, согласно критериям оптимальности по числу и максимальной загруженности задействованных вычислительных узлов. Приводится детальное описание алгоритма и набора предварительных условий, которые сужают область поиска переробной части алгоритма.

© Ильяшенко М. Б., 2007

ВВЕДЕНИЕ

Алгоритмы управления распределенными вычислительными ресурсами, как правило, используют одну из двух возможных парадигм: централизованное управление ресурсами [1, 2] или контроль ресурсов локальными приложениями [3, 4]. Каждая парадигма имеет свои достоинства и недостатки, в частности, централи-