УДК 621.396

А. Н. ОЛЕЙНИКОВ, канд. техн. наук, Д. М. СОСНОВЧИК

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ МЕТОДОМ АДАПТИВНОЙ ФИЛЬТРАЦИИ

Защита речевой информации занимает важное место в комплексной системе обеспечения информационной безопасности. Несанкционированный съем речевой информации может реализовываться непосредственно через акустический (воздушный или вибрационный) канал утечки информации, либо с использованием различных составных технических каналов утечки информации, включающих в себя акусто-электронные, акусто-оптические и другие каналы утечки. Для обеспечения технической защиты акустической информации в настоящее время используется большое число методов, основными из которых являются:

– информационное скрытие, предусматривающее техническое закрытие (частотное и временное аналоговое скремблирование и использование вокодеров) и цифровое шифрование речевых сигналов;

– энергетическое скрытие, осуществляющееся способами звукоизоляции, звукопоглощения, глушения в помещениях и зашумления функционального канала связи помехами, обеспечивающими маскировку речевых сигналов;

– обнаружение и идентификация сигналов закладных устройств (ЗУ), а также локализация и нейтрализация самих ЗУ.

Аналоговые скремблеры и вокодеры относительно недорогие устройства, но обеспечивают в основном тактический уровень защиты. Аппаратура шифрования, применяемая в функциональных линиях связи и гарантирующая стратегический уровень защиты, очень дорогая. Кроме этого, данные устройства требуют наличия полукомплектов аппаратуры у обоих абонентов и не могут быть применены для защиты речевых сигналов в помещениях. Современные методы обнаружения и нейтрализации ЗУ не обеспечивают стопроцентную вероятность их отсутствия после проведения поисковых работ. Поэтому сейчас весьма перспективными являются методы энергетического скрытия речевых сигналов, совмещенные с устройствами адаптивной фильтрации. Адаптивные фильтры позволяют санкционированному получателю, который сам является постановщиком помехи с известными параметрами, извлечь полезную речевую информации из смеси сигнал+помеха. В настоящее время известны устройства, построенные по данному принципу для защиты речевой информации как в телефонных каналах связи, так и в помещениях. Это односторонние маскираторы телефонных разговоров и электронные «комнаты» для ведения конфиденциальных переговоров[1,2]. Основой этих устройств являются адаптивные фильтры, характеристики которых определяют качество работы устройств защиты речевой информации.

В данной статье проведен сравнительный анализ между двумя различными адаптивными алгоритмами подстройки коэффициентов цифрового фильтра методом наименьших квадратов (МНК) и алгоритмом последовательной регрессии (АПР) [3-5], а также сравнительная характеристика эффективности работы алгоритмов при наличии заграждающих помех различной структуры.

Особенностью работы систем адаптивной фильтрации является то, что априори требуется знать либо вид обрабатываемого сигнала, либо вид заграждающей помехи. В нашем случае производится анализ работы алгоритмов при обработке речевых сообщений, которые предварительно неизвестны, а известен вид заграждающей помехи, которую мы формируем сами. Как было сказано выше, адаптивный алгоритм корректирует (подстраивает) коэффициенты цифрового фильтра. С практической точки зрения более удобными являются трансверсальные фильтры (без обратных связей). Фильтры с обратными связями, как и любая система, могут быть нестабильными. Поэтому необходимо контролировать диапазон изменения коэффициентов фильтра, что на практике трудно выполнимо. На рис. 1 изображе-

на структурная схема адаптивного фильтра. По своему виду он близок к цифровому фильтру, но имеется дополнительный вход для опорного сигнала, который обозначен как d_k, а w_0, $w_1 \ldots w_n$ – коэффициенты фильтра.

Подробное описание алгоритмов приведено в [3]. Остановимся лишь на общем виде выше упомянутых алгоритмов. Итеративный процесс коррекции коэффициентов фильтра может быть представлен в виде:

а) для метода наименьших квадратов:

$$\mathbf{W}_{k+1} = \mathbf{W}_k + 2\mu\varepsilon_k \mathbf{X}_k .$$

$$\varepsilon_k = d_k - \mathbf{X}_k^T \mathbf{W}_k , \qquad (1)$$

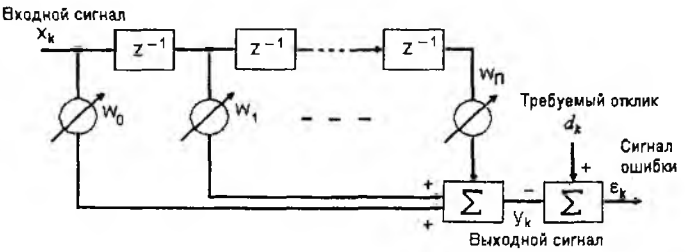

Рис. 1

где $\mathbf{W}_k$ – вектор коэффициентов адаптивного фильтра (w_0, $w_1 \ldots w_n$);

d_k – отсчет опорного сигнала;

$\mathbf{X}_k$, $\mathbf{X}_k^T$ – вектор отсчетов входного сигнала;

2μ – параметр, определяющий скорость сходимости и устойчивость алгоритма;

б) для алгоритма последовательной регрессии:

Первая итерация алгоритма (к=0):

$$\mathbf{Q}_0 = A \times \mathbf{I}; \qquad (2)$$

$\mathbf{W}_0$ = начальный вектор весовых коэффициентов;

$$\mathbf{W}_1 = \mathbf{W}_0 + 2\mu\lambda_{cp}\mathbf{Q}_0\epsilon_0\mathbf{X}_0;$$

последующие итерации алгоритма ($к \geq 1$):

$$\mathbf{W}_{k+1} = \mathbf{W}_k + \frac{2\mu\lambda_{cp}(1-\alpha^{k+1})}{1-\alpha}\mathbf{Q}_k\epsilon_k\mathbf{X}_k;$$

$$\alpha = 2^{-1/\tau};$$

$$\mathbf{S} = \mathbf{Q}_{k-1}\mathbf{X}_k;$$

$$\gamma = \alpha + \mathbf{X}_k\mathbf{S}^T;$$

$$\mathbf{Q}_k = \frac{1}{\alpha}\left(\mathbf{Q}_{k-1} - \frac{1}{\gamma}\mathbf{S}\mathbf{S}^T\right);$$

$$\mu\lambda_{cp} << 1,$$

где $\mathbf{X}_k$ – вектор отсчетов входного сигнала;

$\epsilon_к$ – вычисляется по выражению (1);

А – константа;

I – единичная матрица;

τ – длина стационарного сегмента сигнала;

$2\mu\lambda_{cp}$ – параметр, определяющий скорость сходимости и устойчивость алгоритма.

При анализе свойств и характеристик приведенных адаптивных алгоритмов будем использовать следующие виды заграждающих помех: полигармонический шум, белый шум и речеподобную помеху.

Адаптивный процесс фильтрации при обработке речевых сигналов можно оценивать по качеству выделяемого сигнала из смеси сигнал+шум, времени адаптации процесса и степени

подавления заграждающей помехи. Под временем адаптации следует подразумевать количество выполненных итераций, в течение которых адаптивный алгоритм находит необходимую комбинацию коэффициентов фильтра, в результате чего на выходе прослушивается передаваемое речевое сообщение с минимальным уровнем заграждающей помехи.

В приведенных адаптивных алгоритмах время адаптации зависит от параметров 2μ и $2\mu\lambda_{ср}$. В реальной системе значения этих коэффициентов значительно меньше единицы, что увеличивает время адаптации алгоритма, но обеспечивает его большую устойчивость. Чем ближе параметр сходимости к единице, тем выше вероятность расхождения алгоритма.

Рассмотрим работу алгоритмов при фильтрации речевого сигнала на фоне полигармонического шума, состоящего из пяти частотных составляющих: 500, 750, 1000, 1250, 1500 Гц. Необходимо отметить то, что в нашем случае, производилась цифровая адаптивная фильтрация. При этом использовалась частота оцифровки речи 11025 Гц. Спектры шума и речевого сигнала приведены на рис. 2 а и б соответственно. Мощность шума такова, что при прослушивании смеси шума и речи невозможно однозначно ответить о наличии речевого сигнала.

Рис. 2

Параметры сходимости 2μ и $2\mu\lambda_{ср}$ выбраны равными 0,0005. При этом обеспечивается однозначная сходимость алгоритмов. Для АПР значение коэффициента у матрицы Q_0 (2) взято равным A = 1000, а длина стационарного сегмента сигнала τ = 500. Порядок фильтров N=20. На рис. 3 представлены результаты адаптивной фильтрации. Рядом с временным представлением сигнала (левый рисунок) находится спектр этого сигнала (правый рисунок). Спектры вычислялись по второй половине выходного сигнала, где уже отсутствует влияние процесса адаптации. Рис. 3а – это оригинал передаваемого сообщения; рис. 3б – сигнал на

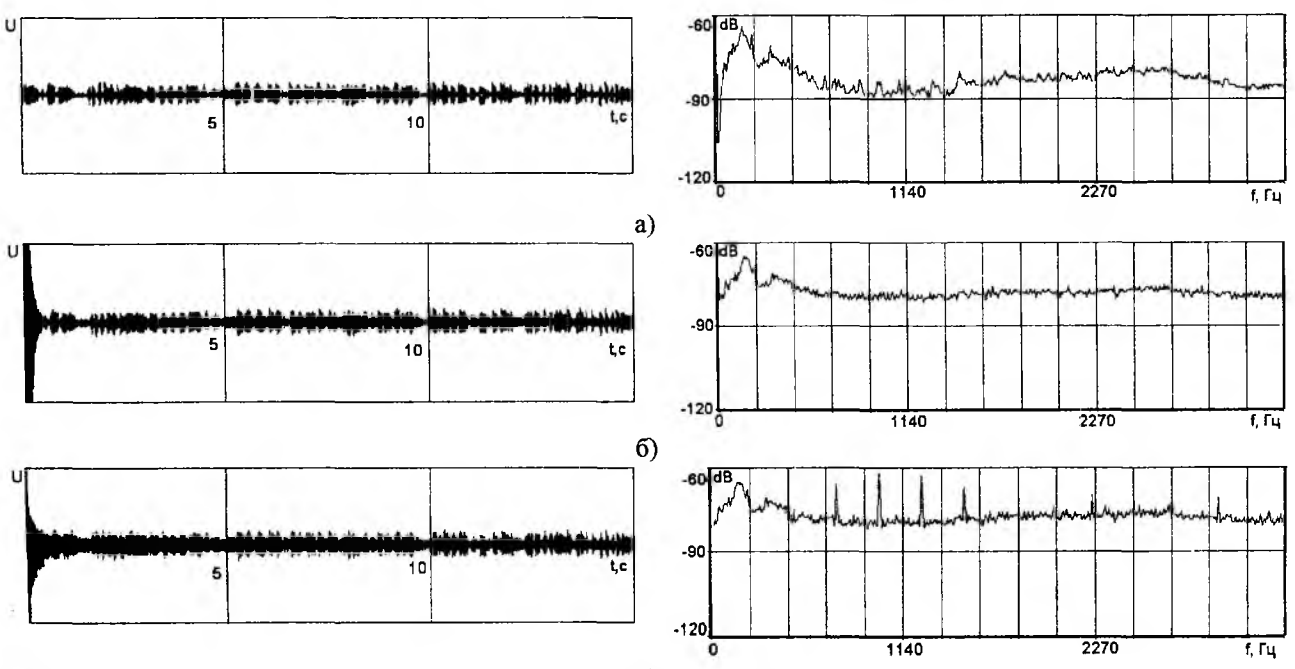

Рис. 3

выходе адаптивного фильтра, коэффициенты которого корректировались по АПР; рис. 3в – сигнал на выходе адаптивного фильтра, коэффициенты которого корректировались по МНК. Сравнивая результаты работы алгоритмов, следует отметить следующее:

а) АПР сходится быстрее, чем МНК, что видно при сопоставлении временных диаграмм сигналов на выходе фильтров с оригиналом;

б) В спектре выходного сигнала, обработанного по МНК, отчетливо видны составляющие шума, но их мощность существенно меньше и можно разобрать передаваемое сообщение. В спектре сигнала, обработанного по АПР, полностью отсутствуют составляющие помехи.

Уменьшим значение параметров 2μ и $2\mu\lambda_{ср}$ до 0,0001 и посмотрим на время адаптации алгоритмов (рис. 4).

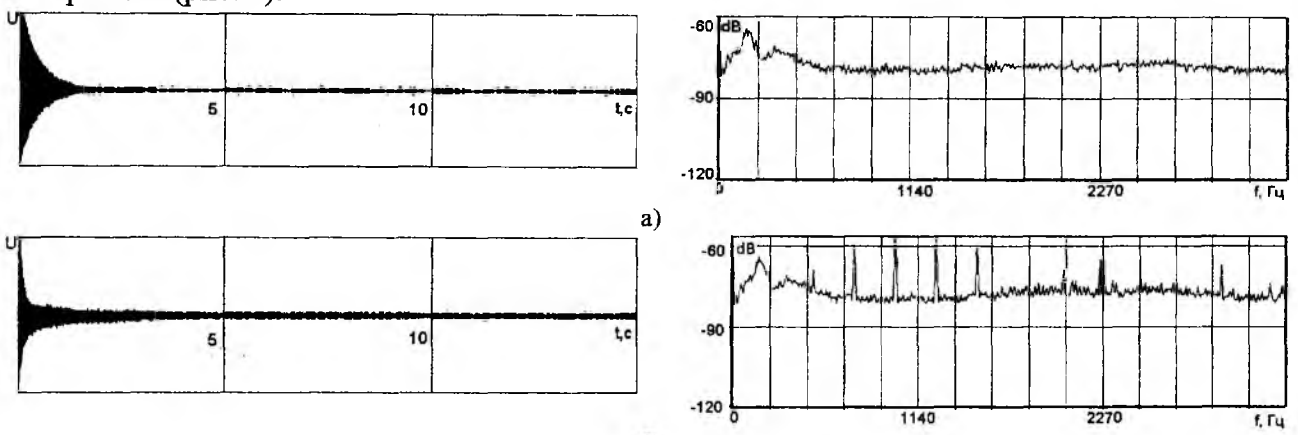

Рис. 4

Рис. 4а показывает процесс сходимости для АПР и здесь видно, что уменьшение уровня помехи происходит близко к экспоненте с постепенно замедляющейся скоростью. Этого не скажешь о МНК (рис.4б). Уменьшение уровня помехи можно аппроксимировать двумя прямыми. На участке первой прямой скорость сходимости МНК выше, чем у АПР. На участке же второй прямой, скорость значительно ниже. Это приводит к тому, что средняя скорость сходимости МНК оказывается ниже, чем у АПР.

Рассмотрим адаптивную фильтрацию речевого сигнала при воздействии белого шума. При этом параметры для алгоритма последовательной регрессии остаются, как и для предыдущего случая: A=1000, τ=500. На рис. 5а изображен сигнал на выходе адаптивного фильтра, работающего по АПР, а на рисунке 5б – по МНК. Величина параметров сходимости 2μ и $2\mu\lambda_{ср}$ равна 0,00005. Сразу бросается в глаза существенное различие во времени адаптации алгоритмов, при этом спектры выходных сигналов близки к оригиналу (рис.3а).

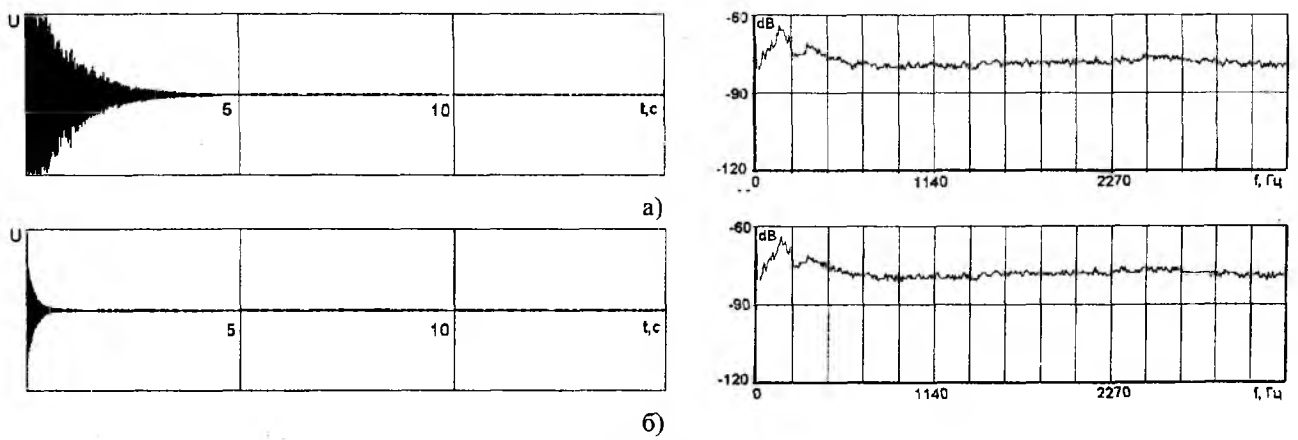

Рис. 5

При уменьшении параметров 2μ и $2\mu\lambda_{ср}$, как и в предыдущем случае, требуется больше времени до полной сходимости.

В алгоритме последовательной регрессии помимо $2\mu\lambda_{ср}$, можно изменять коэффициент А при матрице Q_0 (2), что для случая белого нормального шума приводит к следующему результату. На рис.6 представлен процесс сходимости АПР для случая, когда коэффициент А=1. Видно, что процесс проходит более «гладко», чем на рисунке 5а, хотя условия и параметры, кроме А, остались без изменений.

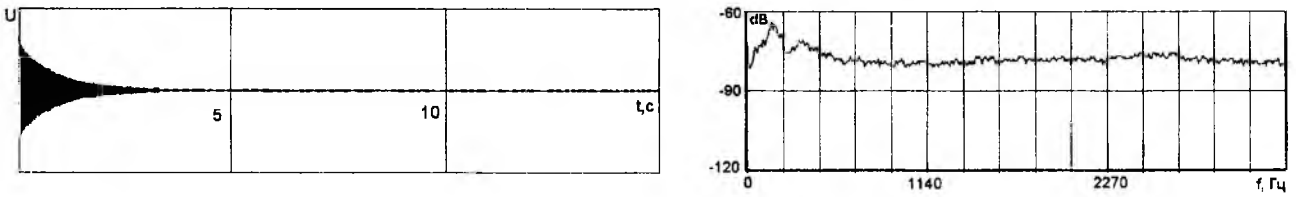

Рис. 6

Особым вариантом шума является речеподобный. Это шум, который коррелирован с речевым сообщением. В настоящее время считается, что наиболее эффективной (минимизирующей достаточный уровень помехи) является речеподобная помеха, формируемая из скрываемого речевого сигнала при многократном его наложении с различными уровнями. Такой помехой, в простом случае, является смесь голосов трех различных людей. В нашем случае речеподобная помеха формировалась как сумма «вырезок» из передаваемого речевого сообщения, которые разнесены на расстояние при отсутствии реверберации сигнала.

Параметры фильтров следующие: параметры сходимости 2μ и $2\mu\lambda_{ср}$ равны 0,0003; коэффициент А = 1000; τ = 500. Передаваемое сообщение представлено на рис.3а. Анализируя спектр речеподобного шума (рис.7а), видим, что его максимум сосредоточен в той области частот (до 1 кГц), где сосредоточен максимум речевого сообщения. А в остальной части спектра шум относительно равномерен. Как и для полигармонического шума, АПР (рис. 7б) сходится значительно быстрее, чем МНК (рис. 7в), при этом спектры восстановленных сигналов обоих алгоритмов близки к оригиналу (рис. 2б).

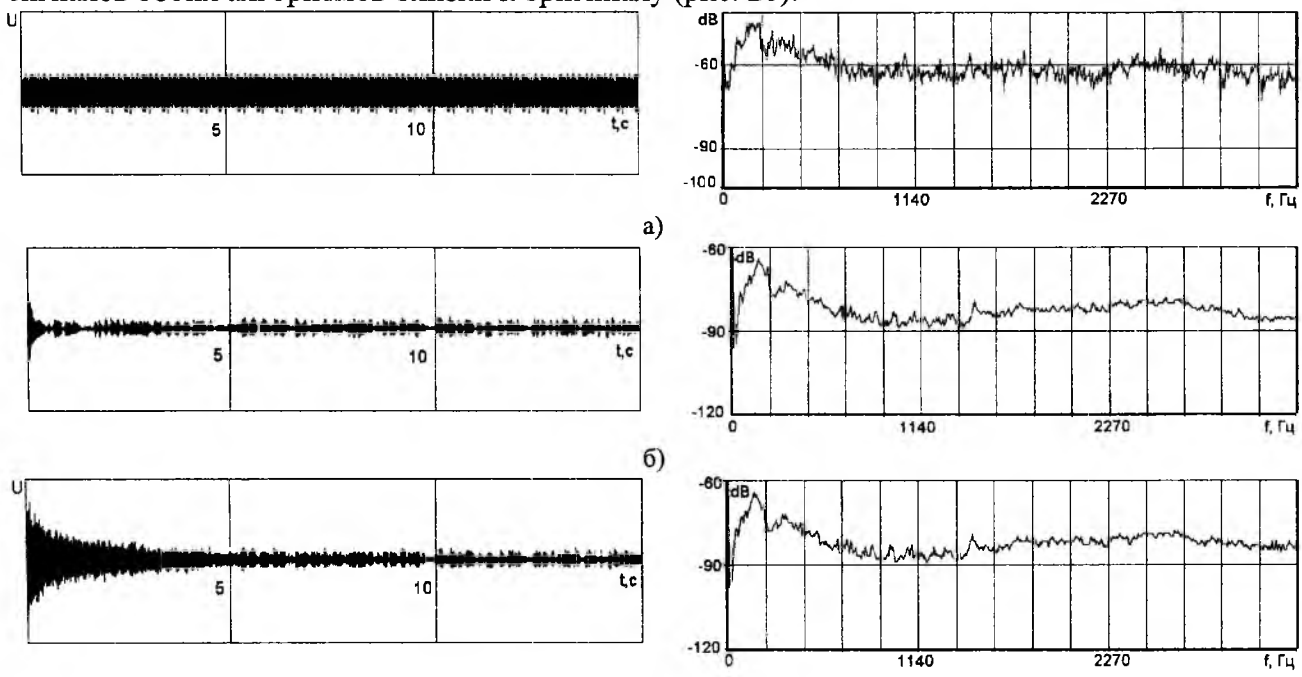

Рис. 7

Подведем промежуточный итог, касающийся применяемых заграждающих помех. Наиболее приемлемыми, в плане наибольшего скрытия передаваемого сообщения, являются шумы, которые практически полностью перекрывают спектр передаваемого сообщения.

Белый шум равномерен во всей полосе частот, что очень хорошо, но при этом необходима достаточная мощность шума, чтобы скрыть передаваемое сообщение. Речеподобный шум, в плане перекрытия частотного диапазона речи, аналогичен белому шуму, и вдобавок проявляется субъективный фактор ошибки. То есть, если уменьшить мощность белого шума до уровня, когда уже можно сказать, что в смеси присутствует речевая информация, так как можно уловить отдельные звуки, слова, в аналогичном случае речеподобного шума нельзя точно ответить, кому они принадлежат – шуму или передаваемому сообщению, так как оба являются речевыми сообщениями.

Любую среду распространения сигнала можно представить в виде фильтра со своей амплитудно-частотной (АЧХ) и фазочастотной характеристикой (ФЧХ). Предположим, что сигнал распространяется в телефонной линии (ТЛ), суммарную АЧХ которой можно аппроксимировать полосно-пропускающим фильтром с полосой 300-3400 Гц. Как известно, этого спектра частот достаточно для нормальной разборчивости речи. Оценим, как влияет на процесс адаптации и качество восстановленного сигнала предварительное искажение смеси сигнала с шумом, получаемое в результате пропускания смеси через фильтр. Такая задача возникает при использовании односторонних маскираторов телефонных разговоров, построенных на основе адаптивных фильтров, в телефонных сетях с нестабильными техническими характеристиками

Линия передачи моделировалась фильтром, описываемым следующим выражением передаточной характеристики в Z-форме:

$$G(z)=\frac{Y(z)}{X(z)}=\frac{b_1+b_2z^{-1}+b_3z^{-2}}{a_1+a_2z^{-1}+a_3z^{-2}}=\frac{0{,}7430-0{,}7430z^{-2}}{1-0{,}3631z^{-1}-0{,}4861z^{-2}}.$$

В дискретной форме выходной сигнал вычисляется по формуле:

$$y(n)=b_1x(n)+b_2x(n-1)+b_3x(n-2)-a_2y(n-1)-a_3y(n-2)=$$
$$=0.7430x(n)-0.7430x(n-2)+0.3631y(n-1)+0.4861y(n-2).$$

Фильтр имеет следующие параметры: полоса пропускания 300-3400 Гц; затухание в полосе пропускания 1 дБ; полоса задержания 200-3800 Гц; затухание в полосе задержания 5 дБ. АЧХ фильтра изображена на рис. 8. В качестве заграждающей помехи используем белый нормальный шум. Значение параметров сходимости 2μ и $2\mu\lambda_{ср}$ равно 0,0005, порядок фильтра 20, параметр A=1000, τ=500. Результаты процесса адаптации, после искажения смеси сигнал+шум выше указанным фильтром, приведены на рис.9. Как видно, фильтрация практически не оказывает влияния на процесс адаптации. Соотношение во временах сходимости процессов для белого шума сохраняется. По-прежнему метод наименьших квадратов (верхний график) сходится быстрее, чем алгоритм последовательной регрессии (нижний график).

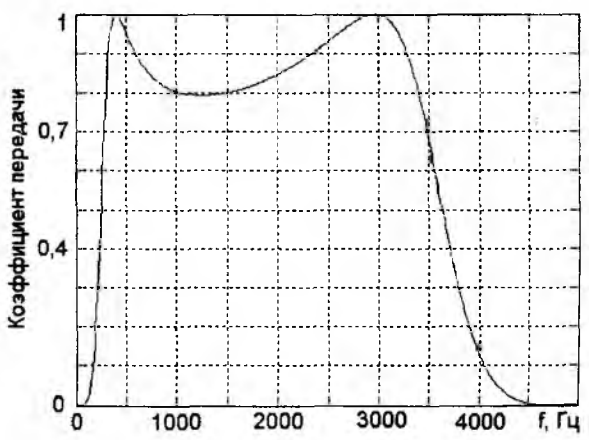

Рис. 8

Аналогичная ситуация наблюдается для других типов шумов и вариантов фильтров. Соотношения во временах сходимости алгоритмов сохраняются, как и для случаев без фильтрации. Возможно, имеет место различие во времени сходимости алгоритма для нефильтрованной и фильтрованной смеси. Однако это различие визуально не фиксируется.

Под действием окружающей среды (температуры, влажности и др.) характеристики ТЛ могут медленно или скачкообразно изменяться, т.е. происходит изменение характеристик

фильтра – полосы пропускания и задержания, а также затухания в них. Проанализируем сходимость алгоритмов для этих двух случаев.

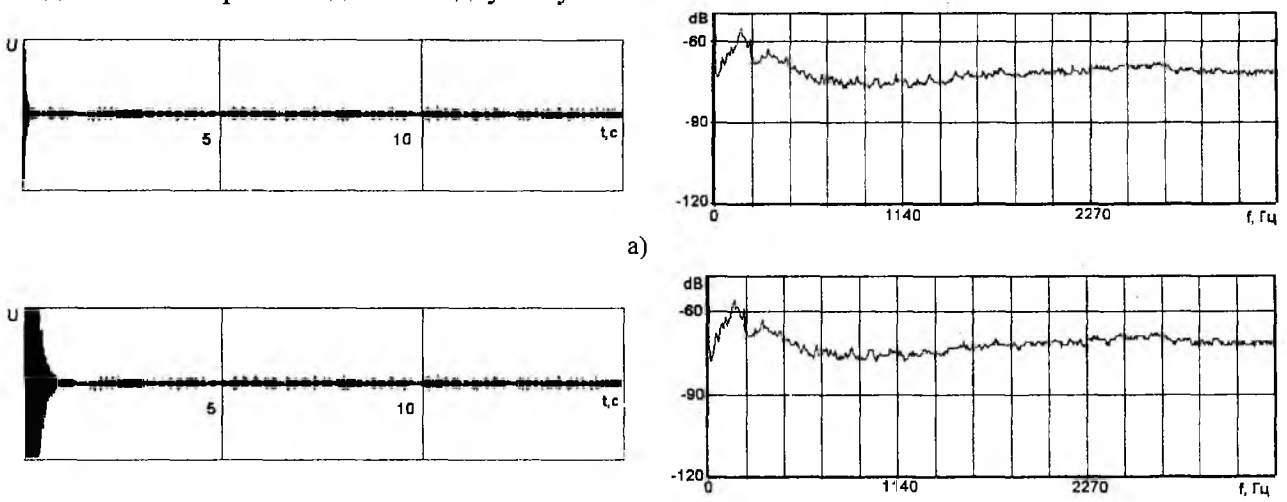

Рис. 9

Рассмотрим случай ступенчатого изменения АЧХ фильтра (рис. 10а). При этом происходит резкий переход от одного фильтра к другому. Порядок переходов 1-2-3-1-2-3…

Характеристики алгоритмов: значение параметров 2μ и $2\mu\lambda_{ср}$ равны 0,0005, порядок адаптивного фильтра 50, значение коэффициента A=1, τ = 500. Заграждающая помеха – белый нормальный шум. Как видно из графиков (рис. 11) при резкой смене фильтра появляются новые участки адаптации. При переходе от первого фильтра ко второму, и от второго к третьему (без учета первой адаптации), из-за относительно слабого различия между ними, фиксируются участки адаптации малой протяженности. При переходе от третьего фильтра к первому имеет место более продолжительный процесс адаптации. Это можно объяснить тем, что более сильно искажается смесь сигнал+шум по отношению к предыдущему состоянию, и необходима более длительная адаптация. Поэтому очень важным фактором в такой ситуации является время адаптации алгоритма. Если изменения фильтра будут очень частыми и с существенными различиями, или если значение параметра сходимости будет достаточно малым, то процесс не будет успевать сходиться что может привести к потере разборчивости речи. Самый верхний график рисунка 11 – это смесь сигнал+шум, прошедшая через ступенчато-изменяющийся фильтр (на рис. 11 и 12 верхняя временная диаграмма принадлежит смеси сигнал+шум прошедшей через фильтр, средняя диаграмма – сигнал на выходе фильтра, коэффициенты которого корректировались по АПР, а ни

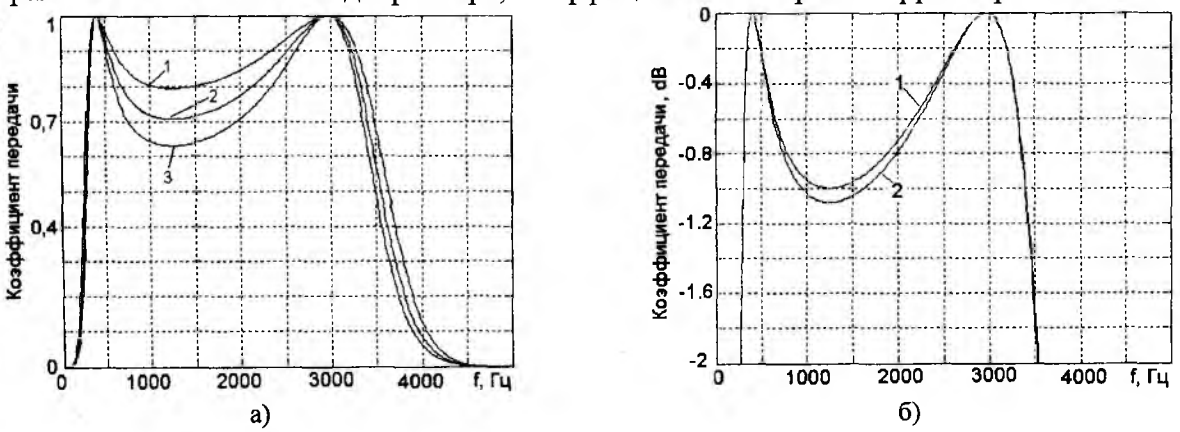

Рис. 10

В случае плавного изменения фильтра (медленный переход от фильтра 1 к 2, и наоборот; рис. 10а) отсутствуют резкие скачки в параметрах фильтра. Поэтому возникающие «паразитные адаптации» очень кратковременны и малы по величине, в результате чего они «маскируются» речевым сообщением (рис. 12).

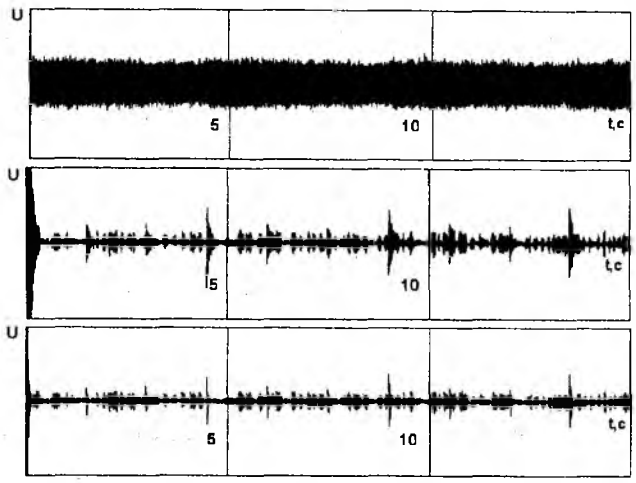

Рис. 11

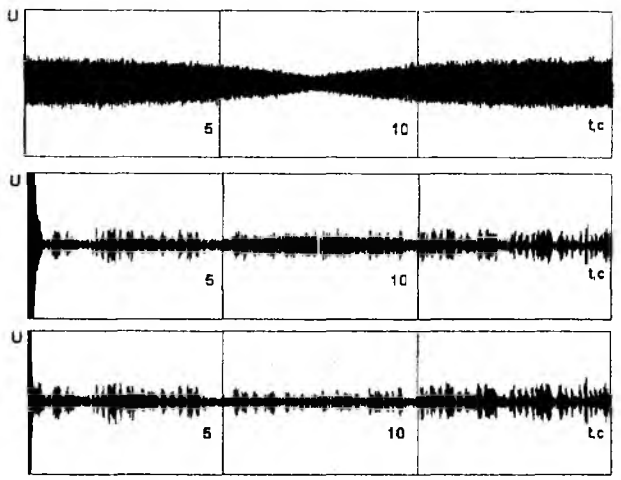

Рис. 12

Заключение: Проведенные исследования показали, что эффективность работы алгоритмов (время адаптации и степень подавления заграждающей помехи) зависят не только от их вида и параметров, но и от типа маскирующей помехи. Например, для быстрого подавления белого шума предпочтительно использовать МНК- алгоритм, а для случая полигармонического – АПР. Эффективность подавления белого шума обоими алгоритмами соизмерима. Полигармонический шум эффективней подавляется алгоритмом последовательной регрессии. Наилучшим скрытием речевого сигнала из всех рассмотренных помех, а именно полигармонической, типа белого шума и речеподобной, обладает последняя [6]. Для речеподобной помехи время адаптации алгоритма последовательной регрессии меньше по сравнению с МНК- алгоритмом, несмотря на то, что время одной итерации для него существенно больше.

Список литературы: 1. *Абалмазов Э.И.* Новая технология защиты телефонных разговоров // Специальная техника.1999. № 2. С. 4 – 8. 2. *Шевырев А.М.* Электронные комнаты для конфиденциальных переговоров на основе технологии подавления микрофонов // Бизнес и безопасность.1999. № 6. С. 17. 3. *Б. Уидроу, С. Стирз.* Адаптивная обработка сигналов / Под ред. В.В. Шахгильдяна. М.: Радио и связь, 1989. 439 с. 4. *Адаптивные фильтры* / Грант П.М., Коуэн К.Ф.Н., Фридлендер Б. и др.; Под ред. К.Ф.Н. Коуэна, П.М. Гранта. Пер. с англ. Н.Н. Лихацкой; Под ред. С.М. Ряковского. М. Мир, 1988. 388 с. 5. *Монзинго Р.А., Миллер Т.У.* Адаптивные антенные решетки: Введение в теорию / Пер. с англ. под ред. В.А. Лексаченко. М.: Радио и связь, 1986. 446 с. 6. *Домарев В.В.* Безопасность информационных технологий. К. ООО «ТИД «ДС», 2001. 688 с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 16.09.2002.