УДК 621.391.2.7

В.Д. КУКУШ, канд. техн. наук, Д.Ю. ВЕРЧИК

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ПОЛОСОВЫХ СКРЕМБЛЕРОВ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В УЗКОПОЛОСНЫХ СИСТЕМАХ СВЯЗИ

Введение

Наряду с развитием компьютерных технологий, методов и средств передачи информации, развиваются и подходы к обеспечению ее конфиденциальности. Работа систем технической защиты информации, обеспечивающих защиту передаваемых речевых сообщений, базируется на изменении характеристик речи таким образом, что речь становится нераспознаваемой для злоумышленников, перехватывающих данное сообщение.

Среди различных систем передачи речи особое место занимают узкополосные системы связи. За счет узкой полосы каждого канала в отдельности (3,1 – 4 кГц) достигается рациональное использование радиочастотного ресурса. Данные системы характеризуются низкими требованиями к стабильности характеристик канала связи и малой стоимостью оборудования. Примерами узкополосных систем связи являются проводные телефонные линии общего и специального назначения, системы специальной, оперативно-технологической и любительской радиосвязи вплоть до диапазона ОВЧ (VHF). В подобных системах наряду с требованиями надежности и оперативности, важны также вопросы обеспечения безопасности передаваемой информации. Устройства скремблирования по-прежнему остаются основным средством обеспечения безопасности в таких системах из-за их узкой полосы и низкого рабочего соотношения сигнал/шум [1 – 5].

Согласно [3] выделяют следующие основные принципы скремблирования: скремблирование в частотной области, скремблирование во временной области, а также двухмерное или комбинированное скремблирование, реализующее одновременно два приведенных выше преобразования речевого сигнала. Для передачи информации по каналу связи в масштабе реального времени, скремблирование в частотной области является более предпочтительным, чем во временной [6]. Это обусловлено тем, что полосовые скремблеры более устойчивы к неравномерности амплитудно-частотной характеристики канала, что позволяет получить минимальные искажения сигнала при дескремблировании. В то же время основным недостатком полосовых скремблеров является то, что скремблированный сигнал характеризуется присущим речи ритмом и сравнительно высоким уровнем остаточной разборчивости [7].

Как правило, основу полосовых скремблеров составляет банк частотно-избирательных фильтров, реализованных в аналоговом, либо в цифровом виде. Реализация банка фильтров в цифровом виде и применение алгоритма быстрого преобразования Фурье (БПФ) позволяет значительно увеличить количество полос, на которые разбивается спектр исходного сигнала [8]. За счет этого возрастает количество возможных вариантов перестановок полос, приводящее к повышению степени закрытия речи. Однако при использовании алгоритма, работающего по принципу по-блочного накопления и обработки отсчетов [9], для корректного дескремблирования речевой информации необходимо обеспечение синхронизации между скремблером и дескремблером. Отсутствие синхронизации приводит к появлению в дескремблированном сигнале «щелчков», следующих с периодом, равным длительности окна БПФ [10].

Проблема синхронизации между скремблером и дескремблером, выполняющих частотные преобразования речевого сигнала с использованием алгоритма БПФ, была детально исследована в ряде работ. Так, в [11] рассмотрена возможность введения дополнительных синхроимпульсов в скремблированный сигнал, как перед началом сеанса связи, так и в процессе передачи речевой информации. В последующих работах [12] предложено использовать поотсчетную, покадровую, а также мультикадровую синхронизацию. Подобный механизм синхронизации реализован также в скремблерах, в которых передача зашифрованных отсчетов речи выполняется с помощью OFDM модуляция

[13]. Это приводит к значительному усложнению алгоритма скремблирования и увеличению его вычислительной сложности [14], что ставит под сомнение заявленную простоту описанных выше методов скремблирования.

В работах [15, 16] представлены альтернативные способы реализации полосовых скремблеров, не требующие синхронизации между скремблером и дескремблером. Данные подходы основаны на реализации банка цифровых фильтров с использованием алгоритма БПФ со скользящим окном [15] либо «быстрого банка фильтров» (Fast Filter Bank) [16]. С точки зрения реализации скремблера эти подходы обладают большей вычислительной сложностью, чем при поблочном накоплении отсчетов [15]. Однако использование данных методов на практике видится более предпочтительным за счет отсутствия необходимости синхронизации и дополнительного введения в передаваемый сигнал служебной информации. Причем использование алгоритма БПФ со скользящим окном [15] является более оправданным с точки зрения временных затрат на разработку скремблера. Это связно с тем, что алгоритм БПФ является стандартной функцией цифровой обработки сигналов (ЦОС).

Однако следует отметить, что в доступных литературных источниках и обзорах технических решений не представлены в полной мере следующие аспекты, относящиеся к эффективности применения полосовых скремблеров и являющихся задачами данного исследования:

1) оптимальное разбиение спектра сигнала при его скремблировании и рекомендации по выбору порядка следования перестанавливаемых полос по критерию минимальной остаточной разборчивости речи в защищаемом канале связи;

2) оценка степени защищенности скремблированного сигнала, то есть его устойчивости к попыткам взлома злоумышленником.

1. Экспериментальная установка для исследования особенностей использования полосовых скремблеров

Экспериментальные исследования особенностей функционирования и эффективности работы полосовых скремблеров проводились на установке, структурная схема которой представлена на рис. 1. Установка включает в себя звуковоспроизводящее устройство и персональный компьютер (ПК) со специализированным программным обеспечением, реализованным в среде MATLAB®. Речевые сигналы, подлежащие скремблированию-дескремблированию, представлялись в виде массивов отсчетов, сохраненных в аудиофайлах либо поступающих с аудио карты ПК. В качестве скремблера-дескремблера использовался алгоритм цифровой обработки сигналов (ЦОС), разработанный по рекомендациям, изложенным в [15]. Его отличительной чертой является простота реализации за счет использования в его составе стандартных функций ЦОС и отсутствие необходимости синхронизации скремблера и дескремблера.

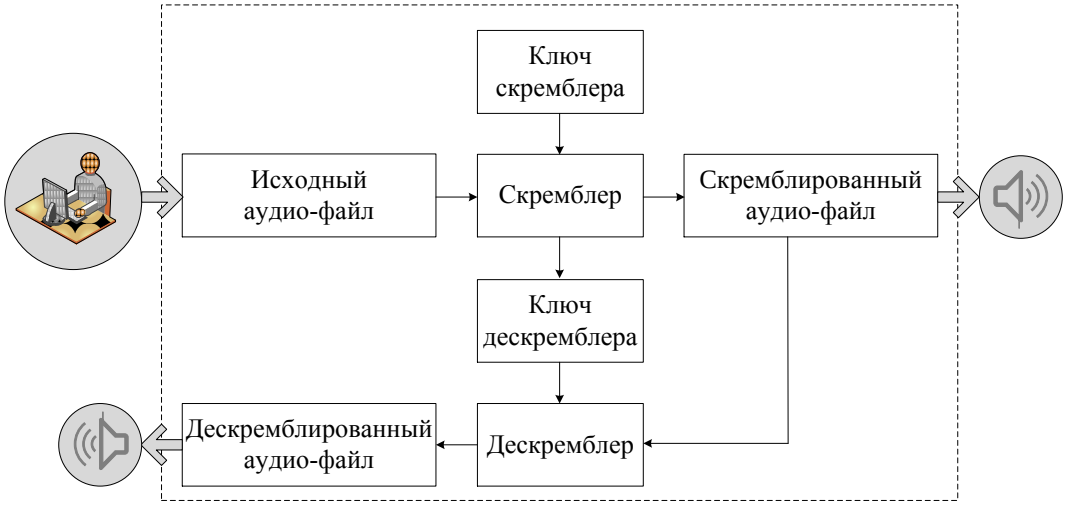

Рис. 1

Алгоритмы скремблирования и дескремблирования идентичны друг другу, поэтому ниже приведено описание только алгоритма скремблирования.

В основе разработанного алгоритма скремблирования (пояснение работы рис. 2) лежит банк цифровых узкополосных фильтров, реализованных на базе БПФ со скользящим окном [15]. За счет использования скользящего окна, которое на каждой итерации сдвигается на один отсчет, данный алгоритм не нуждается в синхронизации скремблера и дескремблера.

Как видно из рис. 2, на каждой итерации работы алгоритма из массива отсчетов входного сигнала $s_{вх}(n)$ скользящим окном выбирается N элементов (где N – размер окна, см. этап А). Выбранные элементы домножаются на весовую функцию $W(n)$ и обрабатываются алгоритмом БПФ. Далее выполняется формирование БПФ-спектра выходного сигнала, состоящее из: перестановки комплексных отсчетов БПФ-спектра входного сигнала в соответствии с ключом скремблера и коррекции фаз полученных отсчетов спектра (блоки М и φ на рис. 2).

Используемый ключ скремблера представляет собой массив:

- граничных частот полос, подлежащих перестановке;
- номеров, задающих порядок перестановки полос;
- флагов инверсии спектра (смены порядка следования его отсчетов) в рамках каждой полосы.

Далее фаза каждого коэффициента на выходе блока М корректировалась в блоке φ согласно формуле (1). За счет этого исключаются скачки фазы спектральных компонент сигнала после выполнения перестановки по частоте в соответствии с ключом скремблера.

$$\varphi'_{i,\ k} = \varphi_{i,\ k} + 2\pi \cdot \Delta f_i \cdot n_k \cdot (1/\ f_s), \tag{1}$$

где i – номер коэффициента БПФ-спектра входного сигнала; k – номер итерации алгоритма скремблирования; $\varphi'_{i,k}$ – фаза комплексного коэффициента БПФ-спектра сигнала на выходе блока φ, соответствующая i-му коэффициенту БПФ-спектра входного сигнала; $\varphi_{i,k}$ – фаза i-го комплексного коэффициента БПФ-спектра входного сигнала; Δf_i – величина сдвига по частоте i-го комплексного коэффициента БПФ-спектра входного сигнала при его перестановке согласно с ключом скремблера; n_k – положение скользящего окна относительно первого элемента массива отсчетов входного сигнала на k-ой итерации алгоритма (рис. 2); f_s – частота дискретизации входного/выходного сигнала.

Для формирования выходного сигнала $s_{вых}(n)$ массив отсчетов БПФ-спектра с выхода блока φ обрабатывается алгоритмом обратного БПФ (ОБПФ). Полученные таким образом отсчеты добавляются к содержимому массива $s_{вых}(n)$ (этап В на рис. 2). Массив $s_{вых}(n)$ на момент старта алгоритма инициализируется нулями. Смещение блоков отсчетов, полученных после ОБПФ, относительно первого элемента массива $s_{вых}(n)$, равно смещению скользящего окна в массиве $s_{вх}(n)$.

На последующих итерациях алгоритма происходит смещение скользящего окна на один отсчет с повтором описанных выше действий. Таким образом, выполняется формирование массива временных отсчетов сигнала $s_{вых}(n)$ из массива $s_{вх}(n)$.

При проведении экспериментальных исследований использовались следующие параметры алгоритма скремблирования:

1) частота дискретизации f_s=8 кГц (ширина спектра исходного сигнала составляет 4 кГц);

2) размер скользящего окна N=512;

3) тип весовой функции $W(n)$: Блэкмана - Харриса (ширина главного лепестка по уровню -3 дБ составляет 29,297 Гц, уровень боковых лепестков равен - 92 дБ).

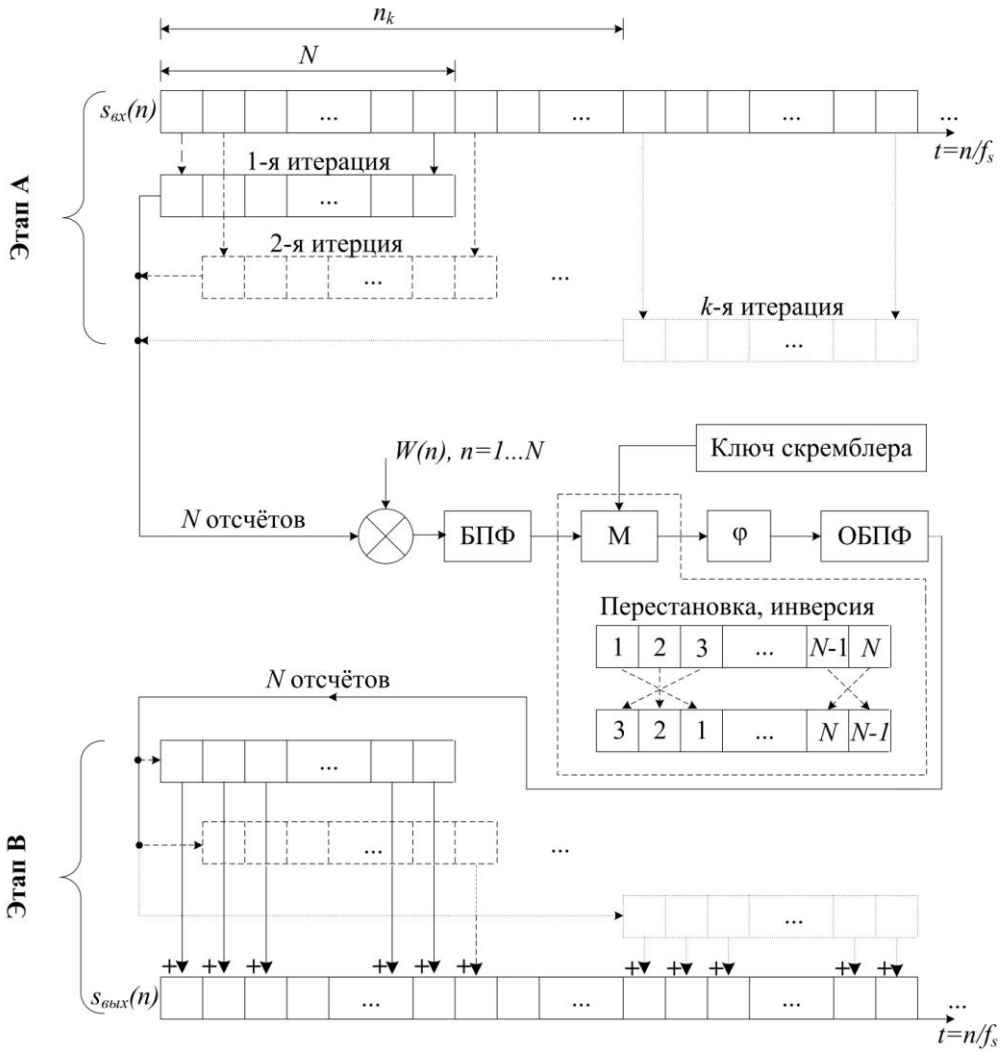

Рис. 2

Для отладки алгоритма полосового скремблера использован тестовый битональный сигнал с линейным ростом частоты. Спектрограмма сигнала представлена на рис. 3, *а*. Выбранный тестовый сигнал за один сеанс скремблирования-дескремблирования позволяет:

1) выполнить контроль правильности разбиения спектра сигнала на полосы в соответствии с ключом скремблера, а также порядка перестановки полос и их инверсий;

2) оценить уровень паразитных компонент, создаваемых каждой составляющей спектра входного сигнала. Эти компоненты возникают, например, из-за эффектов «просачивания спектральных составляющих» и «размытия максимумов спектра» вследствие отличия формы частотной характеристики весовой функции *W(n)* от прямоугольного вида с шириной, обратной длительности окна [17];

3) оценить искажения, возникающие при характерном для речи динамическом изменении частоты преобладающего тона.

Примеры спектрограмм скремблированного и дескремблированного тестового сигнала приведены на рис. 3 (*б, в*). В соответствии с ключом скремблера, используемом в данном случае, спектр исходного сигнала разбивался на три полосы, эти полосы перестанавливались в обратном порядке, при этом спектр второй полосы инвертировался.

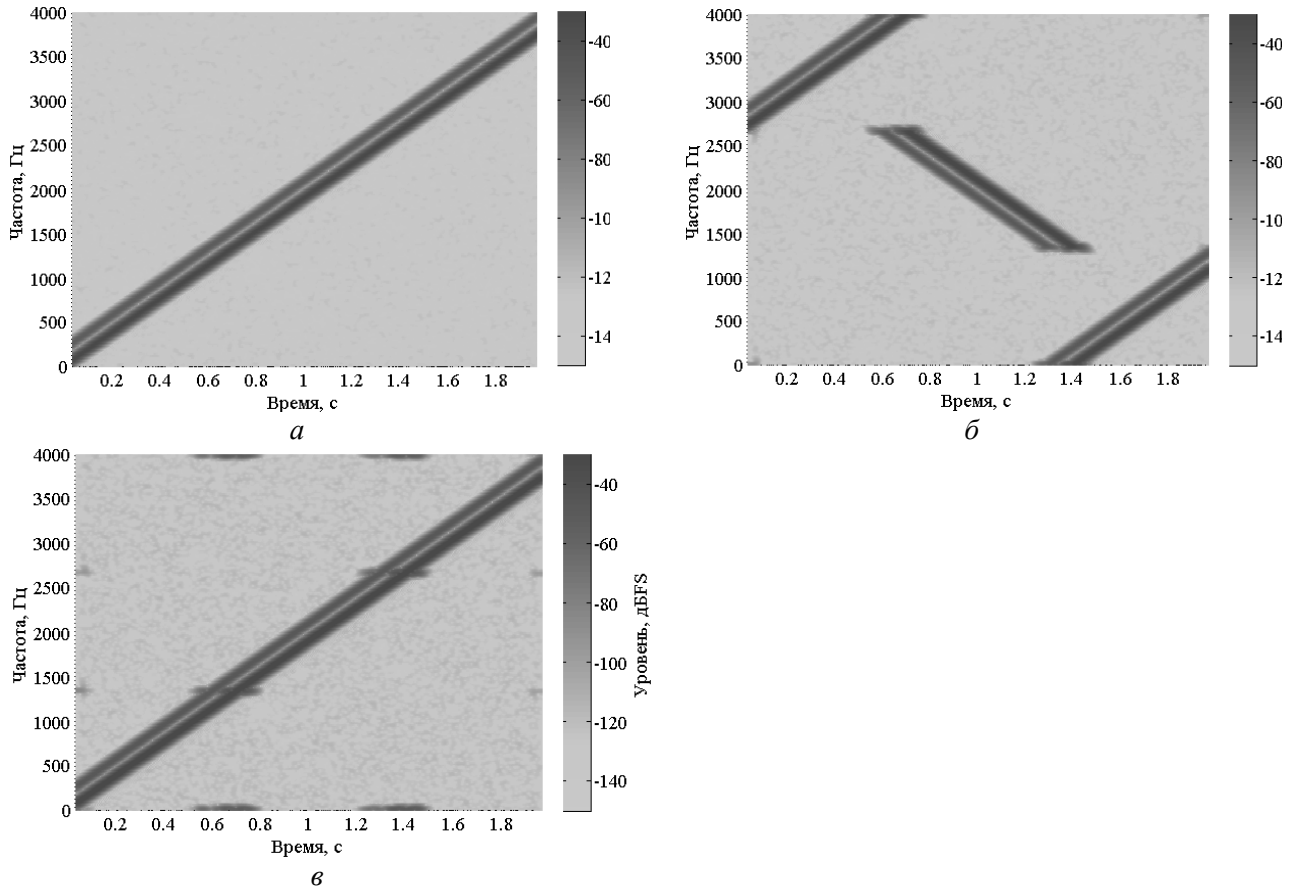

Рис. 3

На рис. 3, *в* видны паразитные спектральные компоненты, причина появления которых указана выше в п. 2. Для подавления этих паразитных компонент могут быть использованы дополнительные полосы режекции между перестанавливаемыми полосами сигнала при скремблировании-дескремблировании. Ширина полос режекции равна ширине главного лепестка используемой весовой функции.

2. Исследование способа разбиения спектра и влияния порядка следования полос на остаточную разборчивость скремблированного сигнала

Оценка остаточной разборчивости скремблированных сигналов выполнялась экспериментально на основе артикуляционных измерений в соответствии с ГОСТ 50840-95. Для проведения таких измерений была задействована группа из трех подготовленных дикторов (одного мужчины и двух женщин) и аудиторов (одного мужчины и двух женщин), не имеющих явных дефектов слуха и речи. Подготовка к эксперименту включала в себя формирование аудиофайлов с тестовыми фразами, начитанными каждым диктором и взятыми из артикуляционных таблиц (Приложение Д ГОСТ 50840-95). Далее аудиофайлы подвергались скремблированию и прослушивались аудиторами, в результате чего оценивалась словесная остаточная разборчивость. Таким образом, каждая оценка разборчивости представляла собой среднюю величину, полученную по результатам прослушивания всеми аудиторами по 50 фраз, надиктованными каждым из дикторов.

Для исследования влияния способа перестановки полос на остаточную разборчивость, спектр исходного сигнала разбивался на 3 полосы и выполнялся перебор всех возможных вариантов перестановок полос и инверсий спектра в полосах. Граничные частоты полос соответствовали двум способам разбиения спектра – эквидистантному и октавному. При эквидистантном способе разбиения спектра, полосы исходного сигнала имели равную ширину (граничные частоты составляли 1,328 и 2,656 кГц при полосе сигнала в 4 кГц). При

октавном ширины полос соотносились как 1:2 по мере возрастания частоты (граничные частоты полос 563 и 1,703 кГц). Выбранное количество полос (три) оптимально с точки зрения трудозатрат на перебор всех комбинаций. Аналогичное количество полос используется в сравнительно простых скремблерах на базе специализированных микросхем, например, PCD4440T производства Philips. Полученные результаты оценки остаточной разборчивости скремблированного сигнала для эквидистантного и октавного способов разбиения спектра исходного сигнала приведены на рис. 4, *а*, *б* соответственно. Нумерация полос, приведенная на рис. 4, осуществлялась от области нижних частот спектра исходного сигнала к верхним.

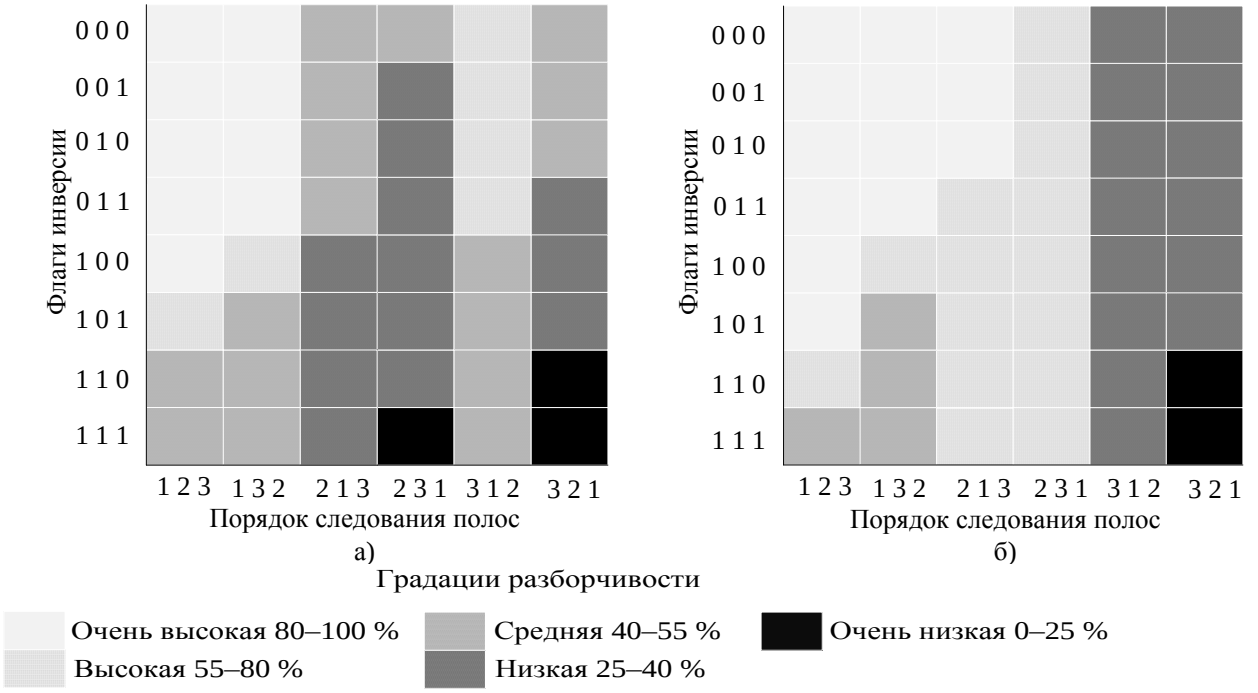

Рис. 4

Приведенные на рис. 4 результаты экспериментальных исследований показывают, что не все из возможных перестановок обеспечивают низкий уровень остаточной разборчивости. Видно, что к таким «эффективным» перестановкам можно отнести те, в которых полосы спектра, содержащие низкочастотные компоненты речи, перемещаются в область верхних частот. Возможность ухудшения разборчивости при подобных перестановках может быть также объяснена тем, что способность уха различать раздельно сигналы с близкими частотами обратно пропорциональна частоте этих сигналов [18]. Поэтому перемещение близко расположенных низкочастотных компонент речи (например, гармоник основного тона) в область верхних частот препятствует раздельному восприятию этих компонент и уменьшает разборчивость скремблированного сигнала.

Из сравнения рисунков 4, *а*, *б* видно, что способ разбиения спектра сигнала на полосы (эквидистантное или октавное) не оказывает значительного влияния на остаточную разборчивость.

3. Оценка защищенности речевого сигнала в системах связи, использующих полосовые скремблеры

При незнании ключа скремблера к наиболее типовым действиям злоумышленника по взлому перехваченного скремблированного сигнала можно отнести:

1) запись и многократное прослушивание сигнала;

2) «полную» инверсию спектра сигнала (зеркальную перестановку всех его спектральных компонент относительно центральной частоты);

3) разбиение спектра сигнала на некоторое количество полос равной ширины с последующей перестановкой полос в обратном порядке либо перебором всех возможных комбинаций перестановок;

4) действия, аналогичные п. 3, за исключением того, что спектр сигнала в каждой полосе инвертируется;

5) анализ спектрограммы скремблированного сигнала для определения граничных частот полос по ее характерным признакам и выполнение действий, аналогичных указанным выше.

При выполнении дальнейших исследований под успешной попыткой взлома принимался результат такого преобразования скремблированного сигнала, когда его разборчивость становилась больше, чем разборчивость до взлома, и принимала значение выше 30 %. Указанное пороговое значение разборчивости соответствует возможности распознавания отдельных слов и выражений [18].

Алгоритм для выполнения «полной» инверсии спектра сигнала видится наиболее эффективным и простым из перечисленных способов взлома, поскольку, как следует из раздела 2, эта операция приблизительно восстанавливает порядок следования полос скремблированного сигнала. Это может привести к увеличению его разборчивости до удовлетворительного уровня и, как следствие, к возможности несанкционированного прослушивания. Алгоритм «полной» инверсии спектра заключается в смене знака перед величиной каждого второго отсчета исходного сигнала:

$$s_{inv}(n) = (-1)^n \cdot s_{вх}(n), \tag{2}$$

где $s_{inv}(n)$ – поток отсчетов сигнала с инвертированным спектром; n – номер отсчета, $n = 1, 2, 3\ldots$.

Экспериментально полученные оценки разборчивости скремблированного сигнала после попыток его взлома с использованием алгоритма «полной» инверсии спектра представлены на рис. 4. Каждая из приведенных оценок разборчивости ξ равна максимальному значению из двух величин:

1) остаточной разборчивости (при попытке разобрать скремблированный сигнал без каких-либо преобразований);

2) разборчивости после попытки взлома скремблированного сигнала алгоритмом «полной» инверсии. Оценки разборчивости ξ получены по результатам попыток взлома сигналов на выходе полосового скремблера при эквидистантном способе разбиения спектра с различным количеством полос. При разбиении спектра сигнала на две-три полосы исследована устойчивость к взлому скремблированного сигнала для всех возможных вариантов перестановок полос и инверсий спектра в полосах. При разбиении на четыре и более полос – для 10 случайно выбранных вариантов перестановок. Предположение о возможном разбросе величин ξ сделано на основании того, что среди всевозможных вариантов перестановок большего числа полос обязательно найдутся те, которые повторяют перестановки с меньшим числом полос.

Из рис. 5 видно, что при разбиении спектра речевого сигнала на 32 и менее полос, речевая информация может быть распознана непосредственно по самому скремблированному сигналу либо по результату инверсии его спектра. Указанное справедливо для речевых сигналов полосой 4 кГц, вне зависимости от величин граничных частот полос, порядка следования и инверсий полос при скремблировании. Однако при разбиении спектра сигнала на 64 полосы и более, такой метод взлома не дает подобного результата. Это связано с тем, что существуют варианты перестановок полос (ключи скремблера), при которых обеспечивается разборчивость ниже 30 % как до, так и после инверсии. Следовательно, для обеспечения устойчивости к взлому скремблированного сигнала с использованием алгоритма «полной» инверсии его спектра необходимо, чтобы количество полос при скремблировании составляло не менее 32 – 64.

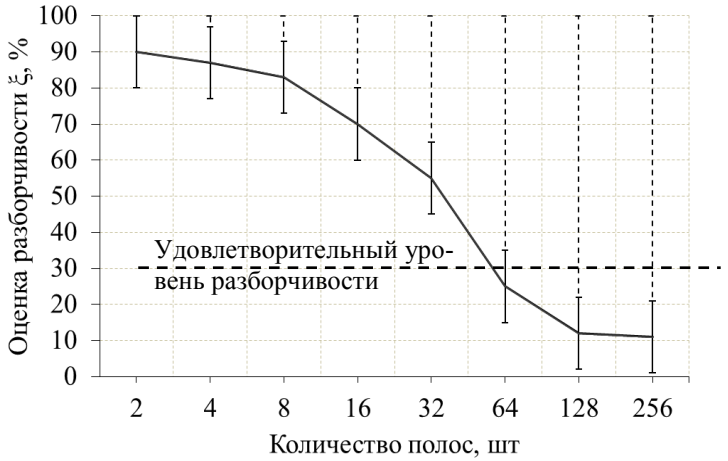

Рис. 5

Одним из эффективных методов обеспечения низкого уровня остаточной разборчивости и увеличения устойчивости к взлому путем инверсии или прямого перебора является увеличение количества перестанавливаемых полос.

Основным параметром, ограничивающим максимальное количество полос, является минимально достижимая величина полосы пропускания фильтров, используемых в составе скремблера. При реализации в скремблере банка цифровых узкополосных фильтров на базе алгоритмов, подобных БПФ, эта величина зависит от ряда факторов.

Во-первых, минимально достижимая величина полосы пропускания зависит от используемой весовой функции и обратно пропорциональна длительности (размеру) окна. Длительность окна определяется допустимым временем задержки на цикл скремблирования-дескремблирования. Величина задержки для узкополосных речевых систем связи должна составлять не более τ_{max} = 50…200 мс [18, 19]. Следовательно, величина длительности окна БПФ должна составлять:

$$\tau_{БПФ_{\max}} \le \tau_{\max}/2;\ \tau_{БПФ_{\max}} \le 25...100 \text{ мс.}$$

Например, при частоте дискретизации исходного речевого сигнала в f_s=8 кГц (период дискретизации равен T_s=1/f_s=125 мкс), максимальный размер окна составляет

$$N_{\max} \le \tau_{БПФ_{\max}}/T_s;\ \ N_{\max} \le 200...800 \text{ отсчетов.}$$

Исходя из особенностей алгоритма БПФ размер окна должен быть кратен 2^N, здесь N – целое число. Следовательно, размер окна N_{max} ограничен значением в 512 отсчетов. Как известно, максимальное число полос, на которое возможно разбить спектр сигнала при использовании алгоритма БПФ, равно половине размера окна [17]. То есть максимальное количество полос скремблера составляет 256.

Во-вторых, максимальное количество полос ограничено уровнем искажений сигнала, возникающих вследствие эффектов «просачивания спектральных составляющих» и «размытия максимумов спектра» после цикла его скремблирования-дескремблирования [17]. Эти искажения могут быть экспериментально оценены по зависимости от количества полос максимума взаимно-корреляционной функции (ВКФ) между исходным речевым сигналом и сигналом, полученным из исходного в результате его скремблирования-дескремблирования. Приведенные на рис. 6 оценки максимумов ВКФ для каждого количества полос получены путем осреднения результатов 10 сеансов скремблирования-дескремблирования исходного речевого сигнала. При скремблировании использовалось два типа весовых функций $W(n)$: прямоугольная и Блэкмана – Харриса, способ разбиения спектра исходного сигнала –

эквидистантный. Остальные параметры алгоритма скремблирования оставались аналогичными приведенным в описании экспериментальной установки.

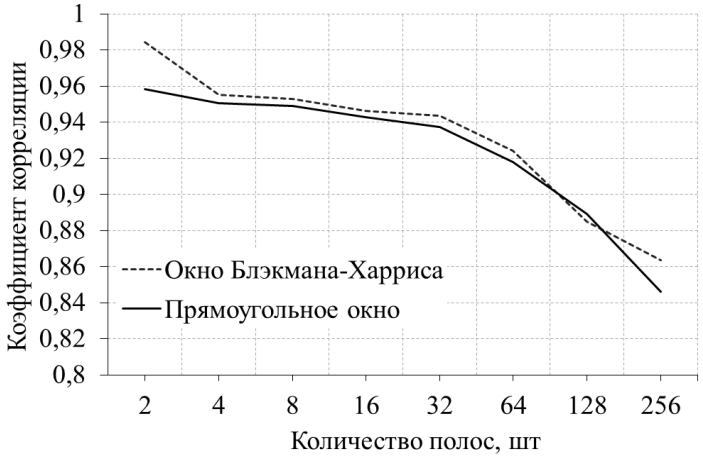

Рис. 6

Результаты, приведенные на рис. 6, подтверждают, что с увеличением количества перестанавливаемых и/или инвертируемых полос увеличивается уровень вносимых искажений в речевой сигнал после цикла его скремблирования-дескремблирования. Эти искажения на слух проявляются в виде металлического оттенка на фоне речевого сигнала, однако ухудшение разборчивости при этом не наблюдалось (величина разборчивости составляла 90 % и более).

Выводы

Исследован ряд актуальных аспектов, связанных с разработкой и эксплуатацией устройств скремблирования речи, которые за счет простоты реализации и свойства оставлять полосу сигнала неизменной могут быть использованы как доступные и недорогие средства защиты информации практически в любых системах связи.

Экспериментальные исследования, выполненные на базе разработанного полосового скремблера и в предположении его использования в узкополосной системе «аналоговой» связи (полоса речевого канала составляет 3,1 – 4 кГц), показали, что, в зависимости от порядка следования и выбора граничных частот полос при скремблировании, остаточная разборчивость скремблированного сигнала варьируется в диапазоне от 10 до 90 %. Следует отметить, что при разборчивости выше 30 % речевые сообщения могут быть восприняты с удовлетворительным качеством, несмотря на скремблирование. Также установлено, что минимальный уровень остаточной разборчивости сигнала на выходе скремблера обеспечивается при таких перестановках полос, которые переносят низкочастотные компоненты речи в область верхних частот.

Выполненные экспериментальные исследования степени защищенности скремблированного сигнала показали, что при количестве полос менее 32 такой сигнал может быть взломан путем применения сравнительно простой операции инверсии его спектра во всей полосе частот. При количестве полос более 32 существуют варианты перестановок полос, обеспечивающие остаточную разборчивость скремблированного сигнала в диапазоне 10 – 20 %, причем скремблированный таким образом сигнал не может быть взломан с помощью операции инверсии его спектра. Также показано, что для речевой системы связи, работающей в масштабе реального времени, максимальное количество полос ограничивается двумя факторами: временем задержки на цикл скремблирования-дескремблирования и вносимыми искажениями после цикла скремблирования-дескремблирования. Так, при задержке в 128 мс, полосе канала связи в 4 кГц и вносимых

искажениях, приводящих к ухудшению разборчивости не ниже 90 %, максимальное число полос составляет 256.

Представленные материалы могут быть использованы при разработке скремблеров, представляющих собой устройства цифровой обработки речевых сигналов. Также данные результаты могут быть полезны при выборе ключей скремблирования, оптимальных по критериям устойчивости к взлому, минимума остаточной разборчивости и уровня вносимых искажений.

Список литературы: 1. *Торокин, А. А*. Инженерно-техническая защита информации : учеб. пособие / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 960 с. 2. *Ленков, С. В*. Методы и средства защиты информации : в 2 т. Т. 2 : Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В. А. Хорошко. – К. : Арий, 2008. – 344 с. 3. *Srinivasan, A*. Review of analog audio scrambling methods for residual intelligibility / A. Srinivasan, P. Selvan // Innovation Systems Design and Engineering. – 2012. – Vol. 3, No. 7. – P. 22–38. 4. *Защита* информации в телекоммуникационных системах / Г. Ф. Конахович, В. П. Климчук, С. М. Паук, В. Г. Потапов. – К. : Арий, 2008. – 344 с. 5. *Горбенко, И. Д*. Принципы защиты речевых сообщений в коммуникационных системах : учеб. пособие / И. Д. Горбенко, А. А. Замула, И. Н. Пресняков. – Харьков : ХТУРЭ, 1997. – 116 с. 6. Jayakurami, J. A review of analog speech scrambling for secure communication / J. Jayakurami, G. Dhanya // Progress in science and engineering research journal. – 2016. – Vol. 2. – P. 194–198. 7. *Lim, Y. C.* Quality analog scramblers using frequency-response masking filter banks circuits / Y. C. Lim, J. W. Lee, S. W. Foo // Syst. Signal Process – 2010. – Vol. 29. – P. 135–154. 8. *Weinstein, S. B*. Sampling-based techniques for voice scrambling / S. B. Weinstein // Proc. Int. Conf. Commun. – 1980, June. – Vol. 1. – P. 16.2.1–16.2.6. 9. *Lee, L. S.* A simple sample value scrambler using FFT algorithms for secure voice communications / L. S. Lee, Y. P. Harn, Y. C. Chen // Proc. Nat. Telecommun. Conf. – 1980, December. – P. 49.4.1–49.4.5. 10. *Верчик, Д. Ю.* Особенности технической реализации и применения алгоритмов скремблирования речи / Верчик Д. Ю., Кукуш В. Д. // 20-й Юбилейный Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. материалов форума. Т. 3. – Харьков : ХНУРЭ. 2016. – 81–82 с. 11. *Andrade J. F*. Speech privacy for modern mobile communication systems / J. F. Andrade, M. Campos, J. A. Apolinario // Acoustics, Speech and Signal Processing. – 2008. – P. 1777–1780. 12. *Matsunaga, A.* An analog speech scrambling system using the FFT technique with high-level security / A. Matsunaga, K. Koga, M. Ohkawa // IEEE Journal on Selected Areas in Communication. – 1989, May. – Vol. 7, No. 4. – P. 540–547. 13. *Jayakurami, J.* An efficient voice scrambling technique for next generation communication systems / J. Jayakurami, G. Dhanya // International Journal of Engineering and Technology. – 2016. – Vol. 8., No. 1. – P. 293–299. 14. *Tseng, D. C*. An OFDM-Based speech scrambler without residual intelligibility / D. C. Tseng, J. H. Chiu // Transactions on Information and Systems. – 2008. – Vol. 9. – P. 2742–2745. 15. *Lee, L. S*. A new frequency domain speech scrambling system which does not require frame synchronization / L. S. Lee, G. C. Chou, C. S. Chang // IEEE Transactions on communication. – 1984, April. – Vol. Com-32, No. 4. – P. 444–456. 16. *Lee J. W*. Efficient fast filter bank with a reduced delay / J. W. Lee, Y. C. Lim // Circuits and Systems. – 2008. – P. 1430–1433. 17. *Айфичер, Э. С.* Цифровая обработка сигналов: практический подход / Э. С. Айфичер, Б. У. Джервис. – 2-е изд. : пер. с англ. – М. : Изд. дом «Вильямс», 2004. – 992 с. 18. *Сапожков, М. А*. Электроакустика / М. А. Сапожков. – М. : Связь, 1978. – 272 с. 19. Руководство по проектированию систем звукового обеспечения на строящихся и реконструируемых объектах г. Москвы [Электронный ресурс]. – 2000. Режим доступа: URL: http://www.docload.ru/Basesdoc/8/8269/index.htm.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 03.09.2017