Александр Архипов, Екатерина Безымянная
НТУУ «КПИ»
УДК 004.056

ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАШУМЛЕНИЯ РЕЧЕВОГО СИГНАЛА

Аннотация: **Проведен анализ эффективности зашумления речевого сигнала помехами и способов оценки эффективности маскировки этих сигналов.**
Summary: **The analysis of the effectiveness of noise on speech signal is interference, as well as analysis of ways to assess the effectiveness of masking these signals.**
Ключевые слова: **Защита речевой информации, речеподобная помеха, артикуляционные испытания.**

I Введение

При проведении переговоров дорогостоящие предварительные проверки помещений на наличие подслушивающей аппаратуры и технических каналов утечки информации могут оказаться бесполезными, так как не исключено, что подслушивающая аппаратура может попасть в помещение накануне проведения конфиденциальных переговоров или будет внесена непосредственно участниками этих переговоров.

Существует различная аппаратура для оперативного контроля службой безопасности участников переговоров. Это, например, металлоискатели и средства обнаружения работающих диктофонов или «жучков», однако эффективное применение этой аппаратуры требует достаточно высокой квалификации и не всегда согласуется с этическим соображением. Причем, если выявление работающих радиомикрофонов – сравнительно несложная задача, то аппаратура, предназначенная для поиска диктофонов, обычно имеет дальность обнаружения не более 50 сантиметров, что создает трудности при практической реализации поиска, обуславливая незначительный процент обнаружения (особенно это относится к цифровым диктофонам в экранированном корпусе) или, при повышении чувствительности, приводит к увеличению ложных срабатываний. Кроме того, надо учитывать, что технику могут пронести в выключенном состоянии.

Следует также принимать во внимание наличие виброакустических каналов утечки речевой информации и плохую звукоизоляцию помещений: для считывания конфиденциальной информации могут использоваться не только аппаратные каналы утечки речевой информации, но и естественные, такие как воздух, несущие конструкции, трубы отопления, водопровода, вентиляционные каналы и т. д.

Задача защиты от утечки состоит в перекрытии всех возможных каналов и нейтрализации средств перехвата (микрофоны, направленные микрофоны, диктофоны, стетоскопы, закладные устройства, лазерные или инфракрасные системы и т. д.). Возможности повышения звукоизоляции связаны со строительными работами по акустической защите выделенных помещений, но они не дают нужной защиты от внедренных в последующем средств съема акустической информации.

Наиболее надежным направлением противодействия несанкционированному получению речевой информации является препятствование звукозаписи переговоров или ее ретрансляции из помещения путем создания шумовой акустической помехи, обеспечивающей скрытие информативного сигнала, при этом соотношение величина шумового сигнала / величина информативного сигнала должно обеспечивать надежное сокрытие информативного сигнала или снижение его разборчивости до необходимых пределов.

Существующие средства защиты акустической информации по вибрационным каналам представляют собой генераторы шума (белого или окрашенного) речевого диапазона частот в комплекте с пьезоэлектрическими или электромагнитными вибропреобразователями. Основное назначение их – создание шумовых помех средствам съема информации в стенах, окнах, инженерных коммуникациях. Основной критерий обеспечения защиты – превышение шума над уровнем наведенного в эти конструкции информативного сигнала. Нормы превышения определены соответствующими нормативно-техническими документами.

Сравнительная оценка эффективности различных видов помех, проведенная специалистами, натолкнула на ряд особенностей применения каждой из них. Исследования показывают, что ограждающие конструкции и поверхности обладают неодинаковым акустическим сопротивлением на различных частотах, кроме того, вибропреобразователи также имеют свои конструктивные особенности, влияющие на частотные характеристики. В результате оказывается, что для оптимальной настройки сигнала помехи, надежно обеспечивающего превышения помехи над информативным сигналом на всех частотах, приходится задавать достаточно высокий уровень помехи. Это приводит к тому, что уровень паразитных акустических шумов на отдельных частотах может быть очень высоким и создавать дискомфорт для людей, работающих в

выделенном помещении. Подобный недостаток прежде всего присущ помехе типа «белый» шум, которая имеет равномерный спектр в полосе частот речевого сигнала.

Для формирования «окрашенного» шума, получаемого из «белого» в соответствии с огибающей амплитудного спектра скрываемого речевого сигнала, в пяти октавных полосах диапазона 100 – 6000 Гц производится оценка параметров речевого сигнала и осуществляется корректировка уровня шума в тех же полосах с помощью встроенных эквалайзеров [1]. Таким образом, обеспечивается энергетическая оптимальность помехи, при которой заданное нормированное соотношение «сигнал/помеха» выдерживается в пределах всего диапазона частот защищаемого речевого сигнала. В некоторых аппаратных комплексах зашумления эта задача решается разделением уровней шумового сигнала по каждому из его выходов. Это позволяет использовать комплекс для одновременного зашумления различных ограждающих конструкций, инженерных коммуникаций, окон и т. п., обладающих неодинаковыми сопротивлением и звукопроводящими свойствами [1].

В большинстве работ, освещающих активные методы защиты речевой информации – маскировки речевого сигнала помехой, – особое место занимают методы, в которых используется так называемая «речеподобная» помеха (РПП), обеспечивающая высокую эффективность защиты в сочетании с достаточным уровнем комфортности сторон, участвующих в речевой коммуникации

II Основная часть

В большинстве публикаций, касающихся самых разных аспектов применения РПП, рассматриваются методы их генерации, способы применения «речеподобных» помех в конкретных (типовых) условиях, оцениваются уровни помех, гарантирующие надежную защиту речевого сигнала и т. п. Эти сведения получены в ходе проведения серий отдельных исследований, выполняемых, как правило, индивидуально, вне рамок какой–либо общей системной методологии, поэтому приводимые результаты в целом носят фрагментарный, отрывочный характер, оставляя невыясненными ряд аспектов, в частности:

Существует ли общее определение РПП?

Специалистами предлагаются различные определения понятия РПП в зависимости от варианта формирования данной помехи. Так, например, некоторые исследователи описывают РПП как помеху, сформированную путем микширования в различных сочетаниях отрезков речевых сигналов, музыкальных фрагментов и шумовых помех, или сформированную из фрагментов скрываемого речевого сигнала при его многократном наложении с различными уровнями, или шум с огибающей амплитудного спектра, подобной огибающей спектра защищаемого речевого сигнала.

В частности, специалистами в области технической защиты информации В. М. Ивановым и А. А. Хоревым предложен способ формирования РПП из речевых сигналов. При этом возможно формирование помехи как из скрываемого сигнала, так и из некоррелированных со скрываемым сигналом речевых отрезков. Характерным представителем помех, формируемых из речевых отрезков, некоррелированных со скрываемым сигналом, является помеха типа «речевой хор»: такая помеха формируется путем смешивания фрагментов речи нескольких человек. Среди помех, формируемых из скрываемого сигнала, можно выделить два типа: «речеподобную» реверберационную и «речеподобную» инверсионную. «Речеподобная» реверберационная помеха формируется из фрагментов скрываемого речевого сигнала путем многократного их наложения с различными уровнями. «Речеподобная» инверсионная помеха формируется из скрываемого речевого сигнала путем сложной инверсии его спектра. Путем смешивания различного вида помех, например, «белый» шум и «речевой хор», формируются комбинированные помехи [2].

Надежными методом зашумления речевого сигнала считается генерация помех с «обратной связью» – адаптивных помех. Суть этого метода генерации заключается в анализе полезного звукового сигнала в помещении посредством встроенного микрофона, после чего генератор автоматически устанавливает уровень шума на тех или иных частотах, что позволяет снизить отрицательные моменты работы людей в зашумленном выделенном помещении.

Наиболее эффективным считается адаптивный речеподобный шум. Он создается прямо из защищаемого разговора путем многократного наложения его фрагментов друг на друга с разными уровнями интенсивности сигнала. Первые же звуки, произнесенные участниками конфиденциальных переговоров, улавливаются генератором и отправляются в блок преобразования. Там они подвергаются обработке, в процессе которой происходит умножение и деление их частотных составляющих. Получившаяся в результате этого процесса помеха излучается колонками. Шум смешивается с информативным смысловым сигналом, отражается от стен, потолка и предметов интерьера и через какой-то промежуток времени снова улавливается микрофоном. Таким образом, получается непрерывный процесс генерации очень эффективного речеподобного шума. Помимо высокой надежности такой генератор имеет еще один плюс – он работает только тогда, когда ведется беседа (когда в помещении тихо – шумы не создаются).

В целом из обзора материалов, связанных с вопросами генерации и применения РПП, можно сделать вывод, что сейчас основной подход к определению понятия «речеподобная» помеха – описательно-технологический, опирающийся на фиксацию способа формирования и применения РПП в каждом конкретном случае.

Как оценивать эффективность применения РПП?

Традиционно для ответа на этот вопрос прибегают к проведению артикуляционных испытаний. При этом обычно их результаты представляются показателями структурного (синтаксического) характера, фиксирующими число неправильно принятых элементов при однократном воспроизведении тестового задания (например, чтения слов из артикуляционных таблиц), что вполне приемлемо в задачах акустики.

Некоторые исследователи считают, что проведение артикуляционных испытаний для оценки эффективности применения шумовых помех, в том числе и РПП, приводит к субъективным, результатам, обусловленным очевидным присутствием человеческого фактора - участвующих в испытаниях дикторов и аудиторов. Поэтому для проверки эффективности различных видов акустических помех, по мнению этих исследователей, целесообразней использовать методы математического (цифрового) моделирования [3]. В качестве модели органа слуха человека принимается корреляционный приемник для обнаружения априорно известного сигнала. Модель процесса обнаружения информативного сигнала представлена на рис. 1.

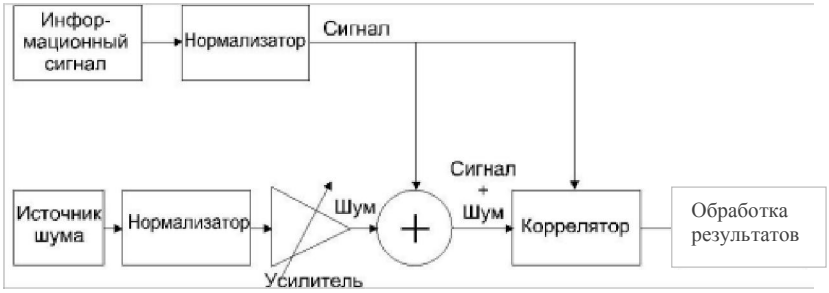

Рисунок 1 – Модель процесса обнаружения информативного сигнала

Информационный сигнал оцифровывается с частотой дискретизации 11025 Гц и поступает на нормализатор, на выходе которого дисперсия сигнала равна 1. Длительность сигнала составляла около 1с.

На выходе источника шума формируется цифровой сигнал (речеподобный или шумовой) с частотой дискретизации 11025 Гц. Шум также проходит операцию нормализации.

В сумматоре происходит аддитивное сложение шума с заданным уровнем сигнала. Таким образом, на один вход коррелятора поступает смесь сигнала и шума, а на второй вход только сигнал. Выходной сигнал коррелятора подвергается статистической обработке. При одном заданном значении сигнал/шум на входе коррелятора проводится 100 измерений различных реализаций шума и программа обработки результатов оценивает математическое ожидание отношения сигнал/шум на выходе коррелятора. Результат обработки представлен на рис. 2.

Данная методика, в частности, показывает, что РПП обладает лучшими маскирующими свойствами, чем белый или розовый шум. Причем наилучшими свойствами обладает РПП, сформированная тем же голосом (например, диктором мужчиной или женщиной), каким был сформирован информативный сигнал [4].

Однако для задач защиты информации основной показатель защищенности речевого сообщения должен отражать уровень его семантического восприятия человеком (в частности, аудитором), при этом следует принимать во внимание возможность многократного воспроизведения записанного сообщения и даже возможность его предварительной шумоочистки. С учетом этого метод артикуляционных испытаний с участием аудиторов может оказаться более надежным и приемлемым для оценки эффективности РПП.

Каков механизм реализации защитного действия РПП?

Обычно предлагаемое объяснение этого механизма эффектом маскировки речевого сигнала помехой исходит из загрубления уровня восприятия биологической речеприемной системы человека воздействующим на нее шумовым сигналом, что приводит к невосприятию переданного речевого элемента (в частности, слова или фразы из артикуляционной таблицы). Процесс восприятия речи в шуме сопровождается потерями составных элементов речевого сообщения. Понятность речевого сообщения характеризуется количеством правильно принятых слов, отражающих качественную степень понятности, которая выражена в категориях подробности справки о перехваченном разговоре, составляемой “противником” (лицом, осуществляющим перехват информации).

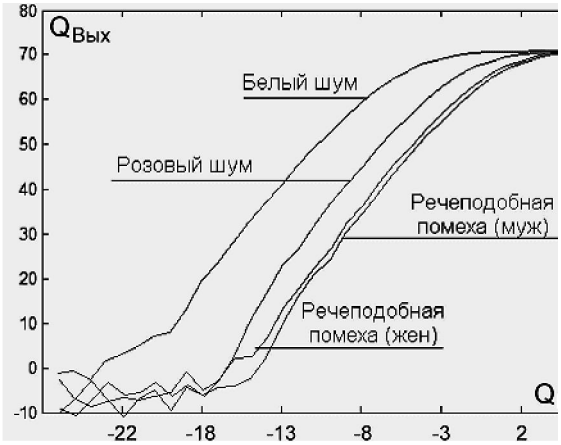

Рисунок 2 – Результат статистической обработки сигнала на выходе коррелятора (Q – отношение сигнал/шум на входе коррелятора; Qвых – отношение сигнал/шум на выходе коррелятора)

В акустике известно, что для каждого звука речи имеются характерные участки частотного спектра, в которых сосредоточена основная энергия звука. Эти участки называются формантами. Человек различает на слух звуки речи только благодаря тому, что каждый из них имеет характерный набор формант. В целом форманты речи заполняют частотный диапазон от 150 до 7000Гц и в наборе составляют гласные и согласные звуки. Каждая из формант вносит свою часть информации о звуках речи независимо от других.

Относительное количество правильно принятых формант A определяет вероятность правильного восприятия отдельных звуков речи. Отношение правильно принятых звуков речи к их общему числу называется звуковой разборчивостью. В свою очередь от правильного восприятия звуков речи зависит насколько будут понятны отдельные слова и речь в целом. Различают смысловую разборчивость J, словесную разборчивость W и слоговую разборчивость S. Они равны отношению правильно понятых фраз, слов или слогов к общему числу и оцениваются в процентах.

Аппаратура подавления с использованием коррелированной помехи ухудшает, прежде всего, смысловую разборчивость записанной речи.

На практике достаточно просто оценить эффективность работы аппаратуры защиты следующим способом.

Имитаторы реальных средств акустического контроля – закладок, микрофонов, диктофонов и т. д. – последовательно устанавливаются в вероятные точки их возможной установки. Производится запись страницы начитанного текста (желательно раздельно мужским и женским голосом). Затем оценивается несколькими экспертами количество понятых смысловых единиц N_1 (фраз или предложений) и усредняется в зависимости от количества экспертов. Далее подсчитывается общее количество смысловых единиц на данной странице текста N_2.

Смысловая разборчивость J оценивается по формуле:

$$J = N_1/N_2 . \qquad (1)$$

Если полученный показатель смысловой разборчивости, усредненный по всем оцениваемым средствам акустического контроля, будет меньше паспортного, значит аппаратура работает и применяется нормально.

Отдельно следует рассматривать вопрос о возможном восстановлении противной стороной записей с помощью компьютерной обработки. Чтобы это проверить, необходимо смоделировать сам процесс такого возможного восстановления. Для этого используются профессиональные специализированные программно-аппаратные средства распознавания речи (так же с успехом в этих целях могут быть использованы современные мультимедийные программные средства с полным набором речевых фильтров) [5, 6]. После компьютерной обработки процесс вычислений по формуле (1) следует повторить уже для обработанной записи.

Для количественной оценки качества перехваченной речевой информации наиболее часто используют показатель – словесная разборчивость речи W, под которой понимается относительное количество (в процентах) правильно понятых слов.

Из практических соображений должна быть установлена некоторая шкала оценок качества перехваченного разговора [5].

1. Перехваченная речевая информация содержит количество правильно понятых слов (фраз), достаточное для составления ***подробной справки*** о содержании перехваченного разговора.

2. Перехваченная речевая информация содержит количество правильно понятых слов (фраз), достаточное только для составления ***краткой справки-аннотации***, отражающей предмет, проблему, цель и общий смысл перехваченного разговора.

3. Перехваченная речевая информация содержит отдельные правильно понятые слова (фразы), позволяющие установить ***предмет*** разговора.

4. При прослушивании фонограммы перехваченного разговора нельзя установить предмет разговора.

Практический опыт показывает, что составление ***подробной справки*** о содержании перехваченного разговора невозможно при словесной разборчивости менее 60 – 70%, а ***краткой справки-аннотации*** – при словесной разборчивости менее 40 – 60%. При словесной разборчивости менее 20 – 40% значительно затруднено установление даже ***предмета*** ведущегося разговора, а при словесной разборчивости менее 10 – 20% это практически невозможно даже при использовании современных методов шумоочистки.

Однако аудиторами в ходе артикуляционной экспертизы часто фиксируется достаточно «четкий» прием аудиообраза, отличного от переданного при относительно низком (в сопоставлении с речевым сообщением) уровнем РПП. Это приводит не только к искажению передаваемой информации, но и к полному семантическому несоответствию содержания принятого сообщения исходной передаваемой информации [7], что позволяет реализовать эффективную защиту речевых сообщений при достаточно комфортных условиях речевой коммуникации.

III Выводы

По результатам рассмотрения и анализа ряда работ, описывающих различные способы зашумления акустической информации, исходя из условия, что поставленная задача защиты речевой информации – не дать злоумышленнику возможность разобраться в смысловом наполнении передаваемого речевого сообщения, наиболее перспективным способом защиты речевой информации представляется использование речеподобной помехи (РПП). При этом учитывается, что РПП дает возможность не просто замаскировать информацию, но и существенно исказить смысл воспринимаемого злоумышленником сообщения.

Что же касается способа оценивания эффективности применения РПП, то наиболее объективным и результативным источником сведений для решения этой задачи является проведение артикуляционных испытаний. В частности, при выполнении ряда требований к составлению артикуляционных таблиц и методу обработки полученных результатов, артикуляционные испытания позволяют выйти за рамки чисто формального структурно-синтаксического оценивания качества приема речевого сигнала, создавая условия и возможности для оценивания уровня семантической близости принятого аудитором сообщения передаваемой исходной (незашумленной) речевой информации.

Список использованной литературы: ***1***. *http://www.confident.org.ua/index.php/stati-po-teme/198-zashchita-rechevoj-informatsii.html.* ***2.*** *Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – 2000. – № 4.– С. 39-45.* ***3***. *http://www.bnti.ru/showart.asp?aid=867&lvl=04.03.01.* ***4***. *Хорев А. А., Макаров Ю. К. Методы защиты речевой информации и оценки их эффективности // Защита информации. Конфидент. – 2001. – № 4. – С. 22-33.* ***5.*** *Радзишевский А. Ю. Основы аналогового и цифрового звука. – М.: Издательский дом «Вильямс», 2006 – 288с.* ***6.*** *Ковалгин Ю. А., Вологдин Э. И. Цифровое кодирование звуковых сигналов. – СПб.: КОРОНА-принт, 2004. – 240 с.* ***7.*** *Архипов А. Е., Архипова Е. А. Анализ и моделирование результатов артикуляционных испытаний // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ – 2010р, випуск 1(25).- с. 21-27.*