УДК:681.327.12:534.782+621.376.57

Об оценке защищенности речевой информации в радиоканалах связи при вокодерных преобразованиях

О.А.Большов

Аннотация

В данной статье представлены результаты исследований, направленных на обеспечение информационной безопасности радиоканалов связи, по которым передаются речевые сообщения при вокодерной связи. На основании эмпирических данных о порогах слуховой чувствительности человека определены некоторые пороговые соотношения сигнал/шум на входе разведывательного приемника, при которых оператор разбирает сообщения слабо, на пределе возможного.

Полученные данные предназначены для разработки норм защищенности цифровых радиоэлектронных средств и систем связи.

Ключевые слова:

вокодер; пороговые сигналы; защита информации.

Информационная революция, происшедшая в мире за последние годы, привела к интенсивному развитию средств связи и вычислительной техники. В процессе информатизации происходит кардинальная смена мировоззрения людей на роль научных знаний и ценность интеллектуальной собственности.

Всякая информация лишь до тех пор чего-нибудь стоит, пока она несет в себе элемент новизны. А новой информация является до тех пор пока она не становится общеизвестной. В противном случае ценность её падает до нуля. Поэтому не случайно, что наряду с интенсивным развитием средств и систем передачи все более значимой становится проблема обеспечения защиты информации. Защита информации в системах связи – весьма важная составляющая обеспечения гарантий безопасности личности. Но не только этого. Различные системы и сети связи всегда использовались для передачи информации конфиденциального характера и с более или менее высоким эффектом применяли разнообразные способы

защиты от ущерба, который может быть причинен несанкционированным доступом к циркулирующим в системах сведениям. Проблемы защиты информации и несанкционированного доступа к ней приняли антагонистический характер в постановке, известной из теории игр. Но применение способов и средств защиты, естественно, должно быть соразмерно степени опасности утечки информации. Применительно к проблеме защиты информации в радиоканалах передачи речи это означает, что целесообразность применения средств и методов обеспечения информационной безопасности должна определяться качеством речи в акустическом канале разведывательного приемника . До тех пор пока оператор средств перехвата не разбирает речевые сообщения – нет необходимости в противодействии радиоэлектронной разведки противника . Но разбирает речевые сообщения – и уже требуется маскировка сигнала от технических средств оппонента. Это положение выдвигает актуальную проблему определения пороговых уровней безопасных мощностей сигналов как в акустических, так и в радио- каналах утечки речевой информации. Актуальность указанной проблемы подтверждается тем, что показатель устойчивости против несанкционированного доступа к сигналу не является основным показателем качества при создании радиоэлектронных систем (РЭС). Так целью защищаемой системы является определение ограничения на нижнее значение соотношения сигнал/шум на входе собственного приемника, когда гарантировано обеспечивается высокая разборчивость на выходе – в акустическом канале приемника абонента. Однако при штатных условиях эксплуатации радиосистемы всегда имеются технические каналы утечки за счет непреднамеренных электромагнитных излучений, которыми сопровождается передача речи. Следовательно, вполне естественным и логичным становится стремление к незаконному, несанкционированному обладанию конфиденциальной информации, передаваемой по связной линии. При этом для системы противодействия представляет интерес оценка максимально допустимого соотношения сигнал/шум на входе разведывательного приемника, при котором еще обеспечивается достаточная защищенность информации и исключается возможность ознакомления несанкционированного пользователя с речевым сообщением. Последнее условие также отражает особую актуальность проблемы защиты информации в радиоканалах передачи речи.

Актуальность исследований в области информационной безопасности констатируется и рядом принятых в последнее время законов, не имеющих аналогов во всей предшествующей истории России, а также соответствующими подзаконными актами, которых уже много, но еще явно недостаточно для четкого и корректного регулирования отношений в области защиты информации.

Учитывая отмеченные выше особенности обеспечения безопасности информации, исходя из практических потребностей, автором для научных исследований была избрана проблема оценки степени защищенности информации, с которой оперируют технические системы, создающие каналы утечки за счет побочных и непреднамеренных электромагнитных излучений речепреобразующих устройств.

Изменение экономических отношений и безусловное признание прав граждан и юридических лиц на владение, использование и распоряжение интеллектуальной собственностью придает особую актуальность проблеме защиты конфиденциальной информации, передаваемой по каналам связи.

Мероприятия и средства обеспечения защиты информации должны планироваться и осуществляться с учетом степени опасности каналов утечки (то есть нормативов защищенности). Оценку степени защищенности каналов передачи речи целесообразно проводить на основе модели идеального средства разведки, использующего всю априорную информацию о сигнале и работающего без потерь энергии сигнала за все время его наблюдения. Для определения показателей защищенности информации в системах связи необходимо основываться на характеристиках разборчивости речи и задавать пороговые уровни безопасных мощностей сигналов в технических каналах утечки информации исходя из этих характеристик.

В настоящее время Российские магистральные системы связи на 96% образованы аналоговыми системами передачи [1]. Такое положение будет оставаться еще достаточно долго: для переоснащения сетей при одновременном их расширении потребуется длительный период. И потому перспектива становления цифровых сетей в качестве реальной альтернативы существующим телефонным каналам связи в области глобальных телекоммуникаций представляется весьма отдаленной. Модем же ликвидирует несоответствие между быстро растущими запросами на цифровую передачу данных и сравнительно скромными в настоящее время техническими средствами, способными осуществлять эту передачу. Модем – устройство для преобразования цифрового информационного сигнала в аналоговый (модуляция) для передачи по аналоговым телефонным сетям, и обратного преобразования принятого аналогового сигнала снова в цифровой [2]. По своему определению модемы всегда связывают два цифровых терминала, например, компьютеры. Таким образом, модем можно рассматривать как с цифровой точки зрения – со стороны компьютера, так и с аналоговой – со стороны телефонной линии.

По мере развития средств и систем передачи данных, все более актуальной становится проблема защиты информации. Модем, поддерживающий возможность защиты

передаваемой информации от доступа к ней неавторизованных пользователей, может реализовывать прямой проход (pass through), метод обратного звонка (dial-back) и, возможно, некоторые другие. В любом случае пользователь сначала вводит свои идентификаторы, которые проверяются с помощью базы данных доступа. Редактирование базы данных доступа модема может быть закрыто паролем. Ниже в данной статье рассматривается проблема скрытности передачи речевой информации в другом аспекте. Во-первых, с точки зрения выделения получателем информации скрытно переданного речевого сообщения с достаточным качеством. Во-вторых, защиты речевых сообщений от перехвата средствами радиоразведки.

Известны условия [4] и [8], при выполнении которых возможно качественное выделение речевого сообщения. Это, прежде всего, ограничение на нижнее значение соотношения сигнал/шум в полосе приемника, при котором обеспечивается достаточная разборчивость речевого сообщения на выходе – в акустическом канале. Однако значения пороговых сигналов, при которых возможно выделение речевого сообщения с достаточным качеством, обычно не исследуются в интересах оценки качества систем связи. Все оценки качества передачи производятся, в основном, для области больших значений соотношения сигнал/шум на входе приемника, когда обеспечивается хорошая разборчивость.

Для систем и средств защиты речевой информации от несанкционированного доступа (перехвата), напротив, интересна оценка предельно малых уровней сигналов на пороге разборчивости (то есть в области, где работает аппаратура несанкционированного доступа к речевым сообщениям). Задача определения таких пороговых сигналов возникает при защите информации в системах связи разных типов и классов. В том числе и в системах связи, использующих звуковые модемы. Такие модемы преобразуют исходный аналоговый речевой сигнал в цифровую форму.

Речевой сигнал, с учетом разброса его параметров и индивидуальных особенностей для разных людей, имеет довольно широкий динамический диапазон. Соответственно он требует для передачи по каналу связи низкого уровня помех и высокой верхней границы неискаженной передачи. В реальных каналах верхняя граница бывает жестко ограничена требованиями согласования при переходах в другие каналы, перегрузкой усилителей и другими причинами. А уровень помех бывает довольно высоким. Поэтому пропустить речевой сигнал через канал без искажений невозможно из-за перегрузки сильных и маскировки слабых по уровню звуков речи. Выход один – сжать или ограничить динамический диапазон речевого сигнала до величины динамического диапазона канала, повысив тем самым помехозащищенность передачи речи и ее разборчивость на приеме.

Компрессия динамического диапазона необходима и для обработки речевого сигнала в тех случаях, когда он должен подвергаться преобразованиям типа вокодерных (от английских слов voice– голос и coder– кодировщик).

Для телефонных каналов в соответствии с принятым стандартом спектр речи ограничивается полосой частот от $f_{\text{Н}} = 300\,\text{Гц}$ до $f_{\text{В}} = 3{,}4\,\text{кГц}$, а частоту дискретизации принимают $f_{\text{Д}} = 8\,\text{кГц}$ [3]. При этих условиях требуемая скорость передачи дискретизированной речи соответствует величине $R_{\text{К}} = f_{\text{Д}} n > 2 f_{\text{В}} = 6{,}8\,\text{кбит/с}$, где n – число двоичных символов в кодовой комбинации, передающей амплитуду речевого сигнала. Покажем, что цифровая передача речевого сигнала имеет очень большую избыточность.

Будем полагать, что под звуками речи понимается фонемы. Точнее фонемой считают наименьшую звуковую единицу данного языка, существующую в целом ряде конкретных звуков речи - вариантов фонем, называемых иногда фоноидами. Таким образом, из-за взаимного влияния соседних фонем, индивидуальной манеры их произношения отдельным человеком число фоноидов значительно превышает число фонем. Отождествляя понятие "фонема" и "звук речи", можно полагать, что "фонема – это то, что человек хочет сказать, а звук речи – это то, что он практически произносит" [3], [4]. Между буквами и фонемами одного и того же языка нет однозначной связи, хотя некоторые буквы и фонемы совпадают. В русском языке обычно различают шесть гласных фонем (у, о, а, э, и, ы), которые по произношению подразделяются на ударные и безударные, а по местоположению в словах – на начальные, серединные и конечные [3]. Согласные фонемы делят на звонкие и глухие. Различные исследователи выделяют различное число фонем. Наиболее часто полагают, что в русском языке от 41 до 48 фонем [4]. Вероятности появления различных фонем в речевом сигнале используются для составления артикуляционных таблиц, применяемых при экспериментальном определении разборчивости речи.

В табл. 1 приведены экспериментальные данные [8] о вероятностях P появления фонем в русской речи с неограниченным словарем. При этом предполагается, что полное число фонем равно 44. В случае использования ограниченного числа слов (например, профессиональных жаргонов) распределение фонем может существенно отличаться от приведенного в табл. 1.

Значения вероятностей появления фонем в русской речи Таблица 1

Фонема	$P \cdot 10^{-4}$	Фонема	$P \cdot 10^{-4}$	Фонема	$P \cdot 10^{-4}$	Фонема	$P \cdot 10^{-4}$
Λ	1316	и	243	ль	162	ф	85
Ь	977	ъ	240	ы	159	сь	85
Т	602	п	232	у	153	ч	59
А	539	р	230	рь	133	мь	56
Й	457	нь	221	з	130	бь	52
Н	392	л	212	дь	126	пь	50
О	379	ш	207	ь	119	кь	36
С	359	м	202	х	102	зь	21
Э	343	ц	197	г	91	фь	8
К	284	ть	196	ж	89	гь	7
В	273	д	177	вь	89	хь	5

Примечание. Λ – безударное а; ь – безударное йэ; ъ – безударное о.

В соответствии с данными табл. 1 можно судить об информативности отдельных фонем: чем реже встречается фонема, тем больше информации она несет. Следовательно, гласные звуки несут гораздо меньшую информацию, чем согласные, а из последних больше информации несут глухие согласные. Гласные в основном служат целям перестройки речевого аппарата для произнесения следующего за ними согласного. Используя данные табл. 1, можно рассчитать энтропию одной фонемы:

$$H_1 = -\sum_{i=1}^{44} P_i \log_2 P_i = 4{,}77 \textit{бит/фонем}. \quad (1)$$

Таким образом, если бы фонемы в слитной речи были независимы, то одна фонема переносила бы 4,77 дв. ед. информации. Средняя длительность произнесения одной фонемы

составляет $t_{\Phi} = 0{,}13\,\text{с}$ [3]. Это означает, что скорость передачи информации речевым сигналом R_1 определяется соотношением:

$$R_1 = \frac{H_1}{t_{\Phi}} = 36{,}7 \textit{бит}/c. \qquad (2)$$

В действительности фонемы в речевом сигнале не являются независимыми. Исследование частоты появления парных комбинаций фонем (статистическая зависимость между фоноидами, получаемыми при объединении фонем, уменьшает скорость передачи информации) [5], [9] дает $H_2 = 3{,}62$ бит/фонему и информативность речевого сигнала имеет вид:

$$R_2 = \frac{H_2}{t_{\Phi}} - 27{,}8 \textit{бит}/c. \qquad (3)$$

Если использовать еще более укрупненные фоноиды, которые в слитной речи будут практически независимы, то можно получить $R = 25\,$бит/с [4]. Эту величину можно считать нижней оценкой скорости речевой передачи информации (то есть информативностью речевого сигнала).

Действительно, если считать, что информационная скорость R речи, – это информативность текста, ей эквивалентного, то $R = 25\,$бит/с. Поэтому при передаче речи по каналам связи эту избыточность стремятся сократить, осуществляя сжатие речевой информации (так как $R << R_{\text{К}}$). Наиболее радикальное сжатие речевой информации достигается с помощью вокодеров. Вокодеры, перед передачей через звуковой модем по каналу связи цифровой последовательности, вычисляют некоторые представительные параметры речевого сигнала. Эта операция осуществляется анализатором речи. Информативность представительных параметров речи существенно ниже, чем исходного речевого сигнала. За счет этого осуществляется сжатие речевой информации. На приемной стороне синтезатор речи восстанавливает с определенной точностью исходный речевой сигнал. Звуковой модем представляет собой отдельное устройство, обеспечивающее передачу данных в соответствии с одним из протоколов, рекомендованных МККТТ.

Формально задача оценки защищенности речевого сообщения, передаваемого с помощью модема, может быть поставлена следующим образом. В канале утечки информации (перехвата) действует сигнал $S(\cdot)$ манипулированный функцией $x(\cdot) \in 0;1$ для передачи в цифровом виде представительных параметров речевого сигнала (звуковые

модемы, работающие в выделенных каналах связи или коммутируемой телефонной сети общего пользования). Представительными параметрами могут быть параметры текущего энергетического спектра речи (полосной вокодер), формант (формантный вокодер) и, возможно, некоторые другие. Цифровой поток, несущий информацию о параметрах речи, с выхода вокодера непосредственно поступает на звуковой модем. Модемом формируется несущее колебание частоты $f_{\text{О}}$. Посылающий модем выступает как генератор несущей. Средняя мощность сигнала в техническом канале утечки информации (на входе приемника средства разведки) $P_{\text{С}}$, а мощность шума – $P_{\text{Ш}}$. Так, что соотношение сигнал/шум, приведенное к входу приемника $q_{\text{ВХ}} = \dfrac{P_{\text{С}}}{P_{\text{Ш}}}$. Считается, что шум имеет равномерную спектральную плотность $N_{\text{О}} = \dfrac{P_{\text{Ш}}}{\Delta f}$ в полосе Δf, занятой спектром сигнала.

В настоящее время в модемах применяются всего три вида манипуляции: частотная, фазоразностная и многопозиционная амплитудно-фазовая манипуляция. Все остальные – не более чем вариации этих трех.

При частотной манипуляции (КИМ-ЧМ) значениям 0 и 1 информационного символа соответствуют свои частоты физического сигнала при неизменной его амплитуде:

$$S(t) = a x(t) \cos 2\pi f_{\text{О}} t + a\left[1 - x(t)\right] \cos 2\pi f_1 t. \qquad (4)$$

Энергетический спектр КИМ-ЧМ по форме совпадает со спектрами двух одиночных видеоимпульсов, разнесенных на частоту $\left|f_{\text{О}} - f_1\right| \geq \dfrac{2}{\tau_{\text{И}}}$, а ширина энергетического спектра $\Delta f \geq \dfrac{4}{\tau_{\text{И}}}$.

При фазоразностной манипуляции (ФРМ) изменяемым в зависимости от значения информационного символа параметром является фаза сигнала S(t) при неизменных амплитуде и частоте. При этом каждому информационному символу ставиться в соответствие не абсолютное значение фазы, а ее изменение относительно предыдущего значения:

$$S_1(t) = \begin{cases} a\cos(\pi f_{\text{О}} t) & 0 \leq t \leq \tau_{\text{И}} \\ a\cos\left[\pi f_{\text{О}} (t - \tau_{\text{И}})\right] & \tau_{\text{И}} \leq t \leq 2\tau_{\text{И}} \end{cases} \qquad (5)$$

$$S_{\text{О}}(t)=\begin{cases} a\cos(2\pi f_{\text{О}}t), & 0\le t\le \tau_{\text{И}} \\ -a\cos[2\pi f_{\text{О}}(t-\tau_{\text{И}})], & \tau_{\text{И}}\le t\le 2\tau_{\text{И}} \end{cases}$$

Сигнал $S_1(t)$ соответствует передаче символа "1" кодовой комбинации (разность фаз $\Delta\varphi = 0$), сигнал $S_{\text{О}}(t)$ – передаче символа "0" (разность фаз $\Delta\varphi = \pi$). Энергетический спектр КИМ-ФРМ по форме совпадает со спектром одиночного видеоимпульса и имеет ширину $\Delta f \ge \frac{2}{\tau_{\text{И}}}$.

При исследовании свойств амплитудно-фазовой манипуляции (АФМ) традиционно используется геометрическая теория сигналов. Сигналы изображаются точками, которые являются концами двумерных векторов на плоскости. Процедура оптимизации расположения сигналов на дискретном регулярном множестве точек рассмотрена в [7], [10] и [11]. Результаты оптимизации сводятся к следующему. При $Y = 4$, где Y – число вариантов сигнала на выходе модема, оптимальным является ансамбль ФМ-4 (четырехпозиционная фазовая манипуляция). Сигналы ФМ-4 отличаются фазами, но имеют равную мощность. При большей информативности модема приходится применять неравномощные сигналы, отличающиеся как фазой, так и амплитудой и размещенные равномерно внутри окружности, радиус которой определяется максимально допустимой энергией сигнала, например, симметричная конфигурация с регулярным расположением сигнальных точек в узлах квадратной сети (QASK, quadrature amplitude - shift keying where the signal array is a rectangular grid).

Структурная схема передачи речевой информации с помощью звукового модема показана на рис.1.

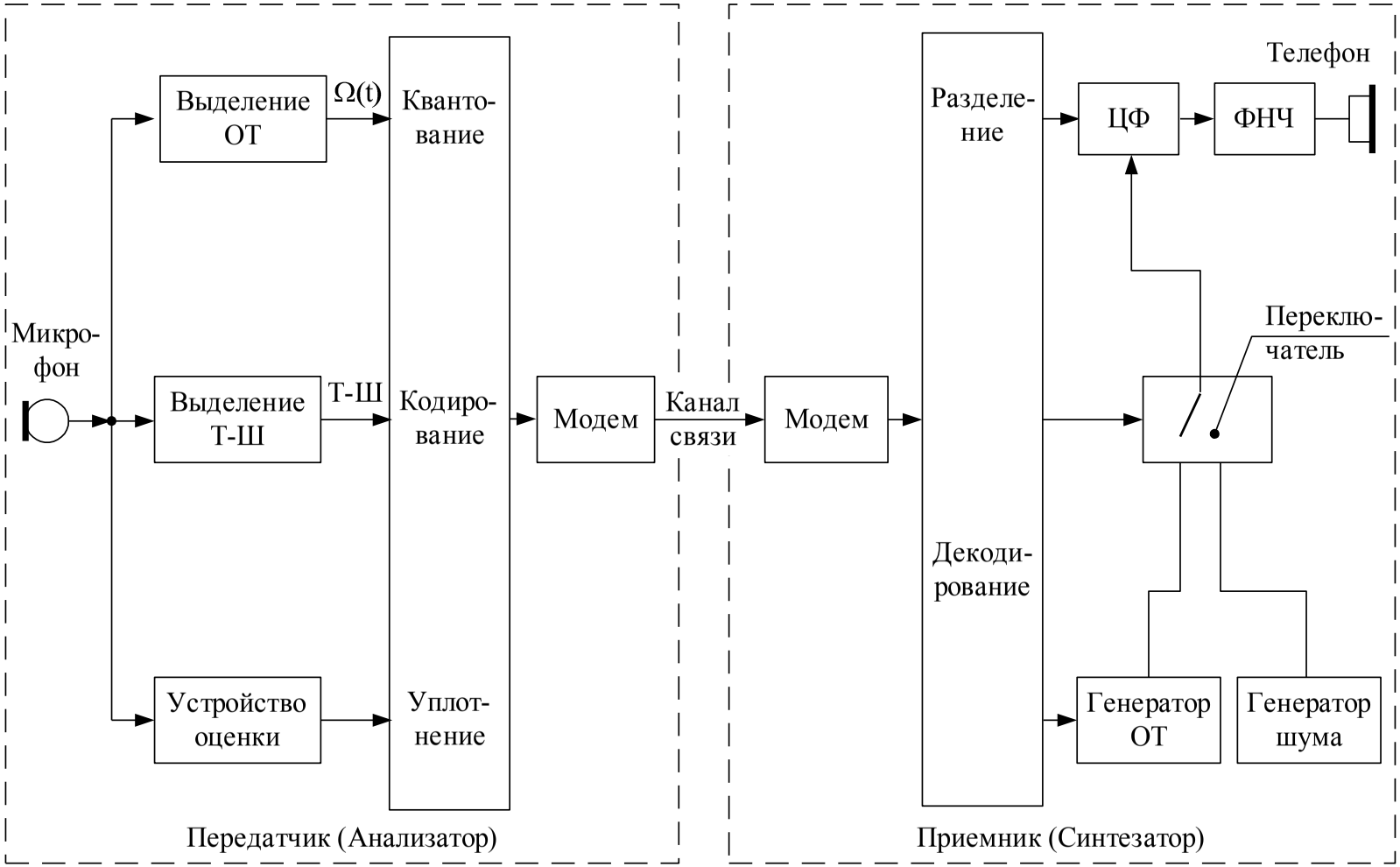

Рис.1. Структурная схема цифровой системы передачи открытого речевого сообщения в узкополосном канале связи.

Компрессия речевых сигналов на передающем конце канала связи производится в анализаторе, выделяющем из речевого сигнала медленно меняющиеся параметры (в устройстве оценки). Речевой сигнал от микрофона поступает также на устройство выделения основного тона (ОТ), на выходе которого формируется сигнал, характеризующий частоту основного тона Ω. Кроме того, в анализаторе выделяется сигнал тон-шум (Т-Ш), характеризующий состав спектра звуков речи – дискретный для вокализованных звуков (тон) или сплошной для невокализованных звуков (шум). Сигналы, полученные на выходе устройства оценки и на выходе устройства выделения основного тона, после квантования вместе с решением тон-шум кодируются, уплотняются и передаются, с помощью модема, на приемную сторону. В синтезаторе речевой сигнал восстанавливается с помощью квазилинейного цифрового фильтра (или набора ЦФ), параметры и характеристики которого устанавливаются равными принятым оценкам периода следования и амплитуды импульсов основного тона или дисперсии шумового возбуждения в зависимости от состояния переключателя.

При анализе пороговых свойств технических каналов утечки информации следует считать, что приемники средств радиоразведки, для выделения представительных параметров речевого сигнала x реализуют оптимальные алгоритмы демодуляции колебания S. Оптимальные в том смысле, что любые технически реализуемые приемники не могут обеспечивать лучшего воспроизведения представительных параметров речевого сигнала.

Полученные при таких условиях оценки качества восстановления (синтезирования) речевого сигнала оказываются верхними, пессимистическими для системы противодействия: реальный приемник в канале перехвата может работать только хуже оптимального.

Исследования и расчеты [3], [7] показывают, что разборчивость речи на выходе – в акустическом канале приемника перехвата определяется как:

$$W = 0{,}2\left[1 - 0{,}004^{k_{\text{О.К.}}L}\right]^4 + 0{,}8\left[1 - 0{,}004^{k_{\text{О.К.}}L}\right]^3, \qquad (6)$$

где W – разборчивость речи (слогов) при воздействии помех; L – коэффициент снижения разборчивости для выбранного типа речепреобразующего устройства:

$$A = 0{,}2\left[1 - 0{,}004^{L}\right]^4 + 0{,}8\left[1 - 0{,}004^{L}\right]^3; \qquad (7)$$

A – разборчивость слогов при отсутствии помех, определяется экспериментально или теоретически (на основе теории разборчивости речи с использованием оценки количества

информации и, возможно, некоторыми другими методами); $k_{О.К.}$ – коэффициент помехоустойчивости [3].

Диаграммы обмена между разборчивостью речи W и вероятностью ошибочного приема двоичного символа $P_{ОШ}$ представлены на рис.2.

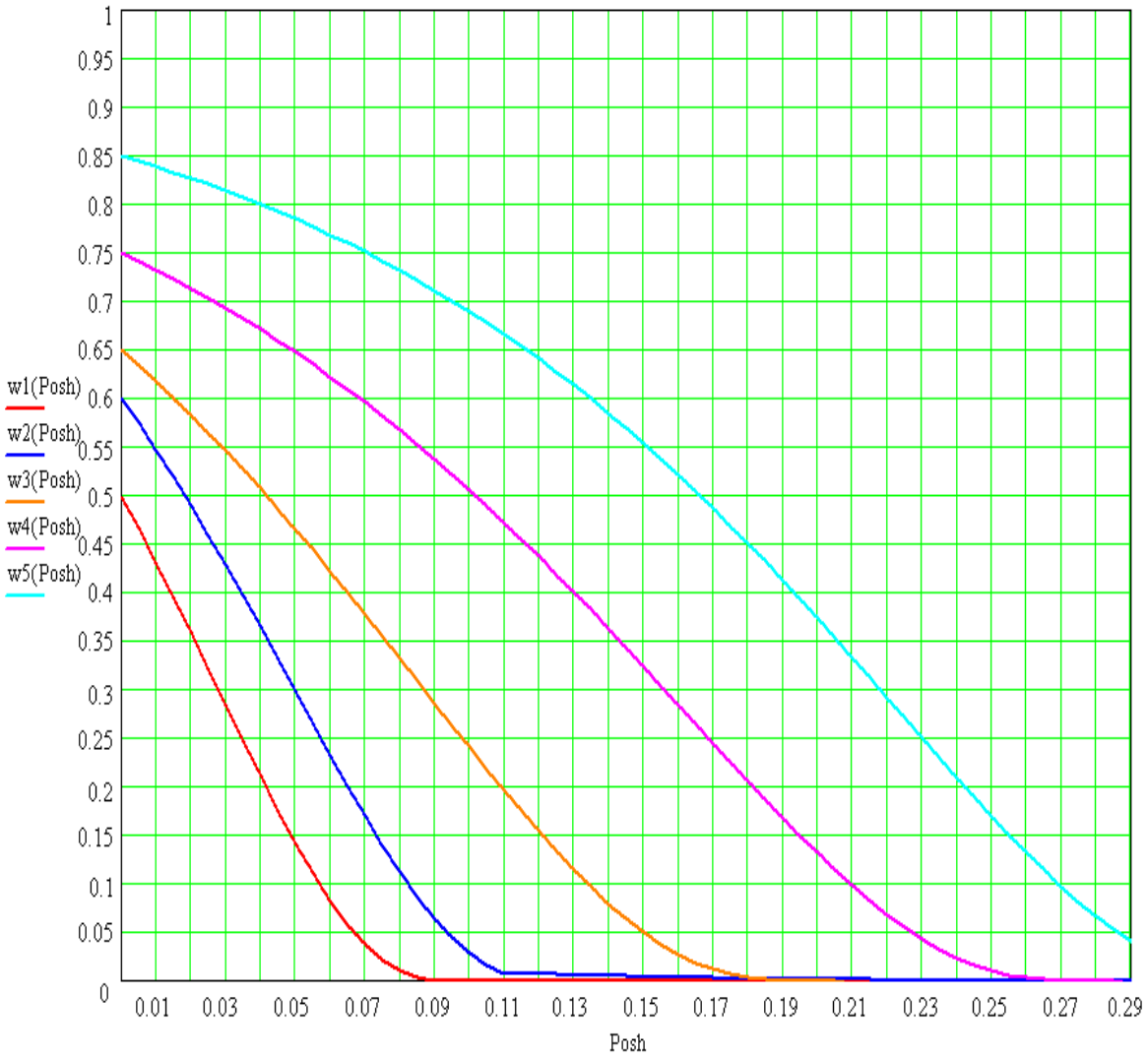

Рис. 2.. Диаграммы для определения допустимых вероятностей ошибок $P_{ОШ}$ при сохранении необходимой разборчивости речи W.

Кривые 1,2 и 4 на рис.2 вычислены для полувокодера**.** Кривая 3 вычислена для вокодера смешанного типа. Кривая 5 вычислена для полосного вокодера. При расчетах были использованы паспортные данные цифровых вокодеров.

В [6], [7] и [11] показано, что вероятность ошибки при когерентном приеме отдельного двоичного символа кодовой комбинации определяется соотношениями:

$$P_{\text{ОШ}} = 1 - \Phi\left[\sqrt{\frac{Q}{N_{\text{О}}}}\right];$$

8)

– для КИМ-ЧМн (частотная манипуляция) и

$$P_{\text{ОШ}} = 1 - \left\{1 - 2\left[1 - \Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}}\sin^2\frac{\pi}{2^K}\right)\right]\Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}\sin^2\frac{\pi}{2^K}}\right)\right\}^{\frac{1}{K}},$$

9)

– для K-кратной фазоразностной манипуляции (ФРМ) первого порядка.

В (8) и (9) обозначено: K – кратность манипуляции ($Y = 2^K$ – число вариантов фаз, используемых при K- кратной манипуляции); $\frac{Q}{N_{\text{О}}} = \frac{P_{\text{С}}\tau_{\text{К}}}{N_{\text{О}}}$; $\tau_{\text{К}}$ – длительность Y-позиционного символа (например, в системе с двукратной ФРМ при той же скорости передачи речевой информации длительность четырехпозиционного символа будет в 2 раза больше, чем при однократной ФРМ, то есть $\tau_{\text{К}} = K\tau_{\text{И}}$); $\tau_{\text{И}}$ – длительность двоичного символа.

– для однократной ФРМ g-ого порядка

$$P_{\text{ОШ}} = \frac{1}{2}\left\{1 - \left[2\Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}}\right) - 1\right]\right\}^{H(g)},$$

(10)

где $H(g) = 2^{V(g)}$; $V(g)$ – число единиц в двоичной записи числа g (вес числа g по Хеммингу).

При $Y = 4$, как уже говорилось, оптимальным является ансамбль ФМ-4 (четырехпозиционная ФМ), [6] и

$$P_{\text{ОШ}} = 1 - \Phi\left(\sqrt{\frac{P_{\text{С}}\tau_{\text{К}}}{N_{\text{О}}}}\right).$$

(11)

При $Y > 4$ наилучшей по помехоустойчивости является симметричная конфигурация с регулярным расположением сигнальных точек в узлах квадратной сети (QASK), [7]:

$$P_{\text{ОШ}} = 1 - \left\{1 - 4\left(1 - \frac{1}{\sqrt{Y}}\right)\left[1 - \Phi\left(\sqrt{\frac{3P_{\text{С}}\tau_{\text{К}}}{2N_{\text{О}}(Y-1)}}\right)\right]\Phi\left(\sqrt{\frac{3P_{\text{С}}\tau_{\text{К}}}{2N_{\text{О}}(Y-1)}}\right)\right\}^{\frac{1}{K}},$$

(12)

где K – кратность манипуляции.

В [4] и [5] показано, что вероятность правильного узнавания слога определяется соотношением:

$$W(q_{\text{ВЫХ}}) = \begin{cases} 1 - 0{,}242 q_{\text{ВЫХ}}^{-0{,}325}; q_{\text{ВЫХ}} \geq 0{,}025 \\ 50 q_{\text{ВЫХ}}^{1{,}5}; q_{\text{ВЫХ}} < 0{,}025 \end{cases}, \quad (13)$$

где $q_{\text{ВЫХ}}$ – соотношение сигнал/шум в акустическом канале.

Диаграммы обмена между соотношением сигнал/шум в акустическом канале $q_{\text{ВЫХ}}$ и соотношением сигнал/шум на входе приемника радиоразведки $q_{\text{ВХ}}$, полученные автором, приведены на рис.3. Диаграммы обмена рассчитаны на основании соотношений (6) и (8)…(13).

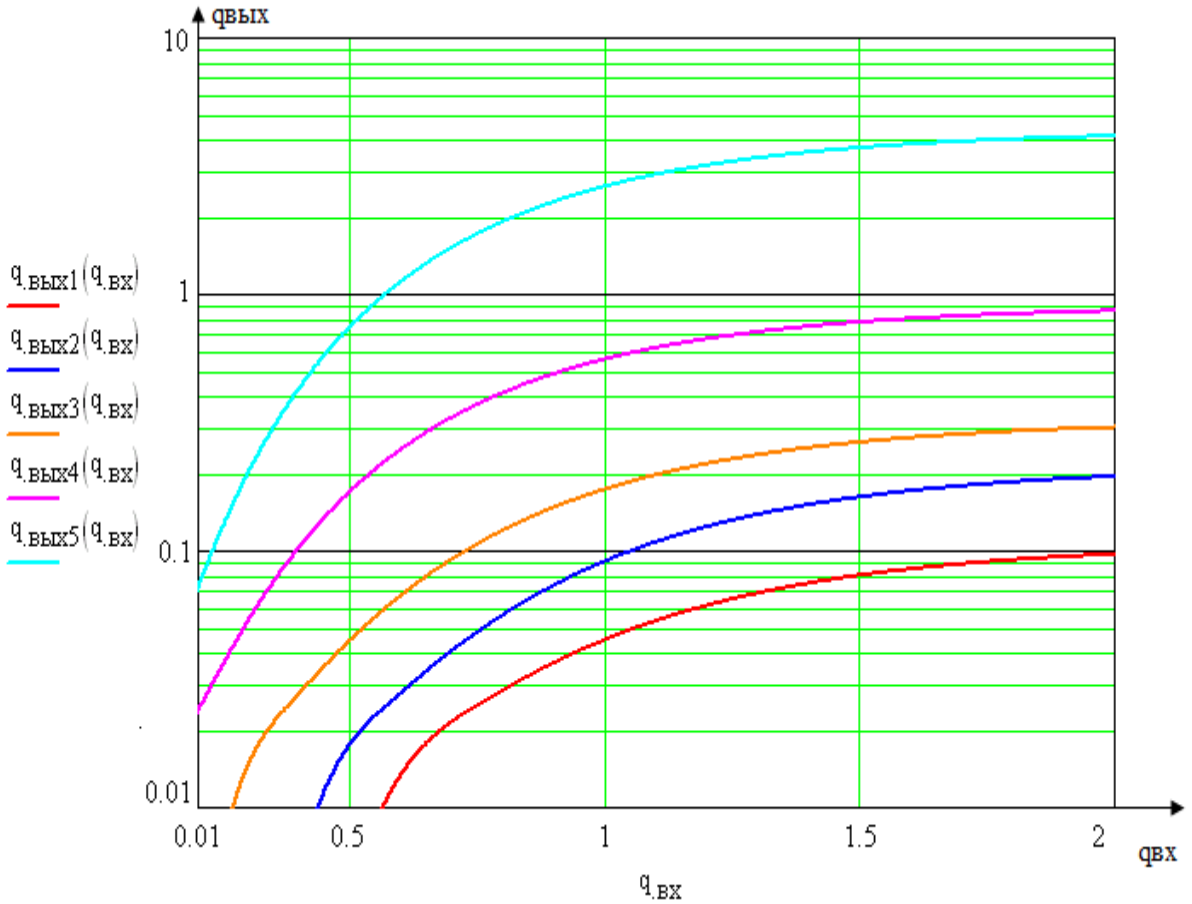

Рис. 3. Диаграммы обмена между соотношением сигнал/шум в акустическом канале $q_{\text{ВЫХ}}$ и соотношением сигнал/шум на входе разведывательного приемника $q_{\text{ВХ}}$.

Полагая граничное значение вероятности правильного узнавания слога $W = 0{,}2$ из (6), (8)…(13) и диаграмм рис2,3 можно найти пороговые (граничные сигналы), при которых уже не обеспечивается разборчивость речи.

В таб.2 для сравнения приведены граничные значения вероятности ошибочного приема символа $P_{\text{ОШ.ГР}}$ и соотношения сигнал/шум на входе приемника $q_{\text{ВХ.ГР}}$ для различных устройств преобразования речи.

Пороговые значения при вокодерных преобразованиях речи Таблица2

Тип речепреобразующего устройства	Граничные значения			W
	$P_{\text{ОШ.ГР}}$	$q_{\text{ВХ.ГР}}$	$q_{\text{ВЫХ.ГР}}$	
Десятиканальный полувокодери при использовании в основном канале дельта - модуляции (кривая 1)	0,041	0,76	0,026	0.2
Восьмиканальный полувокодер при использовании в основном канале предельного ограничения (кривая 2)	0,065	0,58	0,026	0,2
Вокодер смешанного типа с передачей амплитуды и частоты первой форманты при четырех спектральных каналах (кривая 3)	0,11	0,385	0,026	0,2
Восьмиканальный полосной полувокодер с импульсно-кодовой модуляцией в основном канале (кривая 4)	0,18	0,21	0,026	0,2
Шестиканальный полосной вокодер (кривая 5)	0,24	0,125	0,026	0,2

Защита речевых сообщений, передаваемых по связной линии, достигается при санкционированном приеме в надпороговой области (соотношение сигнал/шум, приведенное

ко входу приемника абонента, превышает пороговый уровень) и несанкционированном перехвате непреднамеренных электромагнитных излучений связных систем в подпороговой области. Если последнее условие не выполняется, то необходимо разрабатывать специальные методы и обосновывать оптимальные мероприятия по маскировке речевых сообщений от средств радиотехнической разведки.

Сформулированные условия защищенности и определенные потенциальные характеристики безопасности информации в каналах передачи преобразованной речи предназначены для разработки норм защищенности таких цифровых систем связи, которые не применяют криптозащиту, скремблирование и другие возможные методы обеспечения информационной защиты.

Полученные данные могут быть использованы для оценки предельных характеристик защищенности речевой информации от перехвата и несанкционированного восстановления сообщения средствами радиоразведки.

Библиографический список

1. Кулешов А.П. Протоколы информационно-вычислительных сетей. – М.: Радио и связь, 2006. – 504с.
2. Вильховченко С.Д. Модемы (выбор, установка, настройка) и их бесплатное приложение (терминалы, скрипты, факсы. BBS, Fido). – М.: ABF, 1997. – 560с.
3. Калинцев Ю.К. Разборчивость речи в цифровых вокодерах. – М.: Радио и связь, 1991. – 220с.
4. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Радио и связь, 1962. – 392с.
5. Быков Ю.С. Теория разборчивости речи и повышение эффективности радиотелефонной связи. – М. – Л.: Госэнергоиздат, 1959. – 351с.
6. Окунев Ю.Б. Цифровая передача информации фазомодулированными сигналами. – М.: Радио и связь, 1991. – 297с.
7. Барсуков В.С. Новая информационная технология: искусственный интеллект, концепция банка знаний, экспертные системы. – М.: Знание, 1989. – 187с.
8. Величкин А.И. Передача аналоговых сообщений по цифровым каналам связи. – М.: Радио и связь, 1983. – 240с.
9. Михайлов В.Г. Измерение параметров речи. – М.: Радио и связь, 1987. – 168с.

10. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384с.
11. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – М.: Издательский дом "Вильямс", 2004. – 1104с.

Сведения об авторе

Большов Олег Анатольевич, доцент Московского авиационного института (государственного технического университета), к.т.н.

МАИ, Волоколамское ш., 4, Москва, А-80, ГСП-3, 125993,

тел: 8 (499) 158 – 49 – 33 .