УДК: 681.327.12:534.782+621.376.57

Скрытность передачи речевых сообщений

О.А. Большов

Аннотация

В статье рассмотрена проблема скрытности передачи речевых сообщений по открытым каналам радиосвязи и определены минимальные уровни сигналов, обеспечивающие необходимую разборчивость при цифровых преобразованиях речи.

Ключевые слова

пороговые сигналы; защита информации; сигналы цифровых средств телекоммуникации и связи.

Статья посвящена решению задач обеспечения конфиденциальности информации, законности ее использования. Для этого в работе проводится анализ степени опасности каналов утечки речевой информации и возможных преднамеренных пассивных угроз (то есть угроз, связанных с несанкционированным восстановлением сообщений средствами радиоразведки за счет перехвата излучений). Такой вид угроз считается наиболее вероятным. Так как реализация пассивных угроз требует значительно меньших затрат, чем реализация угроз активных, являющихся следствием попыток перехвата и изменения смысла передаваемой по открытому радиоканалу информации. Однако даже для того, чтобы злоумышленник (активный нарушитель) имел возможность навязать санкционированному пользователю в информационном конфликте (противоборстве, войне) ложную информацию необходимо, как минимум, выполнение следующих событий. Разведывательный приемник должен принять, достоверно обнаружить и идентифицировать сигнал, несущий в себе речевое сообщение.

В настоящее время Российские магистральные системы связи на 96% образованы аналоговыми системами передачи [2]. 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 [3]. 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 скрытно переданного речевого сообщения с достаточным качеством. Во-вторых, защиты речевых сообщений от перехвата средствами радиоразведки.

Данная статья содержит результаты исследований, позволяющих оценить степень (меру) защищенности речевой информации в процессе информационного обмена в системах и сетях связи. Это особенно важно для обоснования целесообразности проведения оперативных мероприятий по противодействию несанкционированному обращению с информационными ресурсами. Актуальность подобных исследований можно подтвердить следующим. Известны ограничения, накладываемые на минимально допустимые соотношения сигнал/шум на входе приемника абонента, при которых санкционированный пользователь с вероятностью, близкой к единице, правильно разбирает элементы (звуки, слога, слова) речевого сигнала. Исследование же разборчивости речи при слабых сигналах на входе приемника имеет специфические отличия от тех, что привели к известным результатам для области сильных сигналов, где работает абонентская аппаратура санкционированного доступа к речевым сообщениям. Поэтому анализ пороговых свойств сигналов в технических каналах утечки информации является актуальной проблемой.

Задача определения таких пороговых сигналов возникает при защите информации в системах связи разных типов и классов. В том числе и в системах связи, использующих модемы. Такие модемы преобразуют исходный аналоговый речевой сигнал в цифровую форму.

Для телефонных каналов в соответствии с принятым стандартом спектр речи ограничивается полосой частот от $f_{\text{Н}} = 300$ Гц до $f_{\text{В}} = 3{,}4$ кГц, а частоту дискретизации принимают $f_{\text{Д}} = 8$ кГц [3]. При этих условиях требуемая скорость передачи дискретизированной речи соответствует величине $R_{\text{К}} = 2 f_{\text{В}} n > 2 f_{\text{В}} = 6{,}8$ кбит/с, где n – число двоичных символов в кодовой комбинации, передающей амплитуду речевого сигнала. Следовательно, цифровая передача речевого сигнала имеет очень большую избыточность. Действительно, если считать, что информационная скорость R речи, – это информативность текста, ей эквивалентного, то из [1] $R = 25$ бит/с. Поэтому при передаче речи по каналам связи эту избыточность стремятся сократить, осуществляя сжатие речевой информации. 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. Избыточность 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 (в канале перехвата) действует сигнал $S(t)$ манипулированный функцией $x(t) \in 0;1$ для непосредственной передачи в цифровом виде речевого сигнала (широкополосные модемы, работающие на высокоскоростных телефонных, радио, спутниковых и оптоволоконных каналах связи) и/или 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.

Цифровая последовательность параметров речи с выхода вокодера непосредственно поступает на звуковой модем. Модемом формируется несущее колебание частоты $f_О$. Посылающий модем выступает как генератор несущей. Средняя мощность сигнала в техническом канале утечки информации (на входе приемника средства разведки) $P_С$, а мощность шума – $P_Ш$. Так, что соотношение сигнал/шум, приведенное ко входу приемника $q_{ВХ} = \frac{P_С}{P_Ш}$. Считается, что шум имеет равномерную спектральную плотность $N_О = \frac{P_Ш}{\Delta f}$ 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:

$$S(t) = ax(t)\cos 2\pi f_О t + a[1 - x(t)]\cos 2\pi f_1 t \quad (1)$$

Энергетический спектр КИМ-ЧМ по форме совпадает со спектрами двух одиночных видеоимпульсов, разнесенными на частоту $|f_О - f_1| \geq \frac{2}{\tau_И}$, а ширина энергетического спектра $\Delta f \geq \frac{4}{\tau_И}$.

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:

$$S_1(t) = \begin{cases} a\cos(2\pi f_О t); 0 \leq t \leq \tau_И \\ a\cos[2\pi f_О (t - \tau_И)]; \tau_И \leq t \leq 2\tau_И \end{cases}$$

$$S_О(t) = \begin{cases} a\cos(2\pi f_О t); 0 \leq t \leq \tau_И \\ -a\cos[2\pi f_О (t - \tau_И)]; \tau_И \leq t \leq 2\tau_И \end{cases} \quad (2)$$

Сигнал $S_1(t)$ соответствует передаче символа "1" кодовой комбинации (разность фаз $\Delta\varphi = 0$), сигнал $S_0(t)$ – передаче символа "0" (разность фаз $\Delta\varphi = \pi$). Энергетический спектр КИМ-ФРМ по форме совпадает со спектром одиночного видеоимпульса и имеет ширину $\Delta f \geq \frac{2}{\tau_и}$.

При исследовании свойств амплитудно-фазовой манипуляции (АФМ) традиционно используется геометрическая теория сигналов. Сигналы изображаются точками, которые являются концами двумерных векторов на плоскости (рис. 1…6). Процедура оптимизации расположения сигналов на дискретном регулярном множестве точек рассмотрена в [5], [8] и [10]. 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).

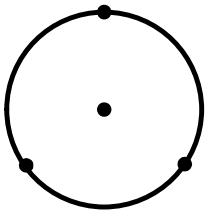

Рис. 1. Двукратный сигнал с АФМ – (1, 3).

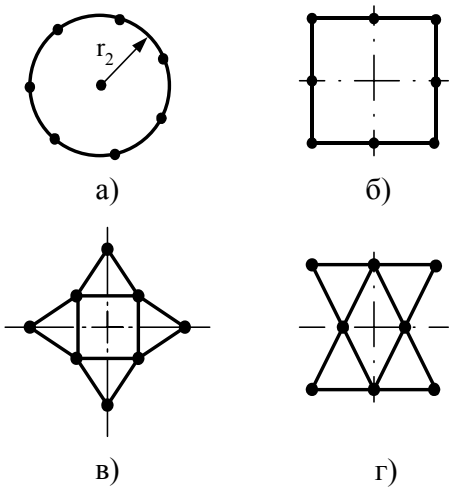

Рис. 2. Восьмипозиционный сигнал с АФМ. Расположение сигнальных точек:

а) круговое, $r_1 = 0; r_2 = 1{,}153$ -(1,7);

б) на основе квадратной сетки – (4, 4);

в) круговое, $r_1 = 0{,}707; r_2 = 1{,}366$ -(4,4);

г) треугольное – (2, 2, 4).

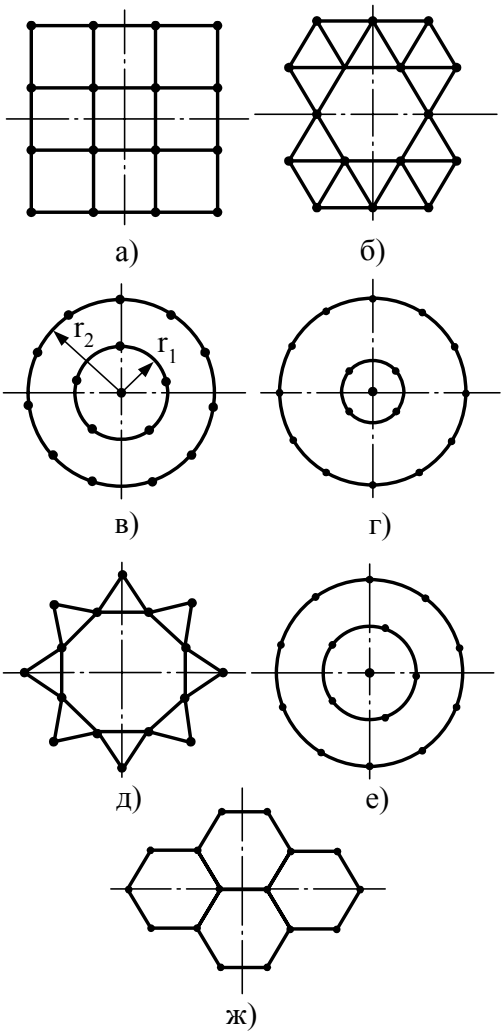

Рис. 3. Шестнадцатипозиционный сигнал с АФМ. Расположение сигнальных точек:

а) на основе квадратной сетки – (4x4);

б) треугольное – (6, 2, 8);

в) круговое, r_1=0,853, r_2=1,72-(5,11);

г) круговое, r_1=0,707, r_2=1,93-(4,12);

д) круговое, r_1=1,305, r_2=2,17-(8,8);

е) круговое, r_1=0, r_2=0,9, r_3=1,8-(1,5,10);

ж) гексагональное – HEX – 16.

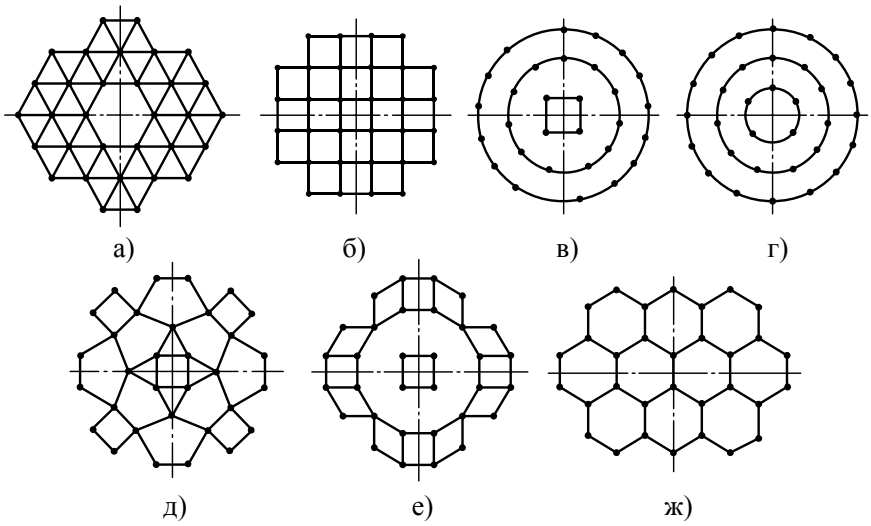

Рис. 4. 32 – позиционный сигнал с АФМ. Расположение сигнальных точек:

а) треугольное; б) на основе квадратной сетки – (4, 12, 16); в) круговое, r_1=0,707, r_2=1,72, r_3=2,68-(4,11,17); г) круговое, r_1=0,853, r_2=1,72, r_3=2,56); д), е) смешанное (комбинированное); ж) гексагональное – HEX – 32.

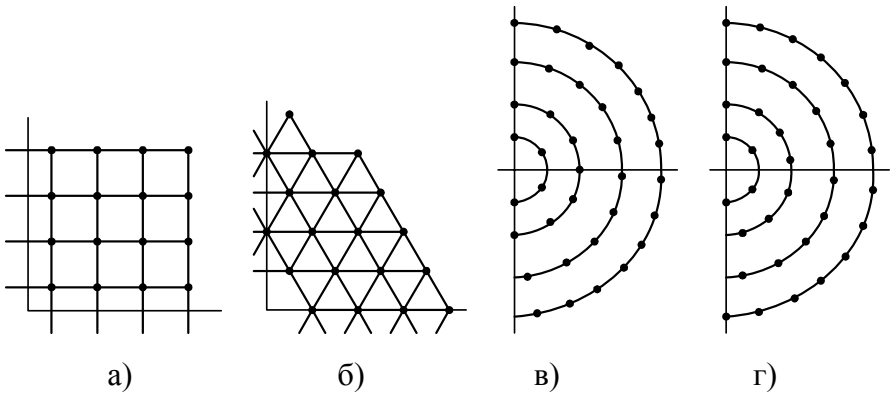

Рис. 5. 64 – позиционный сигнал с АФМ. Расположение сигнальных точек:

а) на основе квадратной сети; б) треугольное; в) круговое, r_1=1, r_2=1,93, r_3=3,04, r_4=4,29-(6,12,19,27); г) круговое, r_1=1, r_2=2,08, r_3=3,04, r_4=4,15-(6,13,19,26).

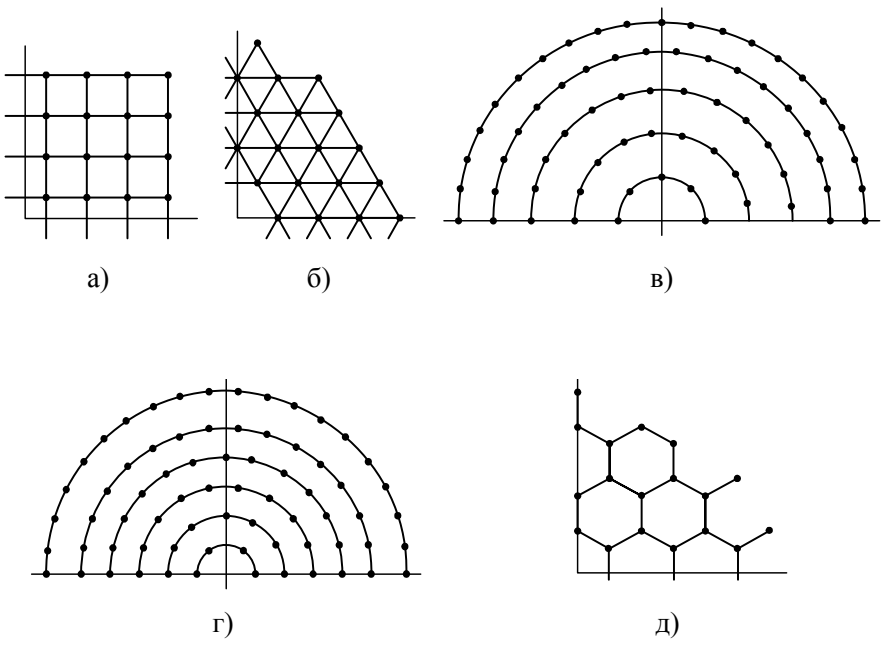

Рис. 6. 128 – позиционный сигнал с АФМ. Расположение сигнальных точек:

а) на основе квадратной сети; б) треугольное; в) круговое, r_1=1,31, r_2=2,68, r_3=3,99, r_4=5,41, r_5=6,25-(8,17,25,34,44); г) круговое, r_1=1, r_2=1,93, r_3=2,88, r_4=3,83, r_5=4,78, r_6=6,05-(6,12,18,24,,30,38); д) гексагональное HEX – 128.

При анализе пороговых свойств технических каналов утечки информации следует считать, что приемники средств радиоразведки, для выделения речевого сигнала $x(t)$ реализуют оптимальные алгоритмы демодуляции колебания $S(t)$. Оптимальные в том смысле, что любые технически реализуемые приемники не могут обеспечивать лучшего воспроизведения 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 [4], [7] и [8] показывают, что в вокодерах всех типов узнаваемость голосов и натуральность звучания речи недостаточно высоки. В тех случаях, когда не требуется существенная компрессия речевых сигналов, качество звучания речи и узнаваемость голосов в акустическом канале приемника абонента могут быть улучшены, если наряду с вокодерными сигналами передавать участок не преобразованной вокодером речи. Устройства, в которых кроме вокодерных сигналов передается участок не преобразованной вокодером речи, называют полувокодерами. Структурная схема полувокодера представлена на рис. 7.

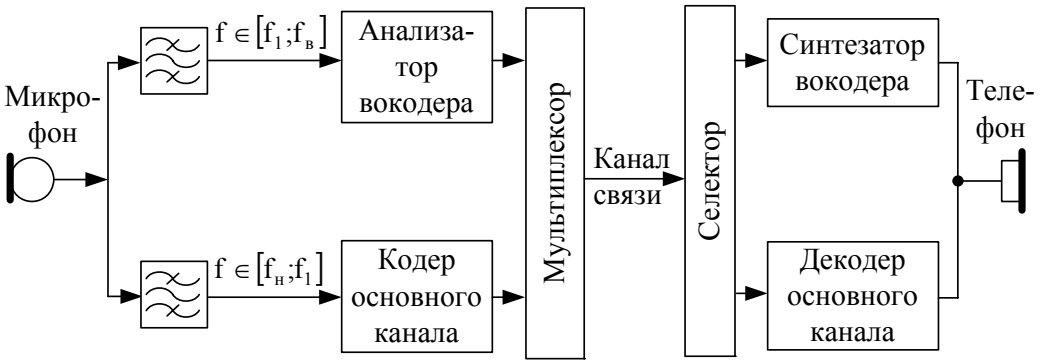

Рис. 7. Структурная схема полувокодера.

Тракт, по которому в аппаратуре проходят речевые сигналы, не подвергающиеся вокодерным преобразованиям, называют основным каналом.

Непосредственное (в отличие от вокодерного) преобразование речевого сигнала сводится к дискретизации и квантованию сигнала на передающей стороне и восстановлению посредством интерполирующего (синтезирующего) фильтра – на приемной стороне защищаемой системы.

Исследования и расчеты [3] [4] показывают, что разборчивость речи на выходе – в акустическом канале приемника перехвата определяется как:

$$W = 0{,}2\left[1 - 0{,}004^{kL}\right]^4 + 0{,}8\left[1 - 0{,}004^{kL}\right]^3, \tag{3}$$

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

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

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 – коэффициент помехоустойчивости.

Помехи, возникающие в канале связи, непосредственно на речевой сигнал не воздействуют, а приводят к тому, что информационные символы, передаваемые по каналу связи, могут изменить свое значение на противоположное. При ложном приеме происходит искажение декодированных речевых сигналов. Эти искажения эквивалентны воздействию помех, мощность которых пропорциональна вероятности ошибочного приема символа кодовой комбинации.

В [3] показано, что коэффициент разборчивости речи при наличии помех в канале связи k определяется соотношением:

$$k = 1 + \gamma P_{\text{ОШ}} \log_2 (\gamma P_{\text{ОШ}}) + (1 - \gamma P_{\text{ОШ}}) \log_2 (1 - \gamma P_{\text{ОШ}}), \quad (5)$$

где $P_{\text{ОШ}}$ – вероятность ошибки при приеме отдельного символа кодовой комбинации; γ – коэффициент, учитывающий порядковый номер символа в кодовой комбинации (при кодово-импульсной манипуляции (КИМ) искажение разных информационных символов, входящих в одну кодовую комбинацию, приводит к неодинаковым изменениям амплитуды восстановленного речевого сигнала: одному информационному символу соответствует увеличение (или уменьшение) амплитуды речевого сигнала на один шаг квантования, другому символу – на два шага, третьему – на четыре шага и т.д.):

– для КИМ с логарифмической шкалой квантования

$$\gamma = \frac{2}{(1 + P_{\text{ОШ}})} \left[1 - \left(\frac{1 - P_{\text{ОШ}}}{2} \right)^n \right]; \quad (6)$$

– для КИМ с линейной шкалой квантования

$$\gamma = \frac{2(2^n - 1)}{2^n}. \quad (7)$$

В [5] и [8] показано, что вероятность ошибки при когерентном приеме отдельного двоичного символа кодовой комбинации определяется соотношениями:

$$P_{\text{ОШ}} = 1 - \Phi \left[\sqrt{\frac{Q}{N_{\text{О}}}} \right]; \quad (8)$$

– для КИМ-ЧМн (частотная манипуляция) и

$$P_{\text{ОШ}} = 1 - \left\{ 1 - 2 \left[1 - \Phi \left(\sqrt{\frac{2Q}{N_{\text{О}}}} \sin^2 \frac{\pi}{2^K} \right) \right] \Phi \left(\sqrt{\frac{2Q}{N_{\text{О}}}} \sin^2 \frac{\pi}{2^K} \right) \right\}^{\frac{1}{K}}, \quad (9)$$

– для K-кратной 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

$$P_{\text{ОШ}} = \frac{1}{2}\left\{1 - \left[2\Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}}\right) - 1\right]\right\}^{H(g)}, \tag{10}$$

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), [10] и

$$P_{\text{ОШ}} = 1 - \Phi\left(\sqrt{\frac{P_{\text{С}}\tau_{\text{К}}}{N_{\text{О}}}}\right). \tag{11}$$

При $Y > 4$ наилучшей по помехоустойчивости является симметричная конфигурация с регулярным расположением сигнальных точек в узлах квадратной сети (QASK), [8]:

$$P_{\text{ОШ}} = 1 - \left\{1 - 4\left(1 - \frac{1}{\sqrt{Y}}\right)\left[1 - \Phi\left(\frac{3P_{\text{С}}\tau_{\text{К}}}{2N_{\text{О}}(Y-1)}\right)\right]\Phi\left(\sqrt{\frac{3P_{\text{С}}\tau_{\text{К}}}{2N_{\text{О}}(Y-1)}}\right)\right\}^{\frac{1}{K}}, \tag{12}$$

где K – кратность манипуляции.

Подставляя в (3) соотношения (8) … (12), можно построить диаграммы обмена между разборчивостью речи и мощностью входного сигнала. Эти диаграммы в координатах $W - q_{\text{ВХ}}$ представлены на рис.8.

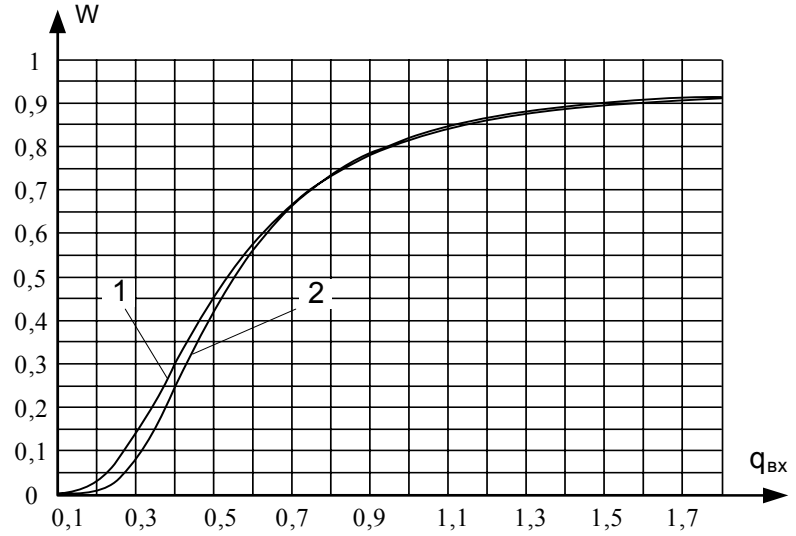

Рис. 8. Диаграммы обмена между разборчивостью речи W и соотношением сигнал/шум в полосе приемника радиоразведки $q_{\text{ВХ}}$.

Кривая 1 вычислена для КИМ с логарифмической шкалой квантования. Кривая 2 вычислена для КИМ с линейной шкалой квантования. Кривые 1, 2 вычислены для различных способов преобразования речи в полосе частот (300...3400) Гц, при $n = 8$.

По диаграммам рис.8 можно определить минимальные соотношения сигнал/шум на входе (в полосе приемника радиоперехвата), при которых обеспечивается необходимая разборчивость речи.

В [1] и [4] показано, что вероятность правильного узнавания слога определяется соотношением:

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

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 $q_{\text{ВХ}}$ приведены на рис.9. Диаграммы обмена рассчитаны на основании тех же соотношений (3) и (8)…(13).

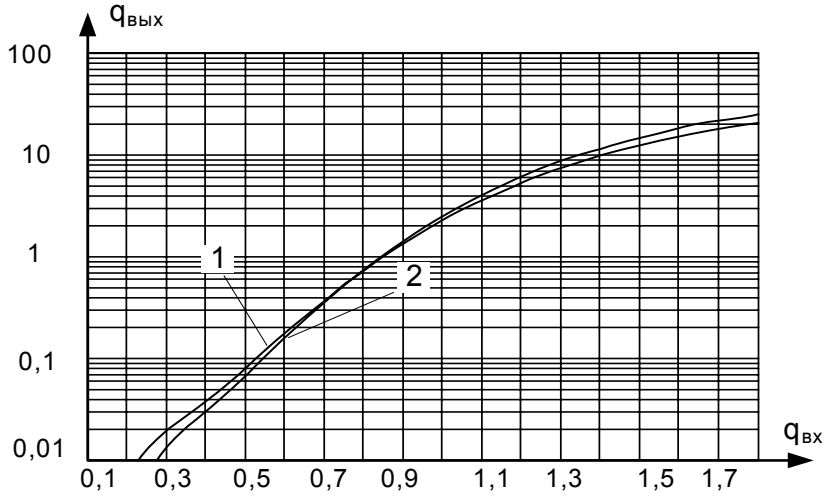

Рис. 9. Диаграммы обмена между соотношением сигнал/шум в акустическом канале $q_{\text{ВЫХ}}$ и соотношением сигнал/шум на входе разведывательного приемника $q_{\text{ВХ}}$.

Полагая граничное значение вероятности правильного узнавания слога $W = 0{,}2$ из (3), (8)…(13) и диаграмм рис8,9 можно найти пороговые (граничные сигналы), при которых уже не обеспечивается разборчивость речи.

В таб.1 для сравнения приведены граничные значения вероятности ошибочного приема символа $P_{\text{ОШ.ГР}}$ и соотношения сигнал/шум на входе приемника радиоразведки $q_{\text{ВХ.ГР}}$.

Пороговые значения при кодово-импульсной модуляции

Таблица1

Способ преобразования речевых сигналов	Граничные значения			W
	$P_{\text{ОШ.ГР}}$	$q_{\text{ВХ.ГР}}$	$q_{\text{ВЫХ.ГР}}$	
КИМ с логарифмической шкалой квантования (кривая 1)	0,122	0,35	0,026	0.2
КИМ с линейной шкалой квантования (кривая 2)	0,112	0,38	0,026	0,2

В настоящей статье приведены результаты исследований, направленных на обеспечение информационной безопасности радиоканалов передачи речевых сообщений в цифровых системах связи. На основании статистических данных о порогах слуховой чувствительности человека-оператора, определены предельно допустимые уровни сигналов на входе разведывательного приемника, при которых оператор средств перехвата разбирает речевые сообщения слабо, на пределе возможного. Эти уровни мощностей позволяют оценить степень опасности утечки речевой информации и необходимость активного противодействия средствам радиоразведки.

Полученные данные могут быть использованы для оценки предельных характеристик защищенности речевого сигнала, передаваемого по связной линии, от перехвата и восстановления сообщения средствами радиоразведки.

Библиографический список

1. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Радио и связь, 1962. – 392с.
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. Быков Ю.С. Теория разборчивости речи и повышение эффективности радиотелефонной связи. – М. – Л.: Госэнергоиздат, 1959. – 351с.
5. Окунев Ю.Б. Цифровая передача информации фазомодулированными сигналами. – М.: Радио и связь, 1991. – 297с.
6. Барсуков В.С. Новая информационная технология: искусственный интеллект, концепция банка знаний, экспертные системы. – М.: Знание, 1989. – 187с.
7. Величкин А.И. Передача аналоговых сообщений по цифровым каналам связи. – М.: Радио и связь, 1983. – 240с.
8. Михайлов В.Г. Измерение параметров речи. – М.: Радио и связь, 1987. – 168с.
9. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384с.
10. Кулешов А.П. Протоколы информационно-вычислительных сетей. – М.: Радио и связь, 1990. – 504с.

Сведения об авторе

Большов Олег Анатольевич, доцент кафедры радиосистем передачи информации и управления Московского авиационного института (государственного технического университета), к.т.н. Контакты: +7 499 158–49–33.