УДК:681.327.12:534.782+621.376.57

Пороговые сигналы при кодово-импульсной манипуляции.

О.А.Большов

В статье рассмотрена проблема оценки степени защищенности сигналов цифровых систем передачи речевой информации и определены предельно допустимые безопасные уровни сигналов в радиоканалах передачи и перехвата связной информации.

Ключевые слова: пороговые сигналы, цифровых сигналы передачи речевой информации

Информатизация государства и общества, а также стремление, как государственных структур, так и физических лиц обладать конфиденциальной информацией выдвигает на первый план проблемы информационной безопасности, то есть диалектического единства проблем защиты информации и проблем защиты от информации. Следовательно, все большую актуальность приобретает противодействие информационной агрессии, направленной на перехват сообщений, нарушение целостности и достоверности информации, ее искажение, подмену или утерю.

В данной статье рассматривалась и решалась задача оценки степени защищенности речевой информации в радиоканалах цифровой связи от несанкционированного приема и восстановления содержания речевых сообщений, выделяемых из перехваченных сигналов побочного и непреднамеренного электромагнитного излучения речепреобразующих устройств.

Следует подчеркнуть, что радиоканал относится к наиболее опасным в информационном плане каналам утечки: в силу оперативности его работы и скрытности перехвата. Следовательно, радиоканал – это самое узкое место систем защиты сообщений и именно он создает наибольшую угрозу нарушения конфиденциальности информации. В статье для радиоканала оценивается возможность и потенциальные характеристики качества несанкционированного съема речевой информации с тем, чтобы это качество максимально снизить. Достоверность и сама возможность добывания информации с помощью радиоканала утечки зависит от уровня опасных сигналов, переносящих защищаемую информацию. Так, если уровень перехваченного излучения не превышает некоторой пороговой величины, то противник не разбирает речевые сообщения. Но работа аппаратуры радиоразведки не всегда ведется в подпороговой области. Могут сложиться и такие условия, когда уровень сигнала в радиоканале утечки информации превышает пороговый и оператор средств радиоперехвата разбирает речевые сообщения с приемлемым качеством. Чтобы сформулировать нормативы контроля обеспечения защищенности, нужно определить эти пороговые уровни сигналов в каналах утечки на входе устройства радиоперехвата информации.

Поскольку речь идет об исследовании сигналов в радиоканале утечки информации, соответствующих сигналам на пороге акустической разборчивости речи, необходимо отметить следующее. Известны условия [1], при выполнении которых возможно качественное выделение речевого сообщения. Это, прежде всего, ограничение нижнего значения отношения сигнал/шум в полосе приемника, при котором обеспечивается достаточная разборчивость речевого сообщения на

выходе – в акустическом канале. Однако, значение пороговых сигналов, при которых возможно выделение речевого сообщения с достаточным качеством, обычно не исследуется в интересах оценки качества систем связи. Все оценки качества передачи производятся, в основном, для области больших значений отношения 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.

Для телефонных каналов в соответствии с принятым стандартом спектр речи ограничивается полосой от $f_н$=300 Гц до $f_в$=3,4 кГц. [2].

При этих условиях требуемая скорость передачи речи $R_k=2f_в \cdot n>2\ f_в$=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 [2] R=25 бит/с. Поэтому при передаче речи по каналам связи эту избыточность стремятся сократить, т.е. осуществить сжатие речевой информации. Наиболее радикальное сжатие достигается с помощью вокодеров, которые вычисляют некоторые представительные параметры речевого сигнала. Информативность представительных параметров речи существенно ниже, чем исходного речевого сигнала. За счет этого осуществляется сжатие речевой информации. При этом исследования [2] и [3] показывают, что в вокодерах всех типов узнаваемость голосов и натуральность звучания речи недостаточно высоки. В тех случаях, когда не требуется осуществлять эффективное кодирование, качество звучания речи и узнаваемость голосов в акустическом канале приемника абонента могут быть улучшены, если передавать не преобразованную вокодером речь.

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. При кодово-импульсной манипуляции (КИМ) речевой сигнал U(t), подлежащий передаче, подвергается дискретизации через интервалы $\Delta t_д = \frac{1}{f_д}$, где $f_д$ – частота дискретизации. Полученные при этом амплитудно-модулированные импульсы квантуются по амплитуде (измеряются с точностью, соответствующей шагу квантования δ). Затем это число преобразуется в n-значный двоичный код $x(t) \in 0;1$. Максимальное число, которое может быть записано в системе счисления с основанием 2 и числом символов n, равно 2^n-1. На приемном конце после демодуляции и декодирования

формируется последовательность импульсов, следующих с частотой $f_{д}$ и имеющих амплитуду $U_{кв.i}=i\cdot\delta$, (i – целое число). Эта последовательность пропускается через фильтр нижних частот, на выходе которого получается восстановленный речевой сигнал.

Ниже для определения порогового соотношения сигнал/шум на входе разведывательного приемника считается, что синтезирующий фильтр имеет нулевое затухание в полосе речевого сообщения и бесконечно большое – вне этой полосы. При передаче двуполярных сигналов с симметричным распределением мгновенных значений, например, речевых, i=0, 1, 2, ..., $2^{n-1}-1$;

$\delta=\frac{U_{огр}}{2^{n-1}-1}$ (для изображения отрицательных двоичных чисел нужно использовать дополнительный символ знака числа). Наибольшее значение амплитуды восстановленного речевого сигнала или напряжения ограничения на передающем конце $U_{огр}$ принимают обычно равным максимальной амплитуде U_{max} передаваемого речевого сигнала. При этом шумы, вызываемые ограничением по амплитуде, отсутствуют. Однако и в том случае, когда U_{max} оказывается несколько больше, чем $U_{огр}$, возникающие нелинейные искажения создают шумы, мощность которых незначительна по сравнению с шумами, вызванными квантованием по амплитуде. Интервалы дискретизации в соответствии с теоремой В.А. Котельникова $\Delta t_{д}\le\frac{1}{2f_{в}}$. В принципе нет необходимости дискретизировать речевой сигнал через более короткие интервалы, чем $\frac{1}{2f_{в}}$, так как точность передачи при этом не повышается. Однако из-за неидеальности характеристик фильтров, сглаживающих выборки после цифро-аналоговых преобразований речевых сигналов на приемной стороне, выбирают $\Delta t_{д}=\frac{1}{2{,}3f_{в}}$ [2].

Количество информации на выходе декодера L_3 определяется в соответствии с [3]:

$$L_3=\left[B(f_{в})-B(f_{н})\right]k_{п.и}\quad,\qquad(1)$$

где L_3 – количество информации на выходе декодера при отсутствии помех; $f_н$, $f_в$ – соответственно нижняя и верхняя граничная частота в спектре передаваемого речевого сигнала; $B(f_в)-B(f_н)$ – относительное количество информации в полосе $\Delta f_р=f_в-f_н$:

$$B(f)=\begin{cases}0{,}4f^{0,4}+0{,}005(f-1)(10-f); & 1\ \text{êÃö}\le f\le 10\ \text{êÃö}\\ 0{,}4f^{2}; & 0\ \text{êÃö}\le f\le 1\ \text{êÃö}\end{cases},$$

$k_{п.и}$ – коэффициент потери информации при дискретизации речевого сигнала по уровню (квантования).

Оценивая шумы при равномерном шаге квантования, будем считать, что к полезному сигналу и амплитудно-модулированным импульсам добавляется ошибка $U \le \frac{\delta}{2}$, имеющая равновероятное распределение мгновенных значений. Соответственно средняя мощность шумов квантования:

$$\overline{P}_{ø.êâ.} = \frac{1}{\delta}\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}} U^2 dU = \frac{\delta^2}{12}. \qquad (2)$$

Мощность полезного сигнала в этом случае для i-ого уровня квантования $P_{c.êâ.i}$ может быть оценена соотношением:

$$P_{ñ.êâ.i} = \left(U_{êâ.i} - \frac{\delta}{2}\right)^2 = \left(\frac{\delta^2}{4}\right)(2i-1)^2, \qquad (3)$$

где $U_{êâ.i} = i\delta$, i=0, 1, 2, ..., 2^{n-1}-1; δ – шаг квантования; $U_{кв.i}$ – уровень квантования с номером i.

Из (2) видно, что мощность шумов квантования не зависит от мощности передаваемого сигнала, и, следовательно, отношение полезного сигнала к шуму квантования изменяется при изменении амплитуды сигнала $U_{кв.i}$:

$$q_{êâ.i} = 10\lg\left(\frac{P_{ñ.êâ.i}}{\overline{P}_{ø.êâ.}}\right) = 10\lg 3 + 20\lg(2i-1). \qquad (4)$$

В [1], [2] и [3] показано, что усредненное соотношение сигнал/шум квантования в децибелах определяется соотношениями:

– для речевого сигнала с нормальным законом распределения вероятностей мгновенных значений, которым аппроксимируется распределение группового телефонного сигнала:

$$\overline{q}_{êâ} = 10\lg 3 + 20\lg(2^n - 3) - 20\lg 4. \qquad (5)$$

– для речевого сигнала с экспоненциальным законом распределения (аппроксимация распределения речевого сигнала):

$$\overline{q}_{êâ} = 10\lg 3 + 20\lg(2^n - 3) - 20\lg 5. \qquad (6)$$

Соотношения (4)…(6) иллюстрируют тот очевидный факт, что при равномерном шаге квантования (δ=const) сигналы с большой амплитудой передаются со значительно большей точностью, чем слабые. Для речевых сигналов это приводит к тому, что в процессе прямого преобразования больше всего искажаются согласные звуки (обладающие наибольшей информативностью), а ударные гласные практически не искажаются.

Поэтому при передаче речи используют неравномерную шкалу квантования. Наибольший интерес представляет логарифмический закон квантования, позволяющий получить одно и то же соотношение сигнал/шум квантования при любом законе распределения мгновенных значений

речевого сигнала и при изменении амплитуды сигнала в пределах всего динамического диапазона. Обычно процесс нелинейного квантования представляют состоящим из двух частей. Входной речевой сигнал вначале компрессируют по заданному закону, а затем квантуют с равномерным шагом квантования. Компрессирование по простому логарифмическому закону $U_{вых}=\lg U_{вх}$ нецелесообразно, так как напряжению $U_{вх}<1$ соответствует $U_{вых}<0$. Такое изменение полярности сигнала недопустимо. Поэтому обычно используют модифицированный логарифмический закон:

$$U_{âûõ}=\frac{\ln\left(1+\mu\left|U_{âõ}\right|\right)}{\ln\left(1+\mu\right)}\operatorname{sign}U_{âõ}, \tag{7}$$

или при нормированном входном напряжении:

$$U_{âûõ}=\frac{\ln\left(1+\mu\dfrac{\left|U_{âõ}\right|}{U_{max}}\right)}{\ln\left(1+\mu\right)}\operatorname{sign}U_{âõ}, \tag{8}$$

где μ – параметр характеристики (степень компрессии);

$$\operatorname{sign}U_{âõ}=\begin{cases}1; & U_{âõ}>0\\ 0; & U_{âõ}=0\\ -1; & U_{âõ}<0\end{cases}.$$

В системах связи нашло широкое применение логарифмическое компандирование, включающее в себя компрессирование на передающей стороне и экспандирование – на приемной. При этом используются различные методы получения логарифмической шкалы квантования. Если вместо натуральных логарифмов в (8) использовать десятичные, то:

$$U_{âûõ}=20\lg\left(1+\mu\frac{\left|U_{âõ}\right|}{U_{max}}\right)\operatorname{sign}U_{âõ}, \tag{9}$$

где $U_{вых}$ – ненормированное выходное напряжение.

Известно [1] и [3], что соотношение сигнал/шум квантования определяется выражением:

$$q_{êâ.i}=20\lg\frac{U_{âõ.ñõ.i}}{U_{ø.ñõ.i}}=20\lg\left[\frac{2\left(U_{âõ.êâ.i}+U_{âõ.êâ.i-1}\right)}{2\left(U_{âõ.êâ.i}-U_{âõ.êâ.i-1}\right)}\right]=20\lg\left(\frac{x+1}{x-1}\right)=\text{const}\left(i\right), \tag{10}$$

где $q_{кв.i}$ – соотношение сигнал/шум для i-го уровня квантования; $x=10^{\left(\frac{\delta}{20}\right)}=\text{const}\left(i\right)$; δ – шаг квантования:

$$\delta=U_{âûõ.êâ.i}-U_{âûõ.êâ.i-1}=\text{const}=20\left[\lg\left(1+\mu\frac{U_{âõ.êâ.i}}{U_{max}}\right)-\lg\left(1+\mu\frac{U_{âõ.êâ.i-1}}{U_{max}}\right)\right]=20\frac{\lg\left(1+\mu\right)}{2^{n-1}-1}. \tag{11}$$

Из (10) и (11) следует, что для КИМ с логарифмической шкалой квантования соотношение сигнал/шум $q_{кв.i}$ одинаково при любой амплитуде сигнала $U_{âõ}(t)$ и не зависит от статистических свойств речевого сигнала:

$$q_{êâ}(i=1)=q_{êâ}(i=2)=...=q_{êâ}\left(i=2^{n-1}-1\right). \quad (12)$$

Зависимость коэффициента потери информации $k_{ï.è.}$ от соотношения сигнал/шум квантования $q_{кв}$ приведена [1] и имеет вид:

$$k_{ï.è.}=\begin{cases}0{,}12\exp\left(\dfrac{q_{êâ}}{7}\right); & q_{êâ}\le 5\ äÁ\\ 1-3{,}376\left(q_{êâ}+15\right)^{-0{,}5}\exp\left\{-\dfrac{\left(q_{êâ}-5\right)^2}{250}\right\}; & q_{êâ}>5\ äÁ\end{cases}. \quad (13)$$

Значение соотношения сигнал/шум квантования $q_{кв}$ подставляется в (13) в децибелах.

Разборчивость речи на выходе – в акустическом канале приемника перехвата определяется [1]:

$$W=0{,}2\left[1-0{,}004^{L_3k_{ï.è}}\right]^4+0{,}8\left[1-0{,}004^{L_3k_{ï.è}}\right]^3, \quad (14)$$

где W – разборчивость речи (слогов) при воздействии помех; $k_{о.к}$– 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 [2] показано, что коэффициент разборчивости речи при наличии помех в канале связи $k_{о.к}$ определяется соотношением:

$$k_{o.k}=1+\gamma P_{îø}\log_2\left(\gamma P_{îø}\right)+\left(1-\gamma P_{îø}\right)\log_2\left(1-\gamma P_{îø}\right), \quad (15)$$

где $P_{ош}$ – вероятность ошибки при приеме отдельного символа кодовой комбинации; γ – коэффициент, учитывающий порядковый номер символа в кодовой комбинации (при кодово-импульсной манипуляции 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:

$$\gamma=\frac{2}{\left(1+P_{îø}\right)}\left[1-\left(\frac{1-P_{îø}}{2}\right)^n\right]; \quad (16)$$

– для КИМ с линейной шкалой квантования:

$$\gamma=\frac{2\left(2^n-1\right)}{2^n}. \qquad (17)$$

Подставляя (1) и (13) в (14), можно построить диаграммы обмена между разборчивостью речи и вероятностью ошибочного приема двоичного символа. Эти диаграммы в координатах $W–P_{ош}$ представлены на рис.1.

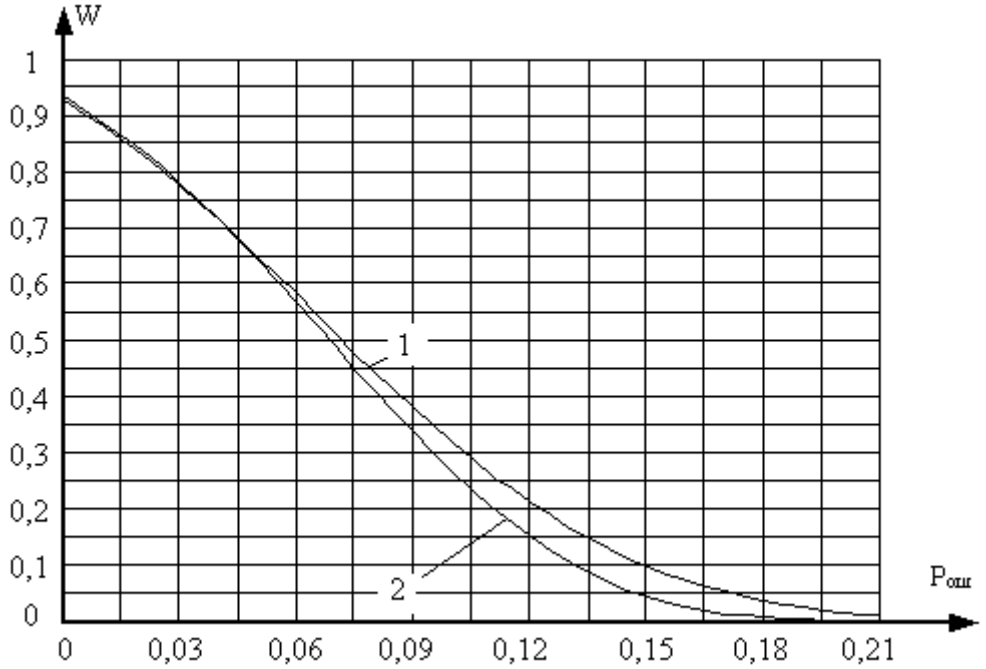

Рис.1. Диаграммы обмена между разборчивостью речи и вероятностью ошибочного приема символа кодовой комбинации (кривые 1 и 2 – широкополосный канал связи).

Кривая 1 вычислена для КИМ с логарифмической шкалой квантования при $\mu=255$. 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.

Используя (14), для пороговой вероятности правильного узнавания слога W=0,2 [1], получаем:

$$k_{o.k}\left(n,\ P_{îø}\right) L_3\left(n\right)=0{,}16651. \qquad (18)$$

Подставляя в (18) соотношения (1) и (13), можно найти пороговое значение вероятности ошибочного приема двоичного символа кодовой комбинации, при которой уже не обеспечивается разборчивость речи. Диаграммы обмена между граничной вероятностью ошибочного приема символа и значностью двоичного безызбыточного кода представлены на рис.2.

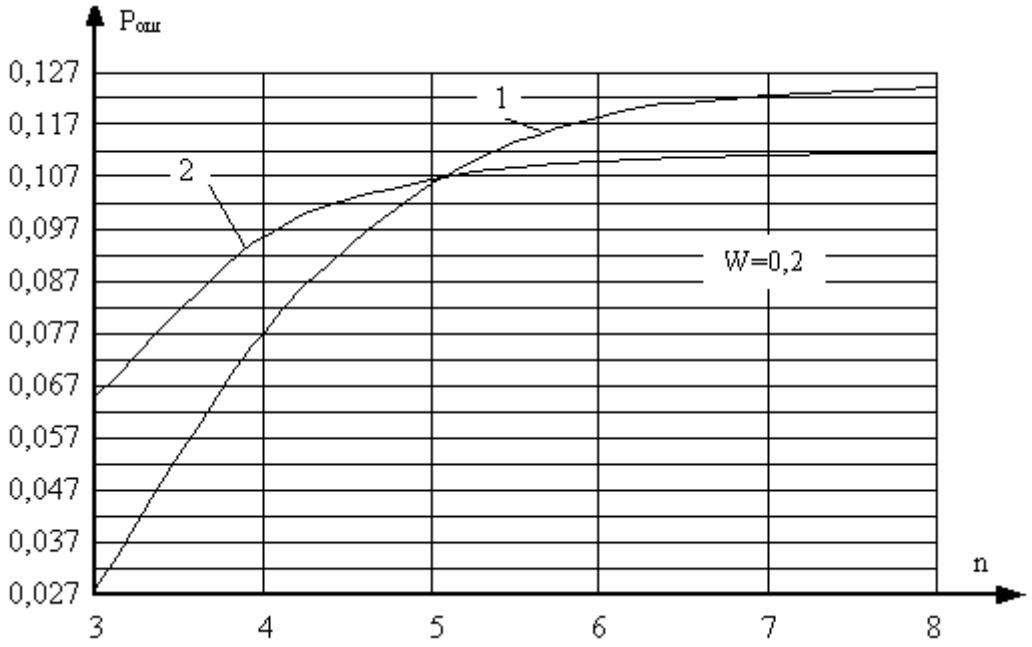

Рис.2. Пороговая вероятность ошибочного приема двоичного символа кодовой комбинации.

Таким образом, по диаграммам на рис. 2 можно определить пороговую вероятность ошибочного приема двоичного символа кодовой комбинации (для непосредственного преобразования речевых сигналов), при которой оператор средств радиоразведки не разбирает сообщения.

В [4] показано, что вероятность ошибки при когерентном приеме отдельного двоичного символа кодовой комбинации определяется соотношениями:

$$Р_{ iø} = 1-Ô\left(\sqrt{\frac{\theta}{N_0}}\right) = 1-Ô\left(\sqrt{\frac{4P_c}{Р_ø}}\right); \qquad (19)$$

– для КИМ-ЧМн (частотная манипуляция) и

$$Р_{ iø} = 1-\left\{1-2\left[1-Ô\left(\sqrt{\frac{2\theta}{N_0}\sin^2\frac{\pi}{2^k}}\right)\right]Ô\left(\sqrt{\frac{2\theta}{N_0}\sin^2\frac{\pi}{2^k}}\right)\right\}^{\frac{1}{k}}, \qquad (20)$$

– для k-кратной ФРМ первого порядка.

В (19) и (20) обозначено: k– кратность манипуляции ($Y=2^k$ – число вариантов фаз, используемых при k-кратной манипуляции); $\frac{\theta}{N_0}=\frac{P_с\cdot\tau_k}{N_0}$; τ_k – 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 $\tau_k = k\cdot\tau_и$); $\tau_и$ – длительность двоичного символа.

– для однократной ФРМ g-ого порядка:

$$Р_{ош} = \frac{1}{2}\left\{1-\left[2Ф\left(\sqrt{\frac{2\theta}{N_0}}\right)-1\right]\right\}^{H(g)}, \qquad (21)$$

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

При Y=4, оптимальным является ансамбль ФМ-4 (четырехпозиционная ФМ), [4] и

$$Р_{ош} = 1-Ф\left(\sqrt{\frac{Р_п \tau_k}{N_0}}\right). \qquad (22)$$

При Y>4 наилучшей по помехоустойчивости является симметричная конфигурация с регулярным расположением сигнальных точек в узлах квадратной сети (QASK), [5]:

$$Р_{ош} = 1-\left\{1-4\left(1-\frac{1}{\sqrt{Y}}\right)\left[1-Ф\left(\sqrt{\frac{3Р_п \tau_k}{2N_0(Y-1)}}\right)\right]Ф\left(\sqrt{\frac{3Р_п \tau_k}{2N_0(Y-1)}}\right)\right\}^{\frac{1}{k}}, \qquad (23)$$

где k– кратность манипуляции.

Используя (19)...(23), можно пересчитать обменные диаграммы на рис.2 ко входу приемника в техническом канале утечки информации. Эти диаграммы в координатах $q_{вх}$–n представлены на рис. 3 для определенной выше пороговой вероятности правильного узнавания слога W=0,2.

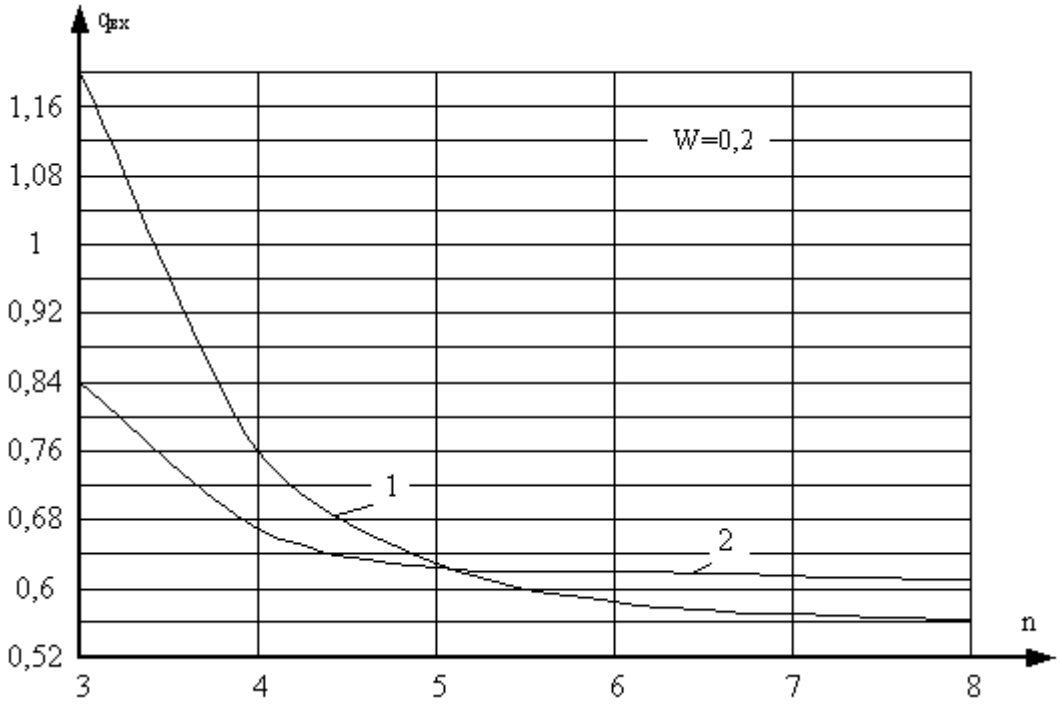

Рис.3. Диаграммы для определения порогового соотношения сигнал/шум в полосе приемника радиоразведки.

Из рис. 2 и 3 видно, что чем выше требования к достоверности передачи речевого сообщения, представляемого в цифровой форме (то есть чем меньше шаг квантования), в основном канале защищаемой системы, тем меньше пороговое соотношение сигнал/шум в канале утечки. С увеличением числа безызбыточных символов, образующих кодовую комбинацию, пороговое

соотношение сигнал/шум уменьшается и на характер этой зависимости не влияет способ цифрового преобразования речевых сигналов.

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 РЭС 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 (например, за счет применения имитирующих помех).

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.

СПИСОК ЛИТЕРАТУРЫ

1. Калинцев Ю. К. Разборчивость речи в цифровых вокодерах. – М.: Радио и связь ,1994.-260с.
2. Покровский Н. Б. Расчет и измерение разборчивости речи. – М.: Связьиздат,1962.-415с.
3. Сапожков М. А. Вокодерная связь. – М.: Радио и связь,1983.-248с.
4. Окунев Ю. Б. Цифровая передача информации фазомодулированными сигналами. – М.: Радио и связь,1991.-296с.
5. Кловский Д. Д. Передача дискретных сообщений по радиоканалам. – М.: Радио и связь,1982.-304с.

СВЕДЕНИЯ ОБ АВТОРЕ

Большов Олег Анатольевич, доцент кафедры радиосистем передачи информации и управления Московского авиационного института (государственного технического университета), к.т.н.