УДК:681.327.12:534.782+621.376.57

Пороговые сигналы при предельном ограничении речи

О.А.Большов

Аннотация

В статье рассмотрена проблема оценки защищенности речевого сообщения от несанкционированного доступа (перехвата) и определены некоторые условия, при выполнении которых обеспечивается достаточная защищенность речевой информации.

Ключевые слова

Пороговые сигналы; защита информации.

Информационное обеспечение является основой любой деятельности людей, а информация становится одним из важных средств решения проблем различных государственных и коммерческих структур, отдельных людей. При этом ценная конфиденциальная информация обладает качествами товара, поэтому она может добываться и в целях последующей продажи заинтересованными лицами и организациям.

Повышенный интерес в получении речевой информации объясняется следующими ее свойствами:

–особый уровень конфиденциальности – очень часто устно делаются такие сообщения (распоряжения), которые не могут быть доверены другому носителю;

–оперативность приема – речевая информация может быть перехвачена (и соответственно использована) в момент ее сообщения;

–высокий уровень индентифицируемости – перехваченная речевая информация является по существу документом с личной подписью того человека, который озвучил сообщение;

–наличие эмоционального оттенка – позволяет сделать заключение о личном отношении говорящего к сообщению.

Эти особые свойства речевых сообщений очень часть вызывают интерес у преступных сообществ и недобросовестных конкурентов. Обычно это относится к информации, которая позволяет конкурентам заключить выгодный для себя контракт или воспользоваться результатами чужого труда, не вкладывая средств в проведение собственных исследований или приобретение этих результатов законным путем. Таким образом, можно утверждать, что защита конфиденциальной информации вообще, а речевой особенно, это «краеугольное» начало благосостояния как личности, так и любого учреждения.

Для незаконного добывания информации в общем случае используются различные методы. Особое место среди них занимает съем информации с помощью намеренно внедренных в помещение и подключенных к средствам обработки информации или каналам связи устройств для негласного съема информации. В общем виде под несанкционированным съемом информации (НСИ) понимается незаконное получение конфиденциальной информации, в том числе и с использованием различных технических средств.

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.

Одним из самых надежных способов защиты информации в цифровых системах речевой связи считается шифрация. Однако криптозащита цифровых сигналов в силу многих причин не универсальна. Другие, альтернативные способы обеспечения информационной безопасности передачи данных могут использовать активную и/или пассивную радиомаскировку. Выбор конкретных мер определяется из условий обеспечения пороговых радиосигналов, при которых информация в каналах утечки может быть восстановлена лишь на нижнем пределе достоверности.

Кроме того, может оказаться, что типичные, штатные условия эксплуатации радиосистемы не требуют защиты от технических средств ведения разведки. (То есть уровень сигнала, наблюдаемого на фоне собственных шумов приемника радиоразведки, не превышает некоторой пороговой величины, и разведчик не разбирает речевые сообщения). А это означает, что несанкционированный прием ведется в подпороговой области. Но такие ситуации не являются единственно возможными. Могут сложиться и такие условия, что уровень перехваченного излучения превышает пороговый и противник получает доступ к речевым сообщениям. Для того, чтобы установить в какой области реально работает средство радиоперехвата – в надпороговой или подпороговой нужно иметь некоторые нормативные показатели защищенности информации. При этом для разработки этих норм необходимо знать и уметь измерять пороговые сигналы на входе устройства перехвата информации, при которых оператор разбирает речевые сообщения слабо, на пределе возможного.

Актуальность исследования пороговых свойств сигналов в радиотехнических каналах утечки информации можно подтвердить следующим. Известны условия [1], [2] накладываемые на минимально допустимые соотношения сигнал/шум в полосе приемника абонента, при которых законный получатель с вероятностью, близкой к единице, правильно разбирает элементы (звуки, слога, слова) речевого сигнала. Отличительной чертой канала утечки информации является слабый сигнал, где работает аппаратура несанкционированного доступа к речевым сообщениям. И для защиты речевой информации требуется знать не условия оптимальной работы аппаратуры, а условия обеспечения неразборчивости на выходе технического канала утечки.

Количественно пороговый эффект характеризуется вероятностью правильного узнавания слога оператором средств радиоразведки. До тех пор пока эта вероятность не превышает пороговой величины, считается, что имеет место неудовлетворительная разборчивость и оператор средств перехвата не разбирает речевые сообщения. Эта пороговая вероятность должна быть взята из границ общепринятых классов качества речи по разборчивости, которые были установлены на основании статистики восприятия речи различными операторами.

Будем считать, что приемники средств радиоперехвата идентичны абонентским приемникам защищаемой системы. Полученные при таких условиях оценки качества воспроизведения речевого сигнала оказываются верхними, пессимистическими для системы противодействия: реальный приемник средства разведки может работать только хуже

идеального (то есть средства разведки, использующего для несанкционированного доступа к информации всю энергию и все априорные сведения о сигнале).

Для телефонных каналов в соответствии с принятым стандартом спектр речи ограничивается полосой от $f_{\text{Н}} = 300$ Гц до $f_{\text{В}} = 3{,}4$ кГц. [2].

При этих условиях требуемая скорость передачи речи $R = 2 f_{\text{В}} \cdot n > 2 f_{\text{В}} = 6{,}8$ 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 [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 [7] 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. 1.

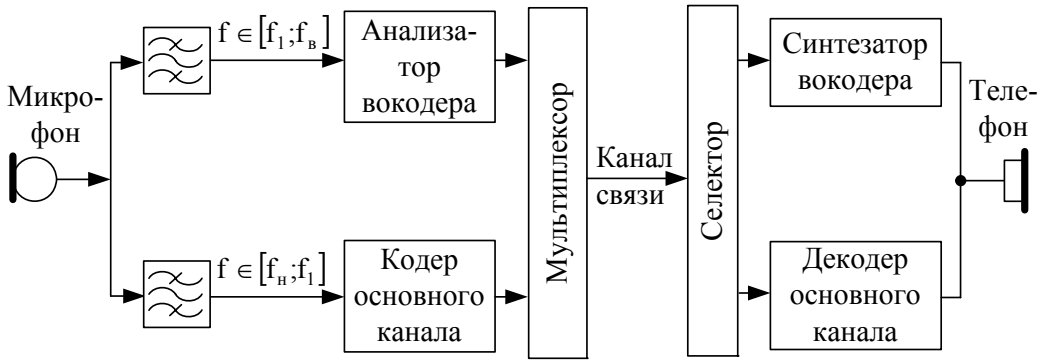

Рис. 1. Структурная схема полувокодера.

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.

При кодово-импульсной манипуляции (КИМ) речевой сигнал, подлежащий передаче, подвергается дискретизации через интервалы $\Delta t_{\text{Д}} = 1/f_{\text{Д}}$, где $f_{\text{Д}}$ – 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 $f_{\text{Д}}$ и имеющих амплитуду $U_{\text{КВ.i}} = i \cdot \delta \,\text{U}$, ($i$ – целое число). Эта последовательность пропускается через фильтр нижних частот, на выходе которого получается восстановленный речевой сигнал.

При использовании однозначного кода $(n = 1)$ КИМ эквивалентна предельному ограничению речевых сигналов с квантованием переходов через нуль по времени. Имеется в виду, что моменты переходов сигнала через нуль сдвигаются по оси времени на место ближайшего следующего импульса частоты квантования $f_{\text{КВ}} \geq f_{\text{Т}}$, где $f_{\text{Т}}$ - тактовая частота следования импульсов в канале связи (при КИМ $f_{\text{Т}} = nf_{\text{Д}}$).

На основании анализа многочисленных экспериментальных данных, полученных различными авторами [3], [5], можно сделать вывод о том, что ухудшение разборчивости речи происходит только при возникновении новой формантной области или исчезновении имеющейся. Если же под действием помех этого не происходит, то разборчивость речевого сообщения не снижается:

$$W = 0{,}2\left[1 - 0{,}004^{k_{\text{ОК}}L}\right]^4 + 0{,}8\left[1 - 0{,}004^{k_{\text{ОК}}L}\right]^3, \quad (1)$$

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

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

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); $k_{ОК}$ – коэффициент помехоустойчивости.

Для вычисления разборчивости слогов необходимо коэффициент потери информации $k_{П.И}$ умножить на относительное количество информации $B(\Delta f)$ в полосе $\Delta f_Р$ и, используя полученное значение

$$L = k_{П.И} B(\Delta f) \tag{3}$$

по формуле (2) определить искомую разборчивость слогов.

При квантовании разборчивость предельно ограниченных сигналов снижается. Обычно это снижение оценивают соотношением сигнал/шум квантования. Мощность помехи при этом вычисляют как мощность прямоугольных импульсов с постоянной единичной амплитудой и переменной длительностью $0 \le \tau \le 1/f_{КВ}$. Эти импульсы представляют собой разность между квантованным и неквантованным предельно ограниченным сигналом. Сигнал и частота квантования взаимонезависимы, поэтому распределение длительности импульсных помех равновероятное и $\tau_{СР} = 1/2 f_{КВ}$. Отношение сигнал/шум в децибелах в этом случае определяется как [2]:

$$R_{КВ} = 20\lg f_{КВ} - 10\lg f_{СР} - 10\lg(0{,}166\Delta f_Р + 0{,}5 f_{СР}), \tag{4}$$

где $\Delta f_Р$ - ширина полосы речевого сигнала: $f_{СР}$ - средневзвешенная частота в спектре сигнала на входе предельного ограничителя.

При предельном ограничении синусоидального сигнала

$$R_{КВ} = 20\lg\left(f_{КВ}/f_{СР} - 1{,}5\right) - 0{,}26\left(f_В/f_{СР}\right) - 2{,}6. \tag{5}$$

Если в этой формуле, как и в (4) принять, что $f_{КВ}/f_{СР} >> 1{,}5$, то обе формулы приводятся к виду:

$$R_{КВ} = 20\lg(f_{КВ}) - \alpha, \tag{6}$$

где α - постоянное слагаемое.

Для полосы стандартного канала тональной частоты 300…3400Гц при использовании идеального микрофона средневзвешенная частота, соответствующая нормированному спектру речи $f_{СР} = 800$ Гц [7]. При этом из (4) $\alpha_1 = 58{,}6$ дБ, а из(5) $\alpha_2 = 65{,}4$ дБ.

Соотношение сигнал/шум при предельном ограничении и квантовании определяется, очевидно, как [8]:

$$R_{\text{П.О}} = R_{\text{ПР}} + R_{\text{КВ}} - 10\lg\left(10^{0,1R_{\text{ПР}}} + 10^{0,1R_{\text{КВ}}}\right). \quad (7)$$

Эта формула получена в предположении, что мощность помех, возникающих при предельном ограничении, и шумы квантования аддитивны (то есть их можно суммировать), а мощность сигналов при предельном ограничении и квантовании одинаковы.

Зависимость коэффициента потери информации $k_{\text{ПИ}}$ от соотношения сигнал/шум $R_{\text{П.О}}$ приведена [1] и имеет вид:

$$k_{\text{ПИ}} = \begin{cases} 0,12\exp\left(\dfrac{R_{\text{П.О}}}{7}\right); & R_{\text{П.О}} \le 5\,\text{дБ} \\ 1 - 3,376\left(R_{\text{П.О}} + 15\right)^{-0,5}\exp\left\{-\dfrac{\left(R_{\text{П.О}} - 5\right)^2}{250}\right\}; & R_{\text{П.О}} > 5\,\text{дБ} \end{cases} \quad (8)$$

Значение соотношения сигнал/шум при предельном ограничении и квантовании $R_{\text{П.О}}$ подставляется в (8) в децибелах.

Относительное количество информации $B(\Delta f)$ в спектре речевого сигнала передаваемого определяется в соответствии с [8]:

$$B(\Delta f) = B(f_{\text{В}}) - B(f_{\text{Н}}), \quad (9)$$

где $f_{\text{Н}}$, $f_{\text{В}}$ – соответственно нижняя и верхняя граничная частота в спектре передаваемого речевого сигнала; $B(f_{\text{В}}) - B(f_{\text{Н}})$ – относительное количество информации в полосе $\Delta f_{\text{Р}} = f_{\text{В}} - f_{\text{Н}}$:

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

Подставляя (3) и (10) в (2), можно построить диаграммы обмена между разборчивостью речи и частотой квантования. Эти диаграммы в координатах $A - f_{\text{КВ}}$ представлены на рис.2.

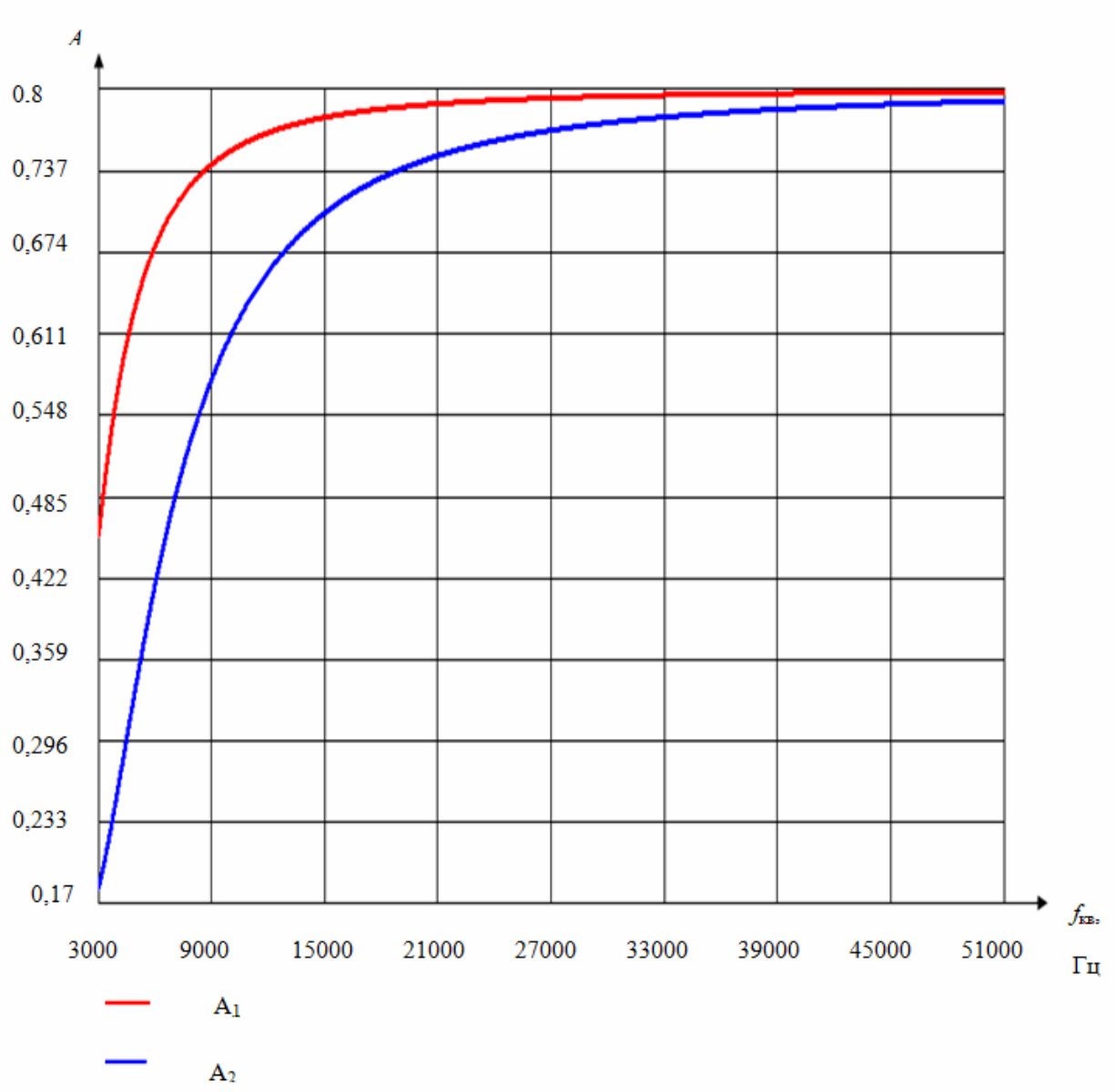

Рис.2. Диаграммы обмена между разборчивостью речи и частотой квантования (кривые 1 и 2 – широкополосный канал связи).

На рис.2 показаны зависимости A от частоты квантования для речевых сигналов в полосе 300…3400 Гц; вычисленные при $R_{\text{ПР}} = 18$ дБ, соответствующих (4) – кривая 1 и (5)– кривая 2.

В [2] и [5] показано, что коэффициент разборчивости речи при наличии помех в канале связи $k_{\text{ОК}}$ определяется соотношением:

$$k_{\text{ОК}} = 1 + \gamma P_{\text{ОШ}} \log_2(\gamma P_{\text{ОШ}}) + (1 - \gamma P_{\text{ОШ}}) \log_2(1 - \gamma P_{\text{ОШ}}), \qquad (11)$$

где $P_{\text{ОШ}}$ – вероятность ошибки при приеме отдельного символа кодовой комбинации; γ – весовой коэффициент, определяемый экспериментально (для предельного ограничения без кодирования $\gamma = 1$ [2]).

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

$$k_{ОК}(P_{ОШ})L(f_{КВ}) = 0{,}16651. \qquad (12)$$

Подставляя в (12) соотношения (3) и (11), 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 частоты квантования представлены на рис.3.

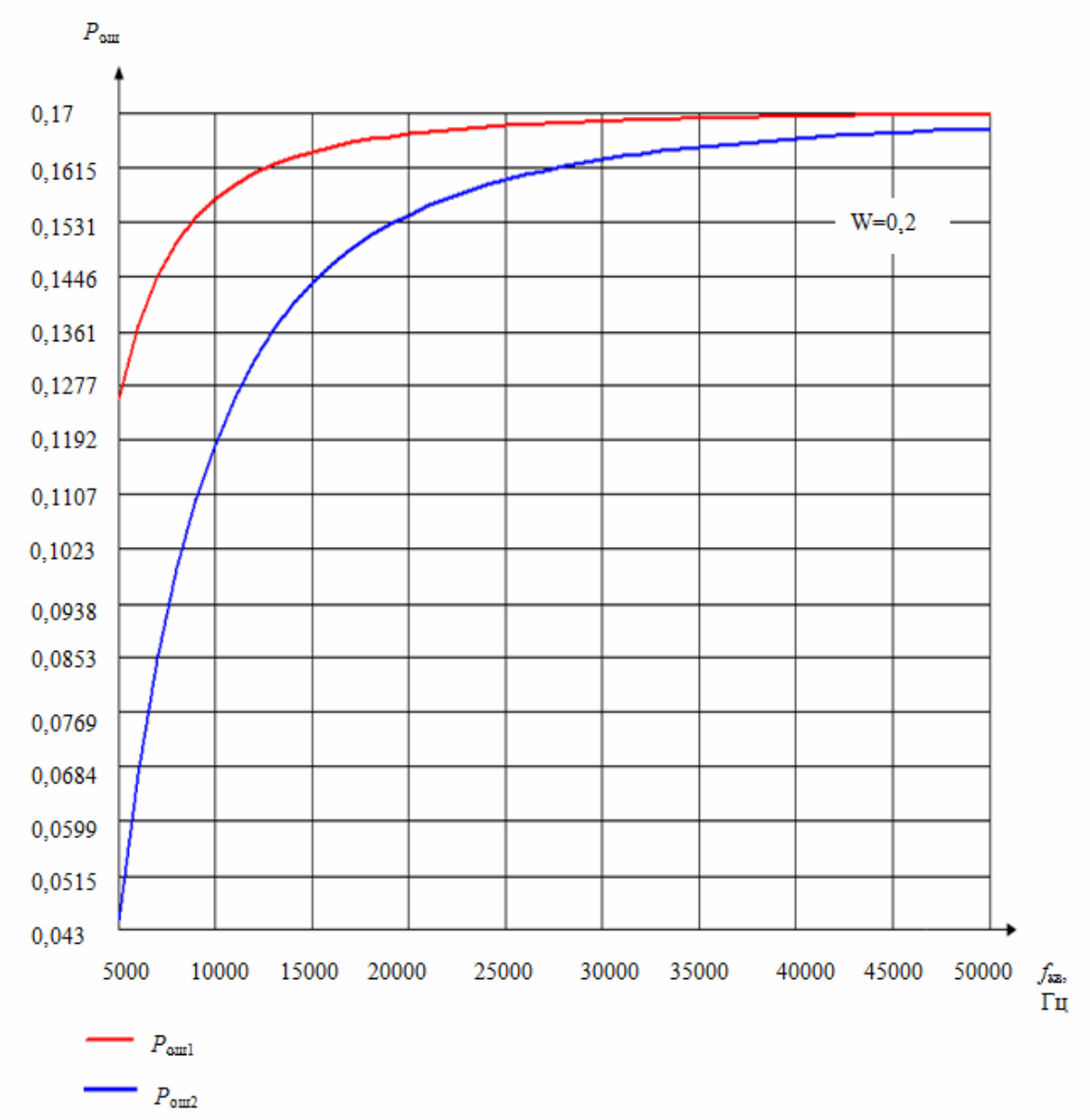

Рис.3. Пороговая вероятность ошибочного приема двоичного символа кодовой комбинации.

В [4] и [6] показано, что вероятность ошибки при когерентном приеме отдельного двоичного символа кодовой комбинации определяется соотношениями:

$$P_{\text{ОШ}} = 1 - \Phi\left[\sqrt{\frac{Q}{N_{\text{О}}}}\right]; \tag{13}$$

– для КИМ-ЧМн (частотная манипуляция) и

$$P_{\text{ОШ}} = 1 - \left\{1 - 2\left[1 - \Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}}\sin^2\frac{\pi}{2^K}\right)\right]\Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}\sin^2\frac{\pi}{2^K}}\right)\right\}^{\frac{1}{K}}, \tag{14}$$

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

В (13) и (14) 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

$$P_{\text{ОШ}} = \frac{1}{2}\left\{1 - \left[2\Phi\left(\sqrt{\frac{2Q}{N_{\text{О}}}}\right) - 1\right]\right\}^{H(g)}, \tag{15}$$

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), [9] и

$$P_{\text{ОШ}} = 1 - \Phi\left(\sqrt{\frac{P_{\text{С}}\tau_{\text{К}}}{N_{\text{О}}}}\right). \tag{16}$$

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

$$P_{\text{ОШ}} = 1 - \left\{1 - 4\left(1 - \frac{1}{\sqrt{Y}}\right)\left[1 - \Phi\left(\frac{3P_{\text{С}}\tau_{\text{К}}}{2N_{\text{О}}(Y-1)}\right)\right]\Phi\left(\sqrt{\frac{3P_{\text{С}}\tau_{\text{К}}}{2N_{\text{О}}(Y-1)}}\right)\right\}^{\frac{1}{K}}, \tag{17}$$

где K – кратность манипуляции; $\Phi(\psi)$ – интегральная функция распределения нормальной случайной величины с нулевым средним значением и дисперсией, равной 1:

$$\Phi(\psi) = 1 - \Phi(-\psi) = 0{,}5 + \Phi_{O}(\psi) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\psi} \exp\left\{-\frac{x^2}{2}\right\} dx =$$

$$= 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\psi} \exp\left\{-\frac{x^2}{2}\right\} dx = 0{,}5 + \frac{1}{\sqrt{2\pi}} \int_{0}^{\psi} \exp\left\{-\frac{x^2}{2}\right\} dx. \quad (18)$$

Используя (13)...(18), можно пересчитать обменные диаграммы на рис.3 ко входу приемника в техническом канале утечки информации. Эти диаграммы в координатах $q_{\text{ВХ}} - f_{\text{КВ}}$ представлены на рис.4 для определенной выше пороговой вероятности правильного узнавания слога $W = 0{,}2$.

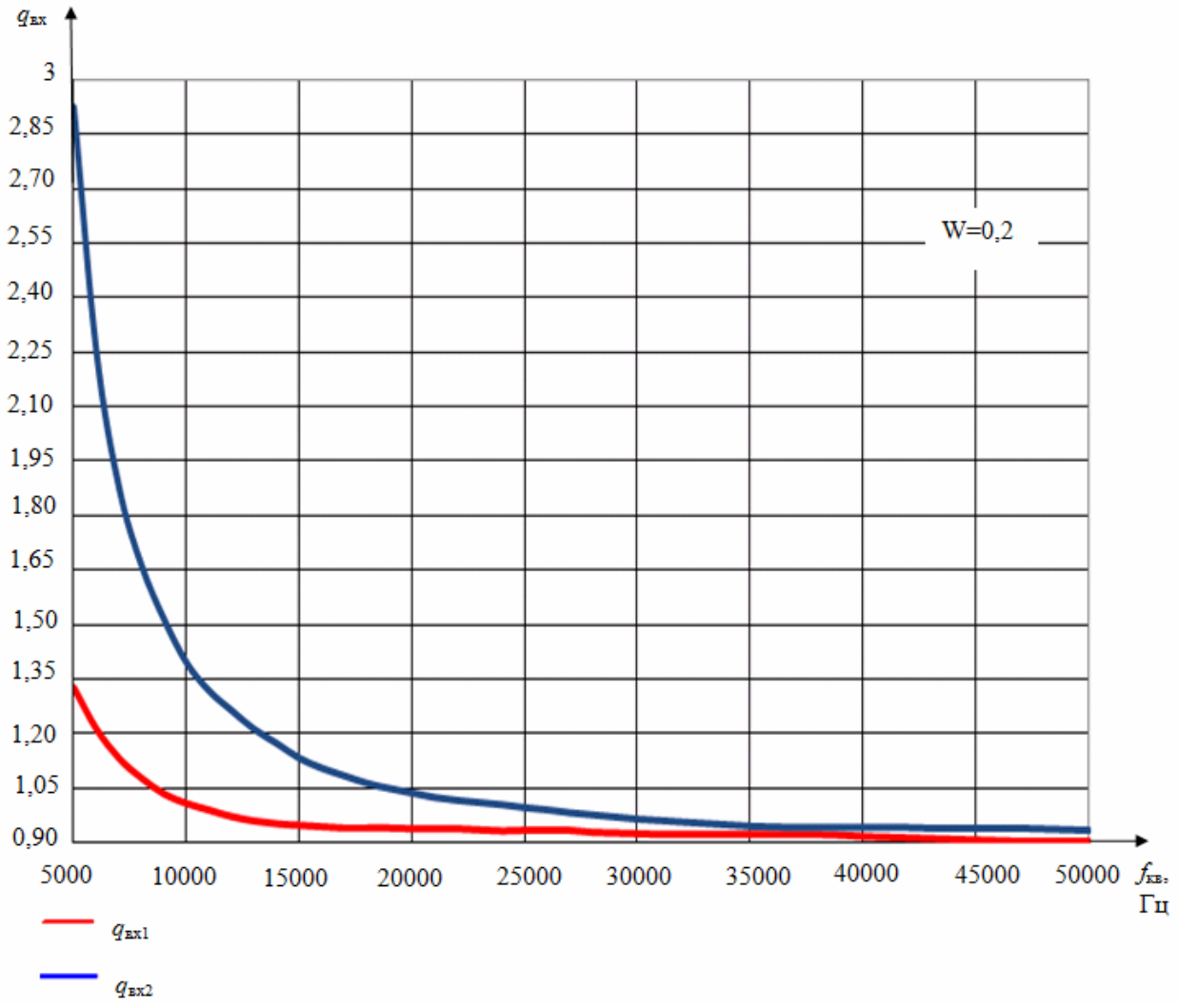

Рис.4. Диаграммы для определения порогового соотношения сигнал/шум в полосе приемника радиоразведки.

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. Калинцев Ю.К. Разборчивость речи в цифровых вокодерах. – М.: Радио и связь, 1991. – 220с.
3. Быков Ю.С. Теория разборчивости речи и повышение эффективности радиотелефонной связи. – М. – Л.: Госэнергоиздат, 1959. – 351с.
4. Окунев Ю.Б. Цифровая передача информации фазомодулированными сигналами. – М.: Радио и связь, 1991. – 297с.
5. Величкин А.И. Передача аналоговых сообщений по цифровым каналам связи. – М.: Радио и связь, 1983. – 240с.
6. Барсуков В.С. Новая информационная технология: искусственный интеллект, концепция банка знаний, экспертные системы. – М.: Знание, 1989. – 187с.
7. Михайлов В.Г. Измерение параметров речи. – М.: Радио и связь, 1987. – 168с.
8. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384с.
9. Кулешов А.П. Протоколы информационно-вычислительных сетей. – М.: Радио и связь, 1990. – 504с.

Сведения об авторе

Большов Олег Анатольевич, доцент Московского авиационного института (государственного технического университета), к.т.н., телефон: 8 (499) 158 – 49 – 33 .