УДК:681.327.12:534.782+621.376.57

ПОРОГОВЫЕ СИГНАЛЫ В КАНАЛАХ ПЕРЕДАЧИ И УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ С ПОМОЩЬЮ ШИРОКОПОЛОСНЫХ МОДЕМОВ

О.А.Большов, А.И.Куприянов

В статье рассмотрена проблема оценки защищенности речевого сообщения, передаваемого с помощью широкополосного модема, от несанкционированного приема и определены минимальные по мощности (пороговые) сигналы на входе приемника радиоперехвата, при которых уже не обеспечивается разборчивость речи.

Современные системы связи более половины всего объема информации, включая речь и потоки цифровых данных, передают по аналоговым телефонным сетям [1], используя модемы. 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. 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. Под защитой речевой информации от несанкционированного доступа (перехвата) понимается определение некоторых пороговых, минимальных по мощности сигналов на входе приемника радиоразведки, при которых оператор средства перехвата разбирает речевые сообщения слабо, на пределе возможного. Особенно важна и интересна такая оценка для систем связи, использующих модемы.

Формально задача оценки защищенности речевого сообщения, передаваемого с помощью модема, может быть поставлена следующим образом. В канале утечки информации (перехвата) действует сигнал $S(t)$ манипулированный функцией $x(t) \in 0;1$. Несущее колебание частоты f_0 формируется самим модемом. Посылающий модем выступает как генератор несущей. Средняя мощность сигнала на входе приемника средства разведки $P_с$, а мощность шума – $P_ш$. Так, что соот-

ношение сигнал/шум, приведенное ко входу приемника $q_{вх} = 10\lg\frac{P_c}{P_ш}$. Считается, что шум имеет равномерную спектральную плотность $N_0 = \frac{P_ш}{\Delta f}$ 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:

$$S(t)=a\,x(t)\cos 2\pi f_0 t + a[1-x(t)]\cos 2\pi f_1 t. \qquad (1)$$

Энергетический спектр КИМ-ЧМ по форме совпадает со спектрами двух одиночных видеоимпульсов, разнесенных на частоту $|f_0 - f_1| \geq \frac{2}{\tau_и}$, 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 ставится в соответствие не абсолютное значение фазы, а ее изменение относительно предыдущего значения:

$$S_1(t)=\begin{cases} a\cos(2\pi f_0 t); & 0 \leq t \leq \tau_и \\ a\cos[2\pi f_0 (t-\tau_и)]; & \tau_и \leq t \leq 2\tau_и \end{cases} \quad S_0(t)=\begin{cases} a\cos(2\pi f_0 t); & 0 \leq t \leq \tau_и \\ -a\cos[2\pi f_0 (t-\tau_и)]; & \tau_и \leq t \leq 2\tau_и \end{cases} \qquad (2)$$

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 $\Delta f \geq \frac{2}{\tau_и}$.

Непосредственное (в отличие от вокодерного) преобразование сигнала сводится к дискретизации и квантованию сигнала на передающей стороне и восстановлению посредством интерполирующего (синтезирующего) фильтра - на приемной. Ниже для вычисления соотношения сигнал/шум на приемной стороне считается, что синтезирующий фильтр имеет нулевое затухание в полосе речевого сообщения и бесконечно большое - вне этой полосы.

При исследовании свойств амплитудно-фазовой манипуляции (АФМ) широко используется геометрическая теория сигналов. Сигналы изображаются точками, которые являются концами двумерных векторов на плоскости. Процедура оптимизации расположения сигналов на дискрет-

ном регулярном множестве точек рассмотрена в [3], [4]. Результаты оптимизации сводятся к следующему. При M=4, где M – число вариантов сигнала на выходе модема, оптимальным является ансамбль ФМ-4 (четырехпозиционная ФМ). При M>4 оптимальными являются 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).

Считается также, что приемники средств разведки, 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 непосредственного воспроизведения речевого сигнала оказываются верхними, пессимистическими для системы противодействия: реальный приемник в канале перехвата не может работать лучше.

Шаг дискретизации речевого сигнала по времени при непосредственном преобразовании выбирают как $\Delta t_д = \frac{1}{2{,}3 f_в}$ [7].

Расчеты [1], [2] и [6] показывают, что количество информации на выходе декодера при отсутствии помех L определяется соотношением:

$$L=[B(f_в)-B(f_н)]k_{пи}, \qquad (3)$$

где B(f)-распределение исходной информации по всему частотному диапазону $f\in[0;\infty)$:

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

$f_н$ и $f_в$– соответственно нижняя и верхняя граничная частота в спектре передаваемого речевого сигнала, кГц; $B(f_н)$ - $B(f_в)$ – относительное количество информации в полосе $\Delta f_р=f_в-f_н$; $k_{пи}$ – коэффициент потери информации при квантовании речевого сигнала по уровню.

Вычисляя шумы при равномерном шаге квантования, можно считать, что к полезному сигналу и амплитудно-модулированным импульсам добавляется ошибка $U\le\delta/2$, имеющая равновероятное распределение амплитуд. Соответственно средняя мощность шумов квантования:

$$\overline{P}_{ш\ кв}=\frac{1}{\delta}\int_{-\frac{\delta}{2}}^{\frac{\delta}{2}}U^2dU=\frac{\delta^2}{12}. \qquad (5)$$

Мощность полезного квантованного сигнала в этом случаем для i-ого уровня квантования $P_{с\ кв\ i}$ может быть оценена соотношением:

$$P_{с\ кв\ i} = \left(U_{кв\ i} - \frac{\delta}{2} \right)^2 = \left(\frac{\delta^2}{4} \right)(2i-1)^2, \quad (6)$$

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

Из (5) видно, что мощность шумов квантования не зависит от мощности передаваемого сигнала, а, следовательно, отношение полезного сигнала к шуму квантования изменяется при изменении амплитуды сигнала $U_{кв\ i}$:

$$q_{кв\ i}=10\lg\left(\frac{P_{с\ кв\ i}}{P_{ш\ кв}} \right)=10\lg 3+20\lg(2i-1). \quad (7)$$

Соотношение (7) иллюстрирует 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. 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. 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 для компрессии используют модифицированное логарифмическое преобразование:

$$U_{вых} = \frac{\ln\left(1+\mu|U_{вх}|\right)}{\ln(1+\mu)} \operatorname{sign} U_{вх} \quad (8)$$

или, при нормированном входном напряжении:

$$U_{вых} = \frac{\ln\left(1+\mu \frac{|U_{вх}|}{U_{max}} \right)}{\ln(1+\mu)} \operatorname{sign} U_{вх}, \quad (9)$$

где μ – параметр характеристики (степень компрессии); $\operatorname{sign} U_{вх} = \begin{cases} 1; U_{вх} > 0 \\ 0; U_{вх} = 0 \\ -1; U_{вх} < 0 \end{cases}$

Логарифмическое компандирование предполагает экспоненциальное преобразование (экспандирование) на приемной стороне и использование различных методов получения логарифмической шкалы квантования. Если вместо натуральных логарифмов в (9) использовать десятичные, то

$$U_{вых} = 20 \lg\left(1 + \mu \frac{|U_{вх}|}{U_{max}}\right) \operatorname{sign} U_{вх}, \tag{10}$$

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

В [1] показано, что соотношение сигнал/шум квантования для i-го уровня квантования определяется выражением (в наших обозначениях):

$$q_{кв\,i} = 20 \lg\left(\frac{x+1}{x-1}\right) = \text{const(i)}, \tag{11}$$

где $x = 10^{\delta/20} = \text{const(i)}$; $\delta = 20 \frac{\lg(1+\mu)}{2^{n-1}-1}$.

Зависимость коэффициента потери информации $k_{пи}$ от соотношения сигнал/шум квантования $q_{кв}$ определяется в соответствии с [6]:

$$k_{пи} = \begin{cases} 0{,}12 \exp\left\{\frac{q_{кв}}{7}\right\}; & q_{кв} \le 5 \text{дБ}; \\ 1 - 3{,}376 (q_{кв} + 15)^{-0{,}5} \exp\left\{-\frac{(q_{кв} - 5)^2}{250}\right\}; & q_{кв} > 5 \text{дБ}. \end{cases} \tag{12}$$

Известно [1], что разборчивость речи W с достаточной точностью может быть оценена двумя членами степенного ряда:

$$W = 0{,}2\left(1 - 0{,}004^{kL}\right)^4 + 0{,}8\left(1 - 0{,}004^{kL}\right)^3, \tag{13}$$

где W – разборчивость слогов, понимаемая как средняя вероятность правильного приема слога; k – коэффициент потери информации при воздействии помех:

$$K = 1 + \gamma P_{ош} \log_2(\gamma P_{ош}) + (1 - \gamma P_{ош}) \log_2(1 - \gamma P_{ош}), \tag{14}$$

$P_{ош}$– вероятность ошибки при приеме отдельного двоичного символа сигнала КИМ; γ – коэф-

фициент, учитывающий порядковый номер символа в кодовой комбинации (при КИМ искажение разных информационных символов, входящих в одну кодовую комбинацию, приводит к неодинаковым изменениям амплитуды восстановленного речевого сигнала).

– для КИМ с логарифмической шкалой квантования

$$\gamma = \frac{2}{(1-P_{ош})}\left[1-\left(\frac{1-P_{ош}}{2}\right)^{n}\right]; \qquad (15)$$

– для КИМ с линейной шкалой квантования

$$\gamma = \frac{2\left(2^{n}-1\right)}{2^{n}}. \qquad (16)$$

Полагая граничное значение вероятности правильного узнавания слога W=0,2 (слабое, но допустимое в особых условиях), можно определить количество информации на выходе декодера при воздействии помех.

Из (13), следует:

$$k(n,P_{ош})L(n)=0{,}16655, \qquad (17)$$

где k – коэффициент потери информации при воздействии помех, определяемый соотношением (14); $L(n)$ – относительное количество информации при отсутствии помех.

Пороговое значение вероятности ошибочного приема двоичного символа кодовой комбинации, при которой уже не обеспечивается разборчивость речи, можно найти из (17) с учетом (3) и (14). Диаграммы обмена между граничной вероятностью ошибочного приема двоичного символа $P_{ош}$ (разборчивость речи W=0,2) и числом двоичных символов, образующих кодовую комбинацию, представлены на рис.1.

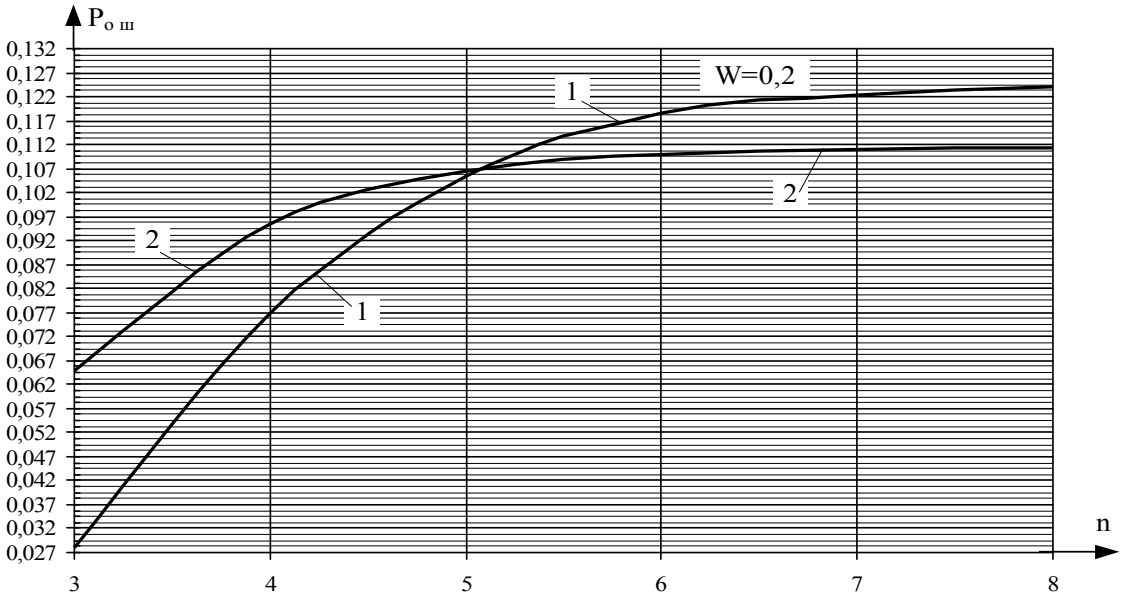


Рис.1. Пороговая вероятность ошибочного приема двоичного символа кодовой комбинации (1 –КИМ с логарифмической шкалой квантования и широкополосный модем; 2 – КИМ с линейной шкалой квантования и широкополосный модем).

Кривая 1 построена для КИМ с логарифмической шкалой квантования при μ=255; кривая 2 – для КИМ с линейной шкалой квантования. При расчетах было принято: $f_н$=0,3 кГц; $f_в$=3,4 кГц.

По диаграммам на рис. 1 можно определить пороговую вероятность ошибочного приема двоичного символа кодовой комбинации, при которой оператор средств радиоразведки не разбирает речевые сообщения.

В [3] и [5] показано, что вероятность ошибки при когерентном приеме отдельного двоичного символа кодовой комбинации определяется соотношениями:

$$P_{ош} = 1 - \Phi\left(\sqrt{\frac{\theta}{N_0}}\right) = 1 - \Phi\left(\sqrt{\frac{4P_c}{P_ш}}\right); \qquad (18)$$

– для КИМ-ЧМн (частотная манипуляция) и

$$P_{ош} = 1 - \left\{1 - 2\left[1 - \Phi\left(\sqrt{\frac{2\theta}{N_0}\sin^2\frac{\pi}{2^k}}\right)\right]\Phi\left(\sqrt{\frac{2\theta}{N_0}\sin^2\frac{\pi}{2^k}}\right)\right\}^{\frac{1}{k}}, \qquad (19)$$

– для k-кратной ФРМ первого порядка

В (18) и (19) обозначено: k– кратность манипуляции ($M = 2^k$ – число вариантов фаз, используемых при k-кратной манипуляции); $\frac{\theta}{N_0} = \frac{P_c \cdot \tau_k}{N_0}$; τ_k – длительность М-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, т.е. $\tau_k = k \cdot \tau_и$); $\tau_и$ – длительность двоичного символа.

– для однократной ФРМ g-ого порядка

$$P_{ош} = \frac{1}{2}\left\{1 - \left[2\Phi\left(\sqrt{\frac{2\theta}{N_0}}\right) - 1\right]\right\}^{H(g)}, \qquad (20)$$

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

При M=4, как уже говорилось, оптимальным является ансамбль ФМ-4 (четырехпозиционная ФМ), [5] и

$$P_{ош} = 1 - \Phi\left(\sqrt{\frac{P_c \tau_k}{N_0}}\right), \qquad (21)$$

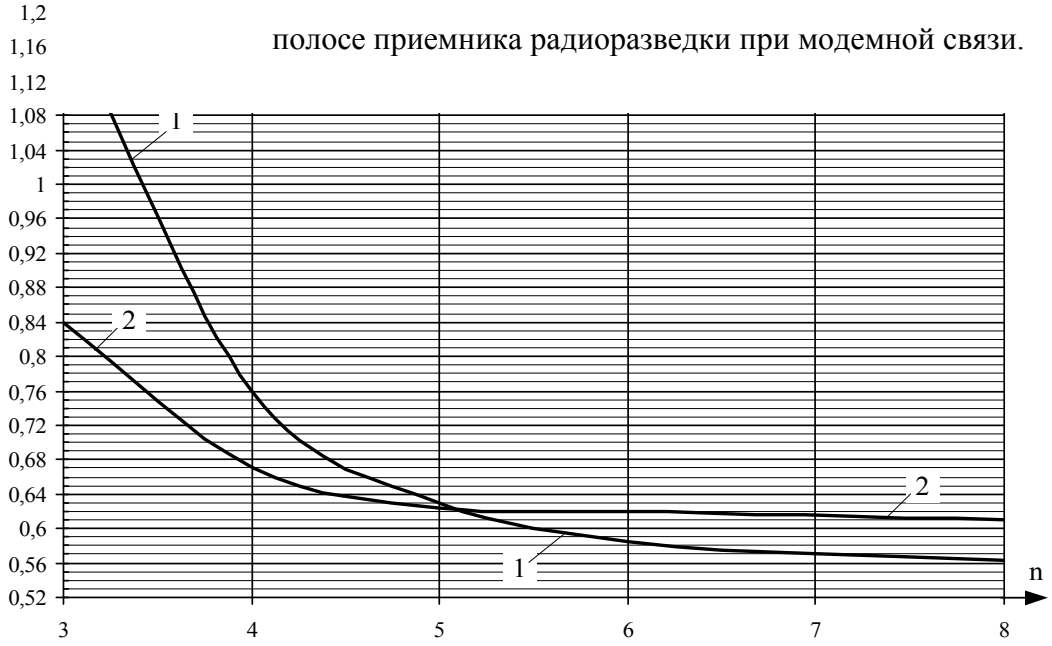
При M>4 наилучшей по помехоустойчивости является симметричная конфигурация с регулярным расположением сигнальных точек в узлах квадратной сети (QASK), [3]:

$$P_{ош} = 1 - \left\{1 - 4\left(1 - \frac{1}{\sqrt{M}}\right)\left[1 - \Phi\left(\sqrt{\frac{3P_c\tau_k}{2N_0(M-1)}}\right)\right]\Phi\left(\sqrt{\frac{3P_c\tau_k}{2N_0(M-1)}}\right)\right\}^{\frac{1}{k}}, \qquad (22)$$

где k– кратность манипуляции; τ_k – длительность M-позиционного символа.

Используя (18)...(22), можно пересчитать обменные диаграммы на рис. 1 ко входу приемника в техническом канале утечки информации. Эти диаграммы в координатах $q_{вх}$–n представлены на рис. 2 для пороговой вероятности правильного узнавания слога W=0,2.

Рис. 2. Диаграммы для определения порогового соотношения сигнал/шум в полосе приемника радиоразведки при модемной связи.



При выборе типа речепреобразующих устройств следует учитывать, что требуемая скорость передачи дискретизированной речи $R_к = f_д \cdot n \geq 2 \cdot f_в = 2 \cdot 3{,}4 = 6{,}8$ кбит/с. Однако коммутируемая телефонная сеть общего пользования, спроектированная для человеческого голоса в диапазоне частот от 300 Гц до 3400 Гц, может использоваться для передачи данных со скоростями до 2400 бит/с. Следовательно, широкополосные цифровые системы, обеспечивающие скорость передачи свыше 2400 бит/с, должны работать на специально выделенных линиях, с отличными от обычных телефонных каналов характеристиками.

Полагая граничное значение вероятности правильного узнавания слога W=0,2 из (3), (17)... (22) и диаграмм рис. 1 и рис. 2 можно найти пороговые (минимальные по мощности) сигналы, при которых уже не обеспечивается разборчивость речи.

Полученные данные могут быть использованы для оценки защищенности речевой информации, передаваемой по линии связи с помощью широкополосных модемов.

СПИСОК ЛИТЕРАТУРЫ

1. Михайлов В. Г. Измерение параметров речи. – М.: Радио и связь, 1981.–495 с.
2. Вильховченко С. Д. Модемы (выбор, установка, настройка) и их бесплатные приложения (терминальты, скрипты, факсы, BBS, Fido). – М.: ABF, 1997.–560 с.
3. Банкет В. Л. АФМ сигналы в системах передачи дискретных сообщений. //Зарубежная радиоэлектроника.–1980, № 9.–с. 49–63.

4. Банкет В. Л. , Ляхов А. И. Применение сверточных кодов в системах связи с фазовой манипуляцией. //Зарубежная радиоэлектроника.–1981, № 8.–с. 3–23.
5. Окунев Ю. Б. Цифровая передача информации фазомодулированными сигналами. – М.: Радио и связь, 1991.–296 с.
6. Покровский Н. Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962.–362 с.
7. Пенин П. И. Системы передачи цифровой информации. – М.: Сов. Радио, 1976.–364 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Большов Олег Анатольевич , аспирант кафедры радиосистем передачи информации и управления Московского государственного авиационного института (технического университета)

Куприянов Александр Ильич , профессор кафедры радиосистем передачи информации и управления Московского государственного авиационного института (технического университета), д.т.н.