

## **Пороговые сигналы при дельта –модуляции**

О.А.Большов

*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; сигналы цифровых систем телекоммуникации и связи; threshold signals, signals of telecommunications

Актуальную практическую задачу выработки новых обоснованных требований к качеству каналов связи, в частности, к защите информации от несанкционированного доступа, невозможно решить без научных исследований. Только на основе таких исследований могут быть приняты законы, регулирующие информационный обмен и отношения в области защиты информации в современных условиях. Представленная статья выполнена на актуальную тему: она лежит в русле решения проблемы оценки степени и показателей защищенности речевой информации, передаваемой по радиоканалам систем и сетей связи. Обеспечение защиты радиоэлектронных средств связи от несанкционированного доступа (перехвата) к информации прежде всего требует определения условий, при которых защищенность информации оказывается достаточной. Актуальность исследований в области защиты информации подтверждается рядом законодательных актов Российской Федерации и нормативных документов директивных органов.

В настоящее время наряду с дальнейшим совершенствованием средств и систем связи все большую научную значимость и интерес приобретает деятельность, направленная на противодействие информационной агрессии, защиту информации. Последнее положение подтверждается как появлением огромного количества публикаций по данной тематике, так и конкретными устройствами, устойчивыми против несанкционированного доступа к информации. При этом вопрос о целесообразности и соразмерности применения специальных средств и методов обеспечения информационной безопасности решался и сейчас решается на основе инженерной интуиции, на практическом опыте. А для организации противодействия информационному нападению и выбора рациональной стратегии поведения в информационном конфликте необходимо уметь оценивать угрозу утечки информации в линиях связи и определять условия, при выполнении которых защищенность речевой информации от радиоперехвата оказывается достаточной, не только экспериментально, но и теоретически. Поэтому основной задачей в статье ставилось выбор критерия и разработка методического аппарата оценивания защищенности информации в радиоканалах передачи

речи. Особенно важна и интересна такая оценка защищенности речевой информации для систем связи, использующих непосредственное преобразование речевых сигналов.

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.

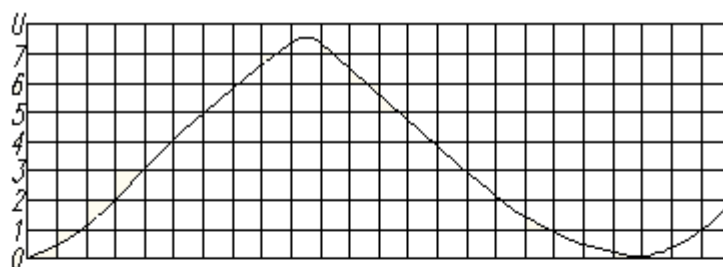
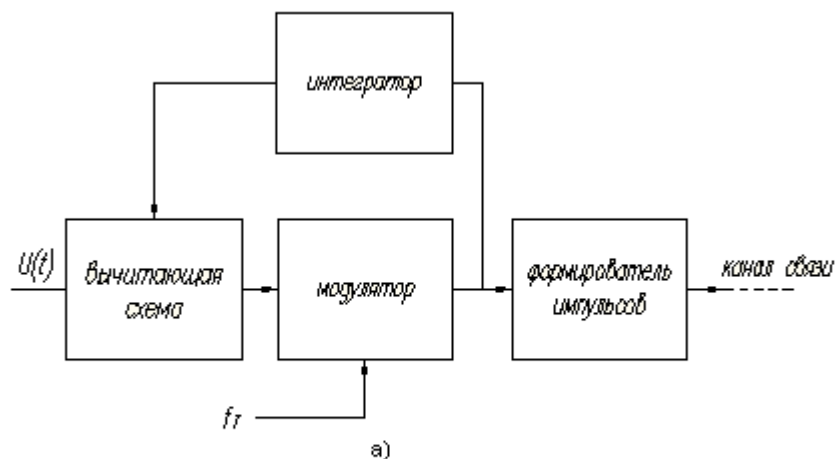
Актуальность исследования пороговых свойств сигналов в радиотехнических каналах утечки информации можно подтвердить следующим. Известны условия [1], [2] накладываемые на минимально допустимые соотношения сигнал/шум в полосе приемника абонента, при которых законный получатель с вероятностью, близкой к 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.

При дельта-модуляция (ДМ) по каналу связи передается информация о приращениях значений самого речевого сигнала. На рис.1,а приведена структурная схема устройства, осуществляющего преобразование. Будем считать, что на один вход вычитающей схемы поступает подлежащий передаче сигнал  $U(t)$  (сплошная кривая на рис.1,б), на другой вход — ступенчатый сигнал, формируемый с помощью интегратора. Разностный сигнал с выхода вычитающей схемы подается на вход модулятора, на другой вход которого поступают импульсы тактовой частоты  $f_T$  (рис.1,в). Если сигнал  $U(t)$  превышает ступенчатый сигнал, то на выход модулятора проходит импульс положительной полярности, в обратном случае — отрицательной полярности. При подаче на вход интегратора импульса положительной полярности ступенчатый сигнал на выходе получает приращение, равное одному шагу квантования  $\delta$ , а при подаче импульса отрицательной полярности сигнал на выходе уменьшается на один шаг квантования.

Для восстановления сигнала на приемном конце используется такой же интегратор, как и на передающем конце, на выходе которого включен фильтр НЧ с граничной частотой  $f_B$ . Формирователь импульсов служит для преобразования последовательности двуполярных импульсов (рис.1,г) в последовательность однополярных импульсов, передаваемых по каналу связи (рис.1,д).



б)



в)



г)



д)

Рис.1 Преобразование сигналов при ДМ.

При дельта- модуляции возникают искажения двух видов: частотные ограничения (перегрузка по крутизне) и дробление. Появление первых обусловлено тем, что ступенчатая кривая на выходе интегратора тем больше отстает от исходного сигнала, чем круче он нарастает, то есть чем выше частота сигнала, тем с большими искажениями он приходит. Дробления возникают на участках, где сигнал имеет постоянную величину или изменяются очень медленно. Дробления бывают особенно заметны в паузах речевых сигналов.

При вычислениях отношения сигнал-шум обычно используют синусоидальный сигнал частотой  $f_C$  а шаг квантования  $\delta$  выбирают так, чтобы исключить перегрузку по крутизне:

$$\delta = 2\pi U_{max} f_C / f_T, \quad (1)$$

где  $U_{max}$  — амплитуда синусоидального сигнала, по которому выбирается шаг квантования.

При этом если шаг квантования подобран для средневзвешенной частоты, то не будут подвержены перегрузке синусоидальные сигналы и с другими частотами, если их мощность

пропорциональна  $1/f_c$ . Для речевых сигналов следует, что это требование удовлетворяется.

Зависимости соотношения сигнал/шум от тактовой частоты, при дельта –модуляции определяется [1]:

$$q_{KB} = 10 \lg \frac{U^2 f_T^3}{8\pi^2 Z U_{max}^2 f_C^2 f_B}, \quad (2)$$

где  $0,18 \leq Z \leq 0,67$ ;  $U$ - амплитуда синусоидального сигнала для которого вычисляется соотношение сигнал/шум.

Количество информации на выходе декодера  $L$  определяется [1]:

$$L = [B(f_B) - B(f_H)] k_{П.И}, \quad (3)$$

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

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

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

В полосе частот до 3.4 кГц сосредоточена практически вся мощность шумов квантования и

$$P_{ш.кв.} = \delta^2 / f_T \quad [1]. \quad (5)$$

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

$$P_{С.КВ.i} = \left( \frac{\delta^2}{4} \right) (2i-1)^2. \quad (6)$$

где  $i=0, 1, 2, \dots, 2^n - 1$ ;  $\delta$  – шаг квантования.

Зависимость коэффициента потери информации  $k_{П.И}$  от соотношения сигнал/шум квантования  $q_{KB}$  приведена в [3] и имеет вид:

$$k_{П.И} = \begin{cases} 0,12 \exp\left(\frac{q_{KB}}{7}\right); q_{KB} \leq 5\text{дБ} \\ 1 - 3,376(q_{KB} + 15)^{-0,5} \exp\left\{-\frac{(q_{KB} - 5)}{250}\right\}; q_{KB} \geq 5\text{дБ} \end{cases} \quad (7)$$

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

$$W = 0,2[1 - 0,004^{LK}]^4 + 0,8[1 - 0,004^{LK}]^3, \quad (8)$$

где  $W$  – разборчивость речи (слов) при воздействии помех;  $k$  – коэффициент помехоустойчивости.

Коэффициент разборчивости речи при наличии помех в канале связи  $k$  определяется соотношением [2]:

$$k = 1 + \gamma P_{Ош} \log_2(\gamma P_{Ош}) + (1 - \gamma P_{Ош}) \log_2(1 - \gamma P_{Ош}), \quad (9)$$

где  $P_{Ош}$  – вероятность ошибки при приеме отдельного символа кодовой комбинации;  $\gamma$  – 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.):

$$\gamma = \frac{3,18}{(1 + P_{Ош})} \left[ 1 - \left( \frac{1 - P_{Ош}}{2} \right)^n \right]. \quad (10)$$

Используя (8), для пороговой вероятности правильного узнавания слога  $W=0,2$  получаем:

$$k(n, P_{Ош})L(n) = 0,16651. \quad (11)$$

Подставляя в (11) соотношения (3) и (9), 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 тактовой частотой представлена на рис.2.

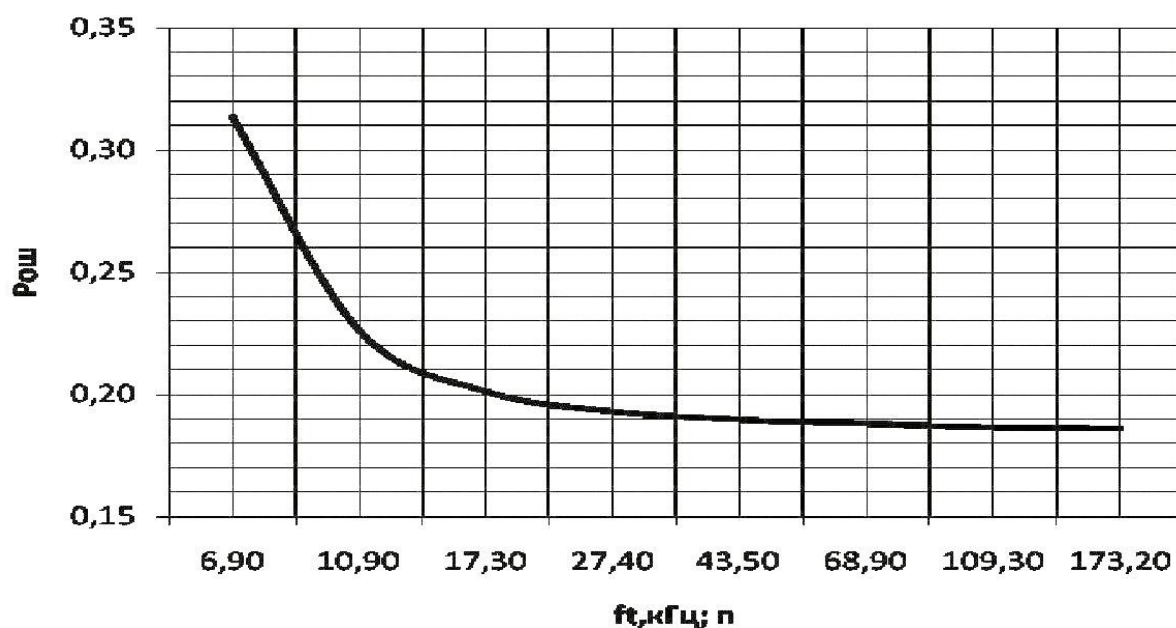


Рис2. Пороговая вероятность ошибочного приема двоичного символа кодовой комбинации.

Таким образом, по диаграмме 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 соотношением:

-для КИМ-ЧМ (частотная манипуляция)

$$P_{ош} = 1 - \Phi(2\sqrt{q_{ВХ}}); \quad (12)$$

-для КИМ-АМ (амплитудная манипуляция)

$$P_{ош} = 1 - \Phi(\sqrt{q_{ВХ}}); \quad (13)$$

-для КИМ-ФМ (фазовая манипуляция)

$$P_{ош} = 1 - \Phi(\sqrt{2q_{ВХ}(1 - \cos 2\varphi)}), \quad (14)$$

где  $q_{ВХ}$  -соотношение сигнал/шум (по мощности) на входе приемника радиоразведки;  $\varphi$  - индекс фазовой модуляции.

Используя (12)...(14), можно пересчитать обменную диаграмму на рис.2 ко входу разведывательного приемника в техническом канале утечки информации.

Отношение сигнал/шум при заданной тактовой частоте может быть улучшено, если вместо ЛДМ использовать дельта -модуляцию с изменяющимся шагом квантования, которую обычно называют адаптивной дельта -модуляцией (АДМ). В этом случае, как в кодере, так и в

декодере осуществляется логическая обработка сигналов, в результате которой можно не только получить нелинейный (изменяющийся) шаг квантования, но и уменьшить шумы дробления, особенно в паузах. Такая возможность обусловлена тем, что тактовая частота значительно превышает наибольшую частоту в спектре кодируемого сигнала, и, следовательно, в кодовых комбинациях, как правило, должно идти подряд несколько одинаковых знаков (нулей или единиц). Если же это условие не выполняется, например, чередуются одиночные единицы и нули, то это свидетельствует о том, что кодируемый сигнал имеет неизменную величину, а появление таких сочетаний кодовых знаков обусловлено спецификой работы кодера.

Как уже отмечалось выше, наибольшую опасность представляют ситуации, в которых злоумышленник в принципе способен принимать речевые сообщения в надпороговой области. В таких ситуациях необходимо специально создавать условия, затрудняющие работу технических средств разведки. Снизить разборчивость речи на выходе технического канала утечки информации можно за счет уменьшения его энергетического потенциала. Для этого необходимо либо уменьшать мощность сигнала, либо применять пространственную развязку, излучая сигнал преимущественно в направлении на приемник абонента. Но возможны случаи, когда оба пути оказываются неприемлемыми или недостаточными по результату. Так, при уменьшении мощности излучаемого сигнала, вместе с разборчивостью речи на выходе технического канала утечки информации снижается и разборчивость в акустическом канале приемника абонента.

Пространственная развязка, связанная с применением остронаправленных антенн, может оказаться неприемлемой по техническим и/или тактическим соображениям: передатчик защищаемой системы располагается на неориентированных объектах, приемники абонента и средства разведки находятся на одном направлении и так далее. При таких условиях единственный путь снижения разборчивости речи в акустическом канале разведывательного приемника это применение активной помехи, маскирующей сигнал от радиоразведки.

Таким образом, определенные в работе пороговые значения безопасных мощностей сигналов в радиоканалах утечки речевой информации соответствующие сигналам на пороге акустической разборчивости, позволяют определить степень опасности перехвата и организовать противодействие системе, осуществляющей информационную агрессию.



## **СПИСОК ЛИТЕРАТУРЫ**

1. Калининцев 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.*