

ОБОСНОВАНИЕ ИЗМЕРИТЕЛЬНОГО СИГНАЛА ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ ПРИ ДИСКРЕТНО-КВАНТОВАННОМ ПРЕОБРАЗОВАНИИ

М.М. БАРАНОВСКИЙ¹, А.Г. ФИЛИППОВИЧ¹,
В.К. ЖЕЛЕЗНЯК², С.В. ЛАВРОВ²

¹*Оперативно-аналитический центр при Президенте Республики Беларусь,
г. Минск, 220030, Республика Беларусь*

²*Учреждение образования «Полоцкий государственный университет
имени Евфросинии Полоцкой»,
г. Новополоцк, 211440, Республика Беларусь*

Введение

Использование современных цифровых технологий неразрывно связано с применением аналого-цифровых и цифро-аналоговых преобразователей. Преобразование аналоговых речевых сигналов в цифровые и их обратное преобразование из цифровой формы в исходный сигнал генерируют новые каналы утечки речевой информации. Установлено, что дискретизация по времени и квантование по уровню речевых сигналов при преобразовании их в цифровую форму являются основными источниками утечки информации [1].

Используемые в настоящее время подходы к оценке защищенности каналов утечки речевых сигналов при их преобразовании в цифровую форму сводятся к отдельной оценке аналогового речевого сигнала и речевого сигнала, представленного в цифровой форме при его передаче по линиям связи.

Для оценки защищенности речевой информации могут использоваться следующие измерительные сигналы [2, 3]:

- гармонический, соответствующий требованиям СТБ 34.101.29-2011;
- шумовой во всей полосе речевого сигнала;
- линейно-частотно-модулированный;
- меандровая последовательность;
- частотно-модулированный без разрыва фазы.

В работе [1] показано, что использование гармонического сигнала не позволяет достоверно оценить защищенность речевого сигнала при высококачественной скоростной передаче в цифровых системах информации, а при выборе измерительных (тестовых) сигналов необходимо учитывать особенности дискретно-квантованного представления речевых сигналов.

Поэтому задачей настоящей работы является обоснование измерительного сигнала для оценки защищенности речевой информации при дискретно-квантованном преобразовании.

Требования к измерительным сигналам для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании

Дискретно-квантованное представление речевых сигналов осуществляют заменой непрерывной шкалы мгновенных значений непрерывного сигнала дискретной шкалой линейно-ломаной аппроксимации. Квантующее устройство является основным преобразующим устройством, содержащим линейный и нелинейный элементы [4]. Идеальным квантующим устройством является нелинейное устройство с нулевой памятью, передаточная характеристика которого представлена ступенчатой функцией с интервалами квантования входного сигнала Δ , находящимися в однозначных соотношениях с кодирующим входным цифровым сигналом с систематической ошибкой квантования, присущей квантующему устройству.

Дискретизация по времени заменяет непрерывную функцию решетчатой, которая определяет совокупность выделенных ординат или дискрет. Если задана непрерывная

функция времени $f(t)$, то ее среднее значение при дискретных значениях аргумента $t = t_n$ преобразуется в решетчатую функцию $f(t_n)$. Разность двух соседних значений аргумента $T_n = t_{n+1} - t_n$ ($t_{n+1} > t_n$) определяет интервал дискретизации (период повторения) по времени, где $n = 1, 2, \dots, m$ [5].

В рабочей полосе частот ограниченной верхней полосы f_B отношение сигнал/шум (SNR) при равномерном квантовании зависит от длины кодовых слов N (бит), частоты дискретизации F_d и формы входного сигнала следующим образом [4]:

$$SNR = 6,02N + 10 \lg \left(\frac{F_d}{2\Delta f_B} \right) + C_s, \quad (1)$$

где C_s – постоянная, учитывающая форму входного (измерительного) сигнала (для гармонических сигналов $C_s = 1,7$ дБ, для звуковых сигналов $C_s = -15 \dots +2$ дБ).

Основными формами (типами) сигнала являются:
 синусоидальный (косинусоидальный);
 прямоугольный (меандр);
 пилообразный (нарастающий или спадающий);
 треугольный.

При равномерном квантовании по уровню из-за нелинейности гармонического сигнала по форме шум квантования не является равномерным в течение периода гармонического сигнала, что не позволяет использовать его в качестве измерительного сигнала (рис. 1). Поэтому наиболее оптимальным является использование линейно нарастающего или линейно спадающего сигнала, которыми являются сигналы треугольной и пилообразной формы. Возникающий при этом шум квантования имеет пилообразную форму, что повышает чувствительность его обнаружения.

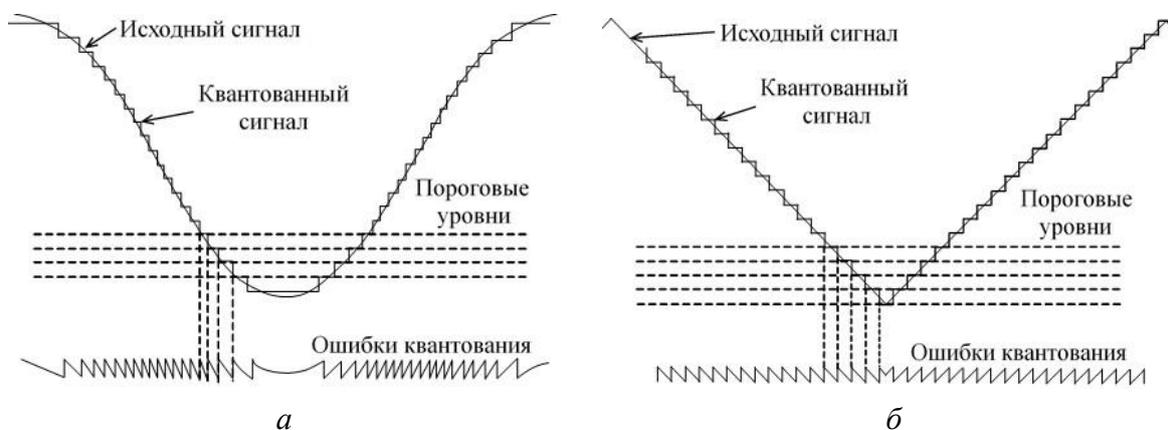


Рисунок 1. – Квантование сигнала: *a* – косинусоидального; *б* – треугольного

Для определения преимуществ некоторых сигналов для их использования в качестве тестовых остановимся на рассмотрении их характеристик. Разложение периодической импульсной последовательности треугольной формы в ряд Фурье имеет следующий вид [5]:

$$f(t) = \frac{8A}{\pi^2} \sum_{k=1}^{\infty} (-1)^{\frac{k-1}{2}} \frac{\sin k\omega t}{k^2}, \quad (2)$$

где A – амплитуда сигнала; k – номер гармоники ($k = 1, 3, 5, \dots$); $\omega = \frac{2\pi}{T_{\Pi}}$ – угловая частота сигнала; T_{Π} – период сигнала.

Разложение импульсов пилообразной формы в ряд Фурье имеет следующий вид [5]:

$$f(t) = \frac{A}{2} - \frac{A}{\pi} \sum_{k=1}^{\infty} \frac{1}{k} \sin k\omega t, \quad (3)$$

где $k = 1, 2, 3, \dots$

Из формул (2) и (3) видно, что для периодической импульсной последовательности треугольной формы четные гармоники отсутствуют, а амплитуды нечетных гармоник убывают пропорционально второй степени номеров гармоник, что позволяет производить оценку защищенности по первой (основной) гармонике. Кроме того, использование в треугольном сигнале нарастающего и спадающего фронтов позволяет в два раза увеличить время обработки сигнала по сравнению с пилообразным сигналом.

Синтез измерительного сигнала

Для использования единого нормативного критерия разборчивости речи в аналоговой форме речевого сигнала и его дискретно-квантованным представлением предложено для формирования измерительного сигнала в качестве исходного (нормированного) сигнала использовать периодическую импульсную последовательность прямоугольной формы с периодом T , равным $1/F_i$, где F_i – средняя частота полосы равной разборчивости речевого сигнала, $i = \overline{1, n}$ $n = 20$ [1], длительность импульса $\tau = \frac{T}{2}$, $F_i = 250; 500; 650; 800; 950; 1125; 1300; 1500; 1700; 1875; 2050; 2250; 2425; 2725; 3100; 3500; 3850; 4550; 6150; 8600$ Гц.

Для преобразования периодической импульсной последовательности прямоугольной формы в периодическую импульсную последовательность треугольной формы используется автокорреляционная функция. В результате преобразования получим необходимый измерительный сигнал, представленный в виде периодической импульсной последовательности треугольной формы с мощностью $A^2\tau$ и длительностью импульса 2τ [1], где A – амплитуда импульса импульсной последовательности прямоугольной формы и $\tau = 2000; 1000; 769; 625; 526; 444; 385; 333; 294; 267; 243; 222; 206; 183; 161; 143; 130; 110; 81; 58$ мкс.

Полученный сигнал периодической импульсной последовательности треугольной формы без его искажения вводят в канал передачи речевого сигнала. На выходе канала передачи получают преобразованный сигнал в виде выборки и ошибки квантования, которые обрабатывают в каждой из полос равной разборчивости. Из периодической импульсной последовательности треугольной формы выделяют спектральные составляющие методом преобразования Фурье с получением основной гармоники гармонического сигнала. Для увеличения отношения сигнал/шум применяют накопление, при котором основная и высшие гармоники сигнала накапливаются по линейному закону, а шум – по среднеквадратичному. Оценку защищенности речевого сигнала выполняют сравнением полученного отношения сигнал/шум с нормированным [1].

Заключение

Таким образом, для повышения достоверности оценки защищенности канала утечки речевых сигналов при дискретно-квантованном преобразовании предложено использование измерительного сигнала треугольной формы. Использование предложенного измерительного сигнала позволяет установить его численную зависимость с численным значением сигнала, принятого в качестве нормированного и сравнить для принятия решения о защищенности речевого сигнала. Полученные результаты позволяют проводить дальнейшие исследования защищенности речевых сигналов при их обратном преобразовании из цифровой формы в исходный сигнал. При этом оценка защищенности аналогового и дискретно-квантованного речевого сигнала будет производиться по единой методике.

Литература

1. Железняк, В.К. Синтез измерительного композитного сигнала для оценки защищенности речевых сигналов при дискретно-квантованном преобразовании / В.К. Железняк, С.В. Лавров, А.Г. Филиппович, М.М. Барановский // Доклады БГУИР. – 2020. – № 18(6), – С. 81–87.
2. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – Санкт-Петербург: ГУАП, 2006. – 188 с.
3. Железняк, В.К., Системный подход: защита информации, помехозащищенность, помехоустойчивость / В.К. Железняк, Д.С.Рябенко, С.В. Лавров // Вестник Полоцкого государственного университета, 2016. – № 4. – С. 2–7.
4. Шкритек, П. Справочное руководство по звуковой схемотехнике / П. Шкритек. – Москва: Мир, 1991 – 446 с.
5. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – Москва: Вильямс, 2007. – 1104 с.