http://dx.doi.org/10.35596/1729-7648-2020-18-4-89-95

Оригинальная статья
Original paper

УДК 004.056.5

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КАНАЛОВ УТЕЧКИ РЕЧЕВЫХ СИГНАЛОВ ПРИ ДИСКРЕТНО-КВАНТОВАННОМ ПРЕОБРАЗОВАНИИ

ЖЕЛЕЗНЯК В.К. [1], ЛАВРОВ С.В.[1], БАРАНОВСКИЙ М.М.[2], ФИЛИППОВИЧ А.Г.[2]

[1]*Полоцкий государственный университет (г. Новополоцк, Республика Беларусь)*

[2]*Оперативно-аналитический центр при Президенте Республики Беларусь, (г. Минск, Республика Беларусь)*

Поступила в редакцию 25 мая 2020

Аннотация. Целью статьи является оценка канала утечки дискретно-квантованного речевого сигнала при амплитудно-импульсной модуляции. Дискретно-квантованное преобразование аналоговых сигналов в цифровую форму рассматривается на примере амплитудно-импульсной модуляции. Разработка математической модели каналов утечки речевых сигналов при дискретно-квантованном преобразовании основана на спектральном представлении периодических сигналов рядами Фурье. В качестве измерительного сигнала предложено использовать периодическую импульсную последовательность треугольной формы. Измерительный сигнал треугольной формы имеет преимущество перед гармоническим сигналом в процессе выделения шума квантования, так как позволяет достичь более высокой точности при его обработке. Для оценки защищенности канала, обусловленного амплитудно-импульсной модуляцией, используется гармонический сигнал, сформированный из периодической импульсной последовательности треугольной формы методом преобразования Фурье. В результате построения спектра амплитудно-импульсного модулированного сигнала установлено, что при каждой гармонической составляющей спектра, соответствующей спектру периодической последовательности импульсов, появляются боковые составляющие, соответствующие спектру модулирующего сигнала, которые вместе с низкочастотной составляющей в полосе речевого сигнала формируют канал утечки информации. Наличие в составе спектра амплитудно-импульсного модулированного сигнала исходного модулирующего сигнала позволяет провести оценку защищенности канала утечки речевого сигнала при амплитудно-импульсной модуляции по низкочастотной составляющей модулирующего сигнала. Представленные в статье материалы являются оригинальными и могут быть использованы при оценке защищенности каналов утечки речевых сигналов, преобразованных в цифровую форму. Кроме того, полученные результаты позволяют проводить дальнейшие исследования защищенности речевых сигналов при их обратном преобразовании из цифровой формы в исходный сигнал.

Ключевые слова: защита информации, канал утечки речевого сигнала, амплитудно-импульсная модуляция.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Железняк В.К., Лавров С.В., Барановский М.М., Филиппович А.Г. Математическая модель каналов утечки речевых сигналов при дискретно-квантованном преобразовании. Доклады БГУИР. 2020; 18(4): 89-95.

MATHEMATICAL MODEL OF SPEECH SIGNAL LEAKAGE CHANNELS DURING DISCRETE-QUANTIFIED CONVERSION

VLADIMIR K. ZHELEZNJAK[1], SERGEI V. LAVROV[1], MIKHAIL M. BARANOUSKI[2], ANDREI G. FILIPOVICH[2]

[1]*Polotsk State University (Novopolotsk, Republic of Belarus)*

[2]*Operational and Analytical Center under the Aegis of the President of the Republic of Belarus (Minsk, Republic of Belarus)*

Submitted 25 May 2020

Abstract. The purpose of the article is to estimate the leakage channel of a discrete-quantized speech signal with amplitude-pulse modulation. Discrete-quantized analog-to-digital conversion of signals in the article is considered by the example of pulse-amplitude modulation. Development of mathematical model of speech signal leakage channels during discrete-quantified conversion is based on the spectral representation of periodic signals by Fourier series. A periodic pulse train of triangular shape as a measuring signal is proposed. Measuring signal of triangular shape has an advantage over a harmonic signal in the process of quantization noise extraction because it allows one to achieve higher accuracy during signal processing. To evaluate the channel security caused by amplitude-pulse modulation, a harmonic signal is used, which is generated from a periodic pulse sequence of a triangular shape by the Fourier transform method. As a result of constructing the spectrum of the amplitude-pulse modulated signal, it was found that for each harmonic component of the spectrum corresponding to the spectrum of the periodic sequence of pulses, side components corresponding to the spectrum of the modulating signal appear. This side components, together with the low-frequency component in the band of the speech signal, form an information leakage channel. The presence of source modulating signal in the amplitude-pulse modulated signal spectrum allows one to digest the security of the leakage channel of the speech signal with amplitude-pulse modulation by the low-frequency component of the modulating signal. The materials presented in the article are original and can be used in assessing the security of leakage channels of speech signals converted into digital form. In addition, the results obtained allow further studies of the security of speech signals during their inverse transformation from digital to the original signal.

Keywords: information security, speech information leakage channel, pulse-amplitude modulation.

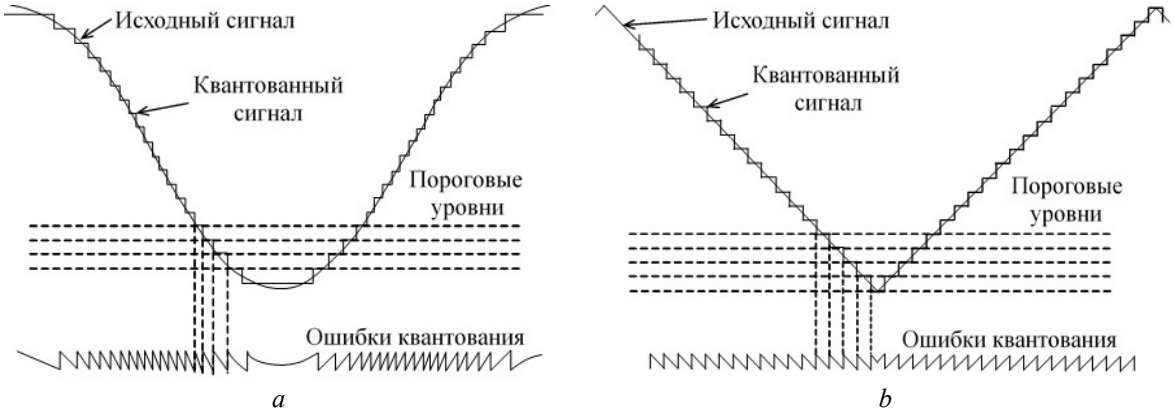
Conflict of interests. The authors declare no conflict of interests.

For citation. Zheleznjak V.K., Lavrov S.V., Baranouski M.M., Filipovich A.G. Mathematical model of speech signal leakage channels during discrete-quantified conversion. Doklady BGUIR. 2020; 18(4): 89-95.

Введение

Высококачественная высокоскоростная передача по широкополосным каналам аналоговых речевых сигналов дискретно-квантованным представлением обусловливает их различные преобразования, из которых важнейшим является амплитудно-импульсная модуляция. Амплитудно-импульсная модуляция формируется воздействием на периодическую импульсную последовательность в диапазоне частот от 44,1 до 192 кГц прошедшего через аналго-цифровой преобразователь аналогового речевого сигнала [1].

При амплитудно-импульсной модуляции определяются мгновенные значения измерительного сигнала в равноотстоящих друг от друга точках, отсчитываемых по временной шкале через операцию дискретизации, осуществляемую с помощью периодической последовательности прямоугольных импульсов. Процессы дискретизации по времени и квантования по уровню на примере косинусоидального и треугольного сигнала с представлением ошибки квантования представлены на рис. 1.



a *b*

Рис. 1. Квантование сигнала: косинусоидального (*a*); треугольного (*b*)
Fig. 1. The quantization of the signal: cosine (*a*); triangular (*b*)

Используемые в настоящее время подходы к оценке защищенности каналов утечки речевых сигналов при их преобразовании в цифровую форму сводятся к раздельной оценке аналогово речевого сигнала и речевого сигнала, представленного в цифровой форме при его передаче по линиям связи, а в качестве измерительного сигнала используют, как правило, гармонический сигнал [2, 3].

Для определения каналов утечки речевой информации при ее преобразовании в цифровую форму в качестве измерительного сигнала целесообразно использовать сигнал треугольной формы, который имеет преимущество перед гармоническим сигналом в процессе выделения шума квантования, так как возникающий при этом шум квантования имеет пилообразную форму, что повышает чувствительность его обнаружения [4]. Разложение периодической импульсной последовательности треугольной формы в ряд Фурье имеет следующий вид [5]:

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

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

Из формулы (1) видно, что для периодической импульсной последовательности треугольной формы четные гармоники отсутствуют, а амплитуды нечетных гармоник убывают пропорционально второй степени номеров гармоник. Поэтому для оценки защищенности канала, обусловленного амплитудно-импульсной модуляцией, в дальнейшем будем использовать гармонический сигнал, сформированный из периодической импульсной последовательности треугольной формы, который соответствует первой (основной) гармонике.

Спектр сигнала при амплитудно-импульсной модуляции

Определим параметры амплитудно-импульсного модулированного сигнала при воздействии на выделенную гармоническую составляющую путем преобразования Фурье периодической импульсной последовательности треугольной формы и последующей обработки для получения спектра с целью определения утечки информации. Представим модулирующий сигнал $c(t)$, выделенный из измерительного сигнала периодической импульсной последовательности треугольной формы преобразованием Фурье, в следующем виде:

$$c(t)=C_{\max}\sin\omega_c t, \qquad (2)$$

где $C_{\max}$ – максимальное значение амплитуды; ω_c – частота модулирующего сигнала.

Амплитудно-модулированный сигнал $s(t)$ представляют следующей формулой [6]:

$$s(t)=\left[1+m_a c(t)\right]f(t), \tag{3}$$

где $c(t)$ – модулирующий сигнал; $f(t)$ – периодическая последовательность прямоугольных импульсов; m_a – коэффициент амплитудной модуляции:

$$m_a=\frac{C_{\max}}{A}, \tag{4}$$

где A – амплитуда прямоугольных импульсов из периодической последовательности.

Периодическая последовательность прямоугольных импульсов $f(t)$ с длительностью импульса $\tau_и$ и периодом $T_д$ может быть представлена как

$$f(t)=\sum_{k=-\infty}^{\infty}\sigma\left(t-kT_д\right), \tag{5}$$

где $\sigma(t)$ – функция, описывающая одиночный импульс последовательности $f(t)$:

$$\sigma(t)=\begin{cases} A \text{ при } -\dfrac{\tau_и}{2}\le t\le\dfrac{\tau_и}{2}, \\ 0 \text{ при } t<-\dfrac{\tau_и}{2},\ t>\dfrac{\tau_и}{2}. \end{cases} \tag{6}$$

Представление периодической последовательности прямоугольных импульсов рядом Фурье с учетом (5) и (6) будет иметь следующий вид [7]:

$$f(t)=A\left[\frac{\tau_и}{T_д}+\frac{2}{\pi}\sum_{n=1}^{\infty}\frac{1}{n}\sin\frac{n\pi\tau_и}{T_д}\cos 2\pi nF_д t\right], \tag{7}$$

где $F_д=\dfrac{1}{T_д}$ – частота дискретизации; $A\dfrac{\tau_и}{T_д}$ – постоянная составляющая; $\dfrac{2A}{\pi n}\sin\dfrac{n\pi\tau_и}{T_д}\cos 2\pi nF_д t$ – гармоники частоты дискретизации.

Подставляя в выражение (3), описывающее амплитудно-модулированный сигнал, $s(t)$ выражения для $f(t)$ из формулы (7) и $c(t)$ из формулы (2), получим спектральный состав амплитудно-модулированного сигнала с учетом тригонометрических преобразований:

$$s(t)=\frac{A\tau_и}{T_д}+\frac{m_a A\tau_и\sin\omega_c t}{T_д}+\frac{2A}{\pi}\sum_{n=1}^{\infty}\frac{1}{n}\sin\frac{n\pi\tau_и}{T_д}\cos 2\pi nF_д t+\frac{m_a A}{\pi}\sum_{n=1}^{\infty}\frac{1}{n}\sin\frac{n\pi\tau_и}{T_д}\sin\left(2\pi nF_д\pm\omega_c\right)t. \tag{8}$$

Согласно формуле (8) спектр амплитудно-импульсного модулированного сигнала содержит:

– постоянную составляющую

$$A_0=\frac{A\tau_и}{T_д}; \tag{9}$$

– исходный модулирующий сигнал

$$A_c=\frac{m_a A\tau_и}{T_д}\sin\omega_c t; \tag{10}$$

– гармоники частоты дискретизации – модулируемой периодической импульсной последовательности

$$A_n=\frac{2A}{\pi n}\sin\frac{n\pi\tau_и}{T_д}\cos 2\pi nF_д t; \tag{11}$$

– боковые составляющие, соответствующие спектру модулирующего сигнала,

$$A_{nб} = \frac{m_a A}{\pi n} \sin \frac{n\pi\tau_и}{T_д} \sin\left(2\pi n F_д \pm \omega_c\right) t . \qquad (12)$$

Графическое изображение спектра амплитудно-импульсного модулированного сигнала представлено на рис. 2.

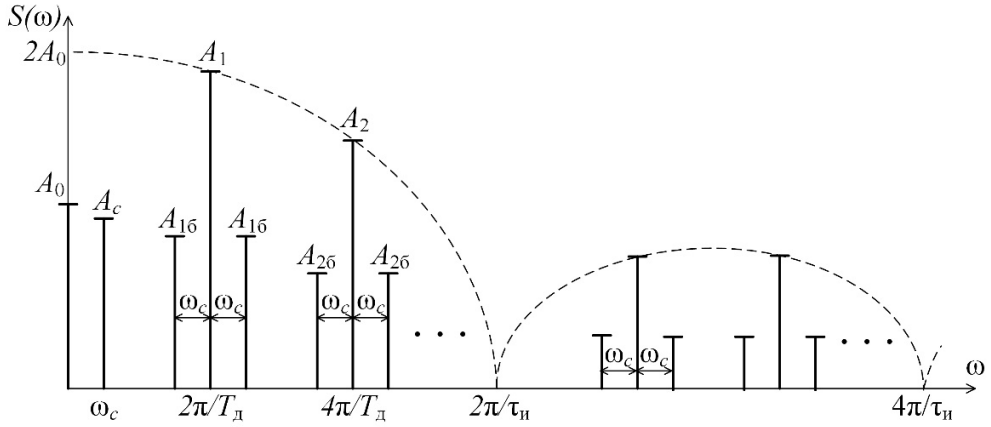


Рис. 2. Спектр амплитудно-импульсного модулированного сигнала
Fig. 2. The spectrum of the amplitude-pulse modulated signal

Из рис. 2 и формулы (8) следует, что при каждой гармонической составляющей спектра A_n, соответствующей спектру периодической последовательности импульсов, появляются боковые составляющие $A_{nб}$, соответствующие спектру модулирующего сигнала, которые вместе с низкочастотной составляющей A_c в полосе речевого сигнала будут формировать канал утечки информации. Таким образом, утечка речевой информации, преобразованной в цифровую форму, возможна на частотах ω_c (низкочастотный канал утечки) и $2\pi n F_д \pm \omega_c$ (высокочастотный канал утечки). При этом основной причиной формирования дополнительного высокочастотного канала утечки речевой информации при преобразовании ее в цифровую форму являются процессы дискретизации по времени и квантования по уровню речевого сигнала.

Формируемый указанными составляющими канал утечки речевой информации в соответствии с формулами (10) и (12) зависит от коэффициента амплитудной модуляции m_a, длительности импульса $\tau_и$ и частоты дискретизации $F_д$. Длительность импульса и частота дискретизации, как правило, известны, а величину коэффициента амплитудной модуляции можно определить путем исключения из низкочастотной составляющей модулирующего сигнала A_c постоянной составляющей A_0:

$$\frac{A_c}{A_0} = \frac{\dfrac{m_a A \tau_и}{T_д} \sin \omega_c t}{\dfrac{A\tau_и}{T_д}} = m_a \sin \omega_c t . \qquad (13)$$

Кроме того, наличие в составе спектра амплитудно-импульсного модулированного сигнала исходного модулирующего сигнала позволяет произвести оценку защищенности канала утечки речевого сигнала при амплитудно-импульсной модуляции по низкочастотной составляющей модулирующего сигнала A_c. Для этого [3]:

1. По полученным значениям параметра измерительного сигнала в точке наблюдения и параметра шума в той же точке наблюдения определяют отношение сигнал/шум.

2. Определяют отношение нормированных параметров сигнала и шума в канале утечки речевого сигнала.

3. Сравнивают отношение сигнал/шум, полученное в процессе оценки в точке наблюдения, с нормированным отношением сигнал/шум из нормированных параметров. Если отношение сигнал/шум нормированных параметров больше отношения измеренных параметров, то принимают решение о защищенности, т. е. отсутствии канала утечки речевой информации. В противном случае – о наличии канала утечки речевого сигнала.

Заключение

Таким образом, произведена оценка канала утечки информации при амплитудно-импульсной модуляции исходя из математической модели спектра сигнала. Установлено, что при каждой гармонической составляющей спектра A_n, соответствующей спектру периодической последовательности импульсов, появляются боковые составляющие $A_{nб}$, соответствующие спектру модулирующего сигнала, которые вместе с низкочастотной составляющей A_c в полосе речевого сигнала формируют канал утечки информации. Наличие в составе спектра амплитудно-импульсного модулированного сигнала исходного модулирующего сигнала позволяет произвести оценку защищенности канала утечки речевого сигнала при амплитудно-импульсной модуляции по низкочастотной составляющей модулирующего сигнала A_c. При этом оценка защищенности аналогового и дискретно-квантованного речевого сигнала производится по единой методике.

Список литературы

1. Крухмалев В.В., Гордиенко В.Н. *Основы построения телекоммуникационных систем и сетей*. Москва: Горячая линия – Телеком; 2018.
2. Бузов Г.А. *Защита информации ограниченного доступа от утечки по техническим каналам*. Москва: Горячая линия – Телеком; 2015.
3. Железняк В.К. *Защита информации от утечки по техническим каналам*. Санкт-Петербург: ГУАП; 2006.
4. Железняк В.К., Лавров С.В., Барановский М.М., Филиппович А.Г. Способ оценки защищенности преобразованного в цифровую форму речевого сигнала в каналах утечки информации. *Комплексная защита информации: материалы XXIV научно-практической конференции*. 2019: 53-59.
5. Сергиенко А.Б. *Цифровая обработка сигналов*. Санкт-Петербург: Питер; 2005.
6. Островский Л.А. *Основы общей теории электроизмерительных устройств*. Ленинград: Энергия; 1965.
7. Кэтермоул К.В. *Принципы импульсно-кодовой модуляции*. Москва: Связь; 1974.

References

1. Krukhmalev V.V., Gordienko V.N. [*Principles of telecommunication systems and networks construction*]. Moscow: Hotline Telecom; 2018. (In Russ.)
2. Buzov G.A. [*Protection of limited access information from leakage through technical channels*]. Moscow: Hotline Telecom; 2015. (In Russ.)
3. Zheleznjak V.K. [*Information leakage protection through technical channels*]. St. Petersburg: SUAI, 2006. (In Russ.)
4. Zheleznjak V.K., Lavrov S.V., Baranouski M.M., Filipovich A.G. [A method for assessing the security of a digitized speech signal in an information leakage channel]. *Integrated information protection: materials of the XXIV scientific-practical conference.* 2019; 53-59. (In Russ.)
5. Sergienko A.B. [*Digital signal processing*]. St. Petersburg: Peter; 2005. (In Russ.)
6. Ostrovsky L.A. [*Principles of the general theory of electrical measuring devices*]. Leningrad: Energy; 1965. (In Russ.)
7. Cathermole C.V. [*Principles of Pulse Code Modulation*]. Editor: V.V. Markov. Moscow: Communication, 1974. (In Russ.)

Вклад авторов

Железняк В.К. определил замысел исследования, осуществил окончательное утверждение рукописи для публикации, ее критический пересмотр в части значимого интеллектуального содержания.

Лавров С.В. принимал участие в разработке математической модели и способа оценки защищенности канала утечки речевого сигнала.

Барановский М.М. принимал участие в разработке математической модели и интерпретации полученных результатов, осуществил редактирование и оформление статьи для публикации.

Филиппович А.Г. осуществил критический пересмотр статьи в части значимого интеллектуального содержания, вносил правки в текст статьи.

Authors' contribution

Zheleznjak V.K. defined the concept of research and delivered the final approval of the manuscript for publication, including its critical review in part of significant intellectual content.

Lavrov S.V. participated in the development of the mathematical model and method for evaluating the security of a speech leakage channel.

Baranouski M.M. participated in the development of the mathematical and in the interpretation of the results, prepared the article for publication.

Filipovich A.G. included its critical review in part of significant intellectual content, edited the text of the article.

Сведения об авторах

Железняк В.К., д.т.н., профессор, заведующий научно-исследовательской опытно-экспериментальной лабораторией технической защиты информации Полоцкого государственного университета.

Лавров С.В., аспирант Полоцкого государственного университета.

Барановский М.М., главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь.

Филиппович А.Г., кандидат технических наук, главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь.

Адрес для корреспонденции

211440, Республика Беларусь,
Витебская обл., г. Новополоцк, ул. Блохина, 29,
учреждение образования «Полоцкий государственный университет»
тел. +375-29-212-74-47;
e-mail: v.zheleznjak@psu.by
Железняк Владимир Кириллович

Information about the authors

Zheleznjak V.K., D.Sci., Professor, Head of the Research Experimental Laboratory of Technical Information Protection of Polotsk State University.

Lavrov S.V., PG Student of Polotsk State University.

Baranouski M.M., chief specialist of the Operational and Analytical Center under the Aegis of the President of the Republic of Belarus.

Filipovich A.G., PhD, chief specialist of the Operational and Analytical Center under the Aegis of the President of the Republic of Belarus.

Address for correspondence

211440, Republic of Belarus,
Vitebsk region, Novopolotsk, Blokhina str., 29,
Educational intitution «Polotsk State University»
tel. +375-29-212-74-47;
e-mail: v.zheleznjak@psu.by
Zheleznjak Vladimir Kirilovich