



<http://dx.doi.org/10.35596/1729-7648-2023-21-2-32-40>

Оригинальная статья

Original paper

УДК 621.381.8.004

ОЦЕНКА ИНФОРМАЦИОННЫХ ПОКАЗАТЕЛЕЙ ШУМА КВАНТОВАНИЯ АНАЛОГО-ЦИФРОВОГО ПРЕОБРАЗОВАНИЯ РЕЧЕВОГО СИГНАЛА

В. К. ЖЕЛЕЗНЯК, К. Я. РАХАНОВ, Е. Р. АДАМОВСКИЙ

*Полоцкий государственный университет имени Евфросинии Полоцкой
(г. Новополоцк, Республика Беларусь)*

Поступила в редакцию 27.09.2022

© Белорусский государственный университет информатики и радиоэлектроники, 2023
Belarusian State University of Informatics and Radioelectronics, 2023

Аннотация. Приведена методика оценки информационных параметров шума квантования, формируемого аналого-цифровым преобразованием измерительного сигнала. Представлены описание алгоритма методики и состав оборудования для имитационно-натурного эксперимента с целью подтверждения корректности способа обработки и выделения информационных параметров сигнала и шума квантования, в котором вместо измерительной антенны используется соединительный кабель. Показаны результаты проведенных измерений в виде графиков зависимостей времени выделения шума квантования путем накопления от влияющих факторов и контролируемых параметров, демонстрирующие предельные значения выделения информационных параметров шума квантования аналого-цифрового преобразования измерительного сигнала. Получено подтверждение гипотезы оценки информационных параметров шума квантования.

Ключевые слова: аналого-цифровое преобразование, измерительный сигнал, шум квантования, канал утечки информации.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Железняк, В. К. Оценка информационных показателей шума квантования аналого-цифрового преобразования речевого сигнала / В. К. Железняк, К. Я. Раханов, Е. Р. Адамовский // Доклады БГУИР. 2023. Т. 21, № 2. С. 32–40. <http://dx.doi.org/10.35596/1729-7648-2023-21-2-32-40>.

EVALUATION OF INFORMATION INDICATORS OF QUANTIZATION NOISE GENERATED BY SPEECH SIGNAL ANALOGUE-DIGITAL CONVERSION

VLADIMIR K. ZHELEZNYAK, KONSTANTIN JA. RAHANOV, YAHOR R. ADAMOVSKIY

Euphrosyne Polotskaya State University of Polotsk (Novopolotsk, Republic of Belarus)

Submitted 27.09.2022

Abstract. The paper presents a technique for estimating the information parameters of the quantization noise generated by the analog-to-digital conversion of the measuring signal. An experiment and algorithm descriptions are presented to confirm the correctness of the method for processing and extracting the information parameters of the signal and quantization noise, in which a connecting cable is used instead of a measuring antenna. The measurement results are shown in the form of graphs of the dependences of the quantization noise extraction time by accumulation on influencing factors and controlled parameters, which demonstrate the limiting values of the extraction of information parameters of the quantization noise of the analog-to-digital conversion of the measuring signal. Confirmation of the hypothesis of estimating the information parameters of the quantization noise is obtained.

Keywords: analog-to-digital conversion, test signal, quantization noise, information leakage channel.

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

For citation. Zheleznyak V. K., Rahanov K. Ja., Adamovskiy Y. R. Evaluation of Information Indicators of Quantization Noise Generated by Speech Signal Analogue-Digital Conversion. *Doklady BGUIR*. 21 (2), 32–40. <http://dx.doi.org/10.35596/1729-7648-2023-21-2-32-40> (in Russian).

Введение

Передача цифровых речевых сигналов по линиям связи является неотъемлемой частью системы комплексной защиты информации [1] и относится к технической защите речевой информации средств коммуникации [2]. Одна из составных частей средств коммуникации – преобразование цифрового речевого сигнала в аналоговую форму с помощью цифро-аналогового преобразователя (ЦАП) с последующей его передачей через линию связи до приемника сигнала.

Полученный аналоговый сигнал передается в анализатор или на излучающее устройство в понятной для человека форме. На этапе аналого-цифрового преобразования (АЦП) сигнала осуществляются дискретизация и квантование сигнала с помощью электронных компонентов, излучающих физические поля – магнитные и электрические, которые могут нести в себе информационные параметры о передаваемом сигнале, что является каналом утечки информации (КУИ). В [3, 4] оценку защищенности такого КУИ предлагается выполнять с помощью периодической последовательности импульсов треугольной формы, которая не вносит методических погрешностей, обусловленных нелинейностью шума квантования.

Наиболее эффективные методы оптимального приема детерминированного сигнала – на основе корреляционного приема. В случае сигнала известной формы более мощным средством обнаружения является функция взаимной корреляции [5]. В связи с этим цель исследований – количественная оценка информационных показателей шума квантования АЦП аналогового речевого сигнала.

Методика оценки информационных показателей

Пример блок-схемы автоматизированной оценки канала утечки информационных полей аналого-цифрового преобразования приведен на рис. 1. Количественная оценка информационных показателей шума квантования должна выполняться с помощью автоматизированной системы, так как излучаемые физические поля характеризуются низким уровнем сигнала в шумах высокого уровня, и поэтому для их выделения потребуются дополнительная обработка и накопление. Блок-схема состоит из трех основных частей: системы приема-передачи, КУИ (излучаемые физические поля) и программно-аппаратного комплекса (ПАК) оценки КУИ.

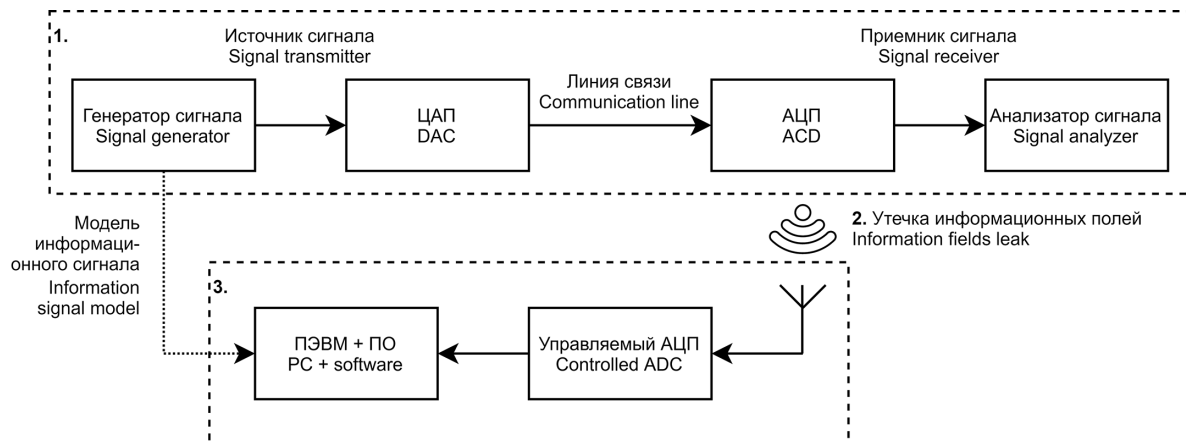


Рис. 1. Блок-схема автоматизированной оценки канала утечки информационных полей аналого-цифрового преобразователя

Fig. 1. Block diagram for automated evaluation of analog-to-digital conversion information fields in a leak channel

Система приема-передачи сигнала включает в себя генератор измерительного сигнала и ЦАП, передающий измерительный сигнал в линию связи, по которой сигнал поступает на АЦП в приемнике сигнала. В момент преобразования сигнала из аналоговой формы АЦП излучает физические поля, характеризующие КУИ. ПАК включает в себя измерительную антенну и персональную электронно-вычислительную машину (ПЭВМ) с установленным специальным программным обеспечением (ПО).

Излучаемые физические поля, возникающие при преобразовании сигнала в цифровую форму, фиксирует измерительная антенна, а затем передает их на управляемый АЦП для выделения и обработки информационных параметров сигнала и шума квантования, которые осуществляются с помощью специального ПО на ПЭВМ. В качестве обработки используется синхронное накопление, позволяющее улучшить отношение сигнал/шум (ОСШ). Алгоритм работы программного обеспечения представлен на рис. 2.

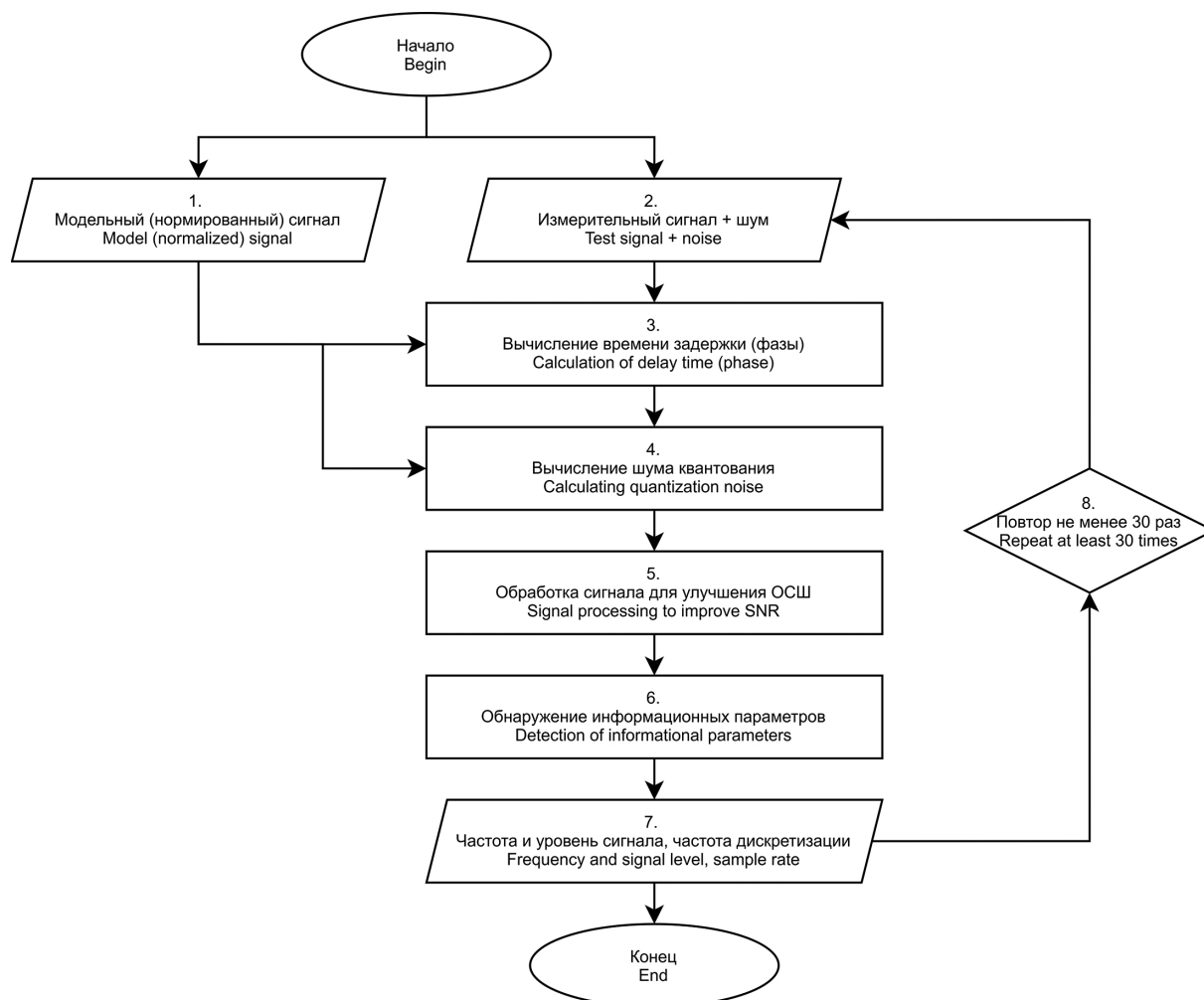


Рис. 2. Алгоритм оценки информационных параметров шума квантования аналого-цифрового преобразователя измерительного сигнала
Fig. 2. Algorithm for estimating the information parameters of quantization noise obtained from the measurement signal in an analog-to-digital converter

Алгоритм включает следующие этапы.

1. Формируется модельный (идеальный) измерительный сигнал в цифровом виде, параметры которого согласованы с генератором сигнала (штриховая линия связи на рис. 1).
2. Захватывается сигнал с помощью измерительной антенны в точке наблюдения. При передаче сигнала по каналу связи значения фазы и амплитуды сигнала неизвестны, а сам сигнал подвергается искажениям и влиянию шумов. Блоки 1 и 2 на рис. 2 выполняются параллельно.
3. Определяется время задержки измерительного сигнала путем расчета взаимной корреляции смеси сигнала и шума с модельным сигналом.
4. Рассчитывается шум квантования путем вычисления разницы принятой смеси сигнала и шума и восстановленной цифровой копией сигнала с учетом фазы.
5. Применяются спектральное накопление и полосовая фильтрация сигналов.
6. Выполняется обнаружение информационных параметров канала утечки.
7. Рассчитанные показатели протоколируются и выводятся на экран.
8. Процедура обнаружения информационных параметров повторяется 30 раз, а результаты усредняются. После этого мощность шума увеличивается, измерения повторяются.

Этапы 5 и 6 можно представить в виде спектрального обнаружителя информационных параметров, блок-схема которого изображена на рис. 3. В обнаружителе для более эффективно накопления выполняется преобразование сигнала в частотную область с помощью операции быстрого преобразования Фурье (БПФ) и его разделение на действительную и мнимую части с независимым накоплением и последующим вычислением общего модуля спектральной составляющей. Требуемое количество накоплений до обнаружения сигнала и обнаруженная частота сигнала учитываются в определении исходного уровня информационного параметра.

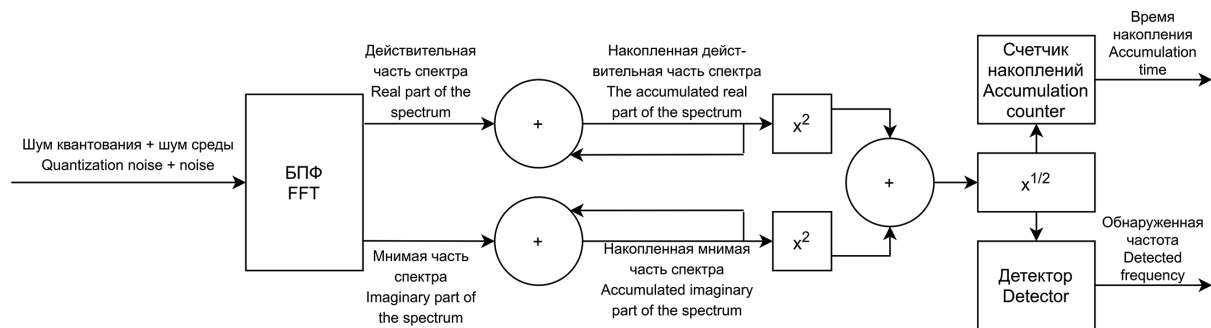


Рис. 3. Блок-схема спектрального обнаружителя информационных параметров
Fig. 3. Block diagram for spectral information parameter detector

В полученном сигнале выполняется поиск максимального элемента, который в спектре шума квантования без аддитивной помехи соответствовал бы его главной гармонике на частоте дискретизации сигнала. Если обнаруженный максимум соответствует частоте дискретизации АЦП, делается вывод о том, что шум квантования накопился и может быть обнаружен над шумами. Постоянная составляющая в виде гармоники на нулевой частоте не учитывается при определении максимума. Записывается количество накоплений, которое потребовалось для выделения гармоники шума квантования при текущем уровне шума среды.

Результаты исследований и их обсуждение

Для подтверждения работоспособности предложенного способа обработки и выделения информационных параметров сигнала и шума квантования проведен имитационный натурный эксперимент, в котором вместо измерительной антенны использовался соединительный кабель, подключенный от выхода ЦАП источника сигнала к аналоговому входу управляемого измерительного АЦП (рис. 4).

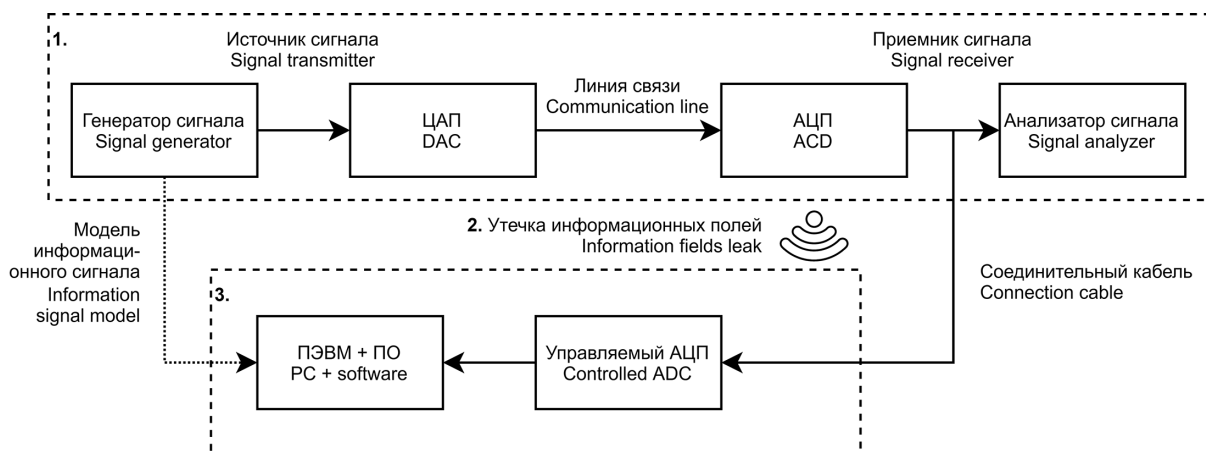


Рис. 4. Блок-схема имитационно-натурного эксперимента
Fig. 4. Block diagram for a simulation-natural experiment

Блок-схема программно-аппаратного комплекса для обработки и выделения информационных параметров сигнала и шума квантования реализована в виде макета для проведения эксперимента (рис. 5).

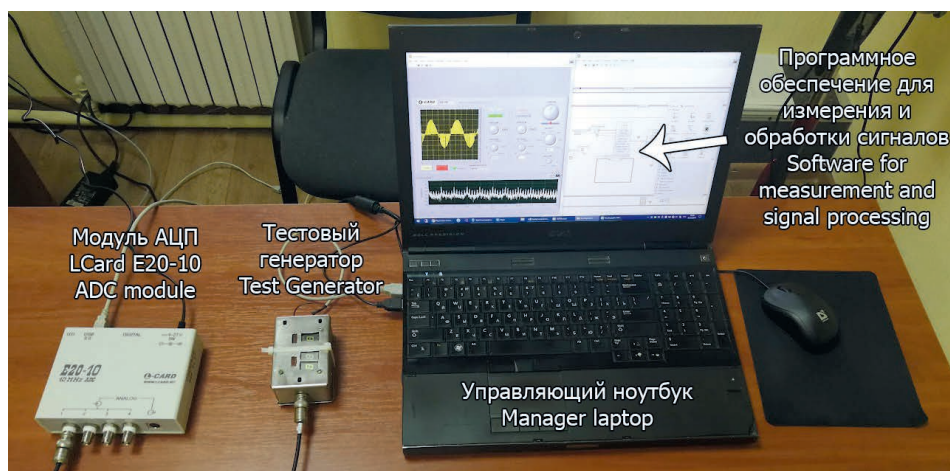


Рис. 5. Макет программно-аппаратного комплекса для обработки и выделения информационных параметров

Fig. 5. The hardware-software complex layout for processing and extracting information parameters

Макет на рис. 5 не предназначен для оценки информационных физических полей АЦП и реализован с целью подтверждения на практике возможности оценки информационных параметров сигнала и шума квантования. Макет включает в себя аппаратную часть и специальное ПО, которое реализует предложенную модель оценки информационных параметров в программной среде LabVIEW. Аппаратная часть включала следующие элементы:

- электронно-вычислительную машину типа ноутбука;
- управляемый модуль АЦП/ЦАП LCard E20-10;
- генератор измерительного сигнала, встроенный ЦАП в ПЭВМ;
- кабель соединительный АЦП-ЭВМ: аналоговый разъем мини-джек (0,5 м);
- кабель управления АЦП/ЦАП USB 2.0 тип А–В, длина 1,5 м;
- внешний источник питания – сетевой адаптер ~220 В.

Эксперимент выполнялся в лаборатории при температуре окружающего воздуха 20 °С. Измерения проводились при изменении количества уровней дискретизации сигнала от 8 ($L = 3$ бита) до 1024 ($L = 10$ бит). Изменение количества уровней дискретизации (разрядности АЦП L) выполнялось программным способом.

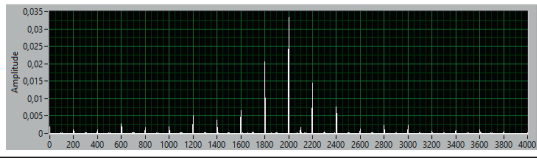
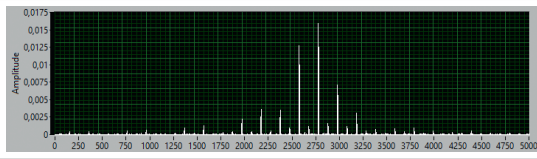
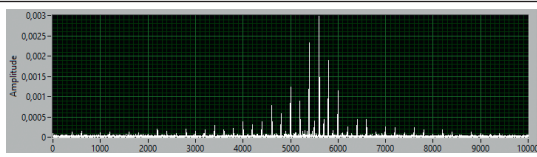
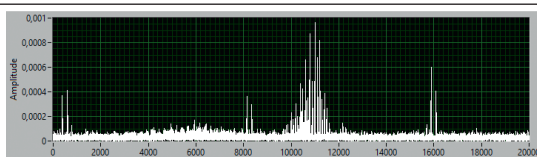
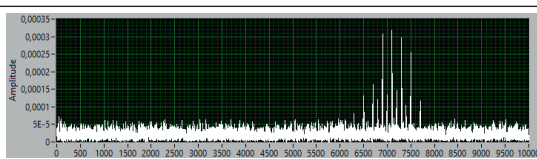
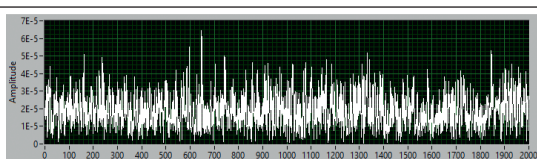
Предельные значения частоты и уровня сигнала устанавливали с помощью параметрической зависимости между влияющими факторами и контролируемыми параметрами как функция многих переменных при 30 повторениях измерения. Более подробное описание обнаружения предельных значений измерений предельных порогов обнаружения приводится в [6]. В табл. 1 представлены результаты обнаружения частоты и уровня шума квантования.

Таблица 1. Результаты обнаружения частоты и уровня шума квантования

Table 1. Frequency and level detection results for quantization noise

Разрядность L / Bit length L	Ожидаемая частота, Гц/ Expected frequency, Hz	Обнаруженная частота, Гц/ Detected frequency, Hz	Уровень шума квантования/ Quantization noise level	Спектр накопленного шума квантования/ Cumulative quantization noise spectrum
3	1600	1600	0,6000	
4	3200	3200	0,1500	

Окончание табл. 1
Ending of Table 1

Разрядность L / Bit length L	Ожидаемая частота, Гц/ Expected frequency, Hz	Обнаруженная частота, Гц/ Detected frequency, Hz	Уровень шума квантования/ Quantization noise level	Спектр накопленного шума квантования/ Cumulative quantization noise spectrum
5	6400	6400	0,0400	
6	12 800	12 800	0,0180	
7	25 600	25 600	0,0050	
8	51 200	51 200	0,0010	
9	102 400	—	0,0005	
10	204 800	—	0,0001	

Приведенные в табл. 1 данные демонстрируют, что обнаружение частоты и уровня шума квантования устойчиво выполняется до $L = 8$ бит. При $L = 9$ бит по спектру сигнала возможно судить о наличии шума квантования, но устойчивого выделения частоты и уровня сигнала не происходит. Для дискретизации при $L = 10$ бит сигнал визуально не наблюдается.

На рис. 6 представлены графики зависимостей среднего количества накоплений для выделения основной гармоники шума квантования из фонового шума от количества уровней дискретизации сигнала, сформированного устройством с разрядностью L . За приемлемое (по критерию времени) количество накоплений возможно оценить лишь некоторые диапазоны ОСШ, при которых гармоники шумов квантования выделяются в пределах 10 итераций.

Анализ рис. 6 показывает, что при увеличении L , которое снижает уровень гармоник шума квантования и повышает их частоту, резко возрастает требуемое для выделения количество накоплений сигнала при аналогичном уровне фонового шума. Добавление 1 разряда эквивалентно увеличению числа уровней квантования в два раза, это вызывает смещение графика на 7–8 дБ в сторону увеличения ОСШ. Например, при исходном ОСШ = -20 дБ сигнал с $L = 5$ в среднем может быть накоплен за восемь раз, а сигнал с $L = 4$ – за один раз.

На рис. 7 представлены графики зависимостей времени накопления шума квантования от ширины полосы фильтра. Ограничение полосы фильтра осуществлялось фильтром с заданной полосой Δf вокруг ожидаемого отсчета смеси.

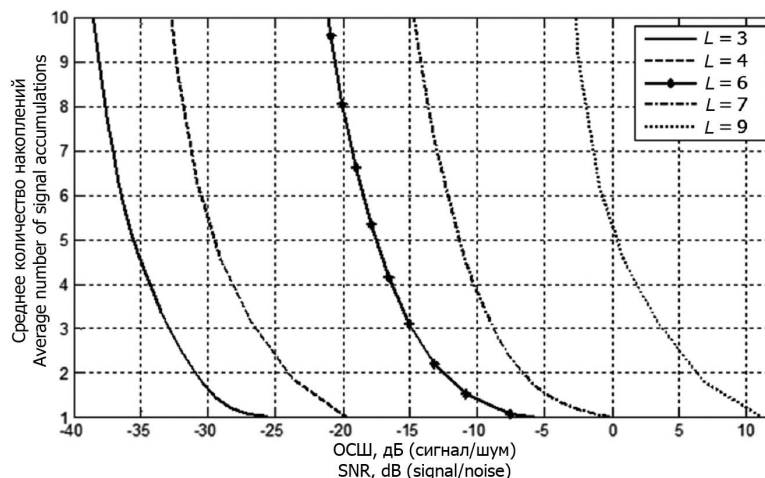


Рис. 6. Зависимость среднего количества накоплений для выделения основной гармонике шума квантования из фонового шума при различной разрядности аналого-цифрового преобразователя L
Fig. 6. Dependence of the accumulations average number for separating the quantization noise first harmonic from the background noise at different of analog-to-digital conversion bit length L

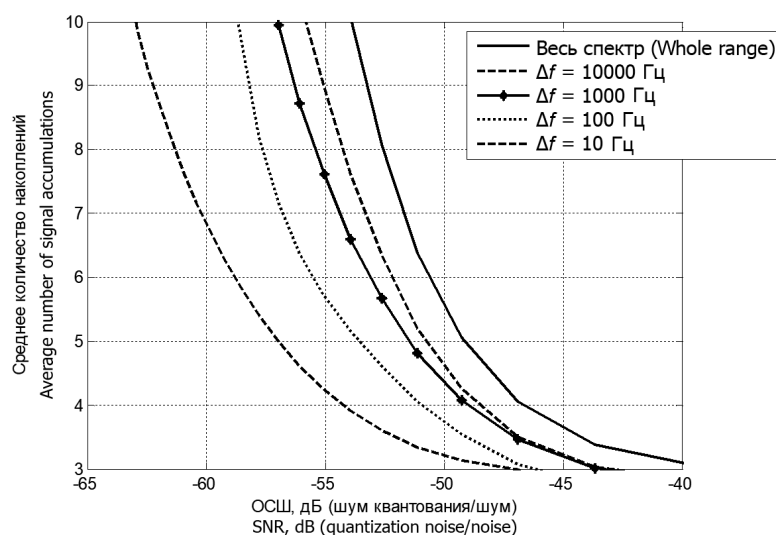


Рис. 7. Зависимость времени накопления шума квантования от ширины полосы фильтра
Fig. 7. Dependence of the quantization noise accumulation time on the filter bandwidth

Из рис. 7 следует, что сужение полосы в 10 раз позволяет уменьшить время накопления на 10–20 %. Это можно заключить из сравнения графиков, например, при ОСШ = -55 дБ. Следовательно, сужение полосы накопленной смеси позволяет уменьшить время выделения шума квантования, что может быть применено на практике перехватчиком сигнала для более быстрого поиска информационных составляющих в шумах при наличии у него сведений о технических характеристиках целевой системы. Это может позволить ему анализировать лишь ограниченную область частотного спектра.

Заключение

1. Разработан макет локальной измерительной схемы, с помощью которого проведен имитационный натурный эксперимент оценки информационных показателей шума квантования аналого-цифрового преобразователя речевого сигнала. В качестве информационных показателей

канала утечки информации использовались частота дискретизации сигнала и амплитуда шума квантования.

2. С помощью макета локальной измерительной схемы выполнен натурный эксперимент, включающий определение параметров информационных составляющих шума квантования в канале утечки информации путем накопления и анализа сигнала. В результате проведения натурального эксперимента подтверждены гипотезы оценки информационных параметров шума квантования, получены численные значения информационных параметров.

3. В результате эксперимента получены зависимости времени накопления от отношения сигнал/шум квантования (фоновый шум) и времени накопления от разрядности аналого-цифрового преобразователя (уровня шума квантования), которые описывают предельные чувствительности и погрешности детектора информационных параметров, зависимости от контролируемых параметров и влияющих факторов. Уточнение предельных значений оценки информационных параметров необходимо исследовать при подключении измерительных антенн.

Список литературы

1. Раханов, К. Я. Обеспечение конфиденциальности информации в сети Интернет / К. Я. Раханов, Н. А. Раханова. Новополоцк: Полоц. гос. ун-т, 2021. 192 с.
2. Железняк, В. К. Защита информации от утечки по техническим каналам / В. К. Железняк. СПб.: Санкт-Петербург. госуд. ун-т аэрокосмич. приборостр., 2006. 188 с.
3. Анализ ошибки равномерного квантования периодической импульсной последовательностью треугольной формы в спектральной области / В. К. Железняк [и др.] // Проблемы инфокоммуникаций. 2022. Т. 15, № 1. С. 39–45.
4. Математическая модель каналов утечки речевых сигналов при дискретно-квантованном представлении / В. К. Железняк [и др.] // Доклады БГУИР. 2020. Т. 18, № 4. С. 89–95. <http://dx.doi.org/10.35596/1729-7648-2020-18-4-89-95>.
5. Железняк, В. К. Оценка разборчивости речи взаимной корреляцией сигнала линейной частотной модуляции в каналах утечки информации / В. К. Железняк, К. Я. Раханов, И. Б. Бураченко // Вестник Полоцкого государственного университета. Серия С, Фундаментальные науки. 2015. № 12. С. 22–27.
6. Раханов, К. Я. Синтез программно-аппаратной системы оценки разборчивости речи методом ЛЧМ-сигнала: результаты эксперимента / К. Я. Раханов // Вестник Полоцкого государственного университета. Серия С, Фундаментальные науки. 2012. № 12. С. 20–26.

References

1. Rakhanov K. Ya., Rakhanova N. A. (2021) *Ensuring the Information Confidentiality on the Internet*. Novopolotsk, Polotsk State University Publ. 192 (in Russian).
2. Zheleznyak V. K. (2006) *Protecting Information from Leaks Through Technical Channels*. Saint Petersburg, Saint Petersburg State University of Aerospace Instrumentation Publ. 188 (in Russian).
3. Zheleznyak V., Rakhanov K., Lavrov S., Adamovskiy Y., Kharchenko S., Filippovich A., Baranovsky M. (2022) Analysis of the Uniform Quantization Error of a Triangular Periodic Pulse Sequence in the Spectral Domain. *Problemy Infokommunikacij = Infocommunication Problems*. 15 (1), 39–45 (in Russian).
4. Zheleznyak V. K., Lavrov S. V., Baranouski M. M., Filipovich A. G. (2020) Mathematical Model of Speech Signal Leakage Channels During Discrete-Quantified Conversion. *Doklady BGUIR = BSUIR Reports*. 18 (4), 89–95. <http://dx.doi.org/10.35596/1729-7648-2020-18-4-89-95> (in Russian).
5. Zheleznyak V. K., Rakhanov K. Ya., Burachenok I. B. (2015) Estimation of Legibility of the Speech by Mutual Signal Correlation of Linear Frequency Modulation in Channels of Information Leakage. *Vestnik Polotskogo Gosudarstvennogo Universiteta. Seriya C, Fundamental'nye Nauki = Herald of Polotsk State University. Series C. Fundamental Sciences*. (12), 22–27 (in Russian).
6. Rakhanov K. Ya. (2012) Synthesis of Software and Hardware Systems Speech Estimation by LFM-Signal: Experimental Results. *Vestnik Polotskogo Gosudarstvennogo Universiteta. Seriya C. Fundamental'nye Nauki = Herald of Polotsk State University. Series C, Fundamental Sciences*. (12), 20–26 (in Russian).

Вклад авторов / Authors' contribution

Все авторы внесли равный вклад в написание статьи / All authors have equally contributed to the writing of the article.

Сведения об авторах

Железняк В. К., д. т. н., профессор Полоцкого государственного университета имени Евфросинии Полоцкой

Раханов К. Я., к. т. н., доцент кафедры вычислительных систем и сетей Полоцкого государственного университета имени Евфросинии Полоцкой

Адамовский Е. Р., магистр, аспирант кафедры вычислительных систем и сетей Полоцкого государственного университета имени Евфросинии Полоцкой

Адрес для корреспонденции

211440, Республика Беларусь,
г. Новополоцк, ул. Блохина, 29
Полоцкий государственный университет
имени Евфросинии Полоцкой
Тел.: +375 33 387-46-89
E-mail: e.adamovsky@psu.by
Адамовский Егор Русланович

Information about the authors

Zheleznyak V. K., Dr. of Sci. (Eng.), Professor of the Euphrosyne Polotskaya State University of Polotsk

Rahanov K. Ja., Cand of Sci., Assistant Professor at the Department of Computing Systems and Networks of the Euphrosyne Polotskaya State University of Polotsk

Adamovskiy Y. R., Master's Student, Postgraduate at the Department of Computing Systems and Networks of the Euphrosyne Polotskaya State University of Polotsk

Address for correspondence

211440, Republic of Belarus,
Novopolotsk, Blokhina St., 29
Euphrosyne Polotskaya
State University of Polotsk
Tel.: +375 33 387-46-89
E-mail: e.adamovsky@psu.by
Adamovskiy Yahor Ruslanovich