IRSTI 20.53.19

10.51889/2959-5894.2023.84.4.009

G. Martyniuk[1], B. Yagaliyeva [2,3], K. Makulov[2], B. Akhmetov[2]*

[1]Mariupol State University, Kyiv, Ukraine
[2]Caspian University of Technology and Engineering named after Sh. Yessenov, Aktau, Kazakhstan
[3] Kazakh National Research Technical University named after K. Satbayev, Almaty, Kazakhstan
**e-mail: bagdat.yagaliyeva@gmail.com*

ANALYSIS OF THE QUALITY OF NOISE GENERATORS

Abstract

A noise signal is a set of simultaneously existing electrical oscillations, the frequencies and amplitudes of which are random. As a rule, it is impossible to trace any regularity in the change in the instantaneous values of the noise. At the same time, such signals have certain probabilistic characteristics. The authors set themselves the task of assessing the quality of acoustic noise generators using various methods: determining the noise quality factor using asymmetry and kurtosis coefficients; determination of the entropy quality factor; determination the entropy coefficient of the quality of the distribution of the envelope of the noise signal. To assess the quality of the generators, an acoustic noise generator, which is used to protect acoustic information in the office, was taken as a control sample. It is also proposed to use a generator created with Python software using a pseudo-random sequence. Based on the results of the work, a conclusion was made about the use of the proposed methods for assessing the quality of noise signal generators.

Keywords: noise generator, noise quality factor; pseudo-random sequence generator; pink noise; entropy coefficient of quality; envelope noise signal.

А. Мартынюк[1], Б. Ягалиева[2,3], К. Макулов[2], Б. Ахметов[2]
[1.]Мариуполь мемлекеттік университеті, Киев қ., Украина
[2.]Ш.Есенов атындағы Каспий технологиялар және инжиниринг университеті, Ақтау қ., Қазақстан
[3.]Қ.Сәтбаев атындағы Қазақ ұлттық зерттеу техникалық университеті, Алматы қ., Қазақстан

ШУ ГЕНЕРАТОРЛАРЫНЫҢ САПАСЫН ТАЛДАУ

Аңдатпа

Шу сигналы – жиіліктері мен амплитудалары кездейсоқ болатын бір уақытта болатын электр тербелістерінің жиынтығы. Әдетте, шудың лездік мәндерінің өзгеру заңдылығын байқау мүмкін емес. Сонымен қатар, мұндай сигналдардың белгілі бір ықтималдық сипаттамалары бар. Авторлар әртүрлі әдістерді қолдана отырып, акустикалық шу генераторларының сапасын бағалау міндетін қойды: ассиметрия және куртоздық коэффициенттерді пайдалана отырып, шу сапасының коэффициентін анықтау; энтропияның сапа коэффициентін анықтау; шу сигналының қабықшасының таралу сапасының энтропия коэффициентін анықтау. Генераторлардың сапасын бағалау үшін бақылау үлгісі ретінде акустикалық шу генераторы алынды, ол кеңседегі акустикалық ақпаратты қорғау үшін қолданылады. Сондай-ақ псевдокездейсоқ тізбекті пайдаланып Python бағдарламалық жасақтамасымен жасалған генераторды пайдалану ұсынылады. Жұмыс нәтижелері бойынша шу сигналының генераторларының сапасын бағалаудың ұсынылған әдістерін қолдану туралы қорытынды жасалды.

Түйін сөздер: шу генераторы, шу сапасының коэффициенті; псевдокездейсоқ реттілік генераторы; қызғылт шу; сапа энтропия коэффициенті; шу сигналының конверті.

А. Мартынюк[1], Б. Ягалиева[2,3], К. Макулов[2], Б. Ахметов[2]
[1]Мариупольский государственный университет, Киев, Украина
[2]Каспийский университет технологий и инжиниринга имени Ш.Есенова, г.Актау, Казахстан
[3]Национальный исследовательский технический университет им. К.Сатбаева, г.Алматы, Казахстан

АНАЛИЗ КАЧЕСТВА РАБОТЫ ГЕНЕРАТОРОВ ШУМА

Аннотация

Шумовой сигнал – это совокупность электрических колебаний, частоты и амплитуды, которые одновременно существуют и носят случайный характер. Как правило, шумовые сигналы характеризуются тем, что невозможно проследить закономерности в их значениях. Однако стоить отметить, что в таких сигналах все же можно выделить некоторые закономерности. Авторы поставили перед собой задачу оценить качество акустических генераторов шума, используя различные методики: определения коэффициента качества шума с использованием коэффициентов асимметрии и эксцесса; определения энтропийного коэффициента качества; определения энтропийного коэффициента качества распределения огибающей шумового сигнала. Для оценки качества генераторов в качестве контрольного образца был взят генератор акустического шума, который используется для защиты акустической информации в офисе. Также предложено использовать генератор, созданный с помощью программного обеспечения Python при помощи псевдослучайной последовательности. По результатам работы сделан вывод об использовании предложенных методик для оценки качества генераторов шумового сигнала.

Ключевые слова: генератор шума, коэффициент качества шума; генератор псевдослучайной последовательности; розовый шум; энтропийный коэффициент качества; огибающая шумового сигнала.

Introduction

The problem of protection and processing of speech information is one of the information security problems. In today's world, with increasing volumes of processed data, the amount of speech information in institutions and enterprises is also growing, in the process of holding various meetings, conferences etc. At Fig. 1 is represented acoustic information leakage channels.

A common feature of the appearance of these channels is the influence of acoustic signals. Thus, you can simply listen to acoustic signals by placing a listening device in the air duct, or remove window vibrations from an acoustic signal using a vibration sensor.

Understanding that acoustic, and even more speech information, can be captured by various devices and is the main source of information leakage, the problem of protecting such information remains relevant. In accordance with the general methods of information security, the following methods are used to protect against eavesdropping [1-2]:

- structural camouflage
- energy hiding.

Structural camouflage can be implemented in the following ways:

- encryption of semantic information in functional communication channels;
- of electrical and radio signals' technical closure through telephone channels;
- disinformation.

Energy hiding can be implemented with:

- sound insulation of the acoustic signal;
- absorption of sound of acoustic waves;
- noisy room with other sounds (noise, interference), which provides masking of acoustic signals;
- detection, localization and extraction of embedded devices.

In this work, the authors decided to investigate noise generators placed in the room to prevent the detection of speech information.

To prevent information leakage during meetings, it is necessary to provide guaranteed information protection, which can be organized using active means, for example, using masking noise generators. A large number of works are devoted to the development and research of various methods for processing and protecting speech information, as well as determining the intelligibility of speech messages as the main indicator of their security, for example [1-6]. However, it must be remembered that a noisy informative signal can be filtered, and in case of poor-quality masking, an attacker will gain access to protected information. Therefore, there is a problem associated with assessing the quality of the noise signal generated by active protection means.

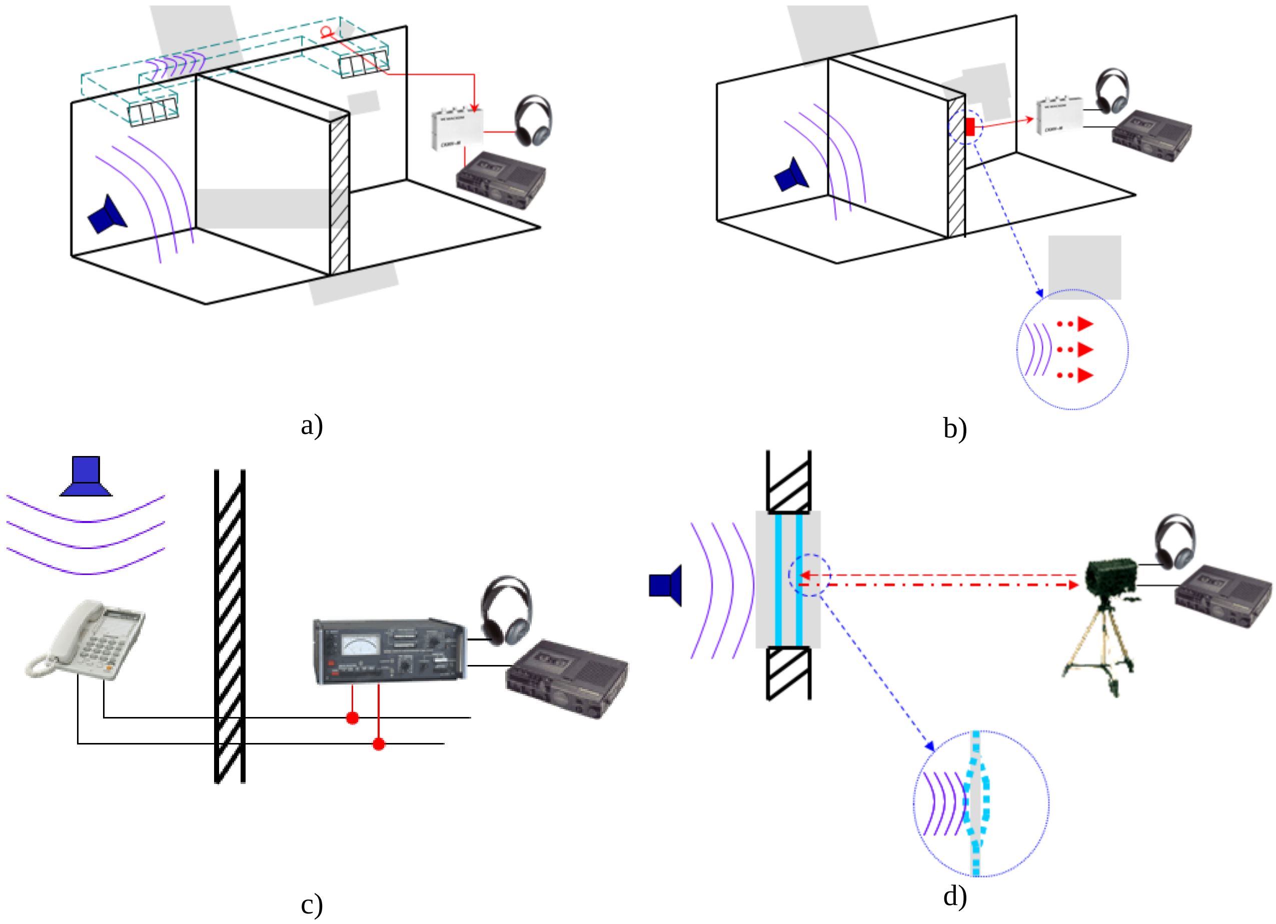

Fig. 1. Examples of acoustic information leakage channels:
a) acoustic; b) vibroacoustic; c) acoustoelectric; d) laser

There are three general trends in the development of such generators. The first trend is the use of feedback to control the spectrum of the noise signal and its level, which is selected depending on the level of the acoustic signal that needs to be masked. The second trend is the creation of a closed communication chain for conversations between negotiators. It is implemented either by encrypting conversations transmitted in a space isolated from the surrounding acoustic environment, or by using special interference outside this space, which does not allow the removal of intelligible acoustic information outside it. The third trend is the use of mixed noise, which consists of soft music, noise and voice signals of several participants in a conversation, shifted in time and inverted in spectrum. Such a mixture of signals does not allow you to remove an intelligible conversation signal. Even if you record a disguised conversation and clean it up with currently known methods, it is impossible to get intelligible signals. With this method of masking, the level of interference emitted into the premises is significantly lower than the noise level emitted when using a conventional generator.

It is crucial to choose the right noise generator for your application. Depending on the application, you may need a generator that produces noise in a specific range of frequencies: white, pink or brown noises. The power of the output signal can be crucial. Also it is essential that the noise generator maintains a constant level of noise over an extended period of time.

Effective confidential information protection using masking noise generators is an important task that use government and commercial institutions. However, there is no unified approach today to assess the quality of masking noises and the existing methods need to be seriously improved.

Information [7, 8] and energy [9, 10] criteria are used to determine the masking noise's estimated characteristics. The first group of criteria takes into account the statistical parameters of the noise signal in the time domain and enables the determination of the digital noise quality factor. Based on mathematical expectation, calculation of variance and entropy of current sample values and their envelope, the degree of approximation of some reference distributions is calculated. Such methods aim to find the degree of uncertainty of the current values of the expressed noise signals, for example, through the entropy quality factor of the masking noise.

The criteria of the second group for guaranteed information protection use the postulate of the need to overcome the noise energy by means of a masked signal. That is why integral indicators are used to check the quality of noise, which take into account the excess level of noise in relation to the level of the information signal. For example, the entire frequency range of noise masking can be divided into several octave bands, in the middle frequencies of each of which the noise level is measured [9].

From the point of view of the energy efficiency of creating masking noise, as well as the direct determination of their probable properties, informative criteria are of the greatest interest.

Research Methodology

Before presenting methods for determining noise quality factors, it is necessary to analyze information about pink noise used in generators to mask information.

Pink noise (flicker noise) is noise whose spectral density changes with frequency *f* according to the *1/f* law. This ensures that the interfering signal has the same energy per octave. Sometimes pink noise is any noise whose spectral density decreases with decreasing frequency (Fig. 2).

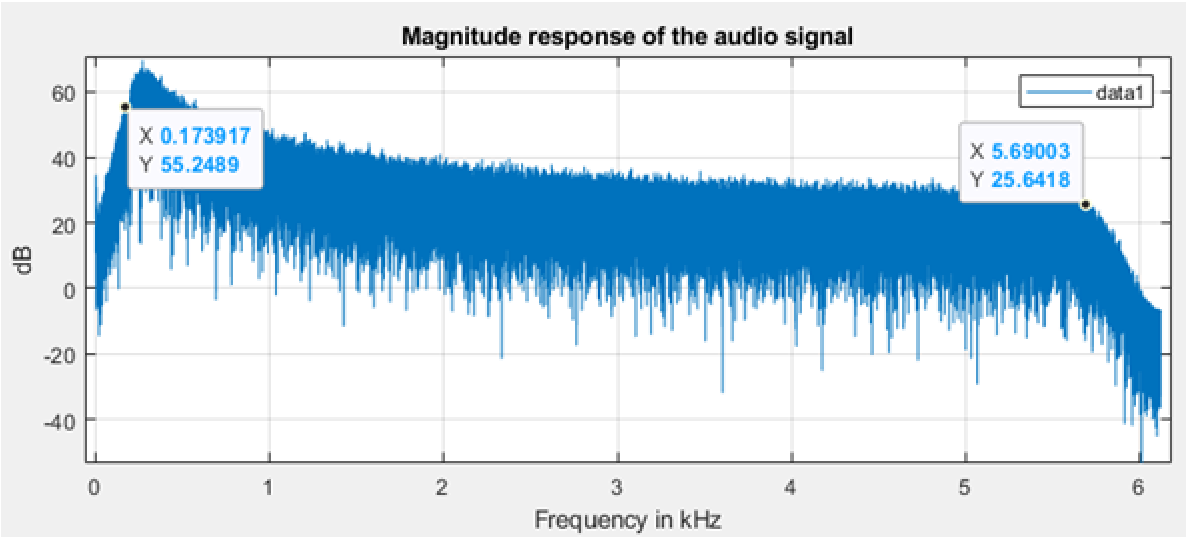

Fig. 2. Graph of the spectral density of the noise signal in the range of 180–5600 Hz

Therefore, pink noise is characterized by the constancy of energy within each octave of frequency change. This means that the spectral density decreases with increasing frequency according to the logarithmic law. Such noise is widespread in nature and many random processes obey it.

The following are the various techniques described in the literature for characterizing the quality of acoustic noise emitted by generators.

Method for determining the noise quality factor using the skewness and kurtosis coefficients.

This technique was developed to assess the quality of the electromagnetic noise field, however, the authors made an attempt to use it for pink noise generators, which are used to actively mask the speech signal. The methodology is as follows [7]:

1. Obtaining a sample of the noise signal in discrete form.
2. Determination of means m_1 of the obtained sample.
3. Calculation of the second m_2, third m_3 and fourth m_4 central moments.

4. Determination of the calculated values of the skewness $\gamma_a = \frac{m_3}{\sqrt{m_2^3}}$ and kurtosis coefficient $\gamma_e = \frac{m_4}{m_2^2} - 3$ of study sample.

5. Determination of the noise quality factor by the formula

$$\Theta = 1.06987 + 3\gamma_e - 1.56\ln\left(e^{2\gamma_e} + 0.037e^{0.23e^{3.43|\gamma_a|}}\right)$$

The following techniques are reduced to a series of computational operations performed on the quantized measured values of the electrical signal into which the masking noise is converted. The basis of these methods is a calculation of degree of uncertainty of the law of distribution of the masking noise's instantaneous values, as well as the entropy of the distribution law of the envelope values of the noise signal.

The papers [9-13] introduce the concept of entropy noise quality factor. These coefficients are calculated according to certain reference distribution laws. Under the restrictions imposed on the mean power, the standard distribution law for instantaneous values of masking noise is normal. At the same time, for the envelope of normally distributed instantaneous values of the masking noise, the reference law is the Rayleigh distribution.

Method for determining the entropy quality factor.

In a number of works [12, 13], instead of finding the noise quality factor described above, it is proposed to find the entropy noise quality factor. Entropy makes it possible to evaluate the masking properties of interfering signals, regardless of the specific methods of their reception and processing. The task of choosing the most effective interference is reduced to determining such a distribution of interference, in which, for given statistical properties of the signal, the reproduced information by means of technical intelligence would be minimal.

The entropy calculation is reduced to constructing a histogram of the probability density distribution $p(x_i)$, after which it is necessary to use the formula

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log(p(x_i)), \qquad (1)$$

where $p(x_i)$ - the probability of a sample element falling into the *i*-th range of the histogram, *n* is the number of histogram ranges.

The entropy noise quality factor is found by the formula

$$\gamma = \frac{e^{2H(x)}}{2\pi e}. \qquad (2)$$

Method for determining the entropy coefficient of the quality of the distribution of the envelope of the noise signal. This technique is similar to the previous one, but the entropy is found not for the sample of the noise generator, but for the sample of the envelope of the noise generator, which must be subject to the Rayleigh distribution. The algorithm for determining the quality factor is as follows [4]:

1. Finding the envelope of the noise signal by the formula

$$A(t) = \sqrt{s(\mathrm{t})^2 + s_{\perp}(t)^2},$$

where $s_{\perp}(t)$ - coupled (according to Hilbert) function, which is defined as the imaginary part of the analytical signal

$$\dot{s}_a(t) = s(t) + is_{\perp}(t).$$

2. Construction of a histogram of the distribution law of the envelope noise signal.
3. Finding the entropy of the distribution law of the envelope by formula (1).
4. Finding the parameter of the standard Rayleigh distribution *r* by the formula

$$\frac{\mu_2^0}{2r^2} + \ln r = M\left[\ln x\right] + 1 + \frac{\gamma}{2} - \ln\sqrt{2},$$

where μ_2^0 - the second moment of the distribution law of the noise signal envelope; $M\left[\ln x\right]$ - the mean of the natural logarithm of the values of the envelope of the noise signal, γ - Euler constant.

5. Finding the entropy of the standard Rayleigh distribution using the formula $\hat{H} = 1 + \frac{\gamma}{2} + \ln\left(\frac{r}{\sqrt{2}}\right)$

6. Finding the entropy quality factor of the distribution of the envelope of the noise signal by the formula $\eta = e^{H_0 - \hat{H}}$.

Research results

The results are also shown for each considered technique separately.

Method for determining the noise quality factor using the skewness and kurtosis coefficients. According to this technique, the noise quality factor should be in the range from 0.8 to 1.0. The authors conducted experimental studies with pink noise generators of various brands, and also conducted an experiment on generators built using a pseudo-random sequence of numbers implemented in the Python software environment. The results for all 10 s samples (441,000 samples) gave the noise quality factor results shown in Table 1.

Table 1. Estimated indicators of noise quality factor using skewness and kurtosis coefficients

Noise generator	***Skewness coefficient***	***Kurtosis coefficient***	***Noise quality factor***
Brand generator	*0.0119*	*-0.1219*	*0.9936*
Created from a pseudo-random sequence	*-0.0089*	*-0.6998*	*0.8823*

As can be seen from Table. 1, this technique has shown that it is possible to use in practice both branded generators of different brands, and a noise signal obtained from a pseudo-random sequence of numbers.

Method for determining the entropy quality factor. Entropy noise quality factor should not exceed 1. However, in the course of research with different pink noise generators, the authors made sure that, using formula (1) to find the entropy, the entropy quality factor exceeds unity hundreds of times, which makes it impossible to use this formula. Therefore, it was decided to use a different formula to find the entropy.

Considering that pink noise generators were used in the study, it should be noted that pink noise obeys the normal distribution law. This was confirmed by finding a histogram for noise generators (Fig. 3). It should also be noted that the obtained histogram results are the same for all generators used in the experiments.

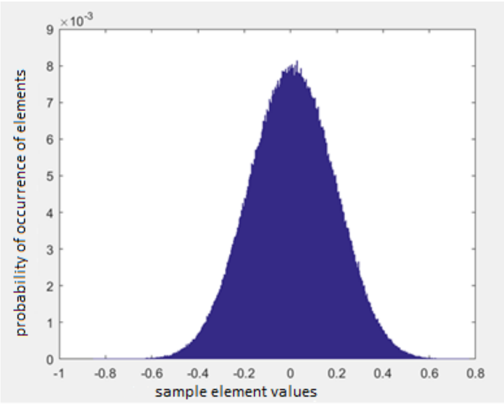

Fig. 3. Histogram of the noise generator

In this regard, it was decided to replace the entropy according to formula (1) by finding the entropy for the normal Gaussian distribution, which has the form

$$H(x) = \ln\left(\sqrt{2\pi e\sigma^2}\right), \tag{3}$$

where σ^2 - sample variance.

Using formula (3) to find the entropy noise factor, the authors obtained the results shown in Table 2.

Table 2. Results of determining the entropy noise quality factor

Noise generator	***Entropy coefficient***	***Average signal power***	***Signal quality factor***
Brand generator	*0.0534*	*0.0533*	*1.0*
Created from a pseudo-random sequence	*0.2118*	*0.2118*	*1.0*

As can be seen from Table. 2, the entropy coefficient is equal to 1 for all types of generators used in the experiment. It should be noted that the authors also changed the sample length (signal duration), changed noise levels and quantization levels, but the results of finding the entropy coefficient of signal quality were always in the range of 0.99-1.0.

Thus, we can conclude about the inefficiency of using the technique for determining the entropy noise quality factor in practice.

Method for determining the entropy coefficient of the quality of the distribution of the envelope of the noise signal. It should be noted that when using formula (1) to find the entropy coefficient by this method, the entropy coefficient was in the range of 0.01-0.02. However, these results are not true.

Therefore, the authors decided instead of using formula (1) to use the formula for finding the entropy of the Rayleigh distribution:

$$H = 1 + \ln\left(\frac{\sigma}{\sqrt{2}}\right) + \frac{\gamma}{2},$$

where σ - standard deviation, $\gamma \approx 0,57721566490153286060$ - Euler constant.

After a series of experiments using this method, the authors obtained the results shown in Table 3.

Table 3. Results of finding the entropy quality factor of the distribution of the signal envelope of the noise generator

Noise generator	***Entropy of the envelope***	***Entropy of the Rayleigh reference distribution***	***Entropy quality factor***
Brand generator	*1.0059*	*0.8661*	*1.15*
Created from a pseudo-random sequence	*0.3124*	*0.8661*	*0.5748*

As can be seen from the obtained results, the method for estimating the entropy quality factor of the noise signal envelope distribution is the only method that gives different results for different types of noise generators and requires further statistical development to determine the interval responsible for the adequate operation of noise generators.

Discussion

After analyzing the currently existing methods for assessing the noise quality factor, the authors came to the conclusion that they need to be improved. In addition, the authors believe that for a more detailed assessment of the masking features of pink noise generators, it is not enough to find only the noise quality factor. It is also necessary to introduce other estimates for a more detailed justification of the expediency of using one or another pink noise generator in practice.

Conclusions

According to the results obtained in the work, the following conclusions can be drawn.

- Various techniques for determining noise quality factors for pink noise generators are considered.
- Practical results are given for each considered method.
- Conclusions are drawn about the expediency of using each of the methods.

References:

1 Blintsov, Volodymyr and Nuzhniy, Sergey and Kasianov, Yurii and Korytskyi, Viktor, Mathematical Model of the System of Active Protection Against Eavesdropping of Speech Information on the Scrambler Generator (May 11, 2020). EUREKA: Physics and Engineering, (3), 11-22, 2020. doi: 10.21303/2461-4262.2020.001241, Available at SSRN: https://ssrn.com/abstract=3753538.

2 C. Wang et al., "mmPhone: Acoustic Eavesdropping on Loudspeakers via mmWave-characterized Piezoelectric Effect," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, 2022, pp. 820-829, doi: 10.1109/INFOCOM48880.2022.9796806.

3 Prokof'ev M., Kulish V., Vaschenko M., Dvorskyi V., Stechenko V., Todorenko A. (2015) Otsiniuvannia koeficienta iakosti shumovoi zavady v systemah aktyvnoho zakhystu informatsii [Evaluation of the quality coefficient of noise interference in active information protection systems] Legal, regulatory and metrological support of information security system in Ukraine, Vol. 1 (29), p. 15-20. (in Ukrainian)

4 Zhelezniak V.K. (2006). Zaschita informatcii ot utechki po tekhnicheskim kanalam: uchebnoe posobie [Protection of information from leakage through technical channels: textbook], 188 p. (in Russian)

5 Gavrilov I.V. (2015) Metodika otsenivaniia kachestva maskiruiuschego shuma [Techniques for estimating the quality of masking noise], Trudy SPIIRAN, Vol. 6 (43), p. 179-190. (in Russian)

6 Horev A.A. (2012). Sposoby zaschity obektov informatixatsii ot utechki po tekhnicheskim kanalam: prostranstvennoe magnitnoe zashumlenie [Ways to protect informatization objects from information leakage through technical channels: spatial electromagnetic noise], Spetsialnaia tehnika, Vol. 6, p. 37-57. (in Russian)

7 Dvoriankin S.V., Makarov Yu.K., Horev A.A. (2007). Obosnovanie kriteriev zaschity pechevoi informatsii ot utechki po tehnicheskim kanalam [Justification of the criteria for the effectiveness of the protection of speech information against leakage through technical channels], Zaschita informatsii. Insaid, Vol. 2, p. 18-25. (in Russian)

8 Martyniuk G., Onikiienko Yu., Scherbak L. (2016). Analysis of the Pseudorandom Number Generators by the Metrological Characteristics. Eastern-European Journal of Enterprise Technologies, 1(9), 25-30.

9 Kozlachkov S.B. (2011). Dopolnitelnye kriterii otsenki zaschischennosti rechevoi informatsii [Additional criteria for assessing the protection of speech information], Spetstehnika i sviaz, Vol. 2, p. 44-47. (in Russian)

10 Tupota V.I. A method of assessing the quality of masking frequency-modulated noise interference // RF Patent No. 2346390. 2009. Byul. No. 4. 6 p. (in Russian)

11 O. Yudin, R. Ziubina, S. Buchyk, O. Bohuslavska and V. Teliushchenko, "Speaker's Voice Recognition Methods in High-Level Interference Conditions," 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019, pp. 851-854, doi: 10.1109/UKRCON.2019.8879937.

12 H. Purwins, B. Li, T. Virtanen, J. Schlüter, S. -Y. Chang and T. Sainath, "Deep Learning for Audio Signal Processing," in IEEE Journal of Selected Topics in Signal Processing, vol. 13, no. 2, pp. 206-219, May 2019, doi: 10.1109/JSTSP.2019.2908700.

13 Kupriianov A.I., Saharov A.V. (2007). Teoreticheskie osnovy radioelektronnoi borby [Theoretical foundations of electronic warfare], 470 p. (in Russian)