UDC 004.942:534.231:621.391.825
DOI: 10.15587/2312-8372.2019.185133

**Blintsov V.,
Nuzhniy S.,
Kasianov Yu.,
Korytskyi V.**

DEVELOPMENT OF A MATHEMATICAL MODEL OF SCRAMBLER-TYPE SPEECH-LIKE INTERFERENCE GENERATOR FOR SYSTEM OF PREVENT SPEECH INFORMATION FROM LEAKING VIA ACOUSTIC AND VIBRATION CHANNELS

Захист мовної інформації відноситься до основних задач інформаційної безпеки і є ознакою відповідального відношення організації (фірми) як до своїх інформаційних ресурсів, так і поваги до партнерів. Об'єктом дослідження є процеси захисту мовної інформації від витоку акустичними та вібраційними технічними каналами на об'єктах інформаційної діяльності. Виключною рисою таких об'єктів є циркуляція, обробка та обговорення питань, що містять інформацію обмеженого доступу, в тому числі й державну таємницю. Особливістю України є вимога про застосування на таких об'єктах виключно технічних засобів, що пройшли відповідну сертифікацію.

Основою системи постановки активної шумової завади є генератор шуму. При цьому, одним з найбільш проблемних питань є те, що в Україні дозволені до використання тільки генератори шумової завади типу «білий» шум та його клони. Системи мають ряд значних недоліків – низький рівень захищеності перехоплених мовних сигналів від фільтрації шуму (завади), значний рівень шуму в приміщеннях, які підлягають захисту, та інші.

Запропоновано структурну схему генератора завади. А також розроблено та досліджено в середовищі Matlab її математичну модель. В ході дослідження проведено порівняльний аналіз вхідних та синтезованих генератором сигналів, досліджені їх тимчасові та спектральні характеристики. Отримані результати свідчать про високу ефективність запропонованого методу захисту мовної інформації. Це пов'язано з тим, що метод формування мовоподібної завади має ряд особливостей, які забезпечують значний деструктивний вплив на мовну інформацію, а саме використання моделі комбінованого скремблера з тимчасовими та частотними перетвореннями. Метод враховує використання динамічних ключів, для систем кодування, та підключення сторонніх джерел мовних сигналів, а також закільцьовування (змішування вхідного та вихідного сигналів) на вході блоку скремблювання. Таке рішення унеможливлює ре-інжиніринг.

Отримані результати підтверджені дослідженням експериментального зразка. Проведено порівняння деструктивного впливу типових шумових завад («білий» шум та його клони) і шумової завади, створеної запропонованим методом, за критерієм залишкова словесна розбірливість мови диктора. Дослідження показали, що, за умови забезпечення не більше 10 % рівня залишкової розбірливості, рівень гучності вихідного сигналу генератора шумової завади можна знизити майже на 6 дБА.

Ключові слова: *генератор мовоподібної завади скремблерного типу, захист мовної інформації, інформаційна безпека.*

Received date: 21.06.2019
Accepted date: 12.07.2019
Published date: 31.10.2019

1. Introduction

Protection of speech information from leakage by acoustic and vibration channels in Ukraine occurs in accordance with legislative [1–3] and regulatory documents and includes three groups of measures:

– organizational;
– organizational and technical;
– technical.

An analysis of the requirements [4–6] shows that the best information protection indicators for speech information are integrated information protection systems (IIPS), which are built on the basis of systems for setting active vibration and acoustic noise (SSAVAN). According to [7, 8], Ukraine has passed certification and is allowed for use at the information activity facilities (IAF) separately and as part of the IIPS, there are seven types of SSAVAN systems:

1) technical protection complex of the MARS-TPC facility (noise signal generators MARS-TPC-4-2 manufactured in Ukraine);

2) vibration and acoustic information protection complex «SKELIA-2» manufactured in Ukraine;

3) active information protection complex «RIAS-AP» (devices «RIAS-2C», «RIAS-2M» manufactured in Ukraine);

4) active information protection complex «Topaz-4» (acoustic noise generator «Topaz ANG-4» manufactured in Ukraine);

5) active information protection complex «Basalt-4» (protection device «Basalt-4GA» manufactured in Ukraine);

6) Audio information protection system «Druid» (DNG-2300 digital noise generator made in Germany);

7) information vibration-acoustic information protection device «OTsZI-VA» manufactured in Ukraine.

As well as a specialized mobile facility – Mobile soundproof phone booth «MTB-01» manufactured in Ukraine.

The main technical characteristics of such systems include the number of output channels (usually 1 or 2) and the initial electrical power or the permissible number of typical emitters per channel (from 8 to 24 pcs.). In all systems, «white» noise generators (or its clones) are used as a noise generator.

However, as analysis [9–11] shows, the use of «white» noise and its clones has a significant drawback – the use of modern systems for digital processing of phonograms can significantly reduce the level of noise interference in the phonogram. And in [12–14] methods of digital processing of digital phonograms, including wavelet transform and correlation analysis, are presented. The informational composition of the intercepted message is substantially restored by the use by an attacker of multi-point «removal» of information from structural elements [15, 16] – this is possible, since several emitters connected to the same channel are used in SSAVAN. This situation discredits IIPS, however, at present in Ukraine there are no methods and technologies that would satisfy modern requirements for the protection of speech information. A mandatory requirement for SSAVAN is their resistance to modern and advanced methods of digital processing of phonograms in order to filter and restore intercepted voice messages.

Thus, there is an urgent need to develop an improved method for generating an interference noise signal for SSAVAN. The method should be integrated into the structure and operating principles of existing IIPS and be able to take into account modern and promising methods of digital processing of phonograms.

Thus, the development of a method for generating acoustic and vibrational interference, which creates a significant destructive effect on the speech signal and is resistant to filtering by modern methods and means of digital processing of phonograms, is relevant.

2. The object of research and its technological audit

The object of research is the process of protecting speech information from leakage by acoustic and vibrational technical channels at the objects of information activity. A feature of such objects is the circulation, processing and discussion of issues containing information of limited access, including state secrets.

To date, methods and technical tools have been created designed to ensure the protection of speech information in specially designated rooms – meeting rooms, offices of responsible employees, middle and senior managers and more.

In Ukraine and the world, technologies are used in which the protection of speech information is provided by passive means (sound insulation, sound absorption, etc.) and systems for setting active noise interference. At the same time, for objects processing information containing state secrets, the use of active speech information protection systems is mandatory. A peculiarity of Ukraine is the requirement to use exclusively technical means that have passed the relevant certification at such facilities.

The basis of the active noise jamming system is a noise generator. One of the most problematic places is that in Ukraine only noise interference generators of the «white» noise type and its clones are allowed to be used. *The systems have a number of significant drawbacks* – a low protection level of intercepted speech signals from noise filtering (interference), a significant noise level in protected rooms, and others.

Currently, protection methods and technologies based on the use of speech-like noises created from the language of speakers and/or manipulations with it have been developed. The most widely used methods are «language choir» («crowd noise») and frequency-time conversions (frequency and temporal reverberation). Such methods have a significantly higher level of destructive effects on the protected signal. However, *one of the most problematic places is* methodology (digital processing of the phonogram of the intercepted signal allows to restore (filter) a dangerous signal) and low resistance to re-engineering («splitting» the crowd into separate speakers).

3. The aim and objectives of research

The aim of this research is improvement of the method of generating a noise signal for systems for setting active vibration and acoustic noise.

To achieve the aim, the following objectives are set:

1. To develop a generalized diagram of a scrambler-type speech-like signal generator.
2. To develop and research a simplified mathematical model of a speech-like signal generator.
3. To carry out the verification procedure of the results of mathematical modeling of a simplified mathematical model of a speech-like signal generator.

4. Research of existing solutions of the problem

The main advantages of «white» noise and its clones over other types of noise are their spectral density and ease of implementation. This led to their widespread use in all active jamming systems. However, the development of methods for filtering and restoring information messages led, first in radio-telecommunication systems, and then in other areas related to the transmission of information messages, to the failure of «white» noise.

Other types of noise that are currently being considered as a substitute for white noise and its clones are speech-like noises:

- created on the basis of the speaker's speech, which is currently in the controlled area;
- created on independent of the speaker, is currently in the controlled area, speech signals.

The use of speech-like noise as the basis for creating speech information protection systems is based on work that was carried out in the middle of the twentieth century. So, in [17], the possibility of using specialized acoustic signals to protect information messages in transmission lines and at the boundaries of the controlled area is substantiated.

The use of acoustic noise in the form of periodic and non-periodic meanders in systems to counteract the interception of information messages in open telecommunication lines is considered in [18]. The paper analyzes the influence of such interference on the intelligibility of a speech signal for various signal/noise ratios.

In [19], the influence of the switching frequency of the acoustic signal and noise interference is considered. Studies of combined signals with different intensities, time and spectral compositions are carried out. The useful signal and the interference signal (noise) are supplied in various combinations and with different signal to noise ratios.

The results of studies conducted by Beranek & Newman from 1948 to 1953 are published in [20, 21]. Their main achievement is the idea of using specialized acoustic noise and systems (devices) to protect speech information in telecommunication networks and at dedicated facilities. The direction of the «Acoustic Interference Control System» is formed.

Further studies of the influence of various types of noise on the protection level of speech information within the controlled zone are divided into several areas that examined individual exposure parameters. These areas include:

- research of pseudorandom sequences with specified parameters of resistance to re-engineering for generators of «white» noise;
- research of the influence of frequency reverberation the possibility of restoring speech information [22–24];
- research of the possibility of distinguishing a «specific» speaker from a conversation, with the simultaneous language of two or more speakers [25, 26];
- development of methods for identifying signs of a speech signal in folding noise phonograms [27, 28].

One of the leading studies of our time is the development of methods for recovering speech information in the presence of noise. The most widely used method is based on MFCC coefficients (*Mel-frequency cepstral coefficients*). It is used both as a research tool and as a basic method for verifying the proposed methods and the obtained results. So, in [22] the influence of reverberation and noise in the conditions of a «cramped» room is considered. It is shown that under certain conditions (the relative position of the signal source and the interference source, signal ratio, etc.) proposed in [22], the binaural system shows significantly better results with respect to the conventional recognition system based on MFCC coefficients (*Mel-frequency cepstral coefficients*). It is shown in the work that the main interval for using the binaural system and MFCC coefficients proposed by the authors is the signal-to-noise ratio with $SNR>0$ dBA. Thus, it is unlikely to recover signals that have been destructively affected by acoustic noise using these methods.

Further development of the research of the possibility of restoring speech information is obtained in [23]. The paper proposes the use of the method of weighing the coefficient *TFR (Term Frequency representation*) of the language using auditory tendency for noise-protective *ASR (Automatic Speech Recognition)*. The combination of a multi-threaded system using the used method and a single-threaded system using the technology of spectral masking *EBM (Estimated Binary Mask)* proposed further reduced *WER (Word Error Rate)*. However, the system remained vulnerable to noise interference with $SNR<0$ dBA.

In [24], the features of using synthesized noises to form an interference signal are considered. The method of frequency reverberation proposed in the work shows quite good results in terms of the level of destructive effect on the test signal. However, the spectrogram presented in the work (Fig. 6 in [24]) quite clearly demonstrates the disadvantages of this method – the presence of signal repeatability (reverberation) in the frequency range. Complications of the interference generation algorithm by the indicated technique are easily leveled using a neural network in the filtering system.

Representatives of the next area of works are [25, 26].

In [25], it is proposed using the probabilistic method to track the perceived step for potentially aperiodic sounds, as well as track pitch from several simultaneous sources. Moreover, the use of an invariant shift of the representation in the region of constant Q allows to simulate the adopted step changes as vertical shifts of the spectra. This allows to track these changes in sounds with an arbitrary spectral profile.

However, the method proposed in [25] does not allow recognition of reverberation signals, which can become a source of significant noise interference.

In [26], Google's laboratory research on speaker recognition (or speaker) against the background of other people's conversation or significant noise interference created by the room's sounding system is presented. The technique proposed in [26] separates the speaker's voice from the signals of several speakers using the reference signal from the speaker's voice. This is achieved by training two separate neural networks:

- 1st network – speaker recognition, forms culturally discriminatory vectors of word representation;
- 2nd network – masking spectrograms, creates a mask based on the received speech signal of the speaker and noise interference.

This approach makes it possible to increase the speaker's speech highlighting level – the *WER* coefficient decreases from 55.9 % to 23.4 % for cases with two speakers (speaker and speaker of the speaker system).

The disadvantages of this method include a rather complex algorithm for training neural networks, which requires the presence of «pure» speaker speech at the initial stage. Also, the signal-to-noise ratio, at which the results are obtained, is not indicated in the work.

To recognize a speech signal against the background of acoustic noise, methods of energy control are also used based on the entropy of the signal spectrum [27]. The studies are carried out for various signals and interference (signals are selected from the *TIDigits* database, and noise was selected from *Noisex*) and at significant levels of noise interference (-10 dBA$<SNR<10$ dBA). The work shows that the use of the entropy of the signal spectrum to identify signs of a speech signal is more effective. At the same time, it should be noted that in the used *Noisex* noise signal base there are no incoming speech-like signals based on the speaker's speech, including from the *TIDigits* database. An analysis of the mathematical dependences used in [27] shows the impossibility of recognizing a speech signal by the indicated methods – energy control and based on the entropy of the signal spectrum.

 ISSN 2664-9969

In [28], the results of studies of the possibility of detecting signs of a speech signal using the *ZCR (Zero Crossing Rate)* and *STE (Short Time Energy)* methods are presented. The results shows that both methods provide sufficient accuracy for the detection of a speech signal with *SNR*>0 dBA. However, with *SNR*≤0 dBA, both methods lose their effectiveness.

Thus, the analysis results allow to conclude that modern methods of digital processing of phonograms are able to filter and restore the speech signal, which has suffered a destructive effect. The use of neural networks makes it possible to identify signs of a speech signal in a noisy phonogram. This allows to filter the «white» noise and its clones, remove reverberation-type noise, and even distinguish the speaker from a conversation in which two or more people participate.

5. Methods of research

5.1. Generalized diagram of a speech-like signal generator. The main idea of the generator is to use a combined method of generating an interference signal. To increase its complexity during the formation process, two additional types of external signals are used – phonograms of narration text that are in the device's additional memory, and signals from a multi-channel receiver built into the generator. A generalized diagram of the device is shown in Fig. 1.

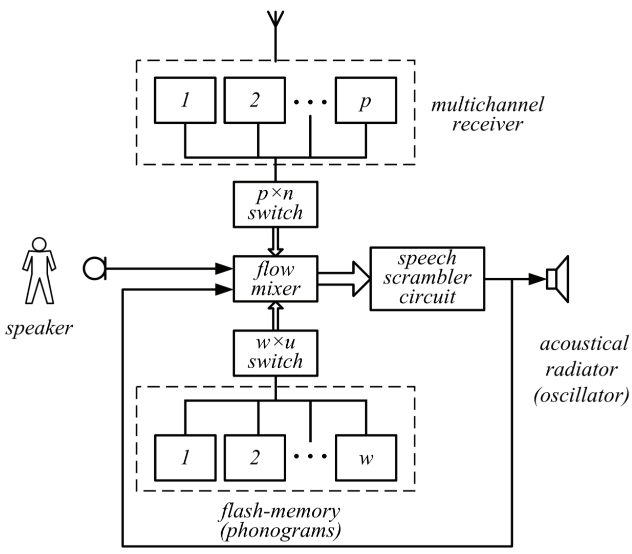


Fig. 1. Generalized structural diagram of a generator of a speech-like interference signal of scrambler-type for counteraction systems of leakage of speech information by acoustic and vibration channels

In general, the method of generating an interference signal in the «Mixing» block is described by the expression:

$$S_i(t)=A_i(t)+SS_{i-1}(t)+\sum_{j=1}^{k_{in}}M_j(t)+\sum_{z=1}^{k_{of}}R_z(t), \quad (1)$$

where $A_i(t)$ – speech signal voiced by the speaker; $S_{i-1}(t)$ – interference signal of the previous cycle; $M_j(t)$ – j-th element of the array, which is a random sequence of $k_{in}=u+rnd(w)$ elements (phonogram numbers); $R_z(t)$ – the z-th element of the array, which is a random sequence of $k_{of}=p+rnd(t)$ elements (receiver numbers); u and w – the minimum number of phonograms that must be connected to the path of the formation of the interference signal and the total number of phonograms in the memory block of the generator; p and r – the minimum number of receiver channels that must be connected to the interference signal conditioning path and the total number of receiver channels are lined up in a generator.

In the «Scrambling» block, the interference signal is encoded on the basis of a complex signal $S_i(t)$, which includes the speaker's speech signal (which is subject to protection). To reduce the effectiveness of reengineering methods, a dynamic change in coding coefficients is used in the Scrambling block.

The synthesis procedure includes two independent transformations – in frequency and time:

$$SS(f,t)=\begin{cases}\sum_{j=1}^{n}\sum_{i=1}^{m}A(f_{b_j+(-1)^{a_j}\cdot i+m\cdot a_j});\\ \sum_{y=1}^{k_t}\sum_{x=1}^{h_t}A(t_{d_y+(-1)^{c_y}\cdot x+h_t\cdot c_y});\end{cases} \quad (2)$$

i and m – the number and amount of tone frequencies in the 1/3-octave bands (determined by the FFT equation (fast Fourier transform)); a_j – j-th element of the bit array $\vec{a}=rnd(0,1)\big|_n$, which is a random bit sequence of n elements (encoding of direct/inverse movement of the bands is provided); b_j – j-th element of the bit array $\vec{b}=rnd(0...1)$, which is a random sequence with n elements; y and k_t – the number and amount of time blocks into which the window of the signal processing period is divided (defined as a random number $k_t=8+rnd(8)$); x and h_t – the number and amount of time bands into which the temporary signal processing unit is divided (defined as a random number $h_t=3+rnd(8)$); c_y – y-th element of the bit array $\vec{c}=rnd(0,1)\big|_{k_t}$, which is a random bit sequence of k_t elements (encoding of direct/inverse movement of time bands is provided); d_{t_y} – the y-th element of the array $\vec{d}_t=rnd(1...k_t)$, which is a random sequence of k_t elements.

When coding an interfering signal, its processing period T is determined according to dependence:

$$T=k_t\cdot h_t\cdot\left[0.05+0.01\cdot rnd(10)\right]=var.$$

5.2. Speech-like signal generator model. The generator is simulated in the *Matlab 15 R2015a/Simulink* environment. When modeling, the simplified structure of the device is used – external sources of speech signals (multichannel receiver and flash memory) are not used. This allows to explore the capabilities of the block «Scrambling» at minimum modes of resistance to re-engineering.

Fig. 2 shows the mathematical model of the generator.

For the test signal, the short phrase «Brought the ship on the landing path» is used. To obtain a continuous signal, the phonogram is looped to playback.

Fig. 3 shows temporary, and Fig. 4 – frequency oscillograms.

The main parameters of the scrambling block, which are adopted unchanged to simplify the analysis of the simulation results, are the size of the window of temporary permutations – 0.52 ms, the number of bands for frequency scrambling – 16.

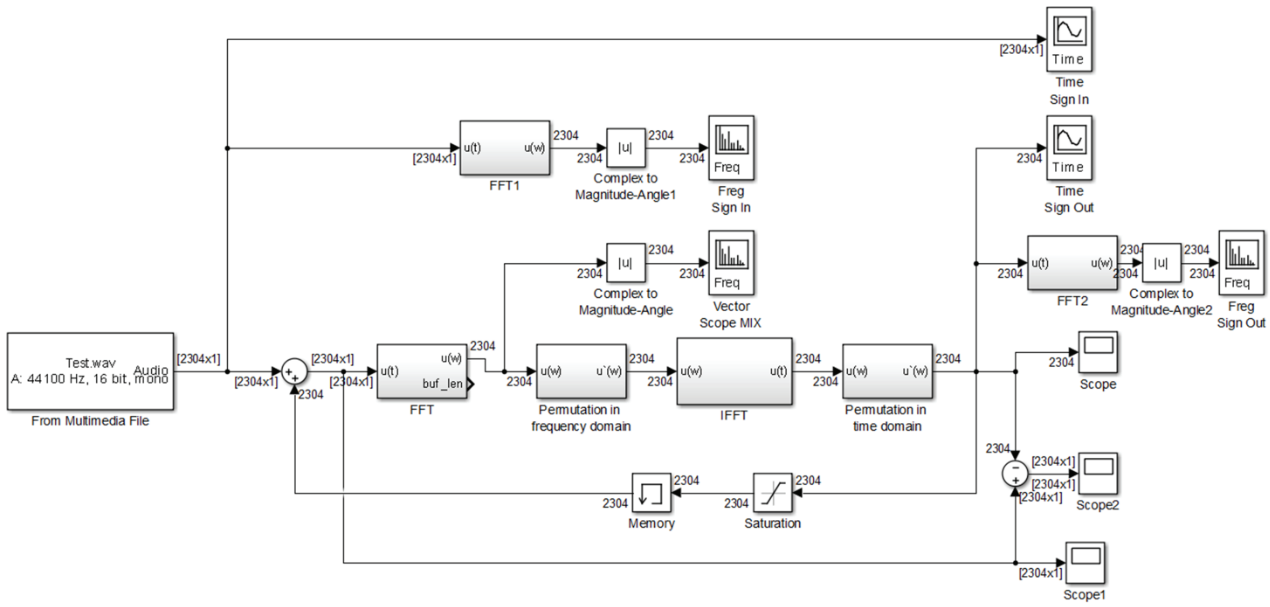
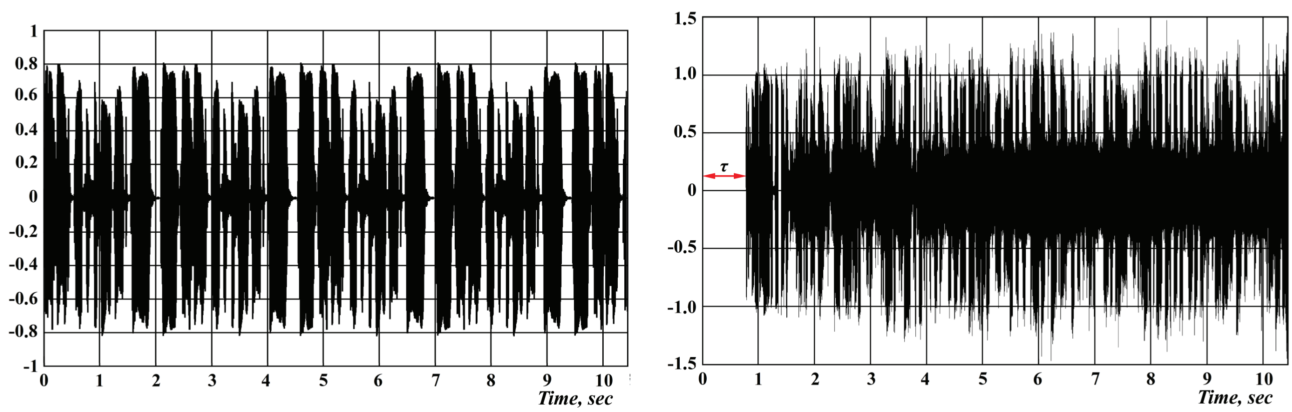
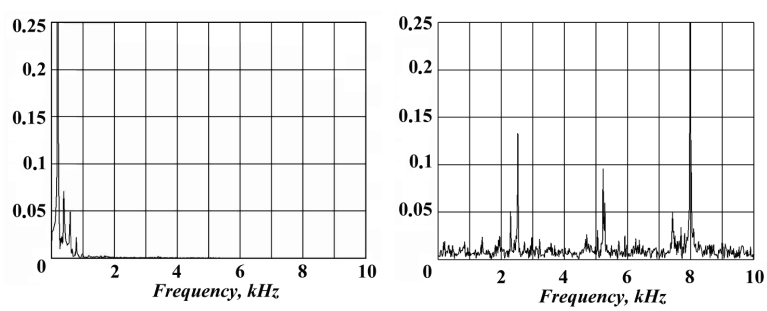


Fig. 2. Scrambler-type speech-like interference signal generator model



a *b*

Fig. 3. Timing diagram: *a* – input test signal (Time Sign In); *b* – output signal (Time Sign Out)



a *b*

Fig. 4. Spectrograms: *a* – input test signal (Time Sign In); *b* – output signal (Time Sign Out)

An analysis of the results shows that:

1. The input test signal meets the requirements of simple continuous speech:

– the length of the test signal is approximately 2 s (Fig. 3, *a*);

– the interval during the repetition of the test signal is 0.2 s (Fig. 3, *a*);

– the number of repetitions of the test signal – more than 5 times (Fig. 3, *a*);

– the main linguistic parameters of phonemes (fundamental frequency F0 and the main formants F1, F2 and F3) are clearly defined (Fig. 4, *a*) and are in the range from 200 Hz to 1000 Hz;

– the frequency range that the signal occupies (from 20 Hz to 5600 Hz) is typical of phonograms processed on a personal computer, without the use of additional hardware and software devices.

2. The output signal is shifted with respect to the input signal by 0.75 s, which is due to the features of the «*Permutation in time domain*» block (Fig. 2) and the dimensions of the window of temporary permutations adopted for modeling.

3. «Process stabilization» of the device to the operating mode, according to Fig. 3, *b*, it is 4 s – it is impossible to single out individual words and phonemes in the output signal.

4. Analysis of the spectrogram of the output signal (Fig. 4, *b*) shows:

– the impossibility of highlighting the main linguistic parameters of phonemes;
– the range of the frequency spectrum of the signal expanded to 10 kHz;
– in the spectrum of the output signal there are three groups of maxima located over an interval of about 2.5...2.6 kHz, however, they are not correlated with each other and the spectrum of the test signal with either a set of frequency components or characteristic features.

6. Research results

6.1. Verification of the research results of a mathematical model of a scrambler-like speech-like interference signal generator. To confirm the research results of the mathematical model of the movable signal generator, a prototype device is developed – the real speech-like interference generator OSSA-1, developed in the laboratory of technical information protection systems of the National University of Shipbuilding (Mykolaiv, Ukraine) [29]. The research results, taking into account the requirements for the protection level of speech information depending on the category of the zone, are shown in Fig. 5.

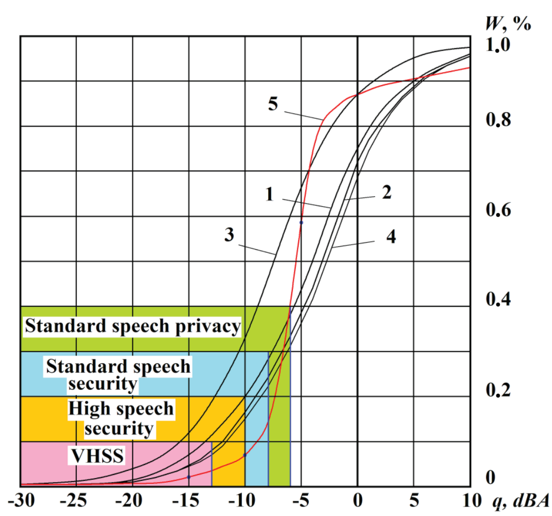


Fig. 5. The dependence of speech intelligibility W on the integral signal-to-noise ratio q: 1 – «white» noise; 2 – «pink» noise; 3 – «brown» noise; 4 – «speech-like» noise; 5 – real speech-like interference formed by the OSSA-1 generator; VHSS – Very high speech protection

When specifying protection zones in Fig. 5 «white» noise is taken as a basis (line 1). Graphs of the dependence of speech intelligibility W on the integral signal-to-noise ratio q for «white», «pink», «brown» and «speech-like» noises are determined experimentally and compared with [30] – the deviation of the obtained values is less than 3 %. When conducting research, the articulation method is used. The setup scheme and research methodology are described in more detail in [29].

Studies have shown a higher interference efficiency generated by the OCCA11 generator compared to conventional methods of generating acoustic noise based on «white» noise and its clones [5]. According to Fig. 5, the OSSA-1 generator synthesizes noise interference (with $SNR \leq -8$ dBA), the influence of which is sufficient to fulfill the requirements for preventing leakage of speech information from a zone of VHSS category.

6.2. Discussion of the research results of a mathematical model of a speech-like scrambler-type interference signal generator. The paper proposes a new approach to the formation of an interference signal for systems for setting active acoustic and vibrational noise – the use of scrambler principles. Despite the fact that the devices themselves (scramblers) are quite common at one time and are widely used in telecommunication networks, their use as interference generators is not recorded in the literature.

The proposed scheme and its mathematical model make it possible to determine several particularly significant parameters:

1. The time the system is ready to work, after turning on or a long pause in the conversation (in the simplest version, which is taken as a basis when creating the model), is 4 s. Thus, it is necessary to take into account the initial stage of the system entering the operating mode and limit the subject of communication to general topics.

2. As can be seen from Fig. 5, when using the proposed method for protecting speech information in the zone with the category «Standard speech private», its effectiveness compared to conventional devices is significant. Significant advantages in the protection level of speech information from leakage by acoustic and vibration channels, the proposed method for the synthesis of interference provides with $SNR \leq -8$ dBA. This is 6...10 dBA less than the level of interference that noise generators must create using standard methods («white» noise and its clones).

7. SWOT analysis of research results

Strengths. Studies of the mathematical model carry out in the *Matlab 15 R2015a/Simulink* environment and their verification on a prototype shows a high level of destructive influence of the proposed method for generating noise interference. Generators of this type at the objects of information activity will provide:

– increasing the protection level of speech information from leakage by acoustic and vibration channels due to increased resistance to modern filtering methods (wavelet transform, correlation and spectral analyzes, etc.);
– reducing the level of acoustic and vibrational noise in a controlled room, which is created by the system of setting active interference by 6...10 dBA, which significantly improves working conditions;
– reduction of the unmasking level of the object by reducing the volume of the noise interference and the use of the «language choir» method – for an outside observer, the signal is intercepted that meets the criteria of an «open» public event;
– modernization of existing IIPS does not require significant material costs – it is necessary to replace only the interference generator.

Weaknesses. Implementation of a scrambler-type of speech-like interference signal generator for counteracting speech information leakage by acoustic and vibration channels in accordance with the structure shown in Fig. 1 requires significant material costs. Tentatively, the cost of the generator will be 30...40 % more than the typical (for those indicated in section 1). However, this drawback is fully compensated by the increased protection level.

Opportunities. The problem of protecting speech information from leakage through technical acoustic and vibration channels and its unauthorized interception by an attacker is promising for all countries of the world. Thus, the proposed methodology is the subject of research in all leading countries, and the results are classified as «know how».

Threats. Possible threats that after some time the product developers will have to confront with the proposed method of jamming are new methods of mathematical processing of digital phonograms implemented on neural networks (artificial intelligence). The use of such systems can lead to unwanted allocation of a dangerous signal (speaker's speech) against the background of noise interference.

The system is able to counteract this threat by taking into account the principles of distinguishing the language of a separate speaker from the language choir – such an upgrade is provided for in the device diagram.

8. Conclusions

1. A mathematical model of a speech-like signal generator is proposed, in which for the first time the combined method of analog coding (scrambling) of a speaker's speech and third-party sources of speech signals is used for systems for setting active vibration and acoustic noise. This makes it possible to clarify the generalized block diagram of the scrambler-type generator of a speech-like interference signal and synthesize analytical dependences for the mathematical apparatus of the model.

The model uses the principle of cumulative ringing of the signal stream (mixing of the input and output signals) and the use of frequency-band and time-band permutations (scrambling), which significantly complicates the re-engineering of the output signal.

The proposed analytical dependencies provide for the use of dynamic keys for coding systems in the block of scrambling and connecting third-party sources of speech signals. It is proposed to use a set of phonograms (on removable flash media) and on-line signals from radio air as extraneous signals. This significantly complicates the reengineering procedure.

2. A simplified mathematical model of a speech-like signal generator was developed and researched in *Matlab 15 R2015a/Simulink*. Studies have shown the high efficiency of the proposed method of forming acoustic noise. It was established that the system has a certain delay when it enters the «operating mode». The delay was 4 s.

The simplified mathematical model does not include third-party speech sources and uses static keys of the coding system parameters. This allows to explore the most vulnerable version of the device. Moreover, the level of destructive influence according to the analysis of temporal and spectral characteristics satisfied the requirements.

3. To verify the reliability of the results of mathematical modeling, laboratory studies of the prototype device – OSSA-1 generator of real speech-like interference – are developed in the laboratory of technical information protection systems of the National University of Shipbuilding (Mykolaiv, Ukraine). Studies are carried out by articulation method. The dependence of speech intelligibility W on the integral signal-to-noise ratio q is established. The results of exposure to typical noise interference («white» noise and its clones) and noise interference created by the generator are compared. The research results show that for the protection of speech information in the zone with the category «Standard speech private» its effectiveness is not worse than conventional devices. However, for the zone with the category «High speech protection» the efficiency has already amounted to 6...10 dBA. This ensures a reduction in the level of acoustic and vibrational noise background in the controlled room, which is created by the active jamming system, to 10 dBA, which significantly improves working conditions.

References

1. *On Protection of Information in Automated Systems. Law of Ukraine No. 80/94-BP.* 05.07.1994. Available at: https://zakon.rada.gov.ua/laws/main/80/94-%D0%B2%D1%80
2. *On State Secret. Law of Ukraine No. 3855-XII.* 21.01.1994. Available at: https://zakon.rada.gov.ua/laws/show/3855-12
3. *On Protection of Personal Data. Law of Ukraine No. 2297-VI.* 01.06.2010. Available at: https://zakon.rada.gov.ua/laws/main/2297-17
4. *Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii ND TZI 2.4-010-2015.* Available at: http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=D90D601C55F63184CFC22F8E76C42F44.app1?art_id=149166&cat_id=89991
5. *Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii ND TZI 2.3-019-2015.* Available at: http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=D90D601C55F63184CFC22F8E76C42F44.app1?art_id=149166&cat_id=89991
6. *Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii ND TZI 2.2-008-2015.* Available at: http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=D90D601C55F63184CFC22F8E76C42F44.app1?art_id=149166&cat_id=89991
7. Perelik zasobiv tekhnichnoho zakhystu informatsii, dozvolenykh dlia zabezpechennia tekhnichnoho zakhystu derzhavnykh informatsiinykh resursiv ta informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom (stanom na 30 lypnia 2018). *DSSZZI Ukrainy.* Available at: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=284094&cat_id=39181
8. Vidomosti pro zasoby tekhnichnoho zakhystu informatsii, na yaki zakinchyvsia termin dii sertyfikativ vidpovidnosti ta ekspertnykh vysnovkiv (stanom na 1 sichnia 2017 roku). *DSSZZI Ukrainy.* Available at: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=234241&cat_id=39181
9. Grigorev, I. A., Kazanovskii, A. I. (2010). Metodicheskii podkhod k ocenke effektivnosti zaschity rechevoi informacii. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta, 5,* 133–136.
10. Nuzhnyi, S. M. (2018). Udoskonalena tekhnolohiia otsinky stupenia zakhystu movnoi informatsii. *Suchasnyi zakhyst informatsii, 1 (33),* 66–73. Available at: http://journals.dut.edu.ua/index.php/dataprotect/article/view/179
11. Khorev, A. A. (2009). Ocenka vozmozhnostei sredstv akusticheskoi (rechevoi) razvedki. *Specialnaia tekhnika, 4,* 49–63.
12. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. *Eastern-European Journal of Enterprise Technologies, 5 (9 (95)),* 26–34. doi: http://doi.org/10.15587/1729-4061.2018.144146
13. Rybalskii, O. V., Solovev, V. I., Zhuravel, V. V. (2017). Fraktalnii podkhod k vyiavleniiu sledov cifrovoi obrabotki v analogovykh fonogrammakh. *Suchasna specialna tekhnika, 1,* 4–9. Available at: http://nbuv.gov.ua/UJRN/sstt_2017_1_4
14. Solovev, V. I., Rybalskii, O. V., Zheleznіak, V. K. (2014). Multifraktalnaia struktura shepota i raspoznavanie rechevykh struktur. *Vestnik Polockogo gosudarstvennogo universiteta. Seriia C, Fundamentalnye nauki, 12,* 16–20.Available at: http://elib.psu.by:8080/handle/123456789/11215

ISSN 2664-9969

15. Bortnikov, A. N., Gubin, S. V., Lobov, V. A., Siromashenko, A. V., Chernyshov, P. V. (2007). Rezultaty eksperimentalnykh issledovanii ocenki vozmozhnostei perekhvata rechevoi informacii pri realizacii metodov dvukhkanalnogo sema. *Voprosy zaschity informacii, 1,* 11–17
16. Lobov, V. A., Siromashenko, A. V., Chernyshov, P. V. (2007). Ocenka vozmozhnostei perekhvata rechevoi informacii pri realizacii metoda mnogokanalnogo sema. *Voprosy zaschity informacii, 4,* 27–35.
17. Licklider, J. C. R. (1948). The Influence of Interaural Phase Relations upon the Masking of Speech by White Noise. *The Journal of the Acoustical Society of America, 20 (2),* 150–159. doi: http://doi.org/10.1121/1.1906358
18. Shannon, C. E. (1998). Communication In The Presence Of Noise. *Proceedings of the IEEE, 86 (2),* 447–457. doi: http://doi.org/10.1109/jproc.1998.659497
19. Miller, G. A., Licklider, J. C. R. (1950). The Intelligibility of Interrupted Speech. *The Journal of the Acoustical Society of America, 22 (2),* 167–173. doi: http://doi.org/10.1121/1.1906584
20. Bolt, R. H., Beranek, L. L., Newman, R. B. (1952). *Handbook of acoustic noise control*. Volume I. Physical Acoustics. doi: http://doi.org/10.21236/ad0012015
21. Rosenblith, W. A., Stevens, K. N. (1953). *Handbook of acoustic noise control*. Volume II. Noise and man. doi: http://doi.org/10.21236/ad0018260
22. Palomäki, K. J., Brown, G. J., Wang, D. (2001). A binaural model for missing data speech recognition in noisy and reverberant conditions. *Consistent & Reliable Acoustic Cues for sound analysis*. Aalborg.
23. Do, C.-T., Stylianou, Y. (2018). Weighting Time-Frequency Representation of Speech Using Auditory Saliency for Automatic Speech Recognition. *Interspeech 2018*. doi: http://doi.org/10.21437/interspeech.2018-1721
24. Prodeus, A. M., Vityk, A. V., Didenko, D. Y. (2017). Subjective evaluation of quality and intelligibility of speech distorted by synthesized noise. *Microsystems, Electronics and Acoustics, 22 (6),* 56–63. doi: http://doi.org/10.20535/2523-4455.2017.22.6.101929
25. Smaragdis, P. (2009). Relative-pitch tracking of multiple arbitrary sounds. *The Journal of the Acoustical Society of America, 125 (5),* 3406. doi: http://doi.org/10.1121/1.3106529
26. Wang, Q., Muckenhirn, H., Wilson, K., Sridhar, P., Wu, Z., Hershey, J. R. et. al. (2019). VoiceFilter: Targeted Voice Separation by Speaker-Conditioned Spectrogram Masking. *Interspeech 2019*. doi: http://doi.org/10.21437/interspeech.2019-1101
27. Renevey, P., Drygajlo, A. (2001). Entropy based voice activity detection in very noisy conditions. *EUROSPEECH-2001,* 1887–1890. Available at: https://www.isca-speech.org/archive/eurospeech_2001/e01_1887.html
28. Özaydın, S. (2019). Examination of Energy Based Voice Activity Detection Algorithms for Noisy Speech Signals. *European Journal of Science and Technology,* 157–163. doi: http://doi.org/10.31590/ejosat.637741
29. Kasianov, Yu. I., Nuzhnyi, S. M. (2016) Otsiniuvannia efektyvnosti heneratora realnoi movopodibnoi zavady za kryteriiem rozbirlyvist movy. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: Avtomatyka, vymiriuvannia ta keruvannia, 852,* 105–110. Available at: http://ena.lp.edu.ua:8080/handle/ntb/36473
30. Khorev, A. A., Makarov, Iu. K. (2001). Metody zaschity rechevoi informacii i ocenki ikh effektivnosti. *Specialnaia tekhnika, 4,* 22–33.

Blintsov Volodymyr, *Doctor of Technical Sciences, Professor, Department of Electronic Engineering of Ship and Robotic Complexes, Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine, ORCID: http://orcid.org/0000-0002-3912-2174, e-mail: volodymyr.blintsov@nuos.edu.ua*

Nuzhniy Sergey, *PhD, Associate Professor, Department of Computer Technologies and Information Security, Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine, ORCID: http://orcid.org/0000-0002-7706-0453, e-mail: s.nuzhniy@gmail.com*

Kasianov Yurii, *Senior Lecturer, Department of Computer Technologies and Information Security, Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine, ORCID: http://orcid.org/0000-0003-2417-0111, e-mail: yukas.nik.ua@gmail.com*

Korytskyi Viktor, *Senior Lecturer, Department of Computer Technologies and Information Security, Admiral Makarov National University of Shipbuilding, Mykolayiv, Ukraine, ORCID: http://orcid.org/0000-0002-9968-1568*