24. Kamenev, A. Yu. Reliability of combined proofs methods of microprocessor interlocking system of railway stations [Text] / A. Yu. Kamenev // Sovremennyie problemyi transportnogo kompleksa Rossii. – 2014. – Vol. 4, Issue 5. – P. 61–66.
25. Kameniev, O. Yu. Prohnozuvannia stanu mikroelektronnykh prystroiv zaliznychnoi avtomatyky pry obmezhenykh statystychnykh danykh [Text] / O. Yu. Kameniev, V. I. Moiseienko, V. V. Haievskyi // Informatsiino-keruiuchi systemy na zaliznychnomu transporti. – Chornomorsk, 2016. – Issue 4. – P. 37.
26. Kustov, V. F. Usovershenstvovanie metodov ispyitaniy mikroprotsessornoy tsentralizatsii na bezopasnost primeneniya [Text] / V. F. Kustov, A. Yu. Kamenev // Aktualnyie voprosyi razvitiya sistem zheleznodorozhnoy avtomatiki i telemehaniki. – 2013. – P. 103–118.
27. Doslidzhennia funktsiinoi bezpechnosti ta elektromahnitnoi sumisnosti mikroprotsesornoi systemy elektrychnoi tsentralizatsii stantsii «Vuhilna» na etapi imitatsiinykh ta stendovykh vyprobuvan [Text]. – UkrDAZT. – No. derzh. reyestr. 0112U006925; inv. No. 0713U007283. – 2012. – 139 p.

Обґрунтовується ефективність використання скремблерів в вузькосмугових системах зв'язку, що працюють в умовах низького відношення сигнал/завада. Оцінюється вплив кількості та порядку перестановки смуг на залишкову розбірливість скрембльогованого сигналу. Досліджується стійкість скрембльованого сигналу до злому. Наводяться практичні рекомендації щодо розробки смугових скремблерів, що реалізують цифрову обробку мовних сигналів з використанням алгоритму швидкого перетворення Фур'є з ковзаючим вікном

Ключові слова: скремблювання, смуговий скремблер, швидке перетворення Фур’є, ковзаюче вікно, залишкова розбірливість

Обосновывается эффективность использования скремблеров в узкополосных системах связи, работающих в условиях низкого отношения сигнал/помеха. Оценивается влияние количества и порядка перестановки полос на остаточную разборчивость скремблированного сигнала. Исследуется устойчивость скремблированного сигнала к взлому. Приводятся практические рекомендации по разработке полосовых скремблеров, реализующих цифровую обработку речевых сигналов с использованием алгоритма быстрого преобразования Фурье со скользящим окном

Ключевые слова: скремблирование, полосовой скремблер, быстрое преобразование Фурье, скользящее окно, остаточная разборчивость

UDC 621.391.2/.7
DOI: 10.15587/1729-4061.2017.101922

RESEARCH INTO THE USE OF SCRAMBLERS IN NARROWBAND COMMUNICATION SYSTEMS

V. Kukush
PhD, Associate Professor*
E-mail: k.vitalii@ymail.com
D. Verchyk*
E-mail: daria.verchik@gmail.com
*Department of computer radio engineering and systems of technical security of information
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

1. Introduction

Along with the development of computer technologies, methods and means for transmission of information, approaches to ensure information security are also being developed. Operation of information security systems which provide protection of transmitted voice messages is based on converting speech signal characteristics. As the result, the speech becomes unintelligible to eavesdroppers after interception of such messages.

Among the variety of voice communication systems narrowband systems occupy a special place. Due to the narrow bandwidth of individual channels the rational use of radio-frequency resource is achieved. These systems are characterized by low requirements to stability of communication channel characteristics and low-cost of equipment. Examples of narrowband communication systems are general- and special-purpose wired telephone lines as well as special, operational-technological and amateur radio systems up to the VHF band. In such systems, along with the requirements of reliability and efficiency, issues of the information transmission security are also of importance.

There are two basic methods of converting speech signals for the purpose of protection against tapping: scrambling and digital encryption [1–5]. The main difference between scrambling and digital encryption is that scramblers are converting the frequency-time characteristics of the original analog speech signal transmitted over the communication channel. The signal after scrambling occupies the same frequency band as the original one. On the contrary, digital encryption devices are encoding bit sequence that is transmitted over the communication channel and determines the samples of the original speech signal [2, 5].

Digital encryption of speech signals using cryptoalgorithms or vocoder devices [5] provides a higher-level security compared to scrambling [4]. Transmission of the obtained stream of encrypted speech samples is carried out mainly through broadband communication channels. In turn, scramblers leave the signal bandwidth without expanding, so they can be used in both broadband and narrowband communication channels [2, 3]. Due to its versatility, scrambling devices are being actively produced by such manufacturers as Transcrypt International (USA), Communico (USA), MX COM (USA), MIDIAN Electronics (USA), Selectone (USA) and used in commercially available special-purposes radio stations. One of such radio stations are the ORION-RS-1S and the ORION-RV-1S transceivers manufactured by ORION Radio Plant PJSC (Ternopil, Ukraine). It confirms the relevance of the works connected with improvement of the speech scrambling devices and investigation of its operation features.

2. Literature review and problem statement

According to [3], the following basic principles of scrambling are distinguished:

1) scrambling in the frequency domain: the spectrum of the speech signal is inverted or split into a series bands which are then permuted and inverted. Inversion means a flipping of the original signal spectrum in the selected frequency band relative to its center. Devices implementing scrambling in the frequency domain are called band scramblers;

2) scrambling in the time domain: the speech signal is divided on fragments which are split into segments and then inverted and/or permuted in the time domain;

3) two-dimensional or combined scrambling simultaneously implements the two principles of speech signals conversion described above.

To transmit information over a communication channel in real time, scrambling in the frequency domain is more preferable than in the time domain [6]. This is due to the fact that band scramblers are more tolerant to distortions of the channel amplitude and phase responses. It allows obtaining minimal signal distortions during descrambling. At the same time, the main disadvantage of band scramblers is that the scrambled signal is characterized by the speech-like rhythm and relatively high levels of residual intelligibility [7].

As a rule, the basis of the band scramblers consist of the bandpass filter bank which is realized in analog or digital form. Implementation of the filter bank in a digital form and application of the fast Fourier transform (FFT) algorithm provide a significant increase of number of bands into which the spectrum of the original signal is split [8]. Due to this, the number of possible band permutations increases and leads to growth of scrambled speech security level. However, implementation of the algorithms using the principle of block-by-block accumulation and processing of samples [9] requires synchronization. The synchronization between the scrambler and the descrambler is necessary in order to correctly descramble the voice information. Lack of synchronization causes distortions in the descrambled signal that are perceived as "clicks", which follow with a period equal to the duration of the FFT window [10].

The problem of synchronization between the band scrambler and descrambler based on the FFT algorithm has been studied in detail in a number of works. For example, the possibility of introducing additional sync pulses into the scrambled speech signal both before the beginning of the communication session and during of the transmission of speech information was considered in work [11]. In subsequent work [12], it was proposed to use the sample-, frame- and multiframe synchronization. A similar synchronization mechanism is also implemented in the scramblers that use OFDM modulation for transmission of encrypted speech samples [13]. It leads to significant complication of the scrambling algorithm and increases its computational complexity [14]. Such additional feature puts in doubt the declared simplicity of the scrambling methods described above.

Works [15, 16] present alternative methods of band scramblers implementation that do not require synchronization between the scrambler and descrambler. These approaches are based on the digital filter bank that uses the sliding window FFT algorithm [15] or the "fast filter bank" [16]. From the practical point of view, these approaches have greater computational complexity than the algorithms based on the block-by-block accumulation and processing of samples [15]. However, practical implementation of these methods is more preferable because they do not require synchronization and adding any service information to the transmitted signal. Moreover, using the FFT sliding window algorithm [15] is more preferable because it requires minimum time expenditure for the development of the scrambler. It is related to the fact that the FFT algorithm is a standard function of digital signal processing (DSP).

However, it should be noted that the following aspects of implementation and application of band scramblers are not fully represented in the available literature sources and reviews of technical solutions:

1) relevance of declared advantages of the scrambling methods over the encryption ones taking into account the modern techniques of compression and transmission of a stream of speech samples through various communication channels in particular reasonableness of using scramblers in narrowband communication systems;

2) optimal splitting of the speech signal spectrum for frequency domain scrambling and recommendations for choosing of a band permutation order for providing minimal level of speech residual intelligibility in a secured communication channel;

3) estimation of the scrambled signal security level, especially, its strength for a various hacking attempts.

3. The goal and the tasks of the research

The goal of the research was to analyze the features of development and operation of band scramblers as well as to estimate the signal security level provided by such class of devices.

To achieve this goal the following tasks were accomplished:

– comparative analysis of the peculiarities of implementation of scrambling and encryption methods in narrowband communication channels based on the generally known theoretical information on the data transfer rate limit and characteristics of modern speech compression methods;

– experimental analysis of the influence of the band permutation order on the scrambled signal residual intelligibility based on the known information of contribution of different speech signal spectrum bands to intelligibility;

– experimental investigation of the scrambled speech signal hacking strength in the communication systems equipped by band scramblers.

4. Comparative analysis of effectiveness of using scrambling and encryption methods in narrowband communication systems

In this article, a narrowband communication system is understood as a speech transmission system in which the bandwidth of the transmitted signal or communication channel is of the order of 3.1 kHz. This frequency band corresponds to the lowest third class of sound broadcasting quality [17].

The main features of such narrowband communication systems are:

1) work in a broadcast or in a conference mode ("one with all" or "all with all");

2) dynamic connection/disconnection of new subscribers;

3) operability in spite of low values of the signal-to-noise ratio (S/N) in a communication channel (from –6 dB);

4) duplex or simplex mode of operation;

5) limitation of the maximum delay in conversation or for reconfiguration of the communication network to 50...200 ms [18, 19]. Such delays are not perceivable to the human ear and do not effect on a comfort of conversation [20].

The possibility of using various encryption methods to secure voice information from leakage is determined by the parameters of the communication channel and the possibility of transmission the stream of encrypted signal samples in real time. Such possibility is complicated by the following:

1) the combination of a narrow band and small S/N values resulting in the data rate that is insufficient for speech samples transmission in real time;

2) the need to perform a "connection establishment procedure" when connecting/disconnecting new subscribers;

3) the need to resolve collisions of packets of signal samples transmitted simultaneously from several communication terminals that use a shared data transmission medium. Such problem is especially crucial when the communication network operates in the conference mode [21].

Consider in detail the problem connected with the insufficient data rate value. The ability to transmit voice in real time as a stream of samples is determined by two factors: the maximum data rate in a communication channel and a stream compressing method.

The physical limit of the data rate over a communication channel is determined by value of C [bit/s] calculated by Shannon's formula [22]:

$$C = B \cdot \log_2\left(1 + S/N_{[\text{times}]}\right), \tag{1}$$

where B is the bandwidth of a communication channel, Hz; $S/N_{[\text{times}]}$ is the signal-to-noise ratio (in terms of power).

As shown in Table 1, physical limit of the transmission rate is C=1...3.1 kbit/s for S/N equal to –6 ... 0 dB. The given S/N values are thresholds for the "analog" communication channel when a speech is still perceived with a satisfactory level of intelligibility [20].

Table 1

Dependence of the physical limit of the transmission data rate in a communication channel with bandwidth B=3.1 kHz on the S/N value

S/N, dB	–6	0	6	20	33	60
C, kbit/s	1	3.1	7.2	20.6	34	56

Modern codecs allow to compress the stream of the speech signal samples in such a way that it is required at least 6 kbit/s for its transmission over a communication channel in real time. This applies, for example, to open-source codecs such as OPUS, SILK, VORBIS which are used in popular IP communication systems like SKYPE® and Viber®. At the same time, the use of classified codecs such as STANAG that is recommended for use in special communication systems of NATO countries allows to reduce the above-mentioned data rate to 1.2...2.4 kbit/s [23].

It should be noted that even with higher S/N values the compression remains a necessary operation for transmission of speech samples over a narrowband communication channel in real time. Thus, in the case of data transmission over telephone lines at a nominal S/N of 33 dB (as defined in OST 45.36-97) the physical limit of data rate is 34 kbit/s (Table 1). This value is almost half the capacity of the "elementary channel of a digital telephone network" (64 kbit/s) [21], which is required for the transmission of 8-bit speech samples digitized at sampling rate of 8 kHz.

As it follows from the above, application of encryption methods is fundamentally impossible in narrowband communication systems in which the S/N in the channel varies in time and can take values of 0 dB or less. In such cases, only scrambling techniques provide secured transmission of voice signal in real time and with satisfactory intelligibility level after descrambling. For S/N values above 6 dB, the use of encryption methods in narrowband communication systems is possible but the development of such devices requires significantly higher material and time expenditures than for scramblers. This is caused by limitation of the data rate in a narrowband communication channel and the need of compression of speech signal samples stream.

5. Analysis of the influence of band permutation order on the residual intelligibility of the scrambled signal

The main characteristic of the scrambling algorithm is the residual intelligibility of the output signal. Residual intelligibility means a relative or percentage ratio of properly received and recognized elements of speech (phrases, words, syllables) to the total number of these elements [1–5].

The level of degradation of the signal intelligibility when the signal is transmitted over a communication channel can be estimated by the "speech transmission index" (STI). Table 2 shows coefficients α_i corresponding to the weight of each octave band of the signal when calculating the STI value [24].

The octave bands presented in Table 2 lie within the frequency range 300...3400 Hz which corresponds to the speech band transmitted over the narrowband communication channels. It should be noted that the values of α_i of each band are determined both by the peculiarities of a human auditory perception and by the spectral characteristics of the speech itself (by the probability of occurrence of formants in each band [17]). Thus, the spectrum of speech "is matched" with the peculiarities of its perception by the human ear.

Table 2

Weight coefficients of the octave bands of the speech signal spectrum as is assumed during calculation of STI

Central frequencies of octave bands, Hz	250	500	1000	2000	4000
Cut-off frequencies of octave bands, Hz	175...350	350...700	700...1400	1400...2800	2800...5400
Width of octave bands Δf, Hz	175	350	700	1400	2800
Weight of octave band α_i, average for male and female voices	0.122	0.226	0.224	0.318	0.237
$W_{Bperc_i}=(\alpha_i/\Delta f)\cdot 100$ (per each 100 Hz of the band)	0.0697	0.0647	0.032	0.0227	0.0085

During scrambling in the frequency domain the spectral components of speech are permuted while the common signal bandwidth keeps unchanged. It can be assumed that the coefficient of "degradation" of intelligibility of the scrambled speech (γ) will be proportional:

$$\gamma=\frac{r_{scr}}{r_{orig}}\approx\frac{1}{N}\sum_{i=1}^{N}\frac{W_{Bsig_i}\cdot W_{Bperc_i}}{W^2_{Bperc_i}}, \qquad (2)$$

where r_{orig}, r_{scr} are intelligibility estimates of original and scrambled signal; N is the number of signal bands during scrambling; W_{Bsig_i} is contribution of the i-th band to the intelligibility of the speech signal related to its width; W_{Bperc_i} is the contribution of the i-th band to the intelligibility of the speech signal related to its width from the point of view of speech perception by the human ear.

In the absence of scrambling $W_{Bsig_i}=W_{Bperc_i}$, therefore, from formula (2) γ=1. It can be assumed that in order to reduce the value of γ (to obtain the minimum values of the residual intelligibility of the scrambled signal), it is necessary that $W_{Bsig_i}\cdot W_{Bperc_i}\to 0$. Consequently, as it follows from Table 2, during the scrambling process the speech bands that have maximum contributions to intelligibility of a speech signal (maximum values of W_{Bsig_i}) have to be move towards the spectral regions with the minimal values of W_{Bperc_i}.

From an analysis of the values given in Table 2, it can be assumed that the decrease in the level of residual intelligibility is achieved by moving of low-frequency components of speech into the high-frequency region of the spectrum and vice versa. The possibility of decreasing of intelligibility in such permutations can also be explained by the fact that the ability of the human ear to distinguish separately signals with close frequencies is inversely proportional to the frequency of these signals. Therefore, movement of closely spaced low-frequency speech components (e. g. pitch harmonics) towards the high-frequency region prevents separated perception of these components and reduces intelligibility of the scrambled signal.

From the above, it is also possible to make the assumption about the susceptibility of a signal scrambled in the frequency domain to hacking by inversion of its spectrum in the entire frequency band. This operation approximately restores the order of bands of the scrambled signal, which can lead to an increase in its intelligibility to a satisfactory level and, as a consequence, to the possibility of unauthorized tapping.

6. Experimental equipment for research into the use of band scramblers

Experimental investigations of operation and efficiency features of band scramblers were carried out by experimental equipment which block diagram is shown in Fig. 1. The experimental equipment includes a sound reproducing device and a personal computer (PC) with specialized software implemented in the MATLAB® environment. The speech signals to be scrambled-descrambled were represented as arrays of samples stored in audio files or coming from the PC audio card. The algorithm of digital signal processing (DSP) used as the scrambler/descrambler was developed according to the recommendations stated in [15]. Main features of the algorithm are the ease of implementation by using standard DSP functions in its structure and the tolerance to the lack of synchronization between the scrambler and descrambler.

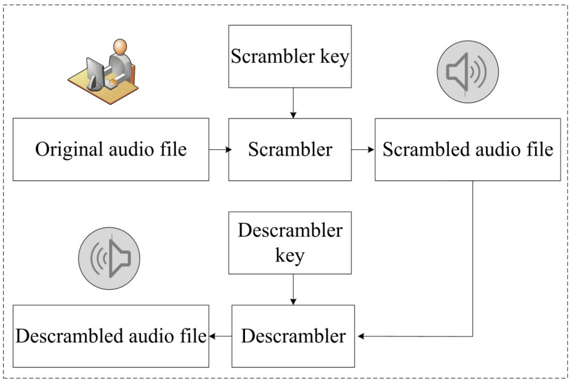

Fig. 1. Block diagram of the experimental equipment

The scrambling and descrambling algorithms are identical to each other, therefore only the scrambling algorithm is described below.

Developed scrambling algorithm (Fig. 2) based on the bank of digital narrowband filters which is realized using sliding window FFT technique [15]. This algorithm does not require synchronization between the scrambler and descrambler due to the use of the sliding window shifted by one sample at each iteration.

As can be seen from Fig. 2, N elements are fetched from the array of input signal samples s_{in} (n) by the sliding window at each iteration of the algorithm (where N is the window size, see step A). The selected elements are multiplied by the weighting function W(n) and processed by the FFT algorithm. During the next step, the output signal FFT spectrum is formed by permutation of the complex samples of the input signal FFT spectrum in accordance with the scrambler key and phase corrections procedure (blocks M and φ in Fig. 2).

The scrambler key used in the algorithm includes:

1) an array of band cut-off frequencies to be permuted;

2) an array specifying the order of band permutations;

3) an array of spectrum inversion flags for each band (enables flipping the order of spectrum samples within appropriate bands).

Further, the phase of each spectrum sample at the output of the block M was corrected in the block φ according to the formula (3). Due to this, phase jumps of the signal spectral components caused by frequency-domain permutations during the scrambling are eliminated.

$$\varphi'_{i,\,k} = \varphi_{i,\,k} + 2\pi \cdot \Delta f_i \cdot n_k \cdot \left(1/f_s\right), \qquad (3)$$

where i is the number of sample in the input signal FFT spectrum; k is the number of iteration of the scrambling algorithm; $\varphi'_{i,k}$ is the phase of the FFT spectrum complex coefficient of the signal at the output of the block φ which corresponds to the i-th FFT spectrum complex coefficient of the input signal; $\varphi_{i,k}$ is the phase of i-th FFT spectrum complex coefficient of the input signal; Δf_i is the frequency shift of the i-th FFT spectrum complex coefficient of the input signal which corresponds to its permutation in accordance with the scrambler key; n_k is position of the sliding window relative to the first element of the array of the input signal samples at the k-th iteration of the algorithm (Fig. 2); f_s is the sampling frequency of the input/output signal.

To form the output signal s_{out} (n), the array of FFT spectrum samples from the output of the block φ is processed by the inverse FFT (IFFT) algorithm. Obtained samples are added to the contents of the array s_{out} (n) (step B in Fig. 2). The array s_{out}(n) at the starting point of the algorithm is zero filled. The offset of the sample blocks obtained after IFFT relative to the first element of the array s_{out}(n) is equal to the offset of the sliding window in the array s_{in} (n).

At subsequent iterations of the algorithm, the sliding window is shifted by one sample and the actions described above are repeated. In such a way, the array of the time-domain samples of the signal s_{out}(n) is formed from the array s_{in}(n).

During the experimental investigations, the following parameters of the scrambling algorithm were used:

1) sampling frequency f_s=8 kHz (therefore bandwidth of the input signal is 4 kHz);

2) the sliding window size N=512;

3) weighting function type W(n): Blackman-Harris (the width of the major lobe at the level of –3 dB is 29.297 Hz, the level of the side lobes is –92 dB).

7. Investigation of the influence of the bands permutation order on the residual intelligibility of scrambled signal

In the course of experimental investigations, the residual intelligibility of the scrambled signals was estimated by the articulatory measurements in accordance with GOST 50840-95. For carrying such measurements, a group of 3 trained speakers (one male and two women) and auditors (one man and two women) without obvious defects of hearing and speech was invited. Preparation for the experiment included formation of audio files with test phrases read by each speaker and taken from articulatory tables (Appendix D, GOST 50840-95). Further, the audio files were scrambled and its verbal residual intelligibility was estimated by auditors. Thus, each estimation of intelligibility is averaged value obtained by all auditors after listening per 50 phrases dictated by each speaker.

For the investigation influence of the band permutation method on the residual intelligibility, the original signal spectrum was divided into 3 bands and all possible variants of the band permutations and spectral inversions were considered. The band cut-off frequencies corresponded to two methods of spectrum splitting: the equidistant and the octave.

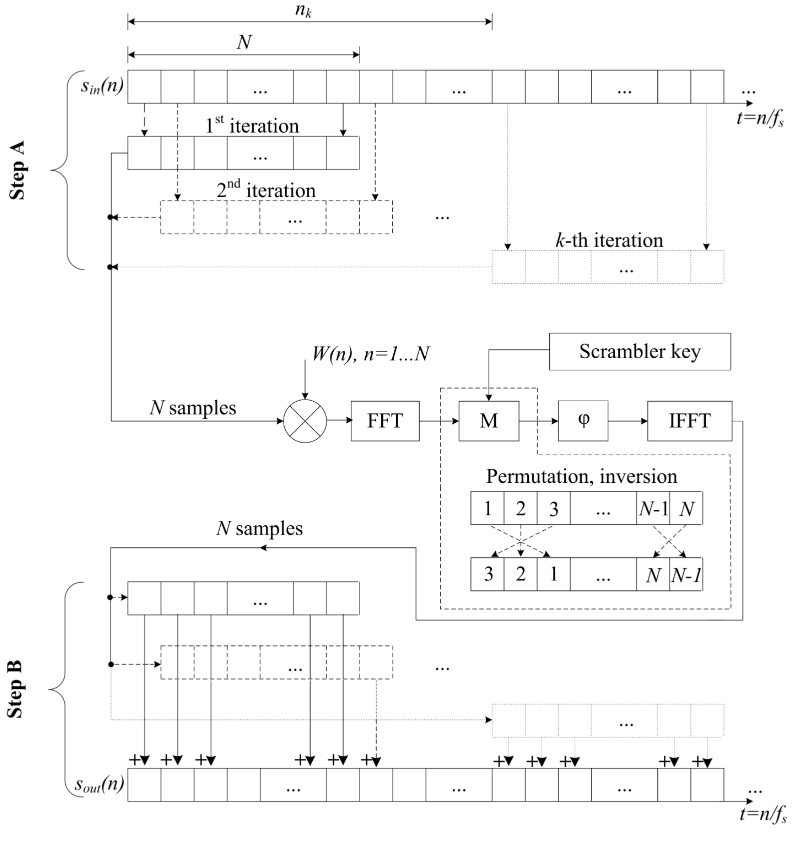

Fig. 2. Function diagram of the developed scrambling algorithm

The equidistant spectrum splitting method assumes that the original signal spectrum divided by bands with an equal width (the cut-off frequencies were 1.328 kHz and 2.656 kHz for 4 kHz signal bandwidth). In case of the octave splitting method, the widths of neighboring bands were related as 1:2 towards increasing of frequency (the cut-off frequencies of bands were 563 Hz and 1.703 kHz). Amount of bands used during investigation (3 bands) was optimal from the point of view of time expenditure required to exhaustive search all combinations. A similar number of bands were used in relatively simple scramblers based on specialized chips, for example, PCD4440T manufactured by Philips (the Netherlands). The obtained estimation of the scrambled signal residual intelligibility for equidistant and octave methods of splitting the spectrum of the original signal are shown in Fig. 3, *a, b*, respectively. Numbering of the bands shown in Fig. 3 was done from the low-frequency region towards high frequencies of the input signal spectrum.

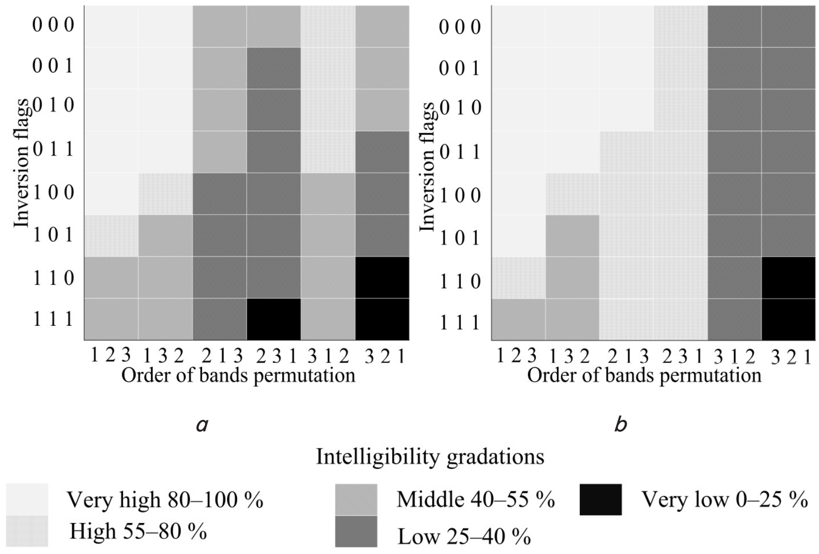

Fig. 3. Dependence of residual intelligibility on the order of permutations and inversions of the spectrum bands during the scrambling. Method of splitting of input signal spectrum: *a* — equidistant; *b* — octave

The results of experimental studies in Fig. 3 show that not all of the possible permutations provide a low level of residual intelligibility. It can be seen that such "effective" permutations include those in which the spectrum bands containing low-frequency speech components are moved to the high-frequency region. This feature corresponds to the assumption earlier made in Section 5. Moreover, the method of signal spectrum splitting (equidistant or octave) does not have a significant effect on the scrambled signal residual intelligibility.

8. Discussion of the results: estimation of speech signal security level in communication systems equipped with band scramblers

In absence of knowledge on the scrambler key, the most typical actions of an eavesdropper trying to hack the intercepted scrambled signal consists the following:

1) recording and multiple listening of the signal;

2) "full" inversion of the signal spectrum (flipping all its spectral components relative to the center frequency);

3) splitting the signal spectrum into a number of bands with equal width and its permutation with reverse order or exhausted search for all possible permutation combinations;

4) actions similar to i. 3 but the signal spectrum in each band is inverted;

5) analysis of the scrambled signal spectrogram for determining the bands cut-off frequencies by its distinctive features and performing the actions similar to those mentioned above.

In carrying out further studies, a successful hacking attempt denotes the result of such scrambled signal conversion after that its intelligibility became greater than the intelligibility of scrambled signal and exceeds 30 %. This threshold value of speech signal intelligibility corresponds to the possibility of recognizing individual words and expressions during tapping [17].

As was shown in Section 5, the algorithm that performs inversion of the entire signal spectrum ("full" inversion) is seems to be the most effective and simple of the listed methods of hacking. This algorithm can be realized simply by changing the sign of the value of every second sample of an input signal:

$$s_{inv}(n)=(-1)^{n}\cdot s_{in}(n), \qquad (4)$$

where $s_{inv}(n)$ is the stream of samples of the signal with inverted spectrum; n is the number of sample, n=1, 2, 3...

Experimentally obtained estimates of the scrambled signal intelligibility after hacking attempts using the algorithm of "full" inversion of its spectrum are shown in Fig. 4. Each of the given estimates of intelligibility (ξ) is equal to the maximum of two values:

1) residual intelligibility (corresponds to perceiving of the scrambled signal without its any transformation);

2) intelligibility after hacking the scrambled signal by the algorithm of "full" inversion. The estimates of intelligibility ξ were obtained from the results of attempts to hack signal scrambled with the equidistant method of splitting the spectrum on various numbers of bands. When the signal spectrum was split into 2...3 bands the strength to hacking of the scrambled signal was investigated using all possible variants of band permutations and band spectrum inversions. When spectrum was split into 4 or more bands, it was chosen 10 randomly variants of band permutations. The assumption of the possible spread of ξ values is based on the fact that among all possible variants of permutations of larger amount of bands there are those that repeat permutations with smaller amount of bands.

It can be seen from Fig. 4 that when speech signal spectrum is split into 32 or less bands voice information can be correctly understood from the scrambled signal itself or from the result of its spectrum inversion. This statement is true for speech signals with 4 kHz bandwidth regardless of values of band cut-off frequencies, the band permutation order and its inversions during scrambling. However, when signal spectrum is split into 64 bands or more this method of hacking does not give a similar result. This is due to the fact that there are variants of band permutations (scrambler keys) which ensure intelligibility below 30 % both before and after hacking by spectrum inversion. Therefore, in order to provide strength to this hacking method the required amount of bands should be at least 32…64.

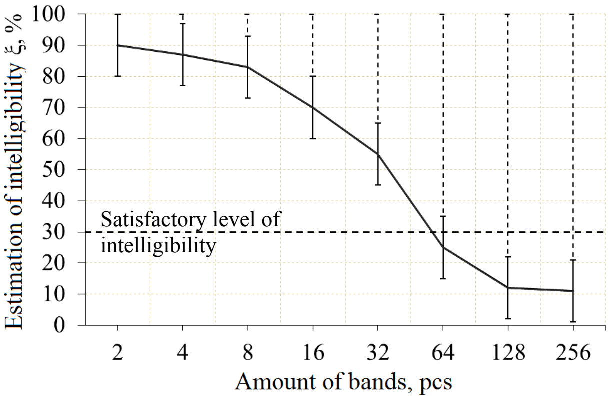

Fig. 4. Intelligibility of the scrambled signal after hacking attempts

One of the effective methods for ensuring low level of residual intelligibility and increasing strength to hacking by spectrum inversion or exhausted search of permutation combination is to increase the amount of permuted bands.

The main parameter which limits the maximum amount of bands is the minimal achievable bandwidth of the filters used in the scrambler. In the case of implementation of such filters in the scrambler using the algorithms similar to FFT, the minimal achievable bandwidth of filters depends on a number of factors.

Firstly, the bandwidth depends on the used weighting function and is inversely proportional to the length (size) of the window. The length of the window is determined by the allowable delay time for the scrambling-descrambling process. As was shown in Section 4, the conversation delay for narrowband speech communication systems should not exceed $\tau_{\max}$=50…200 ms. Therefore, the FFT window length (size) should be:

$$\tau_{\mathrm{FFT}_{\max}} \leq \tau_{\max}/2;\ \tau_{\mathrm{FFT}_{\max}} \leq 25...100\ \text{ ms}.$$

For example, for the sampling frequency of the original speech signal f_s=8 kHz (sampling period is $T_s=1/f_s$=125 μs), the maximum FFT window size is

$$N_{\max} \leq \tau_{\mathrm{FFT}_{\max}}/T_s;\ N_{\max} \leq 200...800\ \text{ samples}.$$

The FFT algorithm requires that the window size must be a multiple of 2^N, here N is an integer number. Therefore, the window size $N_{\max}$ is limited of 512 samples. As is known, the maximum amount of bands into which the signal spectrum can be split is equal to half the window size [25]. Consequently, the maximum amount of bands is 256.

Secondly, the maximum amount of bands is limited by the level of signal distortions that are caused by "leakage of spectral components" and "tailing of spectrum maxima" after the speech signal scrambling-descrambling process [25]. These distortions can be experimentally estimated by the dependence on amount of bands of the maximum of the cross-correlation function (CCF) between the original speech signal and the signal obtained after the scrambling-descrambling process of the original one. The Fig. 5 presents the estimates of the CCF maximum values were obtained by averaging the results of 10 sessions of scrambling-descrambling the original speech signal for different amount of bands. During the scrambling there were used two types of weighting functions W(n): rectangular and Blackman-Harris, the method of original signal spectrum splitting was equidistant. The rest of parameters of the scrambling algorithm remained similar to those given in the description of the experimental equipment.

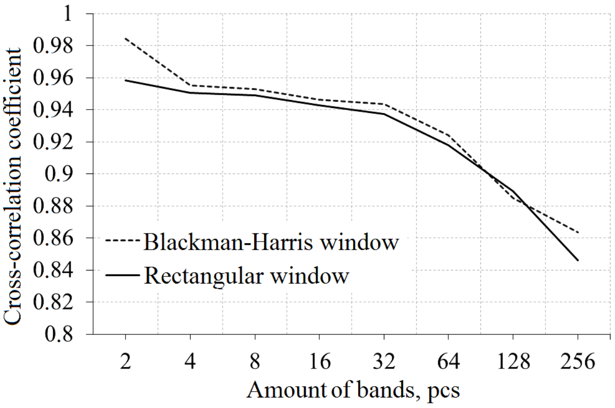

Fig. 5. Estimation of the signal distortions caused by scrambling-descrambling process with different amount of permuted bands

The results shown in Fig. 5 confirm that the level of distortion of speech signal increases with growth of the amount of permuted or inverted bands after scrambling-descrambling. These distortions were heard in the form of a metallic hue against the background of the speech without worsening of intelligibility (the intelligibility was 90 % or more).

9. Conclusions

A number of actual aspects related to the development and operation of speech scrambling devices have been studied. In particular, it was shown that due to the ease of implementation and the property of leaving the signal bandwidth without expending, scramblers can be used as affordable and inexpensive means of information security in speech communication systems.

1. Comparative analysis of scrambling and encryption methods has shown that scrambling is the only method that provides secure transmission of voice information in real-time over narrowband communication channels with a signal-to-noise ratio of 0 dB or less.

2. Experimental studies performed on the developed band scrambler have shown that depending on the band permutation order and choice of cut-off frequencies of the bands, the residual intelligibility of the scrambled signal varies from 10 to 90 %. It should be noted that for intelligibility above 30 %, voice messages can be perceived with a satisfactory quality despite scrambling. It has also been established that the minimum level of residual intelligibility of the scrambler output signal is provided by band permutations which translate low-frequency components of speech to the high-frequency region.

3. The performed experimental studies of the scrambled signal security level have shown that when number of bands less than 32, such signal can be hacked by applying a relatively simple operation of the entire frequency band spectrum

inversion. When the number of bands greater than 32, there are variants of band permutations that provide scrambled signal residual intelligibility in the range of 10...20 %, additionally such scrambled signal cannot be hacked by inversion of its entire spectrum. It was also shown that for real-time speech communication systems the maximum number of bands is limited by two factors: the delay time and the distortion caused by scrambling-descrambling process. Thus, the maximum amount of bands is 256 for the delay of 128 ms, 4 kHz bandwidth of the communication channel and level of distortions which lead to degradation of descrambled signal intelligibility not lower than 90 %.

The presented results show strong sides of use of speech scrambling methods compared to encryption for protection against tapping. The obtained results can be used for development of scramblers based on digital processing of speech signals. In addition, these results can be useful for selection scrambler keys that are optimal by the criteria of strength to hacking, the minimum level of residual intelligibility and the level of distortions caused by scrambling-descrambling process.

References

1. Torokin, A. A. Inzhenerno-tehnicheskaja zashhita informacii [Text]: uch. pos. / A. A. Torokin. – Moscow: Gelios ARV, 2005. – 960 p.
2. Lenkov, S. V. Metody i sredstva zashhity informacii. Vol. 2 [Text] / S. V. Lenkov, D. A. Peregudov, V. A. Horoshko; V. A. Horoshko (Ed.) // Informacionnaja bezopasnost'. – Kyiv: Ariy, 2008. – 344 p.
3. Srinivasan, A. Review of analog audio scrambling methods for residual intelligibility [Text] / A. Srinivasan, P. Selvan // Innovation Systems Design and Engineering. – 2012. – Vol. 3, Issue 7. – P. 22–38.
4. Konahovich, G. F. Zashhita informacii v telekommunikacionnyh sistemah [Text] / G. F. Konahovich, V. P. Klimchuk, S. M. Pauk, V. G. Potapov. – Kyiv: Ariy, 2008. – 344 p.
5. Gorbenko, I. D. Principy zashhity rechevyh soobshheniy v kommunikacionnyh sistemah [Text]: uch. pos. / I. D. Gorbenko, A. A. Zamula, I. N. Presnyakov. – Kharkiv: KNURE, 1997. – 116 p.
6. Jayakurami, J. A review of analog speech scrambling for secure communication [Text] / J. Jayakurami, G. Dhanya // Progress in science and engineering research journal. – 2016. – Vol. 2. – P. 194–198.
7. Lim, Y. C. Quality Analog Scramblers Using Frequency-Response Masking Filter Banks [Text] / Y. C. Lim, J. W. Lee, S. W. Foo // Circuits, Systems and Signal Processing. – 2009. – Vol. 29, Issue 1. – P. 135–154. doi: 10.1007/s00034-009-9113-8
8. Weinstein, S. B. Sampling based techniques for voice scrambling [Text] / S. B. Weinstein // Proc. Int. Conf. Commun. – 1980. – P. 16.2.1–16.2.6.
9. Lee, L. S. A simple sample value scrambler using FFT algorithms for secure voice communications [Text] / L. S. Lee, Y. P. Harn, Y. C. Chen // Proc. Nat. Telecommun. Conf. – 1980. – P. 49.4.1–49.4.5.
10. Verchyk, D. Ju. Osobennosti tehnicheskoj realizacii i primeneniya algoritmov skremblirovaniya rechi [Text] / D. Ju. Verchyk, V. D. Kukush // Radioelektronika i molodezh' v XXI veke. – Kharkiv: KNURE, 2016. – Vol. 3. – P. 81–82.
11. De Andrade, J. F. Speech privacy for modern mobile communication systems [Text] / J. F. de Andrade, M. L. R. de Campos, J. A. Apolinario // 2008 IEEE International Conference on Acoustics, Speech and Signal Processing. doi: 10.1109/icassp.2008.4517975
12. Matsunaga, A. An analog speech scrambling system using the FFT technique with high-level security [Text] / A. Matsunaga, K. Koga, M. Ohkawa // IEEE Journal on Selected Areas in Communications. – 1989. – Vol. 7, Issue 4. – P. 540–547. doi: 10.1109/49.17718
13. Jayakurami, J. An efficient voice scrambling technique for next generation communication systems [Text] / J. Jayakurami, G. Dhanya // International Journal of Engineering and Technology. – 2016. – Vol. 8, Issue 1. – P. 293–299.
14. Tseng, D.-C. An OFDM-Based Speech Encryption System without Residual Intelligibility [Text] / D.-C. Tseng, J.-H. Chiu // IEICE Transactions on Information and Systems. – 2008. – Vol. E91-D, Issue 11. – P. 2742–2745. doi: 10.1093/ietisy/e91-d.11.2742
15. Lee, L.-S. A New Frequency Domain Speech Scrambling System Which Does Not Require Frame Synchronization [Text] / L.-S. Lee, G.-C. Chou, C.-S. Chang // IEEE Transactions on Communications. – 1984. – Vol. 32, Issue 4. – P. 444–456. doi: 10.1109/tcom.1984.1096078
16. Lee, J. W. Efficient fast filter bank with a reduced delay [Text] / J. W. Lee, Y. C. Lim // APCCAS 2008 – 2008 IEEE Asia Pacific Conference on Circuits and Systems. – 2008. doi: 10.1109/apccas.2008.4746299
17. Sapozhkov, M. A. Elektroakustika [Text] / M. A. Sapozhkov. – Moscow: Svyaz', 1978. – 272 p.
18. Rukovodstvo po proektirovaniyu sistem zvukovogo obespecheniya na stroyashchikhsya i rekonstruiruemykh obektakh g. Moskvy [Electronic resource]. – Besplatnaya biblioteka standartov i normativov. – 2000. – Available at: http://www.docload.ru/Basesdoc/8/8269/index.htm
19. Flanagan, D. L. Analiz, sintez i vospriyatie rechi [Text] / D. L. Flanagan. – Moscow: Svyaz', 1968. – 396 p.
20. Spravochnik po tehnicheskoy akustike [Text] / M. Heckl, H. A. Muller (Eds.). – Leningrad: Sudostroenie, 1980. – 440 p.
21. Olifer, V. G. omp'yuternye seti. Principy, tehnologii, protokoly [Text] / V. G. Olifer, N. A. Olifer. – 4-e izd. – Saint Petersburg: Piter, 2010. – 944 p.
22. Sklar, B. Cifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie [Text] / B. Sklar. – 2-e izd. – Moscow: Izdatel'skij dom «Vil'yams», 2003 – 1104 p.
23. Kondoz, A. M. Digital speech: coding for low bit rate communication systems [Text] / A. M. Kondoz. – 2-nd ed. – John Wiley & Sons Ltd, 2004. – 459 p. doi: 10.1002/0470870109
24. Basics of the STI-measuring method [Electronic resource]. – Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.501.8775
25. Ifeachor, E. C. Cifrovaya obrabotka signalov: prakticheskiy podhod [Text] / E. C. Ifeachor, B. W. Jervis. – 2-e izd. – Moscow: Izdatel'skiy dom «Vil'yams», 2004. – 992 p.