ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)*

UDC 004.056.5+534.8 DOI: https://doi.org/10.30837/ITSSI.2023.23.096

M. MOZHAIEV, O. MOZHAIEV, Y. GNUSOV, V. STRUKOV, P. KLIMUSHIN, D. YEVSTRAT

ANALYSIS OF ACOUSTIC INFORMATION PROTECTION METHODS IN CRITICAL APPLICATIONS

Subject of the study: the process of acoustic information protection in computer systems of critical applications to ensure the required level of system security. **The aim** of the article is to analyze the methods of acoustic information protection in computer systems of critical application by means of masking to ensure the impossibility of unauthorized access to the system. The article solves the following **tasks**: to analyze the software and hardware masking of speech; to study the masking of speech messages in order to introduce unrecognizability; to study the features of speech message compression; to investigate methods of covert transmission of acoustic information. The **results** of the work, which were obtained using mathematical methods of information transformation in computer systems, are potentially possible methods of masking speech messages to ensure the impossibility of unauthorized access to the system. The analysis of the functioning of the presented methods has led to the following **conclusions**. One of the perspective directions of acoustic information protection in communication channels and dedicated premises can be considered the creation and development of computerized speech masking systems along with or in conjunction with traditional technologies of semantic protection of acoustic information, namely, speech signal classification based on cryptographic algorithms. The main requirements for today's systems that provide protection of acoustic information in critical computer systems are speed and efficiency of various speech signal processing procedures using standard inexpensive technical means of computer telephony, namely: a personal computer, sound card, telephone line interface device and/or modem. These requirements can be met by applying digital methods of dynamic spectral analysis, i.e. synthesis of speech and audio signals. The choice of specific methods and means of speech masking as one of the types of semantic protection of acoustic information will depend on the practical requirements for the speech protection system and the technical characteristics of the acoustic information transmission channel. Further research is desirable to analyze the possible use of methods for synthesizing large ensembles of quasi-orthogonal discrete signals with improved ensemble, structural and correlation properties to ensure higher security indicators of acoustic channels in computer systems of critical applications.

Keywords: acoustic information; masking of acoustic information; technical protection; cryptographic protection; steganographic (steganophonic) protection; speech modification; speech message compression; computer systems.

Introduction

Protecting acoustic (speech) information is one of the most important tasks in the overall set of measures to ensure the information security of an object or institution.

The unique features of speech information (SI) circulating in closed rooms and outside them: a large volume and speed of exchange, high confidentiality of some messages, the ability to identify the person making the message, and even the ability to determine the personal attitude to the information being voiced and to draw up a psychological portrait of the person concerned determine the relevance and extreme importance of solving the problem of protecting speech confidential information (SCI). Despite the growing role of automated information systems, speech information still plays a key role in information traffic (up to 80 per cent of the total information flow) [1, 2]. This is especially important today in the context of Russia's military aggression. Therefore, in recent years, more and more attention has been paid to ensuring the security of acoustic information. On the one hand, this is due to the high polyinformativeness of acoustic information. On the other hand, it is due to the diversity of information threats in relation to acoustic (speech) information and the peculiarities of their development and implementation scenarios. All of this is reflected in a wide variety of modern methods, algorithms, software and hardware for protecting acoustic information from unauthorized access. The main areas of acoustic information protection are considered to be technical, cryptographic and steganographic (steganophonic) protection.

A separate section is devoted to the issue of acoustic information protection by masking acoustic information based on modern computer technologies. In recent years, this area has been gaining more and more practical interest among software manufacturers. In order to provide basic security services for audio signals, complex software systems are being created, new methods for receiving, transmitting, processing, and presenting audio signals are being developed and used. Therefore, this article is devoted to the analysis of methods for

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

protecting acoustic information that exists in modern information systems of critical applications to ensure a higher level of security of such systems.

Literature analysis

To intercept speech information, an alleged "adversary" (a person or group of persons interested in obtaining this information) can use a wide range of portable acoustic speech intelligence tools that allow intercepting speech information by direct acoustic, vibroacoustic, electroacoustic and opto-acoustic-electronic means, including [3, 4]:

– portable sound recording equipment (small-sized recorders, tape recorders and recording devices based on digital circuitry)

– directional microphones;

– electronic stethoscopes;

– electronic devices for intercepting speech information (bugging devices) with microphone and contact type sensors with transmission of intercepted information via radio, optical (in the infrared wavelength range) and ultrasonic channels, power supply network, telephone lines, connecting lines of auxiliary technical means or special lines;

– optoelectronic acoustic systems, etc.

Portable sound recording equipment and embedded devices with microphone-type sensors (transducers of acoustic signals propagating in air and gas environments) can be installed when individuals ("agents") are uncontrollably present directly in designated (protected) premises. This equipment provides recording of medium-loud speech when the microphone is removed at a distance of up to 15...20 m from the source of speech [3, 4].

Recently, both developers and consumers of semantic protection of acoustic information have been observing an increasingly steady trend to use new computer technologies for ensuring the security of speech communications without the use of classical cryptographic methods. In this regard, computer-based technologies for masking acoustic information are becoming increasingly attractive. However, one should not forget about cryptographic methods of protecting acoustic information, such as instantaneous crypto analysis of GSM with only ciphertext [5]; real-time crypto analysis of the assumed A5 stream cipher [6, 7]; crypto analysis of anomalous behavior of a computer system [8]; crypto-resistant methods and random number generators in the Internet of Things (IoT) devices [9].

The aim of the article is the analysis of methods for protecting acoustic information in critical computer systems by means of masking to ensure the impossibility of unauthorized access to the system.

To achieve this goal, we need to solve the following partial tasks:

– analyze the software and hardware language masking;

– to conduct a study of speech message masking for the purpose of introducing unrecognizability;

– to study the features of speech message compression;

– to study methods of covert transmission of acoustic information.

Masking of acoustic information on the basis of modern computer technologies

In this part of the article, we will study the effect of acoustic information masking based on modern computer technologies. For this purpose, Fig. 1 shows a generalized classification of acoustic information masking methods.

At lower financial costs for the development (primarily software), distribution and acquisition of such technologies, they can become a kind of buffer between cryptographic systems and systems of physical (technical) protection of acoustic information in communication channels. In addition, with the help of such technologies, it is possible to solve a number of other no less important tasks of ensuring the security of acoustic information than the technical closure of speech communication in order to protect it from unauthorized access by introducing indecipherability. For example, it is possible to covertly transmit acoustic information through various communication channels, change one's voice to achieve unrecognizability while maintaining natural sound.

Software and hardware language masking

Recently, a lot of software and hardware tools for language closure have appeared. These tools are essentially software analogues of well-known technical means of masking (maskers and scramblers). Under software and hardware speech closure, we will understand speech masking technologies, which refer to methods and means of semantic protection of acoustic information. They are aimed at ensuring the illegibility of a speech message. Their implementation in practice can be expressed in the mixing of speech with noise

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

and interference and/or in the modification of speech messages according to parameters calculated from its description according to a known transformation law (closure – recovery).

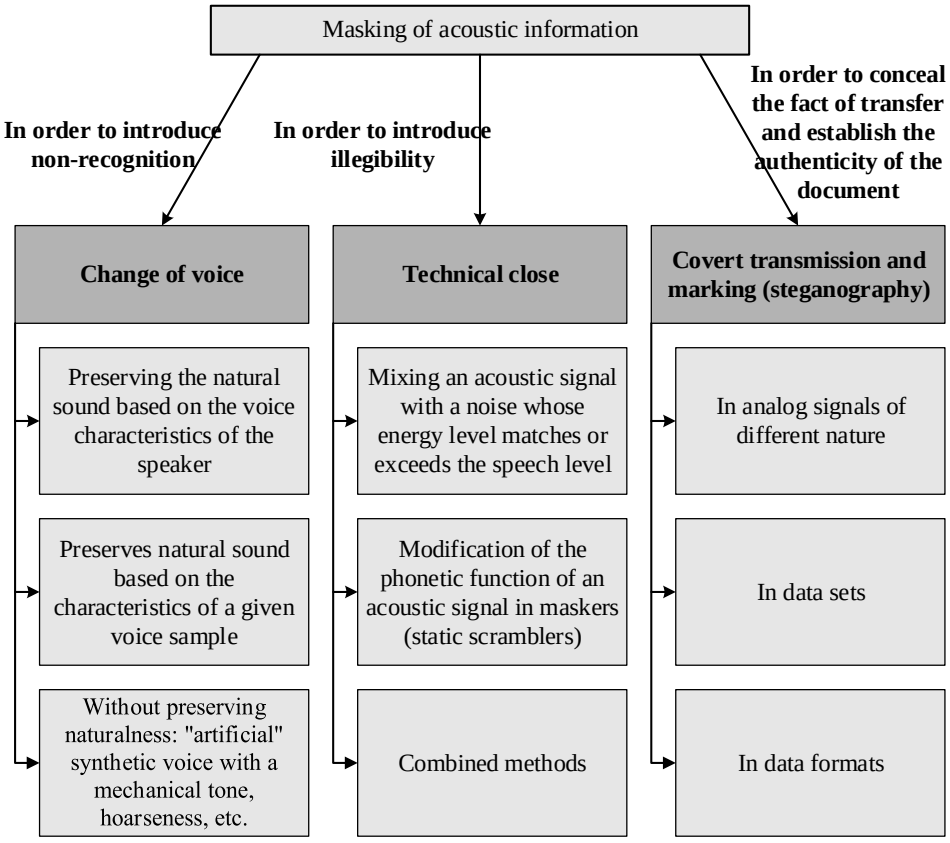


Fig. 1. General classification of acoustic information masking methods

A common type of software and hardware speech closure is the mixing of the original speech message with interference in order to transmit a new audibly indistinguishable sound signal, usually in the same frequency band as the original. Knowing the nature of the change and the type of interference, the receiving end of such a secure speech communication channel neutralizes its effect with additional cleaning and amplification of the restored speech signal. Thus, the lower panel of Fig. 2 shows the result of removing a quasi-harmonic interference from the payload, which significantly exceeds the energy level of the speech communication of interest.

There are different types of implementations of this type of masking: when the interference is comparable in power to the original speech message or significantly higher, when the interference is noise, quasi-harmonic or speech-like, etc.

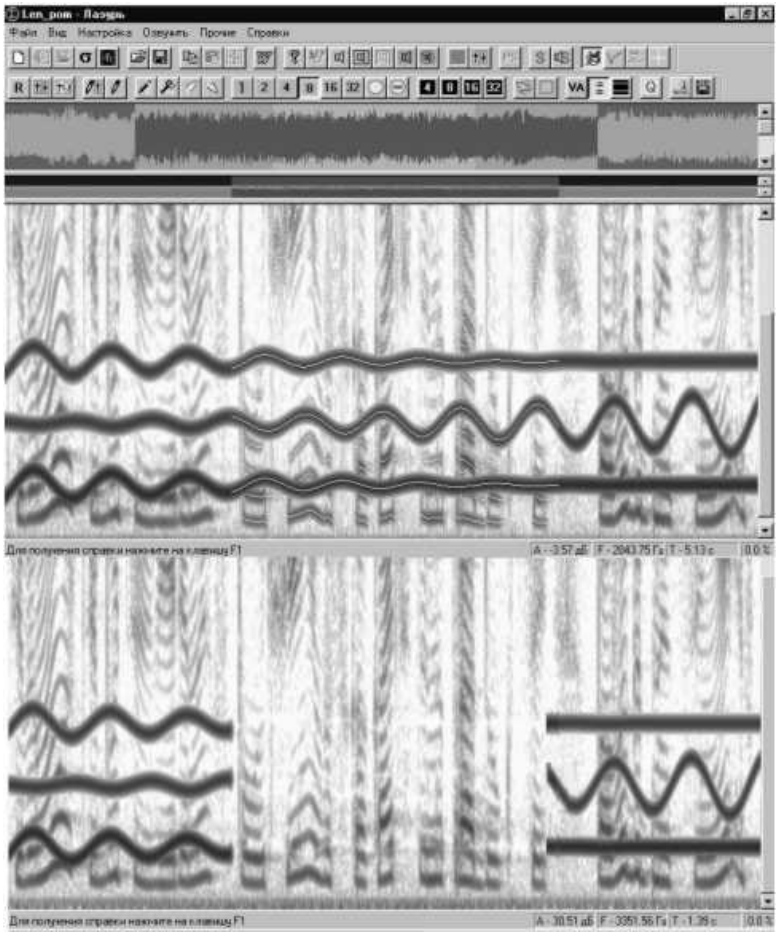
Speech modification will be understood as a transformation of the original speech signal, primarily its phonetic function, in order to achieve its illegibility and/or unrecognizability according to a known given law, when the parameters of this transformation at the transmitting end of the communication channel are either known in advance or are extracted from the original signal itself and do not change during the entire communication session.

At the receiving end, these transformation parameters are either also known in advance or are extracted from the received modified signal in order to restore the unintelligible speech message according to the same known law.

It should be noted that at the receiving end, it is not always necessary to restore the original signal in the form in which it was originally. For example, this applies to acoustic information synthesized from a graphical image of a sonogram recovered from a closed image without taking into account the initial values of the phase spectral components. In this case, the waveforms (oscillograms) of the original and restored speech message will be different, and their intelligibility and sound will be exactly the same. This fully reveals the properties of

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

human auditory perception, which is weakly dependent on the phase relations of simple narrowband components of a complex sound signal. Hence the conclusion: if the images of correctly calculated dynamic spectrograms of different acoustic signals are similar, they will sound (be perceived by ear) in the same way.



Upper – creating a powerful quasi-harmonic interference in the speech signal.
Bottom – removing the interference from the useful mixture at the receiving end of the communication channel.
Fig. 2. Masking speech with a quasi-harmonic barrier

The main task that is solved by software and hardware speech closure using the described approach is to modify the speech so that the modified speech is completely unintelligible. This task is solved by dynamically changing the envelope of the amplitude spectrum of the speech message, i.e., by modifying its formant structure.

Examples of practical implementation of methods for such modification of a speech message include a simple inversion of speech in the tone frequency channel band. More labor-intensive, and not previously used in practical applications, is the procedure of inversion of the cyclic shift of the spectrum envelope, while maintaining the same harmonic structure of the original speech message. It is also possible to implement combined methods of software and hardware acoustic information closure: modification of a speech message with simultaneous imposition of interference. An example is spectrum inversion plus quasi-harmonic interference.

It should be noted that in some publications, speech maskers, such as spectrum inverters and the like, are referred to as a simple type of analogue static scramblers in which the speech conversion "key" does not change during the entire session or during a group of communication sessions. In other words, when we talk about closing acoustic information, we mean the use of permanent specific laws of speech conversion that introduce illegibility into acoustic information and are implemented in speech maskers, and when we talk about classifying a speech message, we mean the use of cryptographic algorithms.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

It is also possible to combine the implementation of software and hardware methods of acoustic information classification: modification of the speech message with the simultaneous imposition of interference. An example is spectrum inversion plus quasi-harmonic interference.

In other words, when we talk about acoustic information closure, we mean the use of permanent specific laws of speech transformation that introduce illegibility into acoustic information and are implemented in speech maskers, and when we talk about speech message classification, we mean the use of cryptographic algorithms.

Thus, the technologies of software and hardware closure of acoustic information.

Masking of speech messages to introduce non-recognition

The impetus for widespread use of these technologies for masking sounds and speech has been provided by the rapid development of multimedia and new approaches to the description and processing of speech signals in recent years. One of them is an approach to the construction of special software and hardware for ensuring the security of speech communications, which combines the idea of translating a sound (speech) signal into the form of corresponding graphic images and back from image to sound or speech without loss of information content and/or intelligibility with the capabilities of known and promising digital image processing methods.

The main core of such an approach is the development and application of methods for detecting and reconstructing the parameters of the narrow-band Hilbert signals present in these images. Such a parametric description of a complex initial acoustic (speech) signal allows either to completely reproduce its sound or to restore and sound a "new" sound signal according to the properties changed and specified in such a parametric description.

To study such an approach to ensuring the security of speech messages using acoustic signal masking, it is feasible to apply methods of processing speech messages by transforming graphical images of the corresponding spectrograms. As an analytical representation of the speech signal, we use its Hilbert description:

$$(t) = G(t)Cos\Psi(t), \qquad (1)$$

where $G(t)$ – envelope of speech signal,

$\Psi(t)$ – full phase of the speech signal.

These parameters describe this signal as a narrowband process in a limited frequency band and are related to each other using the Hilbert transform:

$$s(t) = \frac{1}{\pi}\int_{\infty}^{i}\frac{s_G(\tau)}{(\tau - t)d\tau}\ ,$$
$$s_G(\tau) = \frac{-1}{\pi}\int_{\infty}^{i}\frac{s(\tau)}{(\tau - t)d\tau}, \qquad (2)$$

where $s_G(\tau)$ – the function associated by Hilbert with the output signal $s(t)$.

Then

$$G(t) = \sqrt{s^2(t) + s_G^2(t)}\ ,$$
$$\Psi(t) = arctg\frac{s(t)}{s_G(t)}. \qquad (3)$$

To describe a complex speech message, it can be represented as a whole narrowband signal or as a set of elementary K narrowband processes:

$$s(t) = G(t)\cos\Psi(t) = \sum_{k=1}^{K} g_k(t)Cos\Psi_k(t), \qquad (4)$$

where $g_k(t)$ – Hilbert component,

$\Psi_k(t)$ – full phase of the k-th narrowband component.

However, it is now recognized that the most adequate form of an elementary narrowband signal is its representation as a Morlet wavelet. Given this assumption, we can obtain:

$$s(t) = G(t)\cos\Psi(t) = \sum_{k=1}^{K_{i\Omega}} A_i e^{-t^2/\sigma_{ik}}\cos(\omega_{0k}t + \varphi_{0k}) + s_з, \qquad (5)$$

where A_i is the corresponding amplitude of the k-th envelope;

σ_{ik} is the attenuation coefficient of the k-th envelope amplitude;

ω_{0k}, $.\varphi_{0k}$ are, respectively, the center frequency and initial phase $K_{i\Omega}$ of the narrowband signals or wavelets that make up the speech signal;

$s_з$ – a function of the error of representation or noise.

According to model (5), at short time intervals within each R-step of temporal analysis, the following parameter vectors can act as primary descriptions of a speech message represented as a superposition of elementary narrowband processes:

$$\{A_k, \omega_{0k}, .\varphi_{0k}\}_{t=\tau R} \qquad (6)$$

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23) ISSN 2524-2296 (online)

In most speech information protection programs, only the first two parameters are sufficient, and then the parameter vector can be represented as:

$$\{A_k, \omega_{0k}\}_{t=\tau R}. \quad (7)$$

Studies based on model (5) have shown that the data necessary to calculate the parameters of elementary narrowband signals that make up the original sound or speech can be contained in the dynamic spectral images of this acoustic signal, namely, in the images of correctly calculated amplitude sonograms and/or spectrograms. Such images can be obtained in the course of dynamic spectral analysis – synthesis of sounds and speech, sliding over the original signal with the selected analysis window with the transition from the samples weighted by it to their frequency image based on the adopted orthogonal basis. One example of such procedures is short-term analysis, i.e., Fourier synthesis of audio signals. Although, in some applications of speech communication security, not only harmonic, but also other bases, such as Wavelet functions, can be used to perform dynamic spectral analysis - synthesis of sounds and speech, short-term analysis – Fourier synthesis of audio signals and speech is traditionally used more often [10–11].

The parameters of narrow-band Hilbert elementary sound signals, which constitute the sound of the original sound or speech, are detected in the images of dynamic spectrograms as a set of contours (lines) of brightness difference or tracks (chains) of local and global extremes of colour saturation in the levels of one colour. With the help of special software (for the example shown in Fig. 3. the program "Real Time Audio 3D Spectrum 1.1" was used) along similar contours (tracks), which are visible on the frequency-time grid of dynamic spectrograms (see Fig. 3, top panel), it is possible to distinguish frequencies, amplitudes, phases of elementary sounds of a complex acoustic (speech) signal, and then reconstruct, modify, destroy, and create them anew to solve a specific task of ensuring the security of speech communication using various known methods and tools of digital image processing. Thus, the selected area in the center of the upper panel of Fig. 3. of the graphic image of the speech signal can be applied to a powerful arsenal of tools provided by well-known graphic editors such as Adobe Photoshop, Corel Draw, Photo Editor and others. After the necessary processing of this section of the spectrogram image in the selected graphic editor, it can be inserted back into its original place for further synthesis and listening to the new acoustic or speech signal modified in this way.

It should be noted that currently the choice of special software tools for sonogram processing is quite wide. The most well-known software products can be cited: Real Time Audio 3D Spectrum, Adobe Audition of various versions, SmartSound SonicFire Pro, etc. However, most of them only allow you to obtain sonograms of speech messages. Only a few of them allow you to perform the full processing cycle (including the backward embedding of processed sonograms), and these programs are not freely distributed software.

Let us consider in more detail the different classes of acoustic information masking realized by the proposed approach to processing speech messages through the processing of their graphical images.

Artificial voice systems

While traditional voice changers have not paid much attention to the sound quality (naturalness and authenticity) of artificial speech, the situation is changing. For example, there are reports of software products that search by voice pattern. Often, when conducting investigations, operatives have to impersonate another person for disguise. All this leads to the task of qualitative voice alteration in the course of measures for the comprehensive protection of acoustic information.

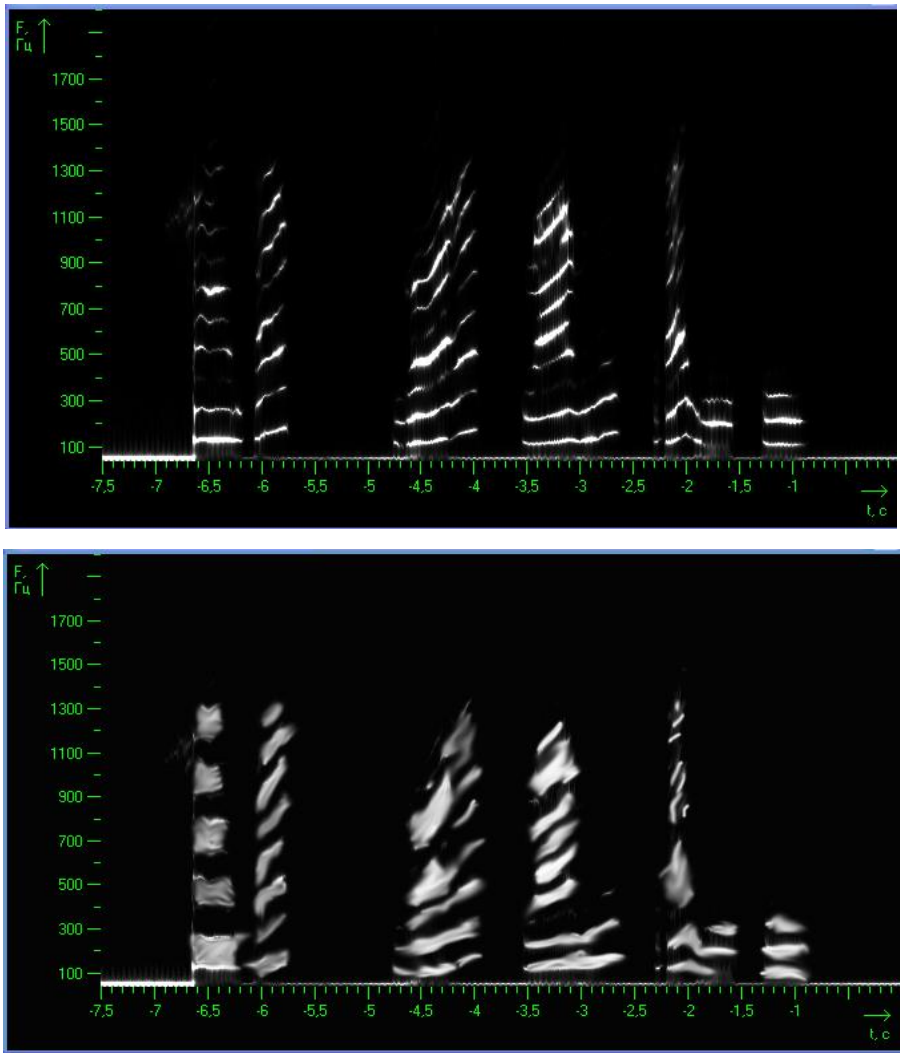
This is a rather difficult task, as each person's voice is individual and recognizable. Moreover, auditory perception is so perfect that it allows us to recognize the subtlest shades of the speech signal. The human ear can accurately determine the signs of artificiality and naturalness of speech.

A speech message can be represented in the form of a speech signal, which in turn can be used for reverse speech reproduction. In other words, it is possible to put an equivalence sign between the sound language and its representation in the form of a speech signal, including in the digitized form contained in computer files.

It is known that speech is a complex process of communication between people, which includes both information about the individual voice of the speaker and information about phonetic quality. Therefore, it is important to ensure the correct choice and justification of the system of features that will determine the principle of speech construction. The main features responsible

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

for the individual colouring of speech can be divided into two groups: those related to the physiological mechanisms of speech production and those related to the ways of putting it into action (activity, articulation).



Above: a natural male voice with the trajectories of narrowband speech components highlighted.
At the bottom, an artificial male voice synthesized according to a given sample.
The maximum power of the studied signal in the frequency-time grid node is indicated in white, the minimum power in black, and the intermediate values in gray.

Fig. 3. Sonogram of the phrase "Kharkiv is a city of traditions"

The first group of features is based on the well-known model of the speech tract, which consists of a transmission function of the resonant system and an excitation signal pulse generator. The transfer function almost completely characterizes the individual geometric shape of the cavities of the speech apparatus. The main parameters here are the characteristics of the four formant regions (average frequency, frequency range, and energy), spectrum envelope, formant trajectories and derivatives of these parameters.

To calculate parameters related to the physiological characteristics of the speech tract, spectral-time analysis methods are most often used. Such methods of speech signal analysis are adequate to the natural mechanism of speech perception. Such methods are often based on classical Fourier analysis or parametric autoregressive analysis (linear prediction as a special case).

The second group of parameters also includes intonational characteristics of the speech stream, such as intensity, intonation, stress system, and rhythmic pattern of the speech phrase.

Among the parameters of the speech signal that determine the individuality of a person's voice,

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

it is necessary to distinguish integral parameters of speech that cannot be attributed to any of the groups considered, but they are strongly correlated with them and are formed under the influence of the anatomical features of the speech-forming tract and human articulation. That is, the analysis of integral parameters makes it possible to determine the peculiarities of individual pronunciation for speech segments of different phonetic content.

The creation of high-quality voice changers based on standard office equipment is possible when implementing the proposed approach through image processing of its graphic images. Specialized software of such a computer system should modify both the harmonic structure of the speech signal, which usually contains individual features of the speaker.

Such procedures can already be carried out on images of dynamic sonograms with the subsequent synthesis of a new artificial speech signal from the modified graphic image. A combination of such actions with correctly performed calculations will likely achieve the desired result. Some difficulties may arise when modifying paused areas. Therefore, the task of reliable detection of tonal and noise areas in the speech stream requires a solution.

It is clear that only through software implementation on standard hardware will such a voice changer be not only much cheaper than existing analogues, but also provide a better, truly natural sounding artificial speech signal. Software implementation will allow for smoother voice changes from male to female, from child to adult.

Compression of speech messages

The task of compressing speech messages can also be solved by processing sonogram images. The processing scheme is as follows: first, the speech message is converted into its graphical image – a sonogram within the selected analysis window during dynamic spectral analysis – synthesis of sounds and speech; then this sonogram image is compressed using one of the image compression methods, and the compression ratios are transmitted to the communication channel; using the received compression ratios, the image of the original sonogram is reconstructed at the receiving end of the communication channel, which is then used to synthesize a new speech message. The advantage of this method of speech coding is that only one initial description of the speech message is used – a sonogram with traces of phono objects, based on which it is possible to obtain almost any required speech coding rate, which is determined by the bandwidth of the communication channel at a given time. At the same time, the maximum possible intelligibility and sound quality of the restored speech is preserved. The results of some recent studies have shown that by applying fractal or special wavelet-based compression methods to sonogram images, a minimum encoding rate of 800 bps can be achieved while maintaining verbal intelligibility of about 80%.

The sonogram of the initial speech area, the image of which will be used for compression by digital image processing methods, is shown in the upper panel of Fig. 4. A rough oscillogram of the entire speech message under study is drawn above the sonogram, indicating the location of the selected fragment.

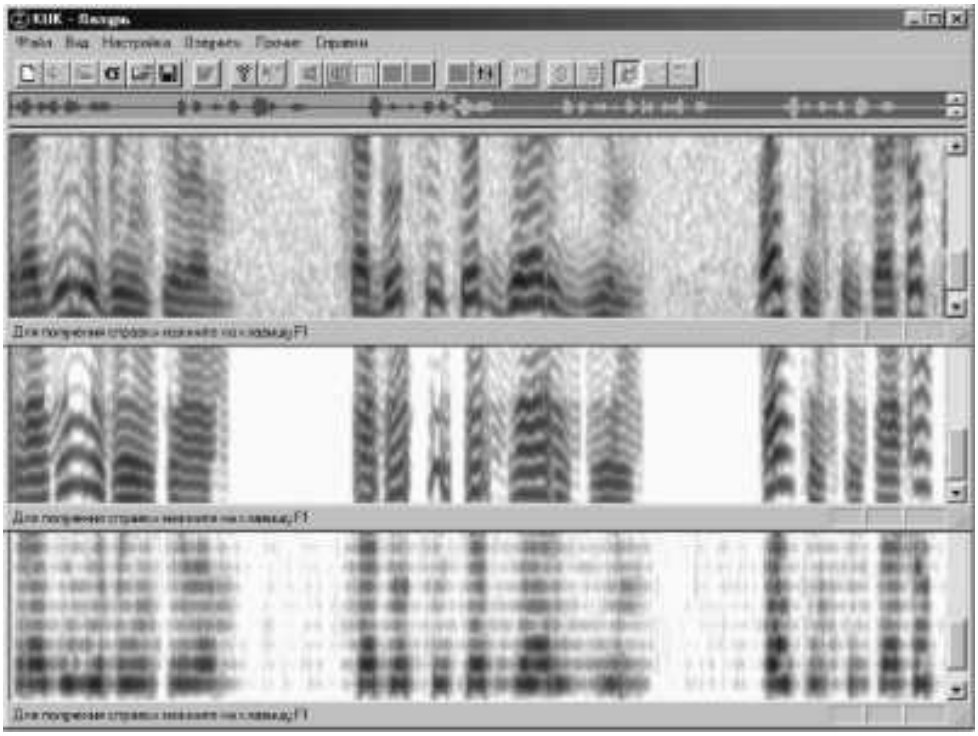
A sonogram of the same speech segment restored after compression using the proposed method to a rate of 1000 bits/s and a sonogram of the same speech segment restored after compression to 800 bits/s by extracting information about the melody of the main tone using digital image processing methods are shown in the middle and lower panels of Fig. 4. I t is possible to see that the sonogram of the speech recovered after compression at 1000 bits/s is more similar to the sonogram of the original speech message than the sonogram of the signal recovered after compression of the image obtained by means of the fundamental tone equalization. That is why the first restored speech message sounds better and more natural than the second, despite their equal high intelligibility.

Hidden transmission of acoustic information

At present, measures to ensure the security of voice communications can be aimed not only at preventing unauthorized acquisition of acoustic information, but also at concealing the very fact of its transmission, by using standard technical means, conventional, traditional information exchange protocols and publicly available communication channels for these purposes.

In recent years, this area of information security in computer telecommunication systems, called "stegology" (sometimes "stealthology"), has been actively developing around the world.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)



Above: a sonogram of the original speech fragment under study.
In the center, a sonogram of the speech signal recovered after compression at 1000 bits/s using one of the image compression algorithms of the original sonogram.
Bottom – a sonogram of the speech signal restored after compression to 800 bits/s with the exclusion of information about the fundamental tone.

Fig. 4. Examples of speech compression

A particularly popular part of stegology has recently become steganography, which is used to hide confidential information in graphic images transmitted over computer networks. At the same time, the progress made in the development of acoustic information transmission devices, as well as in computer technology, opens up new opportunities for both covert transmission of confidential information in analogue and digital audio signals and speech, and for covert transmission in information containers of various kinds, based on the use of new multimedia technologies, computer and cellular telephony, etc. This area of digital technology in the field of protecting confidential information covertly present inside or over an openly transmitted audio signal is now commonly referred to as "steganophony."

Currently, computerized steganography methods are widely used based on the use of natural noise containing digital arrays obtained by standard conversion methods from analogue acoustic and video signals. These noises are quantization errors and cannot be completely eliminated. The use of noise bits to transmit additional confidential information allows you to create a hidden data channel. As noise bits, we usually consider the lowest bits of the count values, which are noise in terms of measurement accuracy and carry the least amount of information contained in the count. Such bits are commonly referred to as least significant bits (LSBs).

One of the most common methods of steganophonic concealment of confidential information is the method based on the use of Least Significant Bits of audio (and/or any other multimedia) data [12, 13].

Certain statistical criteria have been developed to detect the fact of concealing a confidential information message in the EIS of audio signals [14, 15].

The statistical analysis of the audio data revealed a number of significant properties that affect the secrecy of confidential data and, accordingly, the security of such methods using noise bits. Among these properties, the following should be highlighted:

– heterogeneity of sample sequences;

– the presence of certain dependencies between bits in the samples;

– the presence of certain dependencies between the samples themselves;

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

– unequal probability of conditional distributions in the sequence of samples;

– presence of long series of identical bits;

– correlation between UXO and high bits.

Today, we can offer the following requirements for hiding confidential acoustic information and setting steganophonic markers in signals, arrays and data formats of various nature:

– the perception of signals and data with confidential acoustic information embedded in them should be practically indistinguishable from the perception of the original, "open" message contained in this signal or array;

– confidential speech data transmitted over publicly available communication channels, masked by various signals or implicitly contained in their parameters, should not be easily detected in these carrier signals by widely used methods and technical means of analysis currently available;

– in a number of applications, the setting and detection of steganographic markers should not depend on the synchronization of these processes and on the availability of any standards;

– special methods for setting and detecting steganophonic markers should be implemented on the basis of standard computer equipment or special software and hardware based on it;

– it should be possible to embed and detect authenticity features in an acoustic (speech) signal that are detected when it is illegally copied or modified, regardless of the type of representation and transmission of this signal (analogue or digital);

– should provide the possibility of hiding confidential acoustic information in data sets regardless of the type of information presented in them.

Sonogram images can be used to transmit and store speech on paper as stegomarkers. When implementing "speech signature" technologies associated with a protected document, which are similar in meaning and content to an electronic digital signature, two to four minutes of telephone-quality speech in the form of various patterned drawings can be applied to a standard sheet of paper. In this case, the authenticity of the document can be established not only by the presence of the relevant signatures and stamps, but also by the information contained in the "speech signature", which can be scanned, synthesized and voiced to make it possible to hear the key points of the document's content voiced by the voice of the responsible person.

A discrepancy between the voiced information and the information contained in the document indicates that it has been falsified. It is virtually impossible to forge a "speech seal" or "speech signature". It should be noted that such a cheap "speech signature" technology can be implemented on standard office equipment: a computer with a sound card plus a printer and scanner.

Conclusion

Thus, based on the above, it can be assumed that one of the promising areas of acoustic information protection in communication channels and dedicated premises is the creation and development of computerized speech marking systems along with or in conjunction with traditional technologies for semantic protection of acoustic information, namely, the classification of speech signals based on cryptographic algorithms.

The choice of specific methods and means of speech masking as one of the types of semantic protection of acoustic information will depend on the practical requirements for the speech protection system and the technical characteristics of the acoustic information transmission channel.

Computer technologies for digital signal and image processing are becoming more and more widely used in modern security systems for voice communications. The main requirements for today's systems that provide protection of acoustic information in critical computer systems are the speed and efficiency of various speech signal processing procedures using standard inexpensive technical means of computer telephony, namely: a personal computer, sound card, telephone line interface device and/or modem. These requirements can be met by applying digital methods of dynamic spectral analysis, i.e., synthesis of speech and audio signals.

The given examples of using the proposed approach to solve the most common problems of ensuring the security of speech messages have shown its high potential capabilities in the implementation of various, even very complex and new audio signal processing algorithms that are already applicable today to create computer systems for protecting speech messages in public communication channels. This approach can become the basis for the design of new acoustic information security systems and the evaluation of the effectiveness of the use of speech message protection devices that already exist on the market of special equipment.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)*

Further research is desirable to analyze the possible use of methods for synthesizing large ensembles of quasi-orthogonal discrete signals with improved ensemble, structural, and correlation properties to ensure higher security of acoustic channels in computer systems for critical applications.

References

1. Kosenko, V. (2017), "Principles and structure of the methodology of risk-adaptive management of parameters of information and telecommunication networks of critical application systems", *Innovative technologies and scientific solutions for industries*, No 1 (1), P. 75–81. DOI: https://doi.org/10.30837/2522-9818.2017.1.046
2. Kosenko, V. (2017), "Mathematical model of optimal distribution of applied problems of safety-critical systems over the nodes of the information and telecommunication network", *Advanced Information Systems*, Vol. 1, No. 2, P. 4–9. DOI: https://doi.org/10.20998/2522-9052.2017.2.01
3. Karen Bailey, Kevin Curran. Steganography. – *BookSurge Publishing*, 2005 p. – 118 p.
4. Johnson N., Duric Z., Jajodia S. Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, New York – NY.: Kluwer Academic Pub, 2000 p. URL: https://link.springer.com/chapter/10.1007/0-387-25096-4_6
5. Elad Barkan. Instant Ciphertext-Only Cryptanalysis of GSM. Encrypted Communication. / Elad Barkan, Eli Biham, Nathan Keller. // *Journal of Cryptology*, Volume 21, Number 3, July 2008, P. 392–429 (38).
6. J. Golic. Cryptanalysis of Alleged A5 Stream Cipher. – Proceedings of EUROCRYPT'97, LNCS 1233, P. 239–255, Springer-Verlag 1997.
7. Alex Biryukov. Real Time Cryptanalysis of A5/1 on a PC. / Alex Biryukov, Adi Shamir, David Wagner – Springer Berlin / Heidelberg, 2001. − ISBN: 978-3-540-41728-6. URL: https://cryptome.org/a51-bsw.htm
8. Mozhaiev O. Development of a method for determining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples / Mozhaiev O., Semenov, S., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Y., Yevstrat, D., Chyrva, Y., Kuchuk, H.// *Eastern-European Journal of Enterprise Technologies*, 6 (4 (120)), P. 40–49. DOI: https://doi.org/10.15587/1729-4061.2022.269128
9. Mozhaiev O. Crypto-resistant methods and random number generators in internet of things (iot) devices/ Mozhaiev O., Klimushyn P., Solianyk T., Gnusov Y., Manzhai O., Svitlychnyi V. // *Innovative technologies and scientific solutions for industries*, 2022 № 2 (20), P. 22–34. DOI: https://doi.org/10.30837/ITSSI.2022.20.022
10. Mozhaiev O. Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things/ Mozhaiev O, Klimushyn P., Solianyk T., Kolisnyk T. // *Advanced Information Systems*, 2021. Vol. 5, No 3. P. 103–111. DOI: https://doi.org/10.20998/2522-9052.2021.3.14
11. Klimushyn, P., (2021), "Hardware support procedures for asymmetric authentication of the internet of things",/ Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., Yanov V// *Innovative Technologies and Scientific Solutions for Industries*, No. 4 (18), P. 31-39. DOI: https://doi.org/10.30837/ITSSI.2021.18.031
12. J. Friedrich, G. Miroslav, R. Du. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghampton, New York: SUNY, 2001. URL: http://www.ws.binghamton.edu/fridrich/research/acm_2001_03.pdf
13. J. Fridrich, R. Du, and L. Meng, "Steganalysis of LSB Encoding in Color Images", *ICME 2000*, New York City. DOI: https://doi.org/10.1109/ICME.2000.871000
14. W. Brock. W. Dechert and J. Scheinkman. "A test for independence based on the correlation dimension", *Working Paper, University of Wisconsin*, 1987. DOI: https://doi.org/10.1177/1536867X211025796
15. Wu H. C., Wu N. I., Tsai C. S., Hwang M. S. Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods // *IEEE Transactions on Image and Signal Processing, 2005*. – № 5. – P. 611–615. DOI: https://doi.org/10.1049/IP-VIS:20059022

Received 28.03.2023

Відомості про авторів / About the Authors

Можаєв Михайло Олександрович – доктор технічних наук, Науково-дослідний центр судової експертизи з питань інтелектуальної власності Міністерства юстиції України, заступник директора, Київ, Україна; e-mail: mozhayev.misha89@gmail.com; ORCID: https://orcid.org/0000-0003-1566-9260

Можаєв Олександр Олександрович – доктор технічних наук, професор, Харківський національний університет внутрішніх справ, професор кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: mozhaev1957@gmail.com; ORCID: https://orcid.org/0000-0002-1412-2696

Гнусов Юрій Валерійович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, завідувач кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: duke6969@i.ua; ORCID: https://orcid.org/0000-0002-9017-9635

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23) *ISSN 2524-2296 (online)*

Струков Володимир Михайлович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, професор кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: struk_vm@ukr.net; ORCID: https://orcid.org/0000-0003-4722-3159

Клімушин Петро Сергійович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, доцент кафедри протидії кіберзлочинності, Харків, Україна; e-mail: klimushyn@ukr.net; ORCID: https://orcid.org/0000-0002-1020-9399

Євстрат Дмитро Іванович – кандидат технічних наук, доцент, Харківський національний економічний університет ім. С. Кузнеця, доцент кафедри інформаційних систем, Харків, Україна; e-mail: dmitry.yevstrat@gmail.com; ORCID: https://orcid.org/0000-0001-8393-6063

Mozhaiev Mykhailo – Doctor of Technical Sciences, Scientific Research Centre for Forensic on Intellectual Property of the Ministry of Justice of Ukraine, Deputy Director, Kyiv, Ukraine.

Mozhaiev Oleksandr – Doctor of technical science, professor, Kharkiv National University of Internal Affairs, professor of Cyber Security and DATA-Technologies Department, Kharkiv, Ukraine.

Gnusov Yurii – Candidate of technical science, associate professor, Kharkiv National University of Internal Affairs, head of department Cyber Security and DATA-Technologies, Kharkiv, Ukraine.

Strukov Volodymyr – Candidate of technical science, associate professor, Kharkiv National University of Internal Affairs, professor of Cyber Security and DATA-Technologies Department, Kharkiv, Ukraine.

Klimushin Petro – Candidate of technical science, associate professor, Kharkiv National University of Internal Affairs, associate professor of Countering Cybercrime Department, Kharkiv, Ukraine.

Yevstrat Dmytro – Candidate of technical science, associate professor, Simon Kuznets Kharkiv National Economic University, associate professor of Department of Information Systems, Kharkiv, Ukraine.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Предмет дослідження – процес захисту акустичної інформації в комп'ютерних системах критичного застосування для забезпечення необхідного рівня безпеки системи. **Метою** статті є аналіз методів захисту акустичної інформації в комп'ютерних системах критичного застосування за допомогою маскування для забезпечення неможливості несанкційного доступу до системи. У роботі вирішуються такі **завдання**: проаналізовано програмно-технічне маскування мови; досліджено маскування мовних повідомлень з метою введення невпізнання; визначено особливості стиснення мовних повідомлень; вивчено приховану передачу акустичної інформації. **Результатами** роботи, отриманими за допомогою математичних **методів** перетворення інформації в комп'ютерних системах, є потенційно можливі методи маскування мовних повідомлень для забезпечення неможливості несанкційного доступу до системи. Аналіз функціонування запропонованих методів дав змогу сформувати конкретні **висновки**. Одним із перспективних напрямів захисту акустичної інформації в каналах зв'язку й виділених приміщеннях є створення та розвиток комп'ютеризованих систем маскування мови за умови їх сумісного використання з традиційними технологіями смислового захисту акустичної інформації, а саме засекречуванням мовних сигналів на основі криптографічних алгоритмів. Нині основними вимогами, що висуваються до систем, які забезпечують захист акустичної інформації в комп'ютерних системах критичного застосування, є швидкість і ефективність виконання різних процедур оброблення мовного сигналу з використанням стандартних недорогих технічних засобів комп'ютерної телефонії, зокрема: персонального комп'ютера, звукової карти, пристрою стику з телефонною лінією і/або модема. Задовольнити зазначені вимоги можна, застосовуючи цифрові методи динамічного спектрального аналізу-синтезу мовних і аудіосигналів. Вибір конкретних методів і засобів маскування мови як одного з видів смислового захисту акустичної інформації залежатиме від практичних вимог, що висуваються до системи мовного захисту й технічних характеристик каналу передачі акустичної інформації. Подальші дослідження буде присвячено аналізу можливого використання методів синтезу великих ансамблів квазіортогональних дискретних сигналів із поліпшеними ансамблевими, структурними й кореляційними властивостями для забезпечення вищих показників захищеності акустичних каналів у комп'ютерних системах критичного застосування.

Ключові слова: акустична інформація; маскування акустичної інформації; технічний захист; криптографічний захист; стеганографічний (стеганофонічний) захист; модифікація мови; стиснення мовних повідомлень; комп'ютерні системи.

Бібліографічні описи / Bibliographic descriptions

Можаєв М. О., Можаєв О. О., Гнусов Ю. В., Струков В. М., Клімушин П. С., Євстрат Д. І. Аналіз методів захисту акустичної інформації в системах критичного застосування. *Сучасний стан наукових досліджень та технологій в промисловості*. 2023. № 1 (23). С. 96–107. DOI: https://doi.org/10.30837/ITSSI.2023.23.096

Mozhaiev, M., Mozhaiev, O., Gnusov, Y., Strukov, V., Klimushin, P., Yevstrat, D. (2023), "Analysis of acoustic information protection methods in critical applications", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (23), P. 96–107. DOI: https://doi.org/10.30837/ITSSI.2023.23.096