http://doi.org/10.35596/2522-9613-2022-28-3-60-64

Original paper

UDC [004.934+004.056.5]:811.411.21

RESEARCH ON SAFETY RISKS OF SPEECH INFORMATION

HENADZI V. DAVYDAU[1], VASILI A. PAPOU[1], ALEKSANDR V. PATAPOVICH[1], LI YE[2], WU XIAOMING[2], WANG FUQIANG[2], ZHANG PENG[2], BI XIAOYAN[2]

[1]*Belarusian State University of Informatics and Radioelectronics (Minsk, Belarus)*

[2]*Jinan National Supercomputer Center, China*

Submitted 27 April 2022

Abstract. The paper presents the results of research on the assessment of the security risks of speech information. It is shown that for speech information circulating in an acoustic form in a room, the main indicator of security is confidentiality. Confidentiality is determined by an indicator equal to 1, when complete confidentiality of speech information is provided, and an indicator equal to 0, when information has lost confidentiality, there are no intermediate values of this indicator. It is shown that the loss of confidentiality of speech information can occur due to the implementation of at least one of the possible threats. Methods for assessing the security risks of speech information are considered. For speech information, security risks consist of the risks of leakage through acoustic channels outside the security area of the room and the risks associated with the human factor, since the carrier of speech information is also a person. The risks associated with the leakage of speech information through acoustic channels are considered in details. The mechanism for ensuring zero risk of leakage of speech information through the acoustic channel is considered and specific recommendations for its implementation are given.

Keywords: security risk, speech information, confidentiality, speech intelligibility, information security.

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

Gratitude. This work was financially supported by grant funding from the Belarusian Republican Foundation for Basic Research, grant № F20KITG-002 and the National Key Research and Development Project, grant № 2018YFE0119700.

For citation. Davydau H.V., Papou V.A., Patapovich A.V., Li Ye, Wu Xiaoming, Wang Fuqiang, Zhang Peng, Bi Xiaoyan. Research on Safety Risks of Speech Information. *Digital Transformation*. 2022; 18(3): 60-64.

Introduction

The basic level of information security, determined in accordance with international standards, establishes a qualitative risk assessment. Information security should be determined by the following indicators: confidentiality, integrity, accessibility.

One of the key documents describing the requirements for information security risk assessment is the international standard "STB ISO 31010-2020 Risk Management. Guidelines". The process of calculating information security risks is relevant at all stages of the speech information protection system. In accordance with the STB, the following definition of risk is given. Risk – the impact of uncertainty on the targets. In other

papers, the definition of risk is somewhat different: risk is a consequence of the influence of uncertainty on the achievement of targets. At the same time, this definition is given 5 notes as an explanation, which somewhat complicates the very concept of risk after translating this notion from English. This is due to the fact that the definition of risk and risk management given in regulatory documents relate to all areas of human activity. In the context of the Russian language, the most appropriate definition of risk for the field of information protection is: risk – the probability of losses in the event of the worst-case scenario.

The choice of a method for assessing information security risks can be made in terms of time, financial, and information indicators. The possibility of obtaining quantitative estimates of the output data for these indicators may be different depending on the method and stage of information security risk assessment. For the safety of speech information presented in the form of acoustic vibrations of the medium and the lack of means of recording, reproducing and transmitting it, the main indicator of its security is confidentiality, since accessibility and integrity are evaluated by the speaker himself during pronunciation.

Risk of speech information's confidentiality loss

The risk of the confidentiality loss of speech information can be defined as an indicator of the correct perception of words – the units of speech in the background. At the same time, the concept of information is defined as data, regardless of the form of their presentation. In accordance with STB GOST R 50922-2000, information is data about persons, objects, facts, events, phenomena and processes, regardless of the form of their presentation.

In this paper [1], information security risks are considered as a result of the impact of a threat on assets and are determined in accordance with the expression:

$$R_i = P_i \times U_i \left(1 - P_{im}\right), \quad (1)$$

where R_i is the risk from the impact of the threat i; P_i is the probability of the threat i; U_i is the damage from the i-type damage; P_{im} is the probability of overcoming the protection mechanism when exposed to the threat i.

The risk of the confidentiality loss of speech information in terms of the probability of loss of confidentiality can vary from zero to one and take values on this segment without causing any doubts about their unacceptability. However, the concept of confidentiality is more complicated. Confidentiality can be considered complete or 100 %. On the other hand, what kind of privacy is it if it is not 100 %, but for example 50 %. It's impossible to interpret. Therefore, to assess confidentiality, it is proposed to use the concept of complete confidentiality or simply confidentiality and lack of confidentiality. In time, this indicator is equal to 1 in the case of confidentiality of information and is equal to 0 in the absence of confidentiality, there are no intermediate values.

The risk from the impact of all possible threats to information assets will be determined from the expression:

$$R_{gen} = \sum_{i=1}^{N} P_i \times U_i \left(1 - P_{im}\right), \quad (2)$$

where N – the number of threats.

For speech information, the risk of the confidentiality loss may occur from the implementation of one of the threats and then the expression (2) is converted to the form

$$R_{gen} = U \times \sum_{i}^{N} P_{im}\ , \quad (3)$$

where U is the damage caused by the loss of privacy when implementing one of several or several threats at the same time; P_{im} is the probability of overcoming the protection mechanism of the i threat, N is the number of threats.

If the number of threats of confidentiality loss for speech information can be quite large, including dialogue participants, then the implementation of one of them may lead to loss of confidentiality. Since assessing the impact of threats to the confidentiality loss of speech information coming from each dialogue participant is a very difficult and to a greater extent socio-psychological task, from now on only the leakage of speech information through technical acoustic channels risks will be considered. This includes acoustic channels of leakage of speech information through walls, floor,

ceiling, doors, windows, heating and water supply communication systems, ventilation ducts. The speech information leakage acoustic channels formation mechanism and methods of masking speech information with various types of signals, including "white" noise, speech-like signals and combined signals, in order to protect it from loss of confidentiality are considered in papers [2–4].

When masking speech information with acoustic signals, speech intelligibility decreases. Masking signals cannot be extremely large, so as not to complicate communication between people in the room. If the intelligibility of speech decreases during the dialogue in the room, the speaker automatically tries to increase the volume of the speech he utters. The main issue in assessing the security risks of speech information concerns the threshold level of verbal intelligibility of speech at which the confidentiality of speech information is not violated. A person has the ability to understand the meaning of a statement in several words, i.e. to conjecture. In this regard, it is difficult to determine the acceptable threshold level of speech intelligibility, at which its confidentiality is preserved. Even one word recognized by the violator has a semantic meaning and thus can reduce the security of speech information. In the paper [5], it is proposed to assess the security of speech information using indicators of intelligibility, audibility and cadence (rhythm). Speech intelligibility refers to the ratio of correctly recognized words to all words spoken by the speaker. Speech intelligibility can also be expressed as a percentage. Audibility is characterized by a lack of speech intelligibility (the number of correctly recognized words is zero), but the auditor hears the speaker's timbre in speech-masking noises and if he knows this timbre, he can determine which of the speakers is speaking. The auditor can recognize individual phonemes of words; which pronunciation conveys the timbre of speech. Cadence is when the auditor hears the rhythm of the speaker's pronunciation, but cannot recognize a single word, as well as recognize the timbre, since the timbre of pronunciation is unidentifiable. This means that the auditor cannot recognize any of the phonemes spoken by the speaker. Thus, from the point of view of reducing the security risk of speech information, it would be advisable to ensure speech intelligibility at the border of the security area equal to zero by setting the necessary levels of speech masking signals. Audibility, in the concept that is accepted in the paper [5], will be present and it will be possible to characterize the timbre of the speaker. With this approach, the security risks of speech information due to its leakage through acoustic channels will be eliminated. However, the security risks of speech information due to the fact that the participants of the conversation or dialogue remain its carriers are not equal to zero, although the leakage of speech information through acoustic channels was provided equal to zero. The question of the effectiveness of providing one hundred percent protection against leakage of speech information through technical channels and at the same time reducing the security risks of speech information as a whole remains open.

Speech intelligibility as an indicator of its security

The well-known methods for assessing speech intelligibility are based on the experimental dependencies of speech intelligibility on the integral ratio of speech sound pressure to the sound pressure of masking signals (there is an experimental dependence for each type of masking signals and each language). However, these methods are focused on assessing speech intelligibility for auditors with average auditory sensitivity and do not give an estimate for intelligibility of zero percent. In addition, when assessing speech intelligibility using these methods, it is impossible to establish the limits of acceptable parameter variations, i.e. confidence limits for graphs with a given authenticity. In the number of papers [6–8], it is proposed to evaluate speech intelligibility using the limit state method, since it is very laborious to find the boundaries of the confidence domain for the graph of the dependence of speech intelligibility on the integral ratio of the speech signal / masking noise due to the need for a large amount of experimental research. As mentioned above, the dependences of speech intelligibility on the integral ratio of the sound pressure of speech to the sound pressure of masking signals were obtained for auditors with average auditory sensitivity. Such dependencies cannot be used to assess the security of speech information and assess security risks. As shown in papers [9–11], when conducting experimental studies on speech intelligibility, it is necessary to select and train auditors with increased auditory sensitivity and speakers with clear pronunciation.

In accordance with the above requirements, experimental studies were conducted to find the threshold value of the speech signal / masking “white” noise ratio, at which speech intelligibility is zero.

Experimental studies were carried out in accordance with the methodology described in the paper [7]. At the same time, the selection of speakers was carried out in accordance with the requirements for clear pronunciation at a given speed of reading a phonetically balanced text. The selection of auditors was based on high auditory sensitivity and the ability to recognize speech against the background of intense broadband acoustic noise. It is established that with the integral ratio of the speech signal / masking "white" noise at minus 28 dB, the intelligibility of Russian speech is zero.

The integral value of the speech signal implies the RMS value of the speech sound pressure in the frequency range from 100 to 8000 Hz and an average speech rate of 75 words per minute. These research results were obtained for the condition when the speaker makes a speech in a protected room with an RMS sound pressure value of 70 dB and a peak speech factor of no more than 18 dB. However, in real conditions of work to ensure the safety of speech information during meetings or other events with verbal communication, situations may arise with emotional speech when the sound pressure level of the speaker's speech exceeds 70 dB, but the level of the masking signal does not change. At the same time, there is a risk of loss of confidentiality of speech information. To eliminate such a situation, a speech information security device “Priboi” has been developed, which monitors the sound pressure level of acoustic signals in the protected room, and if its value exceeds 70 dB, the level of speech masking signals automatically increases.

An important aspect in ensuring the security of speech information is the relationship between the risk of loss of confidentiality and the probability of overcoming protection, between the losses from confidentiality loss and the costs of ensuring information security, as well as the income from overcoming information security and the costs of overcoming information security. When the losses from the possible loss of confidentiality of information exceed the funds spent on the security of speech information, it is economically advantageous to ensure the protection of information. If the funds spent on overcoming security exceed the possible income from overcoming the security system, then it makes no sense to overcome the information protection system and it is not economically justified. The described scenarios of information security and the conditions for overcoming protection can be written in the following relations:

$$C_{spe} \le B_{los}, \quad (4)$$

$$C_{spe} \le B_{ben}, \quad (5)$$

where, C_{pro} – the funds spent on the protection of information; C_{spe} – funds spent on overcoming protection; B_{los} – possible losses due to loss of confidentiality of information; B_{ben} – possible benefits from overcoming protection and gaining access to information.

The ratios indicated in expressions 4 and 5 are marginal. Depending on the magnitude of possible losses and possible benefits, which, as a rule, are known, the amount of funds spent on ensuring the security of information may also change, and on the other hand, the funds spent on overcoming protection may also change.

Conclusion

From the point of view of the security of speech information, it is characterized by only one parameter – confidentiality. The integrity of speech information in acoustic form and its accessibility do not need to be considered, since it is very difficult to imagine it in relation to speech information in acoustic form. The conducted studies have shown that the security risks of speech information have two components. One is due to the risks of leakage of speech information through acoustic channels outside the premises and the protected area. The second component is related to the risks of loss of privacy through its carrier, it being a person. It is very difficult and extremely time-consuming to assess this component of risk, which is associated with a psychological portrait of a person. It is possible to reduce the risks of this component of the security of speech information by reducing the number of people who have access to speech information. The component of the security risk of speech information, which is caused by a possible leak through the acoustic channel, must be set to zero the information that is caused by a possible leakage through the acoustic channel must be set to zero. This is achieved by using acoustic masking speech signals.

References

1. Anischenko, V. V. Metody otsenki effektivnosti zashchity aktivov na ob'yektakh informatsionnykh tekhnologiy [Methods for Assessing the Effectiveness of Asset Protection in Information Technology Facilities] / V. V. Anischenko, A. M. Krishtofik // Informatics. – 2004. – No. 3. – P. 95–105. (In Russ.)
2. Davydau H.V., Kavan D.M. Metody obnaruzheniya i opredeleniya kharakteristik vozmozhnykh kanalov utechki rechevoy informatsii [Methods for Detecting and Determining the Characteristics of Possible Channels of Speech Information Leakage] // Doklady BGUIR. – 2011. – Vol. 5 (59). – P. 19–25. (In Russ.)
3. Lynkov L.M., Kavan D.M., Davydau H.V. Osobennosti zashchity rechevoy informatsii ot utechki po akusticheskomu kanalu [Features of Protection of Speech Information from Leakage through an Acoustic Channel] // Security of Information Technologies. – 2012; Vol. 1 (180-181). – P. 19–25. (In Russ.)
4. Davydau H.V., Kavan D.M., Popou V.A., Patapovich A.V. Zashchita rechevoy informatsii ot utechki po akusticheskim kanalam [Protection of Speech Information from Leakage through Acoustic Channels] // Doklady BGUIR. – 2009. – Vol. 4 (42). – P. 49–54. (In Russ.)
5. Bradley J.S., Cover. B.N. Designing and Assessing the Architectural Speech Security of Meeting Rooms and Offices: IRC Research Report, RR – 187. 2006.
6. Spekers and auditors selection technique in assessing speech information security / Y. N. Seitkulov [et al.] // Journal of Theoretical and Applied Information Technology. – 2019. – Vol. 97 (12). – P. 3306–3316.
7. Method for speech intelligibility assessment with combined masking signals / Y. N. Seitkulov [et al.] // Journal of Theoretical and Applied Information Technology. – 2020. – Vol. 98 (8). –P. 1173–1186.
8. Algoritym of forming speech base units using the method of dynamic programming / Y. N. Seitkulov [et al.] // Journal of Theoretical and Applied Information Technology. – 2018. – 96 (23). – P. 7928–7941.
9. Seitkulov, Y. N. Requirements for auditors and announcers when assessing the security of speech information / Y. N. Seitkulov, H. V. Davydau, A. V. Patapovich // Abstracts of the XII Belarusian-Russian Scientific and Technical Conference "Technical Means of Information Security. – Minsk, 2014. – P. 11–12.
10. Boranbayev, S. N. Spekers and auditors selection technique in assessing speech information security / S. N. Boranbayev, H. V. Davydau, A. V. Patapovich // Journal of Theoretical and Applied Information Technology. – 2019. – Vol. 97(12). – P. 3306–3316.
11. Gotovko, M. A. Assessment of the security of speech information. Information Technologies and Systems / M. A. Gotovko, A. V. Davydau, Y. N. Seitkulov // Proceedings of the International Scientific Conference, BSUIR, Minsk, Belarus, October 23, 2013 Information Technologies and Systems 2013 (ITS 2013). – Minsk, 24th October 2013. – P. 268–269.

Authors contribution

Davydau H. V. carried out the formulation of the problem for the study, prepared the manuscript of the article.

Papou V. A. defined research objectives.

Patapovich A. V. developed the general concept for assessing information security risks.

Li Ye developed a generalized risk assessment methodology. Wu Xiaoming, Wang Fuqiang calculated the risks of losing information confidentiality. Zhang Peng, Bi Xiaoyan calculated speech intelligibility, conclusion.

Information about the authors

Davydau H. V., Cand. Of Sci., Researcher at SRL 5.3 of R&D Department of the Belarusian State University of Informatics and Radioelectronics.

Papou V. A., Researcher at SRL 5.3 of R&D Department of the Belarusian State University of Informatics and Radioelectronics.

Patapovich A. V., Researcher at SRL 5.3 of R&D Department of the Belarusian State University of Informatics and Radioelectronics.

Li Ye, Deputy Director of the National Supercomputing Center of Jinan.

Wu Xiaoming, Wang Fuqiang, Zhang Peng, Bi Xiaoyan Researchers at the National Supercomputing Center of Jinan.

Address for correspondence

20013, Republic of Belarus, Minsk, P. Brovka St., 6,
Belarusian State University of Informatics and Radioelectronics
tel. +375 29 670-30-40; e-mail: nil53@bsuir.edu.by
Patapovich Aleksandr Vladimirovich