

Научная статья

УДК 004.056.53

<https://doi.org/10.31854/1813-324X-2025-11-5-21-27>

EDN:IRBHCD



Алгоритм формирования адаптивной речеподобной помехи для защиты конфиденциальной речевой информации в офисных помещениях

© Мария Владимировна Волчихина, mariyamoiseeva@mail.ru

Тамбовский государственный технический университет,
Тамбов, 392000, Российская Федерация

Аннотация

Актуальность исследования. Современные тенденции развития научной мысли в области информационной безопасности обусловлены ростом числа угроз, связанных с утечкой речевой информации из помещений по акустическим и виброакустическим каналам. Применяемые способы пассивной и активной защиты помещений, основанные на генерации шумов и использовании библиотек предзаписанных звуковых сигналов, не всегда позволяют достичь требуемого уровня защиты из-за отсутствия адаптации к параметрам реальной речи и особенностям акустической обстановки в помещении, а также из-за пренебрежения к требованиям нормативных документов по уровню шума в помещении. Все это обусловило необходимость разработки новых алгоритмов активной защиты офисных помещений от утечки, в частности, по акустиковибрационному каналу, основанных на использовании речевых сигналов субъектов переговоров.

Цель исследования заключается в обеспечении требуемого значения коэффициента словесной разборчивости на границе контролируемой зоны офисного помещения на основе совершенствования средств активной защиты информации за счет разработки и применения алгоритма формирования адаптивной к изменению параметров речи субъектов переговоров речевой обстановки в офисном помещении, речеподобной помехи при учете требований нормативных документов по уровню шума. Для решения поставленных задач использованы **методы** теории информации, цифровой обработки сигналов.

Результаты исследования. Разработан алгоритм формирования адаптивной речеподобной помехи для применения в активных средствах защиты информации в офисном помещении. Предложенный алгоритм формирования адаптивной речеподобной помехи позволяет генерировать ее из речевых сигналов субъектов переговоров только при их наличии, что повышает маскирующие свойства помехи.

Научная новизна представленного результата заключается во введении процедур многоканальной генерации формирования адаптивной речеподобной помехи.

Теоретическая значимость исследования состоит в расширении представлений о методах, моделях и способах адаптивного акустического маскирования речевой информации и разработке алгоритма формирования речеподобных помех на основе анализа речевых параметров.

Практическая значимость. Разработанный алгоритм может быть реализован на базе стандартных вычислительных устройств и акустических систем. Это обуславливает его применимость в составе как современных, так и перспективных средств активной защиты речевой информации.

Ключевые слова: алгоритм, безопасность информации, генератор шума, активная защита речевой информации, речеподобная помеха, компенсирующая помеха

Ссылка для цитирования: Волчихина М.В. Алгоритм формирования адаптивной речеподобной помехи для защиты конфиденциальной речевой информации в офисных помещениях // Труды учебных заведений связи. 2025. Т. 11. № 5. С. 21–27. DOI:10.31854/1813-324X-2025-11-5-21-27. EDN:IRBHCD

Original research
<https://doi.org/10.31854/1813-324X-2025-11-5-21-27>
EDN:IRBHCD

An Algorithm for Forming an Adaptive Speech-Like Interference to Protect Confidential Speech Information in Office Spaces

✉ Maria V. Volchikhina, mariyamoiseeva@mail.ru

Tambov State Technical University,
Tambov, 392000, Russian Federation

Annotation

Relevant. Current trends in information security research are driven by the growing number of threats associated with the leakage of speech information from premises via acoustic and vibroacoustic channels. Current methods of passive and active protection of premises, based on noise generation and the use of libraries of pre-recorded audio signals, do not always achieve the required level of protection due to a lack of adaptation to the parameters of real speech and the acoustic environment in the premises, as well as due to disregard for regulatory requirements regarding indoor noise levels. All this has necessitated the development of new algorithms for the active protection of office premises from leakage, particularly via acoustic-vibrational channels, based on the use of speech signals from participants in negotiations.

The aim of the study is to ensure the required verbal intelligibility coefficient at the boundary of a controlled office area by improving active information protection systems through the development and application of an algorithm for generating speech-like interference that is adaptive to changes in the speech parameters of negotiators, the office environment, and noise level regulations. Information theory and digital signal processing methods were used to solve these problems.

In result an algorithm for generating adaptive speech-like interference for use in active information protection systems in offices has been developed. The proposed algorithm for generating adaptive speech-like interference allows it to be generated from the speech signals of negotiators only when they are present, thereby enhancing the interference's masking properties.

The novelty of the study lies in the introduction of multichannel procedures for generating adaptive speech-like interference.

The theoretical significance of this research lies in expanding our understanding of methods, models, and techniques for adaptive acoustic masking of speech information and developing an algorithm for generating speech-like interference based on speech parameter analysis.

Practical significance. The developed algorithm can be implemented using standard computing devices and acoustic systems. This makes it applicable to both current and future active speech protection systems.

Keywords: algorithm, information security, noise generator, active protection of speech information, speech-like interference, compensating interference

For citation: Volchikhina M.V. An Algorithm for Forming an Adaptive Speech-Like in-Terference to Protect Confidential Speech Information in Office Spaces. *Proceedings of Telecommunication Universities*. 2025;11(5):21–27. (in Russ.) DOI:10.31854/1813-324X-2025-11-5-21-27. EDN:IRBHCD

Введение

Современные условия функционирования организаций предъявляют повышенные требования к защите информации, циркулирующей в процессе устных переговоров. Одним из наиболее уязвимых

каналов утечки информации в офисных помещениях является акустиковибрационный канал. Технические средства акустической и виброакустической разведки позволяют перехватывать речевые сигналы за пределами офисного помещения через

конструкции и коммуникации здания или посредством направленных микрофонов. Средства реализации активной защиты речевой информации должны быть спроектированы с учетом адаптивных изменений параметров защищаемых каналов, что соответствует современному подходу к динамическому обеспечению безопасности [1].

Одним из эффективных методов защиты от побочных угроз является создание речеподобной помехи (РПП), которая накладывается на исходный речевой сигнал и препятствует его разборчивому восприятию за пределами контролируемой зоны. В отличие от традиционных генераторов шумов, основанных на случайных или библиотечных звуках, в предложенном алгоритме используются непосредственно речевые сигналы субъектов переговоров, что обеспечивает высокую степень подобия спектрально-временных характеристик помехи и защищаемого сигнала. Модель, основанная на наложении гармоник с аппроксимацией экспериментальных спектров, позволяет точно описывать тональные компоненты речи [2].

В статье приведены результаты исследования по обеспечению активной защиты конфиденциальной речевой информации в офисных помещениях от утечек по акустовибрационному каналу при ограничении на уровень создаваемого помеховым сигналом шума. Показано, что алгоритм формирования адаптивной РПП реализует два параллельных процесса. Таким образом, появляется два помеховых сигнала – собственно, речеподобной и компенсирующей помех [3, 4]. Принципиальным отличием предложенного алгоритма является не только использование непосредственно речевых сигналов субъектов переговоров для формирования помех, что позволяет добиться высокой степени спектрального и временного сходства между помехой и защищаемым сигналом, но и акустической обстановки офисного помещения в помеховом сигнале. Реализация такого алгоритма при построении активных средств защиты предполагает необходимость адаптивного изменения параметров помеховых сигналов [5].

Описание предложенного алгоритма

РПП представляет собой сигнал, синтезированный на основе реальных речевых сигналов и модифицированный путем наложения их фрагментов друг на друга с использованием многоканальной обработки. Такой подход обеспечивает сохранение тембральных характеристик речи, ее динамики и спектрального состава, что делает РПП практически неотличимой от исходного речевого потока [6–10].

Суть части алгоритма, отвечающей за формирование, собственно, РПП, заключается в следующем:

- 1) на микрофон подается речевой сигнал субъекта переговоров $S(t)$;
- 2) из речевого сигнала после аналого-цифрового преобразования формируется РПП $S_d^{(РПП)}(i \cdot \Delta t)$ путем наложения фрагментов скрываемого речевого сигнала, поступающих с N каналов (достаточное количество каналов определено экспериментально);
- 3) организуется процедура прерывания излучения помехового сигнала при отсутствии речевого;
- 4) РПП $S_d^{(РПП)}(i \cdot \Delta t)$ подается на звуковую карту ЭВМ, с линейного выхода которой она может быть подана на звуковую колонку, или на внешний вход генератора шума системы защиты информации (СЗИ).

В ходе реализации алгоритма в целях формирования компенсирующей помехи предлагается следующий порядок действий:

- 1) на микрофон подается речевой сигнал субъекта переговоров $S(t)$;
- 2) речевой сигнал после аналого-цифрового преобразования поступает на фазовращатель, в котором происходит инверсия с учетом задержки (формирование компенсирующей помехи) $S_d'(i \cdot \Delta t)$, после чего этот сигнал подается на звуковую карту ЭВМ, с линейного выхода которой компенсирующая помеха $S'(t)$ излучается в пространство;
- 3) в контрольных точках съема информации речевой сигнал $S(t)$ складывается с компенсирующей помехой $S'(t)$ в пространстве помещения.

Представленная на рисунке 1 схема иллюстрирует структурно-функциональные зависимости между основными этапами алгоритма и последовательность операций, реализующих адаптивное преобразование речевого сигнала.

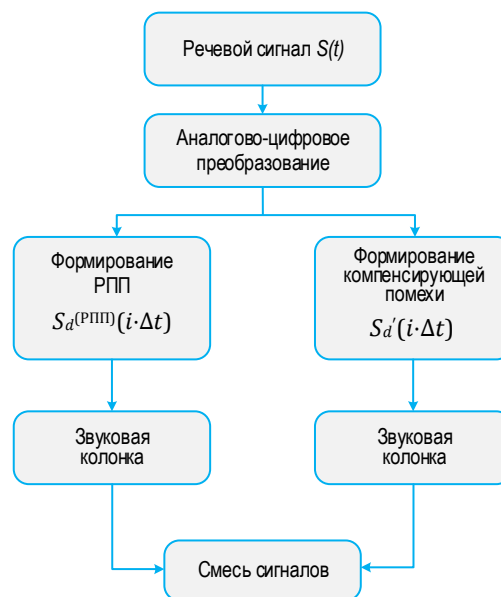


Рис. 1. Структурная схема алгоритма
 Fig. 1. Structural Diagram of the Algorithm

При параллельном формировании, собственно, РПП и компенсирующей помехи в контрольных точках съема информации принимается смесь речевого сигнала, компенсирующей помехи, РПП и помехового сигнала от сторонних источников.

Практическая реализация алгоритма

На практике схема генератора РПП реализуется на базе персонального компьютера, оснащенного звуковой картой. В офисном помещении устанавливаются микрофоны для приема речи и динамики для воспроизведения РПП, размещаемые вблизи потенциальных каналов утечки: окон, дверей и стен (рисунок 2). Такая организация позволяет обеспечить маскировку речи в контрольных точках (КТ1 – КТ4), расположенных за пределами офиса.

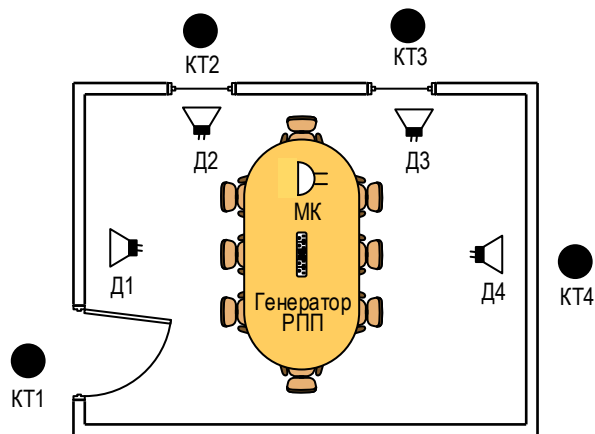


Рис. 2. Положение контрольных точек съема информации и генератора адаптивной речеподобной помехи

Fig. 2. The Position of the Control Points for Information Collection and the Adaptive Speech-Like Interference Generator

Процесс формирования и излучения сигналов проходит в следующей последовательности:

- 1) микрофон принимает речевые сигналы субъектов переговоров;
- 2) генератор адаптивной РПП формирует помеховый сигнал;

3) акустомат обеспечивает автоматическое прерывание генерации в паузах;

4) динамики излучают сформированный сигнал в пространство помещения, создавая акустическую маскировку.

Экспериментальные исследования

Источником для формирования помехового сигнала в генераторе РПП служит выходной сигнал микрофона, установленного в помещении. Процесс многоканального формирования РПП представлен на рисунке 3.

Экспериментальные исследования проводились с использованием лабораторной установки. Комплекс включал прототип автоматизированного программно-аппаратного средства генерации адаптивной РПП, реализованный на базе персональной ЭВМ со специализированным программным обеспечением, а также акустическую систему, анализатор спектра, шумомер и цифровой диктофон, предназначенные для регистрации и анализа параметров сигналов в контрольных точках.

Контрольная точка съема располагалась за дверным проемом, не оборудованным звукоизолирующими элементами, что обеспечивало моделирование реальных условий возможной утечки речевой информации через акустический канал. Измерения проводились при воспроизведении тестового речевого сигнала средней громкости, соответствующего типовой речи. В качестве эталонного средства защиты использовался генератор белого шума типа «Соната-АВ».

Показателем качества защиты выбран уровень словесной разборчивости речевого сигнала, определяемый по методике Н.Б. Покровского с учетом модификаций, предложенных Я.И. Железняком, Ю.К. Макаровым и А.А. Хоревым [10–16]. Сравнение производилось для двух режимов: при использовании традиционного белого шума и при работе адаптивного генератора РПП.

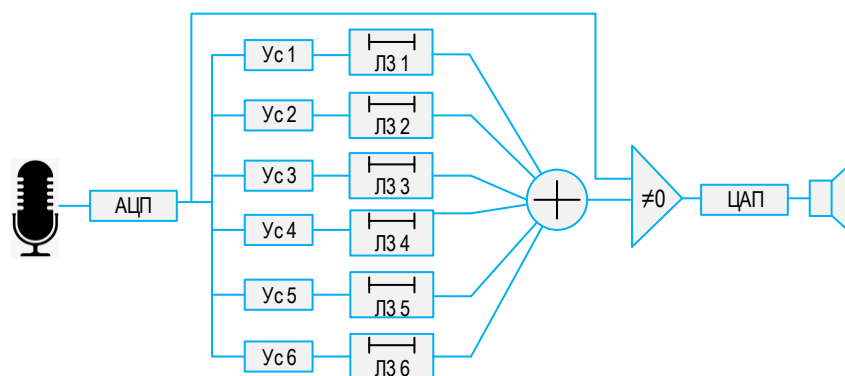


Рис. 3. Процесс многоканального формирования речеподобной помехи

Fig. 3. The Process of Multi-Channel Formation of Speech-Like Interference

Результаты исследований показали, что адаптивная РПП обеспечивает существенное снижение словесной разборчивости речи в контрольной точке по сравнению с белым шумом. При этом сохраняется стабильность маскирующего эффекта при изменении речевой обстановки, что подтверждает высокую степень соответствия разработанного алгоритма реальным акустическим условиям офисных помещений. Экспериментальные данные демонстрируют, что применение предложенного алгоритма позволяет обеспечить требуемый уровень защиты речевой информации в границах контролируемой зоны.

Как показали результаты исследований, проведенных с применением разработанного алгоритма, увеличение количества каналов формирования помеховых сигналов приводит к изменению как спектра генерируемой помехи, так и ее амплитуды [17, 18]. Эти изменения заметны уже при переходе от трехканальной схемы (рисунок 4а) к четырехканальной (рисунок 4б) (амплитуда результирующего сигнала возрастает, а спектр становится более сглаженным и приближенным к спектру речи). Поэтому в процессе эксперимента определялось целесообразное количество каналов. В результате установлено, что увеличение каналов больше шести не приводит к существенным изменениям спектра генерируемой помехи.

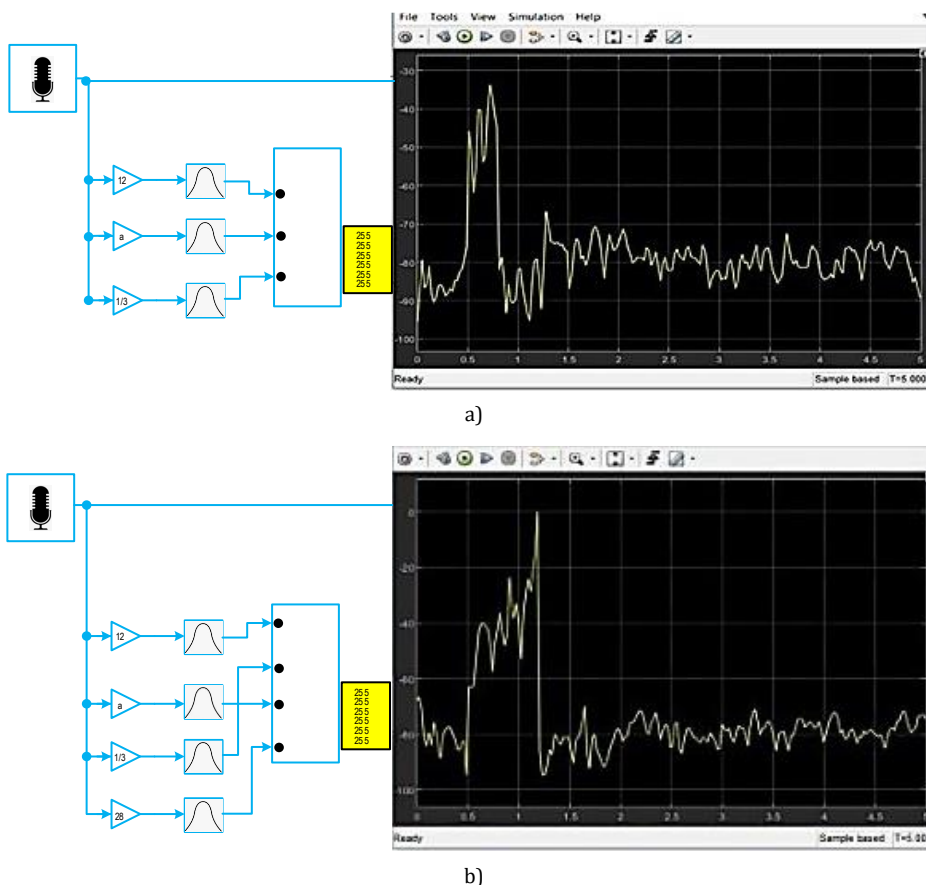


Рис. 4. Трехканальная (а) и четырехканальная (б) схемы генератора речеподобной помехи
 Fig. 4. Three-Channel (a) and Four-Channel (b) Speech-Like Noise Generator Circuits

Заключение

Основным отличием разработанного алгоритма от традиционных генераторов шума (например, «Барон», «Эхо», «Шаман») является использование не предзаписанных заранее звуков, а реальных речевых сигналов субъектов переговоров. Такой подход обеспечивает высокую степень приближения

формируемой средством активной защиты информации помехи к исходному речевому сигналу и исключает возможность выделения информативных компонентов речи при его перехвате.

Увеличение числа каналов (свыше шести) приводит к усложнению аппаратной реализации и росту стоимости системы при отсутствии заметного улучшения характеристик формируемой помехи.

Предложенный алгоритм формирования адаптивной РПП и компенсирующей помехи следует рассматривать как перспективное направление развития средств защиты речевой информации в офисных помещениях [18].

Проведенные исследования позволили подтвердить высокую степень спектрального сходства помехи с речевым сигналом, способность алгоритма адаптироваться к изменениям акустической обстановки, а также целесообразность совместного использования РПП и компенсирующей помехи для повышения уровня защиты.

Алгоритм может быть реализован на базе стандартных вычислительных устройств и акустических систем, что обуславливает его применимость в составе современных систем защиты информации нового поколения. Результаты оценки эффективности применения алгоритма, проведенной артикуляционными и инструментально-расчетными методами, позволили сделать вывод [19], что его применение эффективнее алгоритмов создания РПП, применяемых в существующих СЗИ более, чем на 20 %.

Список источников

1. Супрун А.Ф. Техническая защита информации: учеб. пособие для вузов. Часть 1. СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2021. 242 с.
2. Голубинский А.Н. Расчёт частоты основного тона речевого сигнала на основе полигармонической математической модели // Вестник Воронежского института МВД России. 2009. № 1. С. 81–90. EDN:JXUTKN
3. Волчихина М.В., Фурсова А.В. Модель адаптации параметров средства защиты информации к параметрам речи субъектов переговоров в помещении офисного типа // Вестник Воронежского института МВД России. 2024. № 1. С. 108–114. EDN:NLOJVC
4. Волчихина М.В. Метод адаптации параметров средств защиты информации на основе дискретного изменения амплитуды и тембра субъектов переговоров // Вестник Тамбовского государственного технического университета. 2022. Т. 28. № 2. С. 226–234. DOI:10.17277/vestnik.2022. 02.pp.226-234. EDN:AXWBIN
5. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. М.: Горячая линия – Телеком, 2020. 447 с.
6. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: учеб. пособие. СПб.: НИУ ИТМО, 2012. 416 с.
7. Царегородцев А.В., Тараскин М.М. Методы и средства защиты информации в государственном управлении. М.: Проспект, 2017. 205 с.
8. Лыньков Л.М., Голиков В.Ф., Борботько Т.В. Основы защиты информации и управления интеллектуальной собственностью. Минск: БГУИР, 2013. 243 с.
9. Ворона В.А., Костенко В.О. Способы и средства защиты информации от утечки по техническим каналам // Computational Nanotechnology. 2016. № 3. С. 208–223. EDN:WKNQZD
10. Хорев А.А. Техническая защита информации. М.: НПЦ «Аналитика», 2008. 436 с.
11. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия – Телеком, 2005. 415 с. EDN:QMOJMV
12. ГОСТ Р 50840-95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. М.: Госстандарт России, 1997. 230 с.
13. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Защита информации. Инсайд. 2007. № 2(14). С. 18–25. EDN:TRKKQR
14. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. 2000. № 4. С. 39–45. EDN:YPUIBV
15. Хорев А.А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: системы виброакустической защиты // Специальная техника. 2013. № 4. С. 31–63. EDN:RINYMP
16. Макаров Ю.К., Хорев А.А. Методы защиты речевой информации и оценки их эффективности // Защита информации. Конфидент. 2001. № 4. С. 22–33.
17. Дворянкин С.В., Дворянкин Н.С., Устинов Р.А. Развитие технологий образного анализа-синтеза акустической (речевой) информации в системах управления, безопасности и связи // Безопасность информационных технологий. 2019. Т. 26. № 1. С. 64–76. EDN:VWAQNW
18. Алексеев В.В., Гриднев В.А., Моисеева М.В., Рыжков А.П., Яковлев А.В. Теоретические основы построения и применения научно-исследовательского комплекса мониторинга характеристик защищенности конфиденциальной информации: монография. Тамбов: Издательский центр ФГБОУ ВО «ТГТУ», 2022. 100 с.
19. Волчихина М.В. Оценка уровня словесной разборчивости на границе контролируемой зоны офисного помещения артикуляционным методом // Вестник Воронежского института МВД России. 2022. № 2. С. 105–112. EDN:POMJEB

References

1. Suprun A.F. *Technical Information Security. Part 1*. Peter the Great St. Petersburg Polytechnic University Publ.; 2021. 242 p. (in Russ.)
2. Golubinskiy A.N. Calculation of the Pitch Frequency of a Speech Signal on the Basis of Polyharmonic Mathematical Model. *Vestnik of Voronezh Institute of the Ministry of the Interior of Russia*. 2009;1:81–89. (in Russ.) EDN:JXUTKN


3. Volchikhina M.V., Fursova A.V. Model of Adaptation of Information Security Means Parameters to Speech Parameters of Negotiation Subjects in an Office-Type Premises. *Vestnik of Voronezh Institute of the Ministry of the Interior of Russia*. 2024;1: 108–114. (in Russ.) EDN:NLOJVC
4. Volchikhina M.V. A Method for Adapting the Parameters of Information Security Tools Using a Discrete Change in the Amplitude and Timbre of the Subjects of Negotiations. *Transactions of TSTU*. 2022;28(2):226–234. (in Russ.) DOI:10.17277/vestnik.2022.02.pp.226-234. EDN:AXWBIH
5. Sheluhin O.I. *Network Anomalies. Detection, Localization, Forecasting*. Moscow: Goryachaya Liniya – Telecom Publ.; 2020. 447 p. (in Russ.)
6. Katorin Yu.F., Razumovsky A.V., Spivak A.I. *Information Security by Technical Means*. St. Petersburg: National Research University ITMO Publ.; 2012. 416 p. (in Russ.)
7. Tsaregorodtsev A.V., Taraskin M.M. *Methods and Means of Information Protection in Public Administration*. Moscow: Prospect Publ.; 2017. 205 p. (in Russ.)
8. Lynkov L.M., Golikov V.F., Borbotko T.V. *Fundamentals of Information Protection and Intellectual Property Management*. Minsk: Belarusian State University of Informatics and Radioelectronics Publ.; 2013. 243 p. (in Russ.)
9. Vorona V.A., Kostenko V.O. Ways and Means of Information Protection from Leaks Through Technical Channels. *Computational Nanotechnology*. 2016;3:208–223. (in Russ.) EDN:WKNGZD
10. Khorev A.A. *Technical Information Security*. Moscow: Analitika Publ.; 2008. 436 p. (in Russ.)
11. Buzov G.A., Kalinin S.V., Kondratyev A.V. *Protection against Information Leakage via Technical Channels*. Moscow: Goryachaya Liniya – Telecom Publ.; 2005. 415 p. (in Russ.) EDN:QMOJMV
12. GOST R 50840-95. *Speech transmission over various communication channels. Techniques for measurements of speech quality, intelligibility and voice identification*. Moscow: Gosstandart Rossii Publ.; 1997. 230 p. (in Russ.)
13. Dvoryankin S.V., Makarov Yu.K., Khorev A.A. Justification of the Criteria for the Effectiveness of Speech Information Protection from Leakage via Technical Channels. *Zašita informacii. Inside*. 2007;2(14):18–25. (in Russ.) EDN:TRKKQR
14. Zheleznyak V.K., Makarov Yu.K., Khorev A.A. Some Methodological Approaches to Assessing the Efficiency of Speech Information Protection. *Specialnaya tekhnika*. 2000;4:39–45. (in Russ.) EDN:YPUIBV
15. Khorev A.A. Methods and Means for Protection of Compartmentalized Security Zones Against Voice (Acoustic) Information Leakage Through Service Channels: Speech Protection Systems. *Specialnaya tekhnika*. 2013;4:31–63. (in Russ.) EDN:RINYMP
16. Makarov Yu.K., Khorev A.A. Methods of Speech Information Protection and Evaluation of Their Effectiveness. *Zašita informacii. Confidential*. 2001;4:22–33. (in Russ.)
17. Dvoryankin S.V., Dvoryankin N.S., Ustinov R.A. Improvement of Image Analysis/Synthesis Technologies of Acoustic (Speech) Information for the Control, Safety and Communication Systems. *IT Security (Russia)*. 2019;26(1):64–76. (in Russ.) EDN:VWAQNW
18. Alekseev V.V., Gridnev V.A., Moiseeva M.V., Ryzhkov A.P., Yakovlev A.V. *Theoretical Foundations for the Construction and Application of a Research Complex for Monitoring the Security Characteristics of Confidential Information*. Tambov: Tambov State Technical University Publ.; 2022. 100 p. (in Russ.)
19. Volchikhina M.V. Assessment of the Level of Verbal Intelligibility at the Border of the Controlled Zone of the Office Premises by the Articulation Method. *Vestnik of Voronezh Institute of the Ministry of the Interior of Russia*. 2022;2:105–112. (in Russ.) EDN:POMJEB

Статья поступила в редакцию 01.09.2025; одобрена после рецензирования 10.10.2025; принята к публикации 10.10.2025.

The article was submitted 01.09.2025; approved after reviewing 10.10.2025; accepted for publication 10.10.2025.

Информация об авторе:

ВОЛЧИХИНА
Мария Владимировна

специалист отдела аттестации научных и научно-педагогических кадров
Тамбовского государственного технического университета
 <https://orcid.org/0009-0004-6476-8614>

Автор сообщает об отсутствии конфликтов интересов.

The author declares no conflicts of interests.