



ВЕРОЯТНОСТНЫЙ МЕТОД ОБОСНОВАНИЯ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ЭФФЕКТИВНОСТИ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ ЕЕ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В статье предложено в качестве показателей оценки эффективности защиты речевой информации использовать вероятности вскрытия тематики перехваченного разговора и вероятности составления его аннотации. Получены аналитические соотношения по расчету вероятностей вскрытия тематики перехваченного разговора и составления его аннотации в зависимости от словесной и фразовой разборчивости речи, а также от количества ключевых слов и ключевых фраз, необходимых для определения тематики разговора и составления его аннотации. Предложена методика обоснования критериев эффективности защиты речевой информации.

Приведены результаты оценки зашумленных речевых сигналов методом артикуляционных испытаний. Получены аналитические соотношения для расчета словесной и фразовой разборчивости речи в зависимости от отношения сигнал/шум для 4-х видов шумов: «белый» шум, «розовый» шум, «коричневый» шум и шумовая «речеподобная» помеха.

Для сравнительной оценки эффективности шумовых помех введено понятие «коэффициент эффективности шумовой помехи», под которым понимается отношение сигнал/шум для определенного вида шума к отношению сигнал/шум для «белого» шума, выраженных в дБ, при которой разборчивости речи одинаковы. Получены аналитические соотношения для расчета «коэффициент эффективности шумовой помехи» для трех видов шумовых помех.

Ключевые слова: защита акустической речевой информации, показатели и критерии оценки эффективности защиты речевой информации от ее утечки по техническим каналам, разборчивость речи, вероятностный метод обоснования показателей и критериев оценки эффективности защиты речевой информации.

A PROBABILISTIC METHOD FOR SUBSTANTIATING INDICATORS AND CRITERIA FOR THE EFFECTIVENESS OF PROTECTING SPEECH INFORMATION FROM ITS LEAKAGE THROUGH TECHNICAL CHANNELS

The article suggests using probabilities of revealing the subject of an intercepted conversation and the probability of compiling its annotation as indicators for evaluating the effectiveness of protecting speech information. Analytical ratios have been obtained for calculating the probabilities of opening the subject of an intercepted conversation and compiling its annotation, depending on the verbal and phrasal intelligibility of speech, as well as on the number of keywords and key phrases necessary to determine the topic of the conversation and compile its annotation. A methodology for substantiating the criteria for the effectiveness of speech information protection is proposed.

The results of the evaluation of noisy speech signals by the method of articulation tests are presented. Analytical ratios have been obtained for calculating verbal and phrasal intelligibility of speech depending on the signal-to-noise ratio for 4 types of noise: "white" noise, "pink" noise, "brown" noise" and noise "speech-like" interference.

For a comparative assessment of the effectiveness of noise interference, the concept of "noise interference efficiency coefficient" is introduced, which refers to the signal-to-noise ratio for a certain type of noise to the signal-to-noise ratio for "white" noise, expressed in dB, at which speech intelligibility is the same. Analytical relations have been obtained for calculating the "noise interference efficiency coefficient" for three types of noise interference.

Keywords: *protection of acoustic speech information, indicators and criteria for evaluating the effectiveness of protecting speech information from leakage through technical channels, speech intelligibility, probabilistic method for substantiating indicators and criteria for evaluating the effectiveness of speech information protection.*

Введение

В качестве показателя эффективности защиты речевой информации от ее утечки по техническим каналам наиболее часто используется разборчивость речи (W), отображающая качественную область понятности перехваченного разговора, под которой понимается отношение количества правильно распознанных слов (фраз) к общему количеству слов (фраз) в перехваченном разговоре.

В качестве критерия эффективности защиты речевой информации от ее утечки по техническим каналам используется пороговый критерий, при использовании которого считается, что принятые меры по защите речевой информации от ее утечки по техническим каналам эффективны, если разборчивость речи, перехваченная средствами разведки по данным каналам (W), не превышает установленного порогового значения (W_n).

Таблица 1.

Показатели и критерии эффективности защиты речевой информации от ее утечки по техническим каналам

Цели защиты речевой информации	Показатели эффективности защиты речевой информации	Критерии эффективности защиты речевой информации	Пороговое значение разборчивости речи
Скрытие тематики текста	Словесная разборчивость текста ($W_{сл}$)	Количество правильно распознанных слов не позволяет установить тематику перехваченного разговора ($W_{сл} \leq W_{сл,n}$)	$W_{сл,n} = 0,2$
Скрытие содержания текста	Словесная разборчивость текста ($W_{сл}$)	Количество правильно распознанных слов не позволяет составить аннотацию (краткую справку) о перехваченном разговоре ($W_{сл} \leq W_{сл,n}$)	$W_{сл,n} = 0,3$

Критерии эффективности защиты речевой информации во многом зависят от целей, преследуемых при защите информации, например, скрыть тематику ведущегося разговора или скрыть его смысловое содержание.

В работе [1] на основе метода экспертных оценок предложены следующие критерии эффективности защиты речевой информации от ее утечки по техническим каналам, которые представлены в таблице 1.

Однако не все распознанные слова или фразы относятся к ключевым, по которым можно установить тематику перехваченного разговора и составить его аннотацию.

Следовательно, для оценки эффективности защиты речевой информации необходимо не только рассчитать словесную или фразовую разборчивость речи, но и оценить ко-

личество ключевых слов и фраз, требуемых для определения тематики разговора или составления ее аннотации.

1. Вероятностный метод обоснования критериев эффективности защиты речевой информации от ее утечки по техническим каналам

Будем полагать, что тематика разговора вскрыта, если количество распознанных ключевых слов $N_{сл,кл,p}$ будет не менее установленного порогового значения $N_{сл,кл,min}$, а аннотация разговора составлена, если количество распознанных ключевых фраз $N_{фр,кл,p}$ будет не менее установленного порогового значения $N_{фр,кл,min}$.

Тогда, вероятность вскрытия тематики разговора P_m можно рассчитать по формулам [2]:

$$P_m(N_{сл,кл,p} \geq N_{сл,кл,min}) = \sum_{i=N_{сл,кл,min}}^{N_{сл,кл,p}} P_m(N_{сл,кл,p,i}) \tag{1}$$

$$P_m(N_{сл,кл,p,i}) = \frac{C_{N_{сл,кл}}^{N_{сл,кл,p,i}} \cdot C_{N_{сл} - N_{сл,кл}}^{N_{сл,кл} - N_{сл,кл,p,i}}}{C_{N_{сл}}^{N_{сл,кл}}} \tag{2}$$

где $C_b^a = \frac{b!}{a! \cdot (b-a)!}$ – формула комбинаторики, определяющая количество сочетаний без повторов [3];

$N_{сл}$ – количество слов в перехваченном разговоре;

$N_{сл,кл} = k_{сл} \times N_{сл}$ – количество ключевых слов в перехваченном разговоре;

$k_{сл}$ – среднее относительное количество ключевых слов по данной тематике;

$N_{сл,p} = W_{сл} \times N_{сл}$ – количество распоз-

нанных слов в перехваченном разговоре;

$W_{сл}$ – словесная разборчивости перехваченного разговора;

$N_{сл,кл,p} = W_{сл} \times N_{сл,кл} = W_{сл} \times k_{сл} \times N_{сл}$ – количество распознанных ключевых слов в перехваченном разговоре;

$N_{сл,кл,min}$ – минимальное количество ключевых слов, необходимых для вскрытия тематики перехваченного разговора.

Учитывая, что $b > a$ формулу комбинаторики запишем в виде:

$$C_b^a = \frac{b!}{a! \cdot (b-a)!} = \frac{(a+1) \cdot (a+2) \cdot (a+3) \cdots b}{(b-a)!} = \frac{\prod_{j=a+1}^b j}{\prod_{j=1}^{b-a} j} \quad (3)$$

Подставив (3) в (2) и сократив формулу получим:

$$P_m(N_{сл.кл.p,i}) = \frac{\prod_{j=N_{сл.кл.p,i}+1}^{N_{сл.кл.}} j \cdot \prod_{j=N_{сл.кл.}-N_{сл.кл.p,i}+1}^{N_{сл.кл.}-N_{сл.кл.}} j \cdot \prod_{j=1}^{N_{сл.кл.}-N_{сл.кл.}} j}{\prod_{j=1}^{N_{сл.кл.}-N_{сл.кл.p,i}} j \cdot \prod_{j=N_{сл.кл.}-N_{сл.кл.p,i}+1}^{N_{сл.кл.}-N_{сл.кл.}} j \cdot \prod_{j=N_{сл.кл.}}^{N_{сл.кл.}-N_{сл.кл.p,i}} j \cdot \prod_{j=N_{сл.кл.}+1}^{N_{сл.кл.}} j} \quad (4)$$

Аналогичным образом может быть рассчитана и вероятность составления аннотации разговора $P_{ан}$:

$$P_{ан}(N_{фр.кл.p} \geq N_{фр.кл.min}) = \sum_{i=N_{фр.кл.min}}^{N_{фр.кл.p}} P_{ан}(N_{фр.кл.p,i}) \quad (5)$$

$$P_{ан}(N_{фр.кл.p,i}) = \frac{\prod_{j=N_{фр.кл.p,i}+1}^{N_{фр.кл.}} j \cdot \prod_{j=N_{фр.кл.}-N_{фр.кл.p,i}+1}^{N_{фр.кл.}-N_{фр.кл.}} j \cdot \prod_{j=1}^{N_{фр.кл.}-N_{фр.кл.}} j}{\prod_{j=1}^{N_{фр.кл.}-N_{фр.кл.p,i}} j \cdot \prod_{j=N_{фр.кл.}-N_{фр.кл.p,i}+1}^{N_{фр.кл.}-N_{фр.кл.}} j \cdot \prod_{j=N_{фр.кл.}}^{N_{фр.кл.}-N_{фр.кл.p,i}} j \cdot \prod_{j=N_{фр.кл.}+1}^{N_{фр.кл.}} j} \quad (6)$$

где $N_{фр}$ – количество фраз в перехваченном разговоре;

$N_{фр.кл}$ – количество ключевых фраз в перехваченном разговоре;

$N_{фр.кл.p}$ – количество распознанных ключевых слов в перехваченном разговоре;

$N_{фр.кл.min}$ – минимальное количество ключевых фраз, необходимых для вскрытия тематики перехваченного разговора;

$W_{фр}$ – словесная разборчивости перехваченного разговора.

2. Экспериментальные исследования разборчивости речи условиях шумов

С целью оценки разборчивости речи в условиях различного вида шумов были проведены экспериментальные исследования.

Исследования проводились в четыре этапа.

На **первом этапе** формировались исходные записи тестовых речевых сигналов.

В качестве тестовых речевых сигналов использовались таблицы слов из ГОСТ 16600-72 «Требования к разборчивости речи и методы артикуляционных измерений» и фраз – из ГОСТ 50840-95 «Передача речи по трактам связи методы оценки качества, разборчивости и узнаваемости». Запись тестовых речевых сигналов проводили 4 диктора (2 мужчин и 2 женщины), которые не имели дефектов речи. Чтение слов дикторами осуществлялось ровным

голосом, четко и без подчеркивания отдельных звуков с постоянным уровнем речи. Дикторы выдерживали постоянный ритм речи на протяжении чтения всей таблицы.

Запись тестовых речевых сигналов проводилась в служебном помещении при уровне шума не более 35–40 дБ на профессиональный цифровой диктофон Tascam DR-05X. Режимы записи: 48 кГц, 24 бит, формат записи – wav. Запись проводилась на съемную SD – карту.

Всего каждым диктором было записано 4 аудиофайла: 2 аудиофайла

с 2 таблицами по 50 слов и 2 аудиофайла с 2 таблицами по 50 фраз.

На **втором этапе** формировались помеховые сигналы.

При проведении экспериментальных исследований использовались следующие наиболее часто используемых в системах активной защиты видов шумов:

- 1) «белый» шум (БШ) – шум с равномерной спектральной плотностью;
- 2) «розовый» шум (РШ) – шум со спадом спектральной плотности
- 3) 3 дБ/на октаву;
- 4) «коричневый» шум (КШ) – шум со спадом спектральной плотности 6 дБ/на октаву;
- 5) шумовая «речеподобная» помеха (ШРП) – шум с огибающей спектра, подобной огибающей спектра речевого сигнала.

Типовые уровни речевого сигнала в октавных полосах частотного диапазона речи L_{si}

Номер полосы	Частотные границы полосы ($f_n - f_b$), Гц	Средне-геометрическая частота полосы f_g , Гц	Типовые спектральные уровни речи L_{si} , измеренные на расстоянии 1 м от источника сигнала, дБ			
			Тихая речь (64 дБ)	Речь средней громкости (70 дБ)	Громкая речь (76 дБ)	Очень громкая речь (84 дБ)
1	90 - 175	125	47	53	59	67
2	175 - 355	250	60	66	72	80
3	355 - 710	500	60	66	72	80
4	710 - 1400	1000	55	61	67	75
5	1400 - 2800	2000	50	56	62	70
6	2800 - 5600	4000	47	53	59	67
7	5600 - 11200	8000	43	49	55	63

Для формирования различного вида шумов использовалась ПЭВМ и специальное программное обеспечение Adobe Audition CC 2019 (далее – ПО Audition).

Для формирования шумовой «речеподобной» помехи использовался типовой спектр речевого сигнала, приведенный в таблице 2 [5].

На **третьем этапе** формировались тестовые речевые сигналы с заданным отношением сигнал/шум.

При проведении экспериментальных исследований под отношением сигнал/шум (с/ш) понималось среднее отношение речевой с/ш за весь период чтения диктором артикуляционной таблицы (50 слов или 50 фраз).

Для измерения среднего уровня тестового речевого сигнала из аудиофайла с записью таблиц слов или таблиц фраз, воспроизводимых диктором, с помощью ПО Audition вырезались паузы между словами.

Аудиофайл с записью тестового речевого сигнала с вырезанными паузами воспроизводился через звуковую колонку и с помощью шумомера, установленного на расстоянии 1 м от звуковой колонки, проводилось измерение его уровня.

С использованием инструмента «Усиление/Затухание» в ПО Audition устанавливался уровень усиления, при котором средний уровень тестового речевого сигнала с вырезанными паузами соответствовал уровню речевого сигнала средней громкости (см. таблицу 2).

Далее при фиксированном коэффициенте усиления ПО Audition аудиофайл с записью тестового речевого сигнала с паузами воспроизводился через звуковую колонку и осуществлялась его запись на цифровой диктофон Tascam DR-05X, установленный на расстоянии 1 м от звуковой колонки.

Затем на звуковую колонку с компьютера подавался шумовой сигнал и

с использованием инструмента «Усиление/Затухание» в ПО Audition устанавливался уровень шумового сигнала, при котором обеспечивалось требуемое отношение сигнал/шум частотном интервале 90–11200 Гц: 10 дБ; 5 дБ; 0 дБ; –5 дБ, –10 дБ, –15 дБ; –20 дБ.

Излучаемый звуковой колонкой шумовой сигнал записывался на цифровой диктофон Tascam DR-05X, установленный на расстоянии 1 м от звуковой колонки.

Аудиофайл с зашумленным тестовым речевым сигналом и заданным отношением с/ш формировался путем микширования тестового речевого сигнала и шумового сигнала с требуемым уровнем шума.

Всего каждого вида шумового сигнала было сформировано по 56 аудиофайлов с записями таблиц из 50 слов и по 56 аудиофайлов с записями таблиц по 50 фраз.

На **четвертом этапе** зашумленные тестовые речевые сигналы (аудиофайлы) прослушивались аудиторами и определялась словесная и фразовая разборчивость речи.

Прослушивание осуществляли 14 аудиторами (8 мужчин и 6 женщин), которые не имели дефектов слуха.

Результаты экспериментальных исследований

Отноше- ние с/ш, дБ	Разборчивость речи, W							
	«Белый» шум»		«Розовый» шум		«Коричневый» шум		Шумовая «речеподобная помеха»	
	$W_{сл}$	$W_{фр}$	$W_{сл}$	$W_{фр}$	$W_{сл}$	$W_{фр}$	$W_{сл}$	$W_{фр}$
10 дБ	1	1	1	1	1	1	1	1
5 дБ	0,97	1	1	1	1	1	0,91	1
0 дБ	0,91	0,99	0,9	1	0,9	1	0,78	0,92
- 5 дБ	0,79	0,96	0,69	0,83	0,88	1	0,6	0,78
- 10 дБ	0,57	0,82	0,44	0,59	0,82	0,97	0,29	0,43
- 15 дБ	0,31	0,48	0,23	0,15	0,53	0,83	0,07	0,11
- 20 дБ	0,13	0,13	0	0	0,39	0,59	0	0

Испытания проводились в помещении в нормальных климатических условиях при уровне шума не более 35–40 дБ.

Записи прослушивались аудиторами через головные наушники, подключаемые к линейному выходу звуковой карты ПЭВМ и обеспечивающие высокий уровень изоляции. Услышанные слова и фразы аудиторами записывались в соответствующие таблицы.

Слово считалось правильно понятым аудитором, если он его написал правильно. Фраза считалась правильно понятой аудитором, если он правильно записал ее смысл (орфографические ошибки при этом не учитываются).

По результатам анализа распознанных аудиторами слов и фраз для каждого вида помехового сигнала и для каждого отношения с/ш рассчитывалась словесная ($W_{сл}$) и фразовая ($W_{фр}$) разборчивости речи:

$$W_{сл} = \frac{\sum_{i=1}^k N_i}{k \cdot N_{сл}} \quad (7)$$

$$W_{фр} = \frac{\sum_{i=1}^k M_i}{k \cdot M_{фр}} \quad (8)$$

где N_i – количество правильно распознанных слов i -аудитором;

M_i – количество правильно распознанных фраз i -аудитором;

$N_{сл}$ – общее количество слов, прослушиваемых аудиторами;

$M_{фр}$ – общее количество фраз, прослушиваемых аудиторами;

k – количество аудиторов.

Результаты расчетов представлены в таблице 3.

Зависимости словесной и фразовой разборчивости речи от отношения с/ш с высокой степенью достоверности аппроксимируются формулами:

$$W_{сл} \approx \Phi(Q_{сл.1} \cdot q - Q_{сл.2}) \quad (9)$$

$$W_{фр} \approx \Phi(Q_{фр.1} \cdot q - Q_{фр.2}) \quad (10)$$

где q – отношение сигнал/шум в частотном интервале 90–11200 Гц, дБ;

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) dt \text{ – интеграл}$$

вероятности;

$\Phi^{-1}(x)$ – функция, обратная $\Phi(x)$;

$Q_{сл.1}$, $Q_{сл.2}$, $Q_{фр.1}$, $Q_{фр.2}$ – коэффициенты, характеризующие тестовые речевые сигналы, условия прослушивания и индивидуальные особенности аудиторов.

Выбор значений коэффициентов $Q_{сл.1}$, $Q_{сл.2}$, $Q_{фр.1}$, $Q_{фр.2}$ проводился из условия максимизации достоверности аппроксимации R^2 , которая рассчитывалась по формуле [6]

$$R^2 = 1 - \frac{\sum_{i=1}^m (W_i - W_{э.i})^2}{\sum_{i=1}^m (W_{э.i})^2 - \frac{1}{m} \sum_{i=1}^m (W_{э.i})^2} \quad (11)$$

где W_i – разборчивость речи для i -го отношения с/ш, рассчитанная по формуле (11) или (12);

$W_{э.i}$ – разборчивость речи для i -го отношения с/ш, рассчитанная по результатам экспериментальных исследований;

Таблица 4.

Значения коэффициентов $Q_{сл.1r}$ $Q_{сл.2r}$ $Q_{фр.1r}$ $Q_{фр.2r}$

Вид помехового сигнала	Словесная разборчивость речи			Фразовая разборчивость речи		
	$Q_{сл.1}$	$Q_{сл.2}$	R^2	$Q_{фр.1}$	$Q_{фр.2}$	R^2
«Белый» шум	0,13	1,45	1	0,21	2,98	1
«Розовый» шум	0,14	1,24	0,999	0,21	2,22	0,999
«Коричневый» шум	0,13	2,08	0,993	0,28	5,65	0,996
Шумовая «речеподобная» помеха	0,14	0,85	0,999	0,19	1,69	1

m – количество значений отношений с/ш, для которые разборчивость речи оценивалась экспериментально.

Рассчитанные значения коэффициентов $Q_{сл.1r}$ $Q_{сл.2r}$ $Q_{фр.1r}$ $Q_{фр.2r}$ приведены в таблице 4.

Графики зависимости разборчивости речи от отношения сигнал/шум для различного вида помех приведены на рисунках 1 и 2.

Точками (•) на рисунках обозначены значения разборчивости речи, полученные по результатам экспериментальных исследований.

Анализ рисунков показал, что разборчивость речи зависит не только от отношения сигнал/шум, но и от вида шума.

Для сравнительной оценки эффективности шумовых помех введем понятие «коэффициент эффективности шумовой помехи», под которым будем понимать отношение сигнал/шум для определенного вида шума к отношению сигнал/шум для «белого» шума, выраженных в дБ, при которой разборчивости речи одинаковы:

$$\kappa_{эф.ш} = \frac{q_{ш}}{q_{бш}} \tag{12}$$

$$\Phi^{-1}(W_{ш}) = \Phi^{-1}(W_{бш}) = Q_{1ш} \cdot (q_{ш} \cdot \kappa_{эф.ш}) - Q_{2ш} = Q_{1бш} \cdot q_{бш} - Q_{2бш} \tag{13}$$

где $\kappa_{эф.ш}$ – коэффициент эффективности шумовой помехи;
 $q_{ш}$ – отношение сигнал/шум для определенного вида шума, при котором разборчивость речи равна $W_{ш}$ дБ;
 $q_{бш}$ – отношение сигнал/шум для «белого» шума, при котором разборчивость речи равна $W_{бш} = W_{ш}$ дБ.

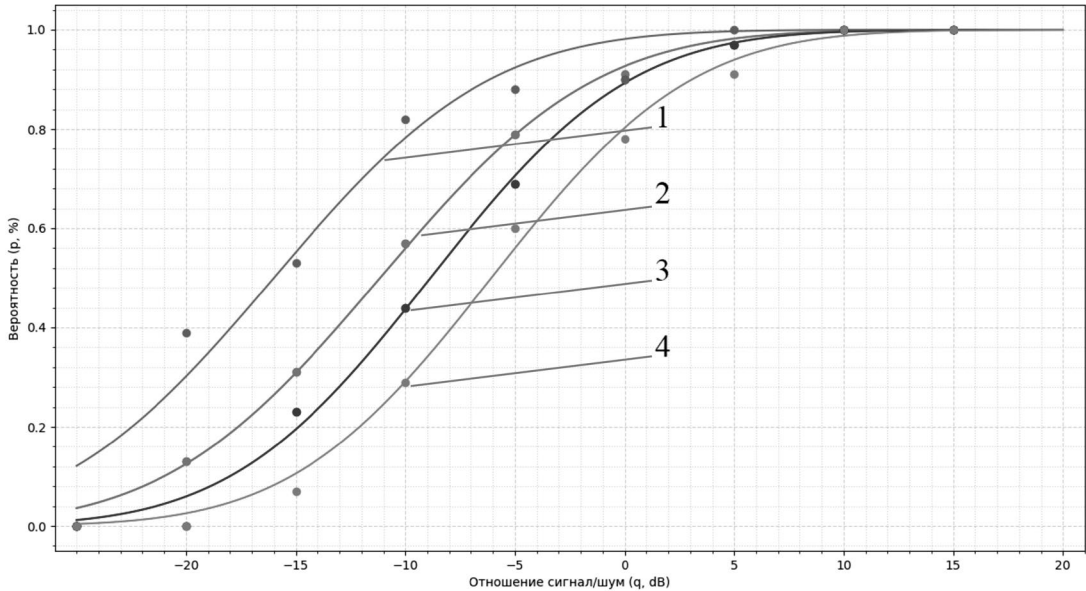


Рис. 1. Графики зависимости словесной разборчивости речи от отношения сигнал/шум: 1 – «коричневый» шум; 2 – «белый» шум; 3 – «розовый» шум; 4 – шумовая «речеподобная» помеха

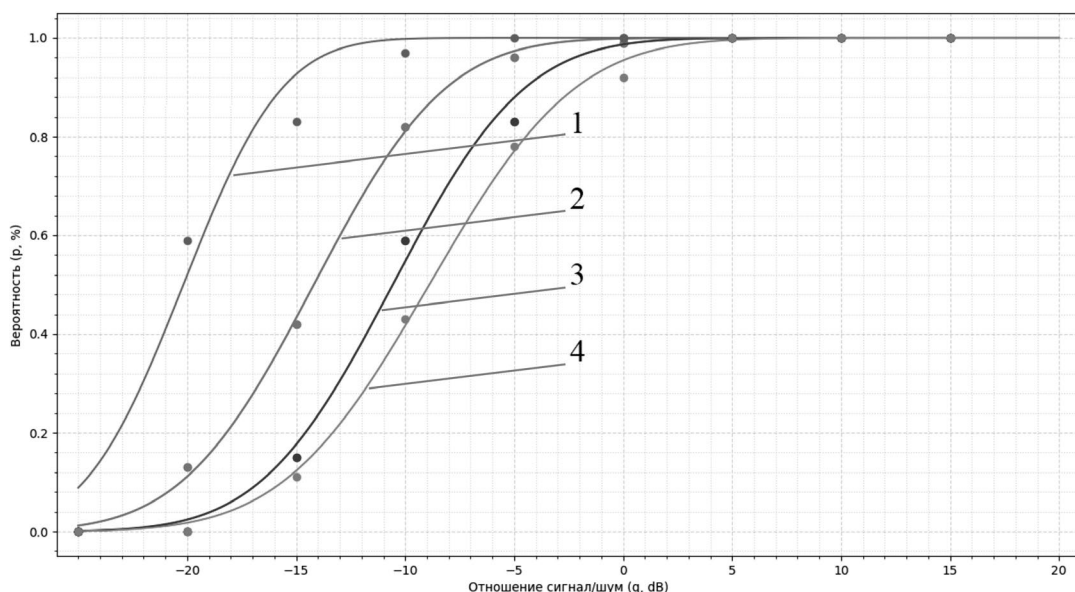


Рис. 2. Графики зависимости фразовой разборчивости речи от отношения сигнал/шум:
1 – «коричневый» шум; 2 – «белый» шум; 3 – «розовый» шум; 4 – шумовая «речеподобная» помеха

Из формулы (15) легко найти значение кэф.ш:

$$K_{эф.ш} = \frac{Q_{1бш} \cdot q_{бш} + Q_{2ш} - Q_{2бш}}{Q_{1ш} \cdot q_{бш}} = \frac{Q_{1бш}}{Q_{1ш}} + \frac{Q_{2ш} - Q_{2бш}}{Q_{1ш} \cdot q_{бш}} \quad (14)$$

Рассчитанные значения коэффициентов $K_{эф.ш}$ для различных видов шумов приведены в таблице 5.

Таблица 5.

Значения коэффициентов $K_{эф.ш}$ для различных видов шумов

Вид помехового сигнала	Формулы для расчета коэффициента кэф.ш	
	Словесная разборчивость речи	Фразовая разборчивость речи
«Белый» шум	$K_{эф.бш} = 1$	$K_{эф.бш} = 1$
«Розовый» шум	$K_{эф.рш} = 0,93 + 1,5/q$	$K_{эф.рш} = 1 + 3,6/q$
«Коричневый» шум	$K_{эф.кш} = 1 + 4,85/q$	$K_{эф.кш} = 0,75 + 9,54/q$
Шумовая «речеподобная» помеха	$K_{эф.рп} = 0,93 - 4,29/q$	$K_{эф.рп} = 1,1 - 6,79/q$

Графические зависимости коэффициентов кэф.ш для различных видов шумов приведены на рисунках 3 и 4.

Таким образом формулы для расчета словесной и фразовой разборчивости речи для различных видов шумов будут иметь вид:

$$W_{сл.ш} \approx \Phi(Q_{сл.1ш} \cdot K_{эф.ш} \cdot q - Q_{сл.ш.2}) \quad (15)$$

$$W_{фр.ш} \approx \Phi(Q_{фр.1ш} \cdot K_{эф.ш} \cdot q - Q_{фр.ш.2}) \quad (16)$$

где кэф.ш – коэффициент эффективности шумовой помехи, значение которого приведено в таблице 5;

$Q_{сл.1}, Q_{сл.2}, Q_{фр.1}, Q_{фр.2}$ – коэффициенты, значения которых приведены в таблице 3.

3. Методика обоснования критериев эффективности защиты речевой информации от ее утечки по техническим каналам

Так как длительность мероприятий конфиденциального характера может изменяться в широких пределах, целесообразно перехваченный разговор разбить на фрагменты, например, длительностью до 10 мин.

Учитывая, что средний темп речи на русском языке 120 – 130 слов в минуту [4], за 10 минут можно в среднем произнести 1200 – 1300 слов или 140 – 180 коротких фраз.

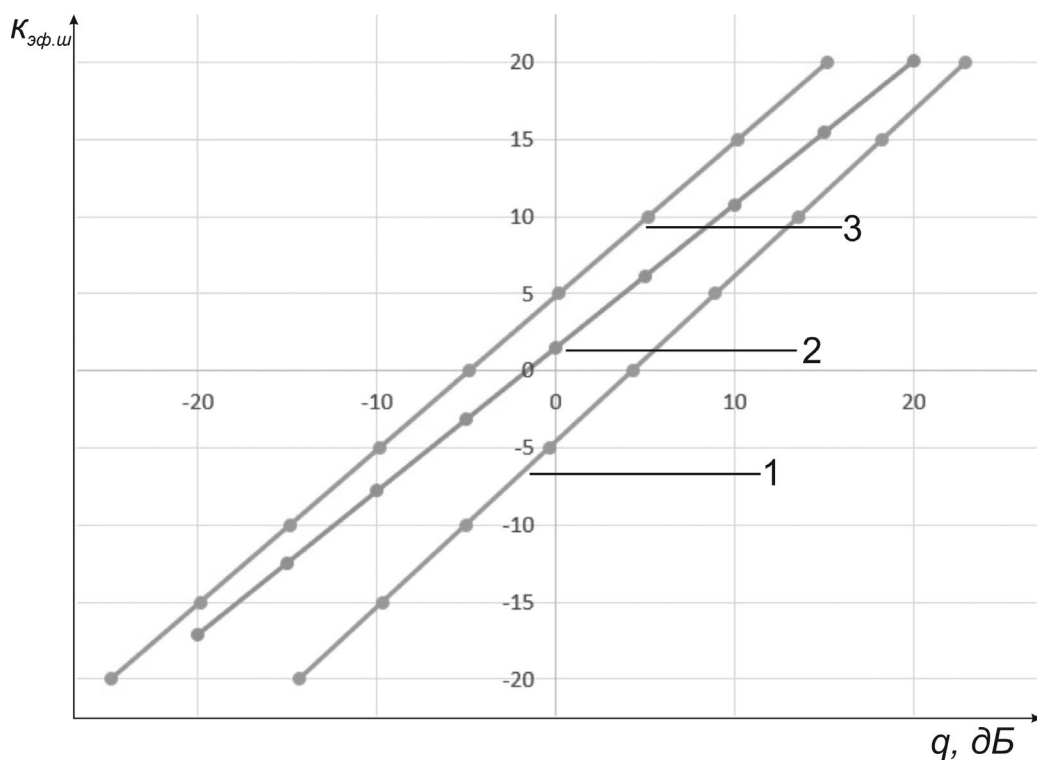


Рис. 3. Зависимости коэффициента эффективности шумовой помехи для словесной разборчивостей речи от вида шума:
1 – шумовая «речеподобная» помеха; 2 – «розовый» шум; 3 – «коричневый» шум

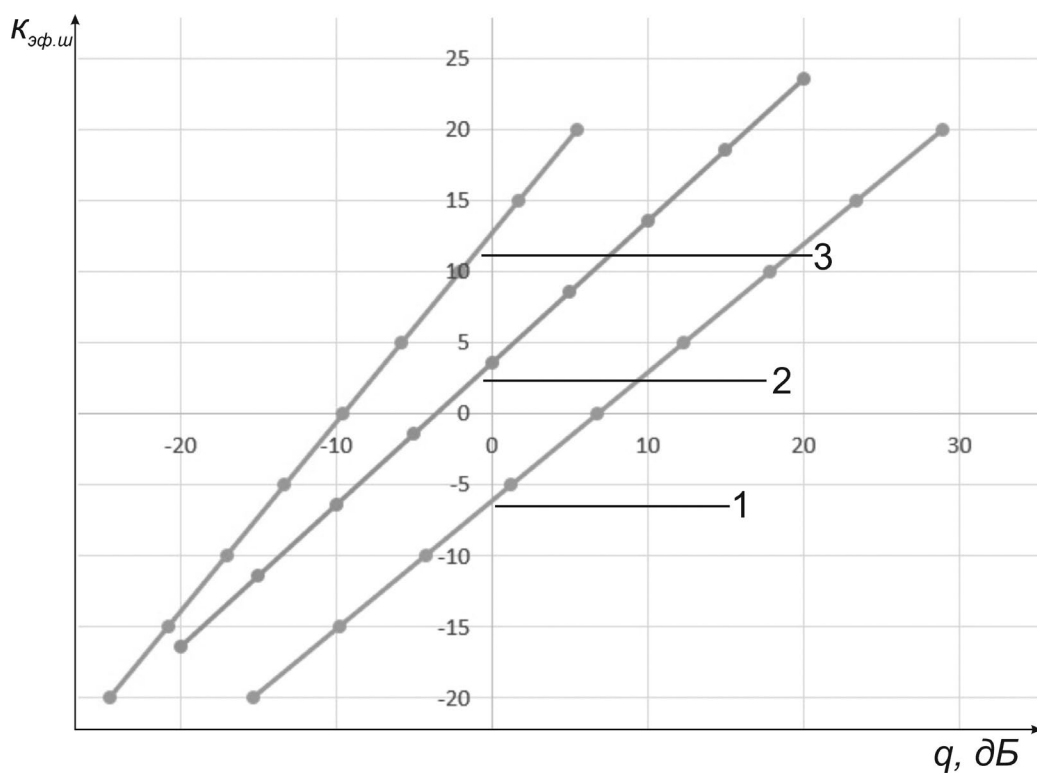


Рис. 4. Зависимости коэффициента эффективности шумовой помехи для фразовой разборчивостей речи от вида шума:
1 – шумовая «речеподобная» помеха; 2 – «розовый» шум; 3 – «коричневый» шум

Для каждого фрагмента разговора необходимо определить его тематику и составить аннотацию.

Будем полагать, что цели защиты речевой информации достигнуты, если для каждого фрагмента разговора нельзя соответственно определить его тематику, или нельзя составить его аннотацию.

С учетом вышесказанного, авторами предлагается следующая методика обоснования критериев эффективности защиты речевой информации от ее утечки по техническим каналам:

1) Экспериментально определяется относительное среднее количество ключевых слов $k_{сл}$ и ключевых фраз $k_{фр}$ по различной тематике.

2) По каждой тематике экспериментально определяются среднее количество ключевых слов $N_{сл.кл}$ и ключевых фраз $N_{фр.кл}$ в разговоре, длительностью 10 минут.

3) По каждой тематике экспериментально определяются минимальное количество

ключевых слов $N_{сл.кл.min}$ необходимых для вскрытия тематики разговора длительностью 10 минут, и минимальное количество ключевых фраз $N_{фр.кл.min}$ необходимых для составления его аннотации.

4) Экспертным методом определяются пороговые значения вероятности вскрытия тематики перехваченного разговора $P_{т.л}$ длительностью 10 минут, и вероятности составления аннотации его аннотации $P_{ан.л}$.

5) По формулам (1) и (2) строится зависимость вероятности вскрытия тематики перехваченного разговора $P_{т}$ длительностью 10 минут, от словесной разборчивости речи $W_{сл}$.

6) По графику зависимости вероятности вскрытия тематики перехваченного разговора $P_{т}$ от словесной разборчивости речи $W_{сл}$ для порогового значения вероятности вскрытия тематики перехваченного разговора $P_{т.л}$ определяется пороговое значение словесной разборчивости речи $W_{сл.п}$.

7) По формулам (5) и (6) строится зависимость вероятности составления аннотации

Таблица 6.

Зависимости вероятностей скрывания тематики разговора ($P_{т}$) и составления его аннотации ($P_{ан}$) от словесной ($W_{сл}$) и фразовой ($W_{фр}$) разборчивости речи от распознанных ключевых слов ($N_{сл.кл.р}$) и ключевых фраз ($N_{фр.кл.р}$)

$W_{сл}$	Вероятность вскрытия тематики разговора $P_{т}$				$W_{фр}$	Вероятность составления аннотации разговора $P_{ан}$			
	$N_{сл.кл.р} \geq 4$	$N_{сл.кл.р} \geq 5$	$N_{сл.кл.р} \geq 6$	$N_{сл.кл.р} \geq 7$		$N_{фр.кл.р} \geq 7$	$N_{фр.кл.р} \geq 8$	$N_{фр.кл.р} \geq 9$	$N_{фр.кл.р} \geq 10$
0,1	0,4	0,209	0,092	0,034	0,1	0	0	0	0
0,15	0,731	0,537	0,345	0,192	0,15	0,003	0	0	0
0,2	0,91	0,799	0,642	0,465	0,2	0,02	0,004	0,001	0
0,25	0,976	0,933	0,85	0,725	0,25	0,069	0,021	0,005	0,001
0,3	0,995	0,982	0,951	0,89	0,3	0,164	0,064	0,02	0,005
0,35	0,999	0,996	0,987	0,965	0,35	0,304	0,147	0,057	0,017
0,4	1	0,999	0,997	0,992	0,4	0,473	0,274	0,13	0,049
0,45	1	1	1	0,998	0,45	0,642	0,434	0,245	0,112
0,5	1	1	1	1	0,5	0,785	0,603	0,397	0,215
0,55	1	1	1	1	0,55	0,888	0,755	0,566	0,358
0,6	1	1	1	1	0,6	0,951	0,87	0,726	0,527
0,65	1	1	1	1	0,65	0,983	0,943	0,853	0,696
0,7	1	1	1	1	0,7	0,995	0,98	0,936	0,836
0,75	1	1	1	1	0,75	0,999	0,995	0,979	0,931
0,8	1	1	1	1	0,8	1	0,999	0,996	0,98
0,85	1	1	1	1	0,85	1	1	1	0,997
0,9	1	1	1	1	0,9	1	1	1	1
0,95	1	1	1	1	0,95	1	1	1	1
1	1	1	1	1	1	1	1	1	1

Показатели и критерии эффективности защиты речевой информации от ее утечки по техническим каналам

Цели защиты речевой информации	Показатели эффективности защиты речевой информации	Критерии эффективности защиты речевой информации		
		Пороговая вероятность скрытия тематики разговора $P_{т.п}$	Пороговая словесная разборчивость речи $W_{сл.п}$	Пороговая фразовая разборчивость речи $W_{фр.п}$
Скрытие тематики текста	Вероятность скрытия тематики разговора $P_{т}$	0,1	0,12	-
		0,2	0,15	-
		0,3	0,17	-
		0,4	0,2	-
Скрытие содержания текста	Вероятность составления аннотации разговора $P_{ан}$	0,1	-	0,45
		0,2	-	0,5
		0,3	-	0,53
		0,4	-	0,56

разговора $P_{ан}$ длительностью 10 минут, от фразовой разборчивости речи $W_{фр.}$

8) По графику зависимости вероятности составления аннотации разговора $P_{ан}$ длительностью 10 минут, от фразовой разборчивости речи $W_{фр.}$ для порогового значения вероятности составления аннотации разговора $P_{ан.п}$ определяется пороговое значение фразовой разборчивости речи $W_{фр.п.}$

Таким образом, для обоснования критериев эффективности защиты речевой информации необходимо рассчитать словесную и фразовую разборчивости речи и оценить среднее количество слов и фраз в перехваченном разговоре.

Среднее количество ключевых слов и ключевых фраз зависит от тематики разговора. Например, по результатам анализа научных докладов по тематике «информационная безопасность» среднее значение ключевых слов составляло 2,4%, по данным, проведенным в работе [5], и 1,97% – по данным приведенным в работе [6]. При этом среднее значение ключевых фраз составило 10,3% по данным, проведенным в работе [5], и 9,67% – по данным приведенным в работе [6].

В качестве примера в таблице 6 приведены зависимости вероятностей вскрытия тематики разговора ($P_{т}$) и составления его аннотации ($P_{ан}$) от словесной ($W_{сл.}$) и фразовой ($W_{фр.}$) разборчивости речи от распознанных ключевых слов ($N_{сл.кл.р}$) и ключевых фраз ($N_{фр.кл.р}$) для разговора, длительностью 10 минут, состоящего из 1300 слов (2,5% из которых ключевые) и 160 фраз (10% из которых ключевые).

Задаваясь пороговыми значениями вероятности скрытия тематики разговора $P_{т.п}$ составления его аннотации, а также значениями минимального количества ключевых слов $N_{сл.кл.мин}$ и ключевых фраз $N_{фр.кл.мин}$ по таблице легко определить пороговые значения словесной $W_{сл.п}$ и фразовой $W_{фр.п}$ разборчивости речи.

В таблице 7 приведены пороговые значения словесной и фразовой разборчивости речи для достижения требуемого уровня защиты информации для разговора, длительностью 10 минут, состоящего из 1300 слов (2,5% из которых ключевые) и 160 фраз (10% из которых ключевые) при $N_{сл.кл.мин} = 7$, а $N_{фр.кл.мин} = 10$.

Анализ результатов экспериментальных исследований, представленные в п. 2, показал, что фразовая разборчивость речи ($W_{фр.}$) связана со словесной разборчивостью ($W_{сл.}$) зависимостью, представленной на рисунке 6, которую можно аппроксимировать функцией:

$$W_{фр.} \approx \Phi(5,15 \cdot W_{сл.} - 1,45) \tag{17}$$

где $\Phi(x) = \frac{1}{2\pi} \cdot \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) dt$ – интеграл

вероятности.

Представленная на рисунке 5 зависимость фразовой разборчивости речи от словесной согласуется с результатами экспериментальных исследований профессора Покровского Н.Б. (на графике 5 точками (•) представлены результаты экспериментальных исследований профессора Покровского Н.Б. [7]).

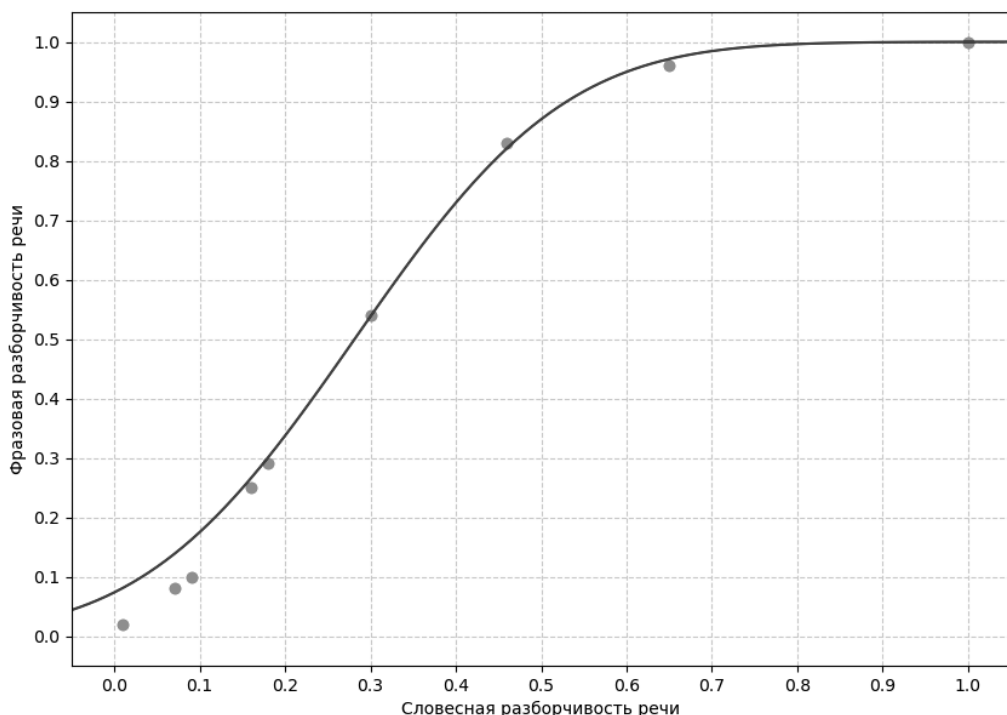


Рис. 5. Зависимость фразовой разборчивости речи ($W_{фр}$) от словесной ($W_{сл}$), рассчитанная по формуле (17)

Из формулы (17) легко найти значение словесной разборчивости речи $W_{сл}$:

$$W_{сл} \approx 0,194 \cdot \left[\Phi^{-1}(W_{фр}) + 1,45 \right] \quad (18)$$

где $\Phi^{-1}(x)$ – функция, обратная интегралу вероятности.

С учетом формулы (18) можно получить зависимость вероятности составления аннотации текста от словесной разборчивости речи для различного минимального количества ключевых фраз ($N_{фр.кл.мин}$).

В табл. 8 приведены показатели и критерии эффективности защиты речевой информации от ее утечки по техническим каналам с учетом пересчета фразовой разборчивости текста в словесную.

Анализ данных, представленных в таблице 8, показывает их корреляцию с данными, представленными в таблице 1.

Полученные результаты исследований могут быть использованы при обосновании показателей и критериев эффективности защиты речевой информации в выделенных помещениях.

Таблица 8.

Показатели и критерии эффективности защиты речевой информации от ее утечки по техническим каналам

Цели защиты речевой информации	Показатели эффективности защиты речевой информации	Критерии эффективности защиты речевой информации	
		Пороговая вероятность скрывания тематики разговора $P_{м.п}$	Пороговая словесная разборчивость речи $W_{сл.п}$
Скрытие тематики текста	Вероятность скрывания тематики разговора P_m	0,1	0,12
		0,2	0,15
		0,3	0,17
		0,4	0,2
Скрытие содержания текста	Вероятность составления аннотации разговора $P_{ан}$	0,1	0,26
		0,2	0,28
		0,3	0,3
		0,4	0,31

Литература

1. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации// Защита информации. Инсайд. – С. Петербург.: 2007. – № 2 – С. 18 – 25.
2. Вентцель Е. С. Задачи и упражнения по теории вероятностей: Учеб. пособие для студ. вузов / Е. С. Вентцель, Л. А. Овчаров. - 5-е изд., испр. - М.: Издательский центр «Академия», 2003. - 448 с.
3. Яремко Н. Н. Краткий курс комбинаторики, теории вероятностей и математической статистики: учеб. пособие / Н. Н. Яремко, О. Г. Никитина. – Пенза: Изд-во ПГУ, 2017. – 134 с.
4. Метлова В. А. Темп речи в свободной коммуникации: социолингвистический аспект// Вестник Пермского университета Российская и зарубежная филология. Пермь: Изд-во Пермск. ун-та, 2014. Вып. – 4 (28). – С. 58-65.
5. Хорев А.А., Суворова В.Ю. Оценка относительного количества ключевых фраз и слов в научных текстах// Всероссийская конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2023». Доклады. – М.: РНТОРЭС имени А.С.Попова. 2023. – С. 412 – 415.
6. Хабирова Л.А. Оценка среднего количества ключевых слов и ключевых фраз в научных текстах: выпускная квалификационная работа: 10.03.01; рук. Хорев А.А. – М.: МИЭТ, 2024. – 72 с.
7. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Гос. Издательство литературы по вопросам связи и радио, 1962. – 392 с.

References

1. Dvoryankin S.V., Makarov YU.K., Khorev A.A. Obosnovaniye kriteriyev effektivnosti zashchity rechevoy informatsii// Zashchita informatsii. Insayd. – S. Peterburg.: 2007. – № 2 – S. 18 – 25.
2. Venttsel' Ye. S. Zadachi i uprazhneniya po teorii veroyatnostey: Ucheb. posobiye dlya stud. vtuzov / Ye. S. Venttsel', L. A. Ovcharov. - 5-ye izd., ispr. - M.: Izdatel'skiy tsentr «Akademiya», 2003. - 448 s.
3. Yaremko N. N. Kratkiy kurs kombinatoriki, teorii veroyatnostey i matematicheskoy statistiki: ucheb. posobiye / N. N. Yaremko, O. G. Nikitina. – Penza: Izd-vo PGU, 2017. – 134 s.
4. Metlova V. A. Temp rechi v svobodnoy kommunikatsii: sotsiolingvisticheskiy aspekt// Vestnik Permskogo universiteta Rossiyskaya i zarubezhnaya filologiya. Perm': Izd-vo Permsk. un-ta, 2014. Vyp. – 4 (28). – S. 58-65.
5. Khorev A.A., Suvorova V.YU. Otsenka otnositel'nogo kolichestva klyuchevykh fraz i slov v nauchnykh tekstakh// Vserossiyskaya konferentsiya «Radioelektronnyye ustroystva i sistemy dlya infotelekkommunikatsionnykh tekhnologiy – REUS-2023». Doklady. – M.: RNTORES imeni A.S.Popova. 2023. – S. 412 – 415.
6. Khabirova L.A. Otsenka srednego kolichestva klyuchevykh slov i klyuchevykh fraz v nauchnykh tekstakh: vypusknaya kvalifikatsionnaya rabota: 10.03.01; ruk. Khorev A.A. – M.: MIET, 2024. – 72 s.
7. Pokrovskiy N.B. Raschet i izmereniye razborchivosti rechi. – M.: Gos. Izdatel'stvo literatury po voprosam svyazi i radio, 1962. – 392 s.

ХОРЕВ Анатолий Анатольевич, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Московский институт электронной техники» (МИЭТ). 124498, Москва, г. Зеленоград, площадь Шокина, дом 1. E-mail: horev@mieee.ru

ПОРСЕВ Илья Сергеевич, старший преподаватель кафедры «Информационная безопасность» федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «Московский институт электронной техники» (МИЭТ). 124498, Москва, г. Зеленоград, площадь Шокина, дом 1. E-mail: ib.labs@yandex.ru

HOREV Anatoly Anatolyevich, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, Federal State Autonomous Educational Institution of Higher Education, National Research University Moscow Institute of Electronic Technology (MIET). 124498, Moscow, Zelenograd, Shokin Square, Building 1. E-mail: horev@mieee.ru

PORSEV Ilya Sergeevich, Senior Lecturer, Department of Information Security, Federal State Autonomous Educational Institution of Higher Education, National Research University Moscow Institute of Electronic Technology (MIET). 124498, Moscow, Zelenograd, Shokin Square, Building 1. E-mail: ib.labs@yandex.ru