http://dx.doi.org/10.35596/1729-7648-2022-20-6-45-51

Оригинальная статья
Original paper

УДК 004.056.5, 534.41

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ МЕТОДА ОЦЕНКИ ЗАЩИЩЕННОСТИ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ПО ОГИБАЮЩЕЙ РЕЧЕВОГО СИГНАЛА

В.К. ЖЕЛЕЗНЯК[1], Е.Р. АДАМОВСКИЙ[1], А.Г. ФИЛИППОВИЧ[2]

[1]*Полоцкий государственный университет (г. Новополоцк, Республика Беларусь)*

[2]*Оперативно-аналитический центр при Президенте Республики Беларусь (г. Минск, Республика Беларусь)*

Поступила в редакцию 15 апреля 2022

Аннотация. Предложен метод оценки защищенности канала утечки информации на основе взаимно-корреляционного анализа огибающей измерительного сигнала в речевом диапазоне частот. Алгоритм включает генерацию измерительного сигнала и выделение его огибающей, излучение и измерение в канале утечки, выделение огибающей результирующего сигнала, вычисление коэффициента корреляции между исходной и полученной огибающими, сравнение с пороговым значением. Описан метод выделения низкочастотной огибающей сигнала с помощью преобразования Гильберта. Приведено описание взаимно-корреляционного анализа на основе коэффициента корреляции Пирсона. Выполнено имитационное моделирование канала утечки, формирования и измерения измерительных сигналов, а также их обработка в программной среде MatLab. Полученные результаты подтверждают большую эффективность использования огибающей по сравнению с исходным сигналом, а также демонстрируют преимущество речевых сигналов перед гармоническими сигналами в качестве измерительных для оценки защищенности канала утечки информации.

Ключевые слова: канал утечки информации, огибающая речевого сигнала, взаимная корреляция, техническая защита информации.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Железняк В.К., Адамовский Е.Р., Филиппович А.Г. Имитационное моделирование метода оценки защищенности канала утечки информации по огибающей речевого сигнала. Доклады БГУИР. 2022; 20(6): 45-51.

SIMULATION OF THE SECURITY ASSESSMENT INFORMATION LEAKAGE CHANNEL METHOD BASED ON THE SPEECH SIGNAL ENVELOPE

VLADIMIR K. ZHELEZNYAK[1], YAHOR R. ADAMOVSKIY[1], ANDREI G. FILIPOVICH[2]

[1]*Polotsk State University (Novopolotsk, Republic of Belarus)*

[2]*Operational and Analytical Center under the Aegis of the President of the Republic of Belarus (Minsk, Republic of Belarus)*

Submitted 15 April 2022

Abstract. A method of information leakage channel security estimating based on the test speech signal envelope cross-correlation analysis is proposed and its includes: test signal generating and extracting its envelope, emitting and measuring in a leakage channel, extracting the resulting signal envelope, calculating the correlation coefficient between the original and received envelopes, and comparing with a threshold value. A metod for extracting a low-frequency signal envelope using the Hilbert transform is shown. A description of the cross-correlation analysis based on the Pearson correlation coefficient is given. The leakage channel simulation modeling, formation and measurement of the test signals was performed in the MatLab. The obtained results confirm the greater efficiency of using the envelope compared to the original signal, and demonstrate the speech signals advantage over harmonic signals as test signals for assessing the information leakage channel security.

Keywords: information leakage channel, speech signal envelope, cross-correlation, technical information security.

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

For citation. Zheleznyak V.K., Adamovskiy Y.R., Filipovich A.G. Simulation of the Security Assessment Information Leakage Channel Method Based on the Speech Signal Envelope. Doklady BGUIR. 2022; 20(6): 45-51.

Введение

Способы оценки каналов утечки информации (КУИ) речевых сигналов являются темой исследований в области технической защиты информации (ТЗИ). Актуальность направления заключается в том, что не выработано единой однозначной модели восприятия речи, а существующие методы оценки дают значительные погрешности [1, 2]. Следовательно, защищенность канала также не может быть однозначным образом оценена.

Питание усилителей осуществляется через сеть переменного тока. Изменение потребления тока нагрузки приводит к нестабильности по току на входе стабилизатора [3]. Таким способом речевой сигнал из питаемой микрофонной системы способен проникать в электромагнитный канал утечки в составе излучения усилителя.

Известно, что речевой сигнал в частотной области характеризуется набором областей (формант) кратных частот в диапазоне от 90 до 10–13 кГц [4]. Во временной области для речевого сигнала может быть вычислена огибающая в инфранизком и низком диапазонах частот (до 20–30 Гц), которая отражает медленные изменения его амплитуды.

Таким образом, для речевого сигнала возможности ограничения полосы в принципе ограничены, поскольку он сам является широкополосным, а его составляющие нестабильны по частоте и амплитуде. В то же время огибающая речевого сигнала преимущественно сосредоточена в известной и сравнительно узкой полосе частот, что открывает возможности для улучшения качества оценки.

В данной работе предлагается метод оценки защищенности КУИ на основе анализа огибающей измерительного речевого сигнала в точке наблюдения.

Методика проведения эксперимента

Рассмотрим аналитический сигнал $s(t)$, который является комплексной функцией, реальная $s_{re}(t)$ и мнимая $s_{im}(t)$ части которого связаны преобразованием Гильберта [5]. Практическая значимость соотношения (1) заключается в возможности выделения из его частей мгновенной амплитуды $u(t)$ (2), фазы $\varphi(t)$ (3) и частоты $\omega(t)$ (4) исходного сигнала, что применимо и к реальным сигналам, представленным на практике в виде компонента $s_{re}(t)$.

$$s_{im}(t) = \int_{-\infty}^{\infty} s_{re}(\tau)/\pi(t-\tau)d\tau\,. \tag{1}$$

$$u(t) = \sqrt{s_{re}^2(t) + s_{im}^2(t)}\,. \tag{2}$$

$$\varphi(t) = \operatorname{arctg}\left(s_{im}(t)/s_{re}(t)\right). \tag{3}$$

$$\omega(t) = d\varphi/dt\,. \tag{4}$$

Набор значений мгновенной амплитуды $u(t)$ соответствует понятию огибающей сигнала, которой оперируют при обработке амплитудно-модулированных (АМ) сигналов. Рассмотрим АМ-сигнал $s(t)$ (5), который получен путем перемножения модулируемого $s_c(t)$ и модулирующего $s_e(t)$ сигналов единичной амплитуды с заданным коэффициентом корреляции m (6):

$$s(t) = (1 + m \times s_e(t)) \times s_c(t)\,, \tag{5}$$

$$m = \frac{s(t)_{\text{макс}} - s(t)_{\text{мин}}}{s(t)_{\text{макс}} + s(t)_{\text{мин}}}\,. \tag{6}$$

В наиболее распространенном на практике случае, когда несущее колебание является гармоническим колебанием (рис. 1), то сигнал $s_e(t)$ соответствует $u(t)$ по частоте и отличается от него в m раз по амплитуде.

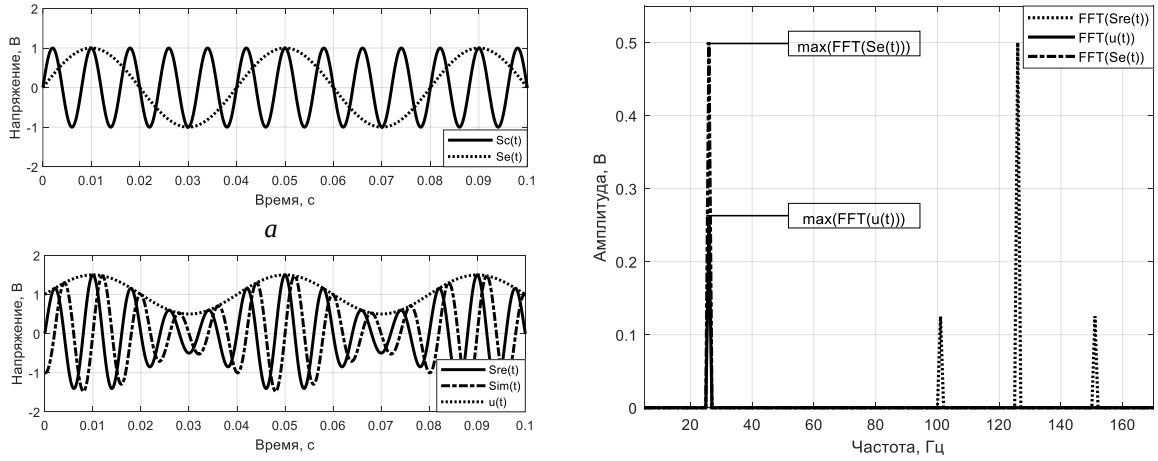


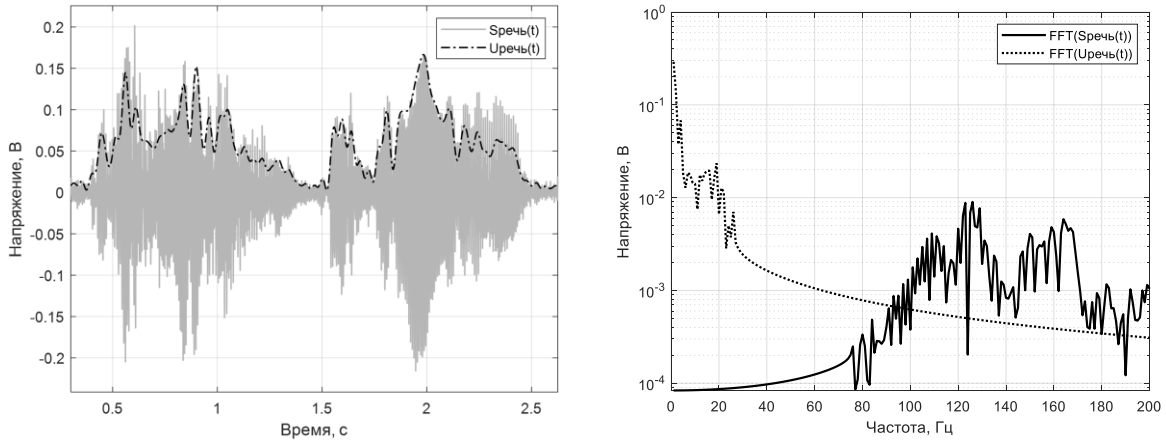
Рис. 1. Структура АМ-сигнала: *a* – несущее и модулирующее колебание; *b* – сигнал и огибающая во временной области; *c* – сигналы в частотной области

Fig. 1. AM-signal and its components structure: *a* – carrier and modulating oscillation; *b* – signal and envelope (time domain); *c* – all signals (frequency domain)

Для случая, когда модулируется не одна, а множество гармоник (речевой сигнал), форма огибающей приобретает сложную форму, поскольку отражает мгновенные амплитуды интерференции составляющих его частот, а не их сумму [5].

На рис. 2 показан речевой сигнал $s_{\text{речь}}(t)$ (запись фразы «Добрый день, как вас зовут?» длительностью 3 с), где область частот ниже 75 Гц вырезана с целью устранения помех сети,

и выделенная огибающая $u_{\text{речь}}(t)$, где частоты выше 30 Гц подавлены. Следует отметить, что в огибающей после фильтрации, соответствующей удалению порядка 99 % спектральных отсчетов, остается около 25 % ее исходной мощности.



a *b*

Рис. 2. Речевой сигнал и его огибающая: *a* – временная область; *b* – частотная область
Fig. 2. Speech signal and its envelope: *a* – time domain; *b* – frequency domain

Присутствие амплитудной модуляции в КУИ может быть вызвано процессами, не связанными с работой устройства, для которого осуществляется оценка защищенности. Таким образом, требуется установить взаимосвязь между излучаемым сигналом и сигналом в точке наблюдения. В качестве меры схожести последовательностей используют коэффициент корреляции Пирсона (7), обозначаемый как *R* [6]:

$$R = \frac{M\left[\left(s(t) - M\left[s(t)\right]\right) \times \left(u(t) - M\left[u(t)\right]\right)\right]}{\sigma_{s(t)} \times \sigma_{u(t)}}, \tag{7}$$

где M – математическое ожидание; σ – стандартное отклонение.

Коэффициент корреляции R отражает то, насколько изменение одной величины влияет на другую, при этом вариация абсолютных амплитуд сигналов не оказывает воздействия на результат.

Метод оценки защищенности канала утечки информации на основе взаимно-корреляционного анализа огибающей измерительного сигнала в речевом диапазоне частот заключается в генерации и излучении измерительного сигнала, огибающая которого сравнивается с огибающей колебания в точке наблюдения. Величина, обратная амплитуде корреляции между ними, определяет степень защищенности КУИ. Алгоритм включает следующие шаги:

1. Генерация измерительного АМ-сигнала $s_{\text{тест}}(t)$ в речевом диапазоне частот (5), (6). При этом модулируемое многочастотное колебание $s_{c.\text{тест}}(t)$ должно включать набор кратных гармоник основного тона $f_N = N \times f_1$, который лежит в области 100–150 Гц, а модулирующее колебание $s_{e.\text{тест}}(t)$ должно иметь квазипериодическую структуру в области до 30 Гц.

2. Выделение огибающей $u_{\text{тест}}(t)$ из измерительного АМ-сигнала (2). В общем случае $u_{\text{тест}}(t)$ эквивалентно $s_{e.\text{тест}}(t)$, следовательно, шаг является необязательным в случае синтезированного сигнала $s_{\text{тест}}(t)$.

3. Излучение измерительного сигнала $s_{\text{тест}}(t)$ в КУИ и его измерение в точке наблюдения как $s_{\text{куи}}(t)$. В простейшей модели полученный сигнал $s_{\text{куи}}(t)$ может быть представлен как аддитивная смесь $s_{\text{тест}}(t)$ с шумом КУИ $w(t)$ (8).

$$s_{\text{куи}}(t) = s_{\text{тест}}(t) + w(t). \tag{8}$$

4. Выделение из $s_{\text{куи}}(t)$ огибающей $u_{\text{куи}}(t)$ аналогично п. 2.

5. Обработка $u_{\text{тест}}(t)$ и $u_{\text{куи}}(t)$ взаимно-корреляционным способом (7).

6. Сравнение полученной величины R с нормативным пороговым значением $R_{\text{порог}}$, определяющим максимально допустимое значение схожести огибающих, при котором канал считается защищенным.

Схема модели представлена на рис. 3.

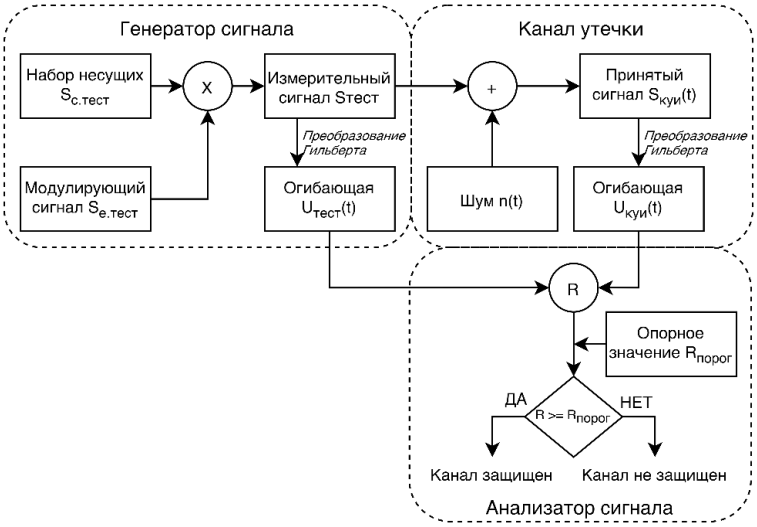


Рис. 3. Алгоритм имитационной модели метода оценки
Fig. 3. Simulation model algorithm of estimate method

Результаты и их обсуждение

Имитационная модель реализована с помощью стандартных инструментов программной среды *MatLab*. В качестве шума КУИ использовался аддитивный белый гауссовский шум (*AWGN*). Речевые сигналы были ограничены частотой 48 кГц, разрядность АЦП 16 бит. Коэффициент корреляции R вычислялся с использованием встроенной функции *corrcoef*.

В табл. 1 показаны результаты имитационного моделирования, которые содержат значения коэффициентов взаимной корреляции R и модуляции m измерительных сигналов как среднее арифметическое 10 измерений; данные получены согласно представленному алгоритму.

Таблица 1. Значения коэффициентов корреляции и модуляции сигналов в зависимости от уровня шума
Table 1. Values of correlation and modulation coefficients of signals depending on the noise level

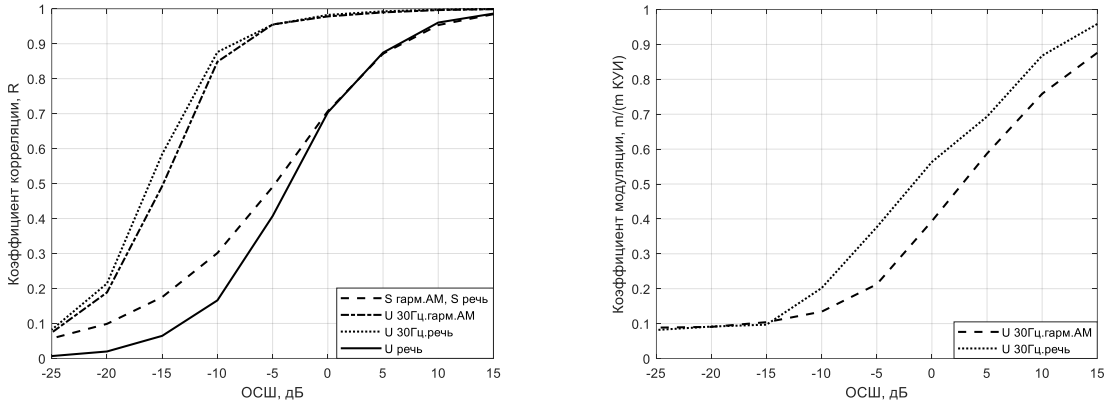
ОСШ, дБ SNR, dB	$U_{\text{речь}}(t)-U_{\text{речь.КУИ}}(t)$				$S_{\text{речь}}(t)-S_{\text{речь.КУИ}}(t)$	$U_{\text{гарм.АМ}}(t)-U_{\text{гарм.АМ.КУИ}}(t)$		$S_{\text{гарм.АМ}}(t)-S_{\text{гарм.АМ.КУИ}}(t)$
	$R_{30\text{Гц}}$	$m_{30\text{Гц.КУИ}}$	R	$m_{\text{КУИ}}$	R	$R_{30\text{Гц}}$	$m_{30\text{Гц.КУИ}}$	R
–	1	1	1	1	1	1	1	1
+15	0,9994	0,9586	0,9863	0,9998	0,9845	0,9989	0,8760	0,9845
+10	0,9975	0,8678	0,9606	0,9997	0,9534	0,9963	0,7586	0,9534
+5	0,9928	0,6932	0,8745	0,9998	0,8715	0,9897	0,5872	0,8715
0	0,9825	0,5633	0,7036	0,9999	0,7067	0,9782	0,3938	0,7071
–5	0,9545	0,3765	0,4071	1	0,4902	0,9552	0,2126	0,4903
–10	0,8762	0,2020	0,1660	0,9985	0,3012	0,8485	0,1342	0,3013
–15	0,5844	0,0970	0,0645	0,9991	0,1745	0,4929	0,1041	0,1753
–20	0,2143	0,0915	0,0198	0,9995	0,0994	0,1886	0,0906	0,0988
–25	0,0821	0,0817	0,0067	0,9992	0,0559	0,0739	0,0884	0,0571

В качестве измерительных сигналов был использован речевой сигнал $S_{\text{речь}}(t)$ – озвученная на русском языке панграмма; выделенная огибающая $U_{\text{речь}}(t)$; гармонический АМ-сигнал $S_{\text{гарм.АМ}}(t)$ (m = 1); выделенная огибающая $U_{\text{гарм.АМ}}(t)$. Исходные речевые сигналы подвергались зашумлению во всей полосе частот с отношением сигнал/шум (ОСШ) по мощности от плюс 15 дБ

до минус 25 дБ с шагом 5 дБ. Также представлен случай, когда шум отсутствует (соответствует первой строке данных табл. 1).

В результате были получены сигналы $S_{\text{речь.КУИ}}(t)$, $U_{\text{речь.КУИ}}(t)$, $S_{\text{гарм.АМ.КУИ}}(t)$ и $U_{\text{гарм.АМ.КУИ}}(t)$ соответственно. Огибающие ограничивались по частоте до 30 Гц. Измерено соотношение исходного m и полученного $m_{30\text{Гц.КУИ}}$ коэффициента модуляции для сравнения со значениями корреляции R. Дополнительно для анализа сигналов $U_{\text{речь}}(t)$ и $U_{\text{речь.КУИ}}(t)$ был реализован вариант без ограничения огибающей по частоте для исследования влияния высокочастотной (ВЧ) составляющей на результаты моделирования, измерено соответствующее значение $m_{\text{КУИ}}$.

На рис. 4, *a* показаны значения R и $R_{30\text{Гц}}$ согласно табл. 1. Анализ табл. 1 показывает, что уровни корреляции между исходным колебанием и его зашумленной копией для речевого и гармонического сигналов практически идентичны, поэтому на рис. 4, *a* они объединены в одну кривую. На рис. 4, *b* показаны значения $m_{\text{КУИ}}$ и $m_{30\text{Гц.КУИ}}$ согласно табл. 1, при этом опущено значение $m_{\text{КУИ}}$ для неограниченной по частоте огибающей речевого сигнала. Из-за влияния шума $m_{\text{КУИ}}$ оставалось приблизительно равным единице и не содержало полезной информации, что подтверждает необходимость ограничения огибающей для последующего анализа.



a *b*

Рис. 4. Результаты имитационного моделирования при различных уровнях шума, сравнение: *a* – коэффициента взаимной корреляции; *b* – коэффициента модуляции

Fig. 4. Simulation modeling results at different noise levels, comparison: *a* – cross-correlation coefficient; *b* – modulation coefficient

Из рис. 4, *a* следует, что оценка корреляционных свойств сигналов во всей доступной частотной полосе дает низкие значения, поскольку в таком случае влияние широкополосного шума значительно снижает величину меры схожести. Это подтверждается быстрым спадом кривых $S_{\text{гарм.АМ}}, S_{\text{речь}}$ и $U_{\text{речь}}$ сигналов, не ограниченных по частоте. Для кривых $U_{30\text{Гц.речь}}$ и $U_{30\text{Гц.гарм.АМ}}$, соответствующих узкополосным сигналам, убывание $R_{30\text{Гц}}$ с увеличением мощности шума происходит более медленно, особенно для огибающей речевого сигнала.

Рис. 4, *b* демонстрирует характер падения коэффициента модуляции $m_{30\text{ГцКУИ}}$, вычисленного по огибающим сигналов. Показано, что модуляция речевого сигнала более устойчива к шуму, чем гармонического модулированного сигнала. Преимущество сохраняется до уровня помех –15 дБ, а затем в обоих случаях $m_{30\text{ГцКУИ}}$ выходит на плато значений 0,09–0,1, соответствующих фоновому уровню m практически случайных колебаний.

Заключение

Представлен метод оценки защищенности канала утечки информации на основе взаимно-корреляционного анализа огибающей измерительного сигнала в речевом диапазоне частот и результаты имитационного моделирования метода. Произведен сравнительный анализ результатов для огибающей речевого сигнала, исходного речевого сигнала и гармонического

амплитудно-модулированного сигнала. Показаны преимущества использования огибающей речевого сигнала для оценки защищенности канала утечки информации.

Список литературы

1. Анохин В.В., Герасименко Е.А., Кондратьев А.В. Рассмотрение критериев защищенности речи на основе словесной и смысловой разборчивости. *Специальная техника*. 2016;6:22-28.
2. Шелухин О.И. *Цифровая обработка и передача речи*. Москва: Радио и связь; 2000: 456.
3. Костиков В.Г., Парфенов Е.М., Шахнов В.А. *Источники электропитания электронных средств. Схемотехника и конструирование*. Москва: Горячая линия – Телеком; 2001: 344.
4. Трушин В.А., Иванов А.В., Рева И.Л. О корректировке методики оценки защищенности речевой информации от утечки по техническим каналам. *Специальная техника*. 2016;6:22-30.
5. Бутырский Е.Ю. Преобразование гильберта и его обобщение. *Научное приборостроение*. 2014;24(4):30-37.
6. Рябенко Д.С., Лавров С.В., Боровкова Е.С. Приложение сигнальных графов и матричного анализа для математического моделирования каналов утечки информации. *Вестник Полоцкого государственного университета. Серия С. Фундаментальные науки*. 2018;4:56-60.

References

1. Anohin V.V., Gerasimenko E.A., Kondrat'ev A.V. [Consideration of speech security criteria based on verbal and semantic intelligibility.] *Special'naya tekhnika=Special equipment*. 2016;6:22-28. (In Russ.)
2. Speluhin O.I. [*Digital processing and transmission of speech*]. Moscow: Radio i svyaz'; 2000: 456. (In Russ.)
3. Kostikov V.G., Parfenov E.M., Shahnov V.A. [*Sources of power supply of electronic means. Circuit engineering and design*]. Moscow: Goryachaya liniya – Telekom; 2001: 344. (In Russ.)
4. Trushin V.A., Ivanov A.V., Reva I.L. [On the correction of the methodology for assessing the security of speech information from leakage through technical channels.] *Special'naya tekhnika=Special equipment*. 2016;6:22-30. (In Russ.)
5. Butyrskij E.Yu. [Hilbert transform and its generalization.] *Nauchnoe priborostroenie=Scientific Instrumentation*. 2014;24(4):30-37. (In Russ.)
6. Ryabenko D.S., Lavrov S.V., Borovkova E.S. [Application of signal graphs and matrix analysis for mathematical modeling of information leakage channels.] *Vestnik Polockogo gosudarstvennogo universiteta. Seriya S. Fundamental'nye nauki=Bulletin of Polotsk State University. Series C. Fundamental sciences*. 2018;4:56-60. (In Russ.)

Вклад авторов / Authors' contribution

Все авторы внесли равный вклад в написание статьи.
All authors contributed equally to the paper writing.

Сведения об авторах

Железняк В.К., д.т.н., профессор Полоцкого государственного университета.

Адамовский Е.Р., м.т.н., аспирант кафедры вычислительных систем и сетей Полоцкого государственного университета.

Филиппович А.Г., к.т.н., главный специалист Оперативно-аналитического центра при Президенте Республики Беларусь.

Адрес для корреспонденции

211440, Республика Беларусь,
г. Новополоцк, ул. Блохина, 29,
Полоцкий государственный университет;
тел. +375 33 387-46-89;
e-mail: e.adamovsky@psu.by
Адамовский Егор Русланович

Information about the authors

Zheleznyak V.K., Dr. of Sci. (Tech.), Professor of the Polotsk State University.

Adamovskiy Y.R., M. Sci. at the Department of Computing Systems and Networks of the Polotsk State University.

Filipovich A.G., Cand. of Sci., Chief Specialist at the Operational and Analytical Center under the Aegis of the President of the Republic of Belarus.

Address for correspondence

211440, Republic of Belarus,
Novopolotsk, Blokhina St., 29,
Polotsk State University;
tel. +375 33 387-46-89;
e-mail: e.adamovsky@psu.by
Adamovskiy Yahor Ruslanavich