УДК 534; 53.089

КОМПЕНСАЦИЯ ВРЕМЕННОГО ЗАПАЗДЫВАНИЯ ИЗМЕРИТЕЛЬНОГО СИГНАЛА НА ВЫХОДЕ КАНАЛА УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

И.Б. БУРАЧЕНОК, В.К. ЖЕЛЕЗНЯК

Полоцкий государственный университет
Блохина, 29, Новополоцк 211440, Беларусь

Поступила в редакцию 30 июня 2016

Предлагается методика оценки защищенности речевого сигнала в канале утечки информации в условиях шумов высокого уровня при значительных неравномерностях АЧХ сложным измерительным сигналом с большой базой в полосах равной разборчивости. Применение математического подхода по производной функции взаимной корреляции между сложным измерительным сигналом с большой базой на входе и выходе канала утечки речевой информации позволяет, установив положение точки на оси, в которой данная производная равна нулю, определить на выходе канала утечки речевой информации с минимальной среднеквадратичной погрешностью его временное запаздывание и частотной сдвиг. Компенсация с высокой точностью временного запаздывания и частотного сдвига сложного измерительного сигнала с большой базой на выходе канала утечки информации позволила значительно повысить точность и чувствительность оценки защищенности речевого сигнала в канале утечки информации.

Ключевые слова: оценка защищенности, компенсация запаздывания, речевой сигнал, канал утечки информации.

Введение

Корреляционный анализ находит широкое применение во многих областях, т.к. за счет снижения влияния некоррелированных с полезным сигналом шумов позволяет получить наиболее точные результаты [1]. В работе [2] при оценке защищенности речевого сигнала в технических каналах утечки информации (КУИ) [3] в соответствии с СТБ 34.101.29-2011 [4] предлагается использовать для выделения слабых измерительных сигналов (ИС) из шумов высокого уровня функцию взаимной корреляции (ВКФ). Использование для оценки защищенности речевых сигналов в КУИ ВКФ между измерительными сигналами на входе и выходе КУИ позволяет ослабить шумовую составляющую, и тем самым при получении максимального значения этой функции повысить точность оптимальной оценки параметров ИС при приеме в шумах высокого уровня [5]. В качестве измерительных, используют сложные ИС с большой базой с обоснованными исходными данными в полосах равной разборчивости [6]. Однако в условиях шумов высокого уровня при значительных искажениях амплитудно-частотной характеристики (АЧХ) сложного ИС с большой базой на выходе КУИ возникают трудности решения данной задачи. В определенной степени данный недостаток можно снизить путем дополнительной фильтрации сложных ИС с большой базой на выходе КУИ, что требует дополнительных затрат. Применение фильтров также связано и с дополнительными искажениями исследуемых на выходе КУИ сложных ИС с большой базой, что сильно отражается на точности оценки защищенности речевого сигнала в КУИ. Получить оптимальные параметры сложного ИС с большой базой на выходе КУИ не позволяют его случайное временное запаздывание по отношению к входному, обусловленное прохождением через среду распространения и эквивалентный временному запаздыванию частотный сдвиг. Поэтому возникает необходимость при использовании ВКФ по времени и частоте для оценки

защищенности речевого сигнала в КУИ в условиях шумов высокого уровня при значительных неравномерностях АЧХ получить с наибольшей точностью значений временного запаздывания и частотного сдвига сложного ИС на выходе КУИ и их компенсации с минимальной среднеквадратичной погрешностью. Компенсация временного запаздывания и частотного сдвига сложного ИС с большой базой на выходе КУИ с минимальной среднеквадратичной погрешностью позволят значительно повысить точность и чувствительность оценки защищенности речевого сигнала в КУИ.

Исходя из этого, целью исследования является обоснование математического подхода для определения временного запаздывания и частотного сдвига с минимальной среднеквадратичной погрешностью при использовании ВКФ между сложными ИС с большой базой на входе и выходе канала утечки речевой информации в условиях шумов высокого уровня при значительных неравномерностях АЧХ.

Методика использования функции взаимной корреляции между сложным измерительным сигналом с большой базой на входе и выходе канала утечки речевой информации для компенсации временного запаздывания и частотного сдвига

Входной $s_1(t)$ и зашумленный в КУИ шумом $n(t)$ выходной $s_2(t) = s_1(t) + n(t)$ сложные ИС с большой базой представим в виде комплексных переменных:

$$\dot{s}_1(t) = s_1(t) \cdot e^{j \cdot \psi_1(t)} \text{ и } \dot{s}_2(t) = s_2(t) \cdot e^{j \cdot \psi_2(t)}, \quad (1)$$

где $\psi(t) = \mathrm{arctg}\dfrac{\mathrm{Im}(t)}{\mathrm{Re}(t)}$ – фазовый угол между вещественной $\mathrm{Re}(t)$ и мнимой $\mathrm{Im}(t)$ составляющими сигнала; $j = \sqrt{-1}$ – мнимая единица.

Их ВКФ во временной и частотной плоскостях представим в виде пары отдельно взятых функций:

$$R_v(\tau,\Omega) = \int_{-\infty}^{+\infty} s_1(t) s_2^*(t-\tau) e^{j\Omega t} dt \text{ или } R_v(\tau,\Omega) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} F_1(\omega) F_2^*(\omega-\Omega) e^{j\omega\tau} d\omega, \quad (2)$$

где τ и Ω – соответственно временной и частотный сдвиги между исходным $s_1(t)$ и принятым на выходе КУИ $s_2(t)$ сложными ИС с большой базой; $F_1(\omega)$, $F_2^*(\omega-\Omega)$ – спектры входного и принятого на выходе КУИ сложных ИС с большой базой; * – операция комплексного сопряжения.

Сначала рассмотрим ВКФ по времени:

$$R_v(\tau,0) = \int_{-\infty}^{+\infty} s_1(t) s_2^*(t-\tau) dt. \quad (3)$$

В момент времени, когда выходной сигнал $s_2(t)$ наиболее подобен входному $s_1(t)$, ВКФ максимальна. Если $s_1(t) = s_2(t)$, то выражение (3) является выражением АКФ. В точке $\tau = 0$ (нулевом временном сдвиге) она численно равна энергии сигнала, выделяющейся на сопротивлении R=1 Ом [7]:

$$R(0) = \int_{-\infty}^{\infty} s^2(t) dt = E. \quad (4)$$

Максимум этой функции, полученный в условиях отсутствия запаздывания, определяет минимальную среднеквадратичную погрешность запаздывания сложного ИС с большой базой на выходе КУИ и его точку отсчета на временной оси. Однако при решении практических задач из-за наличия шумов получить столь очевидный максимум не всегда возможно и, следовательно, величина задержки определяется со значительной погрешностью.

Для примера сформируем сложные ИС с большой базой B = 140 в третьей N_3 полосе равной разборчивости f = [570÷710] Гц, девиацией частоты Δf = 70 Гц и длительностью T_c = 1 с: на входе КУИ с амплитудой U_1 = 0,7 В и на выходе КУИ с амплитудой U_2 = 0,5 В,

задержанный на время $t_д$ = 10 мс. Фрагменты длительностью ΔT_c = 20 мс описанных сложных ИС с большой базой отображены на рис.1.

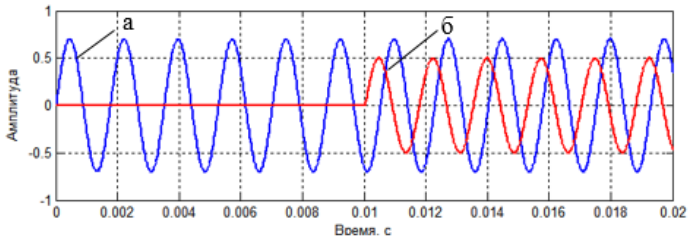

Рис. 1. Фрагменты сложных измерительных сигналов с большой базой:
а – входной $s_1(t)$ с амплитудой U_1 = 0,7 В; *б* – выходной $s_2(t)$ с амплитудой U_2 =0,5 В,
задержанный на время $t_д$ =10 мс

Мощность комплексного колебания можно определить, как сумму мгновенных мощностей действительной и мнимой частей [7]:

$$P_c(t) = \mathrm{Re}^2(t) - j \cdot \mathrm{Im}^2(t) = \dot{s}(t) \cdot \dot{s}^*(t) = s^2(t) \,. \qquad (5)$$

Максимальное значение АКФ сигнала в точке $\tau = 0$ определят энергию сигнала E, следовательно мощность сигнала можно определить также из выражения $E = P_c \cdot T_c$ как $P_c = \dfrac{E}{T_c}$.

Взаимную мощность сложных ИС с большой базой на входе и выходе КУИ определяют согласно выражения:

$$P_{12} = \frac{1}{T}\int_{t_a}^{t_b} s_1(t) \cdot s_2(t) \cdot [e^{j\cdot(\psi_1(t)-\psi_2(t))} + e^{-j\cdot(\psi_1(t)-\psi_2(t))}]dt = \frac{1}{T}\int_{t_a}^{t_b} s_1(t) \cdot s_2(t) \cdot \cos(\psi_1(t) - \psi_2(t))dt \,, \qquad (6)$$

где t_a и t_b – начальный и конечный временные отсчеты сложных ИС с большой базой на входе и выходе КУИ.

Совместное графическое представление модулей АКФ комплексных огибающих не зашумленных сложных ИС с большой базой на входе и выходе КУИ, а также их ВКФ, приведено на рис. 2.

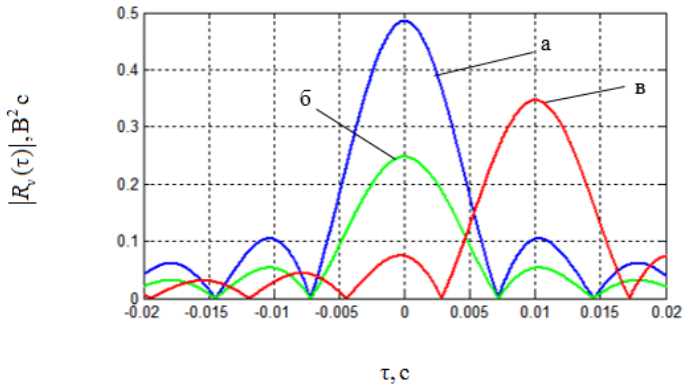

Рис. 2. Совместное отображение огибающих АКФ и ВКФ сложных измерительных сигналов с большой базой: *а* – АКФ $s_1(t)$; *б* – АКФ $s_2(t)$ с временной задержкой $t_д$ = 10 мс; *в* – ВКФ между $s_1(t)$ и $s_2(t)$

Максимум АКФ комплексной огибающей входного $s_1(t)$ сложного ИС с большой базой рис. 2, *а* соответствует его мощности $P_{U_1} = U_1^2 = 0,7^2 = 0,49\,\text{В}^2$, а максимум АКФ принятого на выходе КУИ сложного ИС с большой базой рис. 2, *б* соответствует его мощности $P_{U_2} = U_2^2 = 0,5^2 = 0,25\,\text{В}^2$. Максимальное значение построенной ВКФ $|R_v(\tau)|$ (рис. 2, *в*), представленных на рис. 1 сложных ИС с большой базой, в точке временного сдвига равно их

взаимной мощности $P_{\text{ВКФ}} \approx 0{,}37\ \text{В}^2$.

Максимальное значение времени когерентности входного и выходного сложных ИС с большой базой определяют отношением их комплексных значений ВКФ при задержке сложного ИС с большой базой на выходе КУИ относительно входного сигнала к их ВКФ при компенсации задержки [7]:

$$r(\tau) = \frac{\left|R_v(\tau,0)\right|}{R_v(0)}, \qquad (7)$$

то есть $r(\tau)$ – так называемая нормированная АКФ, или иначе, коэффициент когерентности [7]. При $r(\tau) = 1$ два сигнала полностью совпадают.

Максимум ВКФ соответствует значению искомой задержки t_0 сложного ИС с большой базой на выходе КУИ. Следует заметить, что предельно достижимая точность измерений зависит от шума, сопровождающего полезный сигнал. Однако уже сама возможность использования ВКФ при оценке защищенности речевого сигнала в КУИ позволяет максимально снизить влияние шума. Поэтому основной задачей является определение точки на временной оси, соответствующей максимальному значению ВКФ между сложным ИС с большой базой на входе и выходе КУИ с наибольшей точностью, так как даже незначительная ошибка определения времени запаздывания сказывается на точности оценки защищенности речевого сигнала в КУИ. Таким образом, опираясь на базовые сведения математического анализа, далее осуществим аналитическое исследование возможных экстремумов ВКФ. При выполнении соответствующих условий на непрерывность и гладкость функции точки экстремума $R_v(\tau,0)$ характеризуются тем, что в них производная этой функции проходит через нулевое значение [1]. Для поиска экстремумов воспользуемся построенной согласно выражению (3) ВКФ двух сложных ИС с большой базой, показанных на рис. 1. Их ВКФ и ее огибающая показаны на рис. 3.

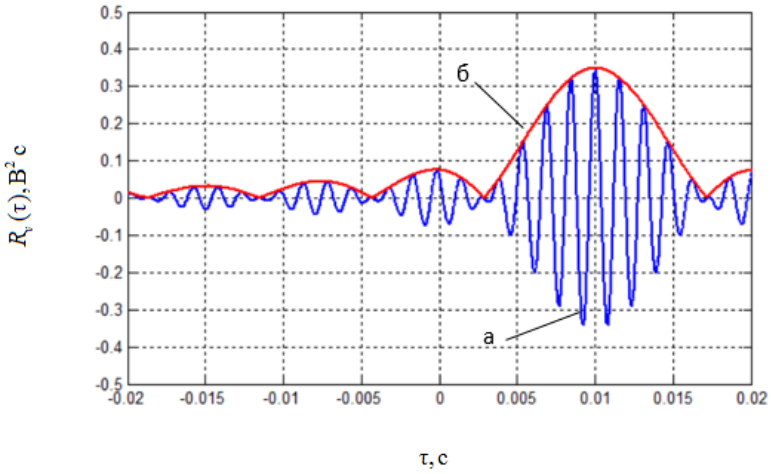

Рис. 3. Совместное отображение ВКФ и ее огибающей сложных измерительных сигналов с большой базой входного $s_1(t)$ и выходного $s_2(t)$ с временной задержкой t_0 =10 мс: *а* – ВКФ; *б* – огибающая ВКФ

Для определения экстремумов ВКФ между сложными ИС с большой базой на входе и выходе КУИ, используя математический метод [1], найдем производную данной функции и определим положение точек, в которой эта производная равна нулю:

$$\frac{\partial R_v(\tau,0)}{\partial \tau} = \int_{-\infty}^{\infty} s_1(t) \frac{\partial}{\partial \tau}\left[s_2^*(t-\tau)\right] dt, \qquad (8)$$

На рис. 4 показаны графики функций $R_v(\tau,0)$ и $\frac{\partial R_v(\tau,0)}{\partial \tau}$, демонстрирующие, что экстремумам ВКФ соответствуют нули ее производной. В точке максимального совпадения входного и выходного ИС производная от ВКФ имеет S-образную форму, пересекающую нулевой уровень [1].

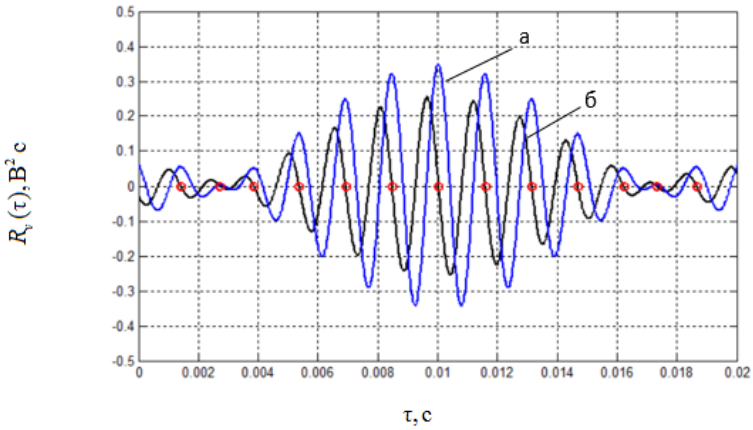

Рис. 4. Совместное отображение ВКФ и ее первой производной сложных измерительных сигналов с большой базой на входе и выходе канала утечки информации: *а* – ВКФ; *б* – первая производная от ВКФ

Результатом решения являются несколько точек экстремума. Точка экстремума, имеющая наибольшее значение позволит определить координаты временного запаздывания. Следовательно, по производной ВКФ можно определить запаздывание, установив положение точки на временной оси, в которой данная производная равна нулю. При наличии даже незначительной задержки, производная от ВКФ выражение (8) с высокой точностью устанавливает положение точки на временной оси, сдвинутое на величину задержки.

Чтобы завершить анализ ВКФ на экстремумы, необходимо определить, какие из найденных точек являются точками минимума, а какие – максимума. Тип экстремума (максимум или минимум) определяется знаком второй производной в этой точке. С этой целью следует рассчитать значения второй производной, согласно выражению:

$$\frac{\partial^2 R_v(\tau,0)}{\partial\tau^2} = \int_{-\infty}^{\infty} s_1(t)\frac{\partial^2}{\partial\tau^2}\left[s_2^*(t-\tau)\right]dt, \qquad (9)$$

и определить ее знак.

На рис. 5 показаны графики функций $R_v(\tau,0)$ и $\dfrac{\partial^2 R_v(\tau,0)}{\partial\tau^2}$.

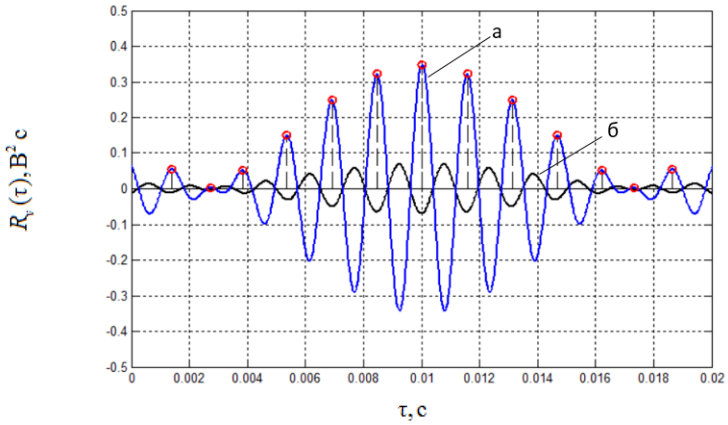

Рис. 5. Совместное отображение ВКФ и ее второй производной сложных измерительных сигналов с большой базой на входе и выходе канала утечки информации: *а* – ВКФ; *б* – вторая производная от ВКФ

Согласно выражениям (8) и (9) была осуществлена оценка величины временного запаздывания t_0 сложных ИС с большой базой в полосах равной разборчивости в условиях отсутствия шума. Оценка величины временного запаздывания t_0 и ее абсолютная λ ($\lambda = |t_0 - t_д|$) и относительная γ погрешности (отношение абсолютной погрешности измерения λ к действительному значению $t_д$) для каждой из полос равной разборчивости показали, что

чем больше значение девиации частоты $2\Delta f$ полосы равной разборчивости, тем выше точность определения временного запаздывания ИС на выходе КУИ. Величина временного запаздывания t_0 в КУИ и ее абсолютная λ и относительная γ погрешности для сложных ИС с большой базой в третьей N_3 и двадцатой N_{20} полосах равной разборчивости приведены в табл. 1.

Таблица 1. **Результаты оценки временного запаздывания сложных ИС с большой базой в третьей N_3 и двадцатой N_{20} полосах равной разборчивости с использованием первой и второй производных от ВКФ**

Номер полосы равной разборчивости, N_k	N_3	N_{20}
Величина задержки, t_0, с	0,010068	0,010023
Абсолютная погрешность оценки, λ, с	$6,8\cdot10^{-5}$	$2,27\cdot10^{-5}$
Относительная погрешность оценки, γ, %	0,68	0,23

По результатам исследований установлено, самую высокую точность оценки временного запаздывания позволяет получить сложный ИС с большой базой в двадцатой N_{20} полосе равной разборчивости. А так как величина девиации частоты $2\Delta f$ как элемент базы ограничена шириной полосы равной разборчивости [6, 9], то при постановке задачи получения результатов в реальном масштабе времени она является ограничивающим фактором и, следовательно точность оценки временного запаздывания сложного ИС с большой базой на выходе КУИ с использованием ВКФ зависит от его длительности. Чем больше длительность сложного ИС с большой базой в пределах полосы равной разборчивости, тем выше точность оценки.

Результаты экспериментов при зашумлении на выходе КУИ (различных отношениях сигнал/шум, не превышающих значение базы сложного ИС в конкретно заданной полосе равной разборчивости [8]) сложных ИС с большой базой в полосах равной разборчивости показали, что наличие шума на выходе КУИ при использовании ВКФ не влияет на погрешность оценки величины временного запаздывания t_0. При проведении экспериментов использовался шум, представленный хаотической импульсной последовательностью, обладающий высоким энтропийным коэффициентом качества и имеющий дифференциальный закон распределения вероятностей мгновенных значений амплитуды, близкий к нормальному [8].

Величина временного запаздывания t_0 в третьей N_3 и двадцатой N_{20} ПРР, оцененная по огибающей ВКФ [9], имеет в сравнении с математическим подходом при использовании производных от ВКФ большее значение абсолютной λ и относительной γ погрешностей. Результаты оценки временного запаздывания сложных измерительных сигналов с большой базой в третьей N_3 и двадцатой N_{20} полосах равной разборчивости по огибающей ВКФ представлены в табл. 2. Следует также отметить и то, что на погрешность оценки величины временной задержки по огибающей ВКФ влияет увеличение отношения сигнал/шум. Погрешность оценки уменьшается при увеличении отношения сигнал/шум.

Аналогичным образом наличие частотного сдвига определяют с использованием первой и второй производной от ВКФ по частоте сложных ИС с большой базой на входе и выходе КУИ, установив положение точки на оси частот, равное величине частотного сдвига:

$$\frac{\partial R_v(0,\Omega)}{\partial\Omega}=\int_{-\infty}^{\infty}F_1(\omega)\frac{\partial}{\partial\Omega}\left[F_2^*(\omega-\Omega)\right]d\omega \text{ и } \frac{\partial^2 R_v(0,\Omega)}{\partial\Omega^2}=\int_{-\infty}^{\infty}F_1(\omega)\frac{\partial^2}{\partial\Omega^2}\left[F_2^*(\omega-\Omega)\right]d\omega. \qquad (10)$$

Выражений (10) позволяет с наибольшей точностью определить частотный сдвиг сложного ИС с большой базой в третьей N_3 полосе равной разборчивости. Таким образом, в качестве идеального измерителя, обеспечивающего минимальную среднеквадратичную ошибку при определении временного запаздывания и частотного сдвига, предложено устройство, реагирующее на производную ВКФ сложных ИС с большой базой на входе и выходе КУИ по соответствующей координате.

Таблица 2. **Результаты оценки временного запаздывания сложных ИС с большой базой в третьей N_3 и двадцатой N_{20} полосах равной разборчивости по огибающей ВКФ**

Номер полосы равной разборчивости, N_k	N_3	N_{20}
Величина задержки, t_0, с	0,010091	0,010045
Абсолютная погрешность оценки, λ, с	$9{,}1\cdot10^{-5}$	$4{,}54\cdot10^{-5}$
Относительная погрешность оценки, γ, %	0,91	0,45

Заключение

Установлена взаимосвязь между сложными ИС с большой базой на входе и выходе КУИ в полосах равной разборчивости как во временной области, так и в области частот. Предложена методика оценки защищенности речевого сигнала в КУИ с применением ВКФ сложных ИС с большой базой на входе и выходе КУИ, позволяющая без дополнительной фильтрации принятого на выходе КУИ сложного ИС с большой базой, уменьшить помехи и исключить искажения его АЧХ. Математический подход, основанный на использовании производных ВКФ, позволил осуществить компенсацию временного запаздывания и частотного сдвига с минимальной среднеквадратичной погрешностью. Это значительно повысило чувствительность и точность оценки защищенности речевого сигнала в КУИ в сравнении с подходом, рассмотренным в работе [9] при использовании огибающей ВКФ.

COMPENSATION DELAY TIME OF MEASURING SIGNAL AT THE LEAKAGE CHANNEL OUTPOOT OF SPEECH INFORMATION

V.K. ZHELEZNYAK, I.B. BURACHONAK

Abstract

Evaluation method of security assessment a speech signal in information leakage channel under high-level noise with significant Bandpass flatness by complex measuring signal with a large base in equal intelligibility bands is proposed. Using the mathematical approach a derivative of cross-correlation function between complex measuring signal with a large base at the inlet and outlet channel speech information leakage allows to determine the position of the axis points in which derivative is zero. After that its time delay and frequency shift at the output of leakage channel of speech information within a minimum mean square error are determined. Compensation with time delay high accuracy and frequency shift complex measuring signal with a large base at the output of information leakage channel allowed to significantly improving the accuracy and sensitivity of the assessment of protection a speech signal in information leakage channel.

Keywords: security assessment, delay compensation, speech signal, information leakage channel.

Список литературы

1. *Батон Д.* Справочник по радиолокационным измерениям. М., 1976.
2. *Железняк В.К.* Защита информации от утечки по техническим каналам: учеб. пособие. СПб., 2006.
3. *Бураченок И.Б., Железняк В.К., Раханов К.Я.* // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2014. № 12. С. 2–12.
4. СТБ 34.101.29-2011 «Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования».
5. *Бураченок И.Б., Железняк В.К., Раханов К.Я.* // Вестн. ПГУ. Сер. С. Фундаментальные науки. №12. 2015. С. 22–27.
6. *Бураченок И.Б., Железняк В.К.* // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2015. № 4. С. 2–13.
7. *Денисенко А.Н.* Статистическая теория радиотехнических систем. М., 2007.
8. *Бураченок И.Б., Железняк В.К.* // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2015. № 12. С. 10–14.
9. *Бураченок И.Б., Железняк В.К.* // Докл. БГУИР. 2016. № 5. С. 60–66.