

УДК 621.391.16; 534

## ОЦЕНКА С ВЫСОКОЙ ТОЧНОСТЬЮ ПАРАМЕТРОВ ИЗМЕРИТЕЛЬНОГО СИГНАЛА КОМПЕНСАЦИЕЙ ЕГО ВРЕМЕННОЙ ЗАДЕРЖКИ В КАНАЛАХ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

В.К. ЖЕЛЕЗНЯК, И.Б. БУРАЧЕНОК

Полоцкий государственный университет  
Блохина, 29, г. Новополоцк 211440, Беларусь

Поступила в редакцию 2 июня 2016

Предложено оценку защищенности речевого сигнала в канале утечки информации проводить взаимокорреляционной частотно-временной обработкой сложного измерительного сигнала с большой базой в пределах полос равной разборчивости. Для снижения порога обнаружения представленный в аналитическом виде преобразованием Гильберта сложный измерительный сигнал с большой базой обрабатывают последовательным  $n$ -кратным синхронным накоплением спектральных составляющих с применением прямого и обратного быстрого преобразования Фурье. Высокая точность и чувствительность оценки параметров сложного измерительного сигнала с большой базой в канале утечки информации на фоне шумов высокого уровня достигнута за счет компенсации с минимальной среднеквадратичной погрешностью его временного запаздывания и частотного сдвига.

*Ключевые слова:* защищенность, речевой сигнал, канал утечки информации, взаимокорреляционная частотно-временная обработка.

### Введение

Методы оценки защищенности речевого сигнала в каналах утечки информации (КУИ) гармоническим измерительным сигналом (ИС), включенным в СТБ 34.101.29-2011 [1], и широкополосным ИС линейной частотной модуляции (ЛЧМ) с предварительной обработкой Вигнера [2], обладают рядом преимуществ, необходимых для получения высокой точности при допустимом времени обработки. Использование гармонического ИС на средних частотах в  $k$ -полосах равной разборчивости допускает увеличение погрешности при оценке защищенности речевого сигнала в КУИ в широком от 100 Гц до 10 кГц диапазоне частот с явно выраженными неравномерностями амплитудно-частотной характеристики (АЧХ). При использовании метода широкополосного ЛЧМ ИС с предварительной обработкой Вигнера при оценке защищенности речевого сигнала в КУИ в условиях значительной неравномерности АЧХ получена высокая чувствительность [3], однако при некоторых методических преимуществах перед методом гармонического ИС, данный метод уступает по времени обработки [4]. Системный анализ и синтез сложных ИС с большой базой  $B \gg 1$  [5] в  $k$ -полосах равной разборчивости позволил выявить наиболее значимые их свойства и обосновать выбор их оптимальных исходных данных [6]. Математическая зависимость, устанавливающая однозначную связь метода оценки защищенности речевого сигнала сложным ИС с большой базой с методом гармонического ИС, показала преимущество первого метода перед вторым, определяемое величиной базы  $B$  сложного ИС, равной произведению длительности сигнала  $T_c$  на удвоенную девиацию частоты  $2\Delta f$  в пределах полосы равной разборчивости  $N_k$ , где  $k=1, \dots, 20$  порядковый номер полосы [7]. Таким образом, с учетом последних достижений в использовании систем измерительных автоматизированных (СИА),

обеспечивающих повышение точности и оперативности представления результатов обработки данных, возникла необходимость в разработке нового метода оценки защищенности речевого сигнала в КУИ с использованием сложных ИС с большой базой в  $k$ -полосах равной разборчивости, позволяющего повысить чувствительность, точность, разрешение по времени и частоте с учетом неравномерностей АЧХ при значительном повышении оперативности представления результатов.

### Постановка задачи

Целью работы является оценка защищенности речевого сигнала в КУИ взаимокорреляционной частотно-временной обработкой, представленного преобразованием Гильберта в аналитическом виде сложного ИС с большой базой в шуме высокого уровня при компенсации с минимальной среднеквадратичной погрешностью его временного запаздывания и частотного сдвига, и получение максимального отношения мощности сигнала к мощности шума на выходе КУИ при допустимом времени обработки.

Важной задачей при оценке защищенности речевой информации является получение на выходе канала утечки (КУИ) параметров измерительного сигнала (ИС) с минимальной среднеквадратичной погрешностью. Следует заметить, что даже небольшое случайное запаздывание длительностью 10–200 мс, обусловленное прохождением ИС через среду распространения, значительно увеличивает погрешность оценки выходных параметров. Для примера, на рис. 1 показаны временные фрагменты (длительность  $\Delta T_c = 0,05$  с) сложного ИС с большой базой ( $B=140$ ) в третьей  $N_3$  полосе равной разборчивости  $f = [570 \div 710]$  Гц и девиацией частоты  $\Delta f = 70$  Гц продолжительностью  $T_c = 1$  с на входе и на выходе КУИ, задержанного на время  $t_0 = 0,02$  с.

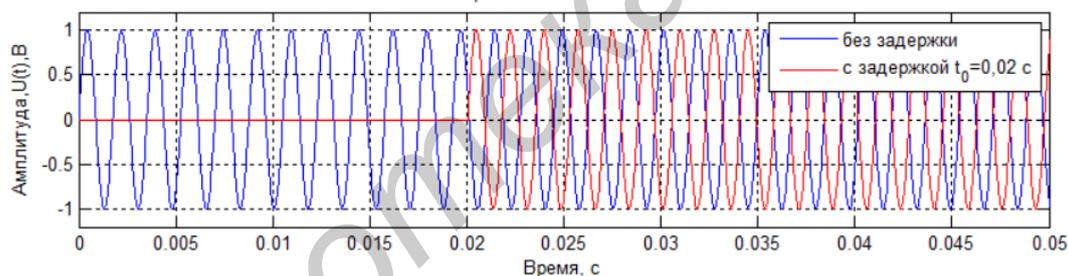


Рис. 1. Фрагменты длительностью  $\Delta T_c = 0,05$  с сложного ИС с большой базой в третьей  $N_3$  полосе равной разборчивости на входе и выходе КУИ

При прохождении сигнала через преграду имеют место и задержки по частоте, т.к. некоторый временной сдвиг эквивалентен частному фазовому сдвигу:  $s(t - \tau) \Leftrightarrow F(f) \cdot e^{-2\pi \cdot j \cdot f \cdot \tau}$ , а частотный сдвиг эквивалентен временному фазовому сдвигу:  $F(f - \phi) \Leftrightarrow s(t) \cdot e^{+2\pi \cdot j \cdot \phi \cdot t}$ . На рис. 2 отображено спектральное представление сложного ИС с большой базой, приведенного на рис. 1.

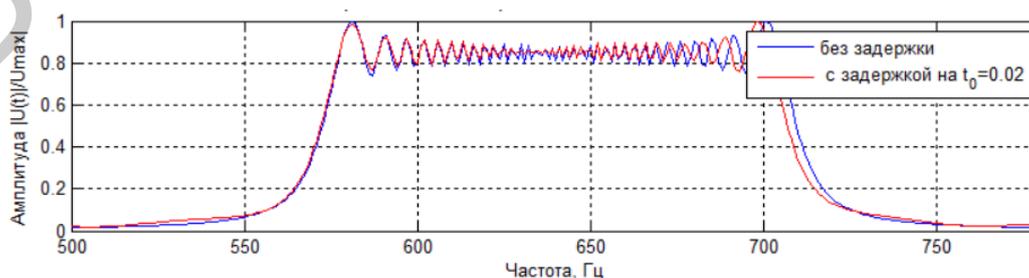


Рис. 2. Спектральное представление сложного ИС с большой базой в третьей  $N_3$  полосе равной разборчивости на входе и выходе КУИ

Как видно из рис. 2, даже при незначительной задержке (например,  $t_0 = 0,02$  с) входного сложного ИС с большой базой амплитудой  $U_0 = 1$  В наблюдаются значительные искажения его АЧХ на выходе КУИ. На рис. 3 показаны характеристики изменения отношения амплитуд сложного ИС с большой базой на выходе и входе КУИ  $\frac{|U_{\text{вых}}(t)|}{|U_{\text{вх}}(t)|}$ , при временном запаздывании  $t_0 = 0,01$  с и  $t_0 = 0,1$  с.

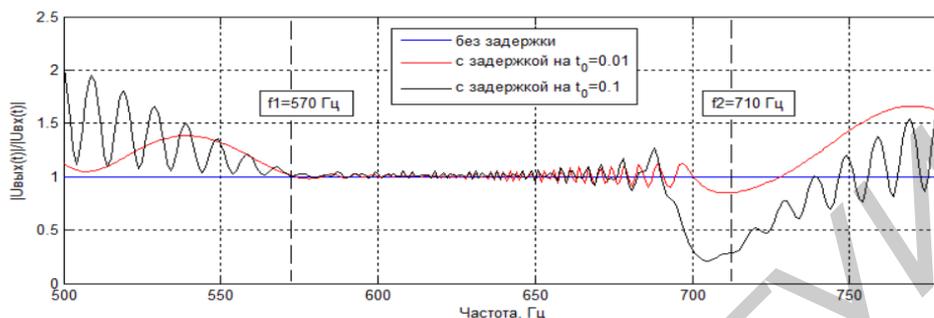


Рис. 3. Осцилляция при заданных значениях задержки сложных ИС с большой базой в третьей  $N_3$  полосе равной разборчивости

Для оценки искажений, связанных с задержкой входного и принятого на выходе КУИ сложного ИС с большой базой, возьмем соотношение размаха вариации (разницы между максимальным и минимальным значением) к среднему значению [8]:

$$K_v = \frac{\left(\frac{U_{\text{вых}}(t)}{U_{\text{вх}}(t)}\right)_{\max} - \left(\frac{U_{\text{вых}}(t)}{U_{\text{вх}}(t)}\right)_{\min}}{\left(\frac{U_{\text{вых}}(t)}{U_{\text{вх}}(t)}\right)_{\text{ср}}}, \quad (1)$$

где  $\left(\frac{U_{\text{вых}}(t)}{U_{\text{вх}}(t)}\right)_{\max}$ ,  $\left(\frac{U_{\text{вых}}(t)}{U_{\text{вх}}(t)}\right)_{\min}$ ,  $\left(\frac{U_{\text{вых}}(t)}{U_{\text{вх}}(t)}\right)_{\text{ср}}$  — соответственно максимальное, минимальное и среднее значения отношений амплитуд  $U_{\text{вых}}(t)$  выходного и входного  $U_{\text{вх}}(t)$  сигналов.

Степень размаха вариации относительно средней называют коэффициентом осцилляции. Рассмотрим, как изменится коэффициент осцилляции при различных заданных значениях временной задержки на выходе КУИ сложных ИС с большой базой. Изменение коэффициента осцилляции  $K_v$  сложного ИС с большой базой в третьей  $N_3$  полосе равной разборчивости при различных значениях его временной задержки  $t_0$  в КУИ представлено на рис. 4.

Полученные значения показывают, что при увеличении временного запаздывания  $t_0$  коэффициент осцилляции  $K_v$  увеличивается и это не позволяет получить оптимальные параметры сложного ИС с большой базой на выходе КУИ. Таким образом возникает необходимость компенсации с минимальной среднеквадратичной погрешностью случайного временного запаздывания выходного сложного ИС по отношению к входному, обусловленное прохождением через среду распространения.

### Компенсация временного запаздывания измерительного сигнала на выходе канала утечки речевой информации

Предлагаемая методика оценки базируется на методах корреляционного анализа исходного сложного ИС с большой базой и сигнала на выходе КУИ с учетом различий между помехой и полезным сигналом. Оценку защищенности речевого сигнала в КУИ осуществим на основании полученного значения энергетического коэффициента, определяемого отношением энергии сигнала  $E$  к спектральной мощности шума  $N_0$  [7].

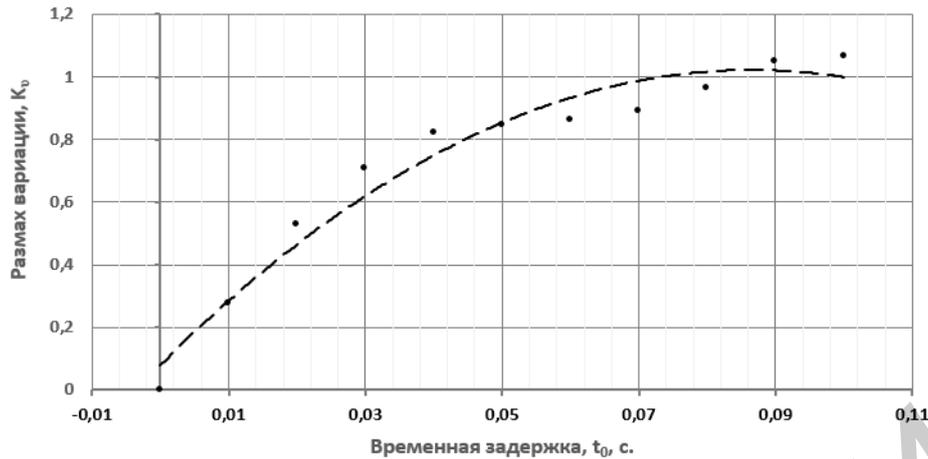


Рис. 4. Изменение коэффициента осцилляции при различных значениях задержки в КУИ сложного ИС с большой базой в третьей  $N_3$  полосе равной разборчивости

Использование для оценки защищенности речевых сигналов в КУИ функции взаимной корреляции (ВКФ) по времени  $R_{1,2}(\tau)$  сложного ИС с большой базой, не зашумленного входного  $s_1(t)$  и зашумленного в КУИ шумом  $n(t)$  выходного  $s_2(t)$ :

$$R_{1,2}(\tau) = \int_{-\infty}^{\infty} s_1(t) s_2(t - \tau) dt, \quad (2)$$

где  $\tau$  – сдвиг по времени между входным  $s_1(t)$  и выходным  $s_2(t) = s_1(t) + n(t)$  сигналами, позволяет с помощью процесса корреляции ослабить шумовую составляющую и тем самым при получении максимального значения этой функции в момент времени, когда выходной сигнал  $s_2(t)$  наиболее подобен входному  $s_1(t)$ , повысить точность оптимальной оценки параметров ИС при приеме в шумах высокого уровня [9].

При условии  $s(t) = s_1(t) = s_2(t)$  выражение (2) является выражением автокорреляционной функции (АКФ) сигнала. Таким образом, АКФ можно рассматривать как частный случай ВКФ при одном и том же сигнале [5]. Так как ВКФ не обязательно симметрична и ее максимум может оказаться не в точке  $\tau = 0$ , то случайное запаздывание можно определить как разность точек, соответствующую времени максимума ВКФ между ИС на выходе и входе КУИ, и максимума АКФ исходного ИС [5].

Если  $s_1(t) \leftrightarrow F_1(\omega)$  и  $s_2(t) \leftrightarrow F_2(\omega)$ , то корреляционную обработку сигналов можно осуществить и в частотной области [10]:

$$R_{1,2}(\Omega) = \int_{-\infty}^{\infty} F_1(\omega) F_2(\omega - \Omega) d\omega, \quad (3)$$

где  $R_{1,2}(\Omega)$  – ВКФ двух сигналов  $s_1(t)$  и  $s_2(t)$  по частоте;  $F_1(\omega)$ ,  $F_2(\omega - \Omega)$  – спектры исходного и принятого сигналов;  $\Omega$  – частотная переменная сдвига по частоте между  $F_1(\omega)$  и  $F_2(\omega)$ . Функция частотной корреляции имеет свойства, аналогичные свойствам ВКФ по времени  $|R_{1,2}(\Omega)| \leq |R_{1,2}(0)|$ , она максимальна при нулевом частотном сдвиге  $\Omega = 0$ .

Временная форма сигнала и его частотное представление позволяют проводить корреляционную оценку одновременно по времени и по частоте, так как оба представления взаимосвязаны и модификация одного из них приводит к изменению другого.

Используя преобразование Гильберта на основании ВКФ по времени (2) и по частоте (3), обобщенную корреляционную функцию комплексных огибающих двух сигналов можно представить во временной и спектральной плоскостях, в виде пары отдельно взятых функций:

$$R_{1,2}(\tau, \Omega) = \int_0^{T_c} \dot{s}_1(t) \dot{s}_2^*(t - \tau) e^{i\Omega\tau} dt \quad \text{или} \quad R_{1,2}(\tau, \Omega) = \frac{1}{2\pi} \int_{\omega_n}^{\omega_b} F_1(\omega - \Omega) F_2^*(\omega) e^{i\Omega\tau} d\omega, \quad (4)$$

где  $\omega_n$ ,  $\omega_b$  – нижняя и верхняя границы частоты заданной полосы сложного ИС с большой базой;  $i$  – мнимая единица; множитель  $e^{i\Omega\tau}$  является быстро меняющейся функцией  $\tau$ , его быстрые флюктуации отражают тонкую структуру сигнала, зависящую от несущей частоты; (\*) – операция комплексного сопряжения. Следует заметить, что использование для оценки защищенности речевого сигнала в КУИ ВКФ комплексно-сопряженных входного и выходного сложных ИС с большой базой позволяет получить дополнительный выигрыш в ОСШ на выходе КУИ на 6 дБ [6].

Исходя из того, что при оценке защищенности речевого сигнала в КУИ необходимо получить наиболее точный результат при наличии шума, то определим возможную точность оценки при использовании ВКФ комплексно-сопряженных входного и выходного сложных ИС с большой базой. Согласно [11], минимальная среднеквадратичная погрешность при оценке временного запаздывания при использовании ВКФ равна

$$\sigma_t = \frac{1}{\beta \sqrt{q_{\text{вых}}^2}}, \quad (5)$$

где  $q_{\text{вых}}^2 = \frac{2E}{N_0}$  – множитель, характеризующий отношение максимальной удвоенной энергии  $E$

сложного ИС с большой базой к спектральной плотности шума  $N_0$  (мощности шума, приходящейся на единицу полосы пропускания) на выходе КУИ, а параметр  $\beta$  определяется из выражения

$$\beta^2 = \frac{\int_{-\infty}^{+\infty} \left| \frac{\partial}{\partial t} a(t) \right|^2 dt \int_{-\infty}^{+\infty} (2\pi f^2) |A(f)|^2 df}{\int_{-\infty}^{+\infty} |a(t)|^2 dt \int_{-\infty}^{+\infty} |A(f)|^2 df}, \quad (6)$$

где функции  $A(f)$  и  $a(t)$  представляют собой пару преобразований Фурье, описывающих сигнал. Следует отметить, что параметр  $\beta$  является нормированным вторым моментом энергетического спектра сигнала, используемым в качестве меры ширины частотного спектра.

Выражение (5) применимо для определения среднеквадратичной погрешности временного запаздывания как в случае измерения запаздывания по одиночному импульсу, так и к случаю измерения по нескольким импульсам [11], при условии, что все импульсы имеют одинаковый спектр, приближенный к прямоугольному. В нашем случае для оценки защищенности речевого сигнала в КУИ используются сложные ИС с большой базой форма спектральной плотности которых близка к прямоугольной, а ее ширина близка к величине  $2\Delta f$  [6].

Наибольшая точность оценки величины запаздывания, которую можно получить при использовании ограниченного по полосе прямоугольного импульса, была определена Сколником [11], который показал, что при базе сигнала  $B \gg 1$  среднеквадратичное значение ширины полосы  $\beta_a$  можно с большой степенью точности аппроксимировать выражением

$$\beta_a \approx \sqrt{\frac{2\Delta f}{T_c}}. \quad (7)$$

Используя выражение (7), можно получить соотношения для предельной погрешности (минимальной теоретической ошибки) оценки временного запаздывания с использованием ВКФ при ограниченном спектре прямоугольного импульса [11]:

$$\sigma_t \approx \sqrt{\frac{T_c}{2\Delta f q_{\text{вых}}^2}}. \quad (8)$$

Таким образом, согласно (8) можно построить зависимости точности измерений для прямоугольных импульсов заданной длительности. На рис. 5. приведены кривые точности

оценки  $\frac{\sigma_t}{T_c}$  для прямоугольных импульсов длительностью  $T_c = 1$  с и  $T_c = 4$  с в зависимости от ширины частотного спектра.

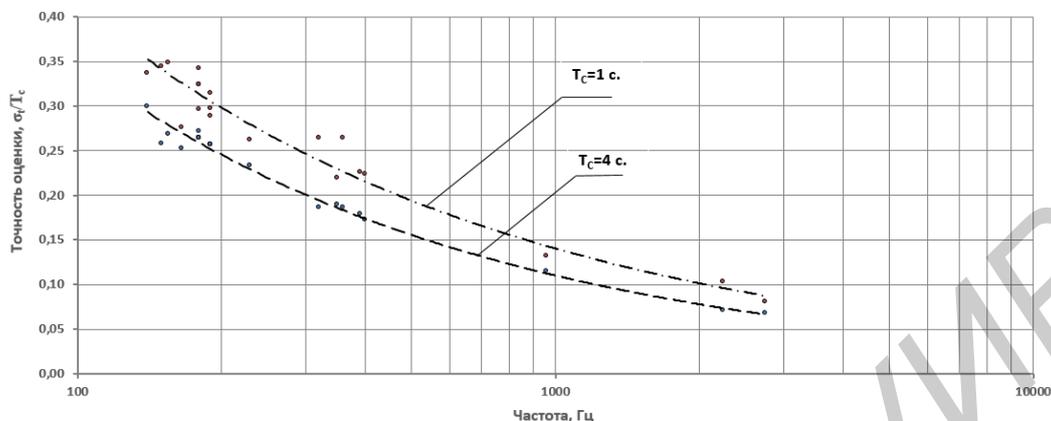


Рис. 5. Зависимость точности оценки от ширины частотного спектра полос равной разборчивости

Поскольку величина девиации частоты  $2\Delta f$  как элемент базы ограничена шириной каждой  $k$ -полосы равной разборчивости [12], то при постановке задачи получения результатов в реальном режиме времени она является ограничивающим фактором. На основании полученных графиков рис. 5 точность оценки временного запаздывания сложного ИС с большой базой с использованием ВКФ для каждой  $k$ -й полосы равной разборчивости определяется в зависимости от его длительности. Чем больше длительность сложного ИС с большой базой, тем выше точность оценки. Самую высокую точность оценки позволяет получить сложный ИС с большой базой в двадцатой  $N_{20}$  полосе равной разборчивости.

### Заключение

Одновременное формирование временных и частотных функций авто- и взаимной корреляции сложного ИС с большой базой на входе и выходе КУИ на основании их аналитического представления преобразованием Гильберта позволило компенсировать с минимальной среднеквадратичной погрешностью временное запаздывание и частотный сдвиг между исходными и принятыми сигналами. Это повысило точность оптимальной оценки параметров ИС при приеме на фоне шумов высокого уровня, исключив погрешности, связанные с его запаздыванием в КУИ и дополнительно увеличило значение ОСШ на выходе КУИ, что позволило получить значение максимального отношения мощности сигнала к мощности шума на выходе КУИ с точностью не более одного периода дискретизации при уменьшении времени обработки.

## ASSESSMENT WITH HIGH PRECISION OF MEASUREMENT SIGNAL PARAMETERS USING COMPENSATION OF ITS TIME DELAY IN LEAKAGE CHANNELS OF SPEECH INFORMATION

V.K. ZHELEZNYAK, I.B. BURACHONAK

### Abstract

This paper proposes to make an assessment of speech signal protection in information leakage channel by frequency-time processing of complex measurement signal with a large base within a band equal intelligibility using Hilbert transform to represent it in an analytical form and preliminary reduction of the detection threshold n-multiples sequential synchronous accumulation

of spectral components using direct and inverse fast Fourier transform. High accuracy and sensitivity assessment of the parameters of a complex measurement signal with a large base in information leakage channel on background high level of noise achieved by compensating with a minimum mean square error its time delay and frequency offset.

*Keywords:* protection of the speech signal, information leakage channel, interrelation time-frequency processing, complex measurement signal.

### Список литературы

1. СТБ 34.101.29-2011 «Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования».
2. Раханов К.Я., Железняк В.К. Методы оценки защищенности речевой информации. // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2011. № 12. С. 2–8.
3. Раханов К.Я., Железняк В.К. // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2011. № 12. С. 35–41.
4. Бураченко И.Б., Железняк В.К., Раханов К.Я. // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2014. № 12. С. 2–12.
5. Варакин Л.Е. Теория сложных сигналов. М., 1970.
6. Бураченко И.Б., Железняк В.К. // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2015. № 4. С. 2–13.
7. Бураченко И.Б., Железняк В.К. // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2015. №12. С. 2–7.
8. Рябушкин, Т.В., Ефимова М.Р., Ипатова И.М. и др. Общая теория статистики: Учебник. М., 1981.
9. Бураченко И.Б., Железняк В.К., Раханов К.Я. // Вестн. ПГУ. Сер. С. Фундаментальные науки. 2015. № 12. С. 22–27.
10. Денисенко А.Н. Статистическая теория радиотехнических систем. М., 2007.
11. Батон Д., Вард Г. Справочник по радиолокационным измерениям. / Под ред. М.М. Вейсбейна. М., 1976.
12. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие. СПб., 2006.