

УДК 534.6: 621.391

АНАЛИЗ ИЗМЕРИТЕЛЬНЫХ СИГНАЛОВ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ В ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ**д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, И.Б. БУРАЧЁНОК**
(Полоцкий государственный университет)

Осуществлен анализ и синтез измерительных сигналов, используемых для оценки защищенности речевой информации в технических каналах утечки в условиях шумов высокого уровня при значительных неравномерностях их амплитудно-частотных характеристик. Выявлены и исследованы наиболее значимые свойства гармонических и сложных измерительных сигналов в полосах равной разборчивости. Исследованы искажения формы автокорреляционных функций, принятых в условиях шумов сложных измерительных сигналов. Предложено использовать сложные измерительные сигналы с регулируемым уровнем эффективной длительности. Наибольшая точность оценки защищенности получена при использовании сложных измерительных сигналов, формируемых при заданном значении уровня эффективной длительности $a = 0,8$ с фиксированной длительностью $T_c = 4$ с в каждой полосе равной разборчивости.

Ключевые слова: измерительные сигналы, технические каналы утечки информации, обработка измерительных сигналов.

Введение. Наиболее распространенным способом обмена информацией между людьми является человеческая речь. Во все времена люди самую важную информацию передавали устно и всегда существовали те, кто пытался ее перехватить (подслушать). Сегодня, учитывая особенности расположения большинства офисов коммерческих предприятий и фирм, размещаемых в помещениях жилых домов с недостаточной акустической защищенностью, задача защиты конфиденциальных переговоров является достаточно дорогим и сложным мероприятием, а совершенствование средств извлечения речевой информации (РИ) и новые методы ее обработки в шумах высокого уровня определяют необходимость улучшения важнейших параметров ее защиты. Защита РИ в подобных помещениях зависит как от ее акустической защищенности по воздушной и структурной (вибрационной) акустической волне, так и от защищенности расположенных в помещении устройств и их элементов от утечки за счет акустопреобразовательного эффекта, побочных электромагнитных излучений и наводок. Отсутствие в соответствующих службах аппаратуры контроля, удовлетворяющей современным требованиям, обуславливает появление технических каналов утечки информации (КУИ) при кажущемся достаточным уровне защиты. Поэтому необходимость усовершенствования средств противодействия перехвату (аппаратуры контроля и защищенности РИ по техническим КУИ), обеспечивающих повышение точности, помехоустойчивости и чувствительности при оценке защищенности РИ в технических КУИ в условиях шумов высокого уровня при значительных неравномерностях амплитудно-частотной характеристики (АЧХ) и приемлемом времени обработки, определяют актуальность представленных исследований.

Целью работы является анализ и синтез измерительных сигналов (ИС), используемых для оценки защищенности РИ в КУИ в условиях шумов высокого уровня при значительных неравномерностях АЧХ для выявления наиболее значимых их свойств, позволяющих получить численные значения параметров оценки защищенности с высокой точностью и разрешающей способностью по частоте и времени при повышении оперативности представления результатов.

Защищенность РИ в КУИ объективно оценивают выделением слабых ИС из шумов высокого уровня с учетом неравномерности АЧХ. Оценку осуществляют на основании измерений отношения мощности акустического сигнала к мощности маскирующего (фоновому) шума (отношение сигнал/шум) в точке приема на выходе КУИ за пределами помещения, предназначенного для конфиденциальных переговоров, и затем определяют коэффициент разборчивости речи [1]. Нормативные значения данного параметра приведены в соответствующих документах. Защита РИ в КУИ считается достаточной, если в местах возможной установки акустических и вибрационных первичных измерительных преобразователей величина показателя измеренного отношения сигнал/шум не превышает его нормативного значения. Основными параметрами и характеристиками при расчете разборчивости речи являются уровни спектральной плотности речевого сигнала и спектральной плотности фонового шума в речевом диапазоне частот, дБ. Для того чтобы учесть основные факторы, влияющие на величину разборчивости речи, отношение сигнал/шум определяется на нескольких несовпадающих частотах (средних частотах третьоктавных полос или в полосах равной разборчивости (ПРР) спектра речевого сигнала (РС). При контроле качества защищенности РИ в КУИ используют ИС: либо белый шум [2], либо гармонический сигнал по ГОСТ 16465–70 [3] в полосе РС. В работе [4] оценку защищенности РИ в КУИ предложено проводить с применением сложных ИС (иногда их называют широкополосными либо шумоподобными [5]) с обоснованными исходными данными в ПРР спектра РС [2] при использовании функций корреляции [5].

Математические модели измерительных сигналов, используемых для оценки защищенности речевой информации в каналах утечки информации.

Чтобы сигналы являлись объектами теоретического изучения и анализа, необходимо иметь их математические модели, отражающие с достаточной полнотой их основные свойства. Поэтому для анализа свойств сравниваемых ИС далее построим их математические модели.

Шумовой измерительный сигнал. Шумовой сигнал, использующийся для оценки защищенности РИ в КУИ, – это случайный процесс, характеризуемый нормальным законом распределения плотности вероятности [6]:

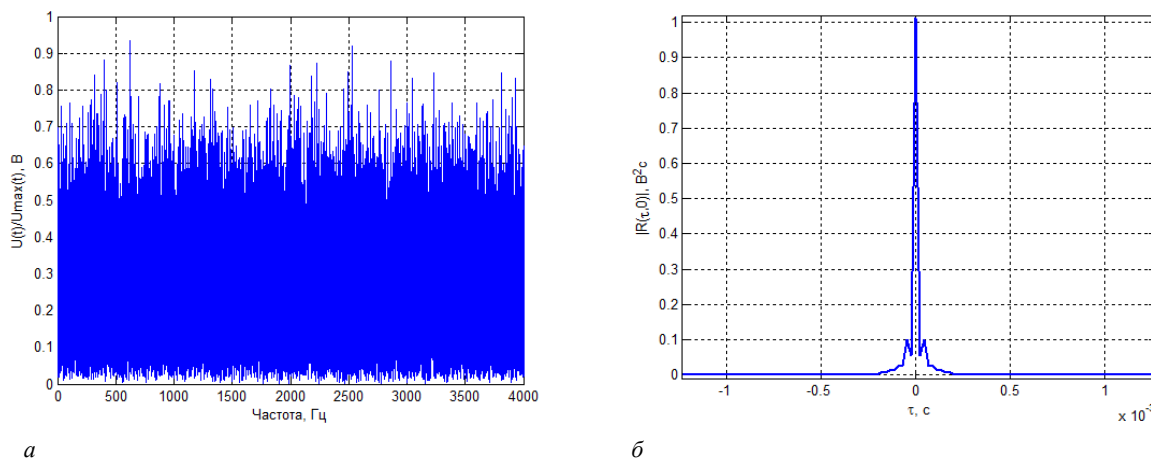
$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\bar{x})^2}{2\sigma^2}}, \tag{1}$$

где σ – среднеквадратическое отклонение (σ^2 – дисперсия) шумового сигнала;

x – вектор выборочных значений;

\bar{x} – математическое ожидание (среднее арифметическое) распределения.

Основными параметрами такого сигнала являются математическое ожидание, дисперсия и автокорреляционная функция (АКФ). Пример шумового ИС показан на рисунке 1. На рисунке 1, *a* отображено его спектральное представление, а на рисунке 1, *б* – АКФ. Особенностью шумового ИС является его АКФ, которая имеет высокий пик (представимый как дельта-функция Дирака [6]) в нуле и равна нулю во всех других точках.



a – спектральное представление; *б* – автокорреляционная функция

Рисунок 1. – Характеристики шумового измерительного сигнала

При измерении уровней шумовых акустических сигналов используют шумомер, который вносит значительные методические погрешности в результаты измерения, так как пропускает помехи, вызванные реверберацией помещения и искусственные, используемые для маскирования речевой информации, в результате чего происходит ухудшение помехоустойчивости обработки, что значительно снижает точность оценки защищенности РИ, поэтому шумовой ИС далее мы не рассматриваем.

Гармонический измерительный сигнал. Уравнение синусоидального сигнала, ограниченного по времени, запишем:

$$\left. \begin{aligned} s(t) &= A_0 \sin(\omega \cdot t + \varphi_0) \text{ для всех } 0 < t < T_c \\ s(t) &= 0 \text{ для всех } t < 0 \text{ и } t > T_c \end{aligned} \right\}, \tag{2}$$

где A_0 – амплитуда;

t – временные отсчеты;

ω – круговая частота, $\omega = 2\pi / T_c = 2\pi f_0$;

T_c – длительность;

φ_0 – начальная фаза;

f_0 – несущая частота.

Гармоническому ИС, в отличие от шумового, не присущи выше перечисленные факторы, снижающие точность оценки защищенности РИ в КУИ, однако обработка гармонического сигнала на сред-

них частотах ПРР допускает увеличение погрешности в КУИ с явно выраженными неравномерностями АЧХ, например, в условиях искусственного зашумления, использующегося при маскировании (защите) полезного речевого сигнала. На точность оценки существенное влияние оказывает также и длительность ИС. Спектральная плотность гармонического сигнала представляет собой одну спектральную линию и не позволяет учесть различные искажения ИС, возникающие при его прохождении через преграду. Что касается АКФ, то следует заметить некоторые ее особенности. Автокорреляционная функция периодического процесса сама является периодической функцией, однако она не содержит сведений о фазовых углах гармоник и воспроизводится в измененном масштабе времени. Она является четной, ее максимум приходится на начало отсчета времени и имеет положительное значение. Значение АКФ убывает с ростом временной задержки. Автокорреляционная функция и спектр мощности связаны преобразованием Фурье. Синусоидальная функция времени имеет АКФ, представленную косинусоидой той же частоты.

Дальнейший анализ проведем в сравнении гармонического и сложных ИС, предлагаемых для оценки защищенности РИ в КУИ в ПРР.

Сложный измерительный сигнал. Для оценки сложный ИС описывается математической моделью [4]:

$$s_{\text{сис}}(t) = \begin{cases} 0, & t < -\frac{T_c}{2}, \\ A_m \sin \left[(\omega_0 t + \frac{\mu}{2} t^2) + \varphi_0 \right], & -\frac{T_c}{2} < t < \frac{T_c}{2}, \\ 0, & t > \frac{T_c}{2}. \end{cases} \quad (3)$$

где A_m – амплитуда;

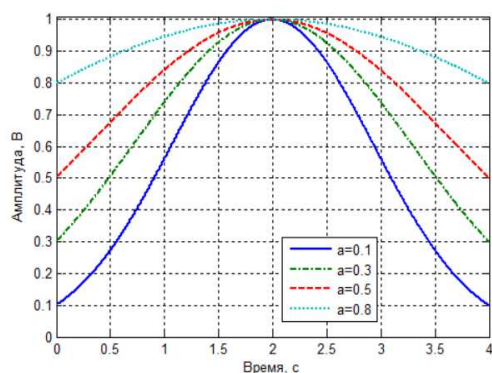
μ – скорость изменения мгновенной частоты во времени;

ω_0 – центральное значение частоты;

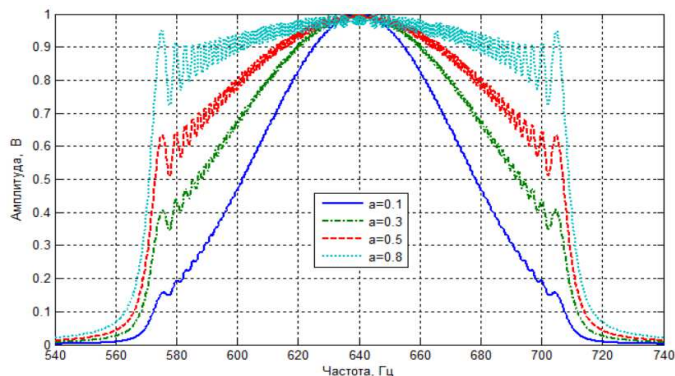
φ_0 – начальная фаза (в нашем случае $\varphi_0 = 0$).

Для формирования модели сложного ИС с регулируемым уровнем эффективной длительности используем функцию вида $f(t) = e^{-(\beta t)^2}$, представляющую собой гауссов импульс, совпадающий по форме с графиком нормального распределения вероятностей, где $\beta = \frac{1}{T_c} \cdot 2 \cdot \sqrt{-\ln(a)}$ – коэффициент наклона,

а $t \in \left[-\frac{T_c}{2}; \frac{T_c}{2} \right]$, a – коэффициент задаваемого уровня эффективной длительности. На рисунке 2 приведены характеристики сложных ИС длительностью $T_c = 4$ с, используемых для оценки защищенности РИ в КУИ: огибающие с различными значениями уровня эффективной длительности a (рисунок 2, а) и модули спектральных плотностей (рисунок 2, б) на примере сложных ИС в третьей N_3 ПРР.



а



б

а – форма огибающих; б – спектральное представление в третьей N_3 полосе равной разборчивости

Рисунок 2. – Характеристики сложных измерительных сигналов длительностью $T_c = 4$ с с различными значениями уровня эффективной длительности a

Особенностью такого сигнала является то, что его форма совпадает с формой спектральной характеристики.

Используемые для оценки РИ в КУИ сложные ИС в ПРР относят к сигналам с большой относительной полосой η , определяемой по следующей формуле [6]:

$$\eta = \frac{(f_B - f_H)}{(f_B + f_H)}, \quad (4)$$

где f_B, f_H – верхняя и нижняя границы частот полос равной разборчивости.

Обозначим ПРР N_k , где k – порядковый номер полосы, $k = 1, \dots, 20$. Величина η для каждой ПРР представлена в таблице 1.

Таблица 1. – Значения величины η относительных полос сложных ИС в двадцати ПРР

N_k	1	2	3	4	5	6	7	8	9	10
η	0,62	0,15	0,11	0,1	0,09	0,08	0,07	0,05	0,05	0,05

Окончание таблицы 1

N_k	11	12	13	14	15	16	17	18	19	20
η	0,04	0,04	0,05	0,06	0,06	0,05	0,05	0,11	0,18	0,16

Из таблицы следует, что относительные полосы всех исследуемых сложных ИС в ПРР изменяются в пределах $\eta \approx 0,16, \dots, 0,62$. Самое высокое значение относительной полосы $\eta = 0,62$ имеет сложный ИС в первой N_1 ПРР. Согласно [6], $\eta = 1$ является максимальной величиной, допускаемой определением.

Важное свойство рассматриваемых сигналов – ширина главного лепестка огибающей АКФ [4], которая обратно пропорциональна девиации частоты сигнала [5] (т.е. огибающая первый раз обратиться в нуль при сдвиге сигнала относительно его копии на интервал времени $\tau = \frac{2\pi}{\mu T_c} = \frac{1}{2\Delta f}$).

В таблице 2 представлены значения τ ширины главного лепестка АКФ и процентное соотношение ξ к длительности сигнала $T_c = 2$ с для сложных ИС в двадцати ПРР спектра РС.

Таблица 2. – Значения ширины главного лепестка АКФ сложных ИС в двадцати ПРР

N_k	1	2	3	4	5	6	7	8	9	10
τ , мс	3,13	6,67	7,14	6,45	6,06	5,26	5,26	5,26	5,56	5,56
ξ , %	0,16	0,33	0,36	0,32	0,30	0,26	0,26	0,26	0,28	0,28

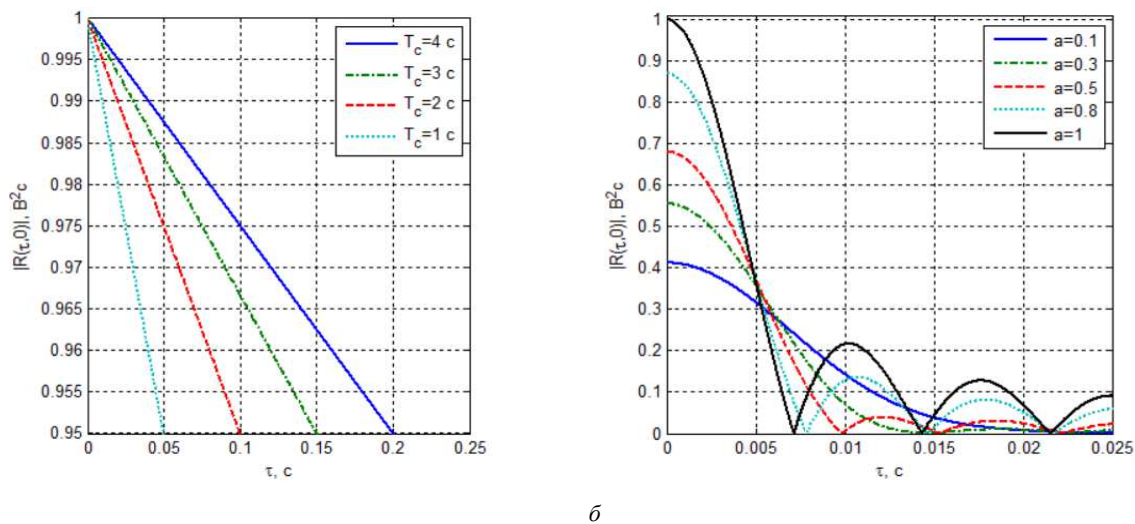
Окончание таблицы 2

N_k	11	12	13	14	15	16	17	18	19	20
τ , мс	5,56	5,56	4,35	2,86	2,50	2,78	2,56	1,04	0,45	0,36
ξ , %	0,28	0,28	0,22	0,14	0,13	0,14	0,13	0,05	0,02	0,02

Все исследуемые сигналы имеют значительную девиацию частоты Δf , и поэтому главный лепесток функции АКФ получается весьма узким. Самый узкий главный лепесток АКФ имеет сложный ИС в двадцатой N_{20} ПРР спектра РС (частотный диапазон $f = [7250 \div 10000]$ Гц, $\Delta f_k = 1375$ Гц), самый широкий – в третьей N_3 (частотный диапазон $f = [570 \div 710]$ Гц, $\Delta f_k = 70$ Гц).

На рисунке 3 показаны формы огибающих АКФ исследуемых гармонических и сложных ИС. Исследования корреляционных свойств гармонических ИС, расположенных на средних частотах ПРР спектра РС, показывают, что форма огибающей их АКФ зависит от длительности сформированного ИС и не зависит от его частоты (рисунок 3, а). Особенность АКФ гармонического сигнала состоит в том, что ее огибающая представляет собой треугольник. Чем больше длительность ИС, тем меньше наклон огибающей его АКФ, что снижает точность определения ее максимального значения. Согласно исследованиям при наложении ограничения на время воздействия гармонического ИС его параметры ухудшаются, что в свою очередь снижает возможность реализации критерия достоверности воспроизведения с высокой точностью.

На рисунке 3, б показаны АКФ сложных ИС с гауссовой огибающей в третьей N_3 ПРР спектра РС с различными значениями уровня эффективной длительности a .



а – гармонических; **б** – сложных с заданными значениями уровня эффективной длительности a в третьей N_3 полосе равной разборчивости

Рисунок 3. – Огибающие автокорреляционных функций исследуемых измерительных сигналов

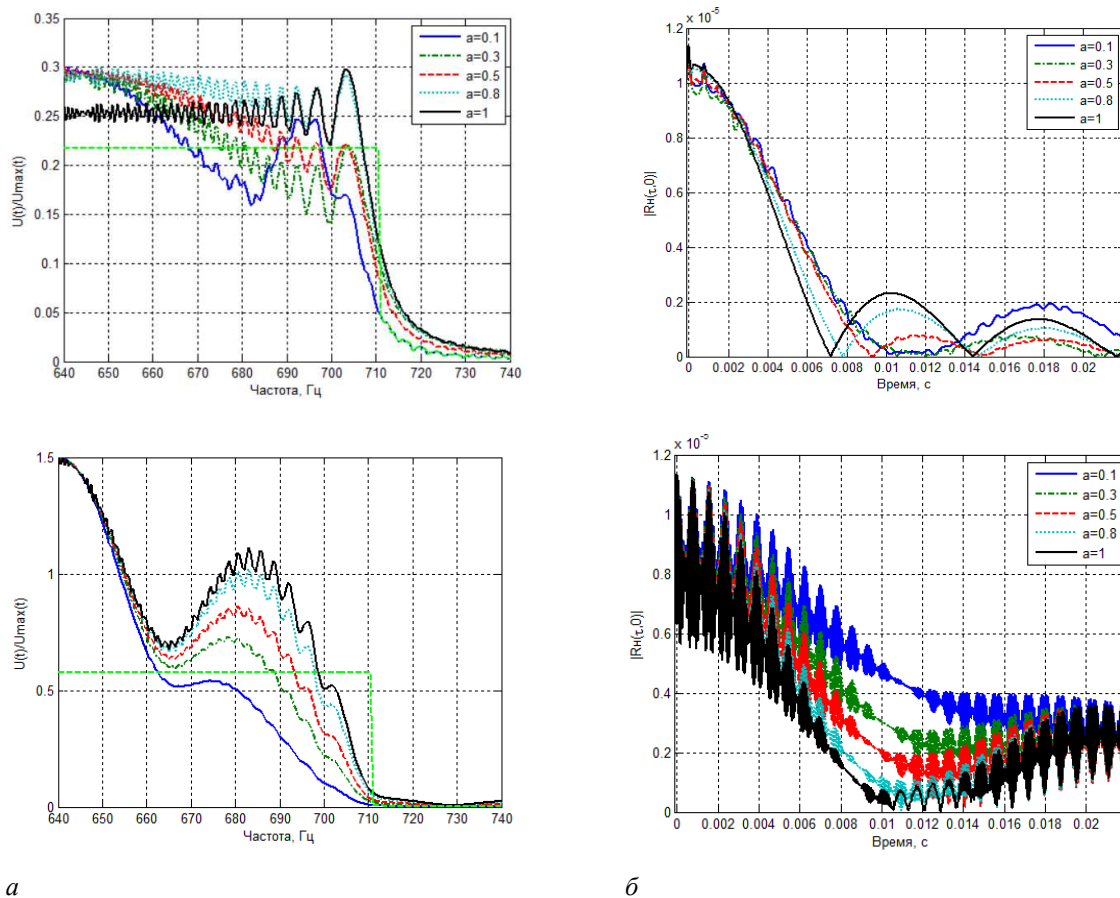
С точки зрения корреляционных свойств сложные ИС с прямоугольной огибающей $a = 1$ имеют такой недостаток, что высота двух первых симметричных боковых лепестков составляет $\approx 0,212$ от высоты центрального лепестка. Чем меньше значение a , тем больше ширина главного лепестка огибающей АКФ сигнала и меньше уровень боковых лепестков. Определенного снижения уровня боковых лепестков можно добиться, применяя в качестве измерительных сложные сигналы с непрямоугольными (типа колокола) [7] огибающими, что в условиях шумов высокого уровня повышает точность определения временного положения сигнала. Использование полностью колоколообразного сложного ИС удовлетворяет условию минимизации боковых лепестков АКФ и позволяет получить оптимальное решение для обеспечения высокой разрешающей способности по частоте, однако приводит к ухудшению разрешающей способности по времени. Чтобы устранить данный недостаток необходимо увеличивать длительность ИС.

При оценке защищенности РИ в КУИ длительность формируемого гармонического ИС в каждой ПРР спектра РС регламентирована $T_c = 1, 10$ и 25 с, исходя из чего суммарное время для передачи двадцати гармонических ИС соответственно равно $T_{\text{сум}} = 20, 200$ и 500 с. Таким образом, чем выше длительность исходного ИС, тем выше точность оценки.

Как элемент базы, девиация частоты предлагаемых для оценки защищенности РИ в КУИ сложных ИС ограничена шириной каждой ПРР, и поэтому при постановке задачи получения результатов в реальном режиме времени она является ограничивающим фактором. Чем больше база сложного ИС, тем выше потенциальные возможности и информативность сигнала, однако труднее реализация: для обеспечения необходимой точности требуются большие временные ресурсы. Обоснование выбора для оценки защищенности РИ в КУИ оптимальных исходных данных: длительности T_c , с; базы B ; изменения мгновенной частоты во времени μ , Гц/с, для сложных сигналов в ПРР спектра РС представлены в работе [4]. Если оценивать суммарное время для передачи всех, одинаковых по длительности $T_c = 4$ с, сложных ИС в двадцати ПРР спектра РС, то оно составит $T_{\text{сум}} = 80$ с. Исходя из этого дальнейшие исследования оценки защищенности РИ в КУИ проводились при формировании сложных ИС в ПРР спектра РС с постоянным значением длительности $T_c = 4$ с при одинаковых шумовых воздействиях. Изменялась лишь форма сложного ИС за счет регулирования уровня его эффективной длительности.

На рисунке 4 представлены основные характеристики сложных ИС в третьей N_3 ПРР в одинаковых условиях зашумления при различных заданных значениях уровня эффективной длительности a , частотой дискретизации $F_s = 44,1$ кГц, длительностью $T_c = 4$ с. На рисунке 4, **а** показаны модули спектров, исследуемых ИС в точке приема на выходе КУИ. На рисунке 4, **б** – огибающие их АКФ.

Форма построенных огибающих АКФ отображает даже незначительные искажения принятых сложных ИС. Использование данной характеристики для оценки искажений гармонических сигналов не обладает такой информативностью. Наиболее точно с использованием огибающих АКФ передаются искажения АЧХ ИС с меньшим значением уровня эффективной длительности сигнала a .



a – спектральное представление; *b* – огибающие их автокорреляционные функции

Рисунок 4. – Графическое представление основных характеристик, исследуемых измерительных сигналов в одинаковых условиях зашумления

Далее исследуем, как искажения влияют на оценку защищенности речевой информации в КУИ. Для оценки используем сложные ИС с различными уровнями эффективной длительности a в одинаковых условиях зашумления. Полученные значения оценки средней мощности P в точке приема на выходе КУИ искаженных ИС представлены в таблице 3.

Таблица 3. – Результаты оценки средней мощности сложных измерительных сигналов в точке приема на выходе каналов утечки информации

N_k	P, B^2				
	$a = 0,1$	$a = 0,3$	$a = 0,5$	$a = 0,8$	$a = 1$
N_1	0,25	0,35	0,43	0,55	0,62
N_2	0,33	0,41	0,48	0,58	0,65
N_3	0,35	0,44	0,51	0,60	0,65
N_4	0,33	0,42	0,48	0,57	0,64
N_5	0,33	0,41	0,47	0,56	0,61
N_6	0,32	0,39	0,45	0,53	0,58
N_7	0,27	0,35	0,43	0,54	0,62
N_8	0,20	0,31	0,40	0,55	0,66
N_9	0,20	0,30	0,39	0,55	0,65
N_{10}	0,24	0,33	0,42	0,54	0,64
N_k	P, B^2				
	$a = 0,1$	$a = 0,3$	$a = 0,5$	$a = 0,8$	$a = 1$
N_{11}	0,29	0,37	0,44	0,54	0,60
N_{12}	0,32	0,40	0,46	0,54	0,59
N_{13}	0,26	0,35	0,42	0,54	0,61
N_{14}	0,27	0,35	0,43	0,56	0,65
N_{15}	0,25	0,34	0,42	0,52	0,59
N_{16}	0,26	0,35	0,43	0,55	0,63
N_{17}	0,26	0,35	0,43	0,56	0,66
N_{18}	0,26	0,35	0,43	0,54	0,62
N_{19}	0,26	0,35	0,43	0,54	0,62
N_{20}	0,26	0,35	0,42	0,54	0,62

Согласно полученным результатам наблюдается следующая зависимость: с уменьшением уровня эффективной длительности a сложного ИС уменьшается и его средняя мощность P , B^2 .

Выводы. На основании проведенного анализа ИС в ПРР спектра РС при использовании наиболее значимых их свойств (спектрального представления и АКФ) установлено, что применение для оценки защищенности РИ в КУИ сложного ИС, в отличие от применения гармонического ИС, позволяет полностью контролировать возникающие искажения АЧХ в пределах каждой из ПРР, на которые разбивается спектр РС, а не в отдельных точках на числовой оси. Исследование деформаций АЧХ гармонического и сложных ИС с регулируемым уровнем эффективной длительности при одинаковых шумовых воздействиях в каждой ПРР показывает, что наилучшие результаты оценки позволяют получить сложные ИС с регулируемым уровнем эффективной длительности $a = 1$. Если использовать $a = 0,8$, то это снижает точность оценки в 1,14 раза, а использование $a = 0,1$ – в 2,3 раза. Однако использование колоколообразного сложного ИС удовлетворяет условию минимизации боковых лепестков АКФ, что является важным при обнаружении ИС на фоне шумов. С учетом сказанного рекомендуется оценку проводить, используя ИС с регулируемым уровнем эффективной длительности $a = 0,8$ длительностью $T_c = 4$ с в каждой ПРР спектра РС.

ЛИТЕРАТУРА

1. Железняк, В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – СПб. : ГУАП, 2006. – 188 с.
2. Левин, Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М. : Сов. радио, 1969. – 752 с.
3. Сигналы радиотехнические измерительные. Термины и определения : ГОСТ 16465–70 (с изм. № 1). – М. : ИПК Изд-во стандартов, 2008. – 30 с.
4. Железняк, В.К. Представление параметров широкополосного линейно-частотно-модулированного сигнала для оценки разборчивости речи в технических каналах утечки информации / В.К. Железняк, К.Я. Раханов, И.Б. Бураченок // Вестник Полоцкого государственного университета. Серия С, Фундаментальные науки. – 2014. – № 12. – С. 2–12.
5. Варакин, Л.Е. Теория сложных сигналов / Л.Е. Варакин. – М. : Советское радио, 1970. – 376 с.
6. Обнаружение радиосигналов / П.С. Акимов [и др.] ; под ред. А.А. Колосова. – М. : Радио и связь, 1989. – 288 с.
7. Слока, В.К. Вопросы обработки радиолокационных сигналов / В.К. Слока. – М. : Сов. радио, 1970. – 256 с.

Поступила 02.03.2017

ANALYSIS OF MEASURING SIGNALS FOR THE ESTIMATION OF SPEECH INFORMATION PROTECTION IN TECHNICAL CHANNELS OF LEAKAGE

V. ZHELEZNYAK, I. BURACHONAK

The analysis and synthesis of measuring signals used to estimate of speech information protection in technical channels of leakage in a high-level noise and significant nonuniformities of their amplitude-frequency characteristics. Identified and investigated most significant properties of harmonic and complex measurement signals in bands of equal intelligibility. The distortion of the form of autocorrelation functions of complex measurement signals received in a noise are investigated. It is proposed to use complex measurement signals with an adjustable level of effective duration. The highest accuracy of the protection rating was obtained by using complex measurement signals with a given level of effective duration $a = 0,8$ s with fixed duration $T_c = 4$ s in each band of equal intelligibility.

Keywords: *measurement signals, technical channels of information leakage, processing of measurement signals.*