ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 534; 53.08:681.3

ПРЕДСТАВЛЕНИЕ ПАРАМЕТРОВ ШИРОКОПОЛОСНОГО ЛИНЕЙНО-ЧАСТОТНО-МОДУЛИРОВАННОГО СИГНАЛА ДЛЯ ОЦЕНКИ РАЗБОРЧИВОСТИ РЕЧИ В ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК; канд. тех. наук К.Я. РАХАНОВ; И.Б. БУРАЧЕНОК
(Полоцкий государственный университет)

Исследованы параметры измерительного широкополосного ЛЧМ-сигнала в полосах равной разборчивости. Предложена оценка защищенности объектов информатизации от утечки речевой информации по низкочастотным техническим каналам утечки широкополосным ЛЧМ-сигналом на основе функции взаимной корреляции в полосах равной разборчивости. Получены исходные данные для реализации метода оценки параметров широкополосного ЛЧМ-сигнала на новых принципах в условиях воздействующих факторов. Метод реализует сокращение времени обработки ЛЧМ-сигнала при сохранении результатов, достигнутых при обработке частотно-временным преобразованием Вигнера по чувствительности, разрешающей способности по частоте и методической погрешности.

Введение. Задача оценки степени защищенности объекта информатизации от утечки информации объекта информатизации (ОИ) по техническим каналам несомненно актуальна. Для этого необходимо выявить каналы утечки (акустический, вибрационный) и оценить защищенность каждого (оценить защищенность выявленного канала утечки в реальном масштабе времени и с высокой точностью по критерию разборчивости речи и критерию отношения сигнал/шум). Защищенность ОИ объективно оценивают выделением слабых измерительных сигналов из шумов высокого уровня в канале утечки (КУ) речевой информации. Методы оценки защищенности речевой информации в полосах равной разборчивости регламентированы в Республике Беларусь СТБ 34.101.29-2011 [1]. Для оценки защищенности КУ речевой информации широко применяется в качестве измерительного гармонический сигнал, обоснованный корреляционной теорией разборчивости речи [2]. Наряду с положительными параметрами и характеристиками данному сигналу присуща методическая погрешность, обусловленная неравномерностями спектральной плотности речевого сигнала в широком диапазоне частот, кривой чувствительности уха, неравномерностью амплитудно-частотной характеристики (АЧХ) преграды, через которую распространяется речевой сигнал (КУ речевой информации), а также из-за ограниченной продолжительности сигнала. К этим факторам относят и неравномерность спектральной плотности фонового шума.

Особенностью КУ информации является неравномерность АЧХ, высокий уровень шумов. Спектр речевого сигнала разбивают на 20 полос равной разборчивости либо на 20 1/3-октавных полос [2].

Реализация широкополосного линейно-частотно-модулированного (ЛЧМ) сигнала для оценки разборчивости речи в КУ речевой информации с обработкой частотно-временным преобразованием Вигнера [3–7] исключает методическую погрешность, присущую гармоническому сигналу, что позволяет значительно повысить информационные параметры по точности, разрешающей способности по частоте и чувствительности. Однако получение достигнутых результатов требует значительного увеличения времени обработки сигналов. Поэтому ***целью работы*** является оптимизация автоматизированной обработки измерительного широкополосного ЛЧМ-сигнала по критерию минимизации временного ресурса в условиях воздействия шумов высокого уровня, деформации его спектральной характеристики при неизменных достигнутых параметрах по предельной чувствительности и высокой точности.

Постановка задачи исследования

1. Исследовать характеристики и параметры широкополосного ЛЧМ-сигнала при разбиении спектра речевого сигнала на 20 полос равной разборчивости. Оценить влияние размера базы и длительности сигнала на чувствительность и точность.

2. Представить параметры широкополосного ЛЧМ-сигнала для оценки разборчивости речи в КУ речевой информации при сокращении времени оценки с сохранением достигнутой чувствительности и методической погрешности.

3. Оценить временную эффективность цифровой обработки широкополосного ЛЧМ-сигнала методом взаимной корреляции.

Анализ широкополосного ЛЧМ-сигнала. В отличие от гармонического сигнала, широкополосный ЛЧМ-сигнал позволяет расширить возможность оценки защищенности речи и контролировать АЧХ в полосах равной разборчивости, на которые разбивается спектр речевого сигнала, а не в отдельных точках на числовой оси [5]. Для оценки защищенности в работах [3; 5] предложено использование широкополосного ЛЧМ-сигнала с большой базой $B > 1$, с прямоугольной огибающей и мгновенной частотой, изменяющейся по линейному закону в пределах времени, равного длительности прямоугольного импульса:

$$f(t) = f_0 + \mu t, \qquad -\frac{T_c}{2} \le t \le \frac{T_c}{2}. \tag{1}$$

Здесь f_0 – средняя частота широкополосного ЛЧМ-сигнала; μ – скорость изменения мгновенной частоты $\left(\mu = \frac{2 \cdot \Delta f}{T_c}, \text{ где } 2 \cdot \Delta f - \text{девиация частоты}\right)$; T_c – длительность импульса.

С учетом (1) уравнение ЛЧМ-сигнала можно представить следующим образом [8]:

$$s_{ЛЧМ}(t) = \begin{cases} A_0 \cos\left[2\pi\left(f_0 t + \frac{\mu}{2} t^2\right) + \varphi_0\right], & |t| \le \frac{T_c}{2}, \\ 0, & |t| > \frac{T_c}{2}, \end{cases} \tag{2}$$

где A_0 – амплитуда сигнала; φ_0 – начальная фаза.

В качестве примера на рисунке 1 изображена спектральная характеристика широкополосного ЛЧМ-сигнала частотой f_0 = 1690 Гц ($2 \cdot \Delta f$ = 180 Гц, девятая полоса равной разборчивости) и базой B = 200 длительностью T_c = 1,1 с.

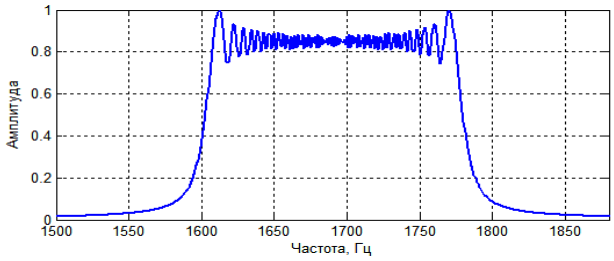

Рис. 1. Спектральная характеристика широкополосного сигнала частотой f_0 = 1690 Гц и базой B = 200 длительностью T_c = 1,1 с

Используя уравнение (2) широкополосного ЛЧМ-сигнала, сформированы и исследованы 20 широкополосных ЛЧМ-сигналов в полосах равной разборчивости при различных исходных размерах базы сигналов и их длительности.

Первоначально в качестве постоянного был установлен безразмерный параметр базы B. При различных значениях базы (B = 200, 500, 5000) определено время пребывания широкополосного ЛЧМ-сигнала в полосе равной разборчивости для каждого отдельно взятого широкополосного ЛЧМ-сигнала. Время пребывания широкополосного ЛЧМ-сигнала в полосе равной разборчивости T_c определялось как [9]:

$$T_c = \frac{B}{2 \cdot \Delta f_N}, \tag{3}$$

где B – база широкополосного ЛЧМ-сигнала; $2 \cdot \Delta f_N$ – девиация широкополосного ЛЧМ-сигнала в пределах полосы равной разборчивости; $N = \overline{1,k}$ (k – порядковый номер полосы равной разборчивости; k = 20 – количество полос равной разборчивости).

При исследовании полученных сигналов установлено, что самое малое значение девиации частоты $2 \cdot \Delta f_{N=3}$ = 140 Гц имеет широкополосный сигнал в третьей полосе равной разборчивости N_3, а самое большое значение девиации частоты $2 \cdot \Delta f_{N=20}$ = 2750 Гц имеет сигнал в двадцатой полосе N_{20}, т.е. значение девиации в двадцатой полосе почти в 20 раз больше значения девиации третьей полосы. Эта разница значительно влияет на оценку сигналов, сформированных при постоянном значении базы, например,

если значение базы равно $B = 200$, длительность широкополосного ЛЧМ-сигнала в N_3 составляет $T_c = 1{,}43$ с, а в полосе N_{20} длительность широкополосного ЛЧМ-сигнала $T_c = 0{,}07$ с.

Особенностью широкополосных ЛЧМ-сигналов с постоянным значением базы является зависимость энергии от ширины полосы. При расширении полосы уменьшается энергия широкополосного ЛЧМ-сигнала. Уменьшение энергии ведет к необходимости сокращения расстояния между источником и приемником сигнала для получения заданной разрешающей способности.

При значении базы $B = 5000$ длительность полученного широкополосного ЛЧМ-сигнала в полосе N_{20} равна $T_c = 1{,}82$ с. При использовании такого же значения базы для формирования широкополосного ЛЧМ-сигнала в третьей полосе N_3 его длительность возрастет до значения $T_c = 35{,}71$ с. Суммарное время при значении базы $B = 200$ равно $T_{сум} = 16{,}86$ с, однако это не позволяет провести оценку разборчивости в полосах равной разборчивости в равных условиях. Чтобы уравнять условия, необходимо использовать постоянное значение базы не менее $B = 5000$. В этом случае суммарное время всех 20-ти широкополосных сигналов составит $T_{сум} = 421{,}79$ с. Данное значение получено без учета времени обработки сигналов на выходе измерителя. При использовании постоянного значения базы не менее $B = 5000$ не представляется возможным сократить общее время оценки технических каналов утечки.

Таким образом, возникла необходимость дальнейшего исследования 20-ти широкополосных ЛЧМ-сигналов в полосах равной разборчивости с постоянным значением длительности сигнала $T_c = 1, 2, 4, 6$ с. Из (3), следует, что

$$B = 2 \cdot \Delta f_N \cdot T_c . \qquad (4)$$

При постоянной длительности были сформированы широкополосные ЛЧМ-сигналы с различными значениями базы в каждой полосе равной разборчивости. При длительности $T_c = 2$ с база широкополосного ЛЧМ-сигнала в третьей полосе N_3 равна $B = 280$, а в полосе N_{20} база $B = 5500$. При длительности $T_c = 4$ с база широкополосного ЛЧМ-сигнала в полосе N_3 и полосе N_{20} составит $B = 560$ и $B = 11000$ соответственно.

Таким образом, если оценивать суммарное время для передачи всех сигналов в 20-ти полосах равной разборчивости, одинаковых по длительности, то суммарное время формирования 20-ти широкополосных ЛЧМ-сигналов при длительности $T_c = 2$ с составит $T_{сум} = 40$ с, при длительности $T_c = 4$ с $T_{сум} = 80$ с.

В результате исследования широкополосных ЛЧМ сигналов в 20 полосах равной разборчивости с постоянным значением базы показано, что с увеличением ширины полосы длительность широкополосных ЛЧМ-сигналов уменьшается и использование широкополосных ЛЧМ-сигналов с постоянным значением базы нецелесообразно. Предложено использовать сигналы, одинаковые по длительности и имеющие различные значения базы. Это сокращает общее время оценки каналов утечки информации.

В таблице 1 представлена зависимость $B = f(2 \cdot \Delta f_N \cdot T_c)$ при $T_c = 4$ с в полосах равной разборчивости.

Таблица 1

Зависимость $B = f(2 \cdot \Delta f_N \cdot T_c)$ при $T_c = 4$ с

Номер полосы N_k	1	2	3	4	5	6	7	8	9	10
Девиация частоты $2 \cdot \Delta f_N$, Гц	320	150	140	155	165	190	190	190	180	180
База B	1280	600	560	620	660	760	760	760	720	720

Продолжение таблицы 1

Номер полосы N_k	11	12	13	14	15	16	17	18	19	20
Девиация частоты $2 \cdot \Delta f_N$, Гц	180	180	230	350	400	360	390	960	2240	2750
База B	720	720	920	1400	1600	1440	1560	3840	8960	11000

При оценке КУ длительность формируемого измерительного гармонического сигнала в каждой полосе равной разборчивости регламентирована: $T_c = 1, 10, 25$ с.

Оценка параметров широкополосного ЛЧМ-сигнала на основе функции взаимной корреляции. При обработке и оценке параметров широкополосного ЛЧМ-сигнала в КУ речевого сигнала необходимо обеспечить синхронность генерируемого измерительного сигнала с сигналом на выходе КУ информации. Для оценки параметров широкополосного ЛЧМ-сигнала в КУ информации с высокой точностью требуется учитывать случайное запаздывание, обусловленное прохождением его через среду распространения, задержками аппаратуры. Даже небольшое случайное запаздывание длительностью 10…200 мс способно значительно увеличить погрешность оценки выходных параметров.

Предложен метод, исключающий погрешности, связанные с запаздыванием сигнала в КУ речевой информации. Данный метод основан на оценке параметров взаимной корреляции между широкополосным ЛЧМ-сигналом, прошедшим через среду распространения с определенной задержкой, и измерительным широкополосным ЛЧМ-сигналом. Случайное запаздывание определяется как разность времени максимума функции взаимной корреляции между сигналом на выходе КУ речевой информации и измерительным широкополосным ЛЧМ-сигналом и времени максимума функции автокорреляции измерительного широкополосного ЛЧМ-сигнала. Это время является временем задержки принимаемого широкополосного ЛЧМ-сигнала.

Следующим параметром является чувствительность оценки, определяемая отношением изменения выходного значения сигнал/шум $Q_{вых}$ к вызывающему его изменению входного отношения сигнал/шум $Q_{вх}$ [10]. Зависимость изменения выходного значения сигнал/шум от изменения входного значения сигнал/шум можно представить как

$$Q_{вых} = f(Q_{вх}), \tag{5}$$

где $Q_{вх} = \left(\frac{P_c}{P_n}\right)_{вх}$ – отношение мощности измерительного сигнала к мощности помехи на входе. Здесь P_c, P_n – соответственно мощности широкополосного ЛЧМ-сигнала и помехи.

При использовании широкополосного ЛЧМ-сигнала предложенным методом для определения $Q_{вых}$ можно воспользоваться следующим выражением [11]:

$$Q_{вых} = 2 \cdot E / N_n, \tag{6}$$

где E – энергия сигнала в канале утечки речевой информации; N_n – спектральная плотность мощности помехи в полосе широкополосного ЛЧМ-сигнала.

Оценку энергии сигнала осуществим на основе корреляционной функции. Согласно исследованиям, корреляционный метод определения сигнала известной формы на фоне белого шума является наиболее оптимальным. Считается, что данный метод позволяет получить наилучшее отношение сигнал/шум [11]. Для этих целей вычисляется статистическая взаимосвязь между случайными величинами из одного ряда с величинами другого ряда, но взятыми со сдвигом. Функция взаимной корреляции определяется [12] согласно выражению

$$R(\tau) = \int_{-\infty}^{\infty} s_1(t)\, s_2(t-\tau)\, dt, \tag{7}$$

где τ – сдвиг по времени между сигналами.

Функция (7) позволяет дополнительно оценить как степень сходства формы двух сигналов, так и их взаимное расположение друг относительно друга по координате. В момент времени, когда выходной сигнал $s_2(t)$ наиболее похож на входной $s_1(t)$, корреляционная функция будет иметь пик. Ширина этого пика, если не брать во внимание шум, будет равна удвоенной длине зондирующего импульса и будет симметричной относительно центрального пика, даже если исследуемый сигнал не является симметричным. Чтобы оценить с высокой точностью зондирующий ЛЧМ-импульс, он должен удовлетворять следующим требованиям: иметь как можно более узкий центральный пик и при этом иметь минимальный уровень боковых лепестков, так как сигнал похож сам на себя только в очень коротком интервале времени.

С использованием выражения (7) построены графики чувствительности 20-ти широкополосных ЛЧМ-сигналов в шумах высокого уровня в пределах $(P_c)_{вых} < (P_n)_{вых}$ и $(P_c)_{вых} > (P_n)_{вых}$ [13].

Графики чувствительности двух широкополосных ЛЧМ-сигналов в полосе N_3 и N_{20} длительностью T_c = 1 с представлены на рисунке 2. Из данных графиков следует, что в надпороговой области имеется выигрыш, одинаковый для обоих случаев. Предельная чувствительность данных сигналов при длительности T_c = 1 с имеет погрешность. Для получения с минимальными разбросами графических зависи-

мостей $Q_{вых} = f(Q_{вх})$, выполнена точечная среднестатистическая обработка выходных 20-ти широкополосных ЛЧМ-сигналов в шумах длительностью T_c = 1, 2, 4, 6 с.

На рисунке 3 показано, что при увеличении длительности широкополосного ЛЧМ-сигнала получен выигрыш в надпороговой области, который имеет линейную зависимость, а его величина одинакова для всех 20-ти ЛЧМ-сигналов. При длительностях сигналов T_c = 1 с, T_c = 2 с, T_c = 4 с выигрыш в надпороговой области составляет 2, 5 и 8 дБ соответственно. При увеличении длительности сигналов уменьшается также погрешность предельной чувствительности для различных полос при отрицательных отношениях сигнал/шум, а при длительности сигналов T_c = 4 с графики практически совпадают для 20-ти полос равной разборчивости. Таким образом, с увеличением T_c точность оценки параметров увеличивается, так как соответственно повышается количество точек дискретизации, однако увеличение количества точек дискретизации увеличивает время обработки сигнала.

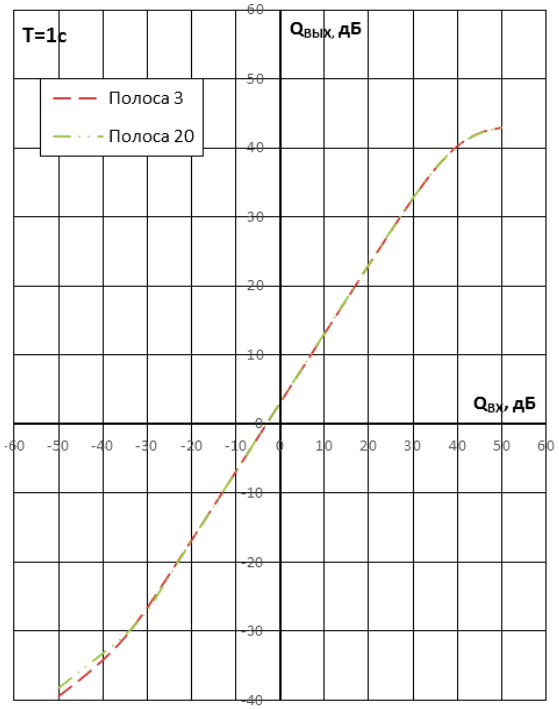

Рис. 2. Зависимость $Q_{вых}$ от $Q_{вх}$ в полосах N_3 и N_{20} с точечной среднестатистической обработкой выходных сигналов в шумах длительностью T_c = 1 с

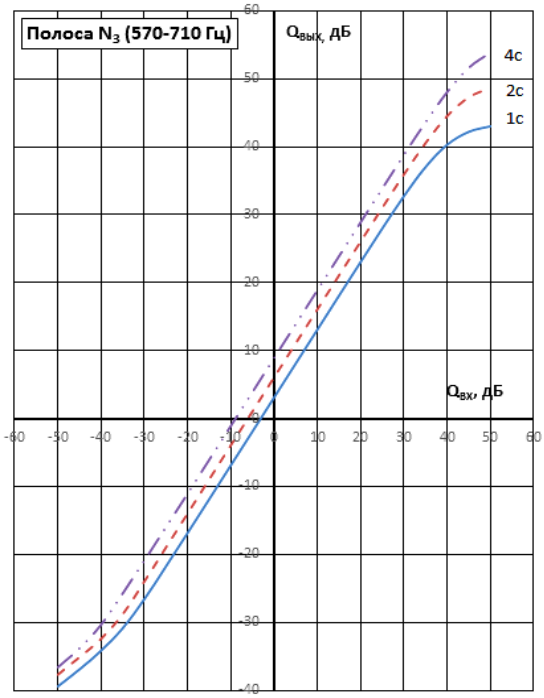

Рис. 3. Зависимость $Q_{вых}$ от $Q_{вх}$ в полосе N_3 с точечной среднестатистической обработкой выходных сигналов в шумах длительностью T_c = 1, 2, 4 с

Графики чувствительности построены на основе статистической обработки ряда измерений. При оценке результатов измерений иногда пользуются понятием максимальной или предельной допустимой погрешности, значение которой определяют в долях σ. В настоящее время существуют разные критерии установления максимальной погрешности, т.е. границы поля допуска $\pm D$, в которые случайные погрешности должны уложиться. На основании информационной теории измерений профессор П.В. Новицкий рекомендует пользоваться значением $D = 2 \cdot \sigma$ [14].

Таким образом, для определения предельной чувствительности измерителя определим относительную погрешность согласно [14]:

$$\gamma \approx \pm \frac{D}{\overline{X}} \cdot 100\ \%, \qquad (8)$$

где D – границы поля допуска, определяющие доверительный интервал значений измеряемой величины от $\overline{X} - D$ до $\overline{X} + D$; $\overline{X}$ – действительное значение измеряемой величины.

По результатам исследования методом на основе функции взаимной корреляции параметров выходных $N_1, \ldots, N_{20}$ широкополосных ЛЧМ-сигналов в конкретно заданной k-той полосе с частотой дискретизации F_s = 44100 Гц и постоянным значением базы B = 200, 300, 500, 600 были получены значения предельной чувствительности для каждой k-той полосы при относительной погрешности $|\gamma| < 3$ %.

На рисунке 4 показана зависимость предельной чувствительности $Q_{вых}$ в полосах равной разборчивости при различном значении базы в каждой *k*-той полосе.

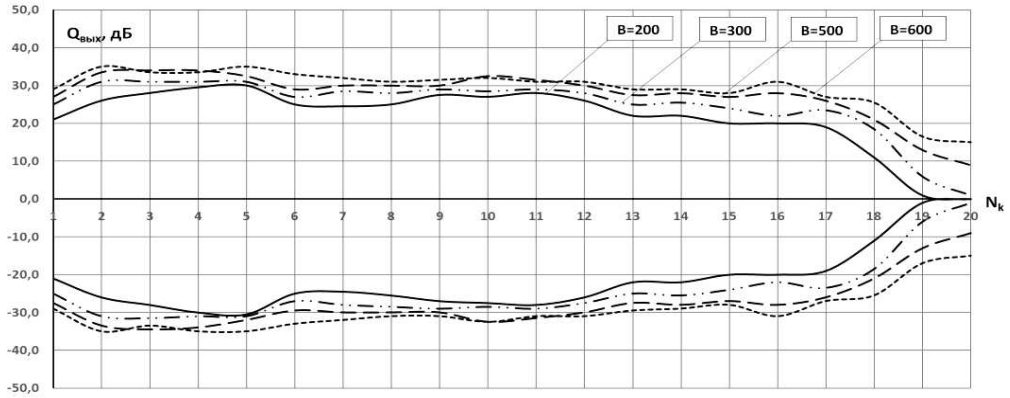

Рис. 4. Предельная чувствительность измерителя выходных ЛЧМ-сигналов
с размером базы *B* = 200, 300, 500, 600 в каждой полосе равной разборчивости в шумах

Из рисунка 4 следует, что при B = 200 в полосах N_{19} (T_c = 0,09 с, Δf = 2240 Гц), N_{20} (T_c = 0,07 с, Δf = 2750 Гц) сигнал практически не обнаруживается. При B = 500 в полосе N_{19} (T_c = 0,22 с), N_{20} (T_c = 0,18 с) сигнал обнаруживается, однако система имеет очень низкий уровень чувствительности.

По результатам эксперимента оптимальное значение базы в полосах N_{19}, N_{20} должно быть не ниже 5000. Если же рассматривать предельную чувствительность в других полосах равной разборчивости, то при значениях базы выше 500 значение предельной чувствительности повышается незначительно, поэтому дальнейшее увеличение значения базы нецелесообразно, так как с увеличением базы резко возрастает и время широкополосных ЛЧМ-сигналов в полосах частот, имеющих меньшее значение девиации частоты, что значительно увеличивает время оценки.

По результатам исследований методом на основе функции взаимной корреляции параметров N_1, ..., N_{20} ЛЧМ-сигналов, каждый в конкретно заданной *k*-той полосе с частотой дискретизации F_s, равной 44100 Гц, и с постоянным значением длительности сигнала при T_c = 1, 2, 4, 6 с были получены значения предельной чувствительности для каждой *k*-той полосы при относительной погрешности $|\gamma| < 3$ %.

На рисунке 5 показана зависимость предельной чувствительности $Q_{вых}$ в полосах равной разборчивости при различной длительности сигналов в каждой *k*-той полосе.

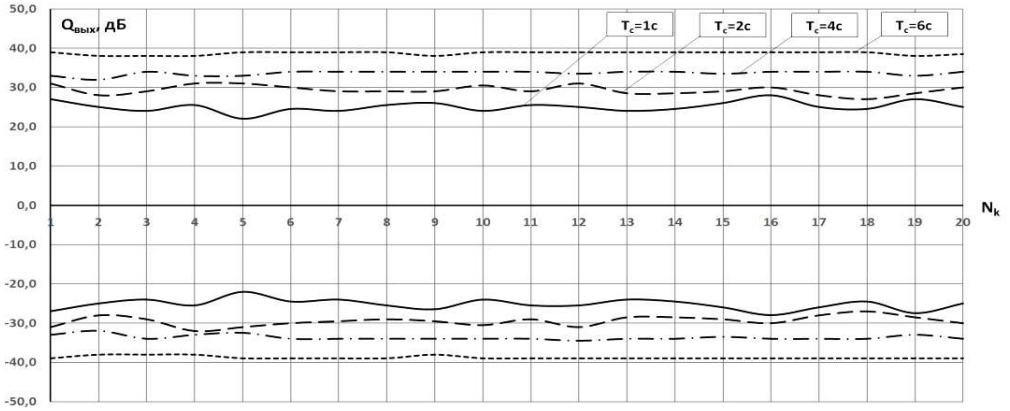

Рис. 5. Предельная чувствительность измерителя выходных ЛЧМ-сигналов
длительностью T_c = 1, 2, 4, 6 с в каждой полосе равной разборчивости в шумах

Из рисунка 5 следует, что чем больше длительность широкополосного ЛЧМ-сигнала, тем меньше значение вариации для каждой *k*-той полосы. Однако, учитывая необходимость выбора минимального значения времени при достижении высокой чувствительности, оптимальным выбором будет T_c = 4 с при условии, что оно имеет постоянное значение для каждой *k*-той полосы. Величины размеров баз 20-ти широкополосных ЛЧМ-сигналов при длительности T_c = 4 с представлены в таблице 1.

Недостатком измерительного широкополосного ЛЧМ-сигнала является наличие порогового эффекта [15]. При уменьшении отношения сигнал/шум до определенного порогового значения [10] наблюдается резкое снижение возможности выделения сигнала из шумов. Снижение порогового эффекта широкополосного ЛЧМ-сигнала осуществляется при помощи синхронного накопления [16]. Синхронное накопление спектральных составляющих позволяет снизить порог чувствительности и повышает точность оценки разборчивости речи [7]. Поэтому, используя данное накопление, получили зависимости $Q_{вых} = f(Q_{вх})$ в шумах высокого уровня при накоплении 10 и 50 раз. Данные зависимости показаны на рисунке 6.

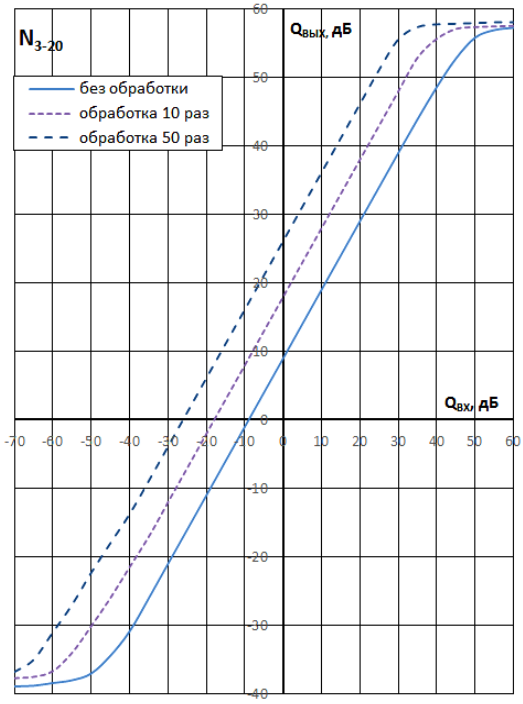

Рис. 6. Зависимость $Q_{вых}$ от $Q_{вх}$ для 20-ти полос равной разборчивости
с точечной среднестатистической обработкой выходных сигналов в шумах длительностью T_c = 4 с

Согласно полученным данным в надпороговой области широкополосный ЛЧМ-сигнал при накоплении 10 раз обладает выигрышем в надпороговой области до 18 дБ. При выделении сигнала из шумов накоплением 50 раз имеем значение выигрыша в надпороговой области, равное 27 дБ. Отношение накопленных энергий широкополосного ЛЧМ-сигнала и помехи растут с увеличением количества накоплений сигнала *n*.

Для оценки параметров широкополосного ЛЧМ-сигнала в условиях воздействия шумов высокого уровня с целью экономии общего времени оценки каналов утечки целесообразно использование 20-ти испытательных сигналов в каждой полосе равной разборчивости длительностью T_c = 4 с. Данное время позволяет сохранить неизменными достигнутые ранее параметры по предельной чувствительности, высокой точности и тонкой структуре обработанного измерительного сигнала.

Оценка временной эффективности цифровой обработки. Практическая реализация программно-аппаратного комплекса, использующего для оценки каналов утечки метод ЛЧМ-сигнала с обработкой частотно-временным преобразованием Вигнера, связана с определенными сложностями [5], что требует значительных временных ресурсов.

Оценим эффективность цифровой обработки широкополосного ЛЧМ-сигнала методом ЛЧМ-сигнала на основе функции взаимной корреляции. Для анализа эффективности цифровой обработки целесообразно использовать подсчет количества выполнения базовых (основных) операций, которые вносят наибольший вклад в общее время выполнения обработки. Время выполнения программной реализации цифровой обработки $T(n)$ на конкретной ПЭВМ можно представить в виде [17]

$$T(n) = c_{op} \cdot C(n), \tag{9}$$

где c_{op} – время выполнения основной операции на ПЭВМ; $C(n)$ – количество выполняемых базовых операций в зависимости от размера входных данных n.

На основании (9) в работе [3] с использованием внешнего модуля АЦП E14-440D $F_s = 2 \cdot 10^5$ Гц при максимальном размере входных данных $n = 4 \cdot 10^5$ было определено итоговое количество базовых операций, равное $C(n) = 1{,}16 \cdot 10^{12}$, для расчета на ПЭВМ (Intel® Core™ Duo U2400), имеющей производительность $3{,}18 \cdot 10^9$ флоп/с. Время выполнения алгоритма

$$T(n) = \frac{1}{3{,}18 \cdot 10^9} \cdot 1{,}16 \cdot 10^{12} = 3{,}65 \cdot 10^2 \text{ с.}$$

Чтобы оценить время выполнения алгоритма оценки параметров на основе функции взаимной корреляции при тех же заданных условиях, выражение (7) представим в цифровой форме:

$$R_j = \sum_{i=0}^{n} S_j \cdot S'_{i-j} \cdot \Delta t. \tag{10}$$

где S – исходный широкополосный ЛЧМ-сигнал; S' – принятый широкополосный ЛЧМ-сигнал; Δt – интервал дискретизации.

Для оценки эффективности цифровой обработки выделим наиболее ёмкие с точки зрения вычисления по времени операции, требующие значительных вычислительных ресурсов, и представим количество выполняемых базовых операций в зависимости от размера входных данных n по основным операциям. Итоговое количество базовых операций алгоритма вычисления классической функции взаимной корреляции $C(n)$ можно описать выражением

$$C(n) = (C_1(n) + C_2(n) + C_3(n)) \cdot C_4(n) = (3n + n + n) \cdot n = 5n \cdot n = 5 \cdot n^2, \tag{11}$$

где $C_1(n)$ – количество базовых операций произведения $S_j \cdot S'_{i-j} \cdot \Delta t$; $C_2(n)$ – количество базовых операций инкрементации индекса i; $C_3(n)$ – количество базовых операций суммирования результатов произведений $S_j \cdot S'_{i-j} \cdot \Delta t$; $C_4(n)$ – количество базовых операций вычисления взаимной корреляции для временного сдвига.

Таким образом, если $n = F_s \cdot T_c = 2 \cdot 10^5 \cdot 2 = 4 \cdot 10^5$, подставив это значение в (11), получим величину базовых операций $C(n) = 5 \cdot (4 \cdot 10^5)^2 = 8 \cdot 10^{11}$. Тогда время выполнения алгоритма обработки

$$T(n) = \frac{1}{3{,}18 \cdot 10^9} \cdot 8 \cdot 10^{11} = 215{,}6 = 2{,}52 \cdot 10^2 \text{ с.}$$

При оценке параметров широкополосного ЛЧМ-сигнала обработкой частотно-временным преобразованием Вигнера при переходе от аналоговой формы распределения Вигнера к дискретной для наиболее достоверного выделения слабого сигнала в шумах высокого уровня широкополосный ЛЧМ-сигнал должен быть дискретизирован с тактовой частотой, более чем в двое превышающей частоту дискретизации Котельникова [5]. Оценка параметров широкополосного ЛЧМ-сигнала обработкой частотно-временным преобразованием Вигнера проводилась с частотой дискретизации, в десять раз превышающей частоту дискретизации Котельникова. В случае оценки параметров широкополосного ЛЧМ-сигнала на основе функции взаимной корреляции в такой величине дискретизации нет необходимости.

Например, при частоте дискретизации $F_s = 44100$ Гц на основании (11) получим величину базовых операций $C(n) = 5 \cdot (4{,}41 \cdot 10^4 \cdot 2)^2 = 3{,}9 \cdot 10^{10}$. Время выполнения алгоритма обработки

$$T(n) = \frac{1}{3{,}18 \cdot 10^9} \cdot 3{,}9 \cdot 10^{10} = 1{,}2 \cdot 10^1 \text{ с.}$$

В результате время оценки параметров широкополосного ЛЧМ-сигнала на основе функции взаимной корреляции позволит значительно сократить количество базовых операций и, следовательно, общее время оценки каналов утечки информации. Эффективность цифровой обработки параметров широкополосного ЛЧМ-сигнала методом на основе функции взаимной корреляции при T_c = 2 с и T_c = 4 с представлена в таблице 2 и таблице 3 соответственно.

Таким образом, время обработки сигнала длительностью 4 с частотой дискретизации F_s = 44100 Гц на основе функции взаимной корреляции с использованием внешнего модуля АЦП E14-440D и ПЭВМ Intel® Core™ Duo U2400 можно сократить в 7,5 раза.

Таблица 2

Эффективность цифровой обработки параметров широкополосного ЛЧМ-сигнала при T_c = 2 с для ПЭВМ разной производительности

Частота дискретизации F_s, Гц	Размер входных данных n при T_c = 2 с	Количество базовых операций $C(n)$	Эффективность цифровой обработки при производительности микропроцессора (Intel® Core™ Duo U2400) $3{,}18 \cdot 10^9$ флоп/с $T(n)$, с	Эффективность цифровой обработки при производительности микропроцессора (Intel® Core™ i7-975 XE) $53{,}328 \cdot 10^9$ флоп/с $T(n)$, с
$1{,}00 \cdot 10^5$	$2{,}000 \cdot 10^5$	$2{,}00 \cdot 10^{11}$	$6{,}29 \cdot 10^1$	3,80
$9{,}60 \cdot 10^4$	$1{,}920 \cdot 10^5$	$1{,}84 \cdot 10^{11}$	$5{,}80 \cdot 10^1$	3,50
$8{,}82 \cdot 10^4$	$1{,}764 \cdot 10^5$	$1{,}56 \cdot 10^{11}$	$4{,}89 \cdot 10^1$	2,90
$4{,}80 \cdot 10^4$	$9{,}600 \cdot 10^4$	$4{,}61 \cdot 10^{10}$	$1{,}45 \cdot 10^1$	0,90
$4{,}41 \cdot 10^4$	$8{,}820 \cdot 10^4$	$3{,}89 \cdot 10^{10}$	$1{,}22 \cdot 10^1$	0,70
$3{,}20 \cdot 10^4$	$6{,}400 \cdot 10^4$	$2{,}05 \cdot 10^{10}$	6,40	0,40

Таблица 3

Эффективность цифровой обработки параметров широкополосного ЛЧМ-сигнала при T_c = 4 с для ПЭВМ разной производительности

Частота дискретизации F_s, Гц	Размер входных данных n при T_c = 4 с	Количество базовых операций $C(n)$	Эффективность цифровой обработки при производительности микропроцессора (Intel® Core™ Duo U2400) $3{,}18 \cdot 10^9$ флоп/с $T(n)$, с	Эффективность цифровой обработки при производительности микропроцессора (Intel® Core™ i7-975 XE) $53{,}328 \cdot 10^9$ флоп/с $T(n)$, с
$1{,}00 \cdot 10^5$	$4{,}000 \cdot 10^5$	$8{,}00 \cdot 10^{11}$	$2{,}516 \cdot 10^2$	$1{,}50 \cdot 10^1$
$9{,}60 \cdot 10^4$	$3{,}840 \cdot 10^5$	$7{,}37 \cdot 10^{11}$	$2{,}318 \cdot 10^2$	$1{,}38 \cdot 10^1$
$8{,}82 \cdot 10^4$	$3{,}528 \cdot 10^5$	$6{,}22 \cdot 10^{11}$	$1{,}957 \cdot 10^2$	$1{,}17 \cdot 10^1$
$4{,}80 \cdot 10^4$	$1{,}920 \cdot 10^5$	$1{,}84 \cdot 10^{11}$	$5{,}800 \cdot 10^1$	3,50
$4{,}41 \cdot 10^4$	$1{,}764 \cdot 10^5$	$1{,}56 \cdot 10^{11}$	$4{,}890 \cdot 10^1$	2,90
$3{,}20 \cdot 10^4$	$1{,}280 \cdot 10^5$	$8{,}19 \cdot 10^{10}$	$2{,}580 \cdot 10^1$	1,50

Выводы

1. Обработка широкополосных ЛЧМ-сигналов на базе корреляционного метода в 20-ти полосах равной разборчивости, одинаковых по длительности, но с разными базами, позволила сократить время оценки в каждой из полос равной разборчивости и суммарное время оценки защищенности КУ информации более чем в 5 раз по сравнению с временем обработки широкополосных ЛЧМ-сигналов с постоянным значением базы и переменным временем.

2. Метод взаимной корреляции между измерительным широкополосным ЛЧМ-сигналом, прошедшим через среду распространения, и измерительным широкополосным ЛЧМ-сигналом позволил упростить процедуру автоматизированных измерений за счет усовершенствования алгоритма и без усложнения аппаратной части программно-аппаратного комплекса сократить время обработки и оценки защищенности КУ информации в 30 раз по сравнению с методом широкополосного ЛЧМ-сигнала с обработкой частотно-временным преобразованием Вигнера. При частоте дискретизации F_s = 44100 Гц время обработки широкополосного ЛЧМ-сигнала длительностью T_c = 4 составит 48,9 с, длительностью T_c = 2 – 12,2 с. Использование более современных ПЭВМ (например, Intel® Core™ i7-975 XE) позволит обрабатывать широкополосный ЛЧМ-сигнал длительностью T_c = 4 около 3 с, длительностью T_c = 2 – 1 с. Результаты получены методом математического моделирования.

ЛИТЕРАТУРА

1. Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования: СТБ 34.101.29-2011. – Взамен: СТБ П 34.101.29-2007: постановление Госстандарта от 25.11.2011 № 83. – Дата введения: 01.03.2012.

2. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.
3. Раханов, К.Я. Широкополосная линейно-частотная модуляция сигнала для оценки разборчивости речи в каналах утечки информации / К.Я. Раханов, В.К. Железняк // Изв. Нац. акад. наук Беларуси. Серия физ.-техн. наук; редкол.: П.А. Витязь (гл. ред.) [и др.]. – Минск: Беларус. навука, 2014. – С. 88–95.
4. Способ измерения максимальной разборчивости речи: МПК G 10L 15/00 / В.К. Железняк, К.Я. Раханов; заявитель Полоц. гос. ун-т. – № a20100004; заявл. 04.01.2010.
5. Железняк, В.К. Методы оценки защищенности речевой информации / В.К. Железняк, К.Я. Раханов // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12. – С. 2 – 8.
6. Раханов, К.Я. Оценка разборчивости речи в каналах утечки информации методом ЛЧМ-сигнала программно-аппаратной системой / К.Я. Раханов, В.К. Железняк // Технические средства защиты информации: тез. докл. X Белорус.- Рос. науч.-техн. конф., Минск, 29–30 мая 2012 г.; редкол.: Л.М. Лыньков (отв. ред.) [и др.]. – Минск: БГУИР, 2012. – С. 12–13.
7. Железняк, В.К. Имитационная модель автоматизированной помехоустойчивой оценки разборчивости речи методом ЛЧМ-сигнала / В.К. Железняк, К.Я. Раханов // Вестн. Полоц. гос. ун-та. Серия С. Фундаментальные науки. – 2011. – № 12. – С. 35–41.
8. Денисенко, А.Н. Статистическая теория радиотехнических систем / А.Н. Денисенко. – М.: АРИ, 2007. – 200 с.
9. Баскаков, С.И. Радиотехнические цепи и сигналы: учебник для вузов по спец. «Радиотехника» / С.И. Баскаков. – 2-е изд., перераб. и доп. – М.: Высш. шк., 1988. – 448 с.
10. Рекомендации по межгосударственной стандартизации. ГСИ. Метрология. Основные термины и определения: РМГ 29-99. – Минск: ИПК Изд-во стандартов, 2000. – 140 с.
11. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М.: Радио и связь, 1985. – 384 с.
12. Сергиенко, А.Б. Цифровая обработка сигналов / А.Б. Сергиенко. – СПб.: Питер, 2005. – 604 с.
13. Железняк, В.К. Представление параметров обработкой сигналом широкополосной линейной частотной модуляции для оценки разборчивости речи в технических каналах утечки информации / В.К. Железняк, И.Б Бураченок // Современные средства связи: материалы XIX междунар. науч.-техн. конф., Минск, 14–15 окт. 2014 года; редкол.: А.О. Зеневич [и др.]. – Минск: УО ВГКС, 2014. – С. 168–169.
14. Новицкий, П.В. Оценка погрешностей результатов измерений / П.В. Новицкий, И.А. Зограф. – 2-е перераб. и доп. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1991. – 304 с.
15. Теория передачи сигналов на железнодорожном транспорте: учебник для вузов ж.-д. трансп. / Г.В. Горелов [и др.]; под общ. ред. М.В. Пономаренко. – М.: Транспорт, 2001. – 415 с.
16. Харкевич, А.А. Очерки общей связи / А.А. Харкевич. – М., 1955. – 268 с.
17. Левитин, А. Алгоритмы: введение в разработку и анализ / А. Левитин; пер. с англ. – М.: Издат. дом «Вильямс», 2006. – 576 с.

Поступила 12.09.2014

REPRESENTATION OF PARAMETERS BROADBAND LINEAR CHIRP SIGNAL FOR ASSESSMENT OF SPEECH INTELLIGIBILITY IN TECHNICAL CHANNELS OF INFORMATION LEAKAGE

V. ZHELEZNYAK, K. RAKHANAU, I. BURACHONAK

Researched the parameters of measuring broadband linear CHIRP-signal in the bands of equal intelligibility. Offered the estimation of the level of informatization objects protection from leakage of speech information through the low-frequency technical channels of leakage by the linear CHIRP-signal based on the cross-correlation function in the bands of equal intelligibility. Obtained original data to implement the method of estimating the parameters of the broadband linear CHIRP-signal on new principles in terms of influencing factors. The method implements the reduction of the processing time CHIR-signal keeping the results achieved by using processing time-frequency transformation Wigner by sensitivity, frequency resolution and methodological errors.