обмеженим доступом, що не становить державної таємниці» // Матеріали до круглого столу за темою: «Обговорення проекту закону України «Про інформацію з обмеженим доступом, що не становить державної таємниці»; Третя науково-технічна конференція «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» 9 жовтня 2001 року: К., 2001. С. 4 – 25. ***4.*** *ст. ст. 28, 30 Закону України „Про інформацію” від 02. 10. 1992 р. // Відомості Верховної Ради України 1992, N48 від 01. 12. 1992 р.* ***5.*** *ст. 505 Цивільного кодексу України // Офіційний Вісник України 2003, N 11, ст. 461.* ***6.*** *ст. 36 Господарського кодексу України // Офіційний Вісник України 2003, N 11, ст. 462.* ***7.*** *ст. 1 Закону України “Про фінансові послуги та державне регулювання ринків фінансових послуг” від 12 липня 2001 року //Офіційний Вісник України 2001, N 32, ст. 1457.* ***8.*** *ст. 60 Закону України „Про банки і банківську діяльність» від 07. 12. 2000 р. // Офіційний Вісник України 2001, 1 - 2 (частина 1) від 26. 01. 2001 р.* ***9.*** *ст. 9 Закону України „Про адвокатуру” // Відомості Верховної Ради України 1993, N9 від 02. 03. 1993 р.* ***10.*** *ст. 40 Основ законодавства України про охорону здоров'я від 19. 11. 92 р. // Відомості Верховної Ради України 1993, N4 від 26. 01. 1993 р.* ***11.*** *Ст. 40 Закону України „Про страхування” // Відомості Верховної Ради України, 1996 р., N 18, ст. 78.* ***12.*** *ст. 31 Конституції України // Відомості Верховної Ради України, 1996 р., N 30, ст. 141.* ***13.*** *ст. 228 Сімейного кодексу України // Офіційний Вісник України 2002, N 7, ст. 273.* ***14.*** *ст. 8 Закону України „Про нотаріат” від 2. 09. 1993 р. // Відомості Верховної Ради України 1993, N39 від 28. 09. 1993 р.* ***15.*** *ст. 71 Конституції України // Відомості Верховної Ради України, 1996 р., N 30, ст. 141.* ***16.*** *ст. 1255 Цивільного кодексу України // Офіційний Вісник України 2003, N 11, ст. 461.* ***17.*** *Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К. Г. Устименка) від 30. 10. 97 р. // Офіційний Вісник України 1997, 46 від 24. 11. 97 р.* ***18.*** *Закон України “Про державну таємницю” від 21. 09. 1999 р. // Відомості Верховної Ради 1999, N 49.* ***19.*** *Див додаток 13 до Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затв. Постановою Кабінету Міністрів України N 1893 від 27. 11. 98 р. // Офіційний Вісник України, 1998, 48 від 17. 12. 98 р.* ***20.*** *ст. 10 Федерального закона РФ «Об информации, информатизации и защите информации» // Российская газета от 15. 01. 2003 г., N 5.* ***21.*** *Алданов Ю. В. Шамсутдінов О. В. Кримінально-правова охорона державних секретів від розголошення в іноземному законодавстві: Огляд. – К. Вид-во НА СБ України, 2001. С. 6.* ***22.*** *Мерзляков Н. С., Радьков В. П. Опыт определения понятий государственных секретов в зарубежных странах // Труды НИИ «Прогноз», 1982, № 2, С. 109.*

УДК 681.391

КОРРЕЛЯЦИОННЫЙ ПАРАМЕТР КАЧЕСТВА АДДИТИВНОГО МАСКИРОВАНИЯ РЕЧЕВЫХ СИГНАЛОВ

Александр Архипов, Владимир Журавлев*, Сергей Завьялов*
*Національний технічний університет України «КПІ», *Запорожский национальный технический университет*

Анотація. **Розглянута методика цифрової кореляційної обробки контрольного фрагменту мови, що дозволяє на основі розрахунку коефіцієнта кореляції обґрунтувати аналітичну оцінку параметра якості передачі сигналу мови каналами зв’язку та проводити аналіз ефективності адитивного маскування мовних сигналів.**
Summary: **The method of check utterance digital correlation processing, which allows to substantiate the communication path quality criteria analytic estimation on the base of correlation coefficient calculation and to analyze the speech signal additive masking effectiveness is under review.**
Ключевые слова: **Речевой сигнал, аддитивное маскирование, корреляционная обработка, параметр качества.**

I Введение

Среди разнообразных средств спецтехники в последние годы интенсивно развивается и совершенствуется рынок устройств, предназначенных для несанкционированного доступа (НСД) к конфиденциальной информации, содержащейся в речевом сигнале (РС), который является первичным общедоступным выражением результата мыслительного процесса человека. В связи с эволюционным развитием речи, как способа помехоустойчивого акустического кодирования мысли, РС адаптированы к

аддитивным природным шумам, которые можно рассматривать как сигналы помех и, вследствие этого, гарантированная защита РС от НСД является актуальной научно-технической проблемой.

II Постановка задачи

В качестве аддитивного сигнала маскирования $h(t)$ РС к настоящему времени достаточно полно исследованы сигналы шума с равномерным («белый» шум) распределения плотности мощности в речевом диапазоне частот $\Delta\omega = \omega_в - \omega_н$ и речеподобные сигналы, состоящие из аддитивной смеси нескольких речевых сигналов («речевой хор») [1, 2]. Критерием эффективности сигнала маскирования принято считать отношение среднеквадратических значений напряжения информационного сигнала $S(t)$ к сигналу шума $h(t)$, при котором обеспечивается параметр определенного вида разборчивости, не превосходящий заданного нормированного значения.

В результате ранее проведенных исследований [3] отмечена более высокая эффективность речеподобных сигналов маскирования по сравнению с рекомендуемыми [4] сигналами со спектром «белого» шума. Однако выполнить объективный сравнительный анализ результатов проведенных исследований невозможно, т. к. они не сопоставлены по методике испытаний, идентичности артикуляционной бригады и отсутствия адекватной математической модели речеподобного сигнала маскирования.

Отдельно необходимо акцентировать внимание на результатах артикуляционных испытаний, считающихся сегодня apriori, объективной мерой качества передачи РС по каналам связи. Ощутимый диапазон отклонений результатов артикуляционных испытаний, проведенных разными артикуляционными бригадами, позволяет сделать вывод о том, что это достаточно субъективная групповая экспертная оценка, которая зависит от времени тренировки, усталости, среднего возраста и индивидуальных акустических характеристик речи и слуха членов бригады [5].

Таким образом, в рамках указанной проблемы, в качестве актуальных можно выделить следующие задачи.

Обоснование объективной аналитической оценки показателя качества (ПК) маскирования РС.

Анализ эффективности сигналов аддитивного маскирования РС.

III Предлагаемые алгоритмы и решения

Аналитический показатель качества передачи РС.

Представим РС $S(t)$ источника информации моделью в виде упорядоченного набора прилегающих друг к другу фрагментов длиной T_c:

$$S(t) = \sum_{i=1}^{m} s_i(t_i), \tag{1}$$

где $s_i(t) = \begin{cases} S(t), & t \in (t_i, t_i + T_c], \quad t_i = t_0 + (i-1)T_c, \quad i = \overline{1,m}, \\ 0, & t_i + T_c < t \le t_i. \end{cases}$

Для упрощения последующего анализа полагаем, что в пределах каждого отличного от 0 фрагмента значений сигнала $s_i(t)$ амплитуды центрированы и распределены по нормальному закону $W[s_i(t)]$ с дисперсией $D[s_i(t)]$.

Пусть существует случайный стационарный маскирующий сигнал $h(t)$, обладающий произвольными статистическими характеристиками, который в канале связи накладывается на сигнал $S(t)$. Сигнал в приемнике $sh(t)$ будет равен сумме сигналов:

$$sh(t) = S(t) + h(t). \tag{2}$$

Введем требование синхронности обработки в приемнике сигналов $sh(t)$ и $s_i(t)$, которое реально выполнимо в системах цифровой обработки с точностью интервала дискретизации. Далее будем полагать, что в пределах каждого полуоткрытого интервала времени $(t_i, t_i + T_c], i = \overline{1,m}$ сигналы $sh(t)$ и $s_i(t)$ являются эргодичными по дисперсии и корреляционной функции. В этой связи удобно вместо сигналов $s_i(t)$ и $sh(t)$ анализировать их автокорреляционные функции (АКФ) $R_{ss}(\tau)$ и $R_{shsh}(\tau)$, соответственно, которые в случае нормального случайного стационарного процесса содержат, с точностью до математического ожидания (МО), всю информацию об этом процессе. Кроме того, интерес представляет и

расчет взаимной корреляционной функции (ВКФ) $R_{ssh}(\tau)$, которая позволит судить о наличии сходства формы реализаций процессов $s_i(t)$ и $sh(t)$, т. е. является функцией параметра качества передачи РС по зашумленному каналу связи.

Исходя из вышеизложенного, определим АКФ и ВКФ:

$$R_{ss}(\tau) = \frac{1}{Tc}\int_0^{Tc} s(t)s(t+\tau)dt,$$

$$R_{shsh}(\tau) = \frac{1}{Tc}\int_0^{Tc} sh(t)sh(t+\tau)dt, \qquad (3)$$

$$R_{ssh}(\tau) = \frac{1}{Tc}\int_0^{Tc} s(t)sh(t+\tau)dt.$$

Числовым параметром, характеризующим степень близости сигналов $s(t)$ и $sh(t)$, является коэффициент корреляции r_{ssh}:

$$r_{ssh} = M\left(\left[\frac{s(t)-M[s(t)]}{\sigma_s}\right]\right)\left(\left[\frac{sh(t)-M[sh(t)]}{\sigma_{sh}}\right]\right), \qquad (4)$$

где σ_s и σ_{sh} – дисперсии сигналов $s(t)$ и $sh(t)$, соответственно.

Таким образом, коэффициент корреляции r_{ssh}, рассчитанный на интервале времени T_c, можно представить как ПК передачи РС по каналу связи с аддитивным шумом.

Анализ эффективности сигналов аддитивного маскирования.

Анализ эффективности маскировки РС целесообразно провести для двух вариантов идентификации сообщений:

- биологического передатчика и приемника;
- корреляционного алгоритма обработки тестового сигнала $s(t)$ и принятого сигнала $sh(t)$.

В первом варианте идентификации при канальном маскировании должны учитываться биологические свойства слуха: предмаскировка, постмаскировка, нелинейность, пороги слышимости и динамический диапазон. С учетом этих свойств слуха маскирующий сигнал с равномерной вероятностью распределения плотности мощности является оптимальным, что доказано многочисленными исследованиями и экспериментами [3]. Однако следует обратить внимание на свойство адаптации слуха (тренировки артикуляционной бригады), которое заключается в улучшении всех видов разборчивости при многократном повторении эксперимента при неизменной методике испытаний [6].

Во втором варианте идентификации, который предполагает синхронную корреляционную обработку сигналов $s(t)$ и $sh(t)$, алгоритм которой приведен в первой части данного раздела, маскирующий сигнал с параметрами «белого» шума является неэффективным, т. к. он отфильтровывается при расчете АКФ сигнала $R_{shsh}(\tau)$.

Рассмотрим выражение оценки АКФ:

$$R_{shsh}(\tau) = \frac{1}{Tc}\int_0^{Tc}[s(t)+h(t)][s(t+\tau)+h(t+\tau)]dt = R_{ss}(\tau)+R_{hh}(\tau)+R_{ssh}(\tau)+R_{shs}(\tau), \qquad (5)$$

где АКФ и ВКФ, входящие в правую часть выражения (5), определяются в соответствии с (3). Для стационарного случая ВКФ $R_{ssh}(\tau)$ и $R_{shs}(\tau)$ равны между собой. В связи с тем, что по условию сигналы $s(t)$ и $h(t)$ независимы, в идеальном случае их ВКФ равны 0.

Таким образом, параметром качества маскирования можно определить корреляционное отношение сигнал/шум RSN:

$$RSN = \frac{\sqrt{\int_0^{Tc} R^2_{ss}(\tau)dt}}{\sqrt{\int_0^{Tc}[R^2_{hh}(\tau) + R^2_{ssh}(\tau) + R^2_{shs}(\tau)]dt}} \cdot \quad (6)$$

Этот параметр чувствителен:

- к энергетическим характеристикам (мощности) шума $h(t)$;
- к уровню статистической связи сигналов шума $h(t)$ и РС s(t).

Данные выводы подтверждают результаты исследований с маскирующим сигналом «речевой хор» [1].

IV Результаты экспериментов

Методика эксперимента.

Анализ сигналов проводился на персональном компьютере, который оснащен звуковой картой SB Audigy 2, диапазоном квантования 16 бит и частотой дискретизации f_s=48 кГц, отношением сигнал/шум порядка 80 дБ. В качестве РС s(t) анализировалось контрольное слово «акула» (сигнал s(t)), которое содержит гласные и согласные, а также вокализованные и невокализованные фонемы. Контрольное слово поизносилось мужским голосом. Программирование алгоритма корреляционной обработки производилось в среде пакета программ MathLab 6.5. Параметр сегментации сигнала s(t) на временные отрезки соответствовал слоговой постоянной времени T_c =21ms, т. о. количество дискретных отсчетов на интервале стационарности T_c составляет n=1024. Свойство центрированности реализации обеспечивается формой РС, симметричной относительно нуля. Интервал дискретизации $1/f_s$=20mks значительно меньше максимального интервала корреляции $1/2\omega_в$ сигнала s(t), что позволяет утверждать о состоятельности выборочных оценок математических ожиданий и дисперсий, рассчитываемых при анализе.

Корреляционные интегралы (3) и коэффициент корреляции (4) рассчитывались стандартными процедурами пакета MatLab. Параметр корреляционного отношения сигнал/шум RSN рассчитывался на интервалах T_c по выражению, исключающему при суммировании первые значения АКФ, равные дисперсии сигналов:

$$RSN = \frac{\sqrt{\sum_{i=2}^{n} R^2_{ss}(\tau)}}{\sqrt{\sum_{i=2}^{n}[R^2_{hh}(\tau) + R^2_{ssh}(\tau) + R^2_{shs}(\tau)]}} \quad (7)$$

В качестве сигнала $h(t)$ со спектральной плотностью мощности «белого» шума формировался массив значений стандартной процедурой пакета MatLab. В качестве речеподобного сигнала шума $h(t)$ применялся сигнал, сформированный из нескольких случайных речевых сигналов.

Пред проведением анализа задавалось отношение сигнал/шум S/N с постоянной интегрирования, равной длительности контрольного слова, рассчитанное по общепринятой методике. Маскировка сигнала $sh(t)$ выполнялась на интервале длительности контрольного слова в соответствии с выражением (2). Для проведения корреляционного анализа сигнал $sh(t)$ сегментировался на m временных интервалов длительностью T_c в соответствии с выражением (1). На каждом интервале рассчитывались точечные оценки корреляционного отношения сигнал/шум RSN (7) и коэффициента корреляции r_{ssh} (4). В связи с тем, что точечные оценки исследуемых параметров имеют m значений и изменяются на длительности контрольного слова (сигнала s(t)), их результирующие значения определялись как средние m точечных оценок параметров.

Результаты эксперимента

В процессе эксперимента исследовались зависимости средних значений корреляционного отношения сигнал/шум $M[RSN(m)]$ и коэффициента корреляции $M[r_{ssh}(m)]$ от отношения сигнал/шум S/N для

двух вариантов аддитивного сигнала шума $h(t)$: «белый» шум и речеподобный шум.

На рис. 1 и 2 приведены результаты работы программы анализа: на рисунке 1 для сигнала $h(t)$ – «белый» шум, на рис. 2 – речеподобный шум. На левых верхних фрагментах рисунков приведена временная диаграмма контрольного слова «акула» (сигнал s(t)), на правых верхних фрагментах сигнал $sh(t)$ с указанием интегрального значения отношения сигнал/шум S/N. На левых нижних фрагментах помещены графики зависимостей точечных оценок коэффициента корреляции r_{ssh} от номера m интервала длительностью T_c с указанием среднего значения $M[r_{ssh}(m)]$. На правых нижних фрагментах приведены графики зависимостей точечных оценок корреляционного отношения сигнал/шум RSN от номера m интервала длительностью T_c с указанием значения $M[RSN(m)]$.

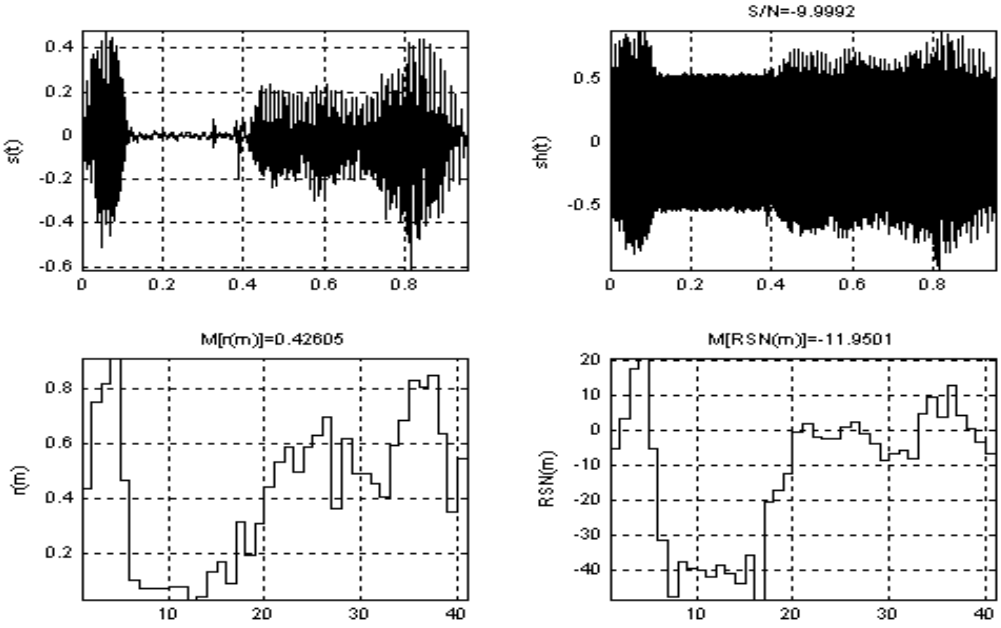

Рисунок 1 – Графики исследования корреляционных параметров аддитивного зашумления сигналом «белый» шум с отношением сигнал/шум S/N =-10дБ

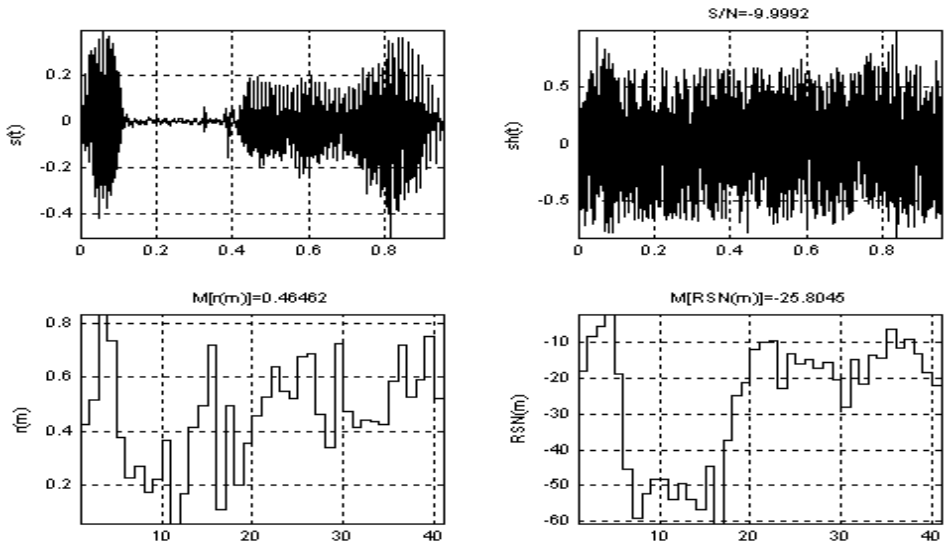

Рисунок 2 – Графики исследования корреляционных параметров аддитивного зашумления сигналом речеподобный шум с отношением сигнал/шум S/N =-10дБ

На рис. 3 и 4 приведены зависимости средних значений точечных оценок коэффициента корреляции $M[r_{ssh}(m)]$ (рис. 3) и корреляционного отношения сигнал/шум $M[RSN(m)]$ (рис. 4) от отношения сигнал/шум S/N при диапазоне изменения последнего от 40дБ до 30дБ с шагом 5дБ. Зависимости исследовались для двух сигналов шумов: «белый» шум и речеподобный шум.

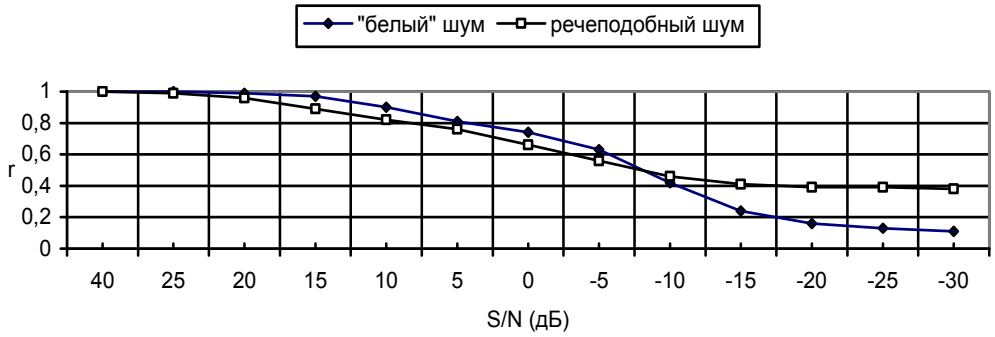

Рисунок 3 – Графики зависимостей средних значений точечных оценок коэффициента корреляции $M[r_{ssh}(m)]$ (на рисунке идентификатор r) от отношения сигнал/шум S/N

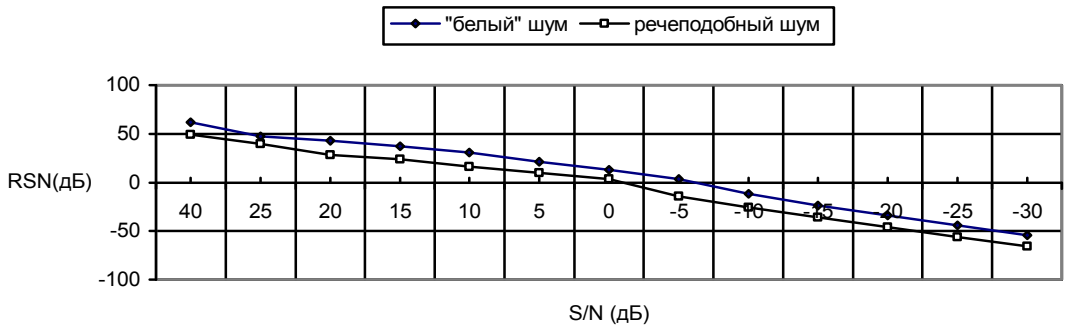

Рисунок 4 – Графики зависимостей средних значений точечных оценок корреляционного отношения сигнал/шум $M[RSN(m)]$ (на рисунке идентификатор RSN) от отношения сигнал/шум S/N

Анализ результатов эксперимента

Анализ рис. 1 и 2 позволяет сделать следующие выводы. Анализ рисунков 1 и 2 позволяет сделать следующие выводы.

1. При маскирующем сигнале «белый» шум наблюдается синхронное изменение значения коэффициента корреляции $r_{ssh}(m)$ и параметра корреляционного отношения сигнал/шум $RSN(m)$, что говорит о тесной связи данных параметров.
2. При маскирующем сигнале «речевой хор» наблюдается несинхронное изменение значения коэффициента корреляции $r_{ssh}(m)$ и параметра корреляционного отношения сигнал/шум $RSN(m)$, что говорит о менее тесной связи данных параметров, а, значит, о более высокой эффективности данного маскирующего сигнала.
3. Вокализованные гласные фонемы («а» и «у») обладают большей помехоустойчивостью по сравнению с вокализованными согласной («л»). Эффективность маскирования гласных и согласных фонем выше у сигнала «речевой хор», чем у сигнала «белый» шум.

Анализ рисунков 3 и 4 позволяет сделать следующие выводы.

4. При изменении отношения сигнал/шум S/N от 40дБ до -5дБ функция коэффициента корреляции $M[r_{ssh}(m)] = f(S/N)$ монотонно убывает для обоих типов шума. Эффективность маскирования по коэффициенту корреляции выше у сигнала «речевой хор» на постоянную величину (порядка 0.1).

5. При изменении отношения сигнал/шум S/N от 5дБ до 30дБ наблюдается качественное изменение поведения функции коэффициента корреляции $\mathrm{M}[\mathrm{r_{ssh}}(\mathrm{m})] = \mathrm{f}(\mathrm{S}/\mathrm{N})$:

- для маскирующего сигнала «речевой хор» функция коэффициента корреляции на участке –5дБ, –15дБ как бы «входит в насыщение» и в дальнейшем, при уменьшении отношения S/N не изменяется. Это объясняется существенным отличием от 0 составляющей смешанного корреляционного момента сигналов $s(t)$ и $h(t)$ в числителе выражения (4), что может быть интерпретировано как невозможность полного разделения информационной и шумовой составляющих в зашумленном сигнале;
- для маскирующего сигнала «белый» шум функция коэффициента корреляции на участке от – 5дБ, до – 30дБ монотонно нелинейно спадает, что, по нашему мнению, означает присутствие информационной составляющей контрольного слова в зашумленном сигнале и возможности его идентификации в аддитивной смеси сигнал плюс шум.

6. При изменении отношения сигнал/шум S/N от 40дБ до – 30дБ функции корреляционного отношения сигнал/шум $\mathrm{M}[\mathrm{RSN}(\mathrm{m})] = \mathrm{f}(\mathrm{S}/\mathrm{N})$ монотонно убывают для обоих типов шума.

7. Линейность изменения и приблизительно постоянная разница (порядка 12 дБ) между значениями функций, по нашему мнению, означает:

- предложенное корреляционное отношение сигнал/шум $\mathrm{M}[\mathrm{RSN}(\mathrm{m})]$, определяемое выражением (7), является состоятельным параметром маскирования;
- эффективность маскирующего сигнала «речевой хор» выше, чем сигнала «белый» шум приблизительно на 12 дБ RSN.

V Выводы

1. Предложенный и исследованный аналитический корреляционный параметр качества $\mathrm{r_{ssh}}$, определяемый в соответствии с выражением (4), является мерой содержания РС в маскированном сигнале.
2. Приведенный анализ эффективности сигналов аддитивного маскирования РС позволяет сделать вывод о состоятельности предложенного корреляционного отношения сигнал/шум $\mathrm{M}[\mathrm{RSN}(\mathrm{m})]$, определяемого в соответствии с выражением (7) как критерия качества маскирования, и позволяет предположить, что эффективность помехи речеподобный шум в сравнении с сигналом «белый» шум выше по предложенному критерию приблизительно на 12 дБ.
3. Отсутствие информационной составляющей РС в маскированном сигнале наблюдается для шума речеподобный шум при значении $\mathrm{M}[\mathrm{RSN}(\mathrm{m})] = -36\mathrm{dB}$.
4. При маскировании сигналом «белый» шум, информационные составляющие РС содержатся вплоть до $\mathrm{M}[\mathrm{RSN}(\mathrm{m})] = -54\mathrm{dB}$
5. Соотношение между полученным параметром ПК и общепринятыми параметрами разборчивости можно проверить проведением артикуляционных испытаний по стандартной методике [6].

Литература: ***1.*** *Бортников А. Н., Губин С. В., Комаров И. В., Майоров В. И. Результаты экспериментальной оценки эффективности защиты речевой информации от утечки по техническим каналам при использовании различных видов помех.// Информация и безопасность. – Воронеж, 1999. – Выпуск № 4.* ***2.*** *Иванов В. М., Хорев А. А. Способ и устройство формирования "речеподобных" шумовых помех// Вопросы защиты информации. – М.: 1999. – № 4.* ***3.*** *Цвикер Э., Фельдкеллер Р. Ухо как приемник информации. /Пер. с нем. под ред. Б. Г. Белкина – М.: Связь, 1971. – 225 с.* ***4.*** *НД ТЗІ – Р – 001 – 2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. НД ТЗІ – Р – 001 – 2000. ДСТСЗІ СБ України. – Київ.: - 2000. – 9 с.* ***5.*** *Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации// Специальная техника. – М.: 2000.– № 4.* ***6.*** *ГОСТ Р 50840-95. Государственный стандарт Российской Федерации. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. Издание официальное. – М.: Госстандарт России, 1997.*