УДК 681.5.015: 004.056.57

Маракова И.И., Комендантов И.И., Сыропятов А.А.
Marakova I.I., Komendantov I.I., Syropjatov A.A.

МОДЕЛИРОВАНИЕ СИСТЕМЫ С ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ ПРИ ОСНОВНОМ СООБЩЕНИИ В ВИДЕ РЕЧЕВОГО СИГНАЛА

WATERMARKING SYSTEM MODELING WITH SPEECH SIGNAL AS COVER MESSAGES

Аннотация. Разработана модель секретной системы с цифровыми водяными знаками при основном покрывающем сообщении в виде речевого сигнала. При формировании стеганографического сигнала учитывались психофизические особенности восприятия для автоматизации обеспечения надежности восприятия, косвенного повышения эффективности декодирования. Рассмотрена адаптация системы с ЦВЗ к воздействию аддитивной помехи.

Summary. Private watermarking system model with using as the cover message of audio signals have been design. During steganografic signal forming the perceptual model have been using for automation ensuring of fidelity and watermarking decoding efficiency increasing by indirection.. The watermarking system adaptation in the condition of additive noise attack are made.

На сегодняшний день технологии беспроводных сетей передачи информации являются весьма перспективными для практического применения благодаря относительно невысоким затратам на их организацию и простоте эксплуатации. Как и в любой другой системе передачи данных возникает проблема обеспечения требуемого уровня информационной безопасности. Традиционным является использование криптографических протоколов шифрования информационных потоков. Осуществление процедуры идентификации и/или верификации передаваемой информации на основе технологий сокрытия информации – цифровых водяных знаков (ЦВЗ) открывает дополнительные возможности по расширению практического применении беспроводных сетей связи [1, 2, 3]. В связи с этим, процесс обеспечения безопасности можно рассматривать не только как усложнение доступа к информационным потокам, но и как установление факта несанкционированных действий с последующим привлечением злоумышленника к ответственности при наличии соответствующей нормативно-законодательной базы.

Поиск новых средств обеспечения безопасности обусловлен уязвимостью криптографической защиты. Увеличение длины ключа шифрования, усложнение алгоритма шифрования может лишь удлинить время взлома.

Целью данной статьи и является разработка системы с ЦВЗ, которая обеспечивает требуемый уровень информационной безопасности, как одной из альтернатив криптографической защиты.

С практической точки зрения наибольший интерес представляют секретные системы с ЦВЗ, использующие в качестве секретного ключа собственно ЦВЗ. Но, прежде всего, необходимо разработать алгоритм формирования стегосигнала (ОПС и ЦВЗ). При этом сразу необходимо отметить, что формирование ЦВЗ в виде цифровой подписи ОПС позволит расширить область применения рассматриваемого подхода обеспечения информационной безопасности.

Для ОПС в виде речевого сигнала в цифровом формате можно сформировать цифровую подпись (ЦП), используя произвольные стандарты хеширования и криптографической обработки. Формирование ЦВЗ в виде ЦП ОПС производится с использованием какого-либо асимметричного стандарта, например, RSA [4]. Пусть $\{K,\ G\}$ являются открытыми ключами, а k – секретный ключ. После хеширования дайджест ОПС $h(C)$ определен на пространстве P битовых слов, т.е. $\{0,\ 1\}^P$. Некоторая функция F реализует преобразование пространства полученного дайджеста ОПС в бинарное, а функция T – инверсное преобразование. Тогда формирование ЦП SA включает следующие шаги $H_c = h(C)$, $f = F(H_c)$, $C_e = (f^k) \bmod G$, $SA = T(C_e)$ или в целом $SA = (T(F(h(C))^k) \bmod G$. Для подтверждения целостности и идентификации ОПС по полученной паре $\{C,\ SA\}$ необходимо вычислить дайджест восстановленного ОПС $h(\overset{\epsilon}{C})$, где $\overset{\epsilon}{C}$ – оценка ОПС; сформировать $\overset{\epsilon}{SA}$ полученной оценки ОПС и сравнить с SA. Совпадение $\overset{\epsilon}{SA}$ и SA подтверждает целостность сообщения. Таким образом, для процедуры идентификации и верификации на основе ЦП, погруженной в ОПС как ЦВЗ, необходимо выполнение следующих требований:

– отличие стегасообщения и ОПС не должно превышать заданный уровень в соответствии с требуемой надежностью восприятия (надежность восприятия стегаобраза определяет степень различия между исходным ОПС и стегасообщением);

– на основе стегасообщения при наличии секретного ключа в виде ЦВЗ восстановление ОПС должно характеризоваться очень высокой вероятностью.

Использование кодов, исправляющих ошибки, позволит повысить эффективность системы с ЦВЗ. Для некоторого бинарного систематического исправляющего ошибки кода $Z \in (m,\ L,\ d)$, где m – размер блока; L – число символов в алфавите; d – минимальное кодовое расстояние; b_{ij} является i-м битом j-го блока кода, причем $i = 1,\ ...,\ m$, $j = 1,\ ...,\ 2^L$. Если в ЦП всего R бит, то размер кодового блока должен быть $R_0 = R/L$. Каждый кодовый блок содержит m символов, причем для погружения одного кодового символа ЦВЗ, сформированного как ЦП ОПС, потребуется $n_o = N/R_o m = NL/Rm$ дискретов ОПС. Правило погружения j-го кодового блока:

$$s(n) = c(n) + \alpha(-1)^{b\left\lfloor \frac{n}{n_O} \right\rfloor + 1, j} w_r(n), \quad n \in A_N, \tag{1}$$

где $1 \le j \le 2^l$; α – целое число, $0 \le \alpha \le 255$; $w_r(n) = \{\pm 1\}$ – псевдослучайная последовательность (ПСП), полученная, например, с помощью линейного рекуррентного регистра сдвига.

В структуре секретной системы с неинформированным детектором, т.е. не использующим при детектировании ОПС, предполагается синхронизация приемной и передающей частей. Корреляционный детектор принимает решение о том, какое кодовое слово принято на основании определения максимального значения функционала детектора

$$\Lambda_j = \max_{0 \le j \le 2^L} \sum_{n=1}^{\frac{N}{R_0}} (s(n) - E\{C\})\alpha(-1)^{b\left\lfloor \frac{n}{n_O} \right\rfloor + 1, j} w_r(n),\ n \in A_N, \tag{2}$$

где ОПС или рассматриваемый фрагмент ОПС предполагается стационарным процессом в широком смысле.

Одной из основных проблем реализации системы с ЦВЗ, наряду с обеспечением требуемого уровня эффективности обнаружения и декодирования ЦВЗ, является обеспечение требуемого уровня надежности восприятия. Данные задачи являются взаимосвязанными и противоречащими друг другу. Использования психофизических особенностей восприятия человека для встраивания ЦВЗ позволит увеличивать параметр N, а значит и эффективность обнаружения и декодирования. Необходимо отметить, что понятие надежности восприятия стегообраза отличается от понятия качества сигнала. Если ОПС характеризуется низким качеством (например, после сжатия с потерями и т.д.), стегообраз должен всегда обладать надежным восприятием, но качеством не выше характерного для оригинала.

Построение систем с ЦВЗ с учетом перцепционной модели, т.е. учета психофизических особенностей восприятия должно обеспечить минимальное различие при сравнении экспертом стегообраза и оригинала и обеспечить возможность обойтись без экспертных оценок. Системы, которые автоматически контролируют незаметность ЦВЗ, можно выделить в подгруппу систем с адаптивным управлением надежности восприятия стегосигнала. Представляется интересным разработка метода погружения ЦВЗ с автоматическим обеспечением незаметности на основании учета ПМ.

С точки зрения надежности восприятия основными признаками аудиовосприимчивости являются частота и громкость. В общем случае ПМ основывается на эффектах маскировки и слияния, обусловленных особенностями визуальной и аудиовосприимчивости человека. Данные свойства находятся в прямой зависимости от особенностей восприятия аудио органами слуха человека. Необходимо четко определить несколько основных положений ПМ, как компромисс между ожидаемым эффектом (незаметности ЦВЗ) и сложностью практической реализации устройства формирования стегасигнала (УФС) и системы в целом.

Реакция восприимчивости человека к аудиосигналам находятся в определенной зависимости от частоты [5]. Тестирование показало, что чувствительность человека к изменению громкости повышается на СЧ, а на ВЧ и НЧ чувствительность к переходам уменьшается.

Для учета зависимости порога слышимости от частоты при построении систем с ЦВЗ и ОПС в виде речевых сигналов необходимо оценивать и учитывать параметр порога слышимости звука

$$DP = 20\log\frac{P}{P_o}, \tag{3}$$

где P – давление источника звука в паскалях; $P_o = 20$ пск – учитывает звуковой фон.

Полученный эмпирически график зависимости (3) иллюстрирует наивысшую чувствительность на 3 кГц, которая ухудшается к очень низким (20 Гц) и особенно очень высоким частотам (10 кГц). Таким образом, учитывая, что вносимые при погружении ЦВЗ изменения ОПС будут менее заметны на высоких уровнях громкости и в зависимости от частотного диапазона, представляется возможным осуществлять частотную маскировку по громкости, что является первой компонентой комплексного учета ПМ для обеспечения незаметности ЦВЗ (более громкие фрагменты ОПС предпочтительнее для погружения ЦВЗ, так как изменения будут менее заметны).

После анализа абсолютного уровня слышимости необходимо выполнить анализ относительного уровня слышимости, т.е. с учетом эффектов маскировки. Для того чтобы получить порог относительной слышимости, прежде всего необходимо представить сигнал в виде окон или фреймов в соответствии со спектральной моделью слуховой системы человека [6]. Эмпирически получено, что в некотором приближении «канал» слухового восприятия можно моделировать линейкой фильтров с перекрывающимися частотными характеристиками разными полосами пропускания. Если рассмотреть узкополосный источник шума на минимально слышимом уровне громкости и его полосу увеличивать, то при достижении некоторого значения увеличиваемой полосы пропускания первоначального уровня громкости будет не достаточно для слышимости.

Таким образом, после разделения ОПС на M фреймов C_m, $m = 1,\ldots M$, перехода в частотную область, например, на основе ДПФ полученные частотные коэффициенты анализируются с точки зрения наличия критических полос, т.е. выявляются частотные полосы, определяются энергетические параметры и характер каждой полосы (шум или тон). Порог относительной слышимости для каждого окна/фрейма является функцией энергии и зависит от характера фрейма (шум или тон). Порог слышимости зависит не только от уровня энергии в текущей частотной полосе, но и от уровня энергии в соседних полосах. Итак, при определении порога относительного уровня слышимости для каждой частотной составляющей ОПС необходимо: определить энергию для каждой критической полосы; определить «мнимую» энергию в каждой критической полосе в следствии влияния соседних; определить характер полосы (шум или тон); определить порог маскировки.

Энергия в каждой критической полосе

$$\Psi(r) = \sum_{f_{\min}}^{f_{\max}} |c(f)|, \tag{4}$$

где $f_{\min}, f_{\max}$ – минимальная и максимальная частоты критической полосы, r; r – номер критической полосы; $|c(f)|$ – амплитуды гармоник спектра в рассматриваемой критической полосе для исследуемого аудиосигнала.

Распределение энергии по критическим полосам моделируется основной мембранной функцией распространения [5]

$$RF(r) = 15{,}81 + 7{,}5(r + 0{,}474) - 17{,}5\sqrt{1 + (r + 0{,}474)^2}\ . \tag{5}$$

Полная энергия в некоторой критической полосе

$$\Psi_{\Sigma}(r) = \sum_{r'=r-r_0}^{r+r_1} \Psi(r - r')RF(r')\ , \tag{6}$$

где r_0, r_1 – номера соседних критических полос, для которых (6) превышает заданный порог.

С другой стороны, если две тоновые составляющие звучат одновременно, то одна может стать не различимой, если их частоты находятся в одной критической полосе и $DP_1 < DP_2$. Кроме того, если частотная составляющая попадает в полосу, удаленную от центральной частоты полосы более чем на 20%, то ее амплитуда резко уменьшается. **А**налитическая оценка критической полосы [5]

$$\Delta_{\text{кр}}(f) = 25 + 75\left[1 + 1{,}4\left(10^{-3} f\right)^2\right]^{0{,}69}. \tag{7}$$

Свойства чувствительности и маскировки могут использоваться как составляющие ПМ при погружении ЦВЗ на одной частоте. Если же ЦВЗ являются коррелированным процессом и содержат несколько частотных составляющих, то анализ необходимо выполнять на всех частотах ЦВЗ.

Характеристика, называемая слиянием, оценивается статистическим параметром, который называется нормой Минковского [5, 6]

$$L_d(\mathrm{C},\mathrm{S}) = (\sum_i \left| P(i)^d \right|)^{\frac{1}{d}}, \tag{8}$$

где C, S– ОПС и стегасигнал, соответственно; $P(i)$ – вероятность того, что эксперт заметит разницу при оценке по определенным параметрам, фрагментам; i = 1,… I – число отличий ОПС и стегасообщений; d = 1 … 4 – рекомендуемая константа [5].

При анализе эффекта маскировки необходимо разделять маскировку тоновой составляющей шумом (рис. 1,а) и маскировку шума тоновой составляющей (рис. 1,б). Возможна так же маскировка одного узкополосного шума другим, что, однако, весьма трудно оценить количественно и потому данный эффект ПМ не будет учитываться.

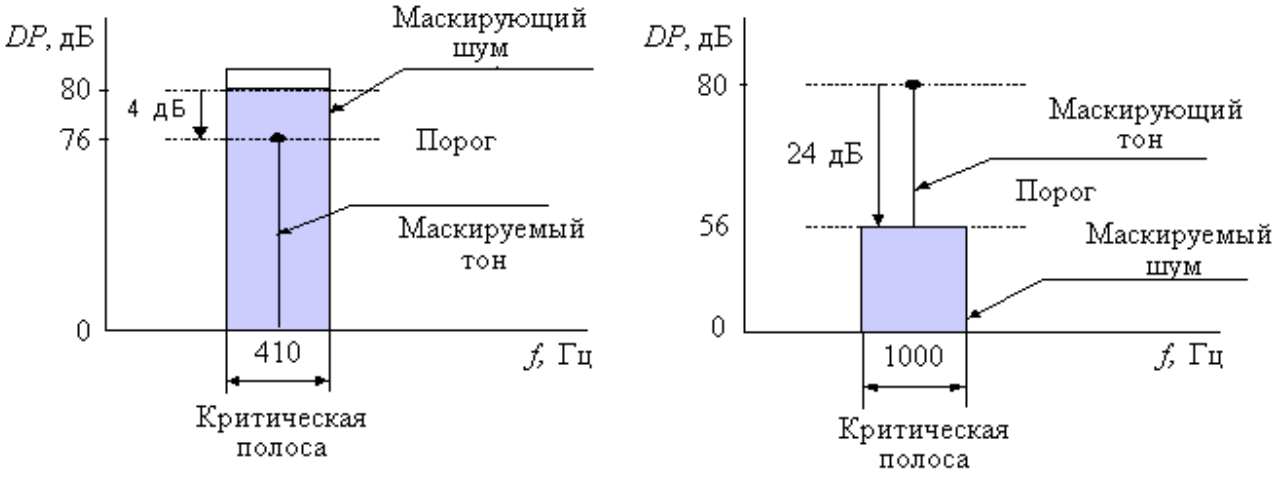

Рисунок 1 – Пример эффекта маскировки за счет чувствительности к окружению тональной составляющей шумом (а), шума тональной составляющей (б)

Таким образом, эффект маскировки зависит не только от энергии в критической полосе, но и от спектральной меры монотонности [5]

$$SM = 10\log_{10}\left[\frac{\left[\prod_{r=1}^{r=r\max} \Psi_\Sigma(r)\right]^{\frac{1}{r_{\max}}}}{\frac{1}{r_{\max}}\sum_{r=1}^{r=r_{\max}} \Psi_\Sigma(r)}\right]. \tag{9}$$

Исходя из спектральной меры монотонности можно оценить коэффициент тональности

$$\alpha_\mathrm{T} = \min(\frac{SM}{-60},1). \tag{10}$$

Если $\alpha_\mathrm{T} = 1$, то составляющая является тональной, если меньше, то шумом. Эмпирически показано, что порог маскировки критической полосы в дБ можно оценить формулой $t(r) = 10\log_{10} IF(r) - \{\alpha_\mathrm{T}(14{,}5 + r) + (1 - \alpha_\mathrm{T})5{,}5\}$ или в паскалях $t(r) = 10^{O(r)\frac{r}{10}}$, где $O(r) = \{\alpha_\mathrm{T}(14{,}5 + r) + (1 - \alpha_\mathrm{T})5{,}5\}$. Для принятия решения о том, насколько какая-либо частота внутри критической полосы может быть изменена, значение порога $t(r)$ в паскалях нормализуется $t_n(r) = \frac{t(r)}{N_{fr}}$, где N_{fr} – число гармоник в критической полосе.

Устройство формирования сигнала с учётом ПМ показано на рис. 2.

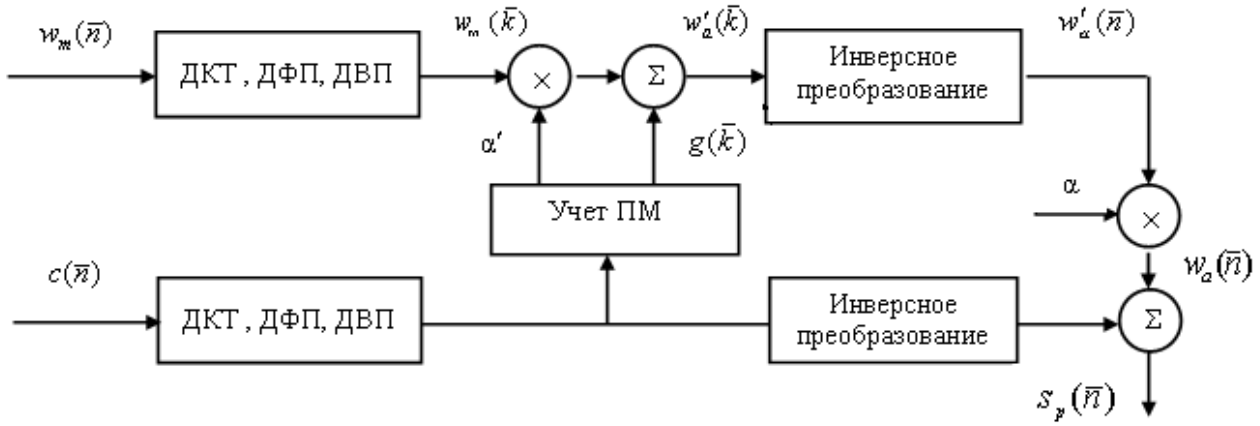

Рисунок 2 - Структура устройства формирования стегосигнала с учетом ПМ

Таким образом, масштабирование ЦВЗ с учетом ПМ (рис. 2) при рассмотрении без потери общности системы с двумя информационными битами

$$w_a(n) = \alpha(\alpha' w_m(n) + g(n)),\ n \in A_N, \qquad (11)$$

где α – скаляр, определяемый в соответствии с ПМ; α' – начальное значение амплитуды ЦВЗ, $\alpha' = \text{const}$, например, $\alpha' = 1$; $g(n) \in G$ – вектор, ортогональный $w_m(n) \in \mathrm{W}_m$, $|w_m| = 1$, который можно рассматривать в качестве маски, с помощью которой достигается наилучшее решение учета ПМ для нахождения указанного ранее компромисса.

Погружая вектор $\mathrm{W_a}$ в ОПС можно ожидать большего значения функционала ЛКД по сравнению со значением функционала при погружении W_m. С другой стороны, становится возможным увеличить энергию $\mathrm{W_a}$, контролируя надежность восприятия стегосигнала. Если при обычном формировании стегосообщения $s(n) = c(n) + \alpha' w_m(n)$, $n \in A_N$, и при наличии ЦВЗ функционал детектора $\Lambda_1 = f(s(n), w_m(n)) = \frac{1}{N}\sum_{\overline{n} \in A_N}(c(n) + w_m(n))w_m$, $n \in A_N$, то с учетом ПМ $s_p(n) = c(n) + \alpha(\alpha' w_m(n) + g(n))$, $n \in A_N$ и функционал ЛКД при наличии ЦВЗ определиться как

$$\Lambda_1' = f(s_p(n), w_m(n)) = \frac{1}{N}\sum_{n \in A_N}(c(n) + \alpha' w_\alpha(n))w_m = \frac{1}{N}\sum_{n \in A_N}(c(n) +$$

$$+ \alpha'\alpha w_m(n) + \alpha g(n))w_m(n) = \frac{1}{N}\sum_{n \in A_N}(c(n) + \alpha(\ \alpha' w_m(n) + g(n)))w_m(n),$$

откуда $\Lambda_1 = f(s(n), w_m(n)) < \Lambda_1' = f(s_p(n), w_m(n))$, $n \in A_N$.

На основании выше изложенного можно отметить, что модель погружения ЦВЗ с автоматическим обеспечением незаметности на основании контроля энергетического порога (анализ чувствительности) весьма проста. Однако наилучшего результата следует ожидать при комплексном учете составляющих ПМ: чувствительности, маскировки и слияния, т.е. оценки (3)–(10). Число частотных каналов, комплексность ПМ определяется с учетом особенностей решаемых задач с помощью системы с ЦВЗ, что определяет сложность технической реализации (рис. 3).

Адаптация полученной модели формирования стегосигнала с учетом ПМ к преобразованиям в канале обработки и атаки еще более усложнит реализацию устройства формирования стегосигнала. Если стегосигнал подвергается только воздействию аддитивного шума, интенсивность которого β определена с точки зрения сохранения надежности восприятия, то для выполнения условия $1/N \sum_{\overline{n} \in A_N} c(\overline{n}) w_m(\overline{n}) \geq \lambda + \beta$, где λ – заданные в соответствие с требуемой эффективностью детектирования ЦВЗ порог детектора, с которым сравнивается функционал (2), в УФС достаточно

обеспечивать постоянство функционала Λ, для чего возможно использование двух походов. В рамках первого в ОПС отыскиваются такие дискреты $c_{fix}(n')$, которые обеспечивают выполнение условия Λ = const при заданном значении α, удовлетворяющем

$$\alpha = \frac{N_{fix}(\lambda+\beta) - \sum\limits_{n' \in A_n} c_{fix}(n') w_m(n)}{\sum\limits_{n \in A_n} w_m(n) w_m(n)}, \; n \in A_N .$$

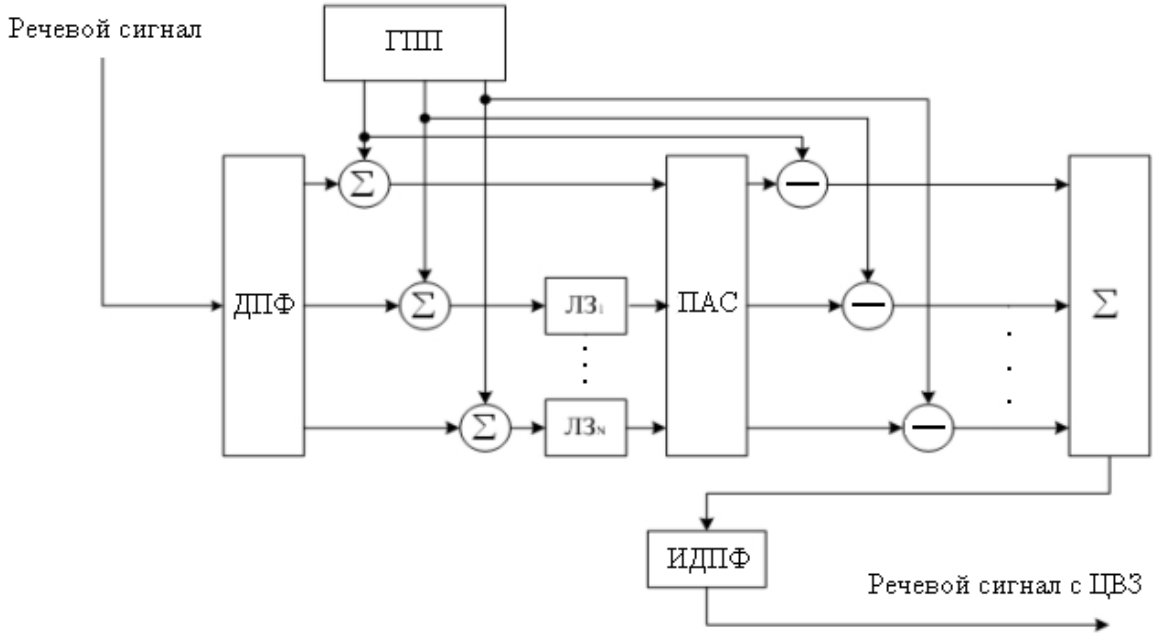

Рисунок 3 - Схема формирования стегосообщения с учетом ПМ:

ГПП – генератор ПСП $\{\pm\alpha\}$; ИДФП – инверсное ДФП; $ЛЗ_n$ – линия задержки на n тактов;
ПАС – перцепционный анализатор спектра

Другим подходом может стать использование адаптивных значений $\alpha(n)$. Для погружения ЦВЗ в случайные дискреты ОПС массив амплитуд ЦВЗ

$$\alpha(n) = \frac{(\lambda+\beta(n)) - c(n) w_m(n)}{w_m(n) w_m(n)}, \; n \in A_N .$$

В заключение следует отметить, что комплексный учёт ПМ в реальном масштабе времени, достаточно сложная задача даже при современном уровне развития вычислительной техники, поэтому после определения особенностей практического применения системы с ЦВЗ, необходимо ограничивать количество критериев.

Литература

1. *Маракова И.И., Сафронов А.С.* Проблематика и перспективы методов сокрытия информации// Тр. Одесск. нац. политехн. ун-та. – 2003. – Вып.1. – С. 184–188.
2. *Bassia P., Pitas I.* Robust Audio Watermarking in the Time Domain – EUSIPCO. – Vol.1 – Rodos, Greece. – 1999. – P. 177–183.
3. Secure Spread Spectrum Watermarking for Images, Audio and Video / *I. Cox, J. Kilian, F.T. Leighton, T. Shamoon* // IEEE Int. Conference on Image Processing. – Vol. 3. –1996. – P. 243–246.
4. *Маракова І.І., Рибак А.І., Ямпольський Ю. С.* Захист інформації. − Кіровоград: Полімед, 2001. − 189 с.
5. *Painter T., Spanias A.* Perceptual Coding of Digital Audio // Proceedings of the IEEE. – 2000. – Vol. 88(4). – P. 413–451.
6. *Moore B.C.J.* Masking in the human auditory system // Collected Papers on Digital Audio Bit-Rate Reduction. – 1996. – P. 9–19.