**Лекция 10**. *Расчет вероятности ошибки для ЦВЗ-УШПС:*

*Основная идея УШПС* – уменьшить влияние ПС, как помехи, на результат «слепого» декодирования

*Погружение:*

$$C_w(n) = C(n) + \left(\beta(-1)^b - \lambda x\right)\pi'(n), n = 1,2...N \tag{22}$$

где $\beta, \lambda$ – некоторые постоянные

$$x = (C,\pi') = \frac{1}{N\alpha^2}\sum_{n=1}^{N} C(n)\pi'(n), \pi'(n) = \alpha\pi(n) \tag{23}$$

*Частный случай:*

$$\lambda = 0, \beta = 1 \Rightarrow C_w(n) = C(n) + \alpha(-1)^b \pi(n) \text{ (ообычно ШПС)}$$

*Атака аддитивным шумом:*

$$C'_w(n) = C_w(n) + \varepsilon(n),$$

$$\text{где } E\{\varepsilon(n)\} = 0, Var\{\varepsilon(n)\} = \sigma_\varepsilon^2 \tag{24}$$

*Правило слепого декодирования:*

$$\Lambda = \frac{1}{N\alpha^2}\sum_{n=1}^{N} C'_w \pi'(n) \Rightarrow \begin{cases} b = 0, \text{если} \Lambda \geq 0 \\ b = 1, \text{если} \Lambda < 0 \end{cases} \qquad (25)$$

Подставляя (22) и (24) в (25) получим:

$$\Lambda = x + \beta(-1)^b - \lambda x + y = \beta(-1)^b + (1-\lambda)x + y, \qquad (26)$$

где $y = \dfrac{1}{N\alpha^2}\sum_{n=1}^{N} \varepsilon(n)\pi'(n)$

Если *λ*=1, то помеха от *C(n)* будет отсутствовать, но это не означает, что *λ*=1 является оптимальной величиной, если принять во внимание искажения ПС после погружения ЦВЗ.

## *Искажения при погружении ЦВЗ*

$$\mathit{\Delta} = E\{\left(C_w(n) - C(n)\right)^2\} = E\left\{\left(\left(\beta(-1)^b - \lambda\frac{\tilde{x}}{\alpha^2}\right)\pi'(n)\right)^2\right\} = \alpha^2 E\left\{\left(\beta(-1)^b - \frac{\lambda}{\alpha^2}\right)^2\right\} =$$

$$= \alpha^2 E\{\beta^2 - \frac{2\beta\lambda\tilde{x}(-1)^b}{\alpha^2} + \frac{\lambda^2}{\alpha^4}x^2\} = \alpha^2\left(\beta^2 + \frac{\lambda^2}{\alpha^4}E\{\tilde{x}^2\}\right), \qquad (27)$$

где $\tilde{x} = \frac{1}{x}\sum_{n=1}^{N} C(N)\pi'(n)$

Преобразуем последний член в (27):

$$E\{\tilde{x}^2\} = E\{\frac{1}{N}\sum_{n=1}^{N} C(n)\pi'(n)\} = \frac{1}{N^2}\sum_{n=1}^{N}\sum_{n'=1}^{N} E\{C(n)C(n')\pi'(n)\pi'(n')\} =$$

$$\frac{1}{N^2}\sum_{n=1}^{N}\sum_{n'=1}^{N} E\{C(n)C(n')\}E\{\pi(n)\pi'(n')\} = \frac{N}{N^2}\alpha^2\sigma_c^2 = \frac{\alpha^2\sigma_c^2}{N} \qquad (28)$$

Подставляя (28) в (27) получим:

$$\mathit{\Delta} = \alpha^2\left(\beta^2 + \frac{\lambda^2\sigma_c^2}{N\alpha^2}\right) = \alpha^2\beta^2 + \frac{\lambda^2\sigma_c^2}{N} \qquad (29)$$

Найдем параметр УШПС $\beta$, при котором искажения ПС при погружении $\Delta$ равны искажениям при погружении обычным ШПС $\Delta = \alpha^2$ :

$$\alpha^2 = \alpha^2 \beta^2 + \frac{\lambda^2 \sigma_c^2}{N} \Rightarrow \beta = \sqrt{\frac{N\alpha^2 - \lambda \sigma_c^2}{N\alpha^2}} \qquad (30)$$

Рассчитаем вероятность ошибки в ЦВЗ-УШПС:

$$p = Q\left( \frac{\left| E\{\Lambda\{ \right|}{\sqrt{Var\{\Lambda a}} \right) \qquad (31)$$

$$E\{\Lambda\{ = E\{\beta(-1)^b + (1-\lambda)x + y\} = \beta(-1)^b \qquad (32)$$

$$Var\{\Lambda\} = E\{ ((1-\lambda)x + y)^2 \} = E\{ (1-\lambda)^2 x^2 + 2(1-\lambda)xy + y^2 \} = (1-\lambda)^2 E\{x^2\} + E\{y^2\} \qquad (33)$$

$$E\{x^2\} = \frac{\sigma_c^2}{\alpha^2 N} \qquad (34)$$

$$E\{y^2\} = \frac{\sigma_\varepsilon^2}{\alpha^2 N} \qquad (35)$$

Подставляя (34),(35) в (33), получим:

$$Var\Lambda = \frac{(1-\lambda)^2 \sigma_c^2 + \sigma_\varepsilon^2}{\alpha^2 N} \qquad (36)$$

Подставляя (30) в (32), (32), (36) в (31) получим:

$$P = Q\left(\sqrt{\frac{N\alpha^2 - \lambda\sigma_c^2}{\left(1-\lambda^2\right)\sigma_c^2 + \sigma_\varepsilon^2}}\right) \tag{37}$$

Частный случай *λ*=0 (обычная ЦВЗ-ШПС)

$$\tilde{P} = Q\left(\sqrt{\frac{N\alpha^2}{\sigma_c^2 + \sigma_\varepsilon^2}}\right) = Q\left(\sqrt{\frac{N\eta_a}{\eta_a\eta_\omega + \eta_\omega - \eta_a}}\right) \approx Q\left(\sqrt{\frac{N}{\eta_\omega}}\right) \tag{38}$$

Что совпадает с (9) (см лекцию 9)

Для получения минимума *P* в (37) параметр *λ* должен быть оптимизирован.

Легко проверить, что когда $\sigma_c^2 / \sigma_\varepsilon^2$ и *N* велико, то $\lambda_{opt} \approx 1$

Тогда получаем из (37)

$$P = Q\left(\sqrt{\frac{N\alpha^2 - \sigma_c^2}{\sigma_\varepsilon^2}}\right) = Q\left(\alpha\sqrt{\frac{N - \eta_\omega}{\sigma_\varepsilon^2}}\right) = Q\left(\sqrt{\frac{\eta_a\left(N - \eta_\omega\right)}{\eta_\omega - \eta_a}}\right) \tag{39}$$

## Сравнение ЦВЗ-ШПС и ЦВЗ-УШПС

Преобразуем (39)

$$P = Q\left(\sqrt{\frac{N-\eta_\omega}{\eta-1}}\right) \tag{40}$$

где $\eta = \dfrac{\eta_\omega}{\eta_a}$

Сравним (40) с вероятностью ошибки для информированного декодера (см. 11 в лекции):

$$P = Q\left(\sqrt{\frac{N}{\eta-1}}\right) \tag{41}$$

Видно, что при $N \gg \eta_\omega$ получаем (приближенное равенство) *P* для ШПС с информированным декодером и УШПС со «слепым» декодером

**Пример:**

$$\sigma_c = 50, \alpha = 5, \sigma_\varepsilon = 5, N = 1000$$

тогда: $\eta_\omega = \dfrac{\sigma_c^2}{\alpha^2} = 100, \quad \eta_a = \dfrac{\sigma_c^2}{\alpha^2+\sigma_\varepsilon^2} = 50 \quad P = Q\left(\sqrt{\dfrac{N}{\eta_\omega}}\right) = Q\sqrt{10} \approx 3\cdot 10^{-3}$

Для УШПС можно получить туже вероятность ошибки, но при уменьшении *N* до 110, что эквивалентно увеличению скорости вложения в 9 раз.

## 6. Построение системы ЦВЗ на принципах, отличных от тех, которые используются в телекоммуникационных системах. (Квантованная проективная модуляция - КПМ)

*Обычная (квантованная индексная модуляция - КИМ)*

*Погружение:*

$$C_w(n) = \begin{cases} Q_0(C(n)), \text{если } b = 0 \\ Q_1(C(n)), \text{если } b = 1 \end{cases} \tag{42}$$

где $Q_i(...)$ – квантователь $i^{го}$ типа

*Декодер*:

$$\tilde{b} = argmin_b \| C'_w(n) - Q_b(C'(n)) \| \tag{43}$$

где || …|| - норма в евклидовом пространстве

**Пример (скалярный квантователь):**

(вставить рис)

Если $C'_w(n) = C_w(n)$нет искажений ЦВЗ), то информация извлекается без ошибок.

Если помехой является $\varepsilon(n) \in N(0, \sigma^2)$, то:

$$P = \sum_{n=-\infty}^{+\infty} \left( Q\left( \frac{\Delta(4n+1)}{\alpha\sqrt{\sigma_\varepsilon^2}} \right) - Q\left( \frac{\Delta(4n+3)}{\alpha\sqrt{\sigma_\varepsilon^2}} \right) \right), Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{\frac{-t^2}{2}} dt \qquad (44)$$

Атака переквантованием:

$$C'_w(n) = \begin{cases} C_w(n), \text{с вероятностью } 0{,}5 \\ C_w(n) \pm \Delta, \text{с вероятностью } 0{,}5 \end{cases}$$ *p*=0,5 (ЦВЗ удалено полностью) (45)

**Диттер КИМ (ДМ)**

*Погружение:* $C_w(n) = Q(C(n) + d(bn)) - d(b_n, n)$ (46)

*Q(…)*-квантователь с шагом «*Δ*»

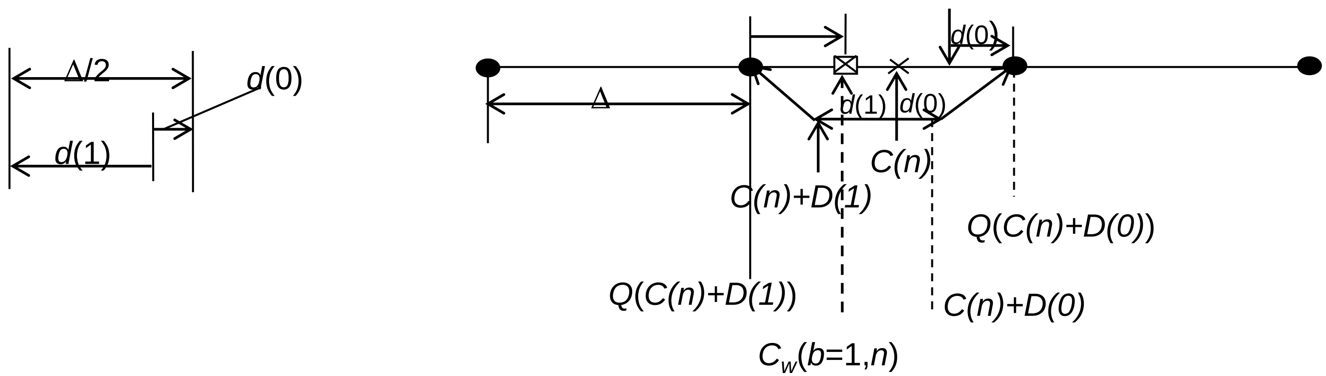
где *d(0,n) – i.i.d*., равномерно распределено на интервале [- *Δ/2,*+ *Δ/2*]

$$d(1,n) = \begin{cases} d(0,n) + \frac{\Delta}{2,} \text{ если } d(0,n) < 0 \\ d(0,n) - \frac{\Delta}{2,} \text{ если } d(0,n) \geq 0 \end{cases} \qquad (47)$$

*Декодер:*

$$\tilde{b} = argmin_b \left\| C'_w(n) - Q\left(C'_w(n) + d(b,n)\right) + d(b,n) \right\| \quad (48)$$

*Графическая иллюстрация для равномерного скалярного квантователя:*




*Основные свойства DM*

1. если $C'_w(n) = C_w(n)$, то $p = 0$

2. если $C'_w(n) = C_w(n) + \varepsilon(n)$, то $p =$ см. (44)

3. если $C'_w(n) = C_w(n) + \tilde{\varepsilon}(n)$, где $\left|\tilde{\varepsilon}(n)\right| < \dfrac{\Delta}{4}$ то $p = 0$

4. Ошибки квантования не зависят от $C(n)$,

что улучшаетсуубьективое качество восприятия

*Векторная КИМ.*

Видно, что скалярная КИМ фактически совпадает с системой НЗБ и имеет все его недостатки.

При векторной КИМ предварительно выбирается кодовая книга (из двух «томов» для вложения одного бита):

$$C_{io}(n), n = 1,2\ldots N, C_{i1}(n), n = 1,2\ldots N, i = 1,2,\ldots L$$

*Погружение:*

$$C_w(n) = \begin{cases} C_{\tilde{i}o}(n), \text{если } b = 0 \\ C_{\tilde{i}b}(n), \text{если } b = 1 \end{cases} \qquad (49)$$

где $C_{\tilde{i}b}(n) = argmin_i \left\| C_w(n) - C_{ib}(n) \right\|$

*Декодер:*

$$\tilde{b} = argmin_b min_i \left\| C'_w(n) - C_{ib}(n) \right\| \qquad (59)$$

**Замечание 1.**

Для обеспечения малых искажений ПС кодовые книги должны выбираться так, чтобы для любого $C(n)$, $||C(_w(n)-C(n)||$ ,были бы малы по сравнению с $||C(n)||$

**Замечание 2.**

Такая система может использоваться в СГС причем она будет устойчива к преднамеренному удалению, если выбор кодовых книг производится секретным образом (по стегоключу)

**Замечание 3.**

Данный метод построения ЦВЗ и СГС хорошо согласуется с *векторным кодированием* речевых сигналов, используемых в вакодерах.

## Квантованная проекционная модуляция (QPD)

*Цель использования QPD:*

Обеспечить защиту от преднамеренного удаления ЦВЗ методом рандомизированного квантования.

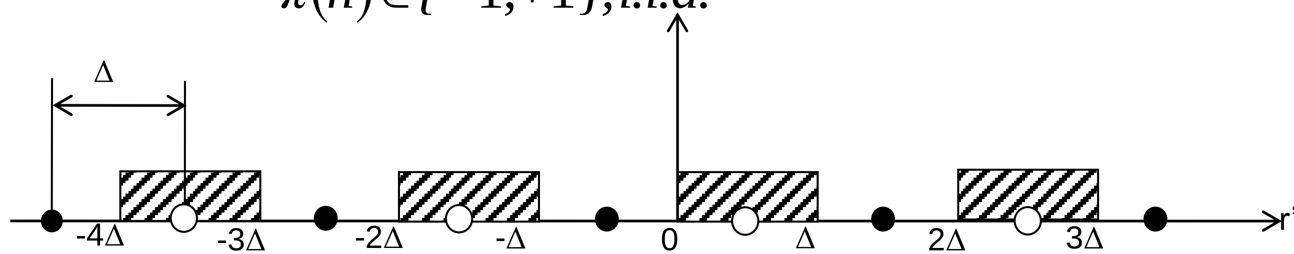
*Погружение:*

$$C_w(n) = C(n) + \frac{Q_b(r) - r}{N}\pi(n), n = 1,2,...,N \qquad (51)$$

где $r = \sum_{n=1}^{N} C(n)\pi(n)$

$Q_b(\ldots)$ – равномерный квантователь с шагом Δ, когда при *b*=0 и *b*=1 берутся чередующиеся точки (см. Рис. ниже)

$$\pi(n) \in \{-1,+1\}, i.i.d.$$




● → *b*=1, ○ → *b*=0, заштрихованные области → 0 , незаштрихованные → 1

Рис… Равномерный квантователь с шагом Δ

*Атака аддитивным шумом:*

$$C'_w(n) = C(n) + \varepsilon(n), \text{где } E\{\varepsilon(n)\} = 0, \qquad (52)$$

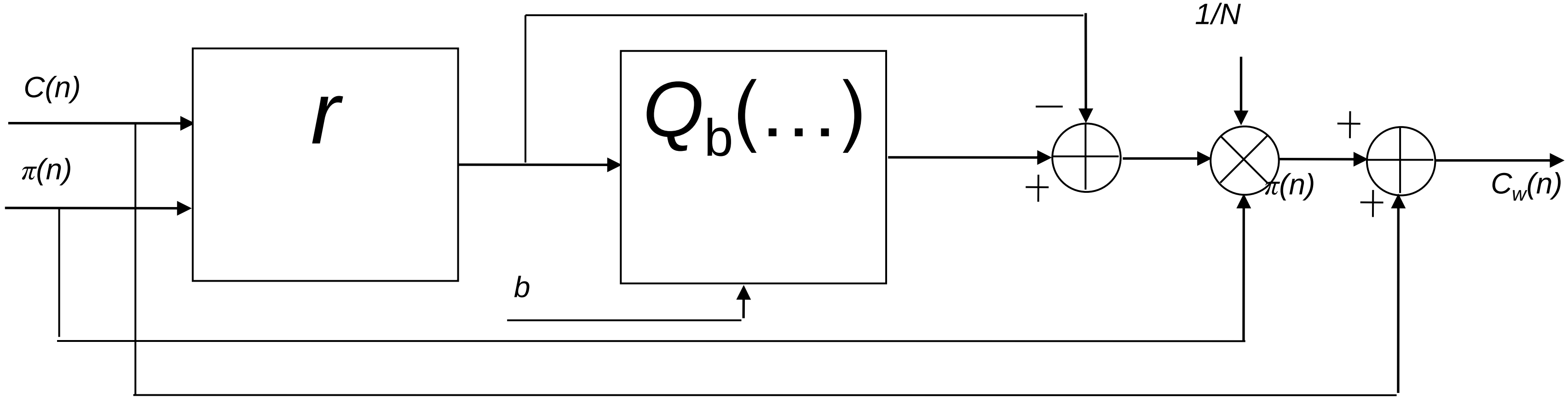
$$Var\{\varepsilon(n)\} = \sigma_\varepsilon^2$$

*Деко* $\tilde{b} = argmin_b \left\| r' - Q_b(r) \right\|^2, b \in \{0,1\} \qquad (53)$

где:

$$r' = \sum_{n=1}^{N} C'_w(n)\pi(n)$$

*Рис 2. Схема погружения ЦВЗ:*



*Восстановление «b» при отсутствии атаки:*

Пусть *b*=0, тогда из (52) получим:

$$r' = \sum_{n=1}^{N} C'_w(n)\pi(n) = \sum_{n=1}^{N}\left(C(n) + \frac{\rho_0}{N}\pi(n)\right)\pi(n) = \sum_{n=1}^{N}\left(C(n)\pi(n) + \frac{\rho_0}{N}\right) =$$

$$\sum_{n=1}^{N} C(n)\pi(n) + \sum_{n=1}^{N}\frac{Q_o\sum_{n=1}^{N} C(n)\pi(n) - \sum_{n=1}^{N} C(n)\pi(n)}{N} =$$

$$\sum_{n=1}^{N} C(n)\pi(n) + Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) - \sum_{n=1}^{N} C(n)\pi(n) = Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) \tag{54}$$

$$Q_0(r) - r_0 = Q_0\left(Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right)\right) - Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) = 0$$

$$Q_1(r) - r_0 = Q_1\left(Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right)\right) - Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) = \mathit{\Delta} \tag{55}$$

При *b*=1, получаем аналогичным образом, что $Q_0(r) - r = \Delta, Q_1(r) - r = 0$

*Вывод:*

При отсутствии всякой атаки декодер дает нулевую ошибку

*Расчет вероятности ошибки при декодировании бита b при атаке аддитивным шумом.*

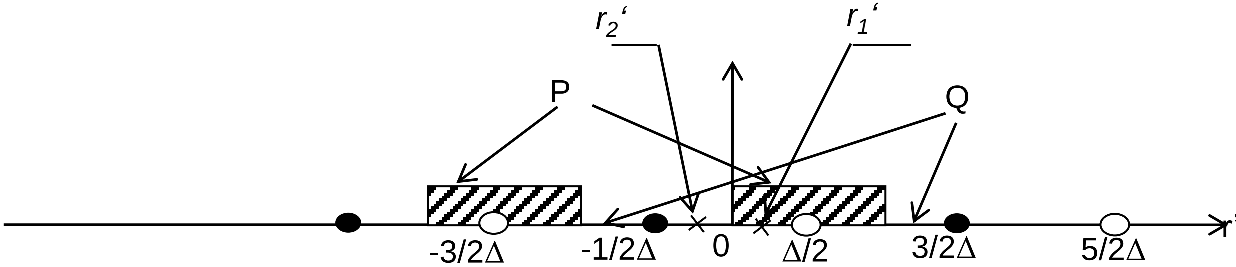
Пусть $b$=0. Тогда из (51), (52) получим:

$$r' = \sum_{n=1}^{N} C'_w(n)\pi(n) = \sum_{n=1}^{N}\left( C(n) + \frac{\rho_0}{N}\pi(n) + \varepsilon(n)\right)\pi(n) = \sum_{n=1}^{N}\left( C(n)\pi(n) + \varepsilon(n)\pi(n) + \frac{\rho_0}{N}\right) =$$

$$\sum_{n=1}^{N} C(n)\pi(n) + \sum_{n=1}^{N}\varepsilon(n)\pi(n) + \sum_{n=1}^{N}\left(\frac{Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) - \sum_{n=1}^{N} C(n)\pi(n)}{N}\right) =$$

$$\sum_{n=1}^{N} C(n)\pi(n) + \sum_{n=1}^{N}\varepsilon(n)\pi(n) + Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) - \sum_{n=1}^{N} C(n)\pi(n) = Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) + \sum_{n=1}^{N}\varepsilon(n)\pi(n) \quad (56)$$

Рассмотрим область принятия решений о символе *b:*




*Алгоритм декодирования на примере заданных величин $r'_1$, $r'_2$*

$$\left|Q_0(r') - r'\right| < \left|Q_1(r') - r'\right| \Rightarrow b = 0$$

$$\left|Q_0(r') - r'\right| \geq \left|Q_1(r') - r'\right| \Rightarrow b = 1$$

$$r'_1 : Q_0(r'_1) = \Delta/2, Q_1(r'_1) = -\Delta/2, \left|\Delta/2 - r'_1\right| < \left|-\Delta/2 - r'_1\right| \Rightarrow b = 0$$

$$r'_2 : Q_0(r'_2) = \Delta/2, Q_1(r'_2) = -\Delta/2, \left|\Delta/2 - r'_2\right| > \left|-\Delta/2 - r'_2\right| \Rightarrow b = 1$$

*Вывод:*

Заштрихованные области (*P*) соответствуют решению *b*=0, а не заштрихованные *b*=1

Потому при вложении символа *b*=0,

$$P = Pr\{r' \notin P\} = Pr\left\{ r' \notin \bigcup_{i=-\infty}^{\infty} \left(2\Delta i, \Delta(2i+1)\right) \right\} \qquad (57)$$

$$r' = Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) + \sum_{n=1}^{N} \varepsilon(n)\pi(n)$$

$$\left.\begin{array}{l} Q_0\left(\sum_{n=1}^{N} C(n)\pi(n)\right) \in \bigcup_{i=-\infty}^{\infty} \Delta(2\mathrm{i}+1/2) \\ r' \notin P \end{array}\right\} \Rightarrow \Lambda = \sum_{n=1}^{N} \varepsilon(n)\pi(n) \in \bigcup_{i=-\infty}^{\infty} (2\Delta i + \Delta/2, 2\Delta i + 3\Delta/2) \Rightarrow$$

$$\Lambda \in \bigcup_{i=-\infty}^{\infty} (2\Delta i + \Delta/2, 2\Delta i + 3\Delta/2) \tag{58}$$

$$\Lambda \in N\left(0, N\sigma_\varepsilon^2\right) \tag{59}$$

$$(58),(59) \Rightarrow P = \sum\nolimits_{i=-\infty}^{\infty}\left(Q\left(\Delta\frac{(2\mathrm{i}+1/2)}{\sqrt{N\sigma_\varepsilon^2}}\right) - Q\left(\Delta\frac{(2\mathrm{i}+3/2)}{\sqrt{N\sigma_\varepsilon^2}}\right)\right) =$$

$$\sum_{i=-\infty}^{\infty} Q\left(\Delta\frac{(4\mathrm{i}+1)}{2\sqrt{N\sigma_\varepsilon^2}}\right) - Q\left(\Delta\frac{(4\mathrm{i}+3)}{2\sqrt{N\sigma_\varepsilon^2}}\right) \tag{60}$$

Пренебрегая «боковыми лепестками» в (60), получим:

$$p \approx 2\mathrm{Q}\left(\frac{\Delta}{2\sqrt{N\sigma_\varepsilon^2}}\right) \tag{61}$$

*Оценка искажений ПС при вложении ЦВЗ и атаке аддитивным шумом:*

$$\eta_\omega = \frac{\sigma_c^2}{E\{\left(C_w(n) - C(n)\right)^2\}} = \frac{\sigma_c^2 N^2}{E\{\left(Q_d(r) - r\right)^2\}} \tag{62}$$

$$где: r = \sum_{n=1}^{N} C(n)\pi(n)$$

Из(62) видно, что $\eta_\omega$ зависит не только от значения *C(n),* но от соседних значений *C(n), n*=1,2,…*N*, причем нелинейным образом.

Однако, справедлива оценка $\left|Q_b(r) - r\right| \le \Delta$ и поэтому получим:

$$\eta_\omega \ge \frac{\sigma_c^2 N^2}{\Delta^2} \tag{63}$$

$$C'_w(n) = C_w(n) + \varepsilon(n), Var\{\varepsilon(n)\} = \sigma_\varepsilon^2 \Rightarrow$$

$$\eta_a = \frac{\sigma_c^2}{E\{\left(C_w(n) - C(n)\right)^2\} + \sigma_\varepsilon^2} = \frac{\sigma_c^2}{\Delta^2 / N^2 + \sigma_\varepsilon^2} \tag{64}$$

Полагая равенства в (63), (64), получаем из них

$$\frac{\sigma_\varepsilon^2 N}{\Delta^2} = \frac{\eta_\omega}{N\eta_a} - 1/N = 1/N\left(\frac{\eta_\omega}{N\eta_a} - 1\right) \tag{65}$$

Подставляя (62) в (61), находим

$$P \le 2Q\left(\frac{1}{2}\sqrt{\frac{N\eta_a}{\eta_\omega - \eta_a}}\right) = 2Q\left(\frac{1}{2}\sqrt{\frac{N}{\eta - 1}}\right) = 2Q\left(\sqrt{\frac{N}{4(\eta - 1)}}\right) \tag{66}$$

где $\eta = \dfrac{\eta_\omega}{\eta_a}$

При более точном расчете искажений для QPD, получаем границу $P \le 2Q\left(\sqrt{\dfrac{0{,}75N}{(\eta - 1)}}\right)$

**Вывод:**

Сравнивая (63) с выражением (11) для вероятности ошибки при информированном декодере и погружением по методу ШПС получаем, что для получения одинаковой достоверности, длина ШПС N должна быть для QPD увеличена примерно в 1,3 раза.

*Оптимизация параметров QPD-СГС*

*Заданы:*

*P*, $\sigma^2_{c.}$ $\eta_a$ Необходимо выбрать такие параметры *Δ* и *N*, которые максимизируют $\eta_\omega$.

**Замечание 1.**

Формулы (63), (64), (66), являются приближенными и потому их нужно уточнять моделированием.

**Замечание 2.**

QPD-СГС, (также как и УШПС) и отличие от ШПС-СГС дает коррелированные искажения ПС на интервале длинной *N* выборок (пикселей).

**Замечание 3.**

Сравнивая QPD с УШПС, для которой (см. начало лекции)

$$P = Q\left(\sqrt{\frac{\eta_a\left(N-\eta_\omega\right)}{\eta_\omega-\eta_a}}\right) = Q\left(\sqrt{\frac{N-\eta_\omega}{\eta-1}}\right)$$

видим, что при слишком больших *N*, УШПС оказывается лучше чем QPD.