

Приём сигналов при воздействии маскирующих помех. Часть 2

А.И. Фалько

Рассматривается структура алгоритмов оптимального приёма дискретных сообщений в приёмнике злоумышленника в условиях действия маскирующих помех. Выведены уравнения функционирования специализированного вычислителя для моделирования работы алгоритмов приёма.

Ключевые слова: алгоритм приёма, маскирующая помеха, вероятность ошибки, корреляционная функция, импульсная характеристика.

1. Введение

Данная статья является логическим продолжением работы [1]. В работе [1] рассмотрена возможность защиты от утечки (перехвата) конфиденциальной информации при помощи маскирующей помехи (МП). В ней синтезированы алгоритмы оптимального приёма сигналов и проведён анализ помехоустойчивости приёма в условиях действия маскирующих помех. При этом структура оптимальных алгоритмов приёма в работе [1] не раскрывалась. В данной статье делается попытка раскрытия алгоритмов оптимального приёма дискретных сообщений с целью выявления возможностей их реализации программными средствами.

Цель работы – вывод уравнений функционирования специализированного вычислителя для моделирования работы оптимальных алгоритмов приёма дискретных сообщений в условиях действия маскирующих помех.

В данной статье сохранены обозначения, принятые в Части 1 [1].

2. Алгоритмы приёма

Алгоритмы оптимального приёма сигналов с одинаковыми энергиями, согласно [1], имеют вид:

$$\operatorname{Re}(\underline{\mu V}_r^*) > \operatorname{Re}(\underline{\mu V}_e^*), \quad r \neq e \quad (1)$$

– для когерентного приёма;

$$|\underline{V}_r| > |\underline{V}_e|, \quad r \neq e \quad (2)$$

– для некогерентного приёма.

В (1), (2) $\underline{V}_r$ определяется формулой

$$\underline{V}_r = \int_T [\underline{Z}'(t) - \hat{\underline{Z}}_{\Pi}(t)] \underline{Z}_r^{(\varepsilon)*}(t) dt. \quad (3)$$

Здесь

$$\hat{Z}_{\Pi}(t) = \int_{t_0}^t Z'(\tau) \underline{Y}_{\Pi}(t, \tau) d\tau = \hat{\mu}_{\Pi} Z_{\Pi}(t) \quad (4)$$

– оценка маскирующей помехи по критерию минимума среднего квадрата ошибки;

$$\underline{Z}_r^{(\Theta)}(t) = \underline{Z}_r(t) - \underline{Z}_r^{\Pi}(t) \quad (5)$$

– эквивалентная сигнальная функция с учётом влияния фильтра оценивания маскирующей помехи, где

$$\underline{Z}_r^{\Pi}(t) = \int_{t_0}^t \underline{Z}_r(\tau) \underline{Y}_{\Pi}(t, \tau) d\tau \quad (6)$$

– сигнальная функция $\underline{Z}_r(t)$ на выходе фильтра оценки маскирующей помехи.

В выражениях (4) и (6) $\underline{Y}_{\Pi}(t, \tau)$ – комплексная импульсная характеристика фильтра оценки маскирующей помехи.

Из (1), (2) видно, что для решения поставленной задачи приёма сигналов в условиях действия маскирующих помех необходимо вычисление $\underline{V}_r$ (3).

Представим (3) в эквивалентной форме:

$$\frac{\underline{V}_r}{v^2} = \frac{1}{2} \int_T dt \int_T \underline{H}(t, \tau) \underline{Z}'(\tau) d\tau \int_T \underline{H}^*(t, x) \underline{Z}_r^*(x) dx, \quad (7)$$

$$\text{где } \underline{H}(t, \tau) = \frac{1}{\sqrt{v^2}} [\delta(t - \tau) - \underline{Y}_{\Pi}(t - \tau)]. \quad (8)$$

Здесь $\delta(t - \tau)$ – дельта-функция Дирака; $\underline{Y}_{\Pi}(t - \tau)$ – импульсная характеристика фильтра оценки маскирующей помехи.

В (8) $[\delta(t - \tau) - \underline{Y}_{\Pi}(t - \tau)]$ – импульсная характеристика «обеливающего» фильтра. Интервал оценивания T в (7) принят совпадающим с интервалом решения (в общем случае они могут отличаться).

Введём в рассмотрение обратное ядро

$$B^{-1}(\tau, x) = \int_T \underline{H}(t, \tau) \underline{H}^*(t, x) dt, \quad (9)$$

связанное с корреляционной функцией смеси маскирующей и флуктуационной помех соотношением

$$\int_T B^{-1}(\tau, x) B(x, u) dx = \delta(\tau - u), \quad (10)$$

$$\text{где } B(x, u) = v^2 \delta(x - u) + B_{\Pi}(x, u). \quad (11)$$

Здесь

$$B_{\Pi}(x, u) = E \left[\underline{Z}_{\Pi}(x) \underline{\mu}_{\Pi}(x) \underline{\mu}_{\Pi}^+(u) \underline{Z}_{\Pi}^+(u) \right] = \underline{Z}_{\Pi}(x) \underline{B}_{\mu_{\Pi}}(x, u) \underline{Z}_{\Pi}^+(u) \quad (12)$$

– корреляционная функция маскирующей помехи.

В (12) E – знак математического ожидания.

Из (7) с учётом (9) получим

$$\frac{\underline{V}_r}{v^2} = \frac{1}{2} \int_T \int_T \underline{Z}'(\tau) B^{-1}(\tau, x) \underline{Z}_r^*(x) d\tau dx, \quad (13)$$

или, вводя обозначения

$$\underline{Y}_r(\tau) = \int_T B^{-1}(\tau, x) \underline{Z}_r(x) dx, \quad (14)$$

$$\text{имеем } \frac{V_r}{v^2} = \frac{1}{2} \int_T \underline{Z}'(\tau) \underline{Y}_r^*(\tau) d\tau. \quad (15)$$

Здесь функция $\underline{Y}_r(\tau)$ в соответствии с (10), (11), (14) определяется неоднородным уравнением Фредгольма:

$$\underline{Z}_r(t) = \int_T B_{\Pi}(t, u) \underline{Y}_r(u) du + v^2 \underline{Y}_r(t), \quad (16)$$

или с учётом (12)

$$\underline{Z}_r(t) = \underline{Z}_{\Pi}(t) \int_T B_{\mu_{\Pi}}(t, u) \underline{Z}_{\Pi}^+(u) \underline{Y}_r(u) du + v^2 \underline{Y}_r(t). \quad (17)$$

Решение таких уравнений методами переменных состояния приведено в [2, т. 2]. Оно связано с переходом от интегральных уравнений к дифференциальным, что значительно упрощает как решение, так и моделирование их компьютерными методами. Для этого комплексная огибающая маскирующей помехи $\mu_{\Pi}(t)$ представляется как вектор состояния, который генерируется динамической системой, описываемой комплексным векторным дифференциальным уравнением [2, т. 1]

$$\frac{d \underline{\mu}_{\Pi}(t)}{dt} = \underline{F}_{\Pi}[\underline{\mu}_{\Pi}(t), t] + \underline{G}_{\Pi}(t) \underline{v}_{\Pi}(t), \quad (18)$$

где $\underline{F}_{\Pi}[\underline{\mu}_{\Pi}(t), t]$ – в общем случае нелинейная матричная функция. В частном случае гауссовской МП она может быть линейной, тогда уравнение (18) можно представить в виде

$$\frac{d \underline{\mu}_{\Pi}(t)}{dt} = \underline{F}_{\Pi}(t) \underline{\mu}_{\Pi}(t) + \underline{G}_{\Pi}(t) \underline{v}_{\Pi}(t). \quad (19)$$

Здесь $\underline{F}_{\Pi}(t)$ и $\underline{G}_{\Pi}(t)$ – матрицы, описывающие динамику системы. Их элементы в общем случае являются непрерывными функциями времени. В частном случае $\underline{F}_{\Pi}(t)$ и $\underline{G}_{\Pi}(t)$ могут быть инвариантными во времени. $\underline{v}_{\Pi}(t)$ – комплексный гауссовский случайный процесс с нулевым средним и ковариационной функцией $E[\underline{v}_{\Pi}(t) \underline{v}_{\Pi}^+(\tau)] = \theta_{\Pi} \delta(t - \tau)$, где E – знак математического ожидания; “+” – знак комплексно-сопряжённой операции транспонирования.

Для перехода от (17) к дифференциальным уравнениям вводится функция

$$\underline{S}_r(t) = \int_T B_{\mu_{\Pi}}(t, u) \underline{Z}_{\Pi}^+(u) \underline{Y}_r(u) du, \quad (20)$$

которая определяется уравнениями

$$\frac{d \underline{S}_r(t)}{dt} = \underline{F}_{\Pi}(t) \underline{S}_r(t) + \underline{G}_{\Pi}(t) \theta_{\Pi} \underline{Z}_{\Pi}^+(t) \underline{\eta}(t), \quad (21)$$

$$\frac{d \underline{\eta}(t)}{dt} = \frac{1}{v^2} \underline{Z}_{\Pi}^+(t) \underline{Z}_{\Pi}(t) \underline{S}_r(t) - \underline{F}_{\Pi}^+(t) \underline{\eta}(t) - \frac{1}{v^2} \underline{Z}_{\Pi}^+(t) \underline{Z}_r(t). \quad (22)$$

С учётом (20) уравнение (17) можно записать в виде

$$\underline{Z}_r(t) = \underline{Z}_{\Pi}(t) \underline{S}_r(t) + v^2 \underline{Y}_r(t), \quad (23)$$

откуда следует выражение для $\underline{Y}_r(t)$

$$\underline{Y}_r(t) = \frac{1}{v^2} [\underline{Z}_r(t) - \underline{Z}_{\Pi}(t) \underline{S}_r(t)]. \quad (24)$$

Используя (24), из (15) получим

$$\underline{V}_r = \frac{1}{2} \int_T \underline{Z}'(t) [\underline{Z}_r(t) - \underline{Z}_{\Pi}(t) \underline{S}_r(t)] dt, \quad (25)$$

где $\underline{S}_r(t)$ определяется моделированием уравнений (21), (22).

В частном случае разложимого ядра корреляционной функции маскирующей помехи

$$B_{\Pi}(t, u) = \sum_{i=1}^k \lambda_i \underline{\phi}_i(t) \underline{\phi}_i^*(u), \quad (26)$$

где λ_i и $\underline{\phi}_i(t)$ – собственные числа и собственные функции ядра. Обратное ядро $B^{-1}(t, u)$ можно представить в виде

$$B^{-1}(t, u) = \frac{1}{v^2} \left[\delta(t - u) - \sum_{i=1}^k \frac{\lambda_i}{\lambda_i + v^2} \underline{\phi}_i(t) \underline{\phi}_i^*(u) \right]. \quad (27)$$

Подстановка (27) в (14) даёт

$$\underline{Y}_r(t) = \frac{1}{v^2} \left[\underline{Z}_r(t) - \sum_{i=1}^k \frac{\lambda_i \underline{\phi}_i(t)}{\lambda_i + v^2} \int_T \underline{Z}_r(u) \underline{\phi}_i^*(u) du \right]. \quad (28)$$

Введем обозначения:

$$h_{\Pi i}^2 = \frac{\lambda_i}{v^2}; \quad \underline{G}_{ri} = \int_T \underline{Z}_r(t) \underline{\phi}_i^*(t) dt. \quad (29)$$

Здесь $h_{\Pi i}^2$ – отношение энергии i -ой составляющей МП к спектральной плотности мощности флуктуационной помехи, $\underline{G}_{ri}$ – комплексный коэффициент взаимной корреляции, определяющий различие структур r -го сигнала и i -ой составляющей МП. Его свойства подробно рассмотрены в [3, п.2.3].

После подстановки (28) в (13) с учётом обозначений (29), получим

$$\underline{V}_r = \frac{1}{2} \int_T \underline{Z}'(t) \left[\underline{Z}_r^*(t) - \sum_{i=1}^k \frac{\overline{h_{\Pi i}^2}}{1 + h_{\Pi i}^2} \underline{G}_{ri}^* \underline{\phi}_i^*(t) \right] dt, \quad (30)$$

или при $\overline{h_{\Pi i}^2} \gg 1$ (условие маскирования)

$$\underline{V}_r = \frac{1}{2} \int_T \underline{Z}'(t) \left[\underline{Z}_r^*(t) - \sum_{i=1}^k \underline{G}_{ri}^* \underline{\phi}_i^*(t) \right] dt. \quad (31)$$

Выражения (30), (31) характерны для квазидетерминированных МП.

Действительная часть первого слагаемого в правой части (30), (31) представляет собой напряжение на выходе фильтра, согласованного с сигналом $\underline{Z}_r(t)$, то есть имеющего импульсную характеристику

$$\underline{Y}_r(t) = \begin{cases} \underline{Z}_r^*(T - t), & t \in T, \\ 0, & t \notin T. \end{cases} \quad (32)$$

Каждое слагаемое по i второго члена в (31) есть взвешенная с весом $\underline{G}_{ri}^*$ комплексная оценка МП, полученная по неклассифицированной смеси сигнала, маскирующей и флуктуационной помехи, то есть $\int_T \underline{Z}'(t) \underline{\phi}_i^*(t) dt$. Действительная часть этого выражения является напряжением на выходе фильтра, согласованного с $\underline{\phi}_i(t)$. Импульсная характеристика этого фильтра

$$\underline{Y}_{\Pi i}(t) = \begin{cases} \underline{\phi}_i^*(T - t), & t \in T, \\ 0, & t \notin T. \end{cases} \quad (33)$$

Согласно (31) тракт обработки сигнала можно рассматривать как единый согласованный фильтр с импульсной характеристикой

$$\underline{Y}_r(t) = \begin{cases} \underline{Z}_r^*(T-t) - \sum_{i=1}^k \underline{G}_{ri}^* \underline{\phi}_i^*(T-t), & t \in T, \\ 0, & t \notin T. \end{cases} \quad (34)$$

Таким образом, в общем случае приёмник должен содержать специализированный вычислитель для моделирования уравнений (21), (22) с целью формирования импульсной характеристики фильтра оценки эквивалентной сигнальной функции $\underline{Y}_r(t)$ (24), а следовательно, и величин $\underline{V}_r$ (25), которые определяют алгоритмы приёма сигналов (1), (2) в условиях действия маскирующих помех.

Для маскирующих помех с разложимым ядром корреляционной функции (26), алгоритмы приёма имеют наглядную физическую интерпретацию (30)...(34).

3. Помехоустойчивость приёма

В работе [1] проведён анализ помехоустойчивости приёма двоичных сигналов с одинаковыми энергиями по правилам (1), (2) при неразложимом ядре корреляционной функции маскирующей помехи. Вероятность ошибки представлена формулами (22)...(25) из [1] и соответствующими графиками.

Здесь приведён результат анализа помехоустойчивости приёма при разложимом ядре корреляционной функции маскирующей помехи при тех же условиях, что и в [1].

Вероятность ошибки как вероятность невыполнения неравенства (1) при передаче первого сигнала (когерентный приём) определяется выражением

$$P_{ош} = 0.5[1 - \Phi(h_3)], \quad (35)$$

в котором $\Phi(h_3) = \sqrt{\frac{2}{\pi}} \int_0^{h_3} \exp(-\frac{x^2}{2}) dx$ – интеграл вероятности (функция Крампа).

Здесь согласно (1) с учётом (30)

$$h_3^2 = h_C^2 \left(1 - \rho - \frac{1}{2} \sum_{i=1}^k \frac{h_{\Pi i}^2 g_i^2}{1 + h_{\Pi i}^2} \right). \quad (36)$$

При $h_{\Pi i}^2 \gg 1$ (условие маскирования)

$$h_3^2 = h_C^2 \left(1 - \rho - \frac{1}{2} \sum_{i=1}^k g_i^2 \right). \quad (37)$$

Здесь $h_C^2 = \frac{\mu^2 E_C}{\nu^2}$ – отношение энергии элемента принятого сигнала к спектральной плотности мощности флуктуационной помехи;

$\rho = \frac{1}{E_c} \int_T Z_1(t) Z_2(t) dt = \frac{1}{E_c} \int_T \tilde{Z}_1(t) \tilde{Z}_2(t) dt$ – коэффициент, характеризующий вид используемых сигналов ($\rho = -1$ для противоположных сигналов, $\rho = 0$ для ортогональных сигналов).

В (36), (37) введено обозначение $g_i^2 = g_{01i}^2 + g_{02i}^2 - 2g_{12}^{(i)}$ – коэффициент, характеризующий различимость сигналов и ϕ_i -ой составляющей МП. Он определяется через коэффициенты взаимной корреляции $g_{0ri}^2 = |\underline{G}_{ri}|^2$ (29) r -го сигнала ($r = 1, 2$) с i -ой составляющей МП и коэффициент $g_{12}^{(i)}$, равный

$$g_{12}^{(i)} = \frac{1}{\lambda_i E_c} (x_i^{(П1)} x_i^{(П2)} + y_i^{(П1)} y_i^{(П2)}),$$

$$\begin{aligned} \text{где } x_i^{(Пr)} &= \int_T \operatorname{Re}[\underline{Z}_r(t)] \operatorname{Re}[\underline{\phi}_i(t)] dt, \\ y_i^{(Пr)} &= \int_T \operatorname{Re}[\underline{Z}_r(t)] \operatorname{Im}[\underline{\phi}_i(t)] dt, \\ r &= 1, 2. \end{aligned}$$

Из выражений (35) – (37) видно, что вероятность ошибки определяется отношением энергии принятого сигнала к спектральной плотности мощности флуктуационной помехи, зависит от вида используемых сигналов, от коэффициентов, характеризующих различимость сигналов и МП. При разложимом ядре корреляционной функции МП при $h_{Пi}^2 \gg 1$ вероятность ошибки не зависит от мощности составляющих маскирующих помех, так как они компенсируются (режектируются) вместе с составляющими сигнала, совпадающими с помехами. Поэтому для достоверного приёма необходима избыточность по сигналу. Если база сигнала

будет равна или меньше базы маскирующей помехи ($1 - \rho - 0.5 \sum_{i=1}^k g_i^2 = 0$), то вероятность

ошибки будет предельная ($p_{\text{ош}} = 0.5$) независимо от h_C^2 , то есть будет полное маскирование полезного сигнала. Заметим, что база сигнала (помехи) определяется произведением полосы частот сигнала (помехи) на длительность элемента сигнала (помехи).

При некогерентном приёме ортогональных двоичных сигналов вероятность ошибки определяется формулой

$$p_{\text{ош}} = 0.5 \exp(-h_{\mathcal{G}}^2 / 2), \quad (38)$$

$$\text{в которой } h_{\mathcal{G}}^2 = h_C^2 \left(1 - \sum_{i=1}^k \frac{h_{Пi}^2 \cdot g_{0i}^2}{1 + h_{Пi}^2} \right), \quad (39)$$

$$\text{или при } h_{Пi}^2 \gg 1 \quad h_{\mathcal{G}}^2 = h_C^2 (1 - \sum_{i=1}^k g_{0i}^2), \quad (40)$$

где $g_{0i}^2 = g_{01i}^2 = g_{02i}^2 = |\underline{G}_{ri}|^2$, ($r = 1, 2$); $\underline{G}_{ri}$ определяется (29).

Из (38) – (40) видно, что и при некогерентном приёме вероятность ошибки зависит от отношения энергии принятого сигнала к спектральной плотности мощности флуктуационной помехи, от коэффициентов различимости сигналов и составляющих МП и при $h_{Пi}^2 \gg 1$ не зависит от интенсивности МП вследствие их режекции. Поэтому при $1 - \sum_{i=1}^k g_{0i}^2 = 0$ вероятность ошибки $p_{\text{ош}} = 0.5$.

Таким образом, маскирующая помеха с базой, соизмеримой с базой сигнала, может полностью замаскировать полезный сигнал, предотвращая утечку (перехват) конфиденциального сообщения злоумышленником.

Литература

1. Фалько А.И. Приём сигналов при воздействии маскирующих помех // Вестник СибГУТИ. - 2013, №3. - С.11-19.
2. Ван Трис Г. Теория обнаружения, оценок и модуляции. М.: Сов. Радио, Т.1. 1972-744с; Т.2. 1975-662с. Т.3. 1977-664с.

3. Сикарев А.А., Фалько А.И. Оптимальный приём дискретных сообщений. – М.: Связь, 1978-328с.

Статья поступила в редакцию 09.12.2013

Фалько Анатолий Иванович

доктор технических наук, профессор кафедры РТУ СибГУТИ, тел. служебный: (383)269-82-64; служебный e-mail: falco@sibsutis.ru

Reception of signals at influence of masking hindrances. Part 2

A.I. Falko

The structure of algorithms of optimum reception of discrete message in the receiver of malicious user in the conditions of masking interference is considered. The equations of functioning of specialized calculator for simulation of algorithms reception operation are calculated.

Keywords: algorithm of reception, masking interference, error probability, correlation function, pulse characteristic.