

УДК 621.391.26

Приём сигналов при воздействии маскирующих помех

А.И. Фалько

Рассматривается возможность защиты от утечки (перехвата) конфиденциальной информации при помощи маскирующей помехи. Проведён синтез оптимальных алгоритмов приёма при воздействии маскирующей помехи. Проанализирована помехоустойчивость приёма.

Показано, что маскирующая помеха структурно неразличима с полезным (для злоумышленника) сигналом (сообщением), предотвращает возможность перехвата конфиденциальной информации.

Ключевые слова: утечка (перехват) конфиденциальной информации, маскирующая помеха, синтез алгоритма, анализ помехоустойчивости.

1. Введение

В работах [1 – 3 и др.] показаны пути утечки (перехвата) конфиденциальной информации, в частности, высокочастотным облучением технических информационных систем при помощи зондирующего сигнала. Для защиты от перехвата полезного сообщения применяют маскирующую (заградительную) помеху.

В данной статье делается попытка исследования возможностей предотвращения перехвата с помощью излучения маскирующей помехи, которая не позволит злоумышленнику выделить из принятого сигнала полезное сообщение. Здесь и далее под полезным сообщением подразумевается сообщение, полезное для злоумышленника. Исследование возможностей перехвата – это прежде всего исследование способов приёма сигнала при воздействии маскирующей помехи.

Цели работы:

- синтез оптимальных алгоритмов приёма сигналов в условиях действия маскирующей помехи;
- анализ помехоустойчивости приёма;
- исследование свойств маскирующей помехи.

Приём дискретных сообщений и приём аналоговых сообщений рассматриваются отдельно.

2. Приём дискретных сообщений

2.1 Синтез оптимальных алгоритмов приёма

Независимо от природы перехватываемого сигнала, несущего конфиденциальную информацию, принятую смесь сигнала с помехами на входе приёмника злоумышленника можно представить в комплексной форме:

$$\underline{Z}'(t) = \underline{\mu} \underline{Z}_r(t) + \underline{\mu}_{\Pi} \underline{Z}_{\Pi}(t) + \underline{\xi}(t), \quad t \in T. \quad (1)$$

Здесь $\underline{\xi}(t) = \xi(t) + j\tilde{\xi}(t)$ – флуктуационная помеха, аппроксимируемая комплексным гауссовским процессом с нулевым средним и спектральной плотностью мощности ν^2 . $\tilde{\xi}(t)$ – функция, сопряжённая $\xi(t)$ по Гильберту. Процесс $\xi(t)$ характеризуется функцией распределения (функция правдоподобия)

$$W(\xi) = \text{const} \cdot \exp\left[-\frac{1}{\nu^2} \int_T \xi^2(t) dt\right]. \quad (2)$$

T – интервал наблюдения.

В выражении (1) $\underline{\mu} \underline{Z}_r(t)$ – принятый полезный сигнал ($r = 1, \dots, m$) с комплексной огибающей $\underline{\mu} = \mu_c - j\mu_s = |\underline{\mu}| \exp(j\psi)$. Здесь μ_c и μ_s – ортогональные составляющие коэффициента передачи канала для сигнала.

$$\underline{Z}_r(t) = Z_r(t) + j\tilde{Z}_r(t),$$

где $Z_r(t)$ – детерминированная интегрируемая в квадрате функция, определяющая переданный сигнал; $\tilde{Z}_r(t)$ – функция, сопряжённая $Z_r(t)$ по Гильберту.

$\underline{\mu}_{\Pi} \underline{Z}_{\Pi}(t)$ – маскирующая помеха (МП), заданная корреляционной функцией $B_{\Pi}(t)$, у которой комплексная огибающая $\underline{\mu}_{\Pi} = \mu_{c\Pi}(t) - j\mu_{s\Pi}(t)$. Здесь $\mu_{c\Pi}$ и $\mu_{s\Pi}$ – ортогональные составляющие коэффициента передачи канала для маскирующей помехи.

$$\underline{Z}_{\Pi}(t) = Z_{\Pi}(t) + j\tilde{Z}_{\Pi}(t),$$

где $Z_{\Pi}(t)$ – произвольная интегрируемая в квадрате функция, $\tilde{Z}_{\Pi}(t)$ – функция, сопряжённая $Z_{\Pi}(t)$ по Гильберту.

Принятый сигнал и МП имеют ограниченную энергию, что всегда выполняется на практике.

Оптимальное решающее правило по критерию максимального правдоподобия определяется неравенством

$$\ln \Lambda_{re} > 0, \quad r \neq e, \quad (3)$$

в котором Λ_{re} представляет собой отношение правдоподобия для r -го сигнала относительно e -го. Его можно записать в форме

$$\Lambda_{re} = \frac{\mathcal{F}(\underline{Z}' / \underline{Z}_r)}{\mathcal{F}(\underline{Z}' / \underline{Z}_e)}. \quad (4)$$

Здесь $\mathcal{F}(\underline{Z}' / \underline{Z}_r)$ – функционал отношения правдоподобия принятой реализации $\underline{Z}'(t)$ при передаче сигнала $\underline{Z}_r(t)$.

Для определения $\mathcal{F}(\underline{Z}' / \underline{Z}_r)$ воспользуемся концепцией порождающего (обновляющего) процесса [4, 5]. Порождающий процесс определяется выражением

$$\zeta_r(t) = \text{Re} \left[\underline{Z}'(t) - \hat{Y}_r(t) \right], \quad (5)$$

где $\hat{Y}_r(t)$ – оценка сигнала и МП по критерию минимума среднего квадрата ошибки, полученная из наблюдений $Z'(t)$ до текущего момента времени. В общем случае оценка $\hat{Y}_r(t)$ нелинейна. Для гауссовских процессов оценивание линейно. Остановимся более подробно на этом случае. Будем полагать

$$\hat{Y}_r(t) = \hat{Z}_{II}^{(\ominus)}(t) + \hat{Z}_r(t). \quad (6)$$

Если сигнал детерминированный, то $\hat{Z}_r(t) = \underline{\mu} Z_r(t)$.

Эквивалентная оценка маскирующей помехи

$$\hat{Z}_{II}^{(\ominus)}(t) = \int_{t_0}^t [\underline{Z}'(\tau) - \underline{\mu} Z_r(\tau)] \underline{Y}_{II}(t, \tau) d\tau = \hat{Z}_{II}(t) - \underline{\mu} Z_r^{II}(t). \quad (7)$$

Здесь $\underline{Y}_{II}(t, \tau)$ – комплексная импульсная характеристика фильтра оценки маскирующей помехи;

$$\hat{Z}_{II}(t) = \int_{t_0}^t \underline{Z}'(\tau) \underline{Y}_{II}(t, \tau) d\tau = \hat{\underline{\mu}}_{II} Z_{II}(t). \quad (8)$$

– собственно оценка МП (в отсутствие сигнала);

$$\underline{Z}_r^{II}(t) = \int_{t_0}^t \underline{Z}_r(\tau) \underline{Y}_{II}(t, \tau) d\tau \quad (9)$$

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

С учётом (6) – (9) выражение (5) примет вид:

$$\zeta_r(t) = \text{Re} \left\{ \underline{Z}'(t) - \hat{Z}_{II}(t) - \underline{\mu} [\underline{Z}_r(t) - \underline{Z}_r^{II}(t)] \right\} = \text{Re} \left[\underline{Z}'(t) - \hat{Z}_{II}(t) - \underline{\mu} \underline{Z}_r^{(\ominus)}(t) \right]. \quad (10)$$

Здесь

$$\underline{Z}_r^{(\ominus)}(t) = \underline{Z}_r(t) - \underline{Z}_r^{II}(t) \quad (11)$$

– эквивалентная сигнальная функция с учётом влияния фильтра оценивания маскирующей помехи.

Рассуждая аналогично [4], можно показать, что порождающий процесс (10) представляет собой белый гауссовский шум с нулевым средним и спектральной плотностью мощности ν^2 . Поэтому

$$\underline{Z}'(t) = \underline{\mu} \underline{Z}_r^{(\ominus)}(t) + \hat{Z}_{II}(t) + \zeta_r(t). \quad (12)$$

Функция правдоподобия $\zeta_r(t)$ аналогична (2). Согласно (2) и (12) функционал отношения правдоподобия принятой реализации $\underline{Z}'(t)$ при передаче $\underline{Z}_r(t)$ будет определяться выражением

$$\mathcal{F}(\underline{Z}' / \underline{Z}_r) = \exp \left\{ \text{Re} \left(\frac{\underline{\mu}}{\nu^2} \int_T [\underline{Z}'(t) - \hat{Z}_{II}(t)] \underline{Z}_r^{(\ominus)*}(t) dt \right) - \frac{|\underline{\mu}|^2}{2\nu^2} \int_T |\underline{Z}_r^{(\ominus)}(t)|^2 dt \right\}. \quad (13)$$

Здесь * – знак комплексно-сопряжённой функции.

Из (3), (4), (13) следует алгоритм приёма полностью известного сигнала

$$\begin{aligned} & \operatorname{Re} \left\{ \frac{\mu}{T} \int \left[\underline{Z}'(t) - \hat{\underline{Z}}_{\Pi}(t) \right] \underline{Z}_r^{(\vartheta)*}(t) dt \right\} - \frac{|\mu|^2}{2} \int \left| \underline{Z}_r^{(\vartheta)}(t) \right|^2 dt > \\ & > \operatorname{Re} \left\{ \frac{\mu}{T} \int \left[\underline{Z}'(t) - \hat{\underline{Z}}_{\Pi}(t) \right] \underline{Z}_e^{(\vartheta)*}(t) dt \right\} - \frac{|\mu|^2}{2} \int \left| \underline{Z}_e^{(\vartheta)}(t) \right|^2 dt, \quad r \neq e. \end{aligned} \quad (14)$$

Из (14) видно, что при когерентном приёме из принятой смеси вычитается оценка МП $\hat{\underline{Z}}_{\Pi}(t)$, оптимальная по критерию минимума среднего квадрата ошибки; после этого происходит перемножение полученной разности на образец сигнала $\underline{Z}_r^{(\vartheta)}(t)$ с учётом влияния на него фильтра оценки маскирующей помехи.

Введём обозначения:

$$\underline{V}_r = \int \left[\underline{Z}'(t) - \hat{\underline{Z}}_{\Pi}(t) \right] \underline{Z}_r^{(\vartheta)*}(t) dt, \quad (15)$$

$$B_r = 0.5 \left\{ 1 - \frac{1}{E_c} \left[\int \underline{Z}_r^*(t) \underline{Z}_r^{\Pi}(t) dt - \frac{1}{2} \int \left| \underline{Z}_r^{\Pi}(t) \right|^2 dt \right] \right\}, \quad (16)$$

$$E_c = \frac{1}{2} \int \left| \underline{Z}_r(t) \right|^2 dt.$$

С учётом этих обозначений алгоритм (14) примет вид

$$\operatorname{Re} \left(\mu \underline{V}_r^* \right) - 0.5 |\mu|^2 E_c B_r > \operatorname{Re} \left(\mu \underline{V}_e^* \right) - 0.5 |\mu|^2 E_c B_e, \quad r \neq e. \quad (17)$$

Для сигналов с пассивной паузой правая часть неравенства (17) равно нулю.

Для сигналов с одинаковыми энергиями ($E_r = E_e = E_c$) и симметричном воздействии МП ($B_r = B_e$), то есть при условии

$$E_c = \operatorname{const}(r), \quad B_r = \operatorname{const}(r), \quad (18)$$

из (17) следует существенно более простой алгоритм:

$$\operatorname{Re} \left(\mu \underline{V}_r^* \right) > \operatorname{Re} \left(\mu \underline{V}_e^* \right), \quad r \neq e. \quad (19)$$

Алгоритм некогерентного приёма сигналов (с неизвестной фазой) можно получить в результате максимизации в (4) по фазе. При условии (18) этот алгоритм можно записать в виде

$$\left| \underline{V}_r \right| > \left| \underline{V}_e \right|, \quad r \neq e, \quad (20)$$

или эквивалентно

$$\left| \underline{V}_r \right|^2 > \left| \underline{V}_e \right|^2, \quad r \neq e. \quad (21)$$

Для замирающих сигналов, например релеевских, правило решения при условии (18) определится неравенством (21).

2.2 Помехоустойчивость приёма

Помехоустойчивость приёма рассмотрим на примере двоичных сигналов с одинаковыми энергиями и симметричном воздействии маскирующих помех, т.е. по правилу (19). Вероятность ошибки как вероятность невыполнения неравенства (19) при передаче первого сигнала определяется известным выражением[6]

$$P_{\text{ош}} = 0.5 [1 - \Phi(h_{\vartheta})], \quad (22)$$

где $\Phi(h_{\vartheta}) = \sqrt{\frac{2}{\pi}} \int_0^{h_{\vartheta}} \exp \left[-\frac{x^2}{2} \right] dx$ – интеграл вероятности (функция Крампа).

Здесь

$$h_{\mathfrak{I}}^2 = \frac{h_C^2}{1 + h_{\varepsilon}^2} \frac{(1 - \rho - g_1 + g_2)^2}{1 - \rho}, \quad (23)$$

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

$h_{\varepsilon}^2 = \frac{\sigma_{\varepsilon}^2}{\sigma_{\xi}^2}$ – отношение дисперсии ошибки оценивания маскирующей помехи к дисперсии флуктуационной помехи;

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

$g_r^2 = |G_{0r}|^2 = \frac{1}{E_C E_{\Pi}} \left| \int \underline{Z}_r(t) \underline{Z}_{\Pi}^*(t) dt \right|^2$, $r = 1, 2$ – коэффициент взаимной корреляции r -го сигнала и МП, характеризующий различие структур r -го сигнала и МП ($0 \leq g_1 \leq 1$, $-1 \leq g_2 \leq 0$ для противоположных сигналов; $0 \leq g_1 \leq 1$, $g_2 = 0$ для ортогональных сигналов).

Из выражений (22) и (23) 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 и от дисперсии остаточной ошибки оценивания (фильтрации) маскирующей помехи.

При некогерентном приёме ортогональных двоичных сигналов вероятность ошибки определяется формулой

$$p_{\text{ош}} = 0.5 \exp(-h_{\mathfrak{I}}^2 / 2), \quad (24)$$

в которой

$$h_{\mathfrak{I}}^2 = \frac{h_C^2}{1 + h_{\varepsilon}^2} (1 - g_1)^2. \quad (25)$$

Из (24) и (25) 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 от остаточной ошибки фильтрации маскирующей помехи.

В качестве иллюстрации на рисунке приведены зависимости вероятности ошибки от отношения энергии элемента сигнала к спектральной плотности мощности флуктуационной помехи для разных условий при приёме фазоманипулированных (противоположных) сигналов. Зависимости рассчитаны по формуле (22) с учётом (23) при воздействии марковской МП, то есть имеющей корреляционную функцию $B_{\Pi}(\tau) = \sigma_{\Pi}^2 e^{-\alpha_{\Pi} |\tau|}$ при $h_{\Pi}^2 = \sigma_{\Pi}^2 / \alpha_{\Pi} \nu^2 = 10^2$; при разных α_{Π} / F_C , где F_C – ширина полосы полезного сигнала; α_{Π} – полоса частот маскирующей помехи; σ_{Π}^2 – мощность МП на входе.

В формуле (23)

$$h_{\varepsilon}^2 = \frac{\sigma_{\varepsilon}^2}{\sigma_{\xi}^2} = h_{\Pi}^2 \frac{\sigma_{\varepsilon}^2}{\sigma_{\Pi}^2} \frac{\alpha_{\Pi}}{F_C},$$

где $\frac{\sigma_{\varepsilon}^2}{\sigma_{II}^2} = \frac{-1 + \sqrt{1 + 2h_{II}^2}}{h_{II}^2}$ – отношение дисперсии остаточной ошибки оценивания МП к дисперсии (мощности) этой помехи на входе. Оно определяется из дисперсионного уравнения в установившемся режиме [7] (в частности, при $h_{II}^2 = 10^2$ $\sigma_{\varepsilon}^2 / \sigma_{II}^2 = 0.132$).

На рисунке кривая 1 соответствует потенциальной помехоустойчивости приёма фазоманипулированных сигналов ($\rho = -1$), то есть в отсутствие МП. Кривая 6 иллюстрирует помехоустойчивость приёма без подавления МП ($h_{\varepsilon}^2 = h_{II}^2 = 10^2$). Зависимости 2, 3, 4, 5 приведены соответственно для $\alpha_{II} / F_C = 10^{-2}$ ($g_1 + g_2 = 10^{-2}$); $\alpha_{II} / F_C = 5 \cdot 10^{-2}$ ($g_1 + g_2 = 5 \cdot 10^{-2}$); $\alpha_{II} / F_C = 0.1$ ($g_1 + g_2 = 0.1$); $\alpha_{II} / F_C = 0.5$ ($g_1 + g_2 = 0.5$).

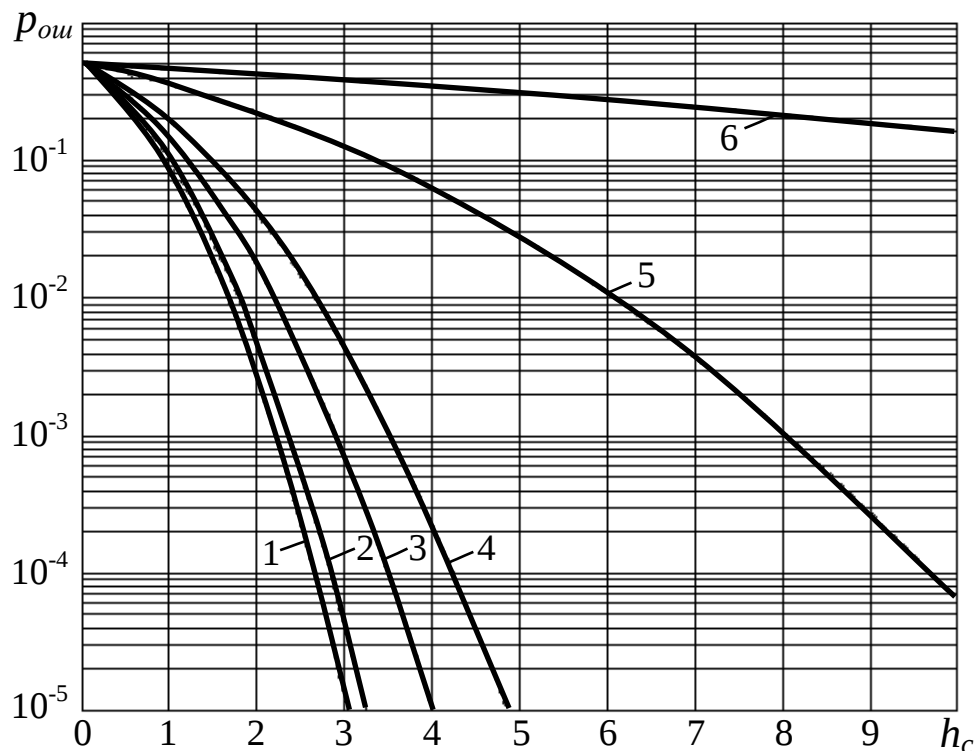


Рис.1 Зависимости вероятности ошибки от отношения энергии сигнала к спектральной плотности мощности шума

Из приведённых зависимостей видно, что в приёмнике, построенном оптимально для условий воздействия МП, подавление маскирующей помехи существенно и зависит от структурных различий сигнала и МП, в частности, от ширины спектра этих помех (кривые 2...5).

Без учёта различия структур сигнала и маскирующих помех (энергетический приёмник) помехоустойчивость определяется суммарным действием флуктуационных и маскирующих помех (кривая 6).

При приёме в условиях воздействия структурно неразличимой с сигналом маскирующей помехи ($1 - \rho - g_1 + g_2 = 0$) вероятность ошибки будет предельная ($p_{ош} = 0.5$) независимо от h_c^2 , т.е. будет полное разрушение сигнала (полная маскировка). В таких условиях не оптимальный (энергетический) приёмник может обеспечивать приём с вероятностью ошибки $p < 0.5$, в зависимости от соотношения энергий сигнала и МП. Например, при соизмеримых значениях мощностей сигнала и помех $h_s^2 = P_C / (\sigma_{\varepsilon}^2 + \sigma_{II}^2) = 1$ будет $p_{ош} = 0.16$.

Увеличением мощности МП можно обеспечить необходимую степень маскировки. Так, при двукратном превышении уровня маскирующей помехи над сигналом вероятность ошибки $p_{\text{ош}} \approx 0.3$.

Таким образом, при приёме дискретных сообщений, применение маскирующей помехи, структурно неразличимой с сигналом, предотвращает возможность достоверного приёма полезных сообщений злоумышленником.

3. Приём аналоговых сообщений

В результате высокочастотного облучения зондирующим сигналом технического средства электросвязи (аппарата), на нелинейном элементе аппарата произойдёт перекрёстная модуляция зондирующего сигнала полезным сообщением $\lambda_c(t)$ с коэффициентом амплитудной модуляции m_c . Вторичное рассеянное поле создаст на входе приёмника злоумышленника компоненту сигнала $U_C(1+m_c\lambda_c(t))\cos w_C t$.

Для защиты «заградитель» передаёт маскирующую помеху (МП), промодулированную маскирующим сообщением $\lambda_{\Pi}(t)$ с коэффициентом амплитудной модуляции m_{Π} . На нелинейном элементе аппарата маскирующая помеха получит в результате перекрёстной модуляции полезным сообщением компоненту помехи, пропорциональную $m_c\lambda_c(t)m_{\Pi}\lambda_{\Pi}(t)\cos w_{\Pi}t$ (где $w_{\Pi} \approx w_C$). Эта компонента создаёт вторичное рассеянное поле. Кроме того, маскирующая помеха ещё и непосредственно воздействует на вход приёмника злоумышленника.

Результирующая смесь сигнала с учётом всех составляющих помехи на входе приёмника злоумышленника определяется выражением:

$$\text{Re}[Z'(t)] = Z'(t) = U_C[1+m_c\lambda_c(t)]\cos w_C t + U_{\Pi 1}[1+m_c\lambda_c(t)m_{\Pi}\lambda_{\Pi}(t)]\cos w_{\Pi}t + U_{\Pi 2}[1+m_{\Pi}\lambda_{\Pi}(t)]\cos w_{\Pi}t + \xi(t) = S(t) + \xi(t). \quad (26)$$

Из этой смеси приёмнику злоумышленника надо выделить полезное сообщение $\lambda_c(t)$.

Функция правдоподобия принятой реализации смеси сигнала и помех согласно (2) с учётом (26) может быть представлена в виде:

$$W(\xi) = \text{const} \cdot \exp \left[-\frac{1}{v^2} \int_T [Z'(t) - S(t)]^2 dt \right]. \quad (27)$$

После раскрытия квадратных скобок в (27) следует, что оптимальный, по критерию минимума среднего квадрата ошибки, приёмник вычисляет корреляционный интеграл $\int_T Z'(t)S(t)dt$. При этом из флуктуационных шумов оптимально выделяется смесь сигнала с маскирующей помехой $S(t)$, а не полезное сообщение $\lambda_c(t)$.

В отличие от приёма дискретных сообщений, сигнал $S(t)$ при приёме аналоговых сообщений не известен (см. (26)). Приёмник может выделить огибающую смеси:

$$S_{or}(t) = U_C[1+m_c\lambda_c(t)] + U_{\Pi 1}[1+m_c\lambda_c(t)m_{\Pi}\lambda_{\Pi}(t)] + U_{\Pi 2}[1+m_{\Pi}\lambda_{\Pi}(t)] + \xi_{or}(t).$$

Из этой огибающей смеси надо выделить полезное сообщение $\hat{\lambda}_c(t)$.

При приёме дискретных сообщений можно использовать различие структур сигнала и маскирующей помехи.

При приёме аналоговых сообщений такой возможности нет, т.к. для компенсации МП необходимо формировать оценку не сигнала, а сообщения МП $\hat{\lambda}_c(t)$, то есть оценку случайной или псевдослучайной модулирующей функции маскирующей помехи.

Если предположить, что формирование оценки МП $\hat{\lambda}_{\Pi}(t)$ возможно, то «заградитель», используя модулирующую функцию маскирующей помехи, структурно неразличимую с полезным сообщением, «вынудит» злоумышленника применять энергетический приёмник, когда выделение соответствующего сообщения определяется только энергетическим различием

полезного и маскирующего сообщения. При этом энергетические возможности «заградителя» и злоумышленника не сопоставимы, т.к. на вход приёмника злоумышленника воздействует вторичное рассеянное поле сигнала полезного сообщения, а излучение маскирующей помехи действует непосредственно.

Оценим через «выигрыш системы» [8] возможности приёмника злоумышленника выделить из флуктационной помехи полезное сообщение вторичного рассеянного поля и маскирующей помехи (прямой компоненты). Обобщённый выигрыш системы ($B = h_{\text{ВЫХ}}^2 / h_{\text{ВХ}}^2$) определяется отношением средней мощности полезного сообщения к спектральной плотности мощности флуктационной помехи на выходе приёмника ($h_{\text{ВЫХ}}^2 = P_{\text{СВЫХ}} / \nu_{\text{ВЫХ}}^2$), отнесённой к отношению средней мощности сигнала к спектральной плотности мощности флуктационной помехи на входе приёмника ($h_{\text{ВХ}}^2 = P_{\text{СВХ}} / \nu^2$). Для амплитудно-модулированного сигнала величина обобщённого выигрыша системы выражается соотношением [8]:

$$B = \frac{m^2}{k_{II}^2 + m^2}. \quad (28)$$

Здесь m – коэффициент амплитудной модуляции (у полезного сообщения $m_c = 10^{-2} \dots 10^{-3}$, у маскирующей помехи $m_{II} \approx 1$);

k_{II} – пикфактор сообщения (например, при телефонной передаче речи $k_{II} \approx 3$).

Из (28) следует, что у полезного сообщения при $m_c = 10^{-2}$ величина выигрыша $B = 10^{-5}$, у маскирующей помехи при $m_{II} = 1$ $B = 0.1$.

Значит, при прочих равных условиях, мощность полезного сигнала на входе приёмника должна в 10^4 раз и более превышать мощность маскирующей помехи.

Если злоумышленник создаст зондирующий сигнал такой мощности, что выделенные в приёмнике полезное и маскирующее сообщения будут соизмеримы, то, например, речь будет неразборчива. При необходимости маскирующую помеху не трудно сделать гораздо более мощную.

Таким образом, используя модулирующую функцию маскирующей помехи, структурно неразличимую с полезным сообщением, можно полностью предотвратить перехват конфиденциальной информации злоумышленником.

4. Заключение

Для исследования возможностей предотвращения перехвата конфиденциальной информации при помощи МП синтезированы алгоритмы оптимального приёма сигналов при воздействии маскирующих помех. Проведён анализ помехоустойчивости приёма.

В результате показано, что для надёжной защиты от утечки (перехвата) конфиденциальной информации, при передаче дискретных сообщений, маскирующая помеха должна быть структурно неразличимой с полезным сигналом, а при передаче аналоговых сообщений маскирующая помеха должна иметь модулирующую функцию, структурно неразличимую с полезным сообщением.

Литература

1. Васильков А.В., Васильков И.А. Безопасность и управление в информационных системах: учебное пособие. – М.: Форум, 2010. – 368с.
2. Новиков С.Н., Солонская О.И. Методы защиты информации: учебное пособие СибГУТИ. – Н., 2009. – 120с.
3. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации: учебное пособие. – М.: Издательский центр «Академия», 2006. – 256с.

4. *Кайлат Т.* Метод порождающего процесса в применении к теории обнаружения и оценки// ТИИЭР. – 1970. – Т.58. - №5.-с.82-99
5. *Липцер Р.Ш., Ширяев А.Н.* Статистика случайных процессов. – М.: Наука, 1974.-696с.
6. *Финк Л.М.* Теория передачи дискретных сообщений. – М.: Советское радио, 1970.-728с.
7. *Ван Трис Г.* Теория обнаружения, оценок и модуляции. Т.1. – М.: Сов. радио, 1972.-744с.
8. *Зюко А.Г.* Помехоустойчивость и эффективность систем связи. – М.: Связь, 1972.-360с.

Статья поступила в редакцию 12.02.2013

Фалько Анатолий Иванович

д.т.н., профессор кафедры БИСС СибГУТИ, (383)269-82-64 служебный,
(383)266-89-81 дом, e-mail: falco@sibsutis.ru

Signal reception effected by masking noise

A.I. Falko

The protection possibility of confidential information leakage by masking noise is considered. The synthesis of reception optimal algorithms affected by masking noise is done. The noise immunity of reception is analyzed. It is demonstrated that interference masking is structurally indistinguishable from the useful (for an attacker) signal (the message), prevents the possibility of confidential information interception.

Keywords: leakage (interception) of confidential information, masking noise, algorithm synthesis, noise analysis.