ISSN 0033-8486

РАДИОТЕХНИКА

9 2003

www.webcenter.ru/~iprzhr/

В НОМЕРЕ:

Журнал в журнале

РАДИОСИСТЕМЫ

Выпуск 72 *Радиоэлектронные комплексы, № 3*

РАДИОТЕХНИКА

Тел./факс: (095) 925-9241
E-mail: iprzhr@online.ru
http://www.webcenter.ru/~iprzhr/

Журнал переводится на английский язык
и издается компанией Begell House, Inc. под названием
TELECOMMUNICATIONS AND RADIO ENGINEERING

Информационная безопасность радиоэлектронных систем

УДК 621.391

Параметрическая скрытность при обнаружении импульсной частотно-временной модуляции шумовой несущей

А.П. Трифонов, В.И. Парфенов

Показано, что одним из способов повышения информационной безопасности радиоэлектронной системы является применение сигналов с импульсной частотно-временной модуляцией шумовой несущей. На основе сравнения характеристик обнаружения при санкционированном и несанкционированном доступах определены условия повышения скрытности факта передачи информации радиоэлектронной системой, использующей такие сигналы.

It was shown that the application of signals with pulse frequency time modulation of noise carrier is one of the method of increasing the information security of a radioelectronic system. On the base of comparison of detection characteristics by the authorised and unauthorised access, the conditions of increasing the security of information transmission of radioelectronic system, using such signals, are found.

Идея применения шумовой несущей (ШН) для передачи информации была предложена довольно давно [1]. Однако несмотря на целый ряд полезных свойств, присущих сигналам с шумовой несущей, в частности, высокую степень скрытности, их практическое использование ограничено в силу целого ряда причин [2]. Одна из наиболее существенных причин, затрудняющих применение сигналов с шумовой несущей для передачи информации, – это трудность технической реализации устройств обработки таких сигналов. Однако предложенные в [3, 4] сигналы с импульсной частотно-временной модуляцией шумовой несущей (ИЧВМ ШН) и алгоритмы их обработки позволяют в значительной степени преодолеть эти ограничения. В соответствии с [3, 4] сигнал с ИЧВМ ШН, принимаемый на интервале времени $[0;T]$, запишется как

$$s(t,\lambda)=\left\{1-I\left[(t-\lambda)/\tau\right]\right\}\xi_1(t)+I\left[(t-\lambda)/\tau\right]\xi_2(t)\ . \quad (1)$$

где τ – длительность модулирующего импульса; $I(x)=1$ при $|x|<\frac{1}{2}$ и $I(x)=0$ при $|x|>\frac{1}{2}$; $\xi_i(t)$ – реализации независимых центрированных гауссовских узкополосных стационарных случайных процессов со спектрами мощности $G_i(\omega)=G_0\left\{f\left[(\nu_i-\omega)/\Omega_s\right]+f\left[(\nu_i+\omega)/\Omega_s\right]\right\}/2,\ i=1,2$; $f(x)=f(-x)$ определяет форму спектра мощности и нормирована так, что $\max f(x)=1$; $\int\limits_{-\infty}^{\infty}f^2(x)dx=1$; ν_i и Ω_s – соответственно центральные частоты и эквивалентная полоса частот процессов $\{\xi_i(t)\}$, причем $\nu_i>>\Omega_s$. Неизвестное временное положение модулирующего импульса λ в (1) принимает значения из априорного интервала $[\Lambda_1;\Lambda_2]$, расположенного внутри интервала наблюдения $[0;T]$, так что $\frac{\tau}{2}<\Lambda_1<\Lambda_2<T-\tau/2$. Следовательно, процессы $\{\xi_i(t)\}$ имеют спектры мощности одинаковой формы, но с разными центральными частотами. Так как $\nu_1\neq\nu_2$, то модуляция шумовой несущей осуществляется изменением параметра λ в соответствии с передаваемым сообщением.

Предположим, что сигнал (1) передается по каналу, в котором действует аддитивный гауссовский белый шум $n(t)$ с односторонней спектральной плотностью N_0. Наблюдателю, которому адресовано сообщение, априори известны статистические характеристики шума, а также все пара-

метры сигнала, кроме временного положения модулирующего импульса λ, используемого для передачи полезной информации. Сторонний наблюдатель для реализации несанкционированного доступа к передаваемой информации с целью ее использования или разрушения должен вначале установить факт наличия ИЧВМ в принятой реализации. При этом несанкционированный доступ осуществляется в условиях, когда стороннему наблюдателю неизвестны некоторые параметры сигнала. Поэтому сторонний наблюдатель для синтеза алгоритма обнаружения ИЧВМ использует некоторые ожидаемые (прогнозируемые) значения параметров сигнала, в общем случае не совпадающие с истинными.

Ниже приведен сравнительный анализ алгоритмов обнаружения ИЧВМ при реализации санкционированного и несанкционированного доступов к передаваемой информации. В результате сопоставления пороговых значений входных отношений сигнал-шум при санкционированном и несанкционированном доступах вводится параметр скрытности, который дает количественную оценку степени скрытности передаваемой информации, обусловленную несовпадением истинных и прогнозируемых параметров сигнала.

Цель работы – *анализ влияния отклонения используемых при несанкционированном доступе значений параметров сигнала от истинных на скрытность передачи информации.*

Введем в рассмотрение гипотезы

$$H_1: \quad x(t) = s(t,\lambda_0) + n(t) \tag{2}$$

– реализация наблюдаемых данных при наличии факта передачи информации (наличии ИЧВМ),

$$H_0: \quad x(t) = \xi_1(t) + n(t) \tag{3}$$

– реализация наблюдаемых данных при ее отсутствии. В (2) λ_0 – истинное значение неизвестного временного положения модулирующего импульса.

Предполагается, что при санкционированном доступе синтез приемного устройства осуществляется с использованием метода максимального правдоподобия (МП). В соответствии с [3,4] структура оптимального по методу максимального правдоподобия обнаружителя ИЧВМ имеет вид

$$\sup L(\lambda) \underset{<}{\overset{H_1}{>}} c\ ,\ \ \lambda \in [\Lambda_1;\Lambda_2]\ , \tag{4}$$
$$H_0$$

где

$$L(\lambda) = \int_{\lambda-\tau/2}^{\lambda+\tau/2} \left[y_2^2(t) - y_1^2(t) \right] dt \Big/ N_0 ,$$

$$y_i(t) = \int_{-\infty}^{\infty} x(v) h_i(t-v)\, dv \tag{5}$$

– сигнал на выходе узкополосного фильтра с импульсной характеристикой $h_i(t)$. Передаточная функция $h_i(\omega) = \int_{-\infty}^{\infty} h_i(t) \exp(-i\omega t)\, dt$ этого фильтра удовлетворяет условию

$$|h_i(\omega)|^2 = 2G_i(\omega) / \left\{ N_0 \left[1 + 2G_i(\omega)/N_0 \right] \right\}.$$

Порог обнаружения c в (4) определяется выбранным критерием оптимальности.

Вероятности ошибок 1-го α_0 и 2-го β_0 родов для обнаружителя (4) найдены в [4]:

$$\alpha_0 = F_1(m,u), \quad \beta_0 = (1-\alpha_0) F_2(u,1,1,z_0)\ , \tag{6}$$

где

$$F_1(m,u) = \begin{cases} 1 - \exp\left[-mu \exp(-u^2/2)/\sqrt{2\pi} \right], & u \ge 1, \\ 1, & u < 1, \end{cases} \tag{7}$$

$$F_2(u,f,\psi,z_0) = \Phi(fu - z_0) -$$

$$-2\exp\left[\psi^2 z_0^2/2 - \psi z_0 (fu - z_0) \right] \Phi\left[fu - (\psi+1) z_0 \right] +$$

$$+\exp\left[2\psi^2 z_0^2 - 2\psi z_0 (fu - z_0) \right] \Phi\left[fu - (2\psi+1) z_0 \right],$$

$$m = (\Lambda_2 - \Lambda_1)/\tau, \quad u = (c + A_0/2)\Big/\sqrt{B_0},$$

$$z_0 = 2A_0 \Big/ \sqrt{B_0}, \quad f = \psi = 1, \quad \mu = \Omega_s \tau / 2\pi,$$

$$A_0 = \mu q^2 \int_{-\infty}^{\infty} \frac{f(x)[f(x) - f(x-\varepsilon_s)]}{1 + qf(x)} dx,$$

$$B_0 = \mu q^2 \int_{-\infty}^{\infty} \left(\frac{f(x) - f(x-\varepsilon_s)}{1 + qf(x)} \right)^2 dx,$$

$$\varepsilon_s = |v_2 - v_1| / \Omega_s, \quad q = 2\max G_i(\omega)/N_0 = G_0/N_0,$$

$$\Phi(x) = \int_{-\infty}^{x} \exp(-t^2/2)\, dt / \sqrt{2\pi}$$

– интеграл вероятности.

Качество обнаружения будем характеризовать параметром q_{0t}, представляющим собой от-

ношение максимального значения спектра мощности сигнала к спектральной плотности помехи (пороговое входное отношение сигнал-шум (ОСШ)). Назовем пороговым входным ОСШ q_{0t} такое значение параметра q, которое обеспечивает заданные величины вероятностей ошибок 1-го и 2-го родов. Из (6) следует, что при $\alpha_0 = \beta_0 = p$ пороговое входное ОСШ q_{0t} можно найти из решения системы уравнений вида

$$F_1(m,u) = p,$$
$$F_2(u,1,1,z_0) = p/(1-p).$$

Рассмотрим теперь эффективность несанкционированного обнаружения факта передачи информации сторонним наблюдателем, которому могут быть неизвестны длительность τ и временное положение λ модулирующего импульса, а также центральные частоты ν_i $(i = 1,2)$ и эквивалентная полоса частот сигнала Ω_s. Простейшим способом несанкционированного доступа к передаваемой информации при неизвестных параметрах сигнала (1) является применение квазиправдоподобного (КП) алгоритма обнаружения. Структура КП обнаружителя, который может быть использован при несанкционированном доступе, имеет вид

$$\sup \tilde{L}(\lambda) \underset{H_0}{\overset{H_1}{\gtrless}} \tilde{c}\ ,\ \lambda \in \left[\tilde{\Lambda}_1; \tilde{\Lambda}_2\right]\ , \qquad (8)$$

где

$$\tilde{L}(\lambda) = \int_{\lambda-\tilde{\tau}/2}^{\lambda+\tilde{\tau}/2} \left[\tilde{y}_2^2(t) - \tilde{y}_1^2(t)\right] dt \Big/ N_0\,,$$
$$\tilde{y}_i(t) = \int_{-\infty}^{\infty} x(\nu)\tilde{h}_i(t-\nu)d\nu\ . \qquad (9)$$

Причем передаточная функция КП обнаружителя $\tilde{h}_i(\omega)$ удовлетворяет соотношению $|\tilde{h}_i(\omega)|^2 = f\left[(\tilde{\nu}_i - \omega)/\tilde{\Omega}_s\right] + f\left[(\tilde{\nu}_i + \omega)/\tilde{\Omega}_s\right]$. Таким образом, структура КП обнаружителя (8), (9) аналогична структуре оптимального обнаружителя (4), (5), за исключением того, что прогнозируемые параметры $\tilde{\tau}, \tilde{\nu}_i$ и $\tilde{\Omega}_s$ могут не совпадать с истинными параметрами τ, ν_i и Ω_s. Кроме того, предполагается, что ожидаемый априорный интервал изменения неизвестного временного положения $[\tilde{\Lambda}_1; \tilde{\Lambda}_2]$ также не совпадает с истинным $[\Lambda_1; \Lambda_2]$.

Определим вероятности ошибок 1-го и 2-го родов для КП обнаружителя (8), (9). Аналогично [3–5] будем считать, что $\tilde{\mu} = \dfrac{\tilde{\tau}\tilde{\Omega}_s}{2\pi} >> 1$. Тогда выходной сигнал КП обнаружителя (9) можно приближенно считать гауссовским случайным процессом [6]. Поэтому ограничимся определением первых двух моментов функции (9) при отсутствии и наличии факта передачи информации посредством ИЧВМ.

Подставляя (3) в (9) и выполняя усреднение аналогично [5, 6], получаем при отсутствии ИЧВМ

$$\left\langle \tilde{L}(l) \right\rangle = \tilde{S}_0(1+\delta_\tau),\ \left\langle \left[\tilde{L}(l_1) - \left\langle \tilde{L}(l_1)\right\rangle\right] \times \right.$$
$$\left. \times \left[\tilde{L}(l_2) - \left\langle \tilde{L}(l_2)\right\rangle\right]\right\rangle = \tilde{B}_1 R_1(l_1, l_2)\ .$$

Здесь

$$\tilde{S}_0 = \frac{\tau}{4\pi}\int_{-\infty}^{\infty} \frac{2}{N_0} G_1(\omega)\left(|\tilde{h}_2(\omega)|^2 - |\tilde{h}_1(\omega)|^2\right) d\omega,$$
$$l = \lambda/\tau,\ \delta_\tau = (\tilde{\tau} - \tau)/\tau, \qquad (10)$$
$$\tilde{B}_1 = \frac{\tau}{4\pi}\int_{-\infty}^{\infty}\left[1 + \frac{2}{N_0}G_1(\omega)\right]^2 \left(|\tilde{h}_2(\omega)|^2 - |\tilde{h}_1(\omega)|^2\right)^2 d\omega,$$
$$R_1(l_1, l_2) = \max\left(0, 1 + \delta_\tau - |l_1 - l_2|\right).$$

При наличии ИЧВМ представим выходной сигнал КП обнаружителя в виде суммы сигнальной и шумовой функций [7], $\tilde{L}(l) = \tilde{S}(l) + \tilde{N}(l)$, где $\tilde{S}(l) = \left\langle \tilde{L}(l)\right\rangle$, $\tilde{N}(l) = \tilde{L}(l) - \left\langle \tilde{L}(l)\right\rangle$. Подставляя в (9) реализацию наблюдаемых данных (2) и выполняя усреднение аналогично [5, 6], получаем

$$\tilde{S}(l) = \tilde{S}_0(1+\delta_\tau) + \tilde{A}C(l, l_0)\ ,$$
$$K_{\tilde{N}}(l_1, l_2) = \left\langle \tilde{N}(l_1)\tilde{N}(l_2)\right\rangle =$$
$$= \tilde{B}_1 R_1(l_1, l_2) + \tilde{B}_2 R_2(l_1, l_2, l_0)\ . \qquad (11)$$

где

$$\tilde{A} = \frac{\tau}{2\pi N_0}\int_{-\infty}^{\infty}\left(G_2(\omega) - G_1(\omega)\right)\left(|\tilde{h}_2(\omega)|^2 - |\tilde{h}_1(\omega)|^2\right) d\omega,$$
$$\tilde{B}_2 = \frac{\tau}{4\pi}\int_{-\infty}^{\infty}\left(\left[1 + \frac{2}{N_0}G_2(\omega)\right]^2 - \left[1 + \frac{2}{N_0}G_1(\omega)\right]^2\right) \times$$

$$\times\left(|\tilde{h}_2(\omega)|^2-|\tilde{h}_1(\omega)|^2\right)^2 d\omega,$$

$$C(l,l_0)=\begin{cases}1+\min(0,\delta_\tau), & |l-l_0|\le|\delta_\tau|/2,\\ 1+\delta_\tau/2-|l-l_0|, & \delta_\tau|/2<|l-l_0|\le 1+|\delta_\tau|/2,\\ l_0=\lambda_0/\tau, & \\ 0, & |l-l_0|>1+|\delta_\tau|/2,\end{cases}$$

$$R_2(l_1,l_2,l_0)=\max\left\{0;\min\left(l_0+\frac{1}{2};\ l_1+\frac{\delta_\tau+1}{2};\right.\right.$$

$$\left.\left.l_2+\frac{\delta_\tau+1}{2}\right)-\max\left(l_0-\frac{1}{2};l_1-\frac{\delta_\tau+1}{2};l_2-\frac{\delta_\tau+1}{2}\right)\right\}.$$

Из (11) следует, что сигнальная функция $\tilde{S}(l)$ имеет плоскую вершину, протяженностью $|\delta_\tau|$, занимающую интервал $\Gamma_0=[l_0-|\delta_\tau|/2;l_0+|\delta_\tau|/2]$. В частности, сигнальная функция максимальна при $l=l_0$, следовательно, выходное отношение сигнал-шум [7] запишется в виде

$$\tilde{z}^2=\frac{\left[\tilde{S}(l)-\tilde{S}_0(1+\delta_\tau)\right]^2}{K_{\tilde{N}}(l_0,l_0)}=$$

$$=\frac{\tilde{A}^2\left[1+\min(0,\delta_\tau)\right]^2}{\tilde{B}_1(1+\delta_\tau)+\tilde{B}_2\left[1+\min(0,\delta_\tau)\right]}.$$

Рассмотрим отдельно два случая: $\delta_\tau=0$ и $\delta_\tau\neq 0$. Предположим вначале, что $\delta_\tau\neq 0$. При выполнении гипотезы H_0 (3) представим $\tilde{L}(l)$ в виде $\tilde{L}(l)=\tilde{S}_0(1+\delta_\tau)+\tilde{N}(l)$, где $\tilde{N}(l)$ – асимптотически (при $\tilde{\mu}\to\infty$) гауссовский стационарный центрированный случайный процесс с корреляционной функцией $\left\langle\tilde{N}(l_1)\tilde{N}(l_2)\right\rangle=\tilde{B}_1R_1(l_1,l_2)$, а $\tilde{S}_0$, $\tilde{B}_1$ и $R_1(l_1,l_2)$ определены в (10). Тогда вероятность ошибки 1-го рода запишется как

$$\tilde{\alpha}=P\left[\sup_{l\in\Gamma}\tilde{L}(l)>\tilde{c}\right]=$$

$$=P\left[\sup_{l\in\Gamma}\tilde{N}(l)>\tilde{c}-\tilde{S}_0(1+\delta_\tau)\right],\ \Gamma=\left[\tilde{L}_1;\tilde{L}_2\right],\quad(12)$$

где $\tilde{L}_i=\tilde{\Lambda}_i/\tau$. Введем в рассмотрение стационарный центрированный гауссовский случайный процесс $r(l)$, корреляционная функция которого имеет вид $K_r(l_1,l_2)=\max(0;1-|l_1-l_2|)$. Тогда (12) перепишется следующим образом:

$$\tilde{\alpha}=1-P\left[\sup_{l\in\Gamma}r(l/(1+\delta_\tau))<\tilde{u}\right],$$

$$\tilde{u}=\left(\tilde{c}-\tilde{S}_0(1+\delta_\tau)\right)\Big/\sqrt{\tilde{B}_1(1+\delta_\tau)}.$$

При $\tilde{m}=\tilde{L}_2-\tilde{L}_1\to\infty$ и $\tilde{u}\to\infty$ в [8] получена аппроксимация функции распределения $P\left[\sup_{l\in\Gamma}r(l)<u\right]$. Воспользовавшись этой аппроксимацией, запишем приближенное выражение для вероятности ошибки 1-го рода:

$$\tilde{\alpha}\approx F_1(\tilde{m}/(1+\delta_\tau),\tilde{u}),\quad(13)$$

где функция $F_1(\cdot)$ определена в (7).

Найдем теперь вероятность ошибки 2-го рода, представив ее аналогично [8] в виде

$$\tilde{\beta}=P\left[\sup_{l\in\Gamma}\tilde{L}(l)<\tilde{c}\right]\approx P[H_N<\tilde{c}]P[H_s<\tilde{c}].\quad(14)$$

Здесь H_N – абсолютный максимум $\tilde{L}(l)$ при $l\in\Gamma_N$, H_s – абсолютный максимум $\tilde{L}(l)$ при $l\in\Gamma_s$, где $\Gamma_s=[l_0-1/2-|\delta_\tau|/2;l_0+1/2+|\delta_\tau|/2]$, а $\Gamma_N=\left[\left[\tilde{L}_1;l_0-1/2-|\delta_\tau|/2\right);\left(l_0+1/2+|\delta_\tau|/2;\tilde{L}_2\right]\right]$. Приближенное выражение для вероятности $P[H_N<\tilde{c}]$ при $\tilde{m}>>1$ можно записать как [8]

$$P[H_N<\tilde{c}]\approx 1-\tilde{\alpha},\quad(15)$$

где $\tilde{\alpha}$ определена в (13).

Найдем вероятность $P[H_N<\tilde{c}]$. При большом $\tilde{z}$ положение $\hat{l}$ абсолютного максимума $\tilde{L}(l)$ лежит в малой окрестности точки l_0, т. е. можно считать, что $\hat{l}\in[l_0-|\delta_\tau|/2;l_0+|\delta_\tau|/2]$. На этом интервале $\tilde{S}(l)=\tilde{S}(l_0)=\tilde{S}_0(1+\delta_\tau)+\tilde{A}[1+\min(0,\delta_\tau)]$, а шумовая функция $\tilde{N}(l)$ является асимптотически (при $\tilde{\mu}\to\infty$) гауссовским стационарным центрированным случайным процессом с корреляционной функцией

$$K_{\tilde{N}}(l_1,l_2)=\begin{cases}(\tilde{B}_1+\tilde{B}_2)R_1(l_1,l_2), & \delta_\tau<0,\\ \tilde{B}_1R_1(l_1,l_2)+\tilde{B}_2, & \delta_\tau\ge 0.\end{cases}$$

Поэтому при $\tilde{z}>>1$ и $\tilde{\mu}>>1$ можно записать

$$P[H_s<\tilde{c}]\approx$$

$$\approx P\left[\max_{\tilde{l}\in[0;\tilde{m}_-]}r(\tilde{l})<\left(\tilde{c}-\tilde{S}_0(1+\delta_\tau)-\tilde{A}[1+\min(0,\delta_\tau)]\right)\Big/\tilde{\sigma}\right],\quad(16)$$

где

$$\tilde{m}_s = \begin{cases} |\delta_\tau|/(1+\delta_\tau), & \delta_\tau < 0, \\ |\delta_\tau|\tilde{B}_1/\left(\tilde{B}_2 + \tilde{B}_1(1+\delta_\tau)\right), & \delta_\tau \geq 0, \end{cases}$$

$$\tilde{\sigma}^2 = \begin{cases} \left(\tilde{B}_1 + \tilde{B}_2\right)(1+\delta_\tau), & \delta_\tau < 0, \\ \tilde{B}_2 + \tilde{B}_1(1+\delta_\tau), & \delta_\tau \geq 0. \end{cases}$$

Вероятность (16) можно найти, если выполняется условие $\tilde{m}_s \leq 1$. Для этого требуется, чтобы

$$\delta_\tau \geq -\frac{1}{2}. \qquad (17)$$

Полагая условие (17) выполненным и используя результаты [9], получаем приближенное выражение для искомой вероятности

$$P[H_s < \tilde{c}] \approx$$

$$\approx \Psi\left\{\left(\tilde{c} - \tilde{S}_0(1+\delta_\tau) - \tilde{A}[1+\min(0,\delta_\tau)]\right)\Big/\tilde{\sigma}; \tilde{m}_s\right\}. \qquad (18)$$

Здесь обозначено

$$\Psi(u,\rho) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u}\Phi\left(\frac{u - x(1-\rho)}{\sqrt{\rho(2-\rho)}}\right)\exp\left(-\frac{x^2}{2}\right)dx -$$

$$-\frac{\sqrt{\rho(2-\rho)}}{2\pi}\exp\left[-u^2/(2-\rho)\right] -$$

$$-\rho u\exp(-u^2/2)\Phi\left(u\sqrt{\rho/(2-\rho)}\right)/\sqrt{2\pi}.$$

Подставляя (15), (18) в (14), находим приближенное выражение для вероятности ошибки 2-го рода

$$\tilde{\beta} \approx (1-\tilde{\alpha})\Psi\left\{\left(\tilde{c} - \tilde{S}_0(1+\delta_\tau) - \tilde{A}[1+\min(0,\delta_\tau)]\right)\Big/\tilde{\sigma}; \tilde{m}_s\right\}.$$

Точность этого выражения возрастает с увеличением $\tilde{m}, \tilde{\mu}$ и $\tilde{u}$.

Рассмотрим теперь случай, когда длительность модулирующего импульса стороннему наблюдателю известна точно, т. е. $\delta_\tau = 0$. Воспользовавшись результатами [4], получаем следующие выражения для вероятностей ошибок 1-го и 2-го родов при $\delta_\tau = 0$:

$$\begin{aligned} &\tilde{\alpha} \approx F_1(\tilde{m}, \tilde{u}_0),\ \tilde{u}_0 = \left(\tilde{c} - \tilde{S}_0\right)\Big/\sqrt{\tilde{B}_1}, \\ &\tilde{\beta} \approx (1-\tilde{\alpha})F_2(\tilde{u}_0, \tilde{f}, \tilde{\psi}, \tilde{z}), \\ &\tilde{f}^2 = \tilde{B}_1\Big/\left(\tilde{B}_1 + \tilde{B}_2\right),\ \tilde{\psi} = 2\Big/\left(1+\tilde{f}^2\right), \\ &\tilde{z}^2 = \tilde{A}^2\Big/\left(\tilde{B}_1 + \tilde{B}_2\right). \end{aligned} \qquad (19)$$

Качество обнаружения при несанкционированном доступе, как и при санкционированном, будем характеризовать пороговым входным ОСШ $\tilde{q}_t$, которое обеспечивает заданные величины вероятностей ошибок 1-го и 2-го родов. Из (19) следует, что при $\tilde{\alpha} = \tilde{\beta} = p$ пороговое входное ОСШ $\tilde{q}_t$ можно найти из решения системы уравнений вида

$$F_1(\tilde{m}/(1+\delta_\tau), \tilde{u}) = p,$$

$$\Psi\left\{\left(\tilde{c} - \tilde{S}_0(1+\delta_\tau) - \tilde{A}[1+\min(0,\delta_\tau)]\right)\Big/\tilde{\sigma}; \tilde{m}_s\right\} = p/(1-p),$$

если $\delta_\tau \neq 0$, или

$$F_1(\tilde{m}, \tilde{u}_0) = p,$$

$$F_2(\tilde{u}_0, \tilde{f}, \tilde{\psi}, \tilde{z}) = p/(1-p),$$

если $\delta_\tau = 0$.

Количественно степень скрытности ИЧВМ будем характеризовать отношением $\varphi = \tilde{q}_t / q_{0t}$, где q_{0t} и $\tilde{q}_t$ – пороговые входные ОСШ при санкционированном и несанкционированном доступах. Чем больше параметр φ, тем большей скрытностью обладает радиоэлектронная система (РЭС), использующая сигналы с ИЧВМ ШН и тем сложнее обнаружить факт передачи информации такой РЭС с помощью КП обнаружителя при несанкционированном доступе.

Проанализируем характер поведения параметра скрытности φ в различных условиях. Предварительно отметим, что обнаружитель является состоятельным [8], если при заданной вероятности ошибки 1-го рода α вероятность ошибки 2-го рода $\beta \to 0$ при неограниченном увеличении выходного ОСШ. Как известно [8], МП обнаружитель всегда является состоятельным, чего нельзя в общем случае сказать о КП обнаружителе. К сожалению, проверить выполнение условия состоятельности КП обнаружителя возможно лишь численно. Как показывают расчеты, при расстройке только по длительности модулирующего импульса, т. е. в случае, когда $\delta_\tau = \left(\tilde{\tau} - \tau\right)/\tau \neq 0$, КП обнаружитель остается состоятельным при любых $\delta_\tau \in [0{,}5; \infty)$. При расстройке только по ширине полосы частот спектра мощности ШН, т. е. при $\delta_\Omega = \left(\tilde{\Omega}_s - \Omega_s\right)/\Omega_s \neq 0$, КП обнаружитель является

состоятельным лишь в некотором интервале $\delta_\Omega \in (\delta_{\Omega\min}; \delta_{\Omega\max})$, где $\delta_{\Omega\min}$ и $\delta_{\Omega\max}$ – соответственно минимально и максимально возможные значения параметра δ_Ω, при которых КП обнаружитель еще остается состоятельным. Аналогично, при расстройке только лишь по центральной частоте спектра мощности ШН, т. е. при $\tilde{\varepsilon} = (\tilde{\nu}_i - \nu_i)/\Omega_s \neq 0$, КП обнаружитель является состоятельным при $\tilde{\varepsilon} \in (\tilde{\varepsilon}_{\min}; \tilde{\varepsilon}_{\max})$, где $\tilde{\varepsilon}_{\min}$ и $\tilde{\varepsilon}_{\max}$ – соответственно минимально и максимально возможные значения параметра $\tilde{\varepsilon}$, при которых КП обнаружитель еще остается состоятельным. Границы областей состоятельности существенно зависят от выбора параметров p, μ, ε_s, m и $\tilde{m}$.

Заметим, что несостоятельность обнаружителя (8), (9) приводит к тому, что скрытность факта передачи информации РЭС абсолютная. Это означает, что обнаружить с помощью КП обнаружителя факт передачи информации РЭС, использующей сигналы с ИЧВМ ШН, с заданными вероятностями ошибок 1-го и 2-го родов не представляется возможным. Если же алгоритм (8), (9) состоятелен, то скрытность факта передачи информации относительна. Это означает, что для обнаружения факта передачи информации РЭС, использующей сигналы с ИЧВМ ШН, с заданными вероятностями ошибок с помощью КП обнаружителя (8), (9) требуется шумовая несущая со значительно большей мощностью, чем при использовании МП обнаружителя (4), (5).

На рис. 1 приведены зависимости параметра скрытности φ, дБ, от расстройки по длительности $\lg(1+\delta_\tau) = \lg(\tilde{\tau}/\tau)$ при $\mu = 100, p = 10^{-2}, \tilde{m} = 100$. При этом предполагалось, что все остальные прогнозируемые параметры, кроме длительности, совпадают с истинными, т. е. $\tilde{\Omega}_s = \Omega_s$, $\tilde{\nu}_i = \nu_i$ $(i = 1,2)$. На рисунке сплошными линиями нанесены зависимости $\varphi(\delta_\tau)$ для прямоугольного спектра мощности, когда $f(x) = I(x)$, а штриховыми – для спектра мощности, описываемого кривой Лоренца, когда $f(x) = \left[1 + (\pi x/2)^2\right]^{-1}$. Кривые *1* построены для $\varepsilon_s = 0.25$, $m = 10$; *2* – $\varepsilon_s = 0{,}5$, $m = 10$; *3* – $\varepsilon_s = 1$, $m = 10$, *4* – $\varepsilon_s = 0{,}5$, $m = 100$. Из анализа рис. 1 следует, что при расстройке по длительности модулирующего импульса скрытность РЭС возрастает с ростом $\tilde{m}$ и уменьшением ε_s.

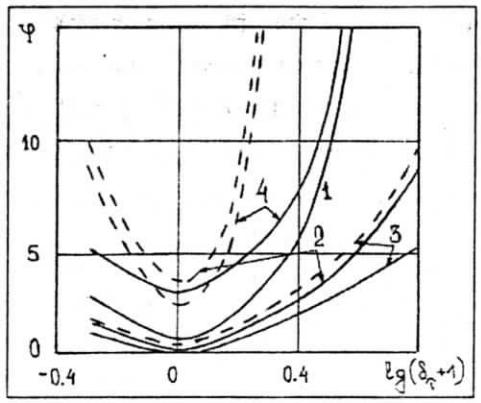

Рис. 1

На рис. 2 представлены зависимости φ, дБ, от $\delta_\Omega = (\tilde{\Omega}_s - \Omega_s)/\Omega_s$ при условии, что остальные прогнозируемые параметры совпадают с истинными, т. е. $\tilde{\tau} = \tau$, $\tilde{\nu}_i = \nu_i$ $(i = 1,2)$. Обозначения на этом рисунке соответствуют обозначениям, принятым на рис. 1. Как уже отмечалось ранее, наличие расстройки по ширине полосы частот спектра мощности ШН может привести к тому, что КП обнаружитель станет несостоятельным. Размер области изменения $(\delta_{\Omega\min}; \delta_{\Omega\max})$ параметра δ_Ω, при котором КП обнаружитель еще остается состоятельным, уменьшается с уменьшением параметров μ, p и ε_s. Так, например, для прямоугольного спектра мощности при $\mu = 100, p = 10^{-2}$, $m = 10$, $\tilde{m} = 100$ и $\varepsilon_s = 0{,}25$ $\delta_{\Omega\min} \approx -0{,}25$, $\delta_{\Omega\max} \approx 0{,}15$, а при $\varepsilon_s = 0{,}5$ $\delta_{\Omega\min} \approx -0{,}45$, $\delta_{\Omega\max} \approx 0{,}5$.

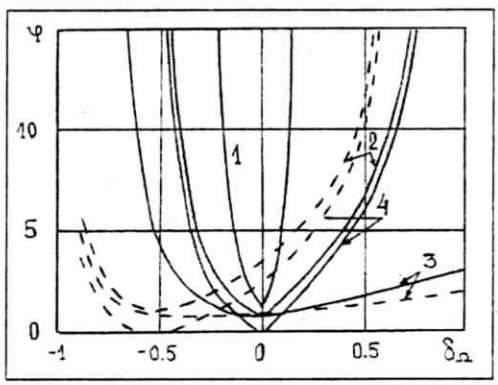

Рис. 2

На рис. 3 приведены зависимости φ, дБ, от $\tilde{\varepsilon} = (\tilde{\nu}_i - \nu_i)/\Omega_s$ при условии, что остальные прогнозируемые параметры КП обнаружителя совпадают с истинными, т. е. $\tilde{\tau} = \tau$, $\tilde{\Omega}_s = \Omega_s$. Также как и на рис. 1,2, сплошными линиями здесь нанесены

зависимости $\varphi(\tilde{\varepsilon})$ для прямоугольного спектра мощности ШН, а штриховыми – для лоренцевского спектра мощности при $\mu = 100, p = 10^{-2}, \tilde{m} = 100$. Кривые *1* построены для $\varepsilon_s = 0{,}5,\ m = 10$; *2* – $\varepsilon_s = 1,\ m = 10$; *3* – $\varepsilon_s = 0{,}5,\ m = 100$. Как и при расстройке по ширине полосы частот, расстройка по центральной частоте спектра мощности ШН может вызвать несостоятельность КП обнаружителя. Причем размер области состоятельности $(\tilde{\varepsilon}_{\min}; \tilde{\varepsilon}_{\max})$ уменьшается с уменьшением параметров μ, p и ε_s. Так, например, для прямоугольного спектра мощности ШН при $\mu = 100,\ p = 10^{-2},\ m = 10,\ \tilde{m} = 100$ и $\varepsilon_s = 0{,}5$ $\tilde{\varepsilon}_{\min} \approx -0{,}25,\ \tilde{\varepsilon}_{\max} \approx 0{,}25$, а при $\varepsilon_s = 1$ $\tilde{\varepsilon}_{\min} \approx -0{,}5,\ \tilde{\varepsilon}_{\max} \approx 0{,}5$.

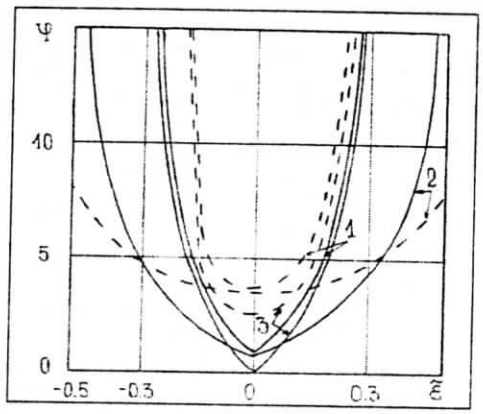

Рис. 3

Анализ рис. 1–3 показывает, что скрытность РЭС, использующей сигналы с ИЧВМ ШН, возрастает с увеличением параметра $\tilde{m}$ и уменьшением параметра ε_s. Причем наибольшее влияние на степень скрытности оказывает наличие расстройки между параметрами спектра мощности ШН Ω_s и ν_i и параметрами $\tilde{\Omega}_s$ и $\tilde{\nu}_i$, определяющими передаточную функцию фильтров КП обнаружителя (8), (9).

- Исследовано влияние расстроек между прогнозируемыми (используемыми при несанкционированном доступе) и истинными параметрами сигнала с импульсной частотно-временной модуляцией шумовой несущей на степень скрытности факта передачи информации. Установлено, что наибольшее влияние на скрытность передачи информации оказывает рассогласование между параметрами фильтров квазиправдоподобного обнаружителя и параметрами спектра мощности шумовой несущей.

Приведенные результаты получены при поддержке Российского фонда фундаментальных исследований.

Литература

1. *Харкевич А.А.* Передача сигналов модулированным шумом. – Избранные труды. Т.2. – М.: Наука, 1973.
2. *Петрович Н.Т, Размахнин М.К.* Системы связи с шумоподобными сигналами. – М.: Сов. радио, 1969.
3. *Трифонов А.П., Парфенов В.И.* Импульсная частотно-временная модуляция шумовой несущей. – Радиотехника и электроника, 1988, т. 33, № 1.
4. *Трифонов А.П., Парфенов В.И.* Теоретическое и экспериментальное исследования квазиправдоподобного приемника случайного сигнала. – Радиотехника и электроника, 1991, т. 36, № 4.
5. *Трифонов А.П., Захаров А.В., Чернояров О.В.* Пороговые характеристики квазиправдоподобной оценки времени прихода случайного радиоимпульса. – Изв. вузов. Сер. Радиоэлектроника, 1998, № 10.
6. *Трифонов А.П., Нечаев Е.П., Парфенов В.И.* Обнаружение стохастических сигналов с неизвестными параметрами. Воронеж: ВГУ, 1991.
7. *Куликов Е.И., Трифонов А.П.* Оценка параметров сигналов на фоне помех. – М.: Сов.радио, 1978.
8. *Трифонов А.П.* Обнаружение сигналов с неизвестными параметрами. – Теория обнаружения сигналов. – М.: Радио и связь, 1984.
9. *Shepp. L.A.* Radon-Nicodym derivatives of Gaussian measures. – Ann. Math. Statist, 1966, v.37.

Поступила 28 ноября 2001 г.