УДК: 681.327.8

Д.Ф. Хисамов

РАСЧЕТ АНАЛОГОВОЙ СИНХРОНИЗАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В УСЛОВИЯХ ПОМЕХ

В условиях мощных организованных помех, возникает необходимость перехода от дискретных к аналоговым методам синхронизации датчиков апериодических псевдослучайных последовательностей (АПСП). Оценка аналоговой синхронизации АПСП затруднена из-за отсутствия приемлемых математических выражений, в том числе генетических алгоритмов [1]. В данной работе впервые с использованием границы Чернова и Гаусса разработаны математические модели для оценки аналоговой синхронизации АПСП на каналах с произвольным законом распределения ошибок.

Синхронизация; псевдослучайная последовательность; алгоритм синхронизации апериодической ПСП.

D.F. Khisamov

MATHEMATICAL SIMULATION OF SYNCHRONIZATION OF APERIODIC PSEUDORANDOM SEQUENCE ON CHANNELS OF POOR QUALITY

On channels of poor quality there is a necessity of a change from discrete to analogue synchronization methods for aperiodic pseudorandom sequence timers (APST). The estimation of analogue synchronization of APST is hampered due to the lack of acceptable mathematical expressions. The given paper has pioneered the mathematical models for estimation of analogue APST synchronization on channels with the arbitrary law of errors distribution with the usage of Chernoff and Gauss bounds.

Synchronization; aperiodic pseudorandom sequence; algorithm synchronization of aperiodic PST.

1. Вывод строгой верхней границы для вероятности неприема пусковой комбинации с использованием неравенства Чернова. Пусть реализация пускового ПС-ФМ сигнала при аналоговой синхронизации имеет вид (1) и в канале присутствует аддитивная помеха ε(t) с произвольным законом распределения [2], нулевым средним и дисперсией σ^2.

$$\begin{aligned} &\alpha = 0, \quad \text{то} \quad S_1(t) = \Pi(t)\,U_C = \cos(\omega_C t + \phi), \\ &\alpha = 1, \quad \text{то} \quad S_2(t) = -S_1(t), \qquad 0 \le t \le T. \end{aligned} \tag{1}$$

где

$$\Pi(t) = \begin{cases} (-1)^{\gamma_k}, & (k-1)T_0 \le t \le kT_0, \quad k = 1,2,3...B \\ 0 & \text{при других} \quad t; \end{cases}$$

U_c – амплитуда сигнала;

T_c – длительность субэлемента сигнала;

T – длительность элемента сообщения;

$\gamma_k = (0,1)$ – псевдослучайная последовательность, неизвестная противнику, которую для краткости будем именовать гаммой.

Тогда на интервале анализа аналоговые отчеты сигнала будут иметь вид:

$$\xi_i = \begin{cases} a(-1)^{\gamma_i} + \varepsilon_i & \text{если } i \text{ принадлежит ПС;} \\ \varepsilon_i & \text{если } i \text{ принадлежит ПС;} \end{cases} \tag{2}$$

где a – амплитуда сигнала;

$\gamma_i = (0, 1)$ – равновероятные и взаимно независимые случайные величины;

$\varepsilon_i = \int\limits_{(i-1)T_0}^{iT_0} \varepsilon(t) \cdot \cos\omega_c\, tdt$ – произвольно распределенная случайная величина с нулевым средним и дисперсией σ^2.

Предположим, что пусковая комбинация (ПК) известна на приеме и состоит из N символов: $S_1, S_2, ..., S_N$. На приеме осуществляется автокорреляционный прием пускового сигнала по правилу (3), что соответствует схеме, изображенной на рис. 1.

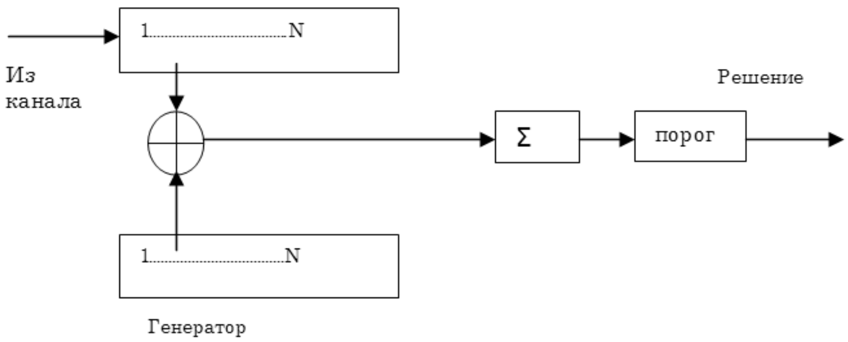

Рис. 1. Автокорреляционный прием пускового сигнала

$$\sum_{i=1}^{N} U_{i+j} \cdot S_i \underset{<}{>} U_0, \tag{3}$$

где $U_1, U_2, ..., U_L$ – принятые из канала L двоичных символов, а $S_1, S_2, ..., S_N$ – известная пусковая комбинация, состоящая из N двоичных символов.

Требуется определить вероятность неприема синхропосылки (СП), если известно, что вся пусковая комбинация входит в интервал анализа.

Рассмотрим случай, когда пусковой и опорный сигналы пересекаются. Тогда можем составить две суммы:

$$1)\ \sum_{i=1}^{N} \xi_i (-1)^{\gamma_i} = \sum_{i=1}^{N} \left(a(-1)^{\gamma_i} + \varepsilon_i \right) \cdot (-1)^{\gamma_i} = aN + \sum_{i=1}^{N} \varepsilon_i (-1)^{\gamma_i} \tag{4}$$

2) $$\sum_{i=1}^{N}\xi_i\left(-1\right)^{\gamma_i}=$$

$$=\sum_{i=1}^{N-T}\left[a\left(-1\right)^{\gamma_{i+T}}+\varepsilon_{i+T}\right]\cdot\left(-1\right)^{\gamma_i}+\sum_{i=N-T+1}^{T}\varepsilon'_{i+T}\cdot\left(-1\right)^{\gamma_i}= \tag{5}$$

$$=aR\left(T\right)+\sum_{i=1}^{N-T}\left(-1\right)^{\gamma_i}\cdot\varepsilon_{i+T}+\sum_{i=N-T+1}^{T}\left(-1\right)^{\gamma_i}\cdot\varepsilon'_{i+T}),$$

где $R(T)$ – автокорреляционная функция АПСП при сдвиге равном “T”.

Очевидно, неприем может произойти только тогда, когда первая сумма будет меньше второй (5):

$$p_{н}=p\left\{aN+\sum_{i=1}^{N}\varepsilon_i(-1)^{\gamma_i}<a\cdot R(T)+\sum_{i=1}^{N-T}(-1)^{\gamma_i}\cdot\varepsilon_{i+T}+\sum_{i=N-T+1}^{T}(-1)^{\gamma_i}\varepsilon'_{i+T}\right\}=$$

$$=p\left\{\left[a(N-R(T))+\sum_{i=1}^{N-T}(-1)^{\gamma_i}\left(\varepsilon_i-\varepsilon_{i+T}\right)+\sum_{i=N-T+1}^{T}(-1)^{\gamma_i}\left(\varepsilon_i-\varepsilon'_{i+T}\right)\right]<0\right\}. \tag{6}$$

Учитывая, что под обоими знаками суммы в правой части неравенства (6) стоят случайные величины с нулевыми средними и одинаковыми дисперсиями равными $2\sigma^2$ формулу (6) можем переписать как:

$$P_H=P\left\{a(N-R(T))+\sum_{i=1}^{N}(-1)^{\gamma_i}\cdot\eta_i<0\right\}, \tag{7}$$

где

$$\eta_i=\begin{cases}(\varepsilon_i-\varepsilon_{i+T}) & при\ \ i=1,2,3,...,N-T;\\ (\varepsilon_i-\varepsilon'_{i+T}) & при\ \ i=1,2,3,...,N.\end{cases}$$

Учитывая слабую коррелированность помехи на интервале субэлемента сигнала, предполагается взаимная независимость отсчетов η_i и поэтому для оценки (7) используем границу Чернова в виде:

$$P\left\{x\le b\right\}\le g(t)\cdot e^{-Bt},\qquad t\le 0, \tag{8}$$

где $g\left(t\right)=M\left\{e^{t\cdot x}\right\}$.

Полагая в (8) $x = a \cdot \left[N - R(T)\right] + \sum\limits_{i=1}^{N} (-1)^{\gamma_i} \cdot \eta_i$ и $B = 0$, получим границу для вероятности неприема СП в виде:

$$p_н \le \min g\left(t\right), \quad при \quad t \le 0, \tag{9}$$

где

$$g\left(t\right) = M\left\{ e^{t \cdot \left[a\left(N - R(T)\right) + \sum\limits_{i=1}^{N} (-1)^{\gamma_i} \cdot \eta \right]} \right\},$$

математическое ожидание вычисляется относительно γ_i ***и*** η_i; $\boldsymbol{i} = 1,2,3,\ldots,\boldsymbol{N}$.

$$M\left\{ e^{t \cdot \left[a\left(N - R(T)\right) + \sum\limits_{i=1}^{N} \left(-1^{\gamma_i}\right) \cdot \eta_i \right]} \right\} = e^{t \cdot a\left[N - R(t)\right]} \cdot \prod_{i=1}^{N} \frac{e^{t\eta_i} + e^{-t\eta_i}}{2} =$$

$$= e^{t \cdot a\left[N - R(t)\right]} \cdot \prod_{i=1}^{N} ch\left(t \cdot \eta_i\right) \le e^{t \cdot a\left[N - R(t)\right] + \frac{t^2}{2} \sum\limits_{i=1}^{N} \eta_i^2}. \tag{10}$$

Найдем математическое ожидание относительно γ_i, где последнее неравенство (10) получено из условия $ch(x) \le e^{\frac{x^2}{2}}$.

Учитывая, что η_i центрированная величина (10) можем переписать как:

$$g(t) \le e^{t \cdot a\left[N - R(T)\right] + t^2 \cdot N\sigma^2}. \tag{11}$$

Легко показать, что показатель степени в (11) минимизируется при:

$$t_{опт} = \frac{-a \cdot \left[N - R(T)\right]}{2N \cdot \sigma^2},$$

тогда окончательно имеем:

$$P_н \le \min_{t \le 0} g(t) = e^{-\frac{a^2\left[N - R(T)\right]^2}{\delta^2 \cdot 2N} + \frac{a^2\left[N - R(T)\right]^2}{\delta^2 \cdot 4N}} = e^{-\frac{H^2\left[N - R(T)\right]^2}{4N}}, \tag{12}$$

где $H^2 = \dfrac{a^2}{\sigma^2}$ – отношение средней энергии элемента сигнала на входе приемника к спектральной плотности помехи.

Для оценки вероятности неприема ПК на всем интервале анализа L используем аддитивную границу Буля [3], тогда окончательно получим:

$$\overline{P}_H \le (L-2N)\cdot e^{-\frac{H^2\cdot N}{4}} + \sum_{i=1}^{N-1} e^{-\frac{H^2[N-R(T)]^2}{4N}}. \quad (13)$$

Неравенство (13) дает строгую верхнюю границу для вероятности неприема ПС при произвольных помехах в канале. Представляет интерес рассмотреть некоторые частные случаи, например, когда помеха в канале типа белого гауссовского шума (БГШ).

2. Вывод точной формулы для вероятности неприема ПК в условиях гауссовских помех. В частном случае, когда помеха гауссовская с нулевым средним и с дисперсией δ^2 легко получить точную формулу. Для этого (7) представим как:

$$P_H = P\left\{\sum_{i=1}^{N}(-1)^{\gamma_i}\cdot\eta_i > a[N-R(T)]\right\} = P\{\tilde{\eta} > a[N-R(T)\}, \quad (14)$$

где $\tilde{\eta} = \sum_{i=1}^{N}(-1)^{\gamma_i}\cdot\eta_i$ гауссовская величина с нулевым средним и дисперсией равной $2N\delta^2$.

Тогда для (14) можем получить точную формулу в виде [3]:

$$P_H = P\{\tilde{\eta} > a[N-R(T)]\} = \int_{a[N-R(T)]}^{\infty} \frac{1}{2\delta\sqrt{\pi N}}\cdot e^{-\frac{x^2}{4n\delta^2}}dx =$$
$$= 1 - F\left(a[N-R(T)\big/\delta\sqrt{2N}\right) = 1 - F\left(H[N-R(T)]\big/\sqrt{2N}\right), \quad (15)$$

где $F(x) = 1\big/\sqrt{2\pi}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}dt$ – интеграл вероятности.

Для определения вероятности неприема пускового сигнала на интервале анализа, опять воспользуемся аддитивной границей и получим окончательное выражение в виде:

$$\overline{P}_H < (L-2N)\cdot\left[1 - F\left(H\sqrt{\frac{N}{2}}\right)\right] + \sum_{T=1}^{N-1}\left[1 - F\left(\frac{H[N-R(T)]}{\sqrt{2N}}\right)\right]. \quad (16)$$

Известно, что в классе помех с произвольным законом распределения, гауссовская помеха всегда дает нижнюю границу для вероятности ошибки [3]. Поэтому выражение (16) можно рассматривать как нижнюю границу вероятности неприема ПК в случае произвольных помех в канале. На рис. 2 приведены нижняя и верхняя границы вероятности неприема ПК $\overline{P}_H = \varphi\left(H^2\right)$ для различных N при аналоговом запуске и произвольных помехах в канале, рассчитанные по (13) и (16) соответственно.

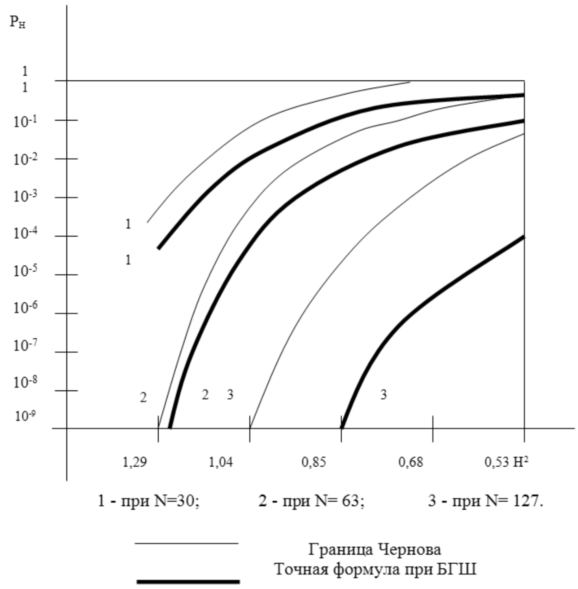

Рис. 2. Нижняя и верхняя границы вероятности неприема ПК $\overline{P}_H = \varphi\left(H^2\right)$ *для различных N при аналоговом запуске*

Известно, что в классе помех с произвольным законом распределения, гауссовская помеха всегда дает нижнюю границу для вероятности ошибки [2]. Поэтому выражение (16) можно рассматривать как нижнюю границу вероятности неприема ПК в случае произвольных помех в канале. На рисунке (см. рис. 2) приведены нижняя и верхняя границы вероятности неприема ПК $\overline{P}_H = \varphi\left(H^2\right)$ для различных N при аналоговом запуске и произвольных помехах в канале, рассчитанные по (13) и (16) соответственно.

Из анализа кривых, приведенных на графике (см. рис. 2) видно, что верхняя граница (13), полученная с использованием неравенства Чернова, дает достаточно плотные результаты (кривые 1 и 2) и, следовательно, будет хорошей оценкой вероятности неприема $\overline{P}_H$ при произвольных слабо коррелированных помехах в канале.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Курейчик В.М.* Об одной модели эволюции Шмальгаузена // Известия ЮФУ. Технические науки. – 2009. – № 4 (93). – С. 7-16.
2. *Коржик В.И., Финк Л.М.* Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. – М.: Связь, 1975.
3. *Хисамов Д.Ф.* Граничные оценки вероятности синхронизации псевдослучайной последовательности на каналах с произвольным распределением ошибок \ Материалы международного конгресса «Математика в XXI веке» // 25-28 июня 2003 г. – Новосибирск: Академгородок, 2003 г. http://www.sbras.ru/ws/MMF-21/.

Хисамов Денис Франгизович
Некоммерческое частное образовательное учреждение высшего профессионального образования «Кубанский институт информзащиты» в г. Краснодаре.
E-mail: kiiz@rambler.ru.
г. Краснодар, Авиагородок, 22, кв. 99.
Тел.: 88612523031.
Кафедра комплексной защиты информации; доцент.

Hisamov Denis Frangizovich
Kuban Information Security Institute, Non-commercial Private Educational Institution of Higher Professional Education, Krasnodar.
E-mail: kiiz@rambler.ru.
22, ap.99, Aviagorodok, Krasnodar, Russia.
Phone: 88612523031.
Department of Complex Information Protection; associate professor.