УДК 519.92

**И. П. Кобяк**, канд.техн.наук
Белорусский государственный университет
информатики и радиоэлектроники
(Республика Беларусь, 220600, Минск, ул. П. Бровки, 6,
тел. 2938617, e-mail: IPKobyak2012@mail.ru)

# Моменты распределения вероятности ошибки при наблюдении автокорреляционной функции в идеальном канале криптографической шумоподобной системы связи

Определены математическое ожидание и дисперсия функции распределения вероятностей ошибки при наблюдении заданных пар векторов в последовательностях случайных событий. Расчеты выполнены на основе производящей функции, позволяющей представить все результаты некоторого класса комбинаторных задач в виде суммы $n-2$ полиномиальных форм. Исследованы свойства точечных оценок автокорреляционной функции: состоятельность, несмещенность, эффективность и достаточность выборочных параметров.

Визначено математичне сподівання і дисперсія функції розподілу ймовірностей похибки при спостереженні заданих пар векторів у послідовностях випадкових подій. Розрахунки базовані на твірній функції, яка дозволяє зобразити всі результати певного класу комбінаторних задач у вигляді суми $n-2$ поліноміальних форм. Досліджено властивості точкових оцінок автокореляційної функції: обґрунтованість, незсуненість, ефективність і достатність вибіркових параметрів.

*К л ю ч е в ы е  с л о в а: элементарные события, дисперсия, идентификация последовательностей, вероятность пропуска ошибки, сигнатурный анализ, производящая функция.*

**Постановка задачи.** Системы кодирования и передачи данных по принципу представления информации в каналах связи могут быть разделены на две большие группы: шумоподобные системы связи (ШПСС) и системы с теоретико-числовым шифрообразующим началом.

Системы связи с многомерными шумоподобными каналами имеют ряд преимуществ перед обычными криптосистемами шифрования информации. В частности, можно считать, что идеальные статистические свойства передаваемых последовательностей со случайной или псевдослучайной природой придают сообщениям дополнительный аспект кодирования, так как время появления передаваемого текста непредсказуемо. Кроме того, обнаружение зашумленных каналов может быть затруднено, если база сообщения достаточно велика, имеет прецизионные вероятностные характеристики, а

текст сообщения неравномерно распределен по базе. При этом повышается помехозащищенность [1] и статистически сглаживаются места объединения информации вида «шум — шифрованное сообщение». Однако длительное пребывание канала в эфире дает достаточно много информации стороннему наблюдателю об использованных методах кодирования и открывает широкие возможности для применения компьютерных систем с целью обнаружения и раскодирования текстов. Основной алгоритм в решении данной задачи — это подбор ключевой последовательности длиной $n$ со свойствами, близкими к статистически эталонным.

В пользу систем поточного шифрования, например на основе цифровых принципов Гиффорда, свидетельствует также следующее обстоятельство. Известно, что выходное сообщение $s(\mu)$ системы шифрования формируется как сумма: сигнал $\mu$ плюс шум $s$. Если длина полезного сигнала определяется числом $n$ (бит), то число последовательностей в области центра распределения может быть представлено в виде [2, 3]

$$2C_n^{0,5n} + 2\sum_{k=1} C_n^{0,5n+k} = \frac{2^n}{\sqrt{0{,}5\pi n}}\left[2 + 2\sum_{k=1} e^{-\frac{2k^2}{n}}\right], \qquad (1)$$

где $0 < k << n$, $n$ — нечетно, что и определяет верхнюю границу длительности вычислений при раскодировании.

Различные методы криптографии, основанные на смешанных алгоритмах теории чисел и шумоподобного шифрования, также дают возможность формировать сообщения длиной $n$ со свойствами, удовлетворяющими свойствам последовательностей (1). Следовательно, раскодирование и тех и других шифрованных сообщений может осуществляться только с использованием случайного перебора, что, в свою очередь, приводит к мысли о возможном использовании только генераторов шума для шифрования сообщений в системах связи.

С учетом изложенной концепции использования ШПСС обнаружение детерминизма в канале связи может быть выполнено различными методами, например посредством анализа функций распределения статистик элементарных событий при переменных значениях длины выборки $n$. При этом, как правило, в качестве событий рассматриваются векторы состояний канала, а для выявления детерминизма используются различные теоретические [4] и эвристические критерии.

Более эффективным алгоритмом обнаружения неслучайных включений в сообщение считается принцип формирования автокорреляционной функции (АКФ) [5, 6], по отклонениям которых от нормы принимается решение о наличии или отсутствии детерминизма в последовательности. В целом вопросы, связанные с анализом каналов на основе выборочных

параметров числа векторов состояний исследованы достаточно широко. Однако комплексные характеристики методов наблюдения эмпирических или теоретических АКФ практически не изучены, что объясняется сложностью получения производящих функций и вычисления диапазона представления сумм соответствующих вероятностей.

Выполним расчет эталонных матожидания, дисперсии и эффективности оценок АКФ при наблюдении пар векторов состояний, сдвинутых одна относительно другой на интервал времени $\tau = 1$.

**Математическое ожидание распределения вероятностей пропуска ошибки при наблюдении пар коррелированных векторов.** В работе [6] показано, что сокращенным соотношением для энумератора вида

$$m_K(0) = m_{k=0}(0) + \sum_{g=2}^{n-1}\left[\sum_{j=1}^{0,5n-3} p^j x_j^2 (x_j + 1 + p)\frac{1 - q_2^{0,5n-j-2} x_j^{n-2j-4}}{1 - q_2 x_j^2} - \right.$$

$$- \sum_{j=1}^{0,5n-2} (p^j q_2^{0,5n-j-2} x_j^{n-2j-3} - p^{j-1} q_1 q_2^{0,5n-j-1} x_j^{n-2j-2} +$$

$$+ p^{j-1}\sqrt{p} q_1 q_2^{0,5n-j-1} x_j^{n-2j-1} + p^j q_1 q_2^{0,5n-j-1} x_j^{n-2j}) -$$

$$\left. - p^{0,5(n-2)} \frac{1}{\sqrt{p}} q_1 x_{\frac{n-2}{2}}^1 + p^{0,5(n-2)} q_1 x_{\frac{n-2}{2}}^2 - p^{\frac{n}{2}} x_{\frac{n}{2}}^0 - \left(1 + \sum_{j=2}^{0,5n-3} p^{j-1}\right)\right]^{n-g}$$

при $t \neq 0$, $n \to \infty$ является соотношение

$$m_K(t) = \sum_{g=2}^{n-1}\left[\sum_{j=1}^{0,5n-3} p^j e^{jt} \frac{1+q_1}{1-q_2} + \xi(t)\right]^{n-g}, \quad p = \frac{1}{m^2}, \quad m = 2^r, \tag{2}$$

где $q_1 = 1 - p$; $q_2 = 1 - 2p$; $K$ — случайная величина, характеризующая число пар векторов. Выполнив дифференцирование соотношения для производящей функции по времени, получим выражение для математического ожидания данного параметра. С учетом (2) запишем соотношение

$$m'_K(t) = \sum_{g=2}^{n-1}(n-g)\left[\sum_{j=1}^{0,5n-3} p^j e^{jt}\frac{1+q_1}{1-q_2} + \xi(t)\right]^{n-g-1}\left[\sum_{j=1}^{0,5n-3} p^j j e^{jt}\frac{1+q_1}{1-q_2} + \frac{\partial}{\partial t}\xi(t)\right],$$

которое при $t = 0$ принимает вид

$$m'_K(0) = \sum_{g=2}^{n-1}(n-g)\left[\frac{1+q_1}{1-q_2}\sum_{j=1}^{0,5n-3} p^j + \xi(0)\right]^{n-g-1}\left[\frac{1+q_1}{1-q_2}\sum_{j=1}^{0,5n-3} j p^j + \frac{\partial}{\partial t}\xi(t)_{|t=0}\right]. \tag{3}$$

Рассмотрим первый множитель в функции (3). Используя параметры $q_1$, $q_2$ а также принцип суммирования рядов, запишем

$$\sum_{g=2}^{n-1}(n-g)\left[\frac{1+q_1}{1-q_2}\sum_{j=1}^{0,5n-3}p^j+\xi(0)\right]^{n-g-1}=\sum_{g=2}^{n-1}(n-g)\left[\frac{2-p}{2}\frac{1}{1-p}+\xi(0)\right]^{n-g-1}. \quad (4)$$

В соотношении (4) необходимо выбрать допустимое значение элемента суммы $\xi(0)$, что обусловлено фактом наличия множителя $[\xi(0)]^0$ в факториальном представлении производящей функции. Данный элемент должен быть выбран исходя из концепции взаимодействия электрических полей в мнимом и реальном пространствах [7]. В противном случае $m_K(0)$ будет либо превышать допустимую величину теоретического параметра, либо иметь отрицательное значение. Учитывая данный факт, из (4) получаем

$$\sum_{g=2}^{n-1}(n-g)\left[\left(1+\frac{p}{2}\right)\frac{1}{1-p}-\frac{1}{1-p}\right]^{n-g-1}=\sum_{g=2}^{n-1}(n-g)\left[\frac{p}{2(1-p)}\right]^{n-g-1}, \quad (5)$$

где $\xi(0)=-1/(1-p)$, т.е. функция $\xi(0)$ выбрана равной «емкостному» значению, чтобы компенсировать вероятностную «индуктивную» составляющую в левой части соотношения (5). При этом знак слагаемого $p/2$ в разности $\frac{2-p}{2}\frac{1}{1-p}=\left(1-\frac{p}{2}\right)\frac{1}{1-p}$ меняется на противоположный, что обусловлено выбором знака $\xi(0)$ и, соответственно, направлением действия «электрических полей» в комплексном пространстве (см. рисунок). Значение $p/2$ интерпретируется как активное сопротивление, которое всегда создает положительно направленное поле.

Для получения численного значения (5) выполним суммирование членов степенного ряда, введя обозначение $a=\frac{p}{2(1-p)}$. Тогда $\sum_{i=1}^{n-2}ia^{i-1}=$ $=\frac{1}{(1-a)^2}$, откуда находим $\frac{1}{(1-a)^2}=\frac{4(1-p)^2}{(2-3p)^2}$. Второй множитель в (3) с учетом изменения знака индуктивной вероятности приводим к виду

$$\frac{1+q_1}{1-q_2}\sum_{j=1}^{0,5n-3}jp^j+\frac{\partial}{\partial t}\xi(t)=\sum_{j=1}^{0,5n-3}jp^{j-1}-\frac{1}{2}\sum_{j=1}^{0,5n-3}jp^j+\frac{\partial}{\partial t}\xi(t)=\left|\sum_{j=1}^{0,5n-3}jp^j\right|, \quad (6)$$

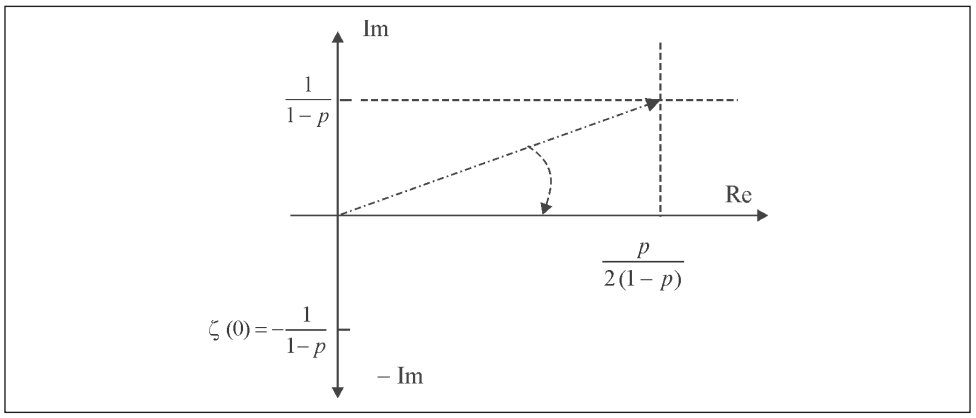


Схема компенсации реактивностей в комплексном пространстве

где

$$\frac{\partial}{\partial t}\xi(t) = -\sum_{j=1}^{0,5n-3} jp^{j-1} - \sum_{j=1}^{0,5n-3} jp^{j} + \frac{1}{2}\sum_{j=1}^{0,5n-3} jp^{j},$$

что необходимо для компенсации индуктивной и емкостной составляющих в равенстве (6). При этом получаем

$$\sum_{j=1}^{0,5n-3} jp^{j} = p\frac{1}{(1-p)^2}.$$

Окончательно математическое ожидание функции распределения вероятностей пропуска ошибки в случайном сообщении при $p = 1/m^2$ определяется равенством

$$m'_K(0) = \frac{4(1-p)^2}{(2-3p)^2}\, p\, \frac{1}{(1-p)^2} = \frac{4p}{(2-3p)^2}. \qquad (7)$$

Полагая, что $m >> 1$ и $(2-3p)^2 \approx 4$, из (7) находим параметр

$$m'_K(0) \to p. \qquad (8)$$

**Дисперсия распределения вероятности ошибки при наблюдении пар векторов.** Для определения дисперсии исследуемого параметра воспользуемся классическим соотношением $D_K = m''_K(0) - [m'_K(0)]^2$. Продифференцируем это равенство для момента $m'_K(t)$, используя вспомогательный параметр $e^t$ степенного ряда производящей функции. При этом вторая производная принимает вид

$$m''_K(t) = \sum_{g=2}^{n-1}(n-g)(n-g-1)\left[\sum_{j=1}^{0,5n-3} p^j e^{jt}\frac{1+q_1}{1-q_2} + \xi(t)\right]^{n-g-2} \times$$

$$\times\frac{\partial}{\partial t}\left[\sum_{j=1}^{0,5n-3}p^j e^{jt}\frac{1+q_1}{1-q_2}+\xi(t)\right]\left[\sum_{j=1}^{0,5n-3}p^j je^{jt}\frac{1+q_1}{1-q_2}+\frac{\partial}{\partial t}\xi(t)\right]+$$

$$+\sum_{g=2}^{n-1}(n-g)\left[\sum_{j=1}^{0,5n-3}p^j e^{jt}\frac{1+q_1}{1-q_2}+\xi(t)\right]^{n-g-1}\frac{\partial}{\partial t}\left[\sum_{j=1}^{0,5n-3}p^j je^{jt}\frac{1+q_1}{1-q_2}+\frac{\partial}{\partial t}\xi(t)\right]. \quad (9)$$

Преобразуем первую составляющую во второй производной к виду

$$m''_{K1}(t)=\sum_{g=2}^{n-1}(n-g)(n-g-1)\left[\frac{1}{2}\sum_{j=1}^{0,5n-3}p^j\right]^{n-g-2}\left[\sum_{j=1}^{0,5n-3}p^j je^{jt}\frac{1+q_1}{1-q_2}+\frac{\partial}{\partial t}\xi(t)\right]^2.$$

Тогда

$$\sum_{g=2}^{n-1}(n-g)(n-g-1)\left[\frac{1}{2}p\frac{1}{1-p}\right]^{n-g-2}=\left|a=\frac{1}{2}p\frac{1}{1-p}\right|=$$

$$=\frac{\partial^2}{\partial a^2}\iint\sum_{g=2}^{n-1}(n-g)(n-g-1)\,a^{n-g-2}da^2=\frac{\partial^2}{\partial a^2}\sum_{g=2}^{n-1}a^{n-g}=$$

$$=\frac{\partial}{\partial a}\frac{1}{(1-a)^2}=\frac{16(1-p)^3}{(2-3p)^3}.$$

С учетом (5) квадратичная форма для $m''_{K1}(t)$ примет вид

$$\left[\sum_{j=1}^{0,5n-3}p^j je^{jt}\frac{1+q_1}{1-q_2}+\frac{\partial}{\partial t}\xi(t)\right]^2=\left[\frac{2-p}{2}\frac{1}{(1-p)^2}+\frac{\partial}{\partial t}\xi(t)\right]^2=$$

$$=\left[\frac{1}{(1-p)^2}-\frac{p}{2}\frac{1}{(1-p)^2}+\frac{\partial}{\partial t}\xi(t)\right]^2=\left[\frac{p}{2(1-p)}\right]^2.$$

Таким образом, первая составляющая во второй производной (9) представляет собой нормированную величину

$$m'_{K1}(0)=\frac{16(1-p)^3}{(2-3p)^3}\frac{1}{4}p^2\frac{1}{(1-p)^2}=\frac{4(1-p)}{(2-3p)^3}p^2\approx\frac{1}{2}p^2.$$

Вторая составляющая второй производной может быть рассчитана в соответствии с аналогичной методикой компенсации вероятностных «реактивных энергий». В частности, полагая, что $t=0$ и $(1+q_1)/(1-q_2)=(2-p)/2p$, на

основании рассуждений, использованных при формировании равенства (5), получим соотношение

$$m''_{K2}(0)=\sum_{g=2}^{n-1}(n-g)\left[\sum_{j=1}^{0,5n-3}p^j e^{jt}\,\frac{1+q_1}{1-q_2}+\xi(t)\right]^{n-g-1}\times$$

$$\times\frac{\partial}{\partial t}\left[\sum_{j=1}^{0,5n-3}p^j je^{jt}\,\frac{1+q_1}{1-q_2}+\frac{\partial}{\partial t}\xi(t)\right]=$$

$$=\sum_{g=2}^{n-1}(n-g)\left[\frac{p}{2}\frac{1}{1-p}\right]^{n-g-1}\left[\frac{2-p}{2p}\,p\sum_{j=1}^{0,5n-3}j^2p^{j-1}+\frac{\partial^2}{\partial t^2}\xi(t)\right]. \qquad (10)$$

На следующем шаге выполняем преобразования вида

$$\int\sum_{j=1}^{0,5n-3}j^2p^{j-1}dp=\sum_{j=1}^{0,5n-3}jp^j=p\frac{1}{(1-p)^2},\quad \frac{d}{dp}\left[p\frac{1}{(1-p)^2}\right]=\frac{1+p}{(1-p)^3}.$$

При этом из (10) следует

$$m'_{K2}(0)=\frac{4(1-p)^2}{(2-3p)^2}\left[\frac{1+p}{(1-p)^3}-\frac{p}{2}\frac{1+p}{(1-p)^3}+\frac{\partial^2}{\partial t^2}\xi(t)\right]=\left|\frac{4(1-p)^2}{(2-3p)^2}\frac{p}{2}\frac{1+p}{(1-p)^3}\right|\approx\frac{p}{2}.$$

Таким образом, с учетом классического соотношения дисперсия распределения вероятностей пропуска ошибки при наблюдении пар коррелированных векторов заданного вида определяется соотношением

$$D_K=\frac{p(1-p)}{2}=\frac{m^2-1}{2m^4}\approx\frac{1}{2m^2}.$$

***Следствие 1.*** Мода *Mo* и математическое ожидание $m'_K(0)$ распределения вероятностей наблюдения пар коррелированных векторов заданного вида равны между собой и не совпадают с медианой *Me* при $r>>4$.

Доказательство. Очевидно, что при $r>>1$ из формулы (8) следует факт близости математического ожидания к окрестности нуля: $m'_K(0)=$ $=p=1/m^2$. В [7, 8] показано, что $Mo=m_{k=0}(0)=0$ при $\mu=r$. Следовательно, $m'_K(0)=p$, $Mo=0$, $Me=n/4$, откуда получаем $m'_K(0)\approx Mo<Me$.

***Следствие 2.*** При $\mu=r$ среднеквадратическое отклонение от матожидания $m'_K(0)=p$ слева должно быть взято равным нулю, а справа — стандартному значению $\sqrt{D_K}$.

**Свойства оценок вероятности наблюдения пар коррелированных векторов.** Полученные соотношения для математического ожидания и дисперсии позволяют записать и доказать ряд свойств оценок вероятности наблюдения пар векторов.

**Свойство 1.** Оценка вероятности наблюдения пар коррелированных векторов значениями выборочной функции является состоятельной, так как $\lim\limits_{n\to\infty} P\,[|\hat{p}-p|<\varepsilon]=1$.

Д о к а з а т е л ь с т в о очевидно и вытекает из законов и равенства произведения вероятностей наблюдения двух векторов состояний:

$$p=1/m^2. \tag{11}$$

При этом в асимптотике число событий заданного вида будет равно $n/m^2$.

**Свойство 2.** Оценка вероятности наблюдения пар коррелированных векторов является смещенной, так как $M(k/n)=p/n$, где $M(k/n)$ — матожидание оценки $k/n$.

Д о к а з а т е л ь с т в о следует из формулы (8). Действительно, рассматривая частоту появления заданного события как случайную величину $K$, получаем

$$M\left(\frac{k}{n}\right)=\frac{1}{n}M(k)=\frac{1}{nm^2}. \tag{12}$$

Учитывая, что правая часть соотношения (12) — матожидание оценки вероятности — стремится к нулю, а вероятность представляет собой равенство (11), можно утверждать, что соответствующая оценка является смещенной. Свойство 2 доказано.

**Свойство 3.** Оценка вероятности пар коррелированных векторов значениями выборочных функций эффективна при $r>1$, $m\geq 4$.

Д о к а з а т е л ь с т в о. При составлении неравенства Рао—Крамера будем учитывать, что левая его часть в физических системах характеризует разброс параметра вокруг математического ожидания «тормозного» пути некоторой информационной системы. Следовательно, правая часть соотношения также должна характеризовать функцию торможения, т.е. знаменатель следует интерпретировать как «ускорение» рассматриваемого информационного объекта, что математически определяется второй производной соответствующей (логарифмической) функции. В такой интерпретации левая и правая части соотношения оказываются эквивалентны. Другие представления информации Фишера в данной задаче не приводят к физико-математической системности сравниваемых параметров и, следовательно, не являются достоверными. Принцип логарифмирования функции в знаменателе позволяет избавиться от постоянных величин, не зависящих от переменных, по которым берется искомая производная.

Итак, неравенство Рао—Крамера для рассматриваемой категории аргументов имеет вид

$$D_K\left(\frac{k}{n}\right) \geq -\frac{1}{M\left(\frac{\partial^2}{\partial p^2}\ln m_{k=\text{const}}(0)\right)}, \tag{13}$$

где при $n = \infty$

$$m_{k=\text{const}}(0) \approx m_K(0) = \sum_{g=2}^{n-1}\sum_{k=1}^{n-g}\sqrt{p}^{\,n-s_1-2s_2-2s_3} q_1^{s_2} q_2^{s_3} \frac{\left(\sum\limits_{j=1}^{0,5(n-2)}\sum\limits_{i=1}^{n-2j} k_{j,i} + k_{\frac{n}{2},0}\right)!}{\prod\limits_{i=1}^{0,5n-2} k_{1,i}! \prod\limits_{i=1}^{0,5n-4} k_{2,i}! \ldots \prod\limits_{i=1}^{1} k_{\frac{n-2}{4},i}!} \approx \frac{1}{2}p. \tag{14}$$

При этом сумма показателей степени у параметра $\sqrt{p}$ имеет вид

$$s_1 + 2s_2 + 2s_3 = g - \sum_{j=1}^{0,5n-1}(2j-1)\sum_{i=1}^{n-2j} k_{j,i} + \sum_{j=1}^{0,5n-2}(2k_{j,n-2j-2} + k_{j,n-2j-1}).$$

В общем случае многомерный вариант неравенства (13) может быть представлен соотношением

$$D_K(\hat{\theta}) \geq -\frac{1}{M\left(\sum\limits_{j=\eta,\omega,\ldots,\lambda}\frac{\partial^2}{\partial p_j^2}\ln F[z_\eta, z_\omega, \ldots, z_\lambda, p_\eta, p_\omega, \ldots, p_\lambda]\right)},$$

где $D_K(\hat{\theta})$ — дисперсия оценки; $F[z_\eta, z_\omega, \ldots, z_\lambda, p_\eta, p_\omega, \ldots, p_\lambda]$ — многомерная функция распределения вероятностей; $z_\eta, z_\omega, \ldots, z_\lambda$ — статистические объекты с вероятностями наблюдения $p_\eta, p_\omega, \ldots, p_\lambda$.

Определим математическое ожидание функции, стоящей в знаменателе формулы (13), с учетом (14):

$$M\left[\frac{\partial^2}{\partial p^2}\ln\frac{1}{2}p\right] = M\left(-\frac{1}{p^2}\right) = -\frac{1}{p^2}.$$

Подставляя данное соотношение в неравенство (13), находим $1/2p > p^2$, $1/2 > p$. Таким образом, свойство 3 доказано.

**Свойство 4.** Оценка вероятности наблюдения пар коррелированных векторов в истинно случайном сообщении обладает большей полнотой, чем оценка вероятности векторов состояний.

Д о к а з а т е л ь с т в о. Сравним соотношения для дисперсии соответствующих оценок, определив неравенство

$$\frac{1}{2n^2}\, p \neq \frac{p(z_\omega)\, q(z_\omega)}{n}, \tag{15}$$

где $p(z_\omega)=1/m$; $q(z_\omega)=1-1/m$. Подставляя в (15) вероятности, выраженные через число состояний $r$-разрядного вектора $m$, получаем

$$\frac{1}{2n^2m^2} < \frac{m-1}{nm^2}, \quad \frac{1}{2n} < m-1.$$

Свойство 4 доказано.

**Свойство 5** [9]. Оценка наблюдения пар векторов оптимальна в среднеквадратическом смысле, так как математические ожидания векторов имеют вид

$$M\,[z_\xi - \hat{\theta}\,(z_\lambda)]^2 = \inf_\theta M\,[z_\xi - p\,(z_\lambda)]^2\,, \tag{16}$$

где $\hat{\theta}\,(z_\lambda)$ — оценка параметра, $\hat{\theta}\,(z_\lambda) \to p\,(z_\lambda)$ при $n \to \infty$.

Д о к а з а т е л ь с т в о. Очевидно, что

$$M\,[z_\xi - p\,(z_\lambda)]^2 = M\,[z_\xi^2] - M\,[2z_\xi p\,(z_\lambda)] + M\,[p\,(z_\lambda)]^2 =$$

$$= \sum_\xi z_\xi^2 p\,(z_\xi) - 2p\,(z_\lambda) \sum_\xi z_\xi p\,(z_\xi) + p^2(z_\lambda)\,,$$

где $p\,(z_\lambda) = p\,(z_\xi) = 1/m$ [2]. Следовательно,

$$M\,[z_\xi - p\,(z_\lambda)]^2 \approx \frac{[1+p\,(z_\lambda)][1-3p^2(z_\lambda)]}{3p^2(z_\lambda)}. \tag{17}$$

Для одномерных оценок $\hat{\theta}(z_\lambda) \to p(z_\lambda)$, и следовательно, левая часть в равенстве (16) стремится к функции (17). Свойство 5 доказано.

**Свойство 6.** Достаточность статистики — это свойство оценки, суть которого заключается в том, что совокупность функций от результатов наблюдений событий содержит ту же статистическую информацию о неизвестных параметрах, что и сами результаты наблюдений. С этой точки зрения, рассматриваемые оценки (вероятности наблюдения пар коррелированных векторов) в частном случае являются достаточными.

Д о к а з а т е л ь с т в о. С учетом результатов, приведенных в работах [7, 10], сформируем функцию правдоподобия в следующем виде:

$$L(p, q_1, q_2, k) \approx m^{s_1+2s_2+2s_3-n} q_1^{s_2} q_2^{s_3}, \tag{18}$$

где $p, q_1, q_2$ — сложный параметр степенного ряда; $k$ — статистика или степень параметра. При этом

$$s_2 + s_3 = \left( k_{1,3} + \sum_{i=1,2,4}^{0,5(n-2)} k_{1,2i} \right) + k_{1,n-3} + \sum_{i=1}^{0,5(n-4)} k_{2,2i} + k_{2,n-5} + \ldots + \sum_{i=1}^{0,5(n-n+2)} k_{\frac{n-2}{2},2i} +$$

$$+ k_{\frac{n-2}{2},1} + (k_{1,3} + k_{1,4}) + \left[ \sum_{i=2}^{0,5(n-4)} i(k_{1,2i+1} + k_{1,2i+2}) \right] + k_{1,n-4} + \sum_{i=1}^{0,5(n-6)} i(k_{2,2i+1} + k_{2,2i+2}) +$$

$$+ k_{2,n-5} + \ldots + \sum_{i=1}^{0,5(n-n+2)} i \left( k_{\frac{n-4}{2},2i+1} + k_{\frac{n-4}{2},2i+2} \right) + k_{\frac{n-4}{2},2} = k_{1,3} + s_2' + k_{1,3} + s_3'.$$

Таким образом, один из вариантов факторизации равенства (18) может быть представлен соотношением

$$L(p, q_1, q_2, k_{1,3}) \approx p^{\frac{n}{2} - \frac{1}{2} s_1 - s_2 - s_3} q_1^{s_2} q_2^{s_3} = p^{\frac{n}{2} - \frac{1}{2} s_1 - (2k_{1,3} + s_2' + s_3')} q_1^{k_{1,3} + s_2'} q_2^{k_{1,3} + s_3'} =$$

$$= \left[ \frac{q_1 q_2}{p^2} \right]^{k_{1,3}} p^{\frac{1}{2}(n - s_1) - (s_2' + s_3')} q_1^{s_2'} q_2^{s_3'}.$$

Следовательно, $L(p, q_1, q_2, k_{1,3}) = T(p, q_1, q_2, k_{1,3}) L'(p, q_1, q_2)$, и оценка является достаточной относительно $k_{1,3}$. Аналогично можно доказать достаточность по другим переменным или их совокупностям. При невозможности факторизации $L(p, q_1, q_2)$ по выбранным параметрам оценка события или группы событий определяется как недостаточная.

## Выводы

1. Математическое ожидание плотности распределения вероятностей пропуска ошибки при наблюдении пар коррелированных векторов в случайном сообщении приблизительно равно нулю для $j = 1$ и практически не изменяется для $j = \text{var}$, так как усложнение эксперимента на единицу $(j+1)$ приводит к умножению соответствующей части производящей функции на вероятность $p = 1/m^2$, что при $r >> 1$, $m = 2^r$ весма незначительно влияет на параметр (8).

2. Математическое ожидание и мода распределения вероятностей пропуска ошибки для пар векторов в криптографическом канале ШПСС практически равны нулю. Слагаемые в функции $m_K(0)$ при возрастании номеров $j$ существенно уменьшаются относительно $j - 1$ отсчетов и непрерывно убывают [7]. Данный факт и определяет близость дисперсии к нулевому значению.

3. Оценки вероятности наблюдения пар коррелированных векторов обладают свойством состоятельности, однако смещены относительно теоретического параметра. Рассматриваемые выборочные функции являются эффективными и обладают большей полнотой по сравнению с оценками наблюдения векторов статических состояний. Оценки АКФ пар заданных векторов при $\tau = 1$ являются также оптимальными в среднеквадратическом смысле.

4. Рассмотренная функция правдоподобия и вариант ее факторизации позволяют сделать вывод о достаточности выбранной статистики и целесообразности ее применения в условиях наблюдения случайных сообщений ограниченной длины.

Mathematical expectation and dispersion function of probability distribution of the error were determined under observation of the preset pairs of vectors in the sequence of random events. The producing function served as a basis for calculations, it enables to present all the results of a certain class of combinatorial tasks in the form of a sum of $n-2$ polynomials. Point estimates of autocorrelation function are investigated such as the consistency, unbiasedness, efficiency and sufficiency of selected parameters.

1. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. — М. : Радио и связь, 1985. — 384 с.
2. *Кобяк И. П.* Сравнительная оценка достоверности методов сигнатурного анализа и счета состояний // Электрон. моделирование. — 1996. — **18**, № 3. — С. 58—62.
3. *Яблонский С. В.* Введение в дискретную математику. 2-е изд., перераб. и доп. — М. : Наука. Гл. ред. физ.-мат. лит. — 384 с.
4. *Weathers G. D., Graf E. R.* The Subsequence Weight Distributions of Summed Maximum Length Digital Sequences // IEEE Trans. on Commun. — 1974. — **com-22**, № 8. — P. 997—1004.
5. *Кобяк И. П.* Включение и исключение аргументов в автокорреляционной функции с по мощью набора (0,1)-коэффициентов // АВТ. — 2001. — № 3. — С. 64—74.
6. *Gold R.* Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions // IEEE Trans. on Information Theory. — 1968. — **IT-14.** — P. 154—156.
7. *Кобяк И. П.* Производящая функция для распределения статистик автокорреляционной функции // Электрон. моделирование. — 2010. — **32**, № 2. — С. 61—76.
8. *Кобяк И. П.* Теория внутрисхемного наблюдения СБИС с использованием автокорреляционных функций // АВТ. — 2009. — № 2. — С. 37—46.
9. *Ширяев А. Н.* Вероятность. — М. : Наука. Гл. ред. физ.-мат. лит., 1980. — 576 с.
10. *Ивченко Г. И., Медведев Ю. И.* Математическая статистика. — М. : Высш. шк., 1984. — 248 с.

Поступила 23.09.11

*КОБЯК Игорь Петрович, канд. техн. наук, доцент кафедры ЭВМ Белорусского государственного университета информатики и радиоэлектроники (БГУИР). В 1982 г. окончил Минский радиотехнический институт (ныне БГУИР). Область научных исследований — прикладная математика в вопросах синтеза и испытания цифровых систем.*