УДК 621.39:623.624+623.77

С.А. ИВАНЧЕНКО

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ШУМОВОЙ ПОМЕХИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Аннотация. Обоснована математическая модель шумовой помехи, учитывающая статистическую связь отсчетов считывания, для гарантированной защиты информации от утечки по техническим каналам. Модель вносит поправки в математическое ожидание и действующее среднеквадратическое отклонение, которые смещают среднюю точку помехи и определяют ее действующую мощность.

Ключевые слова: шум, шумовая помеха, математическая модель, гарантированная защита информации, утечка информации, технические каналы утечки.

ВВЕДЕНИЕ

Обеспечение информационной безопасности государства — одна из наиболее важных задач [1], которая относительно использования информационных и телекоммуникационных систем состоит в сбалансировании применяемых средств и методов защиты к действующим угрозам. В зависимости от используемых критериев безопасности и требуемой степени их обеспечения, особенностей объектов, которые образуют информационную среду, стоимости и важности обрабатываемой информации, а также постоянно усовершенствующихся и возрастающих возможностей нарушителя, решения этой задачи могут иметь различную научную направленность и сложность.

Задача защиты информации от утечки по техническим каналам в настоящее время решается путем выполнения определенных качественных требований и количественных норм. Для обеспечения гарантированной защиты с допустимыми рисками по защищенности [2], очевидно, что эти нормы должны быть математически доказаны и соответствующим образом обоснованы. Также очевидно, что это обоснование необходимо осуществлять относительно действующих условий, определяемых современным уровнем мирового развития науки и техники.

Утечка информации по техническим каналам происходит в результате побочных явлений, которые возникают во время работы технических средств обработки и передачи информации [3, 4] и распространяются в окружающей физической среде на большие расстояния.

Отметим, что процессы прохождения информации по каналу достаточно полно описаны в теориях информации, сигналов, потенциальной помехоустойчивости, а также статистической теории демодуляции сигналов и других теориях, образующих общую теорию связи [5]. Однако касательно каналов утечки не требуется обеспечения наилучшей передачи информации, как для каналов связи. В целях безопасности каналов утечки необходимо создать условия, при которых невозможно прохождение информации от источника к приемнику перехвата. Поэтому применение общей теории связи для решения задач по предотвращению утечки информации является недостаточным и требует пересмотра ее положений с уточнением и обновлением общепринятых допущений и ограничений.

Одним из вопросов безопасности этих каналов являются помехи [3, 4, 6], которые при расчете вероятности ошибки в канале рассматриваются как идеализированный белый шум — случайный, нормально распределенный эргодический процесс с равномерно распределенным спектром по всей полосе частот. При оце-

нивании защищенности используется свойство независимости временных отсчетов белых шумов, которое позволяет доказать связь этой вероятности ошибки с энергетическими условиями в канале [5].

Реальные шумовые помехи и естественного, и искусственного происхождения не являются белыми шумами, их распределения вероятностей могут иметь недопустимые отклонения от нормального закона, а отсчеты — различную статистическую зависимость. Если помехи, которые не соответствуют по распределению, можно отклонить, то статистическая зависимость отсчетов в них имеется практически всегда и даже появляется в белом шуме при ограничении его спектра. Пренебрежение последним, очевидно, может увеличить возможности злоумышленника, не позволит обеспечить требуемую вероятность ошибки в канале утечки, а значит, гарантировать защищенность в целом.

Отметим, что согласно нормативной базе по технической защите информации рекомендуется использовать энтропийный коэффициент маскирующего качества шума [7–9]. Однако последний имеет ряд недостатков, ограничивающих его возможности, а именно:

— он является показателем качества работы средств генерации шума, а не эффективности маскировки шумом, поскольку не учитывает возможной фильтрации при перехвате;

— энтропия, определяющая коэффициент качества, находится с использованием гистограммы по закону распределения мгновенных значений исследуемого процесса без учета их статистической зависимости, которая дает возможность прогнозировать поведение случайного процесса, образующего шумовую помеху, и может повлиять на снижение ее маскировочной эффективности;

— его использование не беспечивает гарантированно доказанную защищенность, т.е. не факт, что составляющая помехи с мощностью, поправленной этим коэффициентом, будет действовать как нормально распределенная помеха.

Таким образом, существует необходимость обоснования математической модели шумовой помехи, которая бы достаточно полно описывала реальные шумы, максимально учитывала их статистические дефекты и была удобной для расчета вероятности ошибки и других показателей защищенности.

ОПИСАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ШУМОВОЙ ПОМЕХИ

Пусть в канале утечки имеет место стационарная нормально распределенная шумовая помеха, которая на приеме воспринимается в виде временных отсчетов (мгновенных значений) через некоторый интервал τ (рис. 1). Отметим, что этот способ приема обусловлен применением современных устройств, которые в настоящее время широко используются и позволяют не только измерять указанные отсчеты с получением их численных значений, но и обрабатывать эти значения с применением различных вычислительных алгоритмов и эффективных технологий [6, 10–13].

Если в каждом отсчете t_i, $i = 1, 2, 3, \ldots$, наблюдаемый процесс непрерывный и имеет нормальное распределение с нулевым средним значением, то его можно описать как случайный многомерный вектор с плотностью распределения вероятностей по k отсчетам [14]

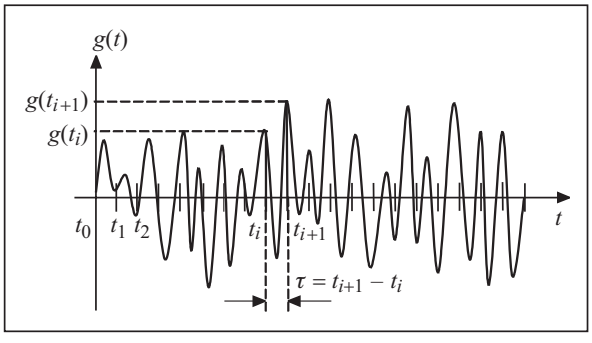

Рис. 1. Временно́е представление шумовой помехи $g(t)$

$$\omega(n_1, n_2, n_3, \ldots, n_k) = \frac{1}{\sigma^k (2\pi)^{k/2} |\, \mathbf{r}^k \,|^{1/2}} \exp\left[-\frac{1}{2\sigma^2 |\, \mathbf{r}^k \,|} \sum_{q,l=1}^{k} A_{ql}^k n_q n_l \right], \quad (1)$$

где n_i, $n_i = g(t_i)$, $i = 1, \ldots, k$ (k должно быть достаточно велико); r_{ql} — коэффициент корреляции величин n_q и n_l:

$$r_{ql} = \frac{1}{\sigma^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} n_q n_l \omega(n_q, n_l)\, dn_q\, dn_l;$$

$|\, \mathbf{r}^k \,|$ — определитель матрицы вида

$$\mathbf{r}^k = \begin{bmatrix} r_{11} & r_{12} & r_{13} & \cdots & r_{1l-1} & r_{1l} & \cdots & r_{1k} \\ r_{21} & r_{22} & r_{23} & \cdots & r_{2l-1} & r_{2l} & \cdots & r_{2k} \\ r_{31} & r_{32} & r_{33} & \cdots & r_{3l-1} & r_{3l} & \cdots & r_{3k} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ r_{q-11} & r_{q-12} & r_{q-13} & \cdots & r_{q-1l-1} & r_{q-1l} & \cdots & r_{q-1k} \\ r_{q1} & r_{q2} & r_{q3} & \cdots & r_{ql-1} & r_{ql} & \cdots & r_{qk} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ r_{k1} & r_{k2} & r_{k3} & \cdots & r_{kl-1} & r_{kl} & \cdots & r_{kk} \end{bmatrix}; \quad (2)$$

A_{ql}^k — алгебраическое дополнение элемента r_{ql} матрицы $\mathbf{r}^k$.

Однако расчет вероятности ошибки в канале с оптимальным приемником предполагает статистическую независимость отсчетов шумовой помехи [5, 6], которая позволяет представить многомерную плотность вероятностей в виде произведения одномерных

$$\omega(n_1, n_2, n_3, \ldots, n_k) = \omega(n_1)\omega(n_2)\omega(n_3) \times \ldots \times \omega(n_i) \times \ldots \times \omega(n_k), \quad (3)$$

где

$$\omega(n_i) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{1}{2} \frac{n_i^2}{\sigma^2} \right].$$

Очевидно, что условие (3) выполнимо для соотношения (1), которое описывает общий случай, если матрица (2) будет единичной. Однако, как показывает практический опыт [15], для реальных процессов матрица (2) не может быть единичной, коэффициенты корреляции для $q \neq l$ отличны от нуля и в зависимости от интервала считывания τ имеют приблизительную характеристику, как изображено на рис. 2.

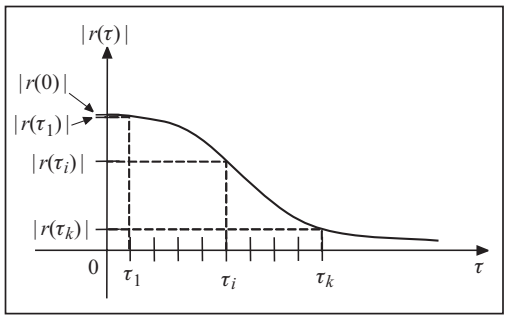

Рис. 2. Типичная характеристика зависимости коэффициента корреляции от интервала считывания для реальных шумовых процессов

Если рассматриваемый процесс эргодический, а такое предположение для реальных шумов допустимо, то элементы матрицы (2) можно заменить экспериментально полученными значениями коэффициентов корреляции (см. рис. 2) и учесть их при расчете показателей защищенности

$$r(\tau) = \frac{1}{P_{\text{п}}} \frac{1}{T} \int_0^T g(t) g(t-\tau) d\tau,$$

где $P_{\text{п}}$ — мощность исследуемого процесса ($P_{\text{п}} = \sigma^2$), T — временной интервал процесса, который должен быть достаточно велик. Полученная матрица коэффициентов корреляции позволит более точно рассчитать вероятность ошибки в канале утечки и обеспечить более достоверную защищенность информации.

Пусть формулой (1) задана многомерная плотность распределения вероятностей. Тогда ее можно записать как произведение условных плотностей

$$\omega(n_1, n_2, n_3, \ldots, n_k) = \omega(n_1)\omega(n_2 / n_1)\omega(n_3 / n_1, n_2) \times \ldots$$
$$\ldots \times \omega(n_k / n_1, n_2, \ldots, n_{k-2}, n_{k-1}). \qquad (4)$$

Каждый i-й элемент в соотношении (4), $i = 1, 2, 3, \ldots, k$, можно выразить как

$$\omega(n_i / n_1, n_2, n_3, \ldots, n_{i-1}) = \omega(n_i / N^{i-1}) = \frac{\omega(n_1, n_2, n_3, \ldots, n_i)}{\omega(n_1, n_2, n_3, \ldots, n_{i-1})} =$$
$$= \frac{1}{\sqrt{2\pi\sigma^2 \dfrac{|\mathbf{r}^i|}{|\mathbf{r}^{i-1}|}}} \exp\left[\frac{1}{2\sigma^2}\left(\frac{1}{|\mathbf{r}^{i-1}|}\sum_{q,l=1}^{i-1} A_{ql}^{i-1} n_q n_l - \frac{1}{|\mathbf{r}^i|}\sum_{q,l=1}^{i} A_{ql}^{i} n_q n_l\right)\right], \qquad (5)$$

где $N^i = (n_1, n_2, n_3, \ldots, n_i)$.

Сравнивая условную плотность (5) с безусловной, можно вычислить действующие параметры, определяющие вероятность ошибки в канале. В работе [5] этими параметрами являются математическое ожидание и дисперсия. Здесь также отмечается, что на уменьшение вероятности ошибки в канале, в результате чего ухудшается защищенность информации от утечки, влияют возрастание смещения среднего значения шумового процесса и снижение его среднеквадратического отклонения. При этом эквивалентом плотности распределения вероятностей этих процессов с указанными статистическими дефектами есть плотность вида

$$\omega(n) = \frac{1}{\sqrt{2\pi\sigma'^2}} \exp\left[-\frac{1}{2}\frac{(n \pm \bar{n}'_{\max})^2}{\sigma'^2_{\min}}\right], \qquad (6)$$

где $\bar{n}'_{\max}$ — максимум смещения среднего значения процесса, возникающего вследствие статистических связей отсчетов; $\sigma'_{\min}$ — действующий минимум среднеквадратического отклонения с учетом статистических связей отсчетов шумового процесса.

Найдем эти параметры с необходимыми поправками.

Определение максимума смещения $\bar{n}'_{\max}$, появившегося в результате его предыстории. Для этого воспользуемся нахождением его регрессии. Для i-го отсчета функция регрессии имеет вид

$$\bar{n}_{i(n_i / N^{i-1})} = \mathrm{M}[n_i / N^{i-1}] = \int_{-\infty}^{\infty} n_i \omega(n_i / N^{i-1})\, dn_i.$$

Несложно убедиться, что если отсчеты независимы, то

$$\mathrm{M}[n_i / N^{i-1}] = \int_{-\infty}^{\infty} n_i \omega(n_i / N^{i-1})\, dn_i = \int_{-\infty}^{\infty} n_i \omega(n_i) dn_i = \mathrm{M}[n_i] = 0,$$

в противном случае

$$\mathrm{M}[n_i / N^{i-1}] \neq 0.$$

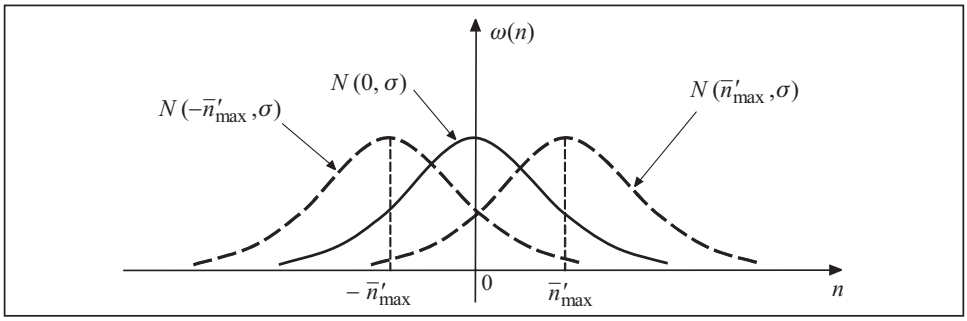

Рис. 3. Плотность нормального распределения вероятностей шумового процесса с поправкой на максимум смещения его среднего значения

Указанное математическое ожидание является смещением средней точки шумового процесса от нуля, которое снижает его маскирующие свойства и может использоваться злоумышленником для обработки этого процесса в целях их минимизации. При этом максимум смещения определяется как максимум модуля регрессии

$$\overline{n}_{\max} = \max_{i,\, N^{i-1}} |\, \overline{n}_{i(n_i/N^{i-1})}|\,.$$

Геометрическая интерпретация плотности нормального распределения вероятностей шумового процесса (6) с поправкой на максимум смещения представлена на рис. 3.

Для аддитивного канала учет такого смещения можно выполнить путем поправки передаваемого сигнала $c(t)$ в динамическом диапазоне. При этом его учетную амплитуду необходимо увеличить на величину $\overline{n}'_{\max}$:

$$|\, c_{\text{рез}}(t)\,| = \max |\, c(t) \pm \overline{n}'_{\max}\,|\,. \tag{7}$$

Эта поправка обеспечит наихудший случай относительно защиты информации от утечки — максимально возможное отношение сигнал/помеха в точке возможного ее перехвата.

При этом защищенность исправленного сигнала (7) можно обеспечить за счет увеличения мощности маскирующей помехи.

Расчет среднеквадратического отклонения $\sigma'_{\min}$ с поправкой на статистические связи отсчетов шумового процесса. Для этого проанализируем аргумент экспоненты в соотношении (5) для возрастающих значений i.

Для $i=1$ предыстории не существует, поэтому плотность распределения одномерная

$$\omega_{i=1}(n') = \omega(n_1) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{n_1^2}{2\sigma^2}\right].$$

Минимум среднеквадратического отклонения совпадает со среднеквадратическим отклонением, определяющим мощность шумовой помехи $\sigma'_{\min\, i=1} = \sigma$.

Для $i=2$ предыстория состоит из одного отсчета, плотность распределения двухмерная, матрица коэффициентов корреляции имеет вид

$$\mathbf{r}^2 = \begin{bmatrix} 1 & r_1 \\ r_1 & 1 \end{bmatrix},$$

а условная плотность

$$\omega(n_2 / n_1) = \frac{1}{\sqrt{2\pi\,(\sigma\sqrt{1-r_1^2}\,)^2}} \exp\left[\frac{(n_2 - r_1 n_1)^2}{2\,(\sigma\sqrt{1-r_1^2}\,)^2}\right]. \tag{8}$$

Из (8) следует, что $\sigma'_{\min\, i=2} = \sigma\sqrt{1-r_1^2} < \sigma'_{\min\, i=1}$.

Для $i=3$ предыстория состоит из двух отсчетов, плотность распределения трехмерная

$$\omega(n_1,n_2,n_3) = \frac{1}{\sqrt{(2\pi\sigma^2)^3}\sqrt{|\mathbf{r}^3|}} \exp\left[\frac{1}{2\sigma^2}(n_1,n_2,n_3)\times(\mathbf{r}^3)^{-1}\times(n_1,n_2,n_3)^{\mathrm{T}}\right], \quad (9)$$

где $\mathbf{r}^3$ — матрица коэффициентов корреляции, которая соответствует матрице (2) для $k=3$:

$$\mathbf{r}^3 = \begin{bmatrix} 1 & r_1 & r_2 \\ r_1 & 1 & r_1 \\ r_2 & r_1 & 1 \end{bmatrix}. \quad (10)$$

Определитель матрицы (10) имеет вид

$$|\mathbf{r}^3| = \begin{vmatrix} 1 & r_1 & r_2 \\ r_1 & 1 & r_1 \\ r_2 & r_1 & 1 \end{vmatrix} = 1+2r_1^2r_2-2r_1^2-r_2^2 = 1-2r_1^2(1-r_2)-r_2^2,$$

ее обратная матрица

$$(\mathbf{r}^3)^{-1} = \frac{\begin{pmatrix} \begin{vmatrix} 1 & r_1 \\ r_1 & 1 \end{vmatrix} & -\begin{vmatrix} r_1 & r_1 \\ r_2 & 1 \end{vmatrix} & \begin{vmatrix} r_1 & 1 \\ r_2 & r_1 \end{vmatrix} \\ -\begin{vmatrix} r_1 & r_2 \\ r_1 & 1 \end{vmatrix} & \begin{vmatrix} 1 & r_2 \\ r_2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & r_1 \\ r_2 & r_1 \end{vmatrix} \\ \begin{vmatrix} r_1 & r_2 \\ 1 & r_1 \end{vmatrix} & -\begin{vmatrix} 1 & r_2 \\ r_1 & r_1 \end{vmatrix} & \begin{vmatrix} 1 & r_1 \\ r_1 & 1 \end{vmatrix} \end{pmatrix}}{\begin{vmatrix} 1 & r_1 & r_2 \\ r_1 & 1 & r_1 \\ r_2 & r_1 & 1 \end{vmatrix}} = \frac{\begin{pmatrix} 1-r_1^2 & r_1r_2-r_1 & r_1^2-r_2 \\ r_1r_2-r_1 & 1-r_2^2 & r_1r_2-r_1 \\ r_1^2-r_2 & r_1r_2-r_1 & 1-r_1^2 \end{pmatrix}}{1-2r_1^2(1-r_2)-r_2^2} =$$

$$= \begin{pmatrix} \frac{1-r_1^2}{1-2r_1^2(1-r_2)-r_2^2} & \frac{r_1r_2-r_1}{1-2r_1^2(1-r_2)-r_2^2} & \frac{r_1^2-r_2}{1-2r_1^2(1-r_2)-r_2^2} \\ \frac{r_1r_2-r_1}{1-2r_1^2(1-r_2)-r_2^2} & \frac{1-r_2^2}{1-2r_1^2(1-r_2)-r_2^2} & \frac{r_1r_2-r_1}{1-2r_1^2(1-r_2)-r_2^2} \\ \frac{r_1^2-r_2}{1-2r_1^2(1-r_2)-r_2^2} & \frac{r_1r_2-r_1}{1-2r_1^2(1-r_2)-r_2^2} & \frac{1-r_1^2}{1-2r_1^2(1-r_2)-r_2^2} \end{pmatrix}.$$

После вычисления произведения матриц в соотношении (9)

$$(n_1,n_2,n_3)\times(\mathbf{r}^3)^{-1}\times(n_1,n_2,n_3)^{\mathrm{T}} =$$

$$= \frac{(n_1,n_2,n_3)\times\begin{pmatrix} 1-r_1^2 & r_1r_2-r_1 & r_1^2-r_2 \\ r_1r_2-r_1 & 1-r_2^2 & r_1r_2-r_1 \\ r_1^2-r_2 & r_1r_2-r_1 & 1-r_1^2 \end{pmatrix}\times(n_1,n_2,n_3)^{\mathrm{T}}}{1-2r_1^2(1-r_2)-r_2^2} =$$

$$= \frac{(1-r_1^2)n_1^2 + (1-r_2^2)n_2^2 + (1-r_1^2)n_3^2 - 2(r_1 - r_1 r_2)n_1 n_2 - 2(r_2 - r_1^2)n_1 n_3 - 2(r_1 - r_1 r_2)n_2 n_3}{1 - 2r_1^2(1-r_2) - r_2^2},$$

получим окончательный вид плотности распределения вероятностей

$$\omega(n_1, n_2, n_3) = \frac{1}{\sqrt{(2\pi\sigma^2)^3}\sqrt{1-2r_1^2(1-r_2)-r_2^2}} \times$$

$$\times \exp\left[\frac{(1-r_1^2)n_1^2 + (1-r_2^2)n_2^2 + (1-r_1^2)n_3^2 - 2(r_1 - r_1 r_2)n_1 n_2 - 2(r_2 - r_1^2)n_1 n_3 - 2(r_1 - r_1 r_2)n_2 n_3}{2\sigma^2(1-2r_1^2(1-r_2)-r_2^2)}\right].$$

Следовательно, условная плотность примет вид

$$\omega(n_3 / n_1, n_2) = \frac{1}{\sqrt{2\pi\left(\sigma\dfrac{\sqrt{1-2r_1^2(1-r_2)-r_2^2}}{\sqrt{1-r_1^2}}\right)^2}} \times$$

$$\times \exp\left(\frac{n_3^2 - 2\dfrac{r_1(n_2 - r_1 n_1) + r_2(n_1 - r_1 n_2)}{1-r_1^2}n_3 - \left(\dfrac{r_2 n_2 - r_1 n_1}{\sqrt{1-r_1^2}}\right)^2}{2\left(\sigma\dfrac{\sqrt{1-2r_1^2(1-r_2)-r_2^2}}{\sqrt{1-r_1^2}}\right)^2}\right).$$

Несложно убедиться, что при $r_3 < r_2 < r_1 < 1$ (см. рис. 2)

$$\sigma'_{\min\, i=3} = \sigma\frac{\sqrt{1-2r_1^2(1-r_2)-r_2^2}}{\sqrt{1-r_1^2}} < \sigma'_{\min\, i=2} < \sigma'_{\min\, i=1}.$$

Для произвольного i $(i = k)$ предыстория состоит из $k-1$ отсчетов, плотность распределения определяется соотношением (1), матрица коэффициентов корреляции (2) принимает вид

$$\mathbf{r}^k = \begin{bmatrix} 1 & r_1 & r_2 & \dots & r_{k-2} & r_{k-1} \\ r_1 & 1 & r_1 & r_2 & \dots & r_{k-2} \\ r_2 & r_1 & 1 & r_1 & \dots & \dots \\ \dots & r_2 & r_1 & 1 & \dots & r_2 \\ r_{k-2} & \dots & \dots & \dots & \dots & r_1 \\ r_{k-1} & r_{k-2} & \dots & r_2 & r_1 & 1 \end{bmatrix}. \qquad (11)$$

Условную плотность (5) можно записать так:

$$\omega(n_k / N^{k-1}) = \frac{1}{\sigma(2\pi)^{1/2}\dfrac{|\mathbf{r}^k|^{1/2}}{|\mathbf{r}^{k-1}|^{1/2}}}\exp\left[-\frac{A_{kk}^k n_k^2 + \sum\limits_{q,l=1}^{k-1} G_{ql} n_q n_l}{2\sigma^2|\mathbf{r}^k|}\right], \qquad (12)$$

где A_{kk}^k — алгебраическое дополнение матрицы (11) элемента пересечения k-го столбца и k-й строки, G_{ql} — коэффициенты произведений $n_q n_l$.

Поскольку $A_{kk}^{k} = |\,\mathbf{r}^{k-1}|$, как минор элемента r_{kk}, соотношение (12) примет вид

$$\omega(n_k / n_1, n_2, n_3, \ldots, n_{k-1}) = \frac{1}{(2\pi)^{1/2}\sigma\dfrac{|\,\mathbf{r}^{k}|^{1/2}}{|\,\mathbf{r}^{k-1}|^{1/2}}}\exp\left[-\frac{n_k^2 + \sum\limits_{q,l=1}^{k-1}\dfrac{G_{ql}}{|\,\mathbf{r}^{k-1}\,|}n_q n_l}{2\sigma^2\dfrac{|\,\mathbf{r}^{k}|}{|\,\mathbf{r}^{k-1}|}}\right] =$$

$$= \frac{1}{(2\pi)^{1/2}\left(\sigma\dfrac{|\,\mathbf{r}^{k}|^{1/2}}{|\,\mathbf{r}^{k-1}|^{1/2}}\right)}\exp\left[-\frac{n_k^2 + \sum\limits_{q,l=1}^{k-1}G'_{ql}n_q n_l}{2\left(\sigma\dfrac{|\,\mathbf{r}^{k}|^{1/2}}{|\,\mathbf{r}^{k-1}|^{1/2}}\right)^2}\right]. \qquad (13)$$

Из (13) следует, что действующее среднеквадратическое отклонение k-го отсчета с учетом его предыстории равно:

$$\sigma'_{\min\, i=k} = \sigma\frac{|\,\mathbf{r}^{k}\,|^{1/2}}{|\,\mathbf{r}^{k-1}\,|^{1/2}},$$

а обобщенное действующее среднеквадратическое отклонение можно определить как

$$\sigma'_{\min} = \min_{i=1,2,3,\ldots}\sigma'_{\min\, i} = \sigma\sqrt{\min_{i=1,2,3,\ldots}\frac{|\,\mathbf{r}^{i}\,|}{|\,\mathbf{r}^{i-1}\,|}}. \qquad (14)$$

Нахождение в соотношении (14) минимума отношения определителей является отдельной задачей, которая может иметь и математическое, и экспериментальное решения путем индивидуальных расчетов для различных источников. При этом очевидно, что при возрастании учитываемой предыстории нахождение этого минимума может оказаться достаточно сложным процессом. Также очевидно, что при $\tau \to 0$ (см. рис. 2), большом k и незначительном отличии соседних элементов ($r_i \approx r_{i+1}$) матрицы (11) определители $|\,\mathbf{r}^{k}\,| \approx |\,\mathbf{r}^{k-1}|$. А это означает, что действующее среднеквадратическое отклонение любой шумовой помехи, а для эргодических процессов равно и их действующая мощность будут стремиться к нулю.

ЗАКЛЮЧЕНИЕ

Таким образом, обоснована математическая модель маскирующей шумовой помехи для защиты информации от утечки по техническим каналам. В отличие от ранее известных она учитывает статистические связи между временными отсчетами (мгновенными значениями) описываемого процесса, которые возникают вследствие недостатков, имеющихся в источниках, и влияют на его маскирующие свойства. Модель вносит поправки в математическое ожидание и среднеквадратическое отклонение нормально распределеной помехи, которые для достоверного расчета требуемой вероятности ошибки в канале утечки информации можно компенсировать завышением амплитуды вытекаемого сигнала и занижением мощности помехи на обоснованные в модели величины.

СПИСОК ЛИТЕРАТУРЫ

1. «Про інфомацію»: Закон України від 02.10.1992. № 2657-XII (поточна редація від 25.06.2016). URL: http://www.zakon.rada.gov.ua/go/1657-12.
2. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].

3. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита информации от утечки по техническим каналам. Москва: Горячая линия – Телеком, 2005. 416 с.
4. Kuhn G. Compromising emanations: eavesdropping risks of computer displays. Technical Report. N 577. December 2003. University of Cambridge. URL: http://www.cl.cam.ac. uk/ techreports.
5. Бураченко Д.Л., Заварин Г.Д., Клюев Н.И. и др. Общая теория связи. Под ред. Л.М. Финка. Ленинград: ВАС, 1970. 412 с.
6. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Т. 1. Несанкционированное получение информации. Киев: Арий, 2008. 464 с.
7. Гаврилов И.В. Методика оценивания качества маскирующего шума. *Труды СПИИРАН*. 2015. Вып. 43. С. 179–190. URL: roceedings.spiiras.nw.ru/ojs/index.
8. Способ оценки качества маскирующего акустического (виброакустического) шума: пат. РФ № 2350023. Тупота В.И., Бортников А.Н., Бурмин В.А., Герасименко В.Г., Самсонов А.А., Железняк В.К., Петигин А.Ф. Опубл. в БИ 20.03.2009 г. URL: http://www.findpatent.ru/patent/235/2350023.
9. Пашук М.Ф., Панычев С.Н., Суровцев С.В. Универсальный показатель для оценки эффективности маскирующих и имитационных радиопомех. URL: www.ntc-reb.ru/article13.html.
10. Раушер К., Йанссен Ф., Минихолд Р. Основы спектрального анализа. Пер. с анл. под ред. Ю.А. Гребенко. Москва: Наука, 2005. 223 с.
11. Antennas HF-VHF/UHF-SHF: Catalog. München: Rohde & Schwarz, 2007. 180 p.
12. Olbrich M., Mittenzwei V., Siebertz O., Schmülling F., Schieder R. A 3 GHz instantaneous bandwidth acousto-optical spectrometer with 1 MHz resolution. 18th International Symposium on Space Terahertz Technology (March 21–23, 2007). California Institute of Technology, Pasadena, California, USA. P. 231–235.
13. Rauscher C., Janssen V., Minihold R. Fundamentals of spectrum analysis. München: Rohde & Schwarz, 2002. 215 p.
14. Ивановский Р.И. Теория вероятностей и математическая статистика. С.-Петербург: БХВ-Петербург, 2008. 528 с.
15. Баскаков С.И. Радиотехнические цепи и сигналы. Москва: Высш. шк., 1988. 448 с.

Надійшла до редакції 13.01.2016

С.О. Іванченко

МАТЕМАТИЧНА МОДЕЛЬ ШУМОВОЇ ЗАВАДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Анотація. Обґрунтовано математичну модель шумової завади, яка враховує статистичний зв'язок відліків зчитування, для гарантованого захисту інформації від витоку технічними каналами. Модель вносить поправки в математичне сподівання та дійове середньоквадратичне відхилення, які зміщують середню точку завади і визначають дійову потужність.

Ключові слова: шум, шумова завада, математична модель, гарантований захист інформації, витік інформації, технічні канали витоку.

S.A. Ivanchenko

MATHEMATICAL MODEL OF NOISE INTERFERENCE FOR INFORMATION PROTECTION AGAINST LEAKAGE BY TECHNICAL CHANNELS

Abstract. The author substantiates the mathematical model of noise interference that takes into account statistical relation of readout samples for secure information protection against leakage by technical channels. The model amends the mathematical expectation and root-mean-square deviation, which shifts the midpoint of noise interference and determoines its effective capacity.

Keywords: noise, noise interference, mathematical model, secure information protection, information leakage, technical channels of leakage.

Иванченко Сергей Александрович,
доктор техн. наук, доцент, профессор специальной кафедры № 1 Института специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: soivanch@ukr.net.