А. В. Балакин, **А. Ю. Гуфан** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Метод маскировки выходной последовательности марковского процесса.**

Пусть в целях безопасной передачи по открытому каналу связи требуется закодировать выходную последовательность марковского процесса (МП) таким образом, чтобы статистические характеристики получившейся последовательности были близки к характеристикам выходной последовательности другого заранее заданного МП. Пусть $H(A,P)$ — кодирующая таблица кода Хаффмана (КХ) для алфавита $A=[a_1,a_2,\ldots,a_n]$ с частотами $P=[p_1,p_2,\ldots,p_n]$; $H(A,P)=[h_1,h_2,\ldots,h_n]$, h_i — последовательность бит, кодирующая символ a_i; $G(A,P)$ — декодирующая таблица. Пусть есть два МП: M_1 и M_2 с состояниями $[B_i^1]_{i=0}^q$ и $[B_i^2]_{i=0}^r$ и матрицами вероятностей переходов $[P_{i,j}^1]_{i,j=0}^q$ и $[P_{i,j}^2]_{i,j=0}^r$; переход в состояние с индексом 0 невозможен. Имеется последовательность, сгенерированная M_1 (состоянию B_i^1 соответствует символ b_i^1), и требуется представить ее в виде последовательности X так, чтобы X была статистически похожа на результат работы M_2.

1. Сформируем последовательность Y. Каждой паре соседних символов $[b_i^1,b_j^1]$ из X поставим в соответствие $c_j^{1,i}$ в Y, а первому символу — символ $c_j^{1,0}$.

2. Каждый символ $c_j^{1,i}$ из Y представим в виде последовательности $g_j^{1,i}$ бит, равной элементу h_i из таблицы $H([c_j^{1,i}]_{j=1}^q,[P_j^{1,i}]_{j=1}^q)$. Получим последовательность Z бит.

3. Построим строку W из символов $[c_j^{2,i}]_{j=1}^r$. Будем считывать биты из Z до тех пор, пока прочитанного фрагмента не хватит, чтобы декодировать его при помощи $G([c_j^{2,i}]_{j=1}^r,[P_j^{2,i}]_{j=1}^r)$. Полученный символ $c_s^{2,1}$ запишем в W. Продолжим чтение из Z до тех пор, пока прочитанного не хватит для декодирования его при помощи $G([c_j^{2,s}]_{j=1}^r,[P_j^{2,s}]_{j=1}^r)$. Полученный символ запишем в W, и т. д. Если фрагмента Z, оставшегося после последнего успешного декодирования, не хватит для формирования последнего символа, дополним его любым заранее оговоренным образом.

4. Сформируем последовательность T символов по W методом, обратным использованному в п. 1.

Декодирование T возможно при помощи обратных действий. При кодировании и декодировании нескольких последних символов, возможно, возникнет необходимость дополнить текст некоторым заранее оговоренным способом. При декодировании последовательности T, соответственно, может обнаружиться фрагмент T, не кодирующий никакую полезную информацию. Эта проблема может быть легко разрешена использованием специального символа окончания сообщения.

Статистические характеристики последовательности T будут указывать на ее происхождение из источника, адекватно моделируемого марковским процессом M_2.

Вышеописанный алгоритм представляет собой общую методику маскировки передачи произвольного сообщения по любому открытому каналу под работу на этом канале любого заранее заданного и достаточно продолжительного процесса, адекватно с точки зрения контролирующего субъекта описываемого в терминах марковских процессов.