ТЕХНОЛОГИЯ ПРИМЕНЕНИЯ АДАПТИВНОГО ВИРТУАЛЬНОГО КОДИРОВАНИЯ В ЗАДАЧАХ ЗАЩИТЫ ДИСКРЕТНОЙ ИНФОРМАЦИИ

Котенко В.В., Евсеев А.С., Дергачев В.С.

Южный федеральный университет

Ростов-на-Дону, Россия

Технология адаптивного виртуального кодирования состоит в формировании виртуальных кодовых последовательностей обеспечивающих выполнение условий:

$$I\left[X^*;Y^*\right]=H\left[X^*\right], \quad (1)$$

$$I\left[X^*;Y^*\right]=I\left[X;Y\right]+\Psi\left[I;I^*\right], \quad (2)$$

где X и X^* - ансамбли исходных и виртуальных сообщений, соответственно; Y и Y^* - ансамбли исходных и виртуальных кодовых комбинаций, соответственно; $\Psi\left[I;I^*\right]$ - оператор виртуализации.

Выражение 1-2 определяет общую модель адаптивного виртуального кодирования. Ее преобразование позволяет получить рекуррентный алгоритм вида:

$$y_i^*=\Phi_k\left\{x_i\right\}+\left[\Phi_k^{-1}\left\{y_{i-n}^*\right\}-\left(x_{i-m}-\left(\Phi_k^{-1}\left\{y_{i-k}\right\}-x_{i-l}\right)\right)\right], \quad (3)$$

где $\Phi_k\left\{!\right\}$ и $\Phi_k^{-1}\left\{!\right\}$ - процедуры кодирования и декодирования.

Программная реализация алгоритма 3 применительно к заданному множеству циклических кодов позволила создать программно-аппаратный комплекс адаптивного виртуального кодирования.

Проведенные исследования показали, что, обеспечивая повышение помехоустойчивости данный комплекс одновременно осуществляет защиту информации от несанкционированного доступа. Для оценки степени данной защиты была исследована степень вносимых искажений в результате виртуализации. Для этого исследовалась вероятность необнаружения ошибки $P_Д$ декодером, реализующим процедуру $\Phi_k^{-1}\left\{y_i\right\}$ в случае поступления на его вход виртуальных кодовых комбинаций y_i^*.

Анализ приведенных зависимостей показывает, что виртуальное адаптивное кодирование практически полностью искажает исходную кодовую комбинацию, что можно трактовать как защиту от несанкционированного доступа. Т.е. защиту от пользователя, которому не известны установленные значения задержек и циклического сдвига. С этих позиций адаптивное виртуальное кодирование можно рассматривать как шифрование с некоторым виртуальным ключом, где значения задержек и циклического сдвига выступают в роли исходных ключевых данных.

СПИСОК ЛИТЕРАТУРЫ:

1. Галлагер Р. Теория информации и надёжная связь. М.: Советское радио, 1974. 720с.