ТЕХНОЛОГИЯ ВИРТУАЛЬНОГО АМПЛИТУДНОГО СКРЕМБЛИРОВАНИЯ

Котенко В.В., Румянцев К.Е., Евсеев А.С.

Южный федеральный университет

Ростов-на-Дону, Россия

Статистическая зависимость между ансамблями сообщений и криптограммы является основной технической проблемой защиты речевых сообщений. Наиболее заметно эта проблема проявляется при практической реализации способов амплитудного скремблирования, когда криптограммы ансамбля E формируются путем изменения выборок ансамбля сообщений U по закону, заданному отсчетами ансамбля K источника ключа. Одним из подходов, позволяющих решить данную проблему, является подход, основанный на виртуализации информационных потоков. В данном случае алгоритм формирования криптограммы определяется выражением

$$I\left[U^*;E^*\right]=I\left[U;E\right]+\Psi\left[I;I^*\right], \quad (1)$$

$$\Psi\left[I;I^*\right]=H\left[K^*/U^*E^*\right]-H\left[K^*/U^*\right]-H\left[U\right]+H\left[U/E\right], \quad (2)$$

где U^*, E^* и K^* виртуальные ансамбли сообщений, криптограмм и ключей соответственно.

Программная реализация алгоритма (1), (2) позволила разработать программный комплекс виртуального амплитудного скремблирования. Особенностью разработанного комплекса является обеспечение доказанного в [1] условия теоретической недешифруемости при статистической зависимости сообщений и криптограмм, состоящего во введении в ансамбль ключей неопределенности, равной среднему количеству информации о сообщениях в криптограммах.

Экспериментальные исследования разработанного комплекса виртуального амплитудного скремблирования (ВАС) показали, что его применение обеспечивает двукратное уменьшение разборчивости по сравнению с аналоговым скремблированием (АС) с 0,035 по 0,018 при идентичных параметрах (таблица 1).

Таблица 1. Экспериментальные исследования разработанного комплекса виртуального амплитудного скремблирования

	Разборчивость		Избыточность	
с/ш	АС	ВАС	АС	ВАС
1	0,892	0,675	0,879	0,652
0,33	0,644	0,350	0,625	0,334
0,05	0,032	0,081	0,025	0,087

При этом выигрыш в разборчивости не сопровождается соответствующим выигрышем в избыточности. Это можно рассматривать как один из недостатков данного комплекса. Однако, довольно существенное уменьшение разборчивости, обеспеченное комплексом позволяет сделать вывод о целесообразности его применения при решении задач защиты речевой информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Котенко В.В., Румянцев К.Е., Поликарпов С.В. Новый подход к оценке эффективности способов шифрования с позиций теории информации. Вопросы защиты информации: Науч.–практ. журн./ ФГУП «ВИМИ», 2004, №1. С. 16-22.