Обзор современных устройств скремблирования

Если информационная атака по телефонному каналу осуществляется за счет подключения к линии связи радиозакладного устройства контактного типа с питанием от самой линии, тогда такие устройства меняют характеристики самой линии, может быть зафиксированным приборами или системами анализа состояния телефонной линии. Получение такой информации может быть поводом для вывода о несанкционированном доступе к данной линии. Например, подключение радиозакладок или телефонных ретрансляторов такого типа приводит к изменению значения питающего напряжения телефонной станции. Причем закладное устройство может подключаться параллельно и последовательно к линии связи и в зависимости от этого напряжение в линии будет меняться на ту или иную величину.

Для передачи цифровой информации используют устройства серии СМ: карманный телекс-шифратор СМ-11, шифратор для телефаксов СМ-13 радиопереговорное четырехканальное устройство СМ-21 для диапазона 134 ... .174 мГц и др.

В речевых системах связи известно два основных метода закрытия речевых сигналов, различающихся по способу передачи по каналам связи: аналоговое скремблирование и дискретизация речи с последующим шифрованием. Под скремблированием понимается изменение характеристик речевого сигнала, таким образом, что полученный модулированный сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает ту же полосу частот, что и исходный сигнал.

Каждый из этих методов имеет свои достоинства и недостатки. Так, для аналоговых скремблеров характерно присутствие при передаче в канале связи фрагментов исходного открытого речевого сообщения, преобразованного в частотной и (или) временной области. Это означает, что злоумышленники могут попытаться перехватить и проанализировать передаваемую информацию на уровне звуковых сигналов. Поэтому ранее считалось, что, несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспечивать лишь низкую или среднюю, по сравнению с цифровыми системами, степень закрытия. Однако новейшие алгоритмы аналогового скремблирования способны обеспечить не только средний, но очень высокий уровень закрытия.

Цифровые системы не передают какой-либо части исходного речевого сигнала. Речевые компоненты кодируются в цифровой поток данных, который смешивается с псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов. Подготовленное таким образом сообщение передается с помощью модема в канал связи, на приемном конце которого проводятся обратные преобразования с целью получения открытого речевого сигнала.

Технология создания широкополосных систем, предназначенных для закрытия речи, хорошо известна, а ее реализация не представляет особых трудностей. При этом используются такие методы кодирования речи, как АДИКМ (адаптивная дифференциальная и импульсно-кодовая модуляция), ДМ (дельта-модуляция) и т.п. Но представленная таким образом дискретизированная речь может передаваться лишь по специально выделенным широкополосным каналам связи с полосой пропускания 4,8–19,2 кГц. Это означает, что она не пригодна для передачи по линиям телефонной сети общего пользования, где требуемая скорость передачи данных должна составлять не менее 2400 бит/с. В таких случаях используются узкополосные системы, главной трудностью при реализации которых является высокая сложность алгоритмов снятия речевых сигналов, осуществляемых в кодерных устройствах.

Посредством дискретного кодирования речи с последующим шифрованием всегда достигалась высокая степень закрытия. Ранее этот метод имел ограниченное применение в имеющихся узкополосных каналах из-за низкого качества восстановления передаваемой речи. Достижения в развитии технологий низкоскоростных дискретных кодеров позволили значительно улучшить качество речи без снижения надежности закрытия.

Аналоговые скремблеры подразделяются на:

• речевые скремблеры простейших типов на базе временных и (или) частотных перестановок речевого сигнала;

• комбинированные речевые скремблеры на основе частотно-временных перестановок отрезков речи, представленных дискретными отсчетами, с применением цифровой обработки сигналов.

Цифровые системы закрытия речи подразделяются на широкополосные и узкополосные.

Говоря об обеспечиваемом уровне защиты или степени секретности систем закрытия речи, следует отметить, что эти понятия весьма условные. К настоящему времени не выработано на этот счет четких правил или стандартов. Однако в ряде изделий основные уровни защиты определяются, как тактический и стратегический, что в некотором смысле перекликается с понятиями практической и теоретической стойкости криптосистем закрытия данных.

- Тактический, или низкий, уровень используется для защиты информации от прослушивания посторонними лицами на период, измеряемый от минут до дней. Существует много простых методов и способов обеспечения такого уровня защиты с приемлемой стойкостью.

- Стратегический, или высокий, уровень ЗИ от перехвата используется в ситуациях, подразумевающих, что высококвалифицированному, технически хорошо оснащенному специалисту потребуется для дешифрования перехваченного сообщения период времени от нескольких месяцев до нескольких лет.

Часто применяется и понятие средней степени защиты, занимающее промежуточное положение между тактическим и стратегическим уровнем закрытия. Следует отметить, что такое понятие, как качество восстановленной речи, строго говоря, достаточно условно. Под ним обычно понимают узнаваемость абонента и разборчивость принимаемого сигнала.

Характеристика	Тип та марка				
	SCR-M1,2	CTA-1000	Орех-А	ACS-2	F-117A (для радіо-станцій)
Загальна кількість комбінацій ключів	$2*10^{25}$	10^{16}	10^{36}	13122	128
Розрядність сеансового ключа, біт	61	Немає даних	Немає даних	Немає даних	Немає даних
Тривалість затримки мовного сигналу, с	0,45	0,32	0,32	Немає даних	Немає даних
Мовна розбірливість %, не менше	Немає даних	Немає даних	90	Немає даних	Немає даних
Час установлення захищеного зв'язку, с, не більше	Немає даних	Немає даних	10	25	Немає даних
Параметри джерела живлення	220 В 50Гц, 10Вт	220 В 50Гц, 6Вт	220 В 50Гц,6Вт	9В	3х1,5В
Габарити, мм	230х275х65	330х260х65	190х300х40	196х64х53	80х50х30
Маса, кг	3	3	2	0,285	0,115