СКРЕМБЛЕР - СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИОННЫХ КАНАЛОВ

Хрипач А.В., Шванц А.О.
Кафедра теоретических основ электроники
Научный руководитель: Кукин Д.П.
e-mail: staisy.a@mail.ru

Аннотация **– Мы живем в такие времена, когда защита телефона от прослушиваний касается буквально всех – начиная от знаменитостей и политиков до бизнесменов и обычных людей. Информационная защита необходима для сохранения не только важной и секретной, но и просто конфиденциальной информации. Как защитить свою информацию? Самое простое – не обсуждать по телефону ничего, что может представлять минимальный интерес для чужих людей. Но понятно, что это не лучший выход в наше время. Поэтому оптимальное решение - системы защиты информации.**

Ключевые слова: скремблер, защита, информация, каналы, шифрование, скремблирование, связь.

Скремблер – это шифровальное устройство речи, используемое в системах телефонной связи. Шифрование выполняется разбиением спектра звукового сигнала на части (поддиапазоны) и дальнейшей частотной инверсией каждой из этих частей. Частотная инверсия равносильна повороту поддиапазона вокруг некоторой точки, при этом происходит преобразование высоких частот внутри поддиапазона в низкие, а низких в высокие. Частота, на которой происходит разделение спектра речевого сигнала на поддиапазоны, называемая точкой разбиения, может быть либо фиксированной, в случае, когда в течение разговора не происходи переключение между режимами скремблирования, либо принимать одно из четырех возможных значений, когда в течение ведения переговоров абоненты переключаются между режимами.

Для того чтобы зашифрованную речь мог слышать и тот человек, с кем ведется беседа, у него также должен быть скремблер с тем же алгоритмом скремблирования, как и на передающей стороне. В данном случае происходит процесс расшифровки (дешифрование).

Расшифровка речи происходит в обратном порядке скремблером, у которого для расшифровки речи выбрана та же точка разбиения, что и у устройства на передающей стороне. Таким образом, работающие синхронно скремблеры одновременно и шифруют, и расшифровывают передаваемую информацию, и разговаривающие между собой люди понимают друг друга, в отличие от тех, кто подключился к их разговору.

В последнее время сфера применения скремблирующих алгоритмов значительно сократилась. Это объясняется, в первую очередь, снижением объемов побитной последовательной передачи информации, для защиты которой были разработаны данные алгоритмы. Практически повсеместно в современных системах применяются сети с коммутацией пакетов, для поддержания конфиденциальности которой используются блочные шифры. А их криптостойкость превосходит, и порой довольно значительно, криптостойкость скремблеров.

Суть скремблирования заключается в побитном изменении потока данных проходящего через систему. Практически единственной операцией, используемой в скремблерах, является XOR – "побитное исключающее ИЛИ". Параллельно прохождению информационного потока, в скремблере по определенному правилу генерируется поток бит – кодирующий поток. Как прямое, так и обратное шифрование осуществляется наложением XOR кодирующей последовательности на исходную.

Генерация кодирующей последовательности бит производится циклически из небольшого начального объема информации – ключа по следующему алгоритму: из текущего набора бит выбираются значения определенных разрядов и складываются по XOR между собой. Все разряды сдвигаются на 1 бит, а только что полученное значение ("0" или "1") помещается в освободившийся самый младший разряд. Значение, находившееся в самом старшем разряде до сдвига, добавляется в кодирующую последовательность, становясь очередным ее битом (см. рис.1).

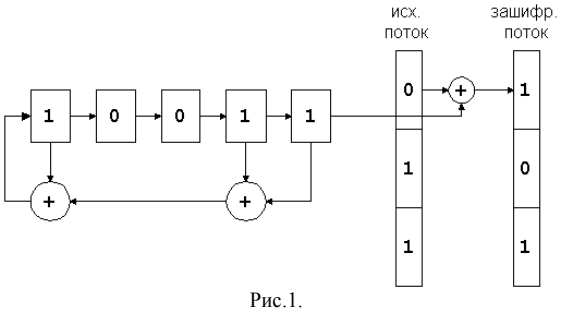

Рис.1.

Как видим, устройство скремблера предельно просто. Его реализация возможна как на электронной, так и на электрической базе, что и обеспечило его широкое применение в полевых условиях. Более того, тот факт, что каждый бит выходной последовательности зависит только от одного входного бита, еще более упрочило положение скремблеров в защите потоковой передачи данных.

[1] Беляев А.В. «Методы и средства защиты информации»
[2] «Коммерческие речевые шифраторы»
[3] «Симметричные криптоалгоритмы», lomasko.com