ИСПОЛЬЗОВАНИЕ ДИНАМИЧЕСКИ ИЗМЕНЯЮЩИХСЯ КЛЮЧЕЙ ДЛЯ ПОВЫШЕНИЯ КРИПТОСТОЙКОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Блочные алгоритмы шифрования данных с симметричным ключом появились достаточно давно и нашли заслуженно широкое распространение при применении их в качестве базовых алгоритмов, используемых в аппаратных и программных системах шифрования [1]. Стойкость шифрования данных такими алгоритмами обеспечивается в первую очередь длиной ключа, поэтому радикальным методом увеличения криптостойкости системы шифрования является использование системы с динамически изменяющимися в процессе шифрования ключами. Предлагаемый авторами способ позволяет изменять ключ в процессе передачи данных по компьютерным сетям, обеспечивая шифрование разных блоков одного сообщения разными ключами.

Сущность способа заключается в периодической смене ключа при передаче данных по компьютерным сетям с шифрованием последующих блоков с использованием измененного ключа. Для смены ключа используется специальный некорректный («битый») пакет, нарушающий тем или иным способом целостность передаваемых по сети пакетов, состоящих из зашифрованных блоков данных, но не нарушающий целостность сетевых данных. Наличие «битого» пакета синхронизирует переход к новому ключу, заранее определенному для двух сторон. «Битый» пакет должен быть абсолютно допустимым для компьютерной сети, не требующим специальной реакции со стороны сетевого оборудования или операционной системы. Для двух сторон, участвующих в процессе передачи зашифрованных данных, создается секретная таблица ключей. Каждый ключ в таблице имеет свой идентификационный номер, определяющий местоположение ключа в таблице. Очень желательно, чтобы в таблице содержалось множество идентификационных номеров псевдонимов для каждого конкретного ключа, и множество идентификационных номеров, соответствующих «пустым ключам», которые не предполагают смену ключей при шифровании и маскируют сам факт смены ключа при криптоанализе.

Идентификационный номер нового ключа может быть передан в любом заранее определенном месте сетевого пакета, например, его очень удобно совместить с передачей контрольных данных сетевого пакета. Этот подход потребует решения

обратной задачи вычисления исходного сообщения для известного контрольного кода. В сетях стандарта Ethernet в качестве алгоритма вычисления контрольной суммы используется тридцатидвухразрядный циклический избыточный код CRC32. Этот код позволяет легко сгенерировать псевдослучайный пакет исходного сообщения исходя из требуемого значения, используемого как идентификационный номер ключа. Для наполнения генерируемого пакета можно использовать не только математические псевдослучайные генераторы, но и физические генераторы случайных последовательностей, что является существенным для повышения криптостойкости.

Предложенный способ позволяет затруднить криптоанализ зашифрованных сообщений, так как в случае его проведения потребуется поиск множества ключей на которых шифровалось передаваемое сообщение.

Список литературы

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на языке С. – 2-е изд. / Б. Шнайер. – Киев: Диалектика, 2017.