ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ PON

Д.В. Глущенко, В.Н. Урядов

Основной особенностью всех PON сетей является то, что нисходящий поток достигает все оптические сетевые блоки (ONU), подключенные к сети. Злоумышленник после некоторых манипуляций с перепрограммированием ONU может добиться того, что будет получать информацию, адресованную другим ONU. Система безопасности PON сетей как раз должна уметь противостоять такого рода угрозам, как "прослушивание".

Другая особенность сети PON состоит в том, что пользователь одного ONU никаким образом не может получить передаваемую информацию пользователем другого ONU, что позволяет передавать в восходящем потоке шифро-ключи и другую важную информацию без необходимости предварительного шифрования этих данных.

Для примера рассмотрим основной алгоритм шифрования, использующийся в технологии GPON — расширенный стандарт криптозащиты (AES — Advanced

Encryption Standard). Этот алгоритм шифрования относится к виду так называемых блочных кодов, который обрабатывает блоки данных длинной 16 байт.

Стандарт AES поддерживает несколько режимов шифрования данных, однако в технологии GPON используется только один из них. Он называется "шифрование со счётчиком" Counter Mode (CTR). Шифратор создает поток, состоящий из 16-байтных псевдослучайных шифроблоков. по заданному алгоритму шифроблоки взаимодействуют с входной нешифрованной информацией, в результате чего на выходе получается зашифрованная информационная последовательность. На приемной стороне происходит обратная операция, в которой участвуют те же самые шифроблоки и зашифрованная информационная последовательность. В результате получается исходная нешифрованная информационная последовательность. В технологии GPON стандартным ключом является ключ длиной 128 битов, хотя могут поддерживаться и ключи большей длины.