СЕКЦИЯ 3. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

МАРШРУТИЗАЦИЯ И ФОРМИРОВАНИЕ СИММЕТРИЧНОГО КЛЮЧЕВОГО ПРОСТРАНСТВА В СИСТЕМАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С САМОСИНХРОНИЗИРУЮЩИМИСЯ КАНАЛАМИ СВЯЗИ

Д.М. Бильдюк

Известно, что симметричные алгоритмы шифрования могут быть использованы в различных режимах криптографического преобразования информации. Традиционно эти режимы классифицируют согласно американскому стандарту FIPS 81. Некоторые из этих режимов шифрования имеют одну общую характеристику — наличие вектора инициализации. Использование вектора инициализации совместно с алгоритмом диверсификации ключа дает возможность построения самосинхронизирующихся криптографических каналов (синхроканалов) связи. Использование синхроканалов для организации ключевого пространства позволяет создавать криптографические системы защиты информации, и накладывает на сеть ее элементов определенную структуру — дерево или лес, где каждый элемент более высокого уровня может создать виртуальный криптографический канал связи с любым элементом более низкого уровня в подчиненной ему ветке дерева. При этом в идентификаторах элементов системы скрыты дополнительные возможности маршрутизации. Используя, например, дизъюнктивный код, наложенный на идентификаторы системы, синхропосылка в шифрованном сообщении может быть использована для маршрутизации в сети. Однако более эффективной маршрутизации можно достичь, используя избыточные коды, их многообразие множества эквивалентных и их двойственных кодов.

Использование кода (7,4) позволяет использовать множество из 7! эквивалентных кодов, причем мощность пересечений их запрещенных и разрешенных комбинаций могут принимать значения 98\2, 100\4, 104\8 и 112\16 соответственно. В каждом конкретном случае мы можем гарантировать прохождение сообщения через два любых элемента системы для 98, 100, 104 и 112 векторов в зависимости от выбранных проверочных матриц. При этом каждый элемент сети может иметь до 7 адресуемых физических каналов связи и глубину адресации в 16 каналов связи.