МАСКИРОВАНИЕ ПОЛЯ ШИФРОВАННЫХ ДАННЫХ В СИНХРОННЫХ РАДИОСЕТЯХ С ВРЕМЕННЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

Я.С. ЯЗЛОВЕЦКИЙ

Доклад относится к вопросам структурной скрытности синхронных радиосетей с временным разделением каналов, в частности маскирования поля шифрованных данных.

Известны синхронные сети с временным разделением каналов, такие как DECT, GSM, синхронная ALOHA и т.п. В таких сетях разметка временных каналов производится путем передачи сигнала синхронизации в начале каждого канального интервала. После сигнала синхронизации в канальном интервале передаются данные служебной информация и шифрованные данные.

Так как длительность и закон образования сигнала синхронизации, и данные служебной информации изменяются незначительно от цикла к циклу, то возможно определение местоположения в канальном интервале поля шифрованных данных.

В докладе описывается три метода маскирования поля шифрованных данных: 1) изменение закона образования сигнала синхронизации при его неизменной длительности, и скремблирование данных служебной информации; 2) изменение местоположения поля шифрованных данных с помощью изменения длительности сигнала синхронизации; 3) изменение местоположения поля шифрованных данных с помощью добавления ложных шифрованных данных различной длительностью.

Предлагается сравнивать степень маскирования поля шифрованных данных на основе теории информации и корреляционного анализа. Для этого на выбранном интервале, середина которого находится в истинном местоположении поля шифрованных данных, сравниваются ко-

эффициенты полуинтервалов взаимной корреляции между сигналами канального интервала соседних циклов передачи.

Таким образом, путем выбора соответствующих параметров сигналов канального интервала можно добиться определенной степени маскирования поля шифрованных данных при учете оценки затрат на аппаратурную реализацию и оценки возможного снижения пропускной способности временного канала.