УДК 621.391.7
Е.С. Конищева, Д.А. Петров, студенты; М.Н. Фунтиков, старший преподаватель
Донецкий национальный технический университет, г.Донецк
E-mail: alynaknisheva@gmail.com

АНАЛИЗ ЦЕЛЕСООБРАЗНОСТИ ПРИМЕНЕНИЯ ДОПОЛНИТЕЛЬНОГО СКРЕМБЛИРУЮЩЕГО УСТРОЙСТВА В УСЛОВИЯХ БЕСПРОВОДНОЙ СВЯЗИ

На сегодняшний день беспроводные сети широко распространены в мире в большинстве случаев благодаря своей мобильности. Довольно много сделано для улучшения их характеристик. Одной из них является – безопасность. Информация всегда представляла особую ценность, и сегодня в условиях глобализации, вопрос защиты ценного ресурса становится все актуальнее.

В разного рода сетях существуют особые способы защиты передаваемой информации. Подавляющее большинство – это различные методы и способы шифрования информации. Одним из наиболее распространённых способов является скремблирование, позволяющее получить на выходе случайную последовательность, в которой появление «0» и «1» равновероятны. Это позволяет в какой-то степени сделать передачу информации безопасной, и защитить ее от злоумышленника.

Выбор метода защиты зависит от многих факторов. Скремблирование является оптимальным по многим параметрам, что позволяет судить о целесообразности его повсеместного применения.

Применение скремблирования позволяет обеспечить высокую степень защиты информации. Это возможно в том случае, когда использующийся алгоритм кодирования обладает высокой криптостойкостью. Такой метод защиты позволяет обезопасить информацию на протяжении всей линии связи, так как злоумышленник не сможет получить исходную информацию при перехвате ее закодированной версии. Для ее декодирования, он должен определить ключ скремблера (секретная составляющая, по которой происходит шифрование информации), что из-за высокой криптостойкости алгоритма займет большой промежуток времени и за это время информация перестанет быть актуальной.

Также скремблеру присущи и недостатки. К таким относятся необходимость синхронизации приемного и передающего устройства и потеря времени на эту синхронизацию.

Таким образом, применение скремблера позволит обеспечить высокий уровень защиты передачи информации в беспроводных сетях. Полученная злоумышленником информация не будет содержать в себе ценности, при условии, что он не имеет ключ скремблера. Однако существующая вероятность получения злоумышленником ключа скремблера (большие вычислительные мощности аппаратуры перехвата злоумышленника в сочетании с большим промежутком времени, человеческий фактор и т.д.) не позволяет говорить о стопроцентной защите информации.