УДК 621.391.7
Д.А. Петров, Е.С. Конищева, студенты; М.Н. Фунтиков, старший преподаватель
Донецкий национальный технический университет
E-mail: petrov94dmitriy@gmail.com

ИССЛЕДОВАНИЕ МОДЕЛИ СКРЕМБЛЕРА ДЛЯ ШИФРОВАНИЯ ТЕКСТОВОЙ ИНФОРМАЦИИ

Прогресс не стоит на месте. В мире идет интенсивное развитие технологий. Они имеют большое значение в жизни каждого, что в свою очередь ведет к тотальной зависимости. Этот процесс позволяет значительно улучшить жизнь человека, однако в виду такого бурного развития необходимо задумываться не только об улучшение функциональных характеристик устройств, но и о вопросах безопасности.

Вопрос обеспечения безопасности на сегодняшний день решается многими способами, одним из которых есть скремблирование информации. Данный метод активно применятся в области телефонии, телевидении и др.

Скремблер – это довольно простое устройство, позволяющее изменить передаваемое сообщение таким образом, что на выходе имеет место случайная последовательность с равновероятным появлением «0» и «1».

В программном обеспечении LabVIEW был создан виртуальный прибор скремблера.

На выходе виртуального прибора текстовое сообщение не имеет никакой информационной ценности. Исходная информация будет доступна лишь тому, кто обладает ключом (конкретным секретным состоянием некоторых параметров преобразования) алгоритма действия устройства. Это значит, что передающее и приемное устройства должны иметь один и тот же ключ алгоритма скремблирования, без знания этого ключа алгоритма полученная информация так и останется зашифрованной.

Таким образом, главным достоинством скремблера является обеспечение высокой надежности защиты информации, однако присутствует и недостаток: приемная и передающая стороны должны быть синхронизированы между собой. В противном случае вся информация теряется.