

Консоль управления – это интерфейс контроля, который системный администратор использует для удаленного управления любой системой, на которой установлен агент (DeviceLock Service). DeviceLock разработан с тремя различными консолями управления: DeviceLock Management Console (оснастка для MMC), DeviceLock Enterprise Manager и DeviceLock Group Policy Manager (интегрирован в редактор групповых политик Windows). DeviceLock Management Console также используется для управления DeviceLock Enterprise Server'ом.

Автоматизированная система для контроля сменных носителей учащихся, была написана с использованием технологии MFC [2] в интегрированной среде разработки Microsoft Visual Studio 2008.

Пример создания конфигурации usb устройства, для пользователя с учетной записью Test, представлен на рис. 3.

Возможности по управлению внешними устройствами, имеющиеся в современных операционных системах, реализуют, как правило, только базовый функционал разграничения доступа и не обеспечивают необходимой гибкости, безопасности и расширенных функций. Таким образом, только специализированные системы контроля доступа к внешним устройствам могут обеспечить приемлемый уровень снижения риска утечек информации.

Список литературы

1. <http://ic-dv.ru/catalog/nsd/devicelock/>
2. А.Мешков, Ю.Тихомиров. Visual C++ и MFC. 2-е изд.перераб. и доп. – СПб.: БХВ-Петербург, 2003. – 1040стр.

МОДЕЛИРОВАНИЕ УСТРОЙСТВА КОДИРОВАНИЯ РЕЧЕВОГО СИГНАЛА

О.М. Галушко, Массембо Элика Селесте

(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Известно, что наиболее надежными методами защиты от прослушивания речевой информации являются криптографические методы:

- преобразование аналоговых параметров речи;
- цифровое шифрование.

Устройства, использующие эти методы, называются скремблерами.

При **аналоговом** скремблировании производится изменение характеристики исходного звукового сигнала таким образом, что результирующий сигнал становится неразборчивым, но занимает ту же частотную полосу. Это дает возможность без проблем передавать его по обычным каналам связи. При этом методе сигнал может подвергаться следующим преобразованиям:

- частотная инверсия;
- частотная перестановка;
- временная перестановка.

В настоящей работе рассмотрена схема скремблера, использующего метод частотной инверсии. Этот метод давно и успешно применяется, например, полицейскими службами и обеспечивает эффективную защиту радио- и телефонных переговоров от постороннего прослушивания.

При реализации данного метода частотно-инвертированный сигнал выделяется из нижней боковой полосы спектра балансного преобразования звукового сигнала с надзвуковой несущей. Две последовательные инверсии восстанавливают исходный сигнал. Устройство работает как кодер и декодер одновременно. Синхронизации двух скремблеров не требуется.

Моделирование данной схемы имеет целью не только детальное освоение соответствующего пакета анализа электронных схем, но и исследование возможности ее дальнейшего усовершенствования.

Функциональная схема скремблера с частотной инверсией приведена на рис. 1, а принципиальная – на рис. 2



Рис. 1 Функциональная схема скремблера с частотной инверсией

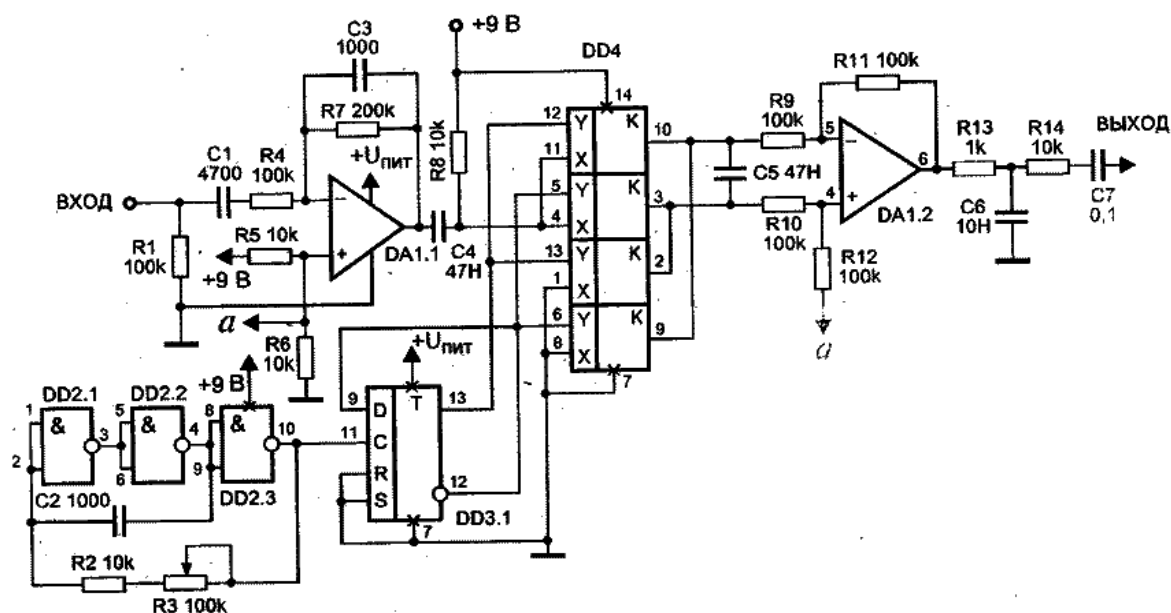


Рис. 2 Принципиальная схема скремблера с частотной инверсией

Устройство состоит из: тактового генератора (мультивибратора) на логических элементах И-НЕ в составе микросхемы DD2, вырабатывающего сигнал частотой 7 кГц; делителя-формирователя несущей - 3,5 кГц на микросхеме DD3.1 (D - триггер); аналогового коммутатора балансного модулятора на микросхеме DD4 (транзисторный коммутатор); входного полосового фильтра с полосой пропускания 300-3000 Гц на операционном усилителе DA1.1 и сумматора балансного модулятора с фильтром низкой частоты на ОУ DA1.2. Подстройка частоты тактовых импульсов, а следовательно частоты несущей, производится многооборотным резистором R3 в схеме мультивибратора.

На рис. 3 представлена схема модели скремблера в пакете EWB 5.12, а на рис. 4 спектры входного и выходного сигналов.

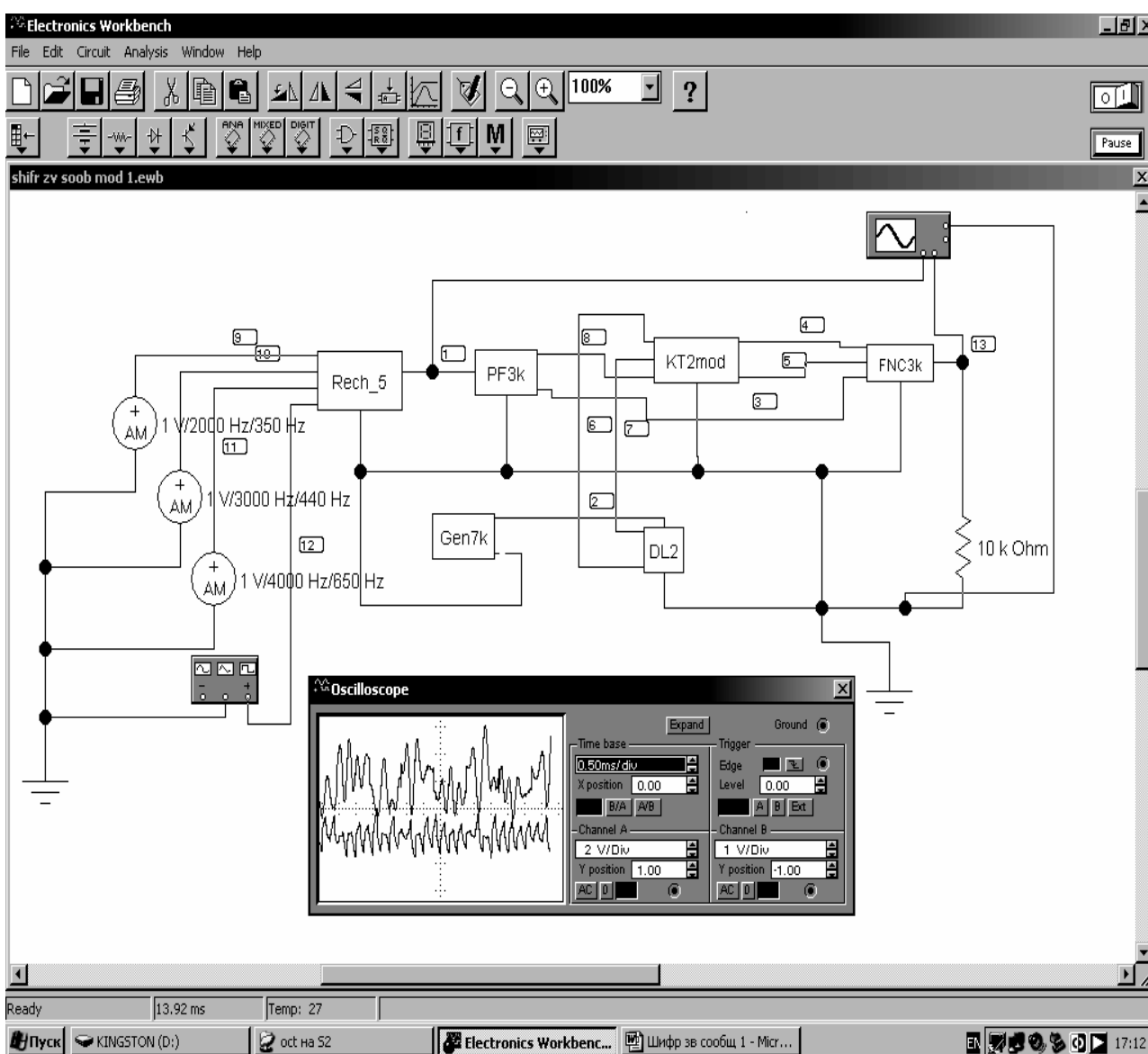


Рис. 3 Схема модели скремблера с частотной инверсией (EWB 5,12).

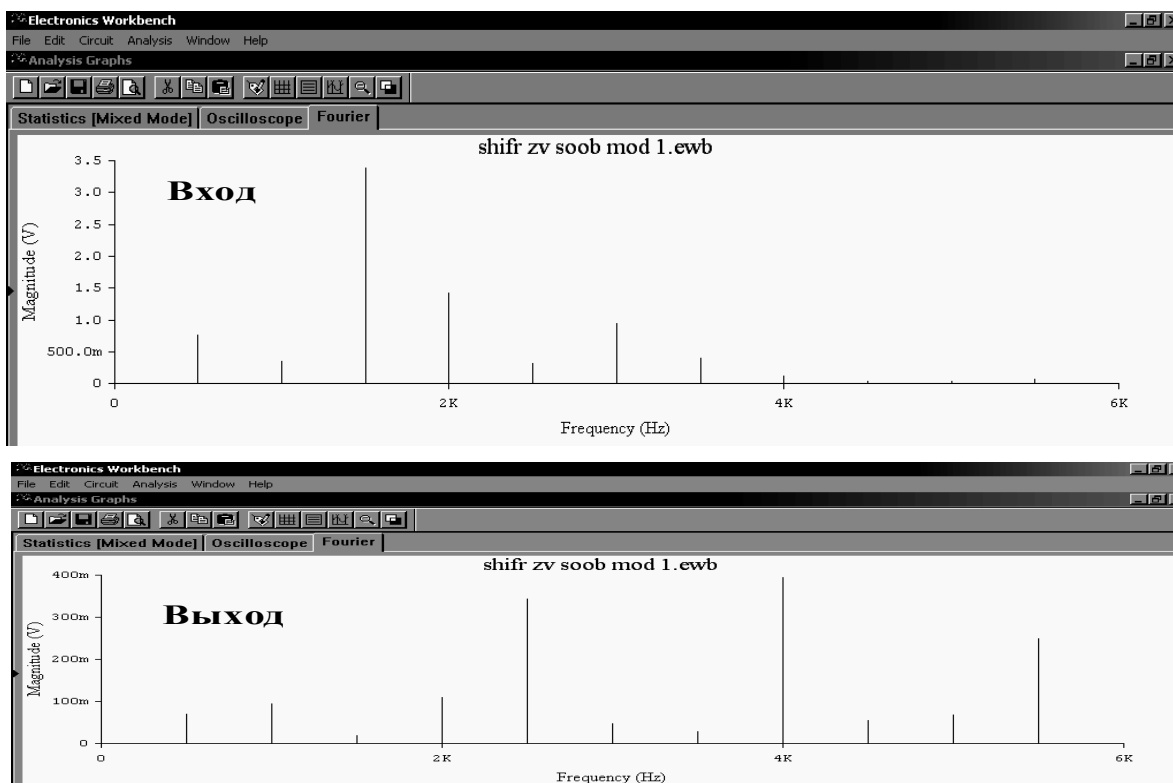


Рис. 4 Спектры входного и выходного сигналов модели скремблера с частотной инверсией.

Таким образом, в пределах полосы частот 300-3000 Гц разборчивость речи после двух преобразований составляет не менее 65%.

Список литературы

1. Петраков А. В. Утечка и защита информации в телефонных каналах: / А. В. Петраков, В. С. Лагутин. - 2-е изд., испр. и доп. М.: Энергоатомиздат, 1997. 298 с.
2. Кардашев Г. А. Виртуальная электроника. Компьютерное моделирование аналоговых устройств. – М., Горячая линия-Телеком, 2002, 264 с.

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ФРАКТАЛЬНОГО СЖАТИЯ АУДИОДАНЫХ

И.М. Удовик, В.С. Долгишев

(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Развитие современных телекоммуникационных сетей характеризуется увеличением доли мультимедийного трафика. Важной составляющей мультимедийного трафика является аудиоинформация, и в частности речевая информация. Проблема, связанная с большим объемом для их передачи и хранения, появилась при работе и на рабочих станциях, и на персональных компьютерах. Известно множество различных алгоритмов архивации аудиоданных, но они либо обеспечивают недостаточные коэффициенты сжатия, либо ведут к существенной потере данных, что в свою очередь связано