2. Таненбаум Э. Компьютерные сети: пер. с англ. СПб. Питер, 2003. 992 с. (Сер. "Классика computerscience").
3. Иванов И.П., Бойченко М.К. Мониторинг ресурсов узлов корпоративной сети // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2010. № 2. С. 114–120.

РАЗРАБОТКА ГЕНЕРАТОРА РЕЧЕПОДОБНОЙ ПОМЕХИ В ПРОГРАММНОЙ СРЕДЕ LABVIEW

Я.И. Грачева, АлтГУ, физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Человеческий разговор, и в частности переговоры, остается важнейшим каналом информационного взаимодействия. Очень часто развитие и введение в эксплуатацию новых систем связи сосредоточено на совершенствование именно этого метода общения. Одновременно усиливается потребность в обеспечении конфиденциальности речевого обмена и защите информации, имеющей речевую природу [1]. В настоящий момент разработан достаточно широкий арсенал различных средств защиты (формальных и неформальных), которые могут обеспечить требуемый уровень защищенности разного рода информации, в том числе и речевой. Из существующих методов защиты речевого сигнала широкое применение нашли методы активной акустической маскировки. В частности в целях данной маскировки используют такие виды помех как белый шум и «речеподобная» помеха.

В настоящей работе был разработан виртуальный прибор, позволяющий генерировать практически любую помеху в зависимости от выбранных параметров и базы файлов. Существует возможность его применения в учебных целях. Прибор создан в среде графического программирования, которая широко используется в промышленности, образовании и научно-исследовательских лабораториях в качестве стандартного инструмента для сбора данных и управления приборами. LabVIEW - мощная и гибкая программная среда, применяемая для проведения измерений и анализа полученных данных [2].

В системах акустической и виброакустической маскировки, как правило, используются шумовые помехи следующих видов: "белый" шум (с постоянной спектральной плотностью в рече-

вом диапазоне частот); "розовый" шум (с тенденцией спада спектральной плотности 3 дБ на октаву в сторону высоких частот); шум с тенденцией спада спектральной плотности 6 дБ на октаву в сторону высоких частот; шумовая "речеподобная" помеха (с огибающей амплитудного спектра, подобной речевому сигналу) [3].

Для исследования эффективности защиты акустического канала связи использовались помехи: белый шум, «речеподобная» типа речевой хор и комбинированная «речеподобная». Для проведения испытаний: в программе Audacity был сгенерирован белый шум; так же в программе Audacity была сформирована «речеподобная» помеха типа речевой хор, методом наложения нескольких звуковых файлов (музыкальный фрагмент, женская, мужская, смешанная речь); в среде разработки LabVIEW был создан виртуальный прибор, генерирующий комбинированную «речеподобную» помеху (рис.1.).

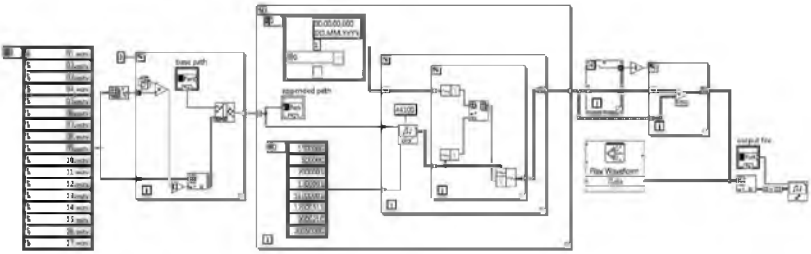

Рис. 1. Блок-схема виртуального прибора генерации речеподобной помехи.

На вход прибора подавалась библиотека из двадцати файлов, состоящая из звуков речи в диапазоне звучания от 90 до 1000 Гц. При смешивании наиболее приемлемым для слуха количеством являются три файла, они выбирались из библиотеки случайным образом, во избежание вырезания одинаковых участков. Далее в каждом файле бралось определенное количество различных его участков по одной секунде. На следующем шаге все файлы накладывались друг на друга. На выходе воспроизводилась и записывалась получившаяся комбинированная «речеподобная» помеха.

Для оценки защищенности канала был использован артикуляционный метод совместно с методом измерения разборчивости по эквиваленту затухания. Артикуляционные испытания эффективно-

сти помехи были реализованы с помощью программы Audacity. Испытания проводила бригада операторов в составе одного диктора, не имеющего явных дефектов речи, и тридцати аудиторов в возрасте от 18 до 51 года, не имеющих дефектов слуха. При подготовке к проведению измерений была осуществлена запись тестового речевого текста (артикуляционных таблиц слов), читаемого диктором. Каждая таблица содержала 10 слов. Диктором было записано 10 таблиц. На них были независимо наложены: сгенерированный в программе Audacity белый шум; сформированная программе Audacity «речеподобная» помеха типа речевой хор; сгенерированная в приборе комбинированная «речеподобная» помеха. Наложение шума происходило в диапазоне [-35; 10] дБ с градацией в 5 дБ.

Проанализировав полученные данные, был получен график зависимости словесной разборчивости от интегрального отношения сигнал/шум (рис. 2.). По оси абсцисс расположен исходный уровень шума в дБ, а по оси ординат словесная разборчивость в процентах.

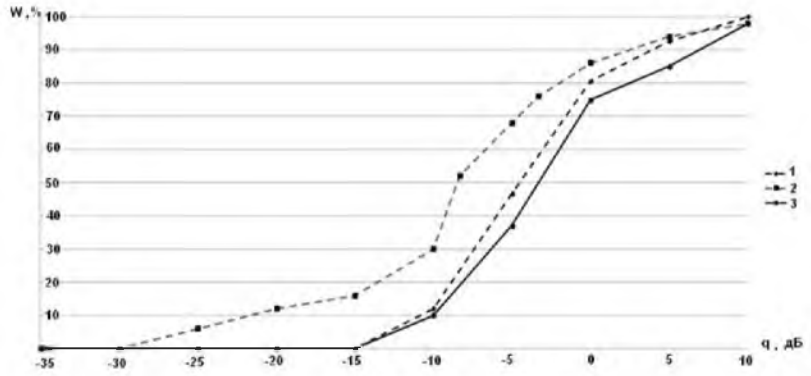

Рис. 2. График зависимости словесной разборчивости W (%) от интегрального отношения сигнал/шум q (дБ) (1 – сигнал + речеподобная помеха типа речевой хор; 2 – сигнал + белый шум; 3 – сигнал + комбинированная речеподобная помеха (прибор)

В результате эксперимента видно, что программная реализация комбинированной «речеподобной» помехи имеет лучшие результаты стойкости зашумления по сравнению с ручным набором помехи в виде «речеподобной» типа речевой хор и белого

шума. Результаты эксперимента согласовываются с литературными данными [4]. Прибор может быть использован для разработки генераторов шума, а так же применяться как встроенный в программно-аппаратный комплекс.

Список литературы

1. А.М. Гришин, Методы защиты речевой информации. // Прикладная Дискретная Математика. – М.:2008. - №2 – С. 67-70.
2. Джеффри Тревис. LabVIEW для всех: Пер. с англ. Клушин Н. А. - М.: ДМК Пресс; ПриборКомплект, 2005. 544 с.
3. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации // Специальная техника. – М.: 2000. – № 5 – С. 46 - 56.
4. Хорев А.А., Макаров Ю.И. Оценка эффективности систем виброакустической маскировки // Вопросы защиты информации. – М.:2001. - №1 – С. 21 – 28.

ПАССИВНОЕ ПРОСЛУШИВАНИЕ И ПЕРЕХВАТ ПАКЕТОВ В БЕСПРОВОДНОЙ WI-FI-СЕТИ

П.С. Ладыгин, АлтГУ, физико-технический факультет, 3к.
Научный руководитель – ***А.В. Мансуров,*** к.т.н., доцент.

В беспроводной сети, построенной по традиционной технологии Wi-Fi, все беспроводные устройства включены в единую среду доступа, образуя один гигантский «хаб» (концентратор) – и любое беспроводное устройство может «видеть» всех беспроводных соседей в сети. При этом приемник, работающий в пассивном режиме (только прослушивание), вообще невозможно определить. Таким образом становится возможен перехват данных посылаемых клиентом на сервер и соответствующий ответ сервера на запрос. Данную особенность беспроводных сетей может использовать злоумышленник, пользуясь своим Wi-Fi – адаптером, который переключается в режим получения всех пакетов (т.н. promiscous-mode), с последующим разбором и анализом полученной информации. [1,2]

Таким образом, технология перехвата трафика подразумевает прослушивание сети, захват, декодирование, исследование и