АППАРАТНЫЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ

Г.В. ДАВЫДОВ, А.И. КУХАРЕНКО, В.А. ПОПОВ, А.А. ТЕРЕНЯ

Генераторы случайных чисел (ГСЧ) широко применяются для создания криптостойких паролей, ключей шифрования, защиты каналов передачи данных и др. Удобно реализовать генератор случайных чисел программными средствами. Однако существует опасность, что алгоритм формирования случайных чисел станет известен нарушителю. Поэтому в системах защиты информации предпочтительно использовать аппаратные генераторы случайных чисел.

Важно при создании ГСЧ использовать источник случайного процесса с высокой энтропией. Известно, что максимальной энтропией при прочих равных условиях обладает так называемый «белый» шум.

Для получения «белого» шума в разработанном ГСЧ использован тепловой шум диода. После усиления шумового сигнала он преобразовывался в цифровую форму с помощью восьмибитового АЦП, выполненного на базе микроконтроллера AT90USB1286. Оцифрованный сигнал передавался по шине USB на персональный компьютер. С помощью программного пакета HEX Editor выполнена оценка плотности распределения вероятностей оцифрованного сигнала по его реализации длительностью 30 мин (6400000 выборок). Получена гистограмма этой оценки. Установлено, что сформированный цифровой «белый» шум имеет распределение вероятностей, близкое к гауссовому.

Конечной целью работы было создание ГСЧ с равномерным распределением цифрового сигнала в диапазоне чисел от 0 до 255. для этого из восьмибитовой выборки цифрового «белого» шума брался один младший разряд. Из полученных n младших разрядов формировалось n-битное значение случайной величины. Получено распределение случайных чисел сформированных из младших разрядов 8-ми разрядных выборок оцифрованного «белого» шума.

Для получения более равномерного распределения случайных величин был разработан специальный алгоритм. Суть алгоритма: из восьмибитовой выборки оцифрованного «белого» шума берётся один младший разряд. Полученные n младшие разряды суммируются по модулю 2. Из вычисленных k значений формировалось k-битное значение случайной величины. По полученным графикам можно судить о степени равномерности распределения случайных чисел. Стоит отметить, что данный алгоритм заметно улучшает распределение, но при этом снижает скорость генерирования последовательности случайных чисел.

Разработанный ГСЧ планируется использовать при создании синтезаторов речеподобных сигналов для систем защиты речевой информации.

АНАЛИЗ КРИТЕРИЕВ ДЕТЕКТИРОВАНИЯ РЕЧИ

ДМ.А. БОРИСЕВИЧ, Г.В. ДАВЫДОВ

Детектор речи предназначен для разделения речи и не речевых сигналов (например, звуковых вызовов факсов, модемов и телефонов, музыки, атмосферных звуковых помех, шума транспорта, длительных пауз в речевых сообщениях и других акустических сигналов, не являющихся речевыми). Детектор речи является необходимым устройством для многих современных устройств телекоммуникаций и средств защиты информации для отделения речи от пауз и сжатия сигналов путём удаления не речевых участков, удаления окружающих шумов во время пауз