УДК 004.312.26
DOI 10.21685/2587-7704-2019-4-1-1

Open Access RESEARCH ARTICLE

Узел цифровой обработки речевого сигнала, обеспечивающий криптографическую защиту интерфейса с блоком шифрования данных для устройства скрытной передачи закрытой информации

А. А. Кулюцин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. Ю. Шабалов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В статье представлена общая функциональная схема устройства скрытной передачи закрытой информации, функциональная схема и алгоритм работы узла цифровой обработки речевого сигнала, работа которого выполняет одну из основных функций. Определена необходимость обеспечения криптографической защиты интерфейса между представленным узлом и блоком шифрования данных устройства.

Ключевые слова: цифровая обработка речевого сигнала, аудиокодек, цифровой сигнальный процессор.

Digital speech signal processing node, providing cryptographic protection of the interface with a data encryption unit for the device of hidden secret data transmission

A. A. Kulyutsin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. Yu. Shabalov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article presents a general functional diagram for the device of hidden secret data transmission, a functional diagram and an algorithm for the operation of digital speech signal processing node, which performs one of the main functions. The need to ensure cryptographic protection of the interface between the presented node and the data encryption unit of the device is determined.

Keywords: digital speech signal processing, audio codec, digital signal processor.

Различные устройства связи по радиоканалу могут использоваться для передачи информации конфиденциального характера. Поэтому не случайно, что наряду с интенсивным развитием устройств передачи речи в радиоканалах все более значимой становится проблема обеспечения защиты информации.

Для обеспечения защиты информации, передаваемой по радиоканалу, могут применяться специальные способы модуляции, позволяющие:

– осуществлять прием информации только при наличии знания специальных структур;

– иметь спектральную плотность мощности сигнала, равную или ниже по уровню спектральной плотности мощности шума.

Также для обеспечения защиты информации может применяться шифрование данных, причем как в совокупности со специальными способами модуляции, так и отдельно.

Реализация устройства, осуществляющего скрытную передачу закрытой информации, включает в себя разработку различных узлов, каждый из которых будет отвечать за работу определенных им функций. Функциональная схема устройства представлена на рис. 1. В нем можно выделить четыре основных узла:

– центральный узел;

– радиомодуль;

– узел цифровой обработки речевого сигнала;

– периферийный узел.

Рис. 1. Функциональная схема устройства

Центральный узел – самая главная часть устройства, он управляет питанием всех узлов, обрабатывает данные, вводимые с клавиатуры, отображает информацию на дисплее, выполняет роль коммутатора между остальными узлами, используя внутренний протокол, содержит в себе блок шифрования данных, так как является доверенной средой.

Радиомодуль осуществляет прием и передачу поступающих сигналов.

Периферийный узел состоит из Bluetooth модуля и GPS модуля. Bluetooth модуль осуществляет передачу данных между центральным узлом и другим удаленным устройством, имеющим Bluetooth модуль. GPS модуль позволяет устройству передавать координаты текущего местоположения.

Узел цифровой обработки речевого сигнала необходим для аналого-цифрового и цифро-аналогово преобразования речи, ее сжатия с помощью программного кодека, формирования пакетов по правилам внутреннего протокола. Он производит обмен данных с центральным узлом устройства по интерфейсу, обеспечивая ему при этом криптографическую защиту. Это необходимо, так как узел цифровой обработки речевого сигнала не является доверенной средой, следовательно, может сгенерировать специальную последовательность сигналов, способную преднамеренно повлиять на блок шифрования данных, который находится в центральном узле.

Так как устройство осуществляет передачу данных, в том числе речи, по радиоканалу, то узел цифровой обработки речевого сигнала в нем необходим, так как цифровая обработка речевого сигнала позволит эффективнее использовать радиоресурсы. Функциональная схема узла представлена на рис. 2.

Рис. 2. Функциональные схема узла цифровой обработки речевого сигнала

Узел состоит из:
– микрофона;
– динамика;
– аппаратного аудиокодека TLV320AIC3204;
– флеш-памяти;
– цифрового сигнального процессора TMS320C5535.

Микрофон и динамик подключены к аналого-цифровому и цифроаналоговому преобразователям аппаратного аудиокодека.

Аппаратный аудиокодек TLV320AIC3204 представляет собой малопотребляющий, низковольтный аудиокодек с программируемыми входами и выходами [1].

Аудиокодек настроен на частоту дискретизации 8000 Гц, значение количества бит, выделяемых на один звуковой отсчет, установлено 16, отрегулированы значения усилителей для получения приемлемого качества звука.

Взаимодействие аппаратного аудиокодека с цифровым сигнальным процессором происходит с помощью интерфейсов I^2S и I^2C. Интерфейс I^2C используется для передачи служебной информации. Интерфейс I^2S используется для передачи оцифрованного речевого сигнала.

Во флеш-памяти хранится прошивка для цифрового сигнального процессора, взаимодействие осуществляется с помощью интерфейса SPI.

Цифровой сигнальный процессор TMS320C5535 обеспечивает высокую производительность и низкую потребляемую мощность за счет увеличения параллелизма. Внутренняя шина процессора состоит из одной программной шины, одной 32-битной шины считывания данных, двух 16-битных шин считывания данных, двух 16-битных шин записи данных и дополнительных шин, предназначенных для работы технологии прямого доступа к памяти. Процессор имеет два блока умножения, центральный 40-битный арифметический и логический блок, который поддерживается дополнительным 16-разрядным арифметико-логическим устройством [2].

Цифровой сигнальный процессор, кроме аппаратного аудиокодека, также взаимодействует с центральным узлом устройства с помощью физического протокола передачи данных UART. На нем реализована работа программного кодека и внутреннего протокола устройства. Необходимость сжатия оцифрованного речевого сигнала обусловлена тем, что до момента сжатия скорость передачи та-

кого сигнала будет равна 125 кбит/с. Чтобы передать такой поток данных, нужны очень большие частотные ресурсы. Для их экономии происходит сжатие сигнала с помощью программного кодека Mixed-excitationlinearprediction, в итоге скорость передачи опускается до 2,4 кбит/с и становится приемлемой. Также процессор осуществляет обработку пакетов, как поступающих из центрального узла, так и отправляемых туда, по правилам внутреннего протокола. Данный протокол содержит множество команд, с помощью которых центральный узел может управлять работой узла цифровой обработки речевого сигнала. Для того, чтобы процессор успевал в реальном времени обрабатывать оцифрованный речевой сигнал и выполнять функции внутреннего протокола, перенос цифровых отсчетов речевого сигнала в память процессора осуществляется с помощью технологии прямого доступа к памяти. Прямой доступ к памяти – режим обмена данными между устройствами процессора или же между устройством и основной памятью, в котором процессор не участвует. Так как данные не пересылаются в процессор и обратно, скорость передачи увеличивается.

Криптографическая защита интерфейса между данными узлами происходит путем наложения гаммы на передаваемые в центральный узел данные, гамма генерируется в блоке шифрования данных и передается в цифровой сигнальный процессор.

Библиографический список

1. TLV320AIC3204 Ultra Low Power Stereo Audio Codec datasheet. – URL: http://www.ti.com/lit/ds/symlink/tlv320aic3204.pdf (дата обращения: 13.10.2018).
2. TMS320C5535 Fixed-Point Digital Signal Processors datasheet. – URL: http://www.ti.com/lit/ds/symlink/tms320c5535.pdf (дата обращения: 13.10.2018).

Образец цитирования:

Кулюцин, А. А. Узел цифровой обработки речевого сигнала, обеспечивающий криптографическую защиту интерфейса с блоком шифрования данных для устройства скрытной передачи закрытой информации / А. А. Кулюцин, А. Ю. Шабалов // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–4. – DOI 10.21685/2587-7704-2019-4-1-1.