

Таблица

Результаты измерений СПЭЯ в спектральных каналах L8 и БКА

	Канал	Зона 1	Зона 2	Зона 3	Среднее отношение $\frac{x_{БКА}}{x_{L8}}$
Синий	L8 blue	103,2	105,7	105,1	0,95
	БКА band_1	98,5	99,2	101,3	
Зеленый	L8 green	116,22	119,1	121,5	0,95
	БКА band_2	108,55	113,7	117,1	
Красный	L8 red	132,2	135,75	140,7	0.98
	БКА band_3	128,4	134,76	136,6	

Литература

1. Черкашин А. К. Принципы организации и обслуживания международной системы подспутниковых полигонов // Четвертый Белорусский космический конгресс. Минск, 2009. В 2 т. Т.2., С.12-19.

**РАЗРАБОТКА СИСТЕМЫ ЗАЩИЩЕННОГО ОБМЕНА
ДАНЫМИ МЕЖДУ ПК И МК ПОСРЕДСТВОМ
СТАНДАРТНЫХ ИНТЕРФЕЙСОВ**

К. А. Скрипко, И. А. Шалатонин

Информационные процессы, происходящие повсеместно в мире, выдвигают на первый план, наряду с задачами эффективной обработки и передачи информации, важнейшую задачу обеспечения безопасности информации. Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

- Ростом количества устройств.
- Расширением сферы использования устройств.
- Повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности.
- Ростом ущерба в результате несанкционированного использования информации.
- Ростом ценности информации.

В настоящее время наблюдается тенденция расположения устройств сбора и первичной обработки информации в пунктах ее получения с последующей передачей в центры последующей обработки. Как правило, эти устройства выполняются на базе современных микроконтроллеров.

Целью работы являлась построение системы защищенного обмена данными между ПК и МК при использовании стандартных интерфейсов.

Работа системы защищенного обмена данными осуществляется на основе протокола TLS (Transport Layer Security).

Протокол TLS основан на протоколе SSL, изначально разработанном в Netscape для повышения безопасности электронной коммерции в Интернете. В соответствии с моделью OSI/ISO протокол SSL был реализован на application-уровне, непосредственно над TCP, что позволяет более высокоуровневым протоколам (таким как HTTP или протоколу электронной почты) работать без изменений. Если SSL сконфигурирован корректно, то сторонний наблюдатель может узнать лишь параметры соединения (например, тип используемого шифрования), а также частоту пересылки и примерное количество данных, но не может читать и изменять их.

Структурная схема разработанного нами комплекса, реализующего защищенный обмен информацией между устройствами пользователя и целевой системой на базе микроконтроллера, приведена на рисунке 1.

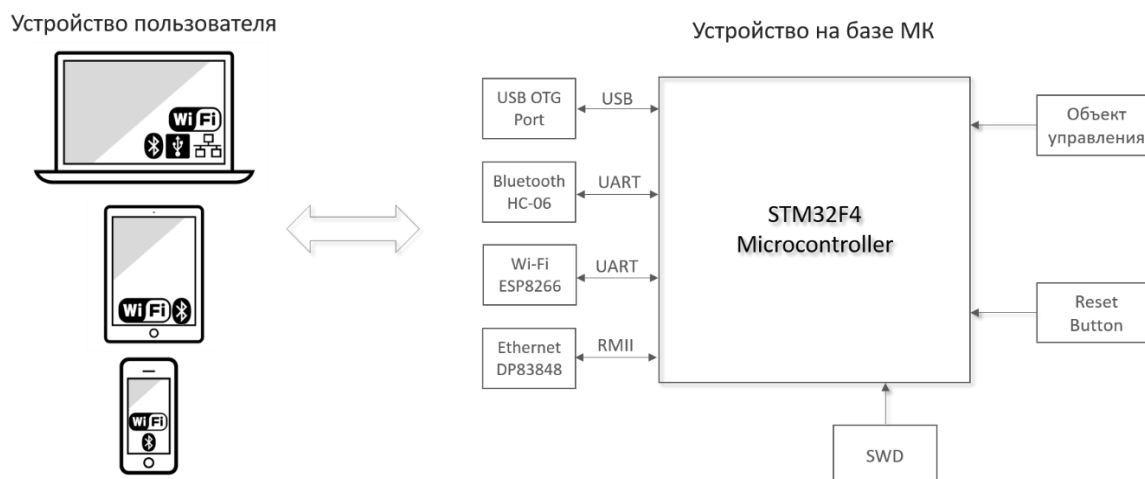


Рис. 1. Структура аппаратной части комплекса

Аппаратная платформа комплекса базируется на отладочной плате STM32F4-Discovery. В основе платы лежит микроконтроллер с ядром ARM Cortex-M4 и максимальной тактовой частотой 168 МГц, что позволяет использовать его в приложениях, где необходимо высокое быстродействие. Объем флэш-памяти составляет 1 МБ, ОЗУ – 192 кбайт. Микроконтроллер содержит все необходимые для подключения устройств пользователя периферийные модули: DAC, ADC, SPI, I2C, PWM, RTC, USB, Ethernet, SDIO. В составе микроконтроллера также присутствует аппаратный генератор случайных чисел.

Взаимодействие комплекса с клиентскими устройствами может осуществляться по следующим интерфейсам:

1. USB.
2. Bluetooth.

3. Wi-Fi.
4. Ethernet.

В процессе создания ПО системы использовались следующие компоненты:

mbedTLS – развиваемая компанией ARM свободная криптографическая библиотека с поддержкой SSL/TLS. Библиотеке mbedTLS свойственна компактность, самодостаточность, модульность и очень низкое потребление памяти.

LwIP – широко используемый TCP/IP-стек с открытым исходным кодом, предназначенный для встраиваемых систем.

mbed OS – бесплатная операционная система для систем на базе процессоров ARM Cortex-M, объединяющая основные функциональные блоки IoT в одном интегрированном наборе программных компонентов. Бесплатна для использования разработчиками и для распространения, поддерживается экосистемой из более чем 100 OEM-производителей и основных поставщиков микросхем.

Взаимодействие программных компонентов системы отображено на рисунке 2.

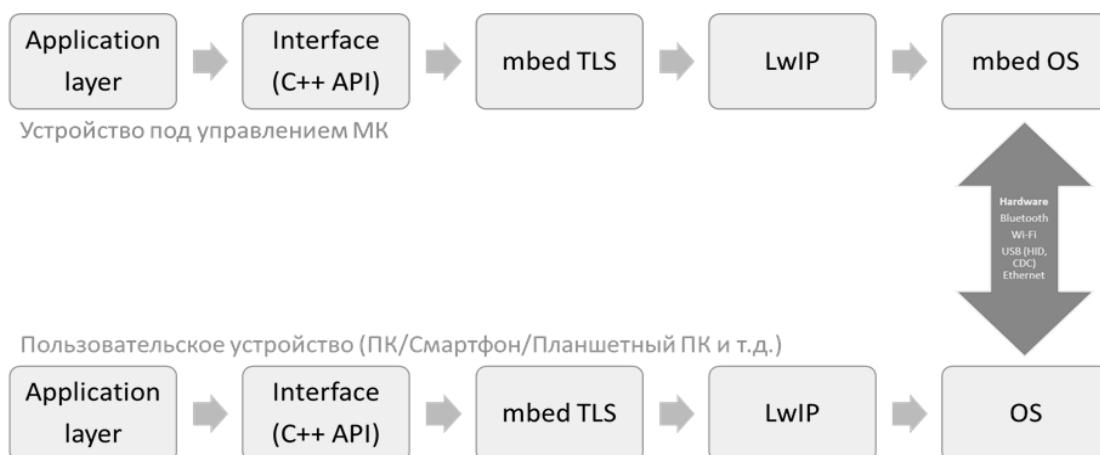


Рис. 2. Программные компоненты комплекса и их взаимодействие

Испытания функционирования предложенной системы защищенного обмена устройств пользователя со встроенной системой проводились нами с использованием Bluetooth-модуля.

Встроенное ПО стенда (firmware) реализовано на языке C++. Демонстрационная программа функционирует на пользовательском устройстве, реализована на C++/QML с использованием Qt Framework и предоставляет следующие возможности:

1. Получение параметров защищенного соединения (ciphersuite);
2. Отправка текстового сообщения на микроконтроллер;

3. Получение текстового сообщения с микроконтроллера;
4. Управление светодиодами (в качестве простейшей модели объекта управления);

ПО демонстрационной программы построено по модульному принципу. Интерфейс демонстрационной программы приведен на рисунке 3. Большую часть интерфейса занимает дамп сетевого трафика. В нем отображается зашифрованный трафик в HEX/ASCII и расшифрованный в ASCII.

Данный комплекс позволяет видеть весь процесс обмена информацией, будь то TLS-Handshake, зашифрованные сообщения или их расшифрованный вид.

Комплекс фиксирует весь трафик и дает возможность проанализировать его, отладить систему защищенного обмена данными, проверить правильность ее работы.

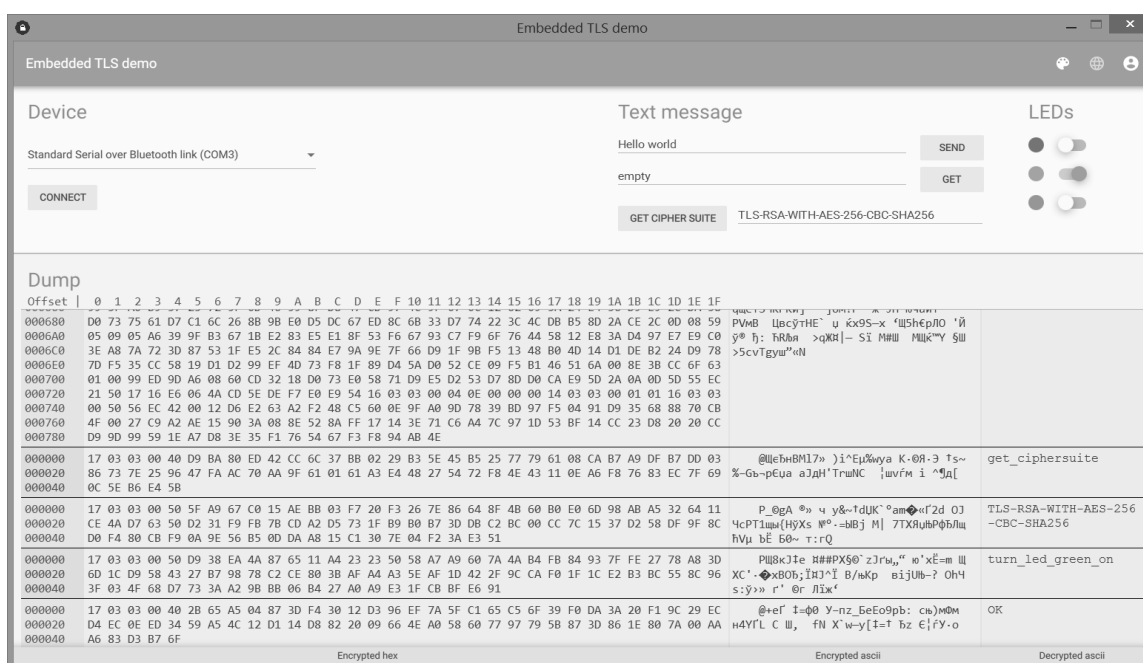


Рис. 3. Интерфейс демонстрационной программы

Совокупность программно-технических средств, используемых в лабораторном комплексе, демонстрирует возможность применения протокола TLS в микроконтроллерных системах при организации защищенного обмена, позволяет проводить изучение работы протокола TLS. Разработанный программно-аппаратный комплекс предполагается использовать при построении лабораторных практикумов по курсам «Программирование МПС на базе МК» и «Программно-аппаратные средства обеспечения информационной безопасности». Предложенная структура построения системы защищенного обмена может быть также применена при создании каналов обмена информацией с реальными встраиваемыми системами.