УДК 004.312

Астапенко Г.Ф., Петрунин А.П., Ращеня Н.А.

АВТОНОМНЫЙ КРИПТОГРАФИЧЕСКИЙ МОДУЛЬ ХРАНЕНИЯ И ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ С USB ИНТЕРФЕЙСОМ

Разработан автономный криптографический модуль хранения и передачи данных, который позволяет хранить ключи и критические данные во внутренней смарт-карте типа simblock, передавать данные по Ethernet сети, взаимодействовать с хост-компьютером через интерфейс USB 2.0.

На данный момент для передачи и хранения конфиденциальной информации широко используется инфраструктура компьютерных систем и сетей. На информационном рынке предлагается широкий спектр услуг в виде аппаратно-программных надстроек в виде виртуальных частных сетей, туннелирования, использования стандартизованных протоколов MACsec, Ipsec, SSL/TLS, HTTPs. Однако эти продукты не всегда обеспечивают необходимый уровень безопасности, имеют экспортные ограничения, не адаптированы для использования отечественных стандартов шифрования, цифровой подписи и распределения ключей. К тому же на практике часто возникают потребности в автономных аппаратно-программных модулях, которые бы легко встраивались в существующие открытые компьютерные и сетевые инфраструктуры и могли бы стать мобильными, безопасными инструментами хранения и передачи конфиденциальных данных.

Нами разработан автономный аппаратно-программный криптографический модуль, который обеспечивает: аппаратные функции шифрования, хэширования, формирования электронной цифровой подписи согласно соответствующим отечественным стандартам; хранение конфиденциальных ключей и критических данных на персональной смарт-карте (форм-фактор – simblock); передачу конфиденциальных данных в сети Ethernet по IPsec туннелю между двумя абонентами, использующими данный модуль; взаимодействие с хост-компьютером по открытому USB-2.0 интерфейсу.

Модуль разработан в двух модификациях – «Икар-1» и «Икар-2». Технические характеристики модулей представлены в таблице 1. Структурная схема модуля «Икар-2» представлена на рисунке 1.

Таблица 1

Технические характеристики модуля «Икар»

Технические характеристики	**Тип модуля**	
	«Икар-1»	**«Икар-2»***
Тип микроконтроллера	TMS320F28034 [1]	Stellaris LM3S9997 [2]
Тактовая частота (МГц)	60	80
Объем флэш-памяти (Кбайт)	128	256
Объем памяти ОЗУ (Кбайт)	20	64
Число программируемых периферийных линий	33	60
Интерфейс взаимодействия со смарт-картой (типа simblock)	ISO 7816-2,3 и 4	ISO 7816-2,3 и 4
Интерфейс взаимодействия с хост-компьютером (USB 2.0)	Скорость передачи – до 12 Мбит/с	Скорость передачи – до 12 Мбит/с
Интерфейс взаимодействия с внешней картой типа microSD	Нет	Объем памяти – 2 Гб
Коммуникационный сетевой интерфейс Ethernet MAC+PHY	Нет	Скорость передачи – 10/100 Мбит/с
* – разработка модуля находится в стадии настройки и отладки.		

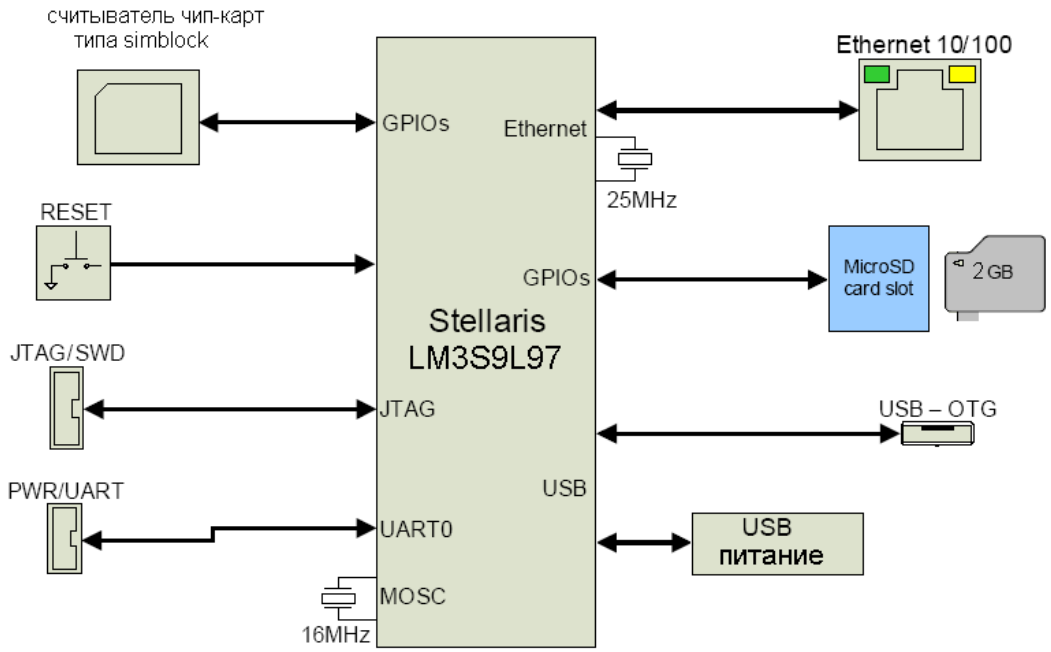

Рисунок 1 – Структурная схема модуля «Икар-2»

В состав программного обеспечения модуля «Икар-1» входят следующие компоненты:

- встроенное программное обеспечение (ВПО) микроконтроллера TMS320F28034,
- встроенное фирменное программное обеспечение USB FIFO чипа (FTDI), с возможностью его перепрограммирования со стороны хост-компьютера через USB интерфейс;
- драйвер и библиотека функций, обеспечивающие программный интерфейс взаимодействия с модулем со стороны хост-компьютера;
- прикладная программа, обеспечивающая тестирование и основные функции взаимодействия и обработки открытых и конфиденциальных данных.

В состав программного обеспечения модуля «Икар-2» входят следующие компоненты:

- ВПО микроконтроллера Stellaris LM3S9997, состоящее из следующих модулей:
  - инициализации и тестирования;
  - диспетчера взаимодействия с хост-компьютером;
  - обеспечения USB-взаимодействия по обмену данными;
  - программное обеспечение сетевого Ethernet взаимодействия на основе стека TCP/IP (с элементами протокола IPsec);
  - обеспечения взаимодействия с внешней картой памяти microSD;
  - обеспечения взаимодействия со смарт-картой в соответствии со стандартом IEEE-7816-3 и IEEE-7816-4;
  - симметричного шифрования данных по ГОСТ 28147-89 и СТБ 34.101.31-2011;
  - вычисления хэш-функции по ГОСТ Р 34.11-94 и СТБ 34.101.31-2011 (функция хэширования);
  - вычисления электронной цифровой подписи по ГОСТ Р 34.10-2001, а также вычисления цифровой подписи и обеспечения функции транспорта ключей по СТБ П 34.101.45-2011;
- встроенное фирменное программное обеспечение StellarisWare, с возможностью его перепрограммирования со стороны хост-компьютера через USB интерфейс;
- драйвер и библиотека StellarisWare, обеспечивающие программный интерфейс взаимодействия с устройством со стороны хост-компьютера;
- прикладная программа icar_mod.exe, обеспечивающая тестирование и основные функции взаимодействия и обработки открытых и конфиденциальных данных.

Основные технические характеристики по реализованным функциям и обмену данными (для модуля «Икар-1»):

- скорость шифрования данных по ГОСТ 28147-89 в режиме гаммирования без обмена с хост-компьютером – не менее 600 кбайт/с;
- скорость шифрования данных по ГОСТ 28147-89 в режиме гаммирования при обмене данными с хост-компьютером – не менее 400 кбайт/с;
- время формирования цифровой подписи при объеме блока данных 1 Кбайт – не более 2 сек;
- время вычисления хэш-функции при объеме данных 400 Кбайт – не более 5 сек.

Размеры изделия («Икар-1»):

- монтажная плата в сборе: 53 × 21 × 6 мм;
- изделие в корпусе: 80 × 30 × 10 мм.

Разработанный модуль обеспечит защиту информации в распределенных информационно-коммуникационных системах.

Список литературы

1. TMS320F28034/35. Datasheet. – Texas Instruments Incorporated, 2009, 138 p.
2. Stellaris LM3S9997 Microcontroller. Datasheet. – Texas Instruments Incorporated, 2011, 1328 p.

The description of autonomous unit, designed in Institute of Applied Physical Problems of name A.N.Sevchenko BSU, is given in this work. The unit allows storing cryptographic keys and critical data in internal smart card such as simblock, to transmit data on the Ethernet network, to interact with host-computer through the interface USB 2.0.

Астапенко Г.Ф., с.н.с. НИИПФП им. А.Н.Севченко БГУ, Минск, Беларусь, e-mail: astapenko@bsu.by.