АППАРАТНО-ПРОГРАММНЫЙ ШИФРАТОР ДАННЫХ, ИСПОЛЬЗУЮЩИЙ USB-ИНТЕРФЕЙС

С.Г. Янковский, А.Л. Труханович

Хранение данных и ограничение доступа к конфиденциальной информации на сегодняшний день одна из важнейших задач пользователя ПК. Для защиты информации от несанкционированного доступа наиболее эффективно использовать криптографическое преобразование данных. Можно применять алгоритмы шифрования, хранящиеся на ПК, но в этом случае возникает проблема хранения ключей и следов криптопреобразования.

Поэтому, для большей надежности, используют внешние шифраторы, которые подключаются к компьютеру, используя стандартный интерфейс связи. Использование микропроцессорных систем позволит более надежно и широко защищать информацию в различных устройствах и при различных способах использования конфиденциальной информации.

На кафедре кибернетики факультета радиофизики и электроники БГУ разработано устройство на основе микроконтроллера M16C/6C, которое по USB интерфейсу подключается к ПК и производит криптографическое преобразование поступающей на него информации.

Микроконтроллеры серии M16C/6C включают в себя ядро процессора серии M16C/60 и флэш-память, используют усложненные инструкции для высокой эффективности. Микроконтроллер способен выполнять команды на высокой скорости, имеет низкое энергопотребление и поддерживает режим работы с дополнительным контролем использования энергии. Интеграция различных периферийных устройств, включая последовательный интерфейс, USB интерфейс, уменьшает количество необходимых системных компонентов [2]. Разработанное устройство имеет следующие основные характеристики:

- частота 32 MHz;
- объем ROM 512 Kbytes;
- объем RAM 31 Kbytes;
- тип памяти: Flash memory.

Для реализации устройства использовался отладочный набор Renesas Starter Kit for M16C6C [3]. В память программ микроконтроллера загружается программа, которая обеспечивает работу устройства, а именно: обеспечивает инициализацию контроллера и его работу, реализует алгоритм шифрования ГОСТ 28147-89, и USB интерфейс связи микроконтроллера с ПК.

В ГОСТ 28147-89 ключевая информация состоит из двух структур данных. Помимо собственно ключа, необходимого для всех шифров, она содержит еще и таблицу замен. Ниже приведены основные характеристики ключевых структур ГОСТа.

Ключ является массивом из восьми 32-битных элементов кода, далее в настоящей работе он обозначается символом К: $\boldsymbol{K} = \{\boldsymbol{K_i}\}_{0 \le i \le 7}$. В ГОСТе элементы ключа используются как 32-разрядные целые числа без знака: $0 \le \boldsymbol{K_i} < 2^{32}$. Таким образом, размер ключа составляет 32·8=256 бит или 32 байта.

Таблица замен является матрицей 8×16, содержащей 4-битовые элементы, которые можно представить в виде целых чисел от 0 до 15. Стро-

ки таблицы замен называются узлами замен, они должны содержать различные значения, то есть каждый узел замен должен содержать 16 различных чисел от 0 до 15 в произвольном порядке. Таблица замен обозначается символом H: $\boldsymbol{H} = \{\boldsymbol{H}_{i,j}\}_{0 \le j \le 15}^{0 \le i \le 7}, 0 \le \boldsymbol{H}_{i,j} \le 15$. Таким образом, общий объем таблицы замен равен: 8 узлов × 16 элементов/узел × 4 бита/элемент = 512 бит или 64 байта. [1]

Для реализации шифрования была разработана функция EncryptData(), на вход которой передается указатель на буфер, состоящий из 8-битных чисел типа UINT8, а также число байт, которые необходимо зашифровать. Далее байты «упаковываются» в 32-х битные числа типа unsigned long, которые подаются на вход функции 32-х циклов основного шага ГОСТ 28147-89. Таким образом, происходит шифрование всего переданного буфера с последующей записью полученного результата в USB канал, для чего используется разработанная функция USBCDC_Write_Async().

Программное обеспечение для верхнего уровня написано на языке программирования java, в среде программирования eclips, с использованием библиотеки для работы со стандартными интерфейсами. Устройство распознается как USB Communication Device Class, это позволяет использовать его как виртуальный COM-порт, что упрощает работу с USB интерфейсом со стороны ПК. Для доступа к COM-порту компьютера был использован пакет javax.comm. Данный пакет не входит в стандартный набор JDK. Программа реализована в консольном режиме и позволяет передавать данные на устройство, принимать данные с шифратора, переводить шифратор в режим шифрования или прозрачный режим.

В результате получилось устройство, позволяющее шифровать информацию, не используя ресурсы компьютера и не храня ключевую информацию на ПК. Устройство способно подключатся по USB интерфейсу и способно зашифровывать информацию, хранящуюся на компьютере, хранить информацию в зашифрованном виде во внутренней флэш-памяти, позволяет осуществить потоковое шифрование информацию, передающуюся в канал связи использующий USB интерфейс. При тактовой частоте контроллера полная скорость шифрования информации с передачей данных по USB каналу составила 1.2 Кбайт/с. Для повышения скорости шифрования можно использовать 32-х разрядные контроллеры с большей тактовой частотой, что должно поднять скорость шифрования в десятки раз. Например, если произвести теоретические расчеты, то при использовании 32-х разрядного процессора с тактовой частотой 144 МГц, скорость шифрования превысит 100 Кбайт/с, а при использовании аппаратной реализации шифрования, подключив к микроконтроллеру программируемую логику, можно повысить скорость шифрования до 80 Мбит/с.

Широкий набор периферийных интерфейсов в микроконтроллере таких как USB, Ethernet, serial, I2C и др. позволяет адаптировать устройство под разные задачи, такие как: устройство шифрования данных на ПК, мост связи с криптопреобразованием для подключения устройство, также можно использовать как защищенное устройство для хранения данных подключаемое по нужному каналу связи.

Исходя из вышеизложенного получается что устройство можно использовать для:

- передачи зашифрованной информации по сетям общего пользования;
- шифрования информации с использованием практически любого алгоритма;
- для взаимодействия с комплектом можно использовать различные интерфейсы, что расширяет область применения данного RSK в том числе и в учебных целях.

Литература

1. *Винокуров А.* Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86. Интернет-адрес: www.twirpx.com/file/218840.
2. M16C/6C Group Hardware Manual , Feb 18, 2008.
3. Renesas Starter Kit for M16C6C User’s Manual Rev.1.00 13.JAN.2009