УДК004.056.53

И.Е. Волкова, А.В. Бухнин, А.Г. Калашникова

УСТРОЙСТВО ДЛЯ ГЕНЕРАЦИИ И ВВОДА ПАРОЛЯ НА БАЗЕ МИКРОКОНТРОЛЛЕРА

Нижегородский государственный технический университет им. Р. Е. Алексеева

В ходе разработки было спроектировано и реализовано устройство для аутентификации пользователя информационной системы. В работе приводится описание алгоритма шифрования и схема управляющей программы микроконтроллера. Описывается процесс создания аппаратной части и прошивки устройства. Практическое использование устройства продемонстрировано на примере аутентификации в операционной системе Microsoft Windows.

Ключевые слова: аппаратный ключ, аутентификация, информационная безопасность микроконтроллер, шифрование.

Процедура проверки подлинности учетной записи пользователя является обязательным условием применения современных программных продуктов, таких как операционные системы, а также системы обработки информации (персональной, деловой, финансовой), доступ к которой должен быть ограничен. Распространенным способом аутентификации является использование пароля. Для обеспечения защиты от подбора пароль должен быть достаточно длинным, состоять из символов разного регистра, включать специальные символы и цифры, не включать целые слова. Пароли, удовлетворяющие этим требованиям, обычно трудны для запоминания, что может побудить пользователя записать пароль на бумаге и сделать его потенциально доступным третьим лицам. Избежать подобных случаев может помочь использование аппаратного ключа, который хранит пароль и позволяет его вводить по запросу. Аппаратный ключ – это устройство, предназначенное для защиты программ и данных от несанкционированного использования, копирования и тиражирования.

Существует множество микроконтроллеров и микропроцессорных устройств, предназначенных для создания различных аппаратных средств: Parallax Basic Stamp, Netmedia's BX-24, Phidgets, MIT's Handyboard и многие другие. Все эти устройства имеют схожие функции и освобождают пользователей от необходимости изучать устройство самого микроконтроллера, давая ему несложный и удобный интерфейс для их программирования [1].Однако в данной статье рассматривается реализация аппаратного ключа на Arduino. Arduino также упрощает процесс работы с микроконтроллерами, но, в отличие от других систем, предоставляет ряд преимуществ – это: низкая стоимость, кроссплатформенность, простая и удобная среда программирования, расширяемое программное обеспечение с открытым исходным кодом, расширяемое открытое аппаратное обеспечение.

В данной статье рассматривается разработка аппаратного ключа на ArduinoUno, т.к. это наиболее распространенная и универсальная модель Arduino. Однако данную разработку, с некоторыми изменениями, можно также реализовывать на других моделях.

В качестве среды разработки была выбрана стандартная среда программирования Arduino – ArduinoIDE, а в качестве языка программирования – язык Arduino.

Спроектированное устройство реализует несколько функций: генерацию символьного пароля, шифрование сгенерированного пароля с помощью ключа, сохранение зашифрованного пароля в энергонезависимой памяти, расшифровку пароля и ввод расшифрованного пароля.

Для создания такого устройства и реализации всех приведенных функций необходимо было решить ряд задач: создать алгоритм шифрования, создать программу на языке Arduino, осуществить перепрошивку загрузчика.

Шифрование пароля в данном устройстве производится с целью демонстрации того, как можно обеспечить безопасность. Однако конкретный алгоритм и его реализация не обеспечивают полную защиту данных в случае дизассемблирования прошивки. Они служат лишь опорной точкой для дальнейшего развития разработки и усложнения устройства.

Для зашифровки пароля используется ключ из случайных символов, хранящийся в энергонезависимой памяти микроконтроллера и генерируемый вместе с новым паролем. Так как мы не добивались полной защищенности от злоумышленника, сложность алгоритма в данном случае не играет роли, ведь при дизассемблировании прошивки с данным методом шифрования будет взломан любой алгоритм.

Длина ключа и пароля в данном случае фиксированы (32 символа), их длина задается при прошивке устройства. Как видно из блок-схемы алгоритма (рис. 1): A[i] – массив символов ключа, B[i] – массив символов пароля. Сначала каждый символ ключа с помощью функции логического умножения умножается на последующий.

В результате получается набор чисел. Далее поочередно берутся все получившиеся числа и из каждого числа с помощью битовой маски выделяется пять первых и пять конечных бит. (В данном случае пять, так как длина пароля тридцать два символа, что равно двум в пятой степени). Получаются пары чисел, попадающие в диапазон от нуля до тридцати одного включительно. Берется первая пара чисел, а далее из пароля выбираются два числа, чьи порядковые номера совпадают с числами из пары и меняются местами.

Таким образом мы получаем «перемешанный» пароль. Новый «перемешанный» пароль с помощью функции сложения по модулю два складываем с первичным ключом. Зашифрованный таким образом пароль сохраняем в энергонезависимой памяти.

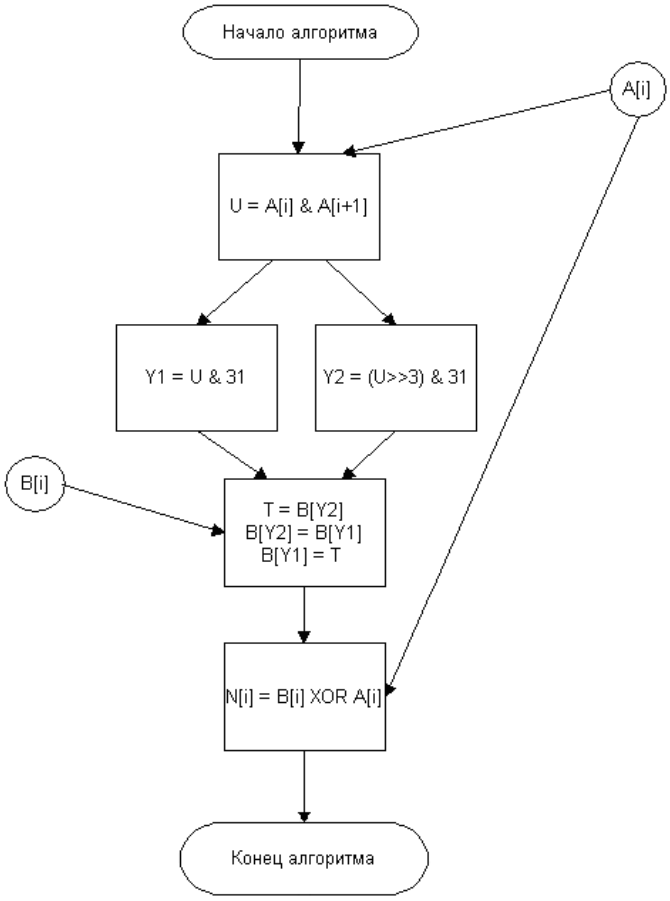

Рис. 1. Блок-схема алгоритма шифрования

При загрузке программы используется Загрузчик (Bootloader) Arduino –небольшая

программа, загружаемая в микроконтроллер на плате. С ее помощью можно загружать программный код без использования дополнительных аппаратных средств [2].

После этих действий можно приступить к проектированию основной программы. Сначала необходимо было создать алгоритм работы программы, для того чтобы четко определить ее структуру и последовательность действий.

После тщательного анализа были определены основные шаги алгоритма (рис. 2):

- выбор нужной функции в зависимости от уровня сигнала на цифровых выводах 2 или 3. На этом этапе в зависимости от того, какая кнопка нажата, программа должна осуществить переход либо на функцию ввода пароля, либо на функцию генерации и сохранения пароля;
- генерация пароля из случайных символов. На данном шаге должна происходить генерация пароля заранее заданной длины, состоящего из случайной последовательности символов – заглавных и маленьких букв и цифр;
- генерация ключа из случайных символов и сохранение его в энергонезависимой памяти. Генерация ключа должна происходить сразу после генерации пароля. Ключ также имеет фиксированную длину;
- шифрование пароля с помощью ключа и сохранение его в энергонезависимой памяти.
- считывание ключа из энергонезависимой памяти;
- расшифровка пароля с помощью первичного ключа, сохраненного в энергонезависимой памяти;
- конвертирование ASCIIкодов символов пароля в HID (human interface device) коды. Это необходимо для того, чтобы вывести символы, так как наше устройство будет определяться как HID;
- передача символов пароля через последовательный порт для их ввода в компьютер.

После создания алгоритма шифрования было решено, что программа будет иметь 14 функций для обеспечения удобства работы программиста. Каждая функция выполняет определенные действия для реализации какого-либо конкретного шага алгоритма программы. Некоторые шаги алгоритма пришлось разбить на несколько функций.

После того, как программа была написана и загружена в микроконтроллер, необходимо было выполнить перепрошивку загрузчика. При использовании стандартной прошивки данное устройство будет определяться компьютером как виртуальный COM-порт и, соответственно, не будет выполнять нужные функции. Поэтому требуется скачать и установить прошивку Arduino-Keyboard-0.3, с которой устройство будет определяться как HID-клавиатура.

Для того чтобы перепрошить загрузчик, необходимо выполнить следующую последовательность действий: сначала с помощью проволоки нужно на короткое время замкнуть два вывода (Reset и GND) Arduino. Затем подключить Arduino к компьютеру, скачать с официального сайта и установить требуемое программное обеспечение (к примеру, программу Flip 3.4.7), а также скачать прошивку. Загрузить прошивку. Переподключить Arduino.

Для завершения аппаратной части устройства потребовалось припаять к плате две кнопки, а также поместить плату в подходящий корпус.

Разработанное устройство работает в двух режимах:

1) режим ввода пароля;
2) режим генерации пароля.

Для того, чтобы ввести пароль, необходимо:

- включить компьютер. Дождаться, когда на экране появятся поля ввода логина и пароля для авторизации;
- подключить устройство к компьютеру с помощью USB кабеля;
- в поле для ввода логина ввести свой логин (если не введен);
- перевести курсор в поле для ввода пароля и нажать кнопку «1» на устройстве. После того, как пароль будет введен, нажать клавишу Enter;

- удостовериться, что пароль был автоматически введен и вход в систему выполнен.

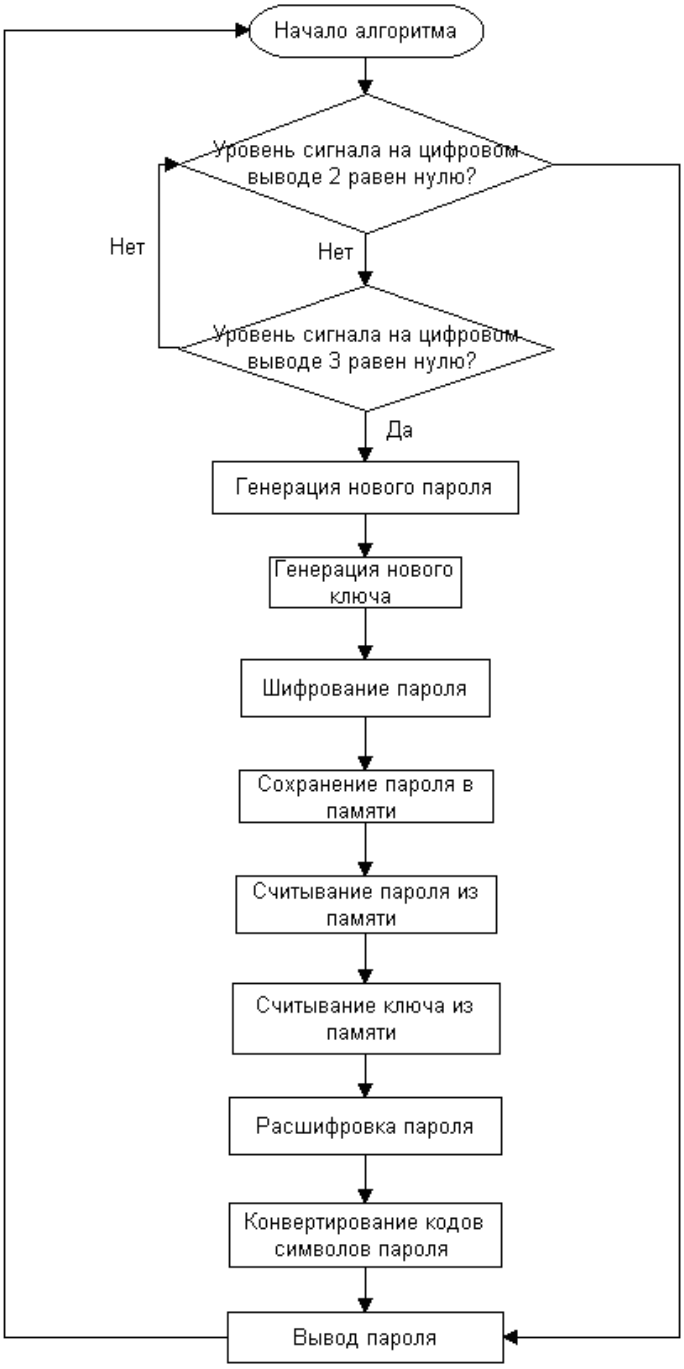

Рис. 2. Блок-схема алгоритма программы

Для того чтобы сгенерировать новый пароль (в системе Windows), необходимо:

- войдя в систему, открыть окно смены пароля (ПУСК->Панель управления -> Учетные записи пользователей -> Выбрать нужного пользователя->Изменение пароля). Подключить устройство к компьютеру с помощью USB кабеля;
- перевести курсор в поле «Старый пароль» и нажать кнопку «1». Удостовериться, что пароль введен;
- теперь перевести курсор в поле «Новый пароль» и нажать кнопку «2». Устройство автоматически сгенерирует новый пароль и сохранит его;

- перейти в поле «Подтверждение» и нажать кнопку «1». Новый пароль будет введен повторно;
- нажать«Изменить пароль» в открытом окне смены пароля.

Пользователю не следует нажимать кнопку «2», если он не собирается менять пароль.

В результате работы было создано устройство для генерации и ввода символьного пароля. Оно является кроссплатформенным аппаратным ключом для входа в информационную систему. Дальнейшим развитием данной разработки может являться усовершенствование алгоритма шифрования, а также создание приложения под операционную систему Windows для обеспечения большей безопасности путем использования шифрующего ключа, привязанного к конкретному компьютеру.

Библиографический список

1. Ардуино в Украине [Электронный ресурс]. – Режим доступа: http://arduino.ua/ru/about/, свободный (16.11.2014);
2. Arduino.ru [Электронный ресурс]. – Режим доступа: http://arduino.ru/Arduino_environment, свободный (16.11.2014).

Дата поступления
в редакцию 11.12.2014

A. V. Bukhnin, I.E. Volkova, A. G. Kalashnikova

A MICROCONTROLLER BASED DEVICE FOR PASSWORD GENERATION AND ENTERING

Nizhny Novgorod state technical university n.a. R.E. Alexeev

The paper describes design and implementation of a device for user authentication. The encryption algorithm and the scheme of the microcontroller control program are presented. The process of hardware assembling and firmware updating is described. Practical use of the device is demonstrated for authentication in Microsoft Windows operating system.

Key words: authentication, encryption, hardware key, information security, microcontroller.