УДК 621.377.6.037

УСТРОЙСТВО ХРАНЕНИЯ И ВВОДА ПАРОЛЕЙ ПО ИНТЕРФЕЙСУ USB

Навумчик П.А.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал «Минский радиотехнический колледж», г. Минск, Республика Беларусь

Научный руководитель: Бойко Д.А. – преподаватель ЦК ПиПРЭС МРК

Аннотация. Проектирование устройства для безопасного хранения паролей пользователя в современном мире. При использовании устройства предполагается существенное увеличение уровня безопасности при создании новых паролей, их последующего хранения, а также быстрого и безопасного ввода при авторизации пользователя в личных и корпоративных сервисах.

Ключевые слова: безопасность, микроконтроллер, пароль

Введение. Безопасность персональных данных напрямую зависит от сложности используемого пароля и места его хранения. Если пароль записан на бумажке или еще хуже – висит на видном месте, то любой человек может получить доступ к рабочим и личным аккаунтам, онлайн-банку или мобильному устройству. Поэтому крайне важно максимально обезопасить свое личное пространство, правильно храня используемые пароли [1].

Большая часть информации в современном мире хранится на разнообразных электронных устройствах – в смартфонах, компьютерах и планшетах. Видео, фотографии, данные о документах и личная переписка, чаще всего защищаются только паролем на вход в устройство. Однако если не следовать достаточно простым правилам, то злоумышленники смогут взломать систему: последствия подобной халатности могут быть достаточно серьезными.

Первым шагом должен стать по-настоящему сложный пароль, в котором будут использованы латинские заглавные и строчные символы, а также цифры. Запомнить подобный набор символов без подсказок смогут немногие. Поэтому вторым шагом следует выбрать метод хранения паролей. В данной статье предложено устройство хранения и ввода паролей по интерфейсу USB [2].

Основная часть. В проектируемом устройстве присутствует разъем USB-C, что соответствует требованиям Еврокомиссии (исполнительного органа Евросоюза) по введению единого порта зарядки и обмена файлами. Это требование основано на мировой тенденции по снижению отходов бытовой и радиоэлектронной аппаратуры, также это позволяет унифицировать провод USB-C для всех устройств и позволяет избежать проблем с поиском нужного провода. Также наличие порта USB-C позволяет подключать провода различной длины, в отличии от устройств, где распаян разъем USB-A или уже разведенных на печатной плате контактов USB 2.0 (устройства с такими вариантами необходимо подключать напрямую к персональному компьютеру или телефону).

Также в проектируемом устройстве имеется экран для вывода информации и кнопки для взаимодействия с устройством. Данная особенность позволяет взаимодействовать с устройством (сохранять и редактировать пароли) без специального программного обеспечения на персональном компьютере.

Для большего понимания рассмотрим структурную схему устройства (рисунок 1).

Напряжение равное 5 В, поступающее через USB, подается на стабилизатор напряжения и понижается до 3,3 В. Пониженное до 3,3 В напряжение необходимо для питания микроконтроллера и дисплея устройства. Для взаимодействия с устройством используются кнопки, изменение состояния которых отслеживает микроконтроллер. Данные пользователя хранятся на энергонезависимом постоянном запоминающем устройстве (ПЗУ) в шифрованном виде. При необходимости данные передаются микроконтроллером по интерфейсу USB.

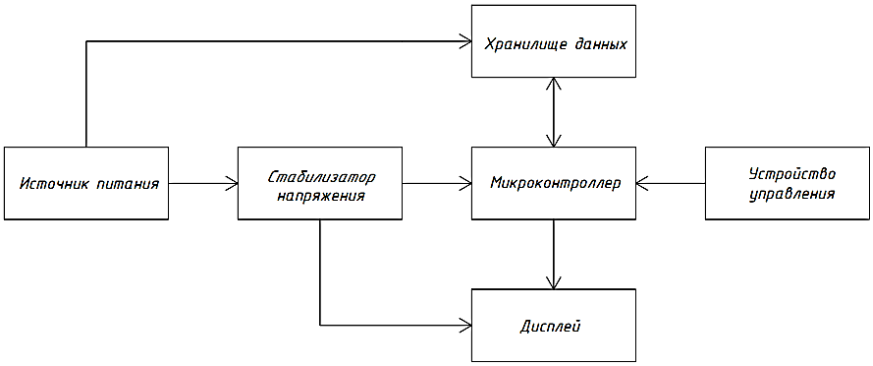

Рисунок 1 – Структурная схема устройства

Для безопасного использования устройства необходимо решить две задачи:

– обеспечить безопасность самого устройства;
– обеспечить безопасность хранящихся данных в устройстве.

Первое требование будет реализовано с помощью начального пин-кода, который будет требоваться при начальном включении устройства.

Для безопасного хранения паролей пользователя будет реализована программная шифровка данных. Сохраненные пароли будут проходить через алгоритм шифровки, а после будут записаны в микросхему EEPROM памяти.

Таким образом, алгоритм взаимодействия устройства будет выглядеть следующим образом (рисунок 2).

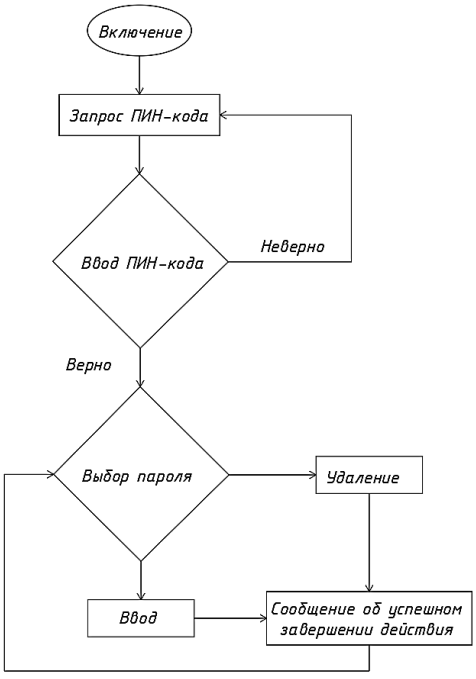

Рисунок 2 – Алгоритм работы устройства

Запись паролей на устройство осуществляется посредством подключения устройства к компьютеру, на котором установлено программное обеспечение (ПО) для взаимодействия с устройством. Также установленное ПО позволяет импортировать записанные в устройство пароли в виде текстового документа. Также возможна полное стирание памяти устройства.

Таким образом, устройство осуществляет контроль за хранимыми данными. Программное обеспечение позволяет взаимодействовать и управлять хранимыми данными на устройстве.

Заключение. Предложен метод хранения паролей, альтернативный традиционному (запись паролей на бумажный носитель).

Выполнен анализ схемы электрической структурной. Описан алгоритм взаимодействия пользователя с устройством. Определен алгоритм записи, удаления, импорта данных с помощью программного обеспечения для персонального компьютера.

Список литературы

1. *Kaspersky Daily [Электронный ресурс] / Пароли, XXI век – Режим доступа : https://www.kaspersky.ru/blog/paroli-xxi-vek/744/. – Дата доступа : 27.03.2022.*

2. *Интернет-технологии [Электронный ресурс] / Хранение паролей: как правильно хранить – Режим доступа : https://www.internet-technologies.ru/articles/newbie/hranenie-paroley-kak-ne-sovershit-oshibku.html. – Дата доступа : 27.03.2022.*

UDC 621.377.6.037

DEVICE FOR STORING PASSWORD AND LOGIN VIA USB INTERFASE

Navumchik P.A.

Minsk radioengineering college, Minsk, Republic of Belarus

Boiko D.A. – Lecturer of the cycle commission of Design and manufacture of radioelectronic facilities

Annotation. Designing a device for secure storage of user passwords in the modern world. When using the device, a significant increase in the level of security is expected when creating new passwords, their subsequent storage, as well as fast and secure entry when authorizing a user in personal and corporate services.

Keywords. security, microcontroller, password