Этот девайс позволяет решить задачу безопасного хранения логинов и паролей от ваших интернет-сервисов. Простой гаджет, подключается к USB и хранит в памяти до 255 пар логин-пароль. Абсолютно недоступно для посторонних. Владелец же, нажав несколько кнопок, легко войдет в любой из своих аккаунтов. Ничего не нужно записывать на бумажке или в файле, который легко может украсть злоумышленник. Наконец-то вы сможете использовать разные, безопасные пароли и регулярно их менять.

Николай Хлюпин (RA4NAL)
г. Киров

Аппаратный менеджер паролей

Успехи всемирной информатизации и цифровизации огромны и неоспоримы. Но бурный рост объема персональных цифровых данных имеет далеко идущие последствия. К сожалению, подавляющее большинство интернет-пользователей полагают, что их данные не могут быть интересны злоумышленникам. Тем временем практически любой компьютер, смартфон или планшет может быть использован преступниками, например, для рассылки спама, организации DDoS атак или отправки фишинговых ссылок через мессенджеры и электронную почту.

Кроме того, похищение персональных данных – обычно прелюдия к краже денег. Например, достаточно знать номер вашей карты Сбербанка (а это не секретная информация) и получить доступ к привязанному к ней телефону или даже просто перехватывать SMS с одноразовыми паролями, что технически вполне реально. И все, "накопленное непосильным трудом" уйдет в неизвестном направлении. Доказать вы потом ничего не сможете. Номер карты ваш, телефон тоже ваш. Какие могут быть претензии к банку? Что это – халатность или злой умысел?..

Но не будем пытаться решать глобальные проблемы. Давайте для начала подумаем, где хранить пароли от множества своих интернет-ресурсов. Если говорить о длине и сложности паролей, то большинство пользователей не привыкли себя утруждать. Наиболее распространенные пароли практически не меняются с годами – "123456", "qwerty", "пароль", "111111", год рождения, марка машины и т.п.

Варианты, содержащие строки "qaz" и "wsx", немногим лучше. Эти буквы удобно располагаются под левой рукой на клавиатуре, поэтому их комбинации злоумышленники проверяют в первую очередь. Так же, как слова любви и бранные выражения.

Вредоносные утилиты из арсенала киберпреступников способны за короткое время проверить тысячи паролей, чтобы получить доступ к данным жертвы. Программы для подбора ключевых сочетаний работают по спискам, которые включают в себя большинство популярных последовательностей. Поэтому уповать на безопасность таких паролей нельзя.

Но сложные и разные пароли трудны для запоминания, поэтому большая часть пользователей выбирает небезопасный способ хранения паролей, которые не может запомнить. Они записывают комбинации символов в блокнот или на листок бумаги, лежащий рядом с компьютером. Кто-то доверяет пароли браузерам, а кто-то сохраняет их в отдельном файле на компьютере.

Итак, где же хранить свои секретные и регулярно обновляемые пароли от множества интернет-ресурсов. В голове? Вряд ли поместятся. Или доверить облачному сервису, который взломают если не сегодня, то завтра обязательно. А может быть понадеяться на бесплатный программный менеджер паролей. Нет, есть более надежное и интересное решение.

Идею подсказала статья в [1]. Автор назвал себя "ge0gr4f". Он подробно описал методику изготовления и программирования аппаратного менеджера паролей. Это такой небольшой девайс, который подключается к USB порту компьютера, представляется USB клавиатурой и хранит в себе логины и пароли от всех ваших аккаунтов. Работает с любой операционной системой, не требует установки драйверов и дополнительного программного обеспечения.

Идея интересная, но ее реализация мне не понравилась. Вот список всего необходимого для изготовления этого гаджета. Основа устройства – отладочная плата IskraJSmini на базе контроллера STM32F411CEU6. Кроме нее нужны OLED дисплей, RFID/NFC модуль, транспортная карта "Единый", работающая по технологии RFID, card-reader SD, SD карта для него, ИК приемник и пульт ДУ. Не слишком ли сложно? Транспортная карта – не проблема для жителя Москвы, а где ее взять в провинции? Да и стоимость этого комплекта получается немалой. За эти деньги наверняка можно приобрести фирменный аппаратный токен, если не боитесь проблем с дополнительным ПО и универсальностью.

Hardware

Мы пойдем другим путем. Из всего списка необходимого оборудования оставим только OLED дисплей с диагональю 1,3″, разрешением 128x64, интерфейсом I2C, а в качестве основы используем доступную и дешевую отладочную плату на базе микроконтроллера STM32F103C8T6. На Aliexpress

суммарная стоимость такой платы и дисплея около 5 USD.

Еще, разумеется, потребуется корпус с кнопками. Я использовал корпус от старой трубки стационарного беспроводного телефона. От стационарных телефонов сейчас многие отказываются, так что такая трубка вполне может валяться в вашем “ящике с хламом”. Или найдется у кого-либо из знакомых. На клавиатуре должно быть не менее 16 кнопок. Желательно, чтобы на них были стандартные телефонные символы – цифры от 1 до 9, *, 0, #, UP, DOWN, OK и ESC (Отмена). Размер окна под дисплей должен соответствовать размеру используемого OLED дисплея.

Срок службы кнопок из проводящей резины, как показал опыт эксплуатации ПДУ от телевизоров, не очень большой. Кроме того, в пультах ДУ для резиновых кнопок используются контактные площадки из какого-то материала, похожего на графит. Сделать что-то подобное на самодельной плате проблематично, а с медью ничего хорошего не получится. Поэтому желательно использовать механические кнопки. На том же Aliexpress их выбор достаточно велик.

Плата моего аппаратного менеджера паролей выглядит вот так (см. **рис. 1-2**).

Принципиальная схема аппаратного менеджера паролей приведена на **рис. 3**.

Как видите, все предельно просто, ничего лишнего. Резистор R1 нужен для подключения и отключения USB, R2 и R3 – подтягивающие резисторы шины I2C. Шина работает с тактовой частотой 400 кГц, поэтому номинал этих резисторов выбран несколько меньше обычно используемого. Динамик HA1 – штатный разговорный от телефонной трубки. Он используется для озвучивания нажатия клавиш. Громкость определяется номиналом R4. Если звук не нужен, динамик можно не подключать. Конденсатор C1 блокировочный по питанию. В принципе, все работает и без него, установил так, на всякий случай.

Индикатор HG1 OLED с диагональю 1,3″, разрешением 128x64, контроллером SH1106 и интерфейсом I2C (4 pin). Я использовал именно такой тип. На Aliexpress есть близкие по параметрам аналоги с контроллером SSD1306, с возможностью выбора интерфейса – SPI или I2C, с диагональю 0,96″. Но я их не тестировал, возможно, для корректной работы индикатора с контроллером SSD1306 потребуется небольшая доработка программы. Так что рекомендую использовать именно SH1106, I2C, 4 pin, 1,3″, 128x64. Тем более, что он один из самых дешевых. Тип контроллера лучше уточнить перед

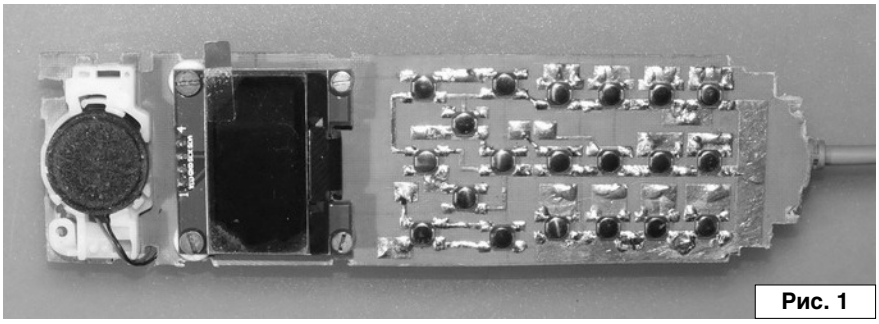

Рис. 1

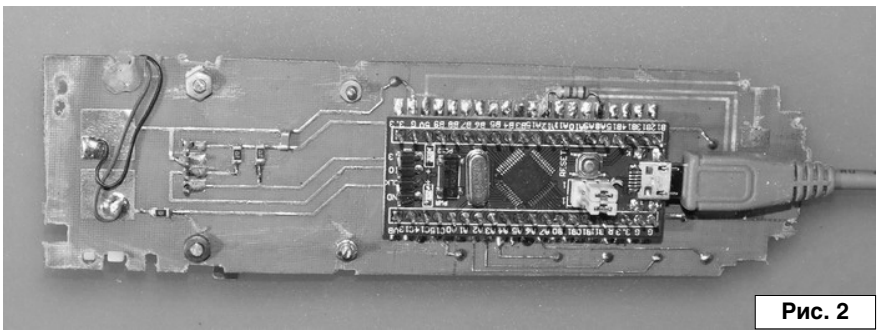

Рис. 2

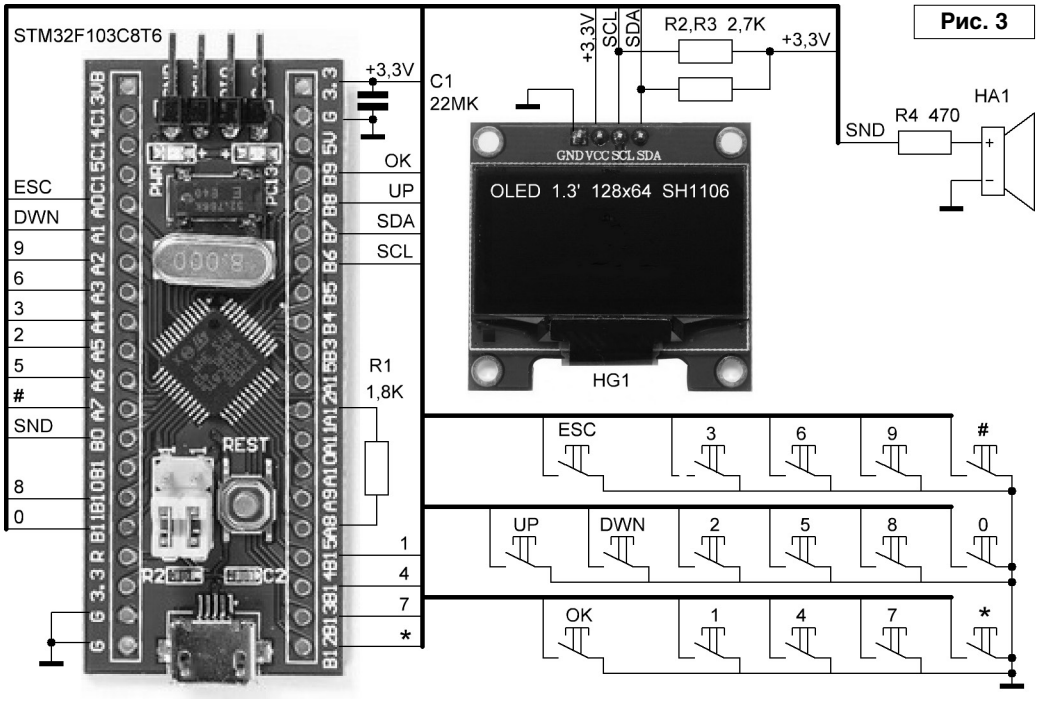

Рис. 3

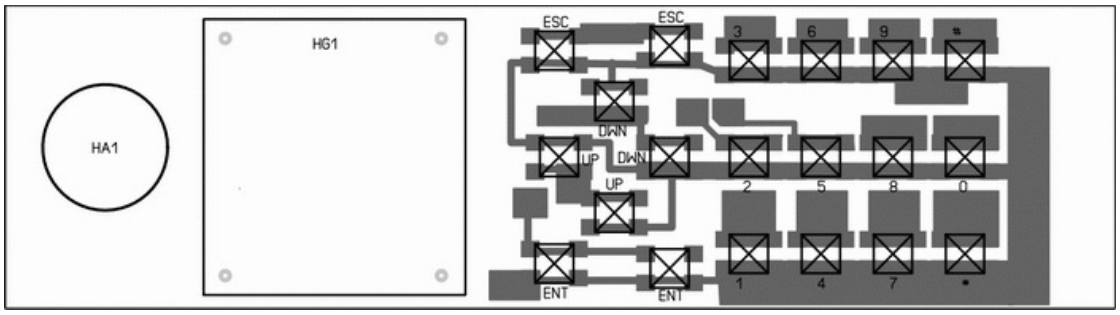

Рис. 4

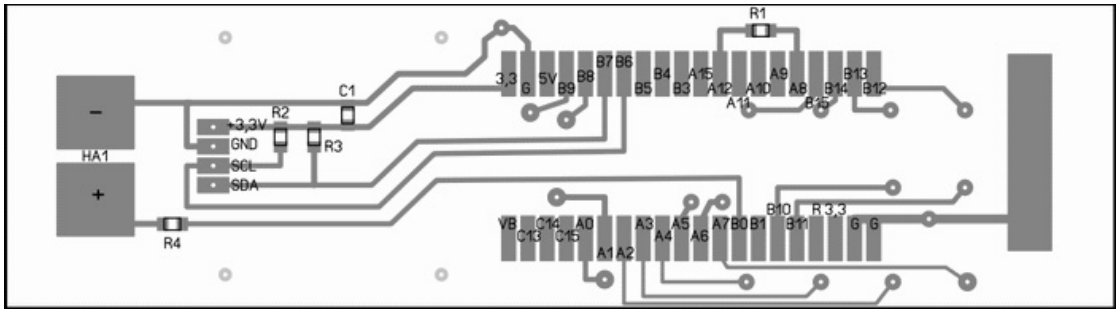

Рис. 5

заказом дисплея у продавца. 0,96'' применять не рекомендую – очень уж мелкие символы, неудобно пользоваться.

Отладочная плата, как я уже писал, на основе контроллера STM32F103C8T6. Самая дешевая и распространенная из серии STM32. Кнопки я не стал объединять в матрицу, как это обычно делается. Выводов у контроллера достаточно, зачем усложнять плату и программу.

Все это собрано на двухсторонней печатной плате, изготовленной лазерно-утюжным методом (см. **рис. 4-5**). На одной стороне смонтированы кнопки и индикатор, на другой – плата с контроллером и дискретные компоненты. На плате установлен разъем microUSB для подключения кабеля от компьютера, я рекомендую включить в него кабель и больше не дергать. А плату разместить в корпусе так, чтобы кабель был зафиксирован. Очень уж ненадежный этот microUSB, ведь корпус вы держите в руках. Если пропадет контакт в разъеме во время записи во FLASH память, очень велика вероятность потери информации. Так что лучше подключать и отключать, при необходимости, второй конец кабеля от компьютера.

Чертеж платы привожу "для сведения", так как размеры платы (147x40 мм) и конфигурация дорожек определяются корпусом. Вряд ли у вас он будет точно такой же, как у меня. Если использовать не отладочную плату, а просто микроконтроллер STM32F103C8T6, размеры печатной платы можно значительно уменьшить и смонтировать менеджер паролей в корпусе от старого кнопочного сотового телефона. Главное, чтобы дисплей поместился в корпусе. Кроме контроллера нужен кварц на 8 МГц и стабилизатор на 3,3 В. Установленный на отладочной плате кварц на 32,768 кГц для работы программы не нужен.

Литература, ссылки

1. ge0gr4f. Творческая ISKRA. - Хакер, 2018, №5(230), с. 36,37.

Продолжение в №8/2019

Аппаратный менеджер паролей

Николай Хлюпин (RA4NAL)
г. Киров

Продолжение. Начало в №7/2019

Software

Теперь о том, как все это работает. Вы подключаете аппаратный менеджер паролей к USB порту компьютера и... ничего не происходит. Если это делаете не вы, то у непосвященного злоумышленника создается впечатление, что это какой-то сломанный телефон. Для включения устройства посвященный пользователь должен кратковременно нажать кнопку “Отбой” – на клавиатуре справа вверху (в дальнейшем я буду называть ее “ESC”), см. **рис. 6**. Затем он должен вслепую ввести PIN код. PIN код может содержать от 0 до 18 цифр и задается пользователем. Как это делается, рассмотрим позже.

На ввод каждой цифры отводится около 4 сек. Если вы ошиблись, нужно подождать 5 секунд и повторить ввод кода с начала. Я не стал закладывать какого-либо ограничения количества попыток ввода. А вдруг ваш ребенок решит понажимать кнопочки на папиной игрушке... Единственное, что я сделал, это ограничил время на ввод PIN кода. Нужно ввести правильный код в течение одной минуты. Не успели? Ничего страшного, нажмите “ESC” и в вашем распоряжении еще одна минута. Но эту особенность нужно знать.

Если вы используете не год своего рождения и не 123, то, учитывая, что на проверку одной комбинации нужно около 10 сек, подбор кода даже из 4 цифр потребует около 14 часов (5000*10/3600 = 13,9). Автоматизировать этот процесс нельзя, разве что сконструировать специальный аппаратный девайс для именно этой конкретной цели.

Если вы считаете, что кто-то будет целый день с утра до вечера нажимать кнопки ради ваших секретов, думаю, вы себе льстите. Да и за это время вы успеете поменять по крайней мере наиболее важные из своих паролей и взлом потеряет смысл. Если секреты того стоят, можно использовать код не из 4, а из 18 цифр. Посчитайте сами, сколько потребуется времени на его подбор.

Примерно через 5 сек после ввода корректного PIN кода устройство включается и определяется компьютером, как HID клавиатура. На дисплей выводится список ваших аккаунтов, в базе данных можно хранить до 255 аккаунтов. Каждый аккаунт имеет три параметра – Name, Login и Password. Name – это имя, под которым аккаунт отображается на дисплее. Login и Password – понятно, что. Все это пользователь имеет возможность редактировать, как это делается, рассмотрим позже.

Имя и пароль могут содержать до 18 символов, а логин – до 28. Почему именно 18? Во-первых, этого вполне достаточно, а во-вторых, именно столько помещается в одну строку на дисплее при выбранном размере шрифта. А почему на логин остается именно 28 – догадайтесь сами. Поддерживаются строчные и прописные буквы латинского алфавита, цифры от 0 до 9 и некоторые специальные символы.

Итак, на дисплее список ваших аккаунтов. Его можно прокручивать по кругу кнопками “Вверх” и “Вниз” (в дальнейшем я буду называть их “UP” и “DOWN”). Скорость прокручивания зависит от времени удержания кнопки, вначале по одной строке, затем по 5. Между первым и последним аккаунтом отображается пустая строка. Список аккаунтов на дисплее отсортирован в алфавитном порядке. Если быть точным, то не совсем по алфавиту, а по ASCII коду первых четырех символов. Выбираем нужный аккаунт.

Открываем в браузере страницу входа в этот аккаунт, устанавливаем курсор в поле ввода логина и нажимаем на аппаратном менеджере паролей кнопку с цифрой “1”. Поле логина заполнилось нужной информацией. Нажимаем кнопку “2”, это имитирует нажатие клавиши “Tab” на основной клавиатуре компьютера. Курсор переходит в поле ввода пароля. Нажимаем кнопку “3”, поле пароля заполняется. Остается нажать “4” или “6”, что имитирует нажатие “Enter” на клавиатуре. Если логин вводить не нужно, нажимаем сразу “3”, затем “4” или “6”. Все, вы вошли в свой аккаунт.

Рис. 6

Если был включен CapsLock, он автоматически выключится, а вот о раскладке клавиатуры нужно позаботиться самому. Автоматизировать эту операцию сложно без потери совместимости с любой операционной системой. Русские символы не поддерживаются опять же из-за обеспечения совместимости.

Если не нажимать больше ни одну из кнопок, через 4 минуты яркость дисплея уменьшается. При последующем нажатии любой кнопки она восстанавливается. Если нажать и удерживать в течение 4 сек кнопку “ESC”, менеджер паролей выключается. Контроллер переходит в режим “STOP”, дисплей гасится, USB отключается, вторая клавиатура исчезает из диспетчера устройств. Для того, чтобы она вновь появилась там, необходимо будет повторить процедуру включения и ввода PIN кода. В выключенном состоянии менеджер паролей практически ничего не потребляет. Потребляет ток только светодиод “Power” и стабилизатор напряжения 3,3 В на плате. Это 2 мА максимум.

Теперь о том, как создать и отредактировать базу данных. Я постарался не изобретать ничего нового, а сделать интерфейс максимально похожим на интерфейс кнопочного сотового телефона при наборе SMS. Для входа в меню нажимаем клавишу “OK” (левая верхняя на клавиатуре). Рассмотрим подробно пункты меню, их всего 4. Зачем все усложнять и запутывать, добавляя функции, которыми вы никогда не будете пользоваться.

Edit account

Редактирование. Вначале редактируем имя, под которым аккаунт отображается на дисплее. Если нажать и удерживать кнопку, например “2”, будут последовательно перебираться символы abcABC2. На кнопке “3” – defDEF3 и т.д. Выбираем нужный символ, и он становится в конец строки в позицию курсора. Так можно ввести до 18 символов. Специальные символы распределены между кнопками “1”, “0” и “*”. Удаление ошибочно набранного символа – кнопка “UP”, отмена удаления – кнопка “DOWN”. Закончив ввод строки нажимаем “OK”, а если передумали редактировать – “ESC”.

Теперь редактируем логин. Все аналогично, только в строке может быть до 28 символов. После ввода первых 18 символов строка сдвигается влево и на экране отображается символ “<”. После ввода логина переходим к редактированию пароля. Его длина может быть до 18 символов. Хочу обратить внимание на одно “know how”.

При нажатии на кнопку “#” на дисплей выводится случайный символ. Он выбирается аппаратно, таймер-счетчик в контроллере непрерывно считает и переполняется 1000 раз в секунду. В момент нажатия на кнопку состояние счетчика запоминается в специальном регистре. По сохраненному коду и выбирается вводимый символ. Момент нажатия на кнопку никак не связан с работой счетчика, так что это чисто случайное, а не псевдослучайное число. Если введенный символ не понравился, сотрите его кнопкой “UP” и повторите ввод.

Заканчиваем редактирование нажатием кнопки “OK”, если вы что-то изменили, поступит запрос на сохранение сделанных изменений. “OK” – подтверждение сохранения, “ESC” – отмена.

New account

Создание нового аккаунта. Все аналогично предыдущему пункту, только создается новый аккаунт, а не редактируется существующий. Если вы уже заняли всю память, будет выведено соответствующее предупреждение, придется удалить какой-либо из ранее созданных аккаунтов. Я не стал делать специального пункта меню для удаления аккаунта. Для удаления достаточно в режиме редактирования очистить строку с именем, так меньше вероятность удалить что-то по ошибке. Для большей секретности можно также очистить логин и пароль, но это не обязательно. Если строка с именем пустая, аккаунт не будет отображаться в списке.

Порядок создания аккаунтов не имеет значения, при выводе на дисплей список сортируется в алфавитном порядке (по ASCII коду первых четырех символов). Соответственно, если вы хотите, чтобы аккаунт был в начале списка, его имя должно начинаться с пробела, знака восклицания, цифры, букв A, B или других символов с кодом 0x20...0x40 из начала таблицы ASCII. И наоборот, имя аккаунта из конца списка должно начинаться со строчной буквы x, y, z.

Edit PIN

Редактирование PIN кода, который используется для включения менеджера паролей. Все аналогично предыдущим пунктам, но вводятся только цифры. Можно ввести до 18 цифр. Если строку ввода оставить пустой, менеджер паролей будет включаться через 4 сек после кратковременного нажатия кнопки “ESC”, без ввода PIN кода. Это на случай, если у вас нет секретов от семьи.

Delete All

Опасный, но необходимый пункт. После соответствующего предупреждения нажатие кнопки “0” полностью очистит базу данных без возможности ее восстановления. Нажатие любой другой кнопки отменит операцию. Это на случай, если вы решите подарить это устройство кому-либо. Могут, конечно, быть на то и другие причины...

Фирма STM гарантирует 10000 циклов записи во FLASH память контроллеров STM32. Даже при регулярной смене паролей лет на 10 этого лимита хватит. Но все же без необходимости не нужно лишний раз модифицировать базу данных.

Окончание в №9/2019

Аппаратный менеджер паролей

Николай Хлюпин (RA4NAL)
г. Киров

Окончание. Начало в №№7-8/2019

Программирование STM32F103C8T6

Теперь о том, как запрограммировать контроллер. В системной памяти STM32 есть Bootloader, который позволяет запрограммировать контроллер через интерфейс USART с помощью USB-USART переходника. Выбор таких переходников на Aliexpress достаточно велик, но приобретать следует такой, который позволяет выбрать логические уровни 5 В или 3,3 В. На плате переходника для этой цели предусмотрен джампер.

Подключаем RX и TX выходы к соответствующим выводам USART1 микроконтроллера. RX переходника подключаем к TX микроконтроллера (A9). TX переходника подключаем к RX микроконтроллера (A10). USB-USART имеет выход питания 3,3 В, поэтому питание на плату можно подать с него. Джампером нужно выбрать напряжение питания 3,3 В.

Чтобы перевести микроконтроллер в режим программирования, надо установить на выводе BOOT0 логическую единицу, а на BOOT1 – логический ноль. Нужное положение перемычек показано на **рис. 7**.

После нажатия кнопки Reset или отключения и подключения питания, микроконтроллер переходит в режим программирования. Программное обеспечение для прошивки – Flash Loader Demonstrator можно скачать с сайта http://st.com/, для скачивания потребуется регистрация.

Запускаем Flash Loader Demonstrator, выбираем порт, с которым будем работать и устанавливаем его параметры (**рис. 8**). Нажимаем Next, если появится сообщение о невозможности установить связь, нажимаем кнопку “RESET” на плате и еще раз экранную кнопку Next.

После этого последовательно появятся две чисто информационные странички, на которых нужно просто нажать Next. Наконец, появляется страница, на которой нужно выбрать файл прошивки, поставить указанные на рисунке точки и, конечно же, снова нажать Next (**рис. 9**).

После завершения прошивки возвращаем перемычку на плате в исходное положение и нажимаем RESET или выключаем и включаем питание.

Важное замечание. Если на странице, где мы выбирали файл прошивки, сделать вот такие установки (**рис. 10**), будет установлена защита от считывания прошивки, а значит, – и всей вашей базы данных.

После этого никто, в том числе и вы сами, не сможет считать базу данных из памяти контроллера. Однако я рекомендую устанавливать защиту прошивки только в том случае, если вам действительно есть что скрывать и есть риск, что менеджер паролей может попасть в руки продвинутых злоумышленников. Операция необратимая, при снятии защиты вся память контроллера стирается.

По крайней мере, так утверждает фирма STM. Хотя хакерам и удалось найти уязвимости в защите, их эксплуатация подразумевает наличие достаточного количества времени и высокого уровня интеллекта у взломщика. С тем и с другим у нас сейчас не очень... Да и я при разработке программы постарался принять меры, усложняющие несанкционированный доступ к памяти.

Вы должны сделать что-то очень плохое, или (и) быть очень состоятельным человеком, чтобы для кого-то имело смысл заниматься взломом вашего менеджера паролей. Первый вариант я категорически отвергаю, а во втором случае вы найдете способ защитить свои персональные данные.

Дистанционно получить доступ к менеджеру паролей невозможно в принципе. Для взлома нужен физический доступ к устройству, причем в лабораторных условиях и на достаточно продолжительное время. Единственное слабое звено – клавиатурные шпионы. Но на них есть антивирусы, в конце концов, при вводе пароля с обычной клавиатуры вы точно так же рискуете.

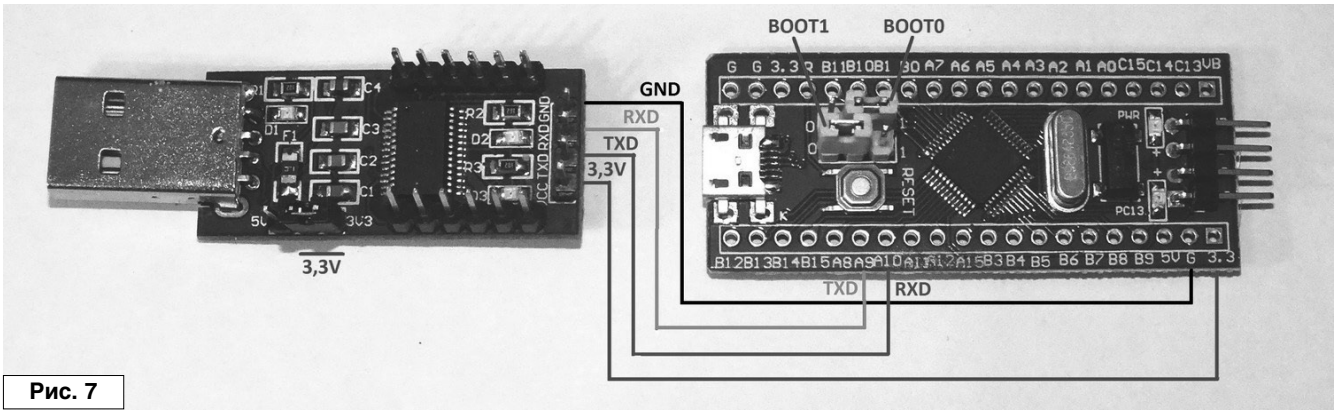

Рис. 7

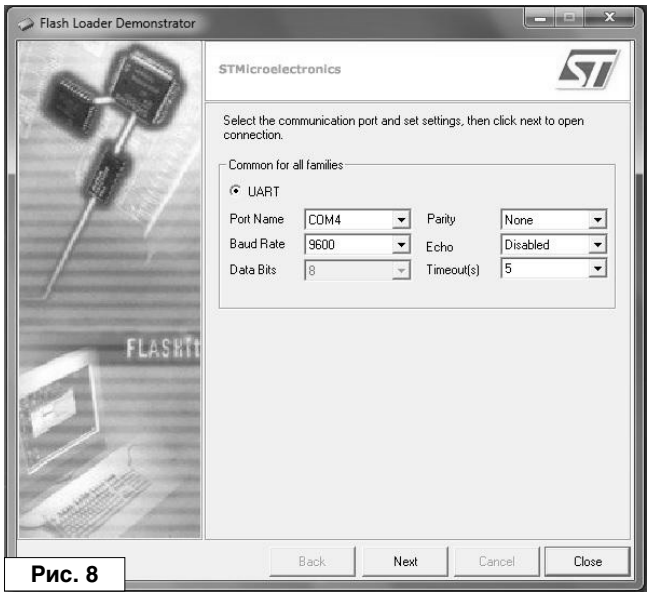

Рис. 8

Рис. 9

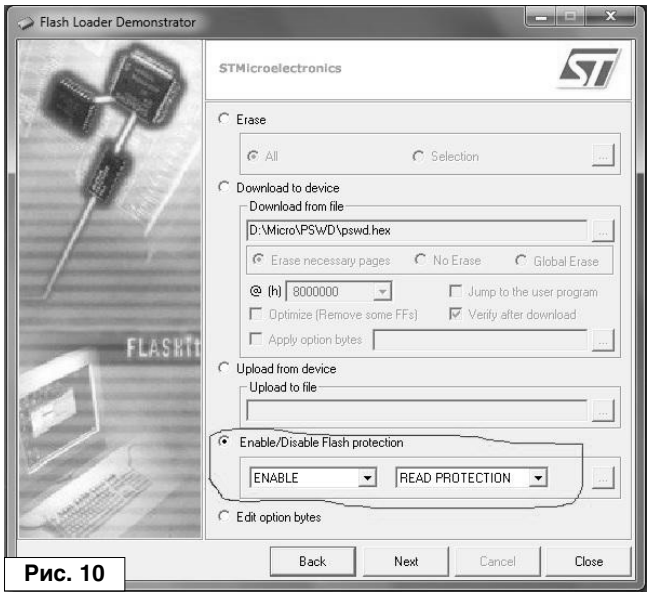

Рис. 10

Если есть сомнения в надежности электроники, можно сделать резервную копию базы данных паролей. Во-первых, если не установлена защита от чтения, можно сохранить память микроконтроллера в файл. Для этого в программе Flash Loader Demonstrator выбирайте операцию “Upload from device”. HEX файл можно хранить на сменном носителе или зашифровать.

Во-вторых, если открыть текстовый редактор, а в аппаратном менеджере паролей выбрать нужный аккаунт, затем нажать последовательно кнопки 1, 2, 3, 4, в строке напечатаются логин и пароль. Имя и комментарии добавьте вручную. Это можно проделать сразу при создании или редактировании аккаунта. Полученный текстовый файл сохраните на сменном носителе или распечатайте.

Программировать STM32 можно также с помощью программатора ST-Link. Его можно приобрести на Aliexpress по цене менее 3 USD. Не буду подробно описывать работу с ним, информации на эту тему много.

Три источника и три составные части марксизма программы

Программу я писал в среде Keil uVision 5. Официальная бесплатная версия от Keil имеет ограничение на размер кода 32 кбайта. Я уложился в этот лимит, программа занимает 25 кбайт в памяти контроллера.

Разумеется, проект создавался не на пустом месте. Во-первых, я использовал информацию из статьи трех пермских авторов в [2]. VID и PID взяты из этой же статьи, от USB клавиатуры Texas Instruments, так что проект не для коммерческого использования.

Во-вторых, Application note AN2824 “STM32F10xxx I2C optimized examples” от STMicroelectronics [3]. И, наконец, библиотеку OLED дисплея SSD1306 by Tilen Majerle, которую доработал для STM32f10x Alexander Lutsai [4]. Я, в свою очередь, чуть-чуть подправил ее для SH1106.

Все остальное пришлось писать самому. Не иронизируйте, господа программисты, но на этот проект я потратил около полугода. Начинал я его летом, когда масса других дел и забот. Кроме того, это всего лишь мой второй проект на STM32, поэтому много времени ушло на изучение datasheet и поиск информации. Ну и возраст, наконец...

Этот проект отличается от всех других моих разработок, описания которых размещены на сайте [5]. Обычно я выкладываю как прошивку, так и исходные тексты программ. В данном случае только прошивка доступна для скачивания. Дело не в жадности или амбициях.

Есть такой класс хакерских атак – BadUSB. BadUSB предназначен для доставки и исполнения на компьютере вредоносного кода. HID-атака – это разновидность BadUSB. Ее суть сводится к тому, что в USB порт вставляется хакерский девайс, эмулирующий устройство ввода, чаще всего клавиатуру. ОС без всяких проверок принимает его команды.

Преимуществ HID-атаки перед атакой вручную несколько: это скорость, незаметность и автоматизация. Все необходимые действия выполнятся быстрее, чем набирать то же на клавиатуре и без опечаток. Подключить к USB порту миниатюрное устройство можно за пару секунд. Это гораздо проще и удобнее, чем садиться за чужую клавиатуру и поминутно оглядываться через плечо. Малогабаритный девайс легко спрятать и пронести через охрану даже на режимный объект.

В общем, эмуляция клавиатуры – опасный инструмент. Вот я и не хочу облегчать жизнь людям с недобрыми намерениями. Немного доработав под свои нужды программу менеджера паролей, можно выдать его за сотовый телефон, а на самом деле использовать, как инструмент хакера. Конечно, можно найти информацию, как сделать BadUSB и в других источниках, но не будем оказывать дополнительную помощь хакерам. Деньги нужно зарабатывать, а не получать.

Информация предназначена для радиолюбителей, автор не несет ответственности за любой возможный вред, причиненный этими материалами.

Видео работы устройства можно посмотреть на авторской страничке на канале YouTube [6] по адресу:
https://www.youtube.com/watch?v=DmlalInC9NY

Рисунок печатной платы (файл pswris.zip) и прошивку микроконтроллера (файл pswprg.zip) вы можете загрузить с сайта нашего журнала:
http://www.radioliga.com (раздел “Программы”)
а также с сайта автора [7-8].

Литература, ссылки

2. Андрей Шаронов, Валерий Володин, Равиль Бикметов. Реализация профиля клавиатуры USB HID на плате STM32 Mini. - Современная электроника, 2014, №1, с. 52.
3. STMicroelectronics. Application note AN2824 “STM32F10xxx I2C optimized examples”.
4. Lutsai Alexander. Библиотека OLED дисплея SSD1306 для STM32 микроконтроллеров. - https://lutsai.ru/stm32/2016/03/08/Library-ssd1306-stm32.html
5. Радиолюбительские конструкции RA4NAL - http://ra4nal.lanstek.ru/index.shtml, http://ra4nal.qrz.ru/index.shtml
6. https://www.youtube.com/channel/UC5R9Ubmh_cb2ppCDvwv7jGw
7. Плата в Sprint Layout и схема в sPlan - http://ra4nal.lanstek.ru/dop/pswris.zip
8. Прошивка STM32F103C8T6 ver. 02/12/2018 - http://ra4nal.lanstek.ru/dop/pswprg.zip