

Контроллер электронного замка с датчиком отпечатков пальцев

Павел Редькин (г. Ульяновск)

Предлагаемое устройство представляет собой встраиваемый электронный модуль, на основе которого возможно быстрое построение биометрического замка, электронного «вахтёра», или иной системы сигнализации, контроля и разграничения доступа. В качестве идентифицирующей информации для управления доступом в устройстве используются отпечатки пальцев.

Принцип действия и основные характеристики

Контроллер замка выполнен на базе недорогого миниатюрного промышленного сканера отпечатков пальцев GT-511C3 фирмы ADH Technology [1], [2], подключённого к цифровому блоку управления, который обеспечивает обмен со сканером командами и данными, интерфейс с пользователем, а также выдачу управляющих сигналов на внешнее исполнительное устройство. В качестве последнего предполагается использование электропривода замка или какой-либо системы сигнализации.

Контроллер работает следующим образом. В ждущем режиме на его выход подключения внешнего исполнительного устройства постоянно выдан пассивный логический уровень, соответствующий состоянию «заперто» («доступ запрещён»). После приложения к поверхности сканера подушечки пальца руки и последующего нажатия на любую из кнопок управления контроллер производит идентификацию. Приложенный палец сравнивается с каждым из хранящихся в энергонезависимой памяти отпечатков пальцев пользователей, обладающих правами доступа. В случае обнаружения совпадения на выход подключения внешнего исполнительного устройства кратковременно выдаётся активный логический уровень, что соответствует состоянию «отперто» («доступ разрешён»).

Помимо обычных пользователей в устройстве также определён пользователь, обладающий правами администратора. Он может настраивать и записывать в энергонезависимую память рабочие параметры устройства: выбирать активный логический уровень выхода (низкий или высокий), задавать значение времени удержания

активного уровня при разрешении доступа, получать информацию об общем количестве хранимых в памяти отпечатков пальцев и об уникальных идентификационных номерах (ID) этих отпечатков, задавать или отменять индивидуально для каждого из этих отпечатков право доступа. Для этого не требуется никаких дополнительных программных и аппаратных средств, кроме органов управления и индикации контроллера.

Также администратор имеет возможность производить снятие (регистрацию) отпечатков пальцев у новых пользователей и добавлять их в базу сканера, удалять из этой базы содержащиеся там отпечатки, выгружать (копировать) всю базу из сканера или загружать её в сканер, например, из другого сканера аналогичного типа, а также выполнять другие сервисные операции с устройством. Перечисленные действия возможны только при подключении к контроллеру через интерфейс управления и настройки персонального компьютера (ПК), работающего в режиме простого терминала с соответствующим программным обеспечением. Активация интерфейса, то есть перевод контроллера в режим управления и настройки, защищена двухуровневой системой контроля администрирования. В качестве идентифицирующей информации она использует отпечатки двух пальцев администратора (администраторов). Заметим, что снятие (регистрация) отпечатков технически осуществляется встроенными аппаратными средствами самого сканера.

Контроллер имеет следующие основные характеристики:

- первичное постоянное напряжение питания – 8...25 В;
- потребляемый ток в ждущем режиме (состояние «заперто»/«отперто») без

учёта тока внешнего исполнительного устройства – 195 и 210 мА соответственно;

- количество каналов подключения внешних исполнительных устройств – 1;
- тип выхода – твёрдотельное реле с полной гальванической развязкой от цепей управления, максимальное коммутируемое напряжение – 60 В (AC/DC), максимальный коммутируемый ток – 1 А (DC), 2 А (AC);
- интерфейс управления и настройки – RS-232, 8-N-1, 9600 бит/с.

Входящий в состав устройства сканер отпечатков пальцев GT-511C3 имеет следующие характеристики:

- технология исполнения сканера – оптическая (на отражение);
- тип сканера – оптический сенсор с эффективными размерами 14 × 12,5 мм, матрица – 216 × 240 пикселей, разрешение – 450 dpi;
- вероятность ложного принятия отпечатка (пропуска незарегистрированного отпечатка) FAR (False Acceptance Rate) – менее 0,001%;
- вероятность ложного отклонения отпечатка (отклонения зарегистрированного отпечатка) FRR (False Rejection Rate) – менее 0,1%;
- угол максимального допустимого отклонения приложенной подушечки пальца от осевой линии поля сканирования при идентификации отпечатка – 30°;
- максимальное количество отпечатков, хранящихся в энергонезависимой памяти сканера – 200;
- время регистрации (снятия одного отпечатка) – менее 3 с;
- время идентификации (для базы из 200 хранящихся в памяти отпечатков) – менее 1 с;
- потребляемый ток – менее 130 мА;
- диапазон питающих напряжений – 3,3...6 В;
- рабочий температурный диапазон составляет –20...+60°C;
- размеры: 37 × 17 × 9,5 мм.

Функционирование сканера GT-511C3 осуществляется в соответствии со следующими принципами.

При снятии (регистрации) отпечатка пальца (Fingerprint) производится ста-

тический захват изображения отпечатка фиксированного размера. В результате получается так называемый образ отпечатка (Fingerprint Image) разрешением 240×216 пикселей, занимающий в памяти сканера объём 51 840 байт. Преимущество этого способа состоит в получении полного изображения без необходимости двигать палец в процессе регистрации.

Затем, согласно определённому алгоритму, из захваченного образа извлекается уникальный набор данных об отпечатке, представляющий собой так называемый шаблон (Template) отпечатка, который по команде пользователя записывается в энергонезависимую память сканера. В памяти GT-511C3 каждый полученный таким образом шаблон занимает всего 506 байт. Это преобразование производится для обеспечения секретности и уменьшения объёма памяти, необходимого для хранения образов отпечатков. Секретность достигается за счёт необратимости преобразования, то есть восстановить исходный образ из шаблона невозможно. В то же время копирование из памяти сканера и запись в неё подготовленных другим сканером шаблонов возможны.

В ходе сеанса получения доступа, после приложения пальца и подачи команды, сканер производит захват образа отпечатка пальца и формирует из него шаблон, помещаемый в оперативную память для последующего анализа и сравнения.

Затем, в зависимости от поданной команды, полученный шаблон сравнивается или с заданным шаблоном из базы сканера (команда «Верификация 1:1»), или же последовательно со всеми хранящимися в базе N шаблонами (команда «Идентификация 1:N»). Заметим, что полное побитное совпадение из-за наличия в процедуре сканирования приближений, перекосов и сдвигов изображения, ошибок аппроксимации процедуры извлечения деталей и т.п. маловероятно. В связи с этим применяется алгоритм оценки степени совпадения, в котором оно считается подтверждённым после превышения заданного порога. В сканерах семейства GT-511Cx используется алгоритм SmackFinger 3.0, выполняющийся на встроенном 32-разрядном микроконтроллере (МК) HT32F2755 с архитектурой ARM Cortex M3.

Помимо основных задач, к которым относится снятие и распознава-

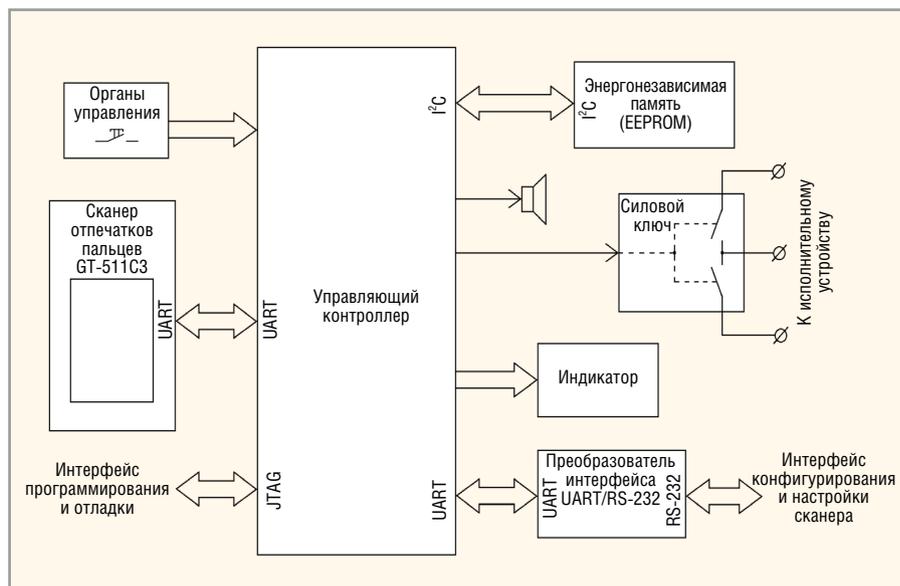


Рис. 1. Структурная схема контроллера замка

ние отпечатков, GT-511C3 имеет набор дополнительных функций, облегчающих построение на его основе систем контроля доступа. Это: загрузка в сканер и выгрузка из него во внешнее устройство как всей базы, так и отдельных шаблонов, выгрузка образа отпечатка непосредственно после его захвата, проверка наличия приложенного к сканеру пальца и т.п.

СХЕМЫ И КОНСТРУКЦИЯ УСТРОЙСТВА

Структурная схема контроллера замка приведена на рисунке 1.

Обмен командами и данными с внешними устройствами, а также конфигурирование и настройка сканера GT-511C3 осуществляется через стандартный интерфейс UART. В нашем случае в качестве внешнего устройства для сканера выступает управляющий контроллер, который, в свою очередь, подключается к внешним по отношению к нему устройствам через свой второй интерфейс UART, снабжённый преобразователем уровней UART/RS-232. В режиме администрирования сканера управляющий контроллер является полностью прозрачным для сигналов UART, то есть обеспечивает сквозное двустороннее их прохождение между двумя своими интерфейсами и беспрепятственное управление сканером. Во всех остальных режимах контроллер блокирует управление сканером, обеспечивая тем самым необходимый уровень секретности замка.

Управляющий контроллер выполнен на базе 32-разрядного МК LPC2129. Для программирования и отлад-

ки встроенной управляющей программы МК используется интерфейс JTAG. В качестве органов управления используются механические кнопки, подключённые к цифровым линиям ввода-вывода МК.

Индикатор, предназначенный для отображения режимов и операций устройства, представляет собой малогабаритный двухстрочный символьный ЖКИ, совместимый со стандартом HD44780. В составе устройства имеется также пьезоизлучатель, генерирующий звуковые сигналы высокого тона (успешное завершение операции, получение доступа и т.п.) и низкого (неудачное завершение операции, отказ в доступе и т.п.).

В качестве силового ключа управления внешним исполнительным устройством используется твердотельное реле с гальванической развязкой цепи управления, пригодное для управления нагрузками, питающимися постоянным или переменным током.

Внешняя многократно программируемая энергонезависимая память EEPROM, подключённая к управляющему контроллеру по шине I²C, используется для хранения задаваемых пользователем текущих настроек устройства: активного логического уровня выхода, значения временного интервала выдачи активного уровня при разрешении доступа, признаков разрешения/запрещения доступа для каждого из хранимых в устройстве отпечатков. Необходимо заметить, что наличие в составе устройства внешней памяти EEPROM не обязательно, однако при её отсутствии все вышеперечисленные поль-

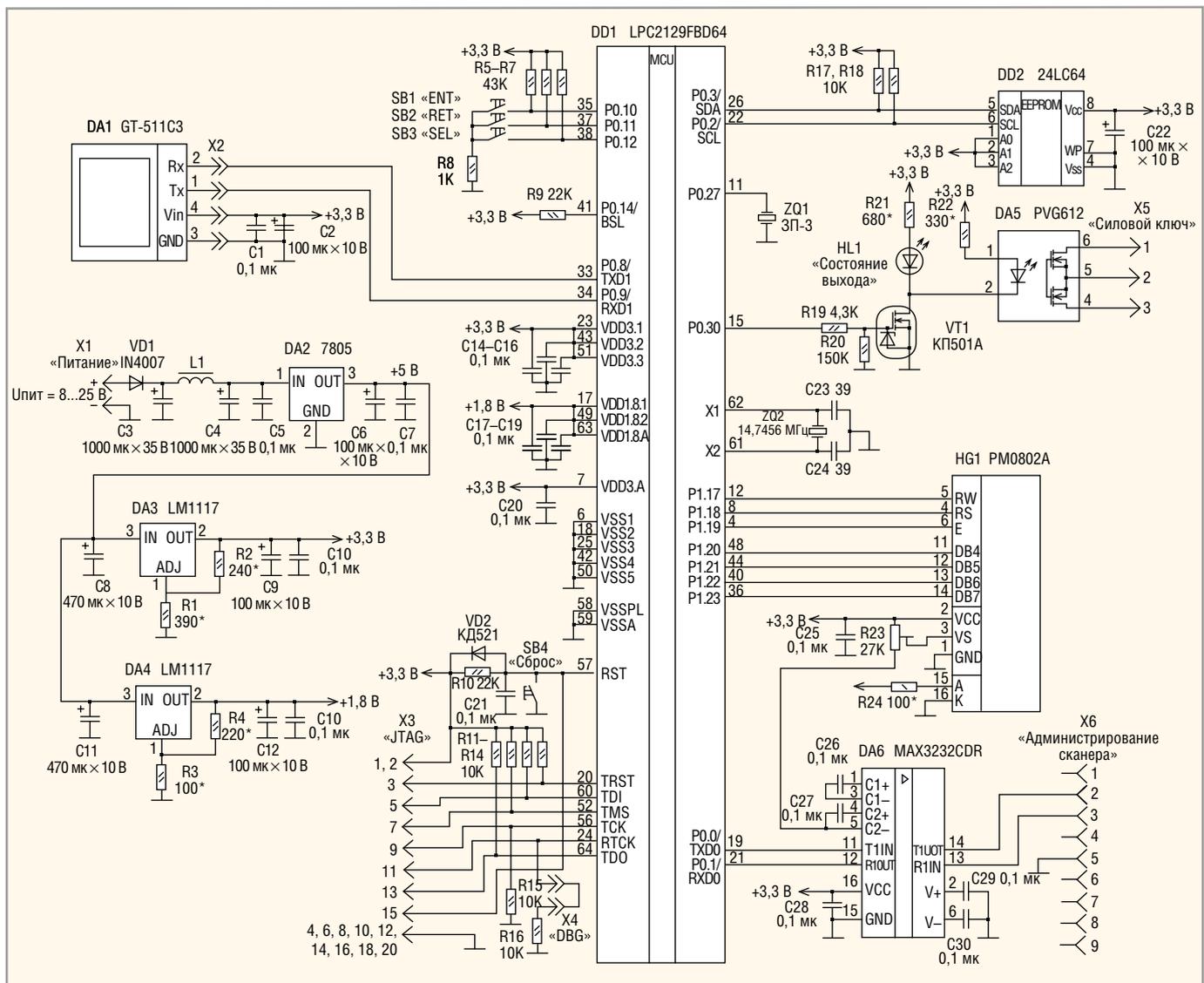


Рис. 2. Принципиальная схема контроллера замка

зовательские настройки станут недоступны для задания и будут автоматически заменяться константами по умолчанию.

Принципиальная схема контроллера замка приведена на рисунке 2.

Для питания устройства в его составе имеются три стабилизатора напряжения. Первичный с выходным напряжением +5 В (DA2) предназначен для дополнительной стабилизации по питанию и расширения диапазона входных питающих напряжений устройства. Два вторичных (DA3, DA4) вырабатывают необходимые для питания МК напряжения +3,3 и +1,8 В соответственно. Заметим, что для построения управляющего контроллера можно без каких-либо переделок использовать готовую отладочную плату LPC-H2129 производства OLIMEX [5]. Подключить её можно с помощью имеющихся на плате разъёмов (за исключением вывода 5 микросхемы DA6).

Устройство содержит четыре кнопки (SB1-SB4). В общем случае кнопка SB3 «SEL» предназначена для выбора операций и команд в пользовательском интерфейсе. Кнопка SB1 «ENT» – для запуска выбранной операции или команды. SB2 «RET» – для отмены выбранной операции или команды и возврата на предыдущий уровень меню. Кнопка SB4 «Сброс» предназначена для «горячего» сброса МК при отладке устройства.

Ёмкость использованной в устройстве микросхемы I2C EEPROM DD2 24LC64 (64 Кбит) выбрана в расчёте на введение в будущем дополнительных функций и для данной версии избыточна.

В зависимости от типа нагрузки возможны различные варианты её подключения, которые показаны на рисунке 3. Они отличаются сопротивлением открытого ключа, для варианта а – не превышающего 0,6 Ом [6], для

варианта б – 0,25 Ом и для варианта в – 0,15 Ом.

Для защиты от взлома контроллера замка необходимо сделать невозможным доступ извне, прежде всего, к цепям подключения внешнего исполнительного устройства, а также к шине UART между МК DD1 и сканером DA1. В авторском варианте контроллер замка выполнен в металлическом литом корпусе размерами 210 × 110 × 20 мм со съёмной задней панелью, на которую выведены разъёмы питания, силового ключа и администрирования сканера. На переднюю панель вынесены кнопки SB1-SB3, индикатор HG1, светодиод HL1 «Состояние выхода», несколько отверстий для пьезоизлучателя и ниша сенсора сканера DA1. Разъём «JTAG», переключатель «DBG» и кнопка «Сброс», используемые при программировании МК, смонтированы непосредственно на плате и извне недоступны.

Внешний вид собранного контроллера замка показан на рисунке 4.

ВСТРОЕННАЯ УПРАВЛЯЮЩАЯ ПРОГРАММА

Встроенная управляющая программа МК позволяет управляющему контроллеру обмениваться командами и данными со сканером отпечатков, конфигурировать и настраивать сканер, управлять режимами и настраивать всё устройство, а также его интерфейс, с пользователями и администраторами.

Устройство может функционировать в трёх режимах:

- пользовательский (ждущий) режим, устанавливающийся по умолчанию после включения питания;
- режим администрирования (с входом только из пользовательского режима по предъявлению отпечатка пальца администратора);
- режим администрирования сканера (с входом только из режима администрирования по предъявлению отпечатка другого пальца администратора).

После включения питания устройство выводит на экран ЖКИ заставку с названием и номером версии встроенного ПО («FPsensor Vx.x»), после чего начинается тестирование сканера отпечатков и памяти EEPROM. Сначала, путём подачи контрольной команды и ожидания в течение заданного времени ответа, программа устанавливает наличие сканера. Далее анализ корректности ответного пакета позволяет проверить исправность сканера при его наличии. В случае отсутствия или некорректного подтверждения от сканера программа выводит на ЖКИ сообщение «Ошибка n GT-511C», где n – номер ошибки (0 – отсутствие, 1 – неисправность сканера), и передаёт управление в бесконечный пустой цикл. При исправном сканере программа кратковременно включает встроенный светодиод его подсветки.

После успешного завершения тестирования сканера программа переходит к тестированию микросхемы EEPROM. Это запись в EEPROM контрольного значения с последующей проверкой правильности записи. В случае ошибки на ЖКИ кратковременно выдаётся сообщение «Ошибка n I2C», где n – номер ошибки (0 – отсутствие ИС памяти, 1 – неисправность EEPROM). Так как отсутствие или неисправность EEPROM для устройства не является фатальным, программа в дальнейшем выполняет

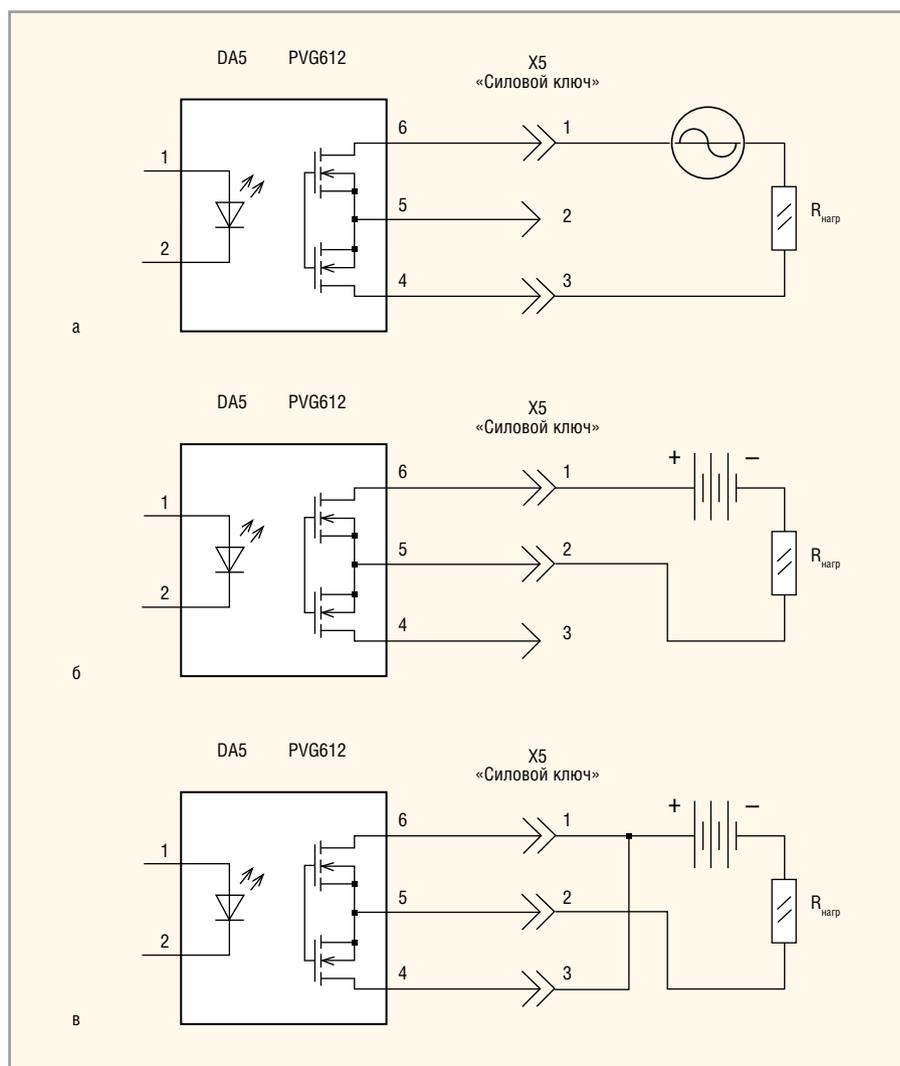


Рис. 3. Варианты подключения нагрузки:

а – управление нагрузкой, питающейся переменным или постоянным током;

б – управление нагрузкой, питающейся постоянным током (вариант 1);

в – управление нагрузкой, питающейся постоянным током (вариант 2)



Рис. 4. Внешний вид контроллера замка: а – лицевая сторона; б – оборотная сторона

функционально ограниченную версию без использования EEPROM.

Далее устройство переходит в пользовательский режим, индицируемый заставкой «Жду палец» на ЖКИ. Выход подключения внешнего исполнительного устройства при этом всё время

находится в пассивном уровне («Заперто»). Для получения пользовательского доступа (открытия замка) пользователь должен приложить подушечку пальца к внешней поверхности матрицы сканера и однократно нажать на любую из кнопок: «ENT», «RET» или «SEL». После

этого сканер произведёт захват отпечатка пальца, обработает его, сделает анализ и сравнит со всеми хранимыми в базе шаблонами. В случае совпадения будет выдано сообщение «Доступ откр. XXX», где XXX – десятичный уникальный номер (ID) шаблона из базы сканера (ID = 1...199 для GT-511C3, ID = 1...19 для GT-511C1). При этом выход подключения внешнего исполнительного устройства на заданный интервал времени перейдёт в активный уровень («Отперто»). После истечения этого интервала устройство вернётся в пользовательский режим. При отсутствии совпадений будет выдано сообщение «Отказ в доступе», а выход подключения внешнего исполнительного устройства останется в пассивном уровне. В случае если после нажатия кнопки сканер не обнаружит приложенного пальца или палец окажется приложен неплотно, будет кратковременно выдано сообщение «Палец не приложен», после чего устройство вернётся в пользовательский режим.

Если палец к сканеру приложит администратор (шаблон его отпечатка хранится в базе под номером ID = 0, т.н. «мастер-палец»), то устройство перейдёт в режим администрирования, кратковременно выдав заставку «Мастер-режим». Затем на ЖКИ будет отображено меню администратора. Выход подключения внешнего исполнительного устройства при этом останется в пассивном уровне, то есть «мастер-палец» замок не откроет.

Меню администратора состоит из следующих строк-опций:

- строка «Акт. ур.» – задание активного уровня подключения внешнего исполнительного устройства;
- строка «Интерв.» – задание значения временного интервала выдачи активного уровня при разрешении доступа;
- строка «Кол. отп» – получение информации об общем количестве хранимых в памяти сканера шаблонов отпечатков;
- строка «Ном. отп» – получение информации о наличии в базе сканера шаблона с заданным ID, а также задание/отмена права доступа для этого шаблона;
- строка «Упр. GT» – переход в режим администрирования сканера, состоящий в активации прямого управления сканером, которое ведётся с подключённого через интерфейс RS-232 ПК.

Кольцевой перебор пунктов меню осуществляется с помощью кнопки «SEL», а выбранный пункт отмечается курсором «>». В каждый момент времени на ЖКИ отображаются только две смежные строки. Курсором отмечается верхняя. Для выбора отмеченного курсором пункта меню нужно нажать кнопку «ENT». Выход из режима администрирования возможен только после сброса МК (кнопка «Сброс») или отключения питания: корректная активация изменённых администратором параметров возможна только после сброса МК управляющего контроллера. Нажатие кнопки «RET» возвращает администратора в верхний ярус меню.

При исправной EEPROM в опции «Акт. ур.» возможно задание активного уровня подключения внешнего исполнительного устройства. Значение действующего уровня отображается на ЖКИ в виде надписей «Низкий» или «Высокий», помеченных значком «*». Для выбора уровня следует нажать кнопку «SEL». При этом каждое новое выбранное значение уже не помечается значком «*», пока не будет записано в EEPROM нажатием кнопки «ENT». Выбранное значение не воспринимается устройством как действующее, если оно не записано в EEPROM.

Аналогичным образом, выбрав опцию «Интерв.», можно задать и записать в EEPROM значение временного интервала выдачи активного уровня при разрешении доступа. Диапазон интервала составляет 1...15 с с дискретностью 1 с.

Выбрав опцию «Ном. отп», можно получить информацию о наличии в базе сканера шаблона с заданным номером ID. Требуемый идентификатор выбирается циклическим перебором при помощи кнопки «SEL» в диапазоне 0...199. Текущий идентификатор при этом отображается на ЖКИ в формате «ID=XXX». Символ «+» справа от числа означает наличие шаблона в базе, а «-» – его отсутствие. Справа от индикатора наличия/отсутствия шаблона отображается признак разрешения доступа для этого шаблона: «+», если доступ разрешён и «-», если запрещён. Для изменения значения признака на противоположное необходимо однократно нажать кнопку «ENT». При этом в EEPROM будет записано новое значение. Заметим, что возможна ситуация, когда шаблон отпечатка с ID в базе имеется, но доступ для него запрещён. В этом случае при попытке получения

доступа в пользовательском режиме на ЖКИ будет выдано сообщение «Отказ в доступе -» (если шаблон в базе отсутствует, то на дисплей будет выведено сообщение «Отказ в доступе» без знака «-»). Для шаблона «мастер-палец» с ID = 0 вне зависимости от значения признака пользовательский доступ всегда запрещён.

При отсутствии или неисправности EEPROM задание активного уровня подключения внешнего исполнительного устройства невозможно. Этот уровень задаётся по умолчанию как высокий. При этом исключается и возможность выбора значения интервала выдачи активного уровня при разрешении доступа. По умолчанию этот интервал будет равен 2 секундам. Также недоступен и выбор признака разрешения/отмены права доступа для каждого шаблона. По умолчанию для всех хранищихся в базе шаблонов, кроме ID = 0, пользовательский доступ будет разрешён.

Опция «Кол. отп» является справочной. Двойное нажатие на кнопку «ENT» выводит на ЖКИ трёхзначное число, соответствующее количеству шаблонов, хранищихся в памяти сканера. В это количество входит и «мастер-палец» с ID = 0. Наличие или отсутствие I²C EEPROM на эту опцию не влияет.

При выборе опции «Упр. GT» программа выводит на ЖКИ вопрос «Палец?», предлагая предъявить отпечаток для перехода в режим администрирования сканера. Для получения доступа в этот режим администратор должен приложить палец к сканеру и нажать на кнопку «ENT», после чего сканер произведёт захват отпечатка, обработает его и сравнит с шаблоном, хранищимся в базе под номером ID = 1 (т.н. «сканер-мастер-палец»). Далее на ЖКИ выводится заставка «Управл. GT-511C», и устройство переходит в режим прямого управления сканером. При этом все данные, поступающие извне в интерфейс RS-232, будут без изменений транслироваться программой в порт подключения сканера UART, а данные от сканера, в свою очередь, будут транслироваться в интерфейс RS-232. Таким образом, администратор получает полный контроль над сканером, в том числе возможность производить все доступные операции с базой шаблонов отпечатков. Выход из режима администрирования сканера возможен только после нажатия кнопки «Сброс» или отклю-

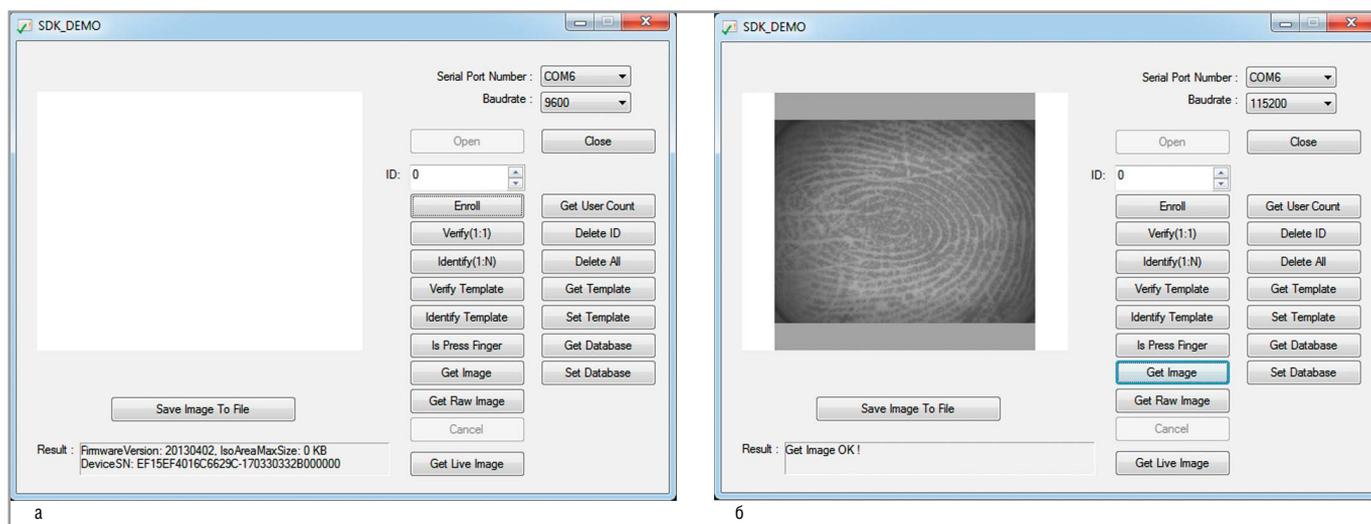


Рис. 5. Окно программы SDK_DEMO: а – после начальной инициализации («открытия») сканера GT-511C3; б – после выполнения команды захвата сканером образа отпечатка (Get Image)

чения питания. Следует заметить, что «сканер-мастер-палец» с ID = 1 может использоваться не только для административного, но и для пользовательского доступа. Заметим также, что в качестве «мастер-пальца» и «сканер-мастер-пальца» невозможно использовать один и тот же отпечаток. Кстати, порядок задания шаблона «сканер-мастер-палец» не отличается от порядка задания шаблона «мастер-палец».

Для повышения отказоустойчивости устройства, в управляющей программе используется встроенный «сторожевой» таймер МК (WDT) с длительностью тайм-аута 4 секунды. Команды перезапуска WDT содержатся в основном цикле программы, а также в её ветвях, осуществляющих обработку продолжительных по времени операций (разрешение/запрещение доступа, переходы между режимами и т.п.).

Программирование и отладка встроенной управляющей программы МК производились с помощью JTAG-адаптера-программатора JetLink 8 (это недорогой «клон» адаптера J-Link), подключаемого к разъёму X3 «JTAG» МК и к ПК хоста через порт USB. Исходный текст управляющей программы (и файл «прошивки» Flash-памяти МК), реализующей функции контроллера замка, содержатся в каталоге проекта Finger, архив которого можно скачать на сайте Soel.ru в дополнительных материалах к данной статье. Проект был подготовлен и отлажен в бесплатной версии (с ограниченным объёмом кода) интегрированной среды разработки IDE IAR Embedded Workbench for ARM V6.40.

Внимание! При программировании Flash-памяти МК на разъёме X4 «DBG»

должна быть установлена перемычка, при нормальной эксплуатации устройства – снята.

НАЛАДКА И РЕГУЛИРОВКА

Устройство практически не требует настройки или регулировки. Единственное, что может потребоваться – это установка уровня контрастности резистором R23, а яркости подсветки – резистором R24.

После выполнения всех вышеперечисленных действий можно переходить к администрированию сканера.

АДМИНИСТРИРОВАНИЕ СКАНЕРА

Администрирование, то есть настройка и конфигурирование сканера правами администратора осуществляется с помощью ПК (хоста), подключённого к контроллеру замка через интерфейс RS-232 в соответствующем режиме устройства. При этом на ПК необходимо запустить работающую под Microsoft Windows компьютерную программу поддержки сканера GT-511Cx SDK_DEMO.exe, которую можно бесплатно загрузить по ссылкам, указанным в литературе к статье [2], [3], [4]. Вид графического окна программы SDK_DEMO показан на рисунке 5.

Для установления связи между хостом и сканером необходимо предварительно в окне программы Serial Port Number выбрать номер COM-порта ПК, к которому подключён контроллер. Затем в окне Baudrate нужно задать скорость обмена (9600 бит/с) и кликнуть на кнопке Open. При этом хост передаст в сканер команду начальной инициализации («Открытие»). В ответ на неё сканер должен выдать информацию о себе,

включающую серийный номер и версию встроенного ПО. Эта информация отобразится в поле Result, как показано на рисунке 5а. В случае успешного завершения инициализации пользователю становится доступным набор операций со сканером, каждая из которых запускается кликом на соответствующей кнопке в окне программы.

Как было сказано ранее, вход в режимы администрирования и администрирования сканера в устройстве защищёны процедурой предъявления соответствующих отпечатков: «мастер-пальца» и «сканер-мастер-пальца». Однако при первом включении устройства в базе сканера нет ещё ни одного отпечатка, поэтому вход в указанные режимы невозможен. В связи с этим до начала эксплуатации устройства необходимо временно подключить сканер к хосту напрямую, минуя контроллер замка. Для этого потребуются дополнительный преобразователь уровней UART/RS-232, схема которого приведена на рисунке 6.

Автор использовал готовый преобразователь MOD-RS232 производства OLIMEX [7], выполненный по схеме, изображённой на рисунке 6.

При прямом подключении необходимо создать и записать в сканер шаблоны отпечатков пальцев администратора с ID = 0 и ID = 1. После сохранения этих шаблонов сканер можно администрировать уже в составе контроллера замка.

Рассмотрим порядок создания и записи одного шаблона отпечатка, например, с ID = 0. В поле ID программы необходимо задать уникальный идентификационный номер, под которым шаблон будет храниться в памяти ска-

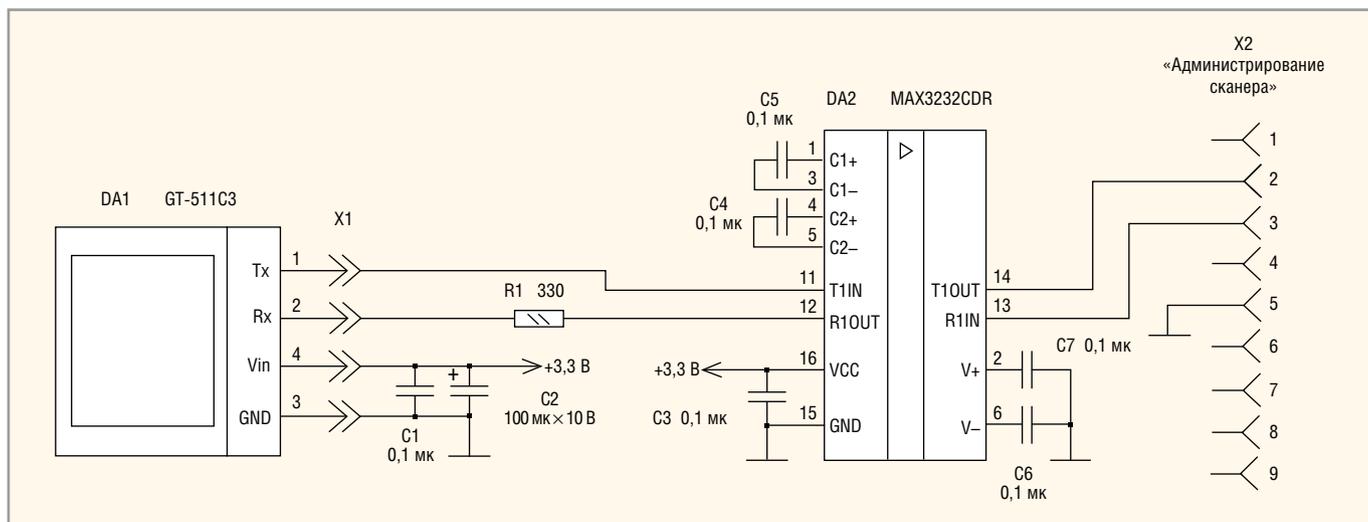


Рис. 6. Дополнительный преобразователь уровней UART/RS-232 для первичного администрирования сканера

нера. Несмотря на то, что встроенное ПО управляющего контроллера использует шаблоны с ID = 0, ID = 1 в качестве административных, а шаблоны с прочими ID – в качестве пользовательских, сам сканер никак не выделяет шаблоны 0 и 1 из общей базы. Процедура их создания ничем не отличается от прочих. Задав в поле ID значение 0, администратор кликает на кнопке запуска регистрации отпечатка Enroll, а затем трижды (каждый раз примерно на полсекунды с такими же интервалами) прикладывает свой палец к полю сенсора. Из трёх последовательно захваченных таким образом изображений отпечатков автоматически формируется шаблон. В случае успешного завершения регистрации в поле Result появится сообщение «Enroll OK (ID = 0)!». Это значит, что шаблон отпечатка с заданным ID = 0 создан и записан в энерго-независимую память сканера. В противном случае будет выдано сообщение об ошибке регистрации или об истечении времени ожидания сканера: процедуру необходимо повторить заново. Опыт эксплуатации показал, что для корректной регистрации шаблона отпечатка требуется некоторый навык.

Зарегистрировав отпечаток, можно сразу проверить реакцию сканера на его предъявление. Для этого нужно, задав соответствующее значение в поле ID, приложить палец к полю сенсора и кликнуть на кнопке команды верификации Verify [1:1]. Сканер захватит изображение отпечатка, сравнит его с шаблоном, имеющим указанный номер, и, при совпадении, выдаст сообщение «ID = 0.» (с указанием времени распознавания в мс). При несопадении сообщение будет таким:

«ID = 0: NG!». Процесс захвата, сравнения и выдачи результата при приложенном пальце будет повторяться циклически. Прервать его можно кликом на кнопке Cancel. При распознавании зарегистрированного отпечатка процедуру пополнения базы отдельным шаблоном можно считать успешно завершённой.

Если, приложив палец, вместо верификации кликнуть на кнопке команды идентификации Identify [1:N], сканер будет циклически сравнивать захваченный отпечаток со всеми шаблонами отпечатков, имеющимися в данный момент в его базе. В случае совпадения будет выдаваться сообщение «ID = 0.» (с указанием времени распознавания в мс), в случае отсутствия совпадений – «NG!».

Аналогичным образом пополняем базу шаблоном с ID = 1.

В спецификации на сканер (Data-sheet) производитель рекомендует использовать для регистрации отпечатка «лучший» образ, а для верификации и идентификации – «не самый лучший». Это, очевидно, следует понимать так: при проведении регистрации подушечка пальца должна быть чистой и содержать полную, «эталонную» картину папиллярных линий с минимальными их повреждениями. В то же время при верификации и идентификации можно и нужно предъявлять как раз загрязнённый и даже поцарапанный палец. Нужно отметить, что встроенное ПО сканера не позволяет дважды произвести регистрацию шаблона одного и того же отпечатка под разными номерами ID. Произвести повторную регистрацию шаблона отпечатка под тем же номером ID также невозможно, пока более ранний шаблон не будет удалён.

Отдельный ненужный шаблон, равно как и вся база шаблонов, может быть стёрт из памяти сканера с помощью команд Delete ID, Delete All соответственно. Отдельный шаблон или всю базу можно выгрузить из сканера в виде файлов (с расширениями .dat и .db соответственно) и загрузить в сканер с помощью команд Get Template, Set Template, Get Database, Set Database. Эти команды удобно использовать для однократного создания и последующего копирования базы, например, на объектах с несколькими электронными «вахтёрами» со сканерами одинаковой модели.

Команда Get User Count возвращает в поле Result значение общего количества шаблонов, хранящихся в данный момент в базе. Команда Is Press Finger позволяет проверить, приложен ли в данный момент палец к полю сенсора. Сканер производит проверку своими встроенными средствами. При обнаружении приложенного пальца выдаётся сообщение «Finger is pressed!». В противном случае – «Finger is not pressed!». Заметим, что указанную проверку сканер производит автоматически каждый раз перед выполнением команды верификации или идентификации.

Команды Get Image, Get Raw Image, Get Live Image, Save Image To File поддерживают операции непосредственно с образами отпечатков, в том числе с необработанными, т.н. «сырыми» (raw). Поскольку в энергонезависимой памяти сканера образы не хранятся, то их графическое отображение на экране, как показано на рисунке 5б, или выгрузка в виде графических файлов (.bmp), возможны только непосредственно после захвата, пока они

хранятся в оперативной памяти. Необходимо помнить, что при выполнении перечисленных четырёх команд через интерфейс сканера передаётся значительный объём данных. На скорости 9600 бит/с, жёстко заданной для обмена со сканером в контроллере замка, передача данных производится довольно медленно. В связи с этим, если имеется необходимость использования операций с образами отпечатков, рекомендуется временно использовать прямое подключение сканера к хосту (см. рис. 6). При этом можно задать в окне Baudrate программы SDK_DEMO более высокую скорость обмена. В ходе начальной инициализации сканера программа перенастроит интерфейс UART на новую скорость.

Команды Verify Template, Identify Template позволяют произвести верификацию и идентификацию в базе образа, не захваченного с поля сенсора, а загруженного (предъявленного) в сканер извне в виде файла.

При наличии в составе устройства микросхемы I²C EEPROM DD2 следует при первом же администрировании установить требуемые настройки

в опциях «Акт. ур.», «Интерв.» и «Ном. отп», как это описано выше. Необходимо добиться корректного отображения диапазона значений интервала выдачи активного уровня путём осуществления полного цикла перебора всех значений «по кольцу».

ЗАКЛЮЧЕНИЕ

В ходе эксплуатации не было отмечено ни одного случая ложного принятия сканером GT-511C3 отпечатка. Что же касается случаев несрабатывания по зарегистрированному отпечатку (FRR), вероятность чего производитель заявляет на уровне менее 0,1%, то их было немало. По оценке автора, величина FRR у используемого экземпляра GT-511C3 составила порядка 10...15%, что, однако, не портит хорошего впечатления от сканера. В случае несрабатывания по зарегистрированному отпечатку процедуру предъявления этого отпечатка необходимо просто повторить. Угол максимального допустимого отклонения приложенной подушечки пальца от осевой линии поля сканирования, по оценке автора, может быть гораздо больше 30°, вплоть до 90°.

Опытным путём было установлено, что даже при достаточно плотном приложении к поверхности матрицы сканера подушечки абсолютно сухого пальца довольно велика вероятность выдачи сообщения «Палец не приложен». Для надёжного детектирования приложенного пальца и перехода к процедуре его распознавания желательно предварительно чуть увлажнить его.

ЛИТЕРАТУРА

1. Fingerprint reader module. www.adh-tech.com.tw/?fingerprint-scanner,83.
2. GT-511C3 / GT-511C31. www.adh-tech.com.tw/?22,gt-511c3-gt-511c31.
3. Fingerprint Scanner – 5V TTL (GT-511C1). Documents: Datasheet, Demo Software. www.sparkfun.com/products/11836.
4. Fingerprint Scanner – TTL (GT-511C3). Documents: Datasheet, Demo Software. www.sparkfun.com/products/11792.
5. www.olimex.com/Products/ARM/NXP/LPC-H2129/.
6. www.irf.com/browse?Dy=1&Nty=1&Ntt=PVG612#tab-tab2.
7. www.olimex.com/Products/Modules/Interface/MOD-RS232/open-source-hardware. ©