RFID-системы контроля доступа с повышенным уровнем безопасности

Александр Самонин, ведущий специалист ООО «Гамма»
E-mail: micro@microchip.ua

В статье описан способ построения безопасной системы контроля доступа с применением оборудования RFID стандарта Mifare.

Самостоятельно сконструировать систему контроля доступа (СКД) сегодня не составляет труда. Во многих открытых источниках неоднократно давалась подробная информация о том, как работает СКД и как собрать собственный контролер системы. Все комплектующие находятся в свободной продаже, решение такой задачи сводится лишь к правильному соединению отдельных блоков. Работать такая система будет не хуже, чем заказанная в какой-то специализированной охранной фирме. Но, собирая ее самостоятельно, шаг за шагом разбираясь, как она устроена, разработчик получает важную информацию о том, где и для каких целей она может быть использована. Всякая система может быть надежна в силу своей простоты, но не всякая надежная система может быть безопасна. И если целью является контроль прохода в помещение и без того оборудованное видеокамерами и пультом охраны с обязательной проверкой пропусков, то Вам вполне достаточно установить СКД с применением бесконтактных меток стандарта EM Marine. Такое решение просто в реализации, к нему не выдвигается специфических требований, кроме одного: из всего множества персонала, передвигающегося по объекту, выбрать и пропустить только тех, кому разрешен доступ в это помещение. Но современное оборудование позволяет с легкостью подделать пропуск к такой системе, поэтому вряд ли ее можно позиционировать как достаточно безопасную.

Таким образом, СКД на базе карт Em Marine можно отнести к классу систем со средним уровнем защищенности. Применять такие контроллеры на серьезных объектах, требующих высокого уровня безопасности, неразумно.

Системы контроля доступа, в которых используются бесконтактные смарт-карты, по уровню защищенности выше, чем СКД на бесконтактных картах. Рассмотрим это на примере стандарта Mifare.

- Бесконтактная смарт-карта Mifare имеет память 1 Кб, разделенную на 16 секторов. Эта память доступна для чтения/записи. Доступ к каждому сектору защищается ключами, которые генерирует сам заказчик СКД. Подделать или скопировать такую карту практически невозможно.
- Использование бесконтактных карт Mifare предоставляет дополнительные возможности по организации и разграничению доступа в СКД. Например, на саму карту можно записывать права доступа и обеспечивать открывание дверей на основе той информации, которая записана на карту. Это эффективно как для территориально-распределенных объектов, так и для крупных бизнес центров.
- Доступ для конкретной группы объектов (помещений, зданий и т.п.) записывается в конкретный сектор карты Mifare. Доступ к этому сектору защищается уникальным ключом (secure sector). Дверной считыватель при считывании карты обращается к соответствующему сектору памяти (предъявляя уникальный ключ, предварительно «зашитый» в этот считыватель) и, после считывания данных из памяти карты Mifare, предоставляет доступ.
- Выдача карт доступа клиентам организуется на новом уровне. При активации карты доступа в соответствующий сектор памяти Mifare записываются данные по режиму доступа, которые защищаются ключами. Кроме того, появляется возможность изменения параметров доступа в режиме on-line, так как при предъявлении карты устройству чтения возможно не только считывание данных, но и запись информации

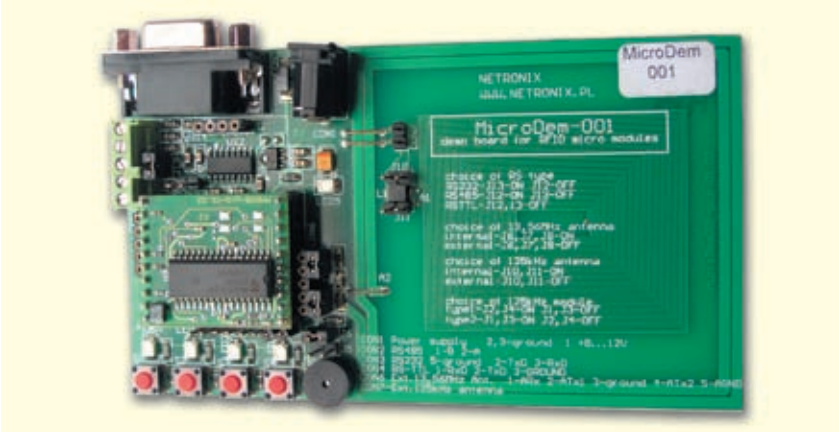

Рисунок 1 **Отладочная плата MicroDem-001 для работы с RFID считывателями Netronix**

в карту. Если требуется оперативно запретить доступ или блокировать карту, это можно сделать при очередном проходе через центральную проходную. В момент поднесения карты к считывателю будут переписаны условия доступа.

Для практического ознакомления с работой меток стандарта Mifare необходимо следующее оборудование:

- Персональный компьютер, хотя опытные программисты могут обойтись только микроконтроллером, но это менее удобно.
- Программа под названием «Framer», предоставленная для свободного пользования компанией NETRONIX.
- Reader-устройство, позволяющее работать с метками стандарта Mifare. Вариантов исполнения много, я применяю reader MM-005 от NETRONIX — законченный блок, позволяющий работать с метками посредствам простых и понятных команд совместно с отладочной платой MicroDem-001 (рис. 1).
- И сама метка стандарта Mifare. Здесь тоже есть разновидности, все сводится к желаемому объему памяти. Так как мы создаем простое устройство СКД, но имеющее высокий уровень безопасности, нам вполне подойдет пластиковая карта Mifare S50, имеющая объем памяти — 1 Кб.

Любая система, использующая пароли, не может работать без них, даже если она новая и пароль еще не задавали. В нашем случае пароль необходим для получения доступа к памяти RFID карты. Для меток, использующихся впервые, значение пароля установлено по умолчанию — *0xff 0xff 0xff 0xff 0xff 0xff.*

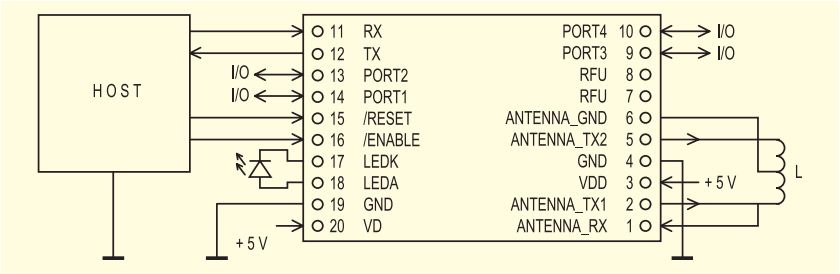

Рисунок 2 **Принципиальная схема подключения модуля MM-005**

Пример установки пароля на сектор памяти карты Mifare S50:

1. Подключите Reader к персональному компьютеру, руководствуясь схемой, приведенной на рис. 2. Запустите «Framer» и укажите ему, к какому порту подключен Reader.
2. Для проверки правильного подключения выберите команду *C_SoftVersion*. Reader вернет данные о своей версии.
3. Теперь выберите команду *C_HLReadBlock* и укажите параметры: *00 01 ff ff ff ff ff ff aa*. Это означает следующее: прочитать значение в ячейке памяти сектора 0, блока 1, используя пароль, установленный по умолчанию (это пароль класса A). Reader вернет значение, записанное в этот блок. Так как карта не использовалась ранее, то этот блок пуст.
4. Пароль для сектора 0 хранится в блоке 3 этого сектора. Поменяем его. Выберите команду *C_HLWriteBlock* и укажите параметры: *a1 a2 a3 a4 a5 a6 ff 07 80 80 ff ff ff ff ff ff 00 03 ff ff ff ff ff ff aa*. Где *a1 a2 a3 a4 a5 a6* — новый пароль, запись в сектор 0, блок 3, с использованием старого пароля — *ff ff ff ff ff ff*. Запись информации в другие блоки памяти производится по этой же команде.
5. Теперь попробуйте прочитать блок 1, как это было сделано в пункте №3. Карта не выдаст информацию, так как указан неверный пароль (мы его только что изменили).
6. Прочитайте блок 1 еще раз, но укажите новый пароль. В ответ Reader вернет значение, записанное в этот блок.

Все описанные действия проиллюстрированы на рис. 3. Описанная процедура доступна для всех 16 секторов, причем пароли у секторов могут быть абсолютно разными.

Таким образом, использование бесконтактных смарт-карт Mifare позволяет организовать систему контроля доступа на высоком уровне безопасности, значительно более высоком, чем при использовании других типов пластиковых карт.

Более детальную информацию можно получить в офисе ООО «Гамма»:
49005, г. Днепропетровск, ул. Фурманова, 15, оф. 101, тел. (0562) 36-07-92, http:// www.microchip.ua

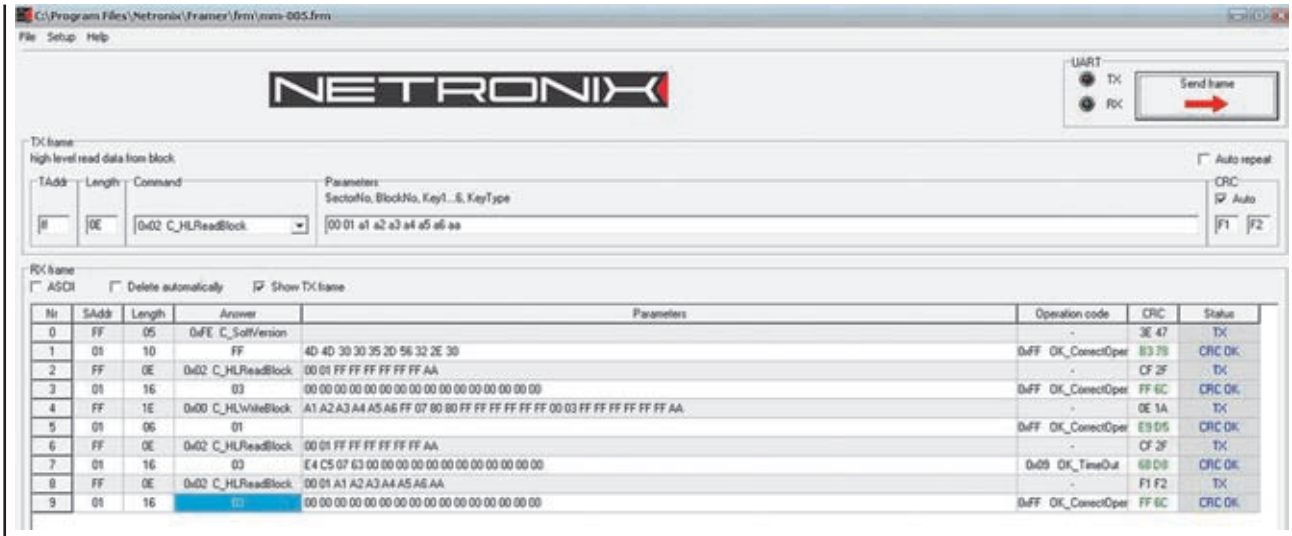

Рисунок 3 **Screenshot программы «Framer» во время выполнения команд**