Протокол OSDP для безопасной, двусторонней коммуникации между считывателем и контроллером

Алексей УМНОВ, технический консультант, компания HID Global (Россия и СНГ)

Электронные системы контроля и управления доступом существуют уже больше 30 лет. За это время технологии, конечно же, развивались, появлялись новые. Считыватели прошли эволюционный путь от устройств с магнитной полосой до считывателей Wiegand, потом появились радиочастотные считыватели близкого и дальнего радиуса действия, биометрические считыватели. В устройствах близкого радиуса действия технологии, которые лежат в основе коммуникаций между считывателем и идентификатором, менялись в сторону наибольшей защищенности.

Итак, системы контроля доступа достаточно динамично эволюционировали. Не менялся лишь интерфейс, который соединяет считыватель с контроллером или интерфейсным модулем, то есть, с тем устройством, к которому он подключен. На протяжение всего этого времени фактически устоялись два интерфейса. Интерфейс Wiegand стал наиболее популярным благодаря массовому использованию карт Wiegand. Позднее позиции устройства на рынке еще больше укрепились благодаря появлению бесконтактных радиочастотных считывателей. Разработка и массовое внедрение считывателей с магнитной полосой сделали популярным интерфейс Clock and Data. Оба интерфейса являются стандартами международной ассоциации по безопасности SIA (Security Industry Association).

Эти интерфейсы, несмотря на определенные различия, имеют очень много общего. Общее можно охарактеризовать следующими моментами. Во-первых, оба интерфейса однонаправленные. Однонаправленность заключается в том, что нет возможности отправить информацию от управляющего устройства к считывателю, - только считыватель может связаться с контроллером. Нет никакой возможности, например, опросить текущее состояние приборов, в том числе, и на предмет того, в исправном ли состоянии они находятся. Если говорить об антивандальной защите считывателей, то некоторые производители внедряли дополнительные схемы, например, использовали датчик взлома, который по отдельным проводам передавал информацию от считывателя к контроллеру. Некоторые делали так называемые контрольные посылки по тому же самому интерфейсу Wiegand, которые проходили с определенной периодичностью, чтобы контроллер «знал», что считыватель исправен и работает.

Во-вторых, оба интерфейса построены по технологии «точка-точка». То есть, интерфейс позволяет соединить только два устройства – считыватель и управляющее устройство. Если предположить ситуацию, что мы подключаем более одного считывателя, то это может привести к возникновению коллизий, когда два устройства одновременно отправят информацию, а так как нет возможности переспросить считыватели, то информация просто потеряется.

Следующий общий момент: оба интерфейса используют для передачи информации два провода. Информация в обоих случаях похожа. Это некая битная посылка. Немного отличается формат передачи посылки. В интерфейсе Wiegand единички передаются по одному проводу, а нолики по другому, то есть два инверсных провода. В интерфейсе Clock and Data и единички, и нолики идут по одному проводу, но за счет второго провода, по которому идут синхроимпульсы, происходит считывание в правильном виде передаваемой последовательности.

Еще один общий момент – отсутствие какой-либо защиты от действий злоумышленников, то есть, отсутствие кодирования информации. Временные и электрические параметры интерфейсов хорошо известны, поэтому ничто не мешает эмулировать чтение карты. Конечно, ведущие производители считывателей сегодня повысили уровень защищенности линии карта-считыватель до максимально возможного, но это все равно не дает

необходимой защищенности. Например, достаточно знать, что передается (какой номер карты, в каком виде, в каком формате информация передается от считывателя к контроллеру), узнать номер карты самого привилегированного служащего, которому разрешен доступ везде и всегда, и войти в помещение, эмулируя эту карту.

Упомянутые выше особенности интерфейсов породили необходимость появления нового протокола, который справится с имеющимися недостатками. Многие производители пытались реализовать свои интерфейсы самостоятельно, не разрабатывая какие-либо стандарты. Но продвижение таких интерфейсов на рынке становилось очень затруднительным делом, так как сейчас есть высокий спрос на гибкие системы, пользователи не хотят быть «привязанными» к считывателям и контроллерам одного производителя, покупать то или иное оборудование на постоянной основе. А, согласитесь, что в случае с частным интерфейсом заказчик жестко привязан к одному производителю.
Все это отчасти и стало главными причинами появления интерфейса OSDP (Open Supervised Device Protocol) или открытого контролируемого протокола устройств. Первоначально он являлся совместной разработкой трех компаний: HID GLOBAL, LENEL и Mercury. Его реализовали на физической основе хорошо известного интерфейса RS485, который в теории позволяет подключать до 128 устройств на одну интерфейсную линию. Реализация этого интерфейса позволила решить те проблемы, которые есть у интерфейсов Wiegand и Clock and Data.

В первую очередь, появилась возможность обеспечить обратную связь со считывателем, и по одному и тому же интерфейсу не только получать информацию от считывателя о его состоянии, номере считываемой карты, или о введенном PIN-коде, но и управлять светодиодной индикацией считывателя, выводить информацию на LCD-монитор. Причем, управление светодиодной индикацией является очень важной опцией. Как это реализовано в интерфейсах Wiegand и Clock and Data? Если на считыватель установлен двухцветный фотодиод, - красный и зеленый, - то один дополнительный провод используется для управления красным сигналом, и еще один - для управления зеленым. Когда этот провод замыкается на «землю», светодиод загорается соответствующим светом. То же самое в отношении звуковой индикации считывателя – дополнительный провод.

Протокол OSDP позволяет управлять светодиодом, поддерживающим палитру цветов вплоть до раскладки rgb. Это очень удобно для большего интерактивного взаимодействия с пользователем. Большое количество цветов дает возможность сообщить пользователю о состоянии считывателя или о состоянии системы, к которой он подключен. Например, появилась возможность информировать пользователя о такой часто возникающей ситуации, как срабатывание функции anti pass back (контроль повторного входа). Если использовать только два цвета, то один говорит о том, что доступ разрешен, другой, что доступ запрещен. Например, событие «доступ запрещен» ничем не отличатся от события «доступ запрещен», потому что запрещен повторный вход. При использовании rgb можно дополнительным цветом сообщить о других событиях. При применении старых интерфейсов для использования rgb-индикации нужно было бы добавить еще один провод. OSDP позволяет просто поменять команду, которая отправляется к считывателю, не добавляя проводов. Это очень удобно.

Использование LCD-дисплеев

До появления протокола OSDP подключение считывателя с LCD-дисплеем требовало использование дополнительного интерфейса RS232 для управления дисплеем. В случае с OSDP можно отдельными командами по этому же интерфейсу выводить информацию на дисплей. Например, если считыватель используется не только как устройство контроля и управления доступом, но и как устройство постановки-снятия с охраны, то мы можем динамично менять сообщения на дисплее в соответствии с происходящими событиями. Можно выводить индикацию о текущем времени прохода. Это очень удобно, если считыватель используется для учета рабочего времени. Так же можно вывести на дисплей

подсказки о функциях тех или иных клавиш. Таким образом, использование LCD-дисплеев становится максимально функциональным.

Сегодня OSDP утвержден как стандарт ассоциацией SIA наравне с протоколами Wiegand и Clock and Data. Немного о самом названии. OPEN и SUPERVISED – открытый и контролируемый. Открытый означает, что данный протокол открыт для всех производителей считывателей, контроллеров и ПО. Это обеспечивает решение того недостатка, который был у разработчиков собственных протоколов. OSDP – расширяемый протокол. Любой производитель может добавить свои расширения и создать тем самым дополнительную к базовой функциональность.

КОНТРОЛИРУЕМЫЙ – контролируемый протокол потому, что он двунаправленный. Контроллер, компьютер или интерфейсный модуль выступает в качестве мастер-устройства, которое производит опрос считывателя. Считыватель выступает в качестве подчиненного устройства и отвечает на направленные ему запросы.

Несколько слов об инсталляции систем, использующих OSDP. Если говорить об инсталляции на новом объекте, то применение OSDP дает существенную экономию средств при монтаже. Кабель, которым подключается считыватель, имеет меньшее количество проводов. Если для интерфейса Wiegand требуется минимум 4 провода, а при наличии управления светодиодной и звуковой индикацией, - еще три, то для OSDP достаточно 4-х. Если модернизировать объект, заменяя ранее установленные устройства на OSDP-считыватели, то можно использовать уже существующий кабель. Даже если характеристики этого кабеля не соответствуют требованиям, предъявляемым к кабелю, которым должен подключаться OSDP-считыватель, например, по волновому сопротивлению, все равно OSDP-считыватель будет работать. Это связано с еще одной особенностью OSDP: при правильном использовании (по спецификации кабеля) протокол позволяет подключить считыватель на расстоянии до 1200 м от контроллера, а Wiegand – на расстоянии до 152 м. Установленный на расстоянии 152 м от контроллера OSDP-считыватель будет работать даже при несоответствии спецификации кабеля.

Физическая основа OSDP - RS485. Этот протокол дифференциальный, или разностный, то есть информация передается по двум линиям A и B таким образом, что осуществляется защита от помех. Дифференциальное преимущество состоит в том, что если идет помеха, и она меняет сигнал в одной из линий, то она же меняет сигнал и во второй линии, но разница между ними останется постоянной.

Защищенность

До недавнего времени слабой стороной OSDP было отсутствие стандартизированной системы защиты при обмене сообщениями. Не было никакого шифрования. Но внедрение стандартизированного протокола SCP позволила решить этот вопрос. При установке соединения с использованием SCP-протокола два устройства должны быть взаимно аутентифицированы, то есть доверять друг другу. Для этого используется набор ключей. В случае если во время обмена информацией обнаруживается какая-то ошибка, то коммуникационная сессия немедленно прерывается, и сессионные ключи, которые использовались, уничтожаются. Такая сессия может быть прервана любой из сторон с помощью принудительного превышения времени ответа (TIME OUT) или посылкой неверного сообщения MAC. Если контроллер «подозревает», что кто-то вклинился на линию, то он прерывает процесс коммуникации.

Сегодня этот протокол поддерживают компании HID GLOBAL, HONEYWELL и LENEL. Протоколу около двух лет, а в СКУД – это очень короткий срок для полномасштабного внедрения новых технологий. Упомянутые в статье преимущества протокола OSDP вселяют надежду, что со временем этот интерфейс будет поддерживаться многими производителями.