

## M&M!-платформа для защищенных мобильных систем

Д. Ю. Счастный

Закрытое акционерное общество "ОКБ САПР", Москва, Россия

*Изложены варианты использования модема в устройстве M&M! (МАРШ! и модем). Рассмотрены примеры применения этого устройства в различных системах.*

*Ключевые слова:* M&M!, МАРШ!, модем.

Идея устройства M&M! (МАРШ! и модем) была озвучена в середине 2012 г. [1—3]. Кратко напомним ее суть: для обеспечения комфортной и в то же время безопасной работы мобильных пользователей предлагалось в изделие МАРШ! добавить модем в качестве неотъемлемого аппаратного компонента. Схема устройства показана на рисунке.

Добавление модема позволило упростить использование СОДС МАРШ! (сетевые настройки резидентной ОС оставались постоянными и не требовали перенастройки при каждом сеансе работы) и обеспечить мобильность пользователей (устройство стало не зависимым от провайдеров сети). На тот момент обеспечение связи для СОДС МАРШ! казалось основным и единственным вариантом использования модема. Но прошедшие четыре года показали, что мы ошибались. Добавление модема к микроконтроллеру, памяти, криптоблоку и USB-каналу привело к качественно новым возможностям использования устройства.

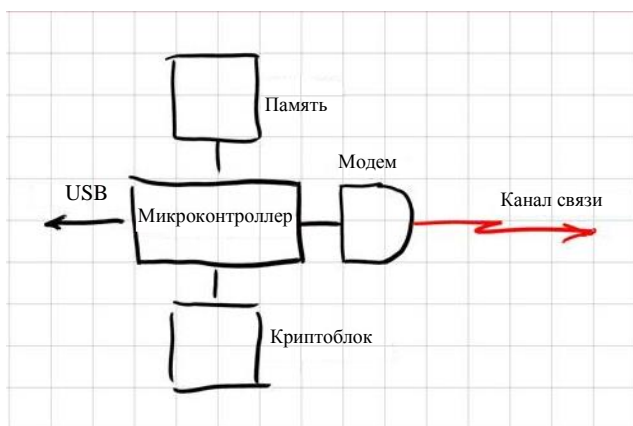


Схема устройства M&M!

Счастный Дмитрий Юрьевич, заместитель генерального директора.

E-mail: DimaS@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

© Счастный Д. Ю., 2016

Во-первых, работа модема контролируется активным микроконтроллером. Появляется возможность как управлять установлением сетевых соединений, так и осуществлять мониторинг всех данных, проходящих через устройство.

Во-вторых, наличие собственного криптоблока позволяет осуществлять различные криптографические преобразования проходящих через устройство данных, а также взаимную криптографическую аутентификацию устройства и ответной стороны. При этом ключи могут храниться в устройстве и быть недоступными ни со стороны компьютера, ни со стороны сети.

В-третьих, микроконтроллер может самостоятельно устанавливать связь и осуществлять прием или передачу данных на заранее определенный сервер.

В-четвертых, наличие памяти, доступной как из компьютера, так и из устройства, позволяет обеспечивать передачу файлов данных в режиме почтового ящика: приложение в компьютере кладет файл данных в эту память, как на обычный диск, а микроконтроллер передает этот файл на заранее определенный сервер.

Все вышеперечисленные функции осуществляются внутри устройства на собственном микроконтроллере без создания нагрузки на центральный процессор компьютера, к которому подключено устройство. Кроме того, код, исполняющийся внутри устройства, не подвержен несанкционированному изменению и не может быть заражен вирусами. Код пишется на Си. Для микроконтроллера разработаны высокоуровневые библиотеки для работы с модемом и прочей периферией.

Таким образом, устройство M&M! может быть использовано в качестве платформы для решения самых различных задач. К последним относятся сбор и передача параметров с различных датчиков в территориально-распределенных системах (например, датчиков уровня паводковых вод или датчиков учета расхода тепла, газа или света). Подобные датчики установлены во множестве мест, в том числе труднодоступных. В таком случае сбор

параметров превращается в продолжительный процесс. Естественным выходом является модификация датчиков с тем, чтобы они могли самостоятельно передавать данные. Можно переразводить плату, добавлять туда модем, встраивать систему защиты, переписывать код. Можно же использовать M&M! в режиме работы почтового ящика, подключив его к датчику по USB-каналу, и незначительно модифицировать код. Похожим образом можно использовать M&M! и в фискальных целях, соединив с кассовыми аппаратами и добавив функцию подписания данных перед отправкой на сервер микропроцессором устройства.

Еще одним вариантом применения M&M! может быть обеспечение гарантированной защищенной доставки данных именно на тот сервер, на который они должны быть доставлены после обработки на компьютере. В этом случае в момент установления соединения с сервером микропроцессор устройства проводит взаимную криптографическую аутентификацию с сервером и в случае положительного результата устанавливается соединение. Опять-таки важно отметить, что повлиять на результат этого процесса программное

обеспечение, функционирующее в компьютере, никак не может.

Такие варианты построения систем можно придумывать до бесконечности. Например, можно создать аппаратный фаервол, позволяющий пользователям посещать строго определенный набор сайтов из некоторого списка. В результате с помощью таких служебных модемов организации смогут экономить на трафике. При этом M&M! сможет самостоятельно получать списки с разрешенными сайтами с сервера компании и актуализировать их после проверки под ними подписи.

Добавление модема в MARCH! действительно качественно расширило возможности применения устройства для построения различных защищенных систем.

#### Литература

1. Коняевский В. А. ДБО — как сделать это безопасным. Часть II // Информационная безопасность. — М., 2012. № 3. С. 8—9.
2. Съёмный носитель информации. Патент на полезную модель № 102139. 10.02.2011, бюл. № 4.
3. Съёмный носитель информации с безопасным управлением доступом. Патент на полезную модель № 123571. 27.12.2012, бюл. № 36.

## M&M! as the foundation for safe mobile systems

*D. Yu. Schastny*

Closed Joint Stock Company "OKB SAPR", Moscow, Russia

*The article is about variants of the modem on board the M&M! device (the MARCH! and the modem) use and variants of this combined device in different systems use.*

*Keywords:* M&M!, MARCH!, modem.

Bibliography — 3 references.

*Received June 26, 2016*