УДК 621.38(06) Электроника.

С.П.СКОРОБОГАТОВ
Кембриджский университет, Великобритания

ЗАЩИТА СОВРЕМЕННЫХ МИКРОКОНТРОЛЛЕРОВ ОТ КОПИРОВАНИЯ

Рассмотрены возможности современных микроконтроллеров по защите памяти программ от несанкционированного копирования. Показано, что массовые модели контроллеров не обеспечивают надежной защиты информации.

При разработке современных электронных приборов широко используются микроконтроллеры (МК), работающие в соответствии с программой, помещенной во внутреннюю память. Для защиты программного обеспечения разработчики МК предусматривают специальные меры по предотвращению несанкционированного копирования.

С точки зрения уровня защиты информации все МК могут быть разделены на две группы – обычные и защищенные. Защищенные МК разработаны для приложений, требующих повышенного уровня безопасности информации, таких, как банковское и медицинское обслуживание, военное оборудование и т.п. Они используют различные уровни доступа и защиты данных не только на выходе кристалла, но и на уровне его внутренней структуры с использованием кодирования информации. Преодоление защиты таких МК требует использования очень сложного и дорогого оборудования и зачастую не оправдано экономически.

Обычные МК, как правило, так же содержат средства защиты информации, однако у разработчиков устройств на основе таких контроллеров не должно быть иллюзий по поводу их эффективности. На сайтах Интернет регулярно появляется информация о методах «вскрытия» содержимого различных МК.

Существующие методы преодоления защиты информации обычных МК разделяются на две группы – инвазивные и неинвазивные. Инвазивные методы требуют вскрытия корпуса МК с последующим воздействием на кристалл лазерных или ионных пучков и/или использования микропробников. Неинвазивные методы основаны на анализе внешних электрических сигналов с целью извлечения необходимой информации. Процедура преодоления защиты зависит от типа программной памяти МК.

В МК с масочным ПЗУ программ доступ к его содержимому запрещается производителем на стадии изготовления. Однако этот запрет может быть преодолен, если МК содержит программу тестирования содержимо-

 ISBN 5-7262-0354-2. НАУЧНАЯ СЕССИЯ МИФИ-2001. Том 1.

го ПЗУ после изготовления. Обнаружить ее достаточно трудно, и самым быстрым способом доступа к содержимому ПЗУ является вскрытие корпуса и считывание информации оптическими методами.

В МК с однократно программируемым ПЗУ на основе ячеек памяти (ЯП) с ультрафиолетовым (УФ) стиранием пользователь может установить бит защиты на стадии программирования. Однако, даже если это сделано, остается возможность использования как инвазивных, так и неинвазивных методов считывания информации. Инвазивные методы основаны на УФ облучении определенных частей кристалла или на разрушении цепи защиты под микроскопом. Неинвазивные методы используют подачу различных электрических сигналов на МК, чтобы перевести внутреннюю схему защиты в неактивное состояние.

Другой способ заключается в контроле мощности потребления во время операции чтения в режиме программирования. Аналогично преодолевается защита в МК с многократно программируемым ПЗУ на основе ЯП с УФ стиранием.

МК с ПЗУ программ на основе ЯП с электрическим стиранием (ЭС) более устойчивы к инвазивным методам, так как контролировать электрические заряды достаточно сложно. Остается возможность использования пробников на внутренних шинах кристалла, однако это требует высокой квалификации исполнителя. В то же время, неинвазивные методы могут быть использованы достаточно легко. Это связано с высокой чувствительностью ЯП с ЭС к электрическим и временным параметрам управляющих сигналов, что позволяет преодолеть защиту либо путем селективного стирания бита защиты, либо путем перевода схемы защиты в нерабочее положение.

Ситуация с МК на основе Флэш-памяти практически аналогична положению с МК на основе ЯП с ЭС. Практически во всех МК на основе ЯП с ЭС и Флэш-памятью удается преодолеть защиту информации.

Таким образом, при выборе типа МК для проектируемого устройства необходимо учитывать возможности несанкционированного копирования программного обеспечения. Учитывая высокую трудоемкость и стоимость инвазивных методов, наиболее оптимальным вариантом защиты информации является использование МК с масочным ПЗУ программ. Более подробная информация содержится в работе [1].

Список литературы

1. *Skorobogatov S.P.* Copy Protection in Modern Microcontrollers. http://www.cl.cam.ac.uk/~sps32/mcu_lock.html