УДК 621.382

М. И. Ершов, К. К. Кондрашов, А. О. Гасников
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Защита микроконтроллеров от несанкционированного доступа

Рассмотрены основные виды программной и аппаратной защиты микроконтроллеров от несанкционированного доступа. Представлено современное состояние разработок и применяемых технологических решений в области информационной безопасности микроконтроллеров. Приведены примеры защиты топологии кристаллов интегральных схем.

Бит защиты, поликремневая плавкая перемычка, активное экранирование, блокировка доступа к интерфейсу ввода/вывода данных ПЗУ, информационная безопасность

Типичный микроконтроллер (МК) представляет собой интегральную схему (ИС), предназначенную для управления различными электронными устройствами, которая сочетает в одном корпусе функции процессора, периферийных устройств, содержит модули памяти и аналоговые блоки.

Для полноценного функционирования, помимо аппаратной реализации, в память микроконтроллера необходимо записать специальную программу, которая и определяет алгоритм его работы.

Наличие функции чтения содержимого памяти микроконтроллера влечет за собой необходимость защиты его программного обеспечения (ПО) от возможности несанкционированного доступа и копирования. Целью данной статьи является анализ различных методов защиты кристаллов микроконтроллеров от несанкционированного доступа.

Программная защита. Одним из первых видов защиты от копирования ПО является использование специализированной ячейки памяти (бита защиты), отвечающей за отключение доступа к данным. В простейшем варианте этот бит контролирует функцию чтения программного интерфейса. В первоначальном исполнении данный модуль располагался вне массива постоянного запоминающего устройства (ПЗУ). Следующим этапом стало изготовление средства защиты как единого целого со всем массивом памяти микроконтроллерной системы (рис. 1) [1].

Дальнейшее совершенствование технологии привело к тому, что часть основной памяти стала использоваться для контроля доступа к данным извне. Это было реализовано за счет фиксирования информации, содержащейся в конкретном адресе, и использования пароля для разрешения доступа к памяти.

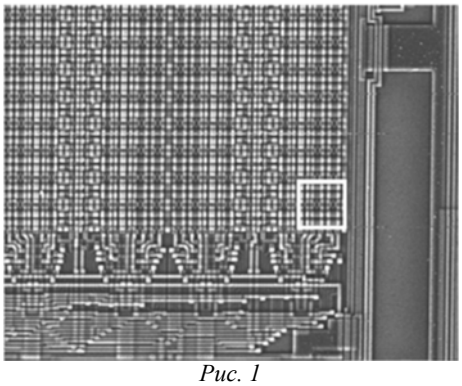


Рис. 1

В ряде случаев ячейки памяти, в которых содержится пароль, могут выполнять и другие функции. Например, область адресного пространства флэш-памяти МК, содержащая 256-битную кодовую последовательность для доступа к ПЗУ, используется также для хранения значений векторов прерываний. Для каждой программы, в зависимости от алгоритма ее работы, набор векторов будет отличаться.

Таким образом, загрузочный файл, записанный в память микроконтроллера, сам создает кодовую последовательность. При этом достигается

высокая степень защиты, так как любое несанкционированное воздействие, позволяющее «сбросить» пароль, приводит к неминуемому изменению программного обеспечения и делает его неработоспособным [2].

Высокая степень безопасности микроконтроллерной системы характеризуется полным отсутствием программного интерфейса. Из соображений безопасности, к примеру, компания NEC не поддерживает возможность чтения данных своих микроконтроллеров. Поэтому операция чтения в них недоступна. Операция проверки устроена так, что данные, отправленные в микросхему для операции проверки, проходят внутреннее сравнение. При этом микросхема возвращает результат 'OK' или 'Ошибка' [3].

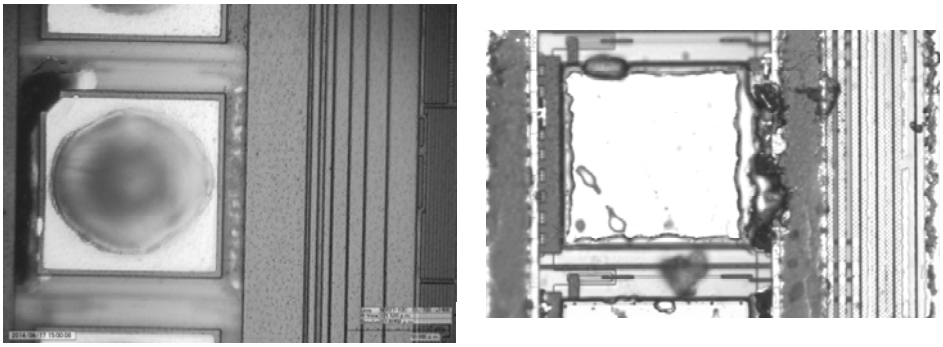
Аппаратная защита. Помимо программных методов реализации защиты от несанкционированного доступа к данным микроконтроллера существуют и аппаратные способы. Одним из таких способов является блокировка доступа к интерфейсу ввода/вывода данных ПЗУ. Реализация данного механизма возможна документированными или недокументированными способами.

К недокументированным способам относятся «выжигание» одного или нескольких выводов микросхемы, предназначенных для чтения и записи данных в ПЗУ. Это делается путем подачи на порт МК напряжений, выходящих за рамки предельных значений. В результате этих воздействий порт «выгорает» и перестает работать. На рис. 2 представлен фрагмент топологии верхнего (*а*) и нижнего (*б*) слоев металлизации микроконтроллерной системы с «выгоревшим» портом. Другие блоки кристалла МК продолжают функционировать в штатном режиме.

К документированным способам относится метод вывода из строя порта ввода/вывода данных путем пережигания специальной плавкой перемычки F (рис. 3, *а*), которая представляет собой узкую полоску поликремния, подключенную непосредственно к линиям «питания» – VDD и «земли» – GND, через мощный транзистор VT (рис. 3, *б*).

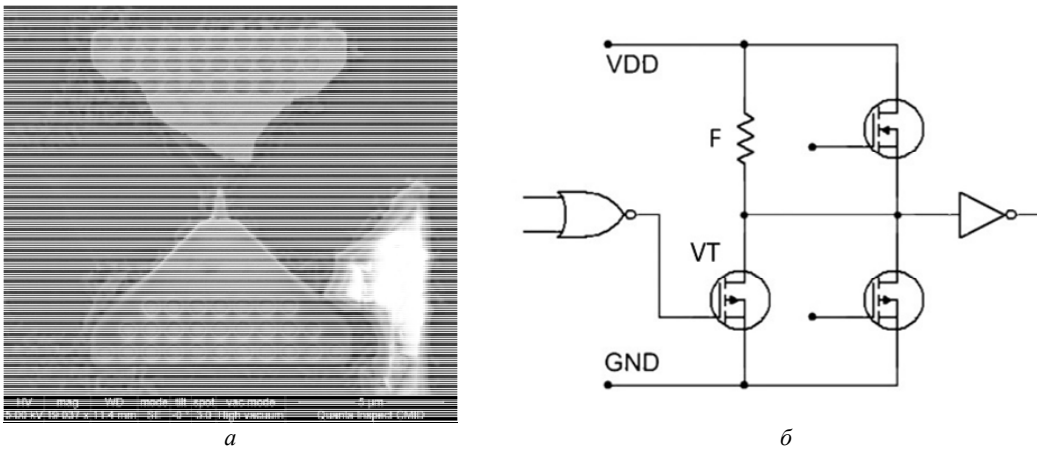
При подаче кратковременного импульса на специализированный вывод МК в цепи начинает течь большой ток, что приводит к плавлению проволоки и переходу из низкоомного состояния в высокоомное [4]. В результате данного воздействия интерфейс чтения/записи данных в ПЗУ МК перестает функционировать.

В современных системах для более надежной защиты подобные перемычки интегрируют во все коммутационные линии интерфейса ввода/вывода данных.



а *б*

Рис. 2



а *б*

Рис. 3

Кроме того, в настоящее время на рынке появляются так называемые защищенные микроконтроллеры. Под этим термином понимаются специализированные полупроводниковые устройства, имеющие на кристалле помимо стандартного процессорного ядра дополнительные аппаратные криптографические блоки. Такие аппаратные модули необходимы для выполнения различных сложных криптографических операций – генерации случайных чисел, шифрования и дешифрования и т. п.

Защита топологии кристаллов интегральных схем. Способы защиты кристаллов ИС от несанкционированного доступа к топологии можно условно разделить:

– на пассивные, которые подразумевают использование защитных слоев, препятствующих анализу структуры элементов кристалла;

– активные, основанные на уничтожении данных и/или элементов топологии при обнаружении факта несанкционированного доступа к кристаллу.

В рамках пассивных способов используется включение в топологию кристалла ИС избыточных дополнительных нефункционирующих элементов, имитирующих стандартно функционирующие элементы: всегда закрытые или всегда открытые транзисторы, непроводящие (ложные) межслойные контакты; дополнительные межсоединения, затрудняющие восстановление истинной электрической схемы и алгоритма функционирования ИС. Применение данных способов не связанно с изменением конструкции элементов и технологического маршрута производства кристалла ИС, а также не требует использования дополнительных фотошаблонов [5].

В основе активных способов лежит активация процессов уничтожения данных ПЗУ и/или топологии ИС при попытке воздействия на кристалл в целом или на его фрагмент.

На рис. 4 приведен пример активного экранирования, которое обычно выглядит в виде сетки.

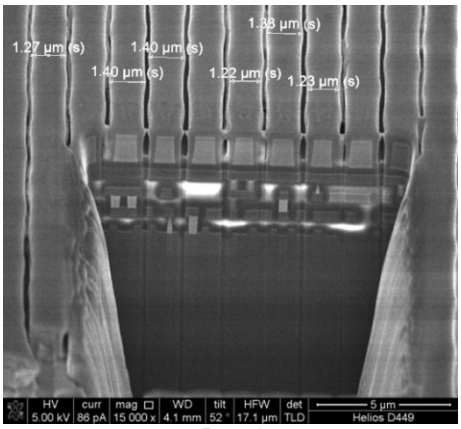


Рис. 4

Данный вид защиты может детектировать электрическое тестирование или разрушающее воздействие с последующим блокированием работы кристалла вплоть до полного стирания программного обеспечения и выхода чипа из строя. Элементы сетки контролируются не только на разрыв, но и по значению емкости. При повышении определенного порогового значения тока, текущего в цепи сетки, ИС теряет свою работоспособность.

Растущая степень защищенности микроконтроллерных систем, а также увеличение степени интеграции и реализация на едином кристалле совокупности различных функций должны превратить процесс несанкционированного доступа к объектам интеллектуальной собственности ИС в уникальную по технологической сложности, временным и экономическим затратам задачу.

СПИСОК ЛИТЕРАТУРЫ

1. Skorobogatov S. P. Semi-invasive attacks: a new approach to hardware security analysis: Ph. D. dissertation. University of Cambridge, 2005. 144 p.

2. MSP430 Programming With the Bootloader (BSL). User's Guide. URL: http://www.ti.com/lit/ug/slau319k/slau319k.pdf.

3. 78K0/LC3. 8-Bit Single-Chip Microcontrollers. User's Manual. URL: http://www.farnell.com/datasheets/24575.pdf.

4. Lee W. T. Blowing of polycrystalline silicon fuses // Applied Physics Letters. 2010. Vol. 97, № 2. C. 023502. P. 1–2.

5. Лучинин В. В., Садовая И. М. Противодействие процессам реинжиниринга кристаллов интегральных схем // Петерб. журн. электроники. 2011. № 1. С. 5–16.

M. I. Ershov, K. K. Kondrashov, A. O. Gasnikov
Saint Petersburg Electrotechnical University «LETI»

PROTECTION OF MICROCONTROLLERS FROM ILLEGAL ACCESS

The main types of software and hardware protection of microcontrollers from illegal access are described. Investigations and applied technology solutions in the field of information security of microcontrollers in the current state presented. Examples of protection topology integrated circuit chip presented.

Protection bit, polycrystalline silicon fuse, active shielding, blocking access to the I/O ROM interface, information security