УДК 621.382

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

# Неразрушающая методика тестирования флеш-памяти микроконтроллера. Доступность и уязвимость по каналу энергопотребления

*На примере 8-битного однокристального микроконтроллера общего назначения исследована возможность организации доступа к флеш-памяти по каналу энергопотребления. Обозначена степень важности проблемы обеспечения целостности конфиденциальной информации, хранящейся во флеш-памяти микропроцессорной техники. Рассмотрены теоретические и практические аспекты процедуры получения и анализа данных о напряжении питания тестируемого устройства. Выявлены и проанализированы различные зависимости амплитуды импульса, возникающего в момент выполнения операции чтения числа из памяти, от конкретной конфигурации установленных бит считываемого однобайтового значения. По результатам исследований сделан вывод об устойчивости протестированного микроконтроллера, описаны необходимые условия для возможности полного либо частичного восстановления содержимого флеш-памяти с помощью доступа по каналу энергопотребления. В общих чертах сформулированы ключевые положения будущей методики тестирования микроконтроллеров для определения степени их уязвимости к извлечению данных флеш-памяти.*

**Неразрушающий анализ, микроконтроллер, флеш-память, энергопотребление**

В современном мире наблюдается постоянный рост темпов внедрения микропроцессорной техники в бытовую жизнь, государственные структуры, оборонно-промышленные и медико-биологические комплексы, различные виды интернет-технологий. Этот процесс сопровождается ростом объемов информации, хранящейся и передающейся в электронном виде, в том числе обладающей значительной ценностью в отношении коммерческой тайны, эксплуатации техногенно-опасных объектов и сферы безопасности человека как личности. Особенно эта проблема касается защиты конфиденциальных данных, содержащихся в микропроцессорной технике.

Сейчас микроконтроллеры имеют встроенную флеш-память, которая, помимо исполняемого программного кода, может хранить и какие-нибудь ценные сведения, например ключи шифрования, пароли, информацию для служебного пользования. Как показывают предыдущие исследования [1], данные, хранящиеся во флеш-памяти, в ряде случаев могут быть уязвимы при проведении неразрушающего анализа по энергопотреблению. Поскольку такая возможность получения конфиденциальной информации представляет потенциальную угрозу, особенно в случае применения микроконтроллеров в технике указанных ранее назначений, встает вопрос о необходимости их тестирования на предмет уязвимости к извлечению данных.

Целью настоящей статьи является демонстрация возможного способа доступа к флеш-памяти микроконтроллера по анализу энергопотребления.

**Базовые положения методов анализа.** Анализ микроконтроллера по энергопотреблению является наиболее популярной разновидностью анализа интегральных микросхем по побочным каналам [1]. Суть всех направлений анализа по побочным каналам состоит в том, что работа вычислительной системы сопровождается различными физическими процессами, исследование закономерностей которых позволяет определять выполняемые устройством операции и данные, участвующие в этих операциях. Одним из таких физических процессов является протекание тока в цепи питания микроконтроллера. Сила этого тока характеризует энергопотребление микропроцессорной системы, ее можно легко измерять и отслеживать. Анализ по энергопотреблению был впервые предложен Полом Кохером в 1999 г. применительно к криптографическим устройствам [2]. В дальнейшем он был распространен

на более широкий класс устройств, в том числе на все типы микроконтроллеров. Этот вид анализа основывается на том, что во время выполнения различных операций система потребляет различное количество электроэнергии, что выражается в изменениях силы тока в цепи питания. Собирая и анализируя данные потребляемой мощности, можно установить, какие операции и с какими числами производились в микроконтроллере на каждом отрезке времени.

Анализ микросхем по энергопотреблению подразделяется на простой и дифференциальный.

*Простой анализ* по энергопотреблению (Simple Power Analysis, SPA) предусматривает анализ непосредственно собранных данных по потребляемой мощности микропроцессорной системы в ходе ее работы. Целью простого анализа является получение общих сведений о выполняемых инструкциях и об обрабатываемых числах. Как правило, он не позволяет извлечь какую-либо конкретную информацию, но успешно используется для нахождения нужного участка осциллограммы, к которому впоследствии применяется дифференциальный анализ.

*Дифференциальный анализ* по энергопотреблению (Differential Power Analysis, DPA) – это метод анализа флуктуаций потребляемой мощности системы с использованием статистической обработки данных для выявления закономерностей. Использование этого метода подразумевает составление выборок по результатам измерений и последующее вычисление разности их усреднений, которая может либо стремиться к нулю, либо к определенному ненулевому значению в различных случаях. В сравнении с методом простого анализа по энергопотреблению данный метод обладает тем преимуществом, что позволяет определить даже самые незначительные зависимости измеряемых величин в условиях влияния шума.

**Экспериментальные исследования.** Процедура дифференциального анализа по питанию содержит серию последовательных этапов.

*Подготовка аппаратуры.* Предусматривает подготовку средств измерения для подключения к устройству, составление и отправку данных на вход системы. Для этих целей используется современный цифровой осциллограф с полосой пропускания минимум 100 МГц, каналы которого подключаются к линиям питания и ввода-вывода исследуемого устройства. Возможна модернизация цепи питания, например последовательное включение резистора небольшого номинала.

*Измерение.* Это непосредственное снятие сигнала с шины питания во время работы устройства, полученные данные сохраняются на компьютере. Для улучшения качества сигнала возможно включение в измерительную цепь различных аналоговых фильтров.

*Обработка сигналов в программном обеспечении.* Здесь используются вычислительные мощности компьютера для обработки сохраненного сигнала с целью избавления от шума или акцентирования определенных областей.

*Выборка.* На основе различных функций выборки и в зависимости от входных данных делаются предположения о состоянии, в котором находится система.

*Усреднение.* Для уменьшения погрешности и обеспечения заданной точности измерений производится усреднение для каждой выборки в зависимости от их функций.

*Оценка.* На заключительном этапе анализируются результаты и формируются соответствующие выводы.

В общем случае дифференциальный анализ по побочным каналам подразумевает исследование корреляции между данными и мгновенной утечкой побочного канала устройства с использованием статистических методов для улучшения эффективности [3].

**Описание объекта исследований.** Центральным объектом для исследования в описываемом случае является коммерческий 8-битный однокристальный микроконтроллер фирмы Renesas Electronics, выполненный в корпусе SSOP с 16 выводами. Он применяется в основном в бытовой электротехнике (кондиционерах, стиральных машинах, пылесосах, блендерах и т. д.).

Микроконтроллер имеет 2 внутренних осциллятора (низкой и высокой частоты), сторожевой таймер, 1 Кбайт встроенной флеш-памяти и 128 байт энергозависимой оперативной памяти. Он характеризуется допустимым напряжением питания от 2 до 5.5 В; температурным диапазоном работы от –40 до +85 °С; минимальным временем выполнения операции – 0.2 мкс [4].

Флеш-память микроконтроллера разделена на 4 блока объемом по 256 байт каждый. Операции стирания и программирования применимы к каждой ячейке памяти индивидуально, также возможно стирание всего блока разом. Отличительной особенностью является невозможность чтения данных флеш-памяти через программатор и

поддержка функции самопрограммирования. Благодаря ей можно реализовать перезапись ячеек в процессе работы.

**Описание испытательной базы.** Для обеспечения надежного питания микроконтроллера использовался источник Tektronix PWS4305, который обладает линейной стабилизацией, выходным напряжением до 30 В, базовыми погрешностями по напряжению 0.03 %, по току – 0.05 %. Также он имеет порт USB на задней панели для подключения к персональному компьютеру и дистанционного управления.

Для измерений использовался цифровой осциллограф Agilent Infiniium 54853A DSO. Данный осциллограф способен снимать сигнал с частотой до 2.5 ГГц, при этом он обладает частотой дискретизации до 20 Гсэмпл/с на всех каналах одновременно.

Для записи исполняемой программы в микроконтроллер использовался программатор BeeProg2, обладающий интерфейсами USB и LPT, разъемом для внутрисхемного программирования (ISP) с расширенными функциями, а также имеющий весьма обширный ряд поддерживаемых устройств.

Для реализации исследования микроконтроллер был помещен на макетную плату, а выводы с его корпуса были соединены со штыревыми выводами платы. Тактовый сигнал для работы микроконтроллера создавался внутренним осциллятором с частотой 8 МГц.

**Процесс исследований.** *Этап 1.* Для проведения первой части исследования был разработан и реализован следующий алгоритм: в начале выполнения программы все 256 ячеек 4-го блока флеш-памяти микроконтроллера пусты (заполнены по умолчанию значением 0xFF). При внешнем воздействии (нажатие на кнопку) возникает прерывание, инициализирующее подпрограмму, которая осуществляет переход к режиму самопрограммирования, стирает данные из выбранного блока, записывает в ячейку памяти значение из переменной-счетчика и затем возвращает микроконтроллер к первоначальному режиму работы. При этом переменная-счетчик в начале работы программы имеет значение 0xFF, а после, при каждом прерывании, осуществляется побитовое смещение данной переменной вправо на один разряд. Таким образом, она принимает значения: 0xFF, 0x7F, 0x3F, 0x1F, 0x0F, 0x07, 0x03, 0x01, 0x00; далее переменная возвращается к ее первоначальному состоянию 0xFF.

*Этап 2.* Для организации второго этапа исследования, в ходе которого в ячейку памяти последовательно записываются все 255 возможных чисел, потребовался алгоритм с большей степенью автоматизации. В данном случае вместо нажатия на кнопку в качестве внешнего воздействия используется подача питания на микроконтроллер. При каждой инициализации программы происходит считывание предыдущего значения из выбранной ячейки памяти, затем эта переменная инкрементируется и результат снова записывается в память.

И на первом, и на втором этапах исследования в основном режиме работы микроконтроллера происходит непрерывное считывание значения из одной анализируемой ячейки памяти в переменную в бесконечном цикле с определенным интервалом. Эта операция непосредственно используется для тестирования флеш-памяти на уязвимость к извлечению данных по каналу энергопотребления.

Принцип процедуры тестирования памяти заключается в обработке осциллограммы сигнала с линии питания микроконтроллера, в который предварительно «зашита» специально подготовленная программа. Общий вид данной осциллограммы показан на рис. 1. Каждому такту микроконтроллера на осциллограмме соответствует 2 характеристических импульса из-за различия тактовой частоты внутреннего осциллятора и рабочей частоты. Для проведения такого рода исследования крайне важна стабильность условий эксперимента, в частности, стабильность источника напряжения для работы микроконтроллера, постоянное значение температуры, отсутствие какого-либо механического воздействия на объект.

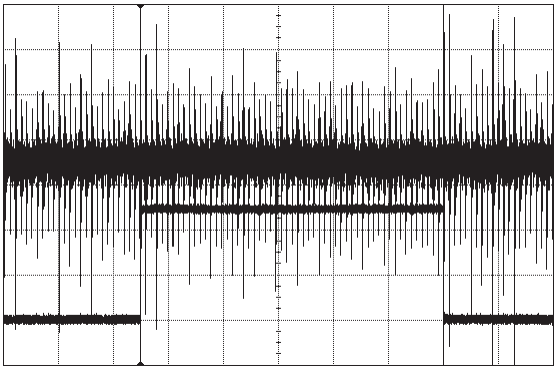

*Рис. 1*

Ключевой задачей первого этапа исследования являлось обнаружение характеристического импульса с выраженной зависимостью амплитуды от считываемого числа. Очевидно, этот им-

пульс следует искать на участке осциллограммы, соответствующем моменту чтения данных из ячейки. Для определения участка осциллограммы необходимо сопоставить число тактов команд программного кода на языке ассемблера с количеством наблюдаемых характеристических импульсов. Фрагмент программного кода, содержащий операцию чтения из ячейки, представлен на рис. 2 и в табл. 1.

```
Disassembly
    01D5    22DA00      CALL    0x00DA
    01D8    22EA00      CALL    0x00EA
    01DB    F50300      MOV     S:P3, #0x00
    01DE    301B        BR      0x01FB
    01E0    0AF3FF      MOV     A, #0xFF
    01E3    E9F8FE      MOV     0xFEF8, A
    01E6    22EA00      CALL    0x00EA
    01E9    F50304      MOV     S:P3, #0x04
    01EC    296003      MOV     A, 0x0360
    01EF    E9F9FE      MOV     0xFEF9, A
    01F2    F0A000      MOVW    AX, #0x00A0
    01F5    F50300      MOV     S:P3, #0x00
    01F8    220E01      CALL    0x010E
    01FB    F749AC      MOV     WDTE, #0xAC
    01FE    29FAFE      MOV     A, 0xFEFA
    0201    1300        CMP     A, #0x00
    0203    3CE4        BZ      0x01E9
    0205    221801      CALL    0x0118
    0208    F40000      MOVW    BC, #0x0000
    020B    29F6FE      MOV     A, 0xFEF6
    020E    225D01      CALL    0x015D
    0211    29F8FE      MOV     A, 0xFEF8
```

*Рис. 2*

В данном случае переменной read в коде Си соответствует переменная A в ассемблеровском коде, а переменная store содержит в себе данные по адресу выбранной ячейки 0x0360. Число тактов, требуемое для выполнения команд в табл. 1, определено по официальной документации устройства [4].

С учетом того, что количество импульсов на осциллограмме в 2 раза больше количества тактов соответствующих операций в микроконтроллере, процесс чтения данных из ячейки флеш-памяти в переменную между двумя командами подачи на вывод P3 сигналов «1» и «0» соответственно занимает 8 + 8 + 6 + 6 = 28 тактов или 28 · 2 = 56 импульсов. Из них самой операции считывания соответствует 8 + 8 = 16 тактов или 32 импульса. Изображение осциллограммы с указанием соответствующих ассемблеровских команд на каждом участке показано на рис. 3.

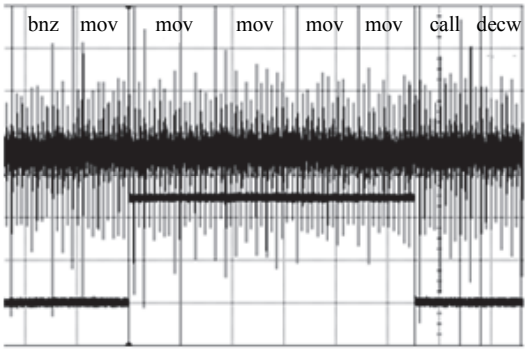


*Рис. 3*

Для автоматизации сбора данных о характеристических импульсах использовался специализированный программно-аппаратный комплекс, в состав которого входят упомянутые ранее источник питания, осциллограф и программатор. Контроль всех компонентов комплекса и процесса измерений обеспечивается отдельным приложением, разработанным в среде LabVIEW и установленным на осциллограф. Интерфейс данного приложения позволяет установить специфические параметры для анализа осциллограмм, такие, как длительность и положение во времени исследуемого фрагмента, тип и диапазон фильтрации сигнала по частотам, параметры распознавания характеристических импульсов, объем выборки для усреднения и др.

На первом этапе исследования измерялись амплитуды 20 первых импульсов операции считывания с усреднением результатов по 100 экспериментам для каждого значения числа в выбранной ячейке памяти. В результате анализа зависимостей амплитуд всех импульсов от считываемого значения было установлено, что наиболее ярко выраженной зависимостью обладает характеристический импульс, показанный на рис. 4.

Для данного импульса наблюдалась характерная корреляция амплитуды и числа в памяти: с каждым побитовым смещением значения вправо (т. е. с его уменьшением) наблюдается увеличение амплитуды по модулю (рис. 5). Полученные зависимости представлены в табл. 2.

*Таблица 1*

| Адрес операции | Название операции | Язык Си | Время выполнения |
|---|---|---|---|
| 01E9 | MOV S:P3, #0x04 | P3= Pn3_OUTPUT_1; | 6 тактов |
| 01EC | MOV A, 0x0320 | read=store; | 8 тактов |
| 01EF | MOV 0xFEF9, A | | 8 тактов |
| 01F2 | MOVW AX, #0x00A0 | P3= Pn3_OUTPUT_0; | 6 тактов |
| 01F5 | MOV S:P3, #0x00 | | 6 тактов |

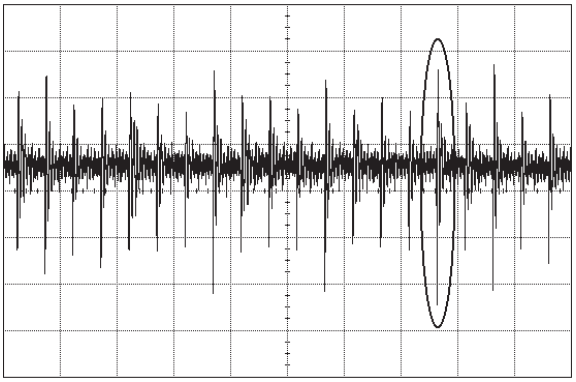

*Рис. 4*

*Таблица 2*

| Записываемое число в шестнадцатеричной системе счисления | Записываемое число в десятичной системе счисления | *U*, мВ |
|---|---|---|
| 0xFF | 255 | –63.6 |
| 0x7F | 127 | –64.4 |
| 0x3F | 63 | –65.3 |
| 0x1F | 31 | –66.1 |
| 0x0F | 15 | –66.7 |
| 0x07 | 7 | –67.4 |
| 0x03 | 3 | –68.4 |
| 0x01 | 1 | –69.7 |
| 0x00 | 0 | –70.3 |

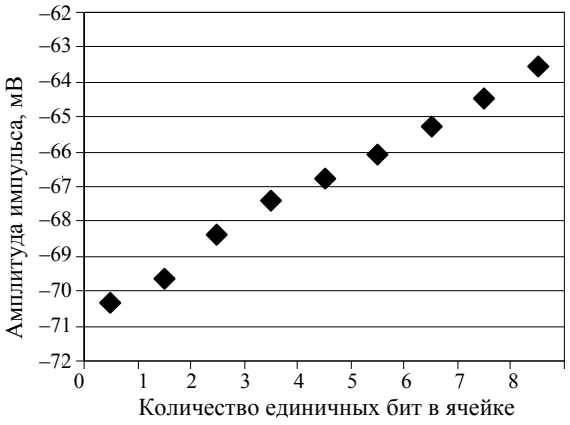


*Рис. 5*

На втором этапе исследования для выбранного характеристического импульса снималась зависимость амплитуды сигнала с линии питания от записанного в ячейку памяти числа во всем диапазоне от 0 до 255. Автоматизированный процесс измерений был реализован с использованием описанного ранее программного алгоритма перезаписи значения. При этом для перехода к следующей итерации необходимо отключить, а затем снова подать питание на микроконтроллер. Такая возможность предусмотрена в управляющем приложении, имеющем опцию автоматической перезагрузки источника питания в ходе эксперимента.

Весь цикл измерений разбивался на 8 частей, в каждой из них были получены данные об амплитуде выбранного импульса для группы из 32 чисел, которые записывались в память (всего 256 чисел). Данное разбиение было призвано оптимизировать процесс исследования, так как проведение такого рода измерений требует существенных временных затрат, а это, в свою очередь, может негативно сказаться на результатах из-за влияния изменяющихся внешних факторов (например, температуры) и увеличения вероятности возникновения ошибок, связанных с работой оборудования и самого микроконтроллера.

Полученная зависимость амплитуды выбранного характеристического импульса от записанного в ячейку флеш-памяти значения представлена на рис. 6.

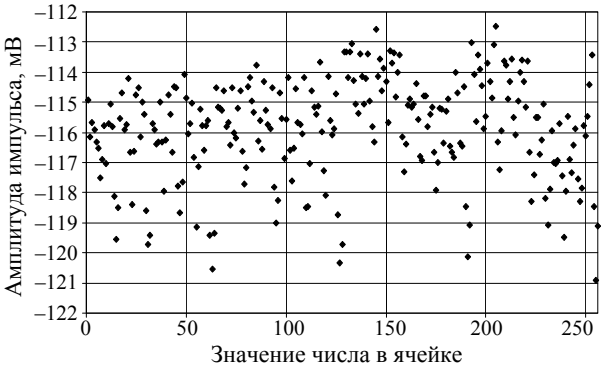


*Рис. 6*

Для оценки возможности выявления числа по амплитуде наблюдаемого импульса необходимо учитывать погрешность измерений, обусловленную аналого-цифровым преобразованием осциллографа. В режиме максимально высокого разрешения она составляет около 3 мВ. Использование статистики позволяет различать более близкие значения амплитуды, но при этом степень достоверности результата оказывается довольно низкой. Извлечение данных из ячеек флеш-памяти исследуемого микроконтроллера методом анализа по энергопотреблению возможно лишь в некоторых частных случаях, таких, как, например, на рис. 5. Похожая зависимость амплитуды импульса от числа обнаруживается также при изменении положения единицы в его двоичном представлении (табл. 3 и рис. 7). Таким образом, если известно, что в ячейке установлен только один бит, можно с высокой точностью определить само число.

*Таблица 3*

| Число в десятичной системе счисления | Число в двоичной системе счисления | $U$, мВ |
|---|---|---|
| 1 | 00000001 | –116.2 |
| 2 | 00000010 | –115.7 |
| 4 | 00000100 | –116.3 |
| 8 | 00001000 | –115.8 |
| 16 | 00010000 | –115.5 |
| 32 | 00100000 | –115.7 |
| 64 | 01000000 | –114.5 |
| 128 | 10000000 | –113.3 |

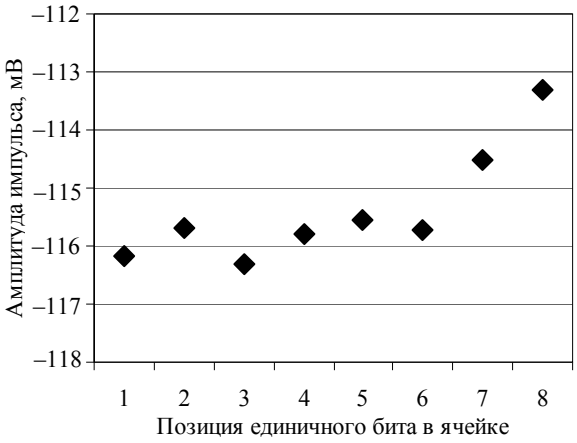


*Рис. 7*

В целом, анализ данного микроконтроллера по энергопотреблению затруднен ввиду некоторых его особенностей. Так, выраженная зависимость от записанного в ячейке памяти числа наблюдалась только у одного импульса сигнала; кроме того, точность существенно ограничена относительно малым размахом значений амплитуды на всем диапазоне измерений (в пределах 10 мВ). Детальное исследование выборок, составленных по результатам второго этапа, показало, что из общего количества чисел (256) могут быть надежно выявлены примерно 60, или 23.4 %. Данный показатель может выступать в качестве критерия степени защищенности микроконтроллера. Ключевые положения и принципы используемого подхода могут лечь в основу общей методики тестирования устройств микроэлектроники.

## СПИСОК ЛИТЕРАТУРЫ

1. Кондрашов К. К., Ершов М. И., Гасников А. О. Современное состояние диагностики микропроцессорных систем по нетрадиционным побочным каналам // Изв. СПбГЭТУ «ЛЭТИ». 2016. Вып. 3. С. 3–9.

2. Standaert F.-X. Introduction to Side-Channel Attacks. Secure Integrated Circuits and Systems. NY: Springer US, 2010. P. 27–42.

3. Introduction to differential power analysis / P. Kocher, J. Jaffe, B. Jun, P. Rohatgi // J. of Cryptographic Engineering. 2011. Vol. 1, № 1. P. 5–27.

4. 78K0S/KY1 + 8-bit Single-Chip Microcontrollers User's Manual. Renesas Electronic Corporation, November 2009 NS. URL: https://www.renesas.com/en-us/doc/DocumentServer/024/U17798EJ1V0PM00.pdf (дата обращения 30.08.2018)

K. K. Kondrashov, A. O. Gasnikov, V. V. Luchinin
*Saint Petersburg Electrotechnical University*

## NON-INVASIVE METHOD OF TESTING THE FLASH MEMORY OF THE MICROCONTROLLER. AVAILABILITY AND VULNERABILITY OVER THE POWER CONSUMPTION CHANNEL

*On the example of an 8-bit single-chip general-purpose microcontroller, the possibility of organizing access to flash memory via the power consumption channel is investigated. The degree of importance of the problem of ensuring the integrity of confidential information stored in the flash memory of microprocessor devices is indicated. Theoretical and practical aspects of the procedure for obtaining and analyzing data on the power supply voltage of the device under test are considered. Various dependences of the pulse amplitude that occurs at the time of performing the operation of reading a number from memory on the specific configuration of the set bits of the read single-byte value are identified and analyzed. Based on the results of the conducted research, a conclusion is made about the invulnerability of the tested microcontroller, and the necessary conditions are described for the possibility of full or partial recovery of the flash memory contents using access via the power consumption channel. In general terms, the key provisions of the future microcontroller testing methodology to determine the degree of their vulnerability to flash memory data extraction are formulated.*

**Non-invasive analysis, microcontroller, flash memory, power consumption**