РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 469 384** (13) **C2**

(51) МПК
G06F 12/14 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010126180/08, 21.11.2008**

(24) Дата начала отсчета срока действия патента:
21.11.2008

Приоритет(ы):
(30) Конвенционный приоритет:
26.11.2007 FR 0708242

(43) Дата публикации заявки: **10.01.2012** Бюл. № 1

(45) Опубликовано: **10.12.2012** Бюл. № **34**

(56) Список документов, цитированных в отчете о поиске: **WO 2000023866 A1, 27.04.2000. FR 2776410 A1, 24.09.1999. RU 2297065 C2, 10.04.2007. RU 2146399 C1, 10.03.2000. US 20070061594 A1, 15.03.2007.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **28.06.2010**

(86) Заявка PCT:
FR 2008/052106 (21.11.2008)

(87) Публикация заявки PCT:
WO 2009/071819 (11.06.2009)

Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО "Союзпатент", Ю.Б.Перегудовой, рег.№ 1103

(72) Автор(ы):
ПЕЛЛЕТЬЕ Эрве (FR),
ДЮМА Паскаль (FR)

(73) Патентообладатель(и):
МОРФО (FR)

(54) СПОСОБ МАСКИРОВКИ ПЕРЕХОДА К КОНЦУ СРОКА СЛУЖБЫ ЭЛЕКТРОННОГО УСТРОЙСТВА И УСТРОЙСТВО, СОДЕРЖАЩЕЕ СООТВЕТСТВУЮЩИЙ КОНТРОЛЬНЫЙ МОДУЛЬ

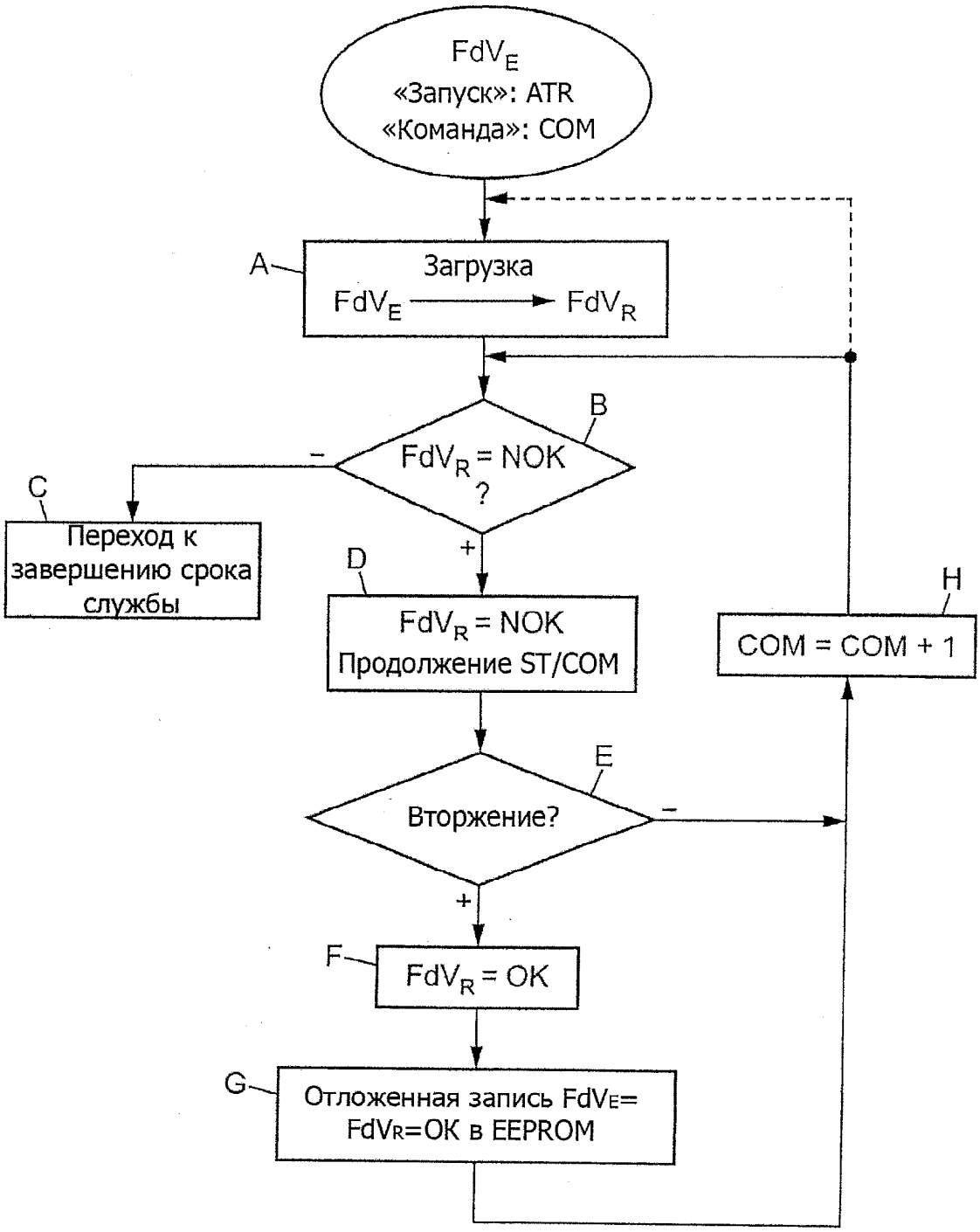
(57) Реферат:

Изобретение относится к средствам защиты электронных устройств. Технический результат заключается в обеспечении надежности процесса перехода к концу службы электронного устройства. Способ маскировки перехода к концу срока службы микропроцессорного электронного устройства, содержащего микропроцессор, энергонезависимую перепрограммируемую память, содержащую переменную состояния конца срока службы (FdV_E). Во время запуска (ATR) в оперативную память загружают (A) значение переменной (FdY_E). До выполнения любой текущей команды (COM) проверяют (B) значение переменной (FdV_R) в оперативной памяти по ложному значению. При получении отрицательного ответа выполняют (C) переход к концу срока службы. В противном случае продолжают (D) инициализацию или выполнение команды (COM). При обнаружении (E) вторжения задают (F) значение переменной состояния завершения срока службы электронного

RU 2469384 C2

RU 2469384 C2

устройства (FdV_R) по истинному значению путем записи только в оперативную память, затем откладывают (G) запись переменной состояния конца срока службы (FdV_E) с истинным значением в энергонезависимую память до выполнения ближайшей операции записи. Способ применяют для любого электронного устройства, микропроцессорной карты или другого устройства. 3 н. и 7 з.п. ф-лы, 7 ил.



Фиг. 1a

RU 2469384 C2

RU 2469384 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 469 384** (13) **C2**

(51) Int. Cl.
G06F 12/14 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010126180/08, 21.11.2008**

(24) Effective date for property rights:
21.11.2008

Priority:
(30) Convention priority:
26.11.2007 FR 0708242

(43) Application published: **10.01.2012** Bull. 1

(45) Date of publication: **10.12.2012 Bull. 34**

(85) Commencement of national phase: **28.06.2010**

(86) PCT application:
FR 2008/052106 (21.11.2008)

(87) PCT publication:
WO 2009/071819 (11.06.2009)

Mail address:
109012, Moskva, ul. Il'inka, 5/2, OOO "Sojuzpatent", Ju.B.Peregudovoj, reg.№ 1103

(72) Inventor(s):
PELLET'E Ehrve (FR),
DJuMA Paskal' (FR)

(73) Proprietor(s):
MORFO (FR)

RU 2469384 C2

(54) METHOD OF MASKING END-OF-LIFE TRANSITION OF ELECTRONIC DEVICE, AND DEVICE INCLUDING CORRESPONDING CONTROL MODULE

(57) Abstract:

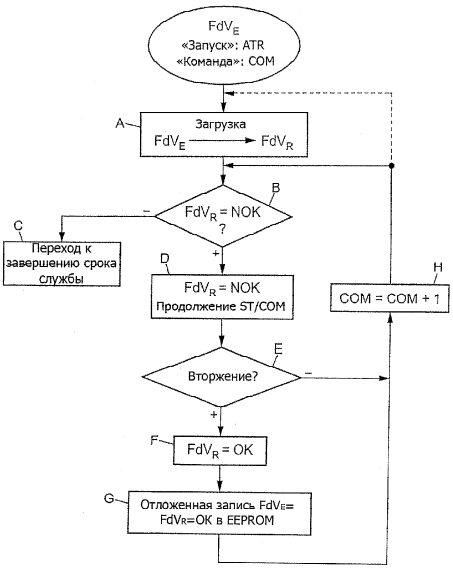
FIELD: information technology.

SUBSTANCE: method for masking the end-of-life transition of an electronic microprocessor device comprising a microprocessor, reprogrammable non-volatile memory containing an end-of-life state variable (FdV_E). On booting (ATR), the value of the variable (FdY_E) is loaded (A) into RAM. Before executing any current command (COM), it is verified (B) whether the value of the variable (FdV_R) stored in RAM is false. If the response is negative, the end-of-life transition is executed (C). Otherwise, initialisation or execution of the command (COM) is continued (D). On detecting (E) intrusion, the value to the end-of-life state variable (FdV_R) is set (F) by writing the true value in RAM only and then deferring (G) writing of the true value to the end-of-life state variable (FdV_e) in the non-volatile memory until the next write operation. The invention is applicable to any electronic device, smart card, etc.

EFFECT: reliable process for end-of-life transition of an electronic device.

10 cl, 7 dwg

RU 2469384 C2



Фиг. 1a

RU 2469384 C2

RU 2469384 C2

Настоящее изобретение относится к способу маскировки перехода к концу срока службы электронного устройства, содержащего входной/выходной порт, микропроцессор, оперативную память, постоянную память и перепрограммируемую энергонезависимую память, содержащую переменную конца срока службы электронного устройства, управляемую контрольным модулем.

Такие электронные устройства неограничительно соответствуют электронным картам или любому электронному устройству, содержащему или связанному, по меньшей мере, с одной электронной картой, в частности, такой как микропроцессорная карта, к которой выдвигаются требования высокой надежности защиты по отношению к любым вторжениям.

Для обеспечения надежной защиты вышеуказанных карт активируют механизм перехода к завершению срока службы при обнаружении определенного числа критических ошибок.

Вместе с тем, процесс перехода к завершению срока службы устройства такого типа, в частности, микропроцессорных карт представляется проблематичным, так как такой процесс в основном основан на процессе записи в перепрограммируемую энергонезависимую память, как правило, память EEPROM, причем этот процесс имеет целью стирание данных и блокировку приложений.

Такой процесс является уязвимым, поскольку он может быть обнаружен за пределами карты, в частности, по причине большого потребления тока в ходе процесса записи в перепрограммируемую энергонезависимую память, и, кроме того, требует определенного времени для исполнения.

Злоумышленник располагает необходимым временем, чтобы помешать такому процессу путем отключения электрического питания устройства или карты.

Задачей настоящего изобретения является обеспечение полной надежности процесса перехода к концу срока службы такого электронного устройства в произвольные сроки после появления критической ошибки, которая является причиной срабатывания перехода к концу срока службы, за счет маскировки, в частности, по отношению к третьему лицу, операции записи в энергонезависимую память, соответствующей переходу к концу срока службы, что на практике предупреждает любую атаку через скрытый канал.

Согласно своему назначению изобретение направлено на обеспечение маскировки любой записи переменной состояния перехода к концу срока службы в энергонезависимую память электронного устройства за счет растворения записи этой операции в нормальном ходе выполнения электронным устройством программы приложения.

Способ маскировки перехода к концу срока службы электронного устройства в соответствии с настоящим изобретением можно применять для любого электронного устройства, содержащего микропроцессор, оперативную память, постоянную память и перепрограммируемую энергонезависимую память, содержащую переменную состояния конца срока службы электронного устройства, управляемую контрольным модулем, и входной/выходной порт.

Способ характеризуется тем, что во время запуска электронного устройства из энергонезависимой памяти в оперативную память загружают значение переменной состояния конца срока службы и до выполнения любой текущей команды микропроцессором проверяют значение этой переменной состояния конца срока службы, записанное в оперативную память, по ложному значению, и при получении отрицательного ответа на эту проверку выполняют операции перехода к концу срока

службы электронного устройства; в противном случае поскольку переменная состояния конца срока службы, записанная в оперативную память, имеет ложное значение, продолжают выполнение текущей команды микропроцессором электронного устройства, а при обнаружении вторжения (интрузивной атаки) с помощью записи только в оперативную память задают значение переменной состояния конца срока службы электронного устройства по истинному значению и продолжают инициализацию и/или выполнение текущей команды, и откладывают запись переменной состояния конца срока службы с истинным значением в энергонезависимую память так, чтобы выполнить эту запись вместо ближайшей операции записи в энергонезависимую память, что позволяет замаскировать запись истинного состояния конца срока службы.

Способ в соответствии с настоящим изобретением отличается также тем, что перед выполнением каждой команды микропроцессором в оперативную память загружают из энергонезависимой памяти значение переменной состояния конца срока службы.

Способ в соответствии с настоящим изобретением отличается также тем, что для всех команд, выполняемых микропроцессором электронного устройства, включая команды, содержащие систематическую запись в энергонезависимую память, и команды, не содержащие записи в энергонезависимую память, независимо от обнаружения или необнаружения вторжения выполняют запись в энергонезависимую запись ложного байта, что позволяет замаскировать любую запись переменной состояния конца срока службы электронного устройства в энергонезависимую память.

Предпочтительно операцию записи этого ложного байта в энергонезависимую память выполняют в той же странице памяти, что и операцию записи переменной состояния конца срока службы электронного устройства.

Кроме того, согласно другому признаку способа в соответствии с настоящим изобретением операцию записи в энергонезависимую память этого ложного байта выполняют перед любым выполнением операции передачи данных по линии связи входного/выходного порта электронного устройства.

Согласно еще одному признаку способ в соответствии с настоящим изобретением включает также после любого этапа записи в энергозависимую память переменной состояния конца срока службы проверку значения переменной состояния конца срока службы по истинному значению и после проверки по этому истинному значению - этап выполнения операций перехода к концу срока службы электронного устройства.

Согласно другому признаку способ в соответствии с настоящим изобретением характеризуется также тем, что после проверки значения этой переменной состояния конца срока службы по истинному значению заменяют операцию записи ложного байта в энергонезависимую память операцией записи в энергонезависимую память значения переменной состояния конца срока службы.

Электронное устройство, являющееся объектом настоящего изобретения, содержит микропроцессор, оперативную память, постоянную память и энергонезависимую перепрограммируемую память, содержащую переменную состояния конца срока службы электронного устройства, управляемую контрольным модулем, и входной/выходной порт (I/O). Контрольный модуль содержит модуль компьютерной программы для выполнения вышеуказанных этапов способа в соответствии с настоящим изобретением.

Способ маскировки перехода к концу срока службы электронного устройства и электронное устройство, содержащее соответствующий контрольный модуль, в соответствии с настоящим изобретением можно применять для любого электронного

устройства предпочтительно, но не ограничительно для электронных устройств, таких как микропроцессорные карты, обрабатывающие и/или хранящие конфиденциальные или секретные персональные данные.

Изобретения будут более понятны из нижеследующего описания со ссылками на прилагаемые фигуры, на которых:

Фиг.1a - пример блок-схемы основных этапов применения способа в соответствии с настоящим изобретением.

Фиг.1b - пример хронограммы различных этапов, выполняемых в ходе применения способа в соответствии с настоящим изобретением, показанного на фиг.1a.

Фиг.1c-1f - детализированные примеры выполнения этапов способа, показанного на фиг.1a.

Фиг.2 - схематичный пример функциональной архитектуры электронного устройства, снабженного модулем контроля перехода к концу срока службы в соответствии с настоящим изобретением.

Далее со ссылками на фиг.1a-1f следует более подробное описание способа маскировки перехода к концу срока службы электронной карты в соответствии с настоящим изобретением.

В целом способ маскировки перехода к концу срока службы электронной карты в соответствии с настоящим изобретением применяется для любого электронного устройства, содержащего микропроцессор, оперативную память, постоянную память и энергонезависимую перепрограммируемую память, содержащую переменную состояния конца срока службы электронного устройства, управляемую контрольным модулем. В частности, электронное устройство может также содержать входной/выходной порт, обеспечивающий обмен данными, например, с прибором клиента или даже в сети. Понятие энергонезависимой перепрограммируемой памяти охватывает электрически перепрограммируемые запоминающие устройства, например память EEPROM, флэш-память.

Во время работы вышеуказанный электронный прибор осуществляет фазу запуска, обозначенную ATR (Answer To Reset), а затем выполняет последовательные текущие команды, обозначенные COM.

В частности, понятно, что соответствующим электронным устройством может быть, например, любая микропроцессорная карта.

Как показано на фиг.1a, способ маскировки перехода к концу срока службы электронного устройства в соответствии с настоящим изобретением содержит этап A, на котором в оперативную память электронного устройства из его энергонезависимой памяти загружают значение, обозначенное как FdV_E, переменной состояния конца срока службы, записанной в энергонезависимой памяти.

Операция, соответствующая этапу A, обозначена следующим образом:

$FdV_E \rightarrow FdV_R$.

В вышеуказанном выражении FdV_R обозначает значение переменной состояния конца срока службы электронного устройства, загруженное в оперативную память.

После этапа A, показанного на фиг.1A, и перед выполнением микропроцессором любой текущей команды COM согласно способу в соответствии с настоящим изобретением далее на этапе B проверяют значение переменной состояния конца срока службы, записанное в оперативную память, по ложному значению. На этапе B, показанном на фиг.1, проверка представлена следующим этапом теста:

FdV_R=NOK?

В этом выражении NOK обозначает ложное значение переменной состояния конца

срока службы электронного устройства, записанное в оперативную память.

При отрицательном ответе на тест этапа B согласно способу в соответствии с настоящим изобретением выполняют C операции перехода к концу срока службы электронного устройства.

В случае положительного ответа на тест, выполняемый на этапе B, поскольку переменная FdV_R состояния конца срока службы является ложным значением NOK, согласно способу в соответствии с настоящим изобретением продолжают инициализацию или выполнение текущей команды COM микропроцессором электронного устройства. Следует отметить, что выполнение текущей команды соответствует любой команде приложения, выполняемой электронным устройством.

В ходе этого выполнения и при обнаружении на этапе E вторжения согласно способу в соответствии с настоящим изобретением на этапе F путем записи только в оперативную память задают значение переменной состояния конца срока службы электронного устройства, то есть переменной FdV_R, по истинному значению и продолжают инициализацию и/или выполнение текущей команды COM.

На этапе F, показанном на фиг.1a, операция введения значения обозначена выражением:

FdV_R=OK.

В вышеуказанном выражении значение OK обозначает истинное значение переменной состояния конца срока службы, записанное в оперативную память.

Наконец, после вышеуказанного этапа инициализации F следует этап G, на котором откладывают запись переменной состояния конца срока службы FdV_R с истинным значением в энергонезависимую память, чтобы выполнить ее вместо ближайшей операции записи в энергонезависимую память. Это позволяет замаскировать запись переменной состояния конца срока службы.

Разумеется, понятно, что после вышеуказанного этапа G следует возвращение к выполнению текущей команды через осуществление этапа H. На вышеуказанном этапе COM+1 обозначает следующую команду.

Как показано на фиг.1A, возвращение для простого выполнения следующей команды происходит на этапе B.

Однако согласно другой возможности выполнения способа в соответствии с настоящим изобретением возвращение можно осуществлять, как показано на фиг.1a пунктирной линией, до загрузки, осуществляемой на этапе A, для возобновления процесса систематической загрузки в оперативную память значения переменной состояния конца срока службы FdV_E. Вместе с тем, такой процесс не является обязательным и может применяться в качестве варианта.

На фиг.1b показана хронограмма операций выполнения этапов, показанных на фиг.1a.

В частности, этап A можно выполнять при запуске ATR или перед выполнением каждой команды COM, как было указано выше.

Тест на этапе B выполняют перед продолжением запуска или выполнения текущей команды, что показано в заштрихованном виде на фиг.1a. Следует напомнить, что отрицательный ответ на тест этапа B автоматически влечет за собой переход к концу срока службы электронного устройства на этапе C.

Продолжение запуска или инициализация или выполнение текущей команды на этапе D по существу соответствует применению процессов алгоритмического манипулирования секретами для электронного устройства, если оно является, например, микропроцессорной картой.

Тест этапа E, соответствующий тесту на обнаружение вторжения, можно осуществлять классически, например, либо путем применения механизмов анти-DFA (Differential Fault Analysis - способ атаки, состоящий во введении ошибки в обработку для извлечения информации об обрабатываемых данных), либо при помощи процессов проверки целостности данных.

Этап введения переменной состояния конца срока службы электронного устройства путем записи только в оперативную память на этапе F выполняет модуль контроля перехода к концу срока службы электронного устройства путем записи этой переменной состояния с истинным значением согласно вышеуказанному выражению:

FdV_R=OK.

После этого этап G обновления переменной состояния конца срока службы FdV_E в энергонезависимой памяти, то есть чаще всего в памяти EEPROM, выполняют как отложенный этап, то есть вместо ближайшей следующей записи, выполняемой в команде.

На фиг.1b эта операция показана в виде заштрихованного пика справа, который иллюстрирует повышение силы тока, потребляемого вышеуказанной памятью, по причине выполнения вышеуказанной операции записи.

Затем за этапом E следует этап возвращения либо на этап B, либо на этап A, что было описано выше со ссылками на фиг.1a.

Следует, в частности, отметить, что ложное значение, обозначенное NOK, переменной состояния конца срока службы электронного устройства, является произвольным цифровым значением. Что же касается истинного значения OK переменной состояния конца срока службы, то оно может быть любым цифровым значением, отличным от вышеуказанного произвольного цифрового значения.

Как показано на фиг.1c, рассматривают любой набор команд, выполняемых микропроцессором электронного устройства, включая команды (COM_w), содержащие систематическую запись в энергонезависимую память, и команду ($\overline{COM_w}$), не содержащую записи в энергонезависимую память. При таком предположении согласно способу в соответствии с настоящим изобретением независимо от обнаружения или необнаружения вторжения осуществляют запись D_2 в энергонезависимую память ложного байта, который обозначен OF. Это позволяет замаскировать любую возможную запись переменной состояния конца срока службы электронного устройства в энергонезависимую память.

Предпочтительно запись ложного байта OF осуществляют в той же странице памяти, что и запись переменной состояния конца срока службы.

На этапе D_2, показанном на фиг.1c, операция записи в той же странице памяти показана в виде выражения:

WAP(OF)=WAP(FdVE).

В вышеуказанном выражении WAP обозначает адрес страницы памяти для записи.

За этапом D2 следует вызов этапа E, показанного на фиг.1a.

Кроме того, как показано на фиг.1c, операцию записи в энергонезависимую память ложного байта выполняют до выполнения любой операции передачи данных на линии входного/выходного порта электронного устройства. На фиг.1 с соответствующая операция символически показана в виде обнаружения любой операции ввода/вывода при помощи выражения:

COM=I/O?

Обнаружение такой операции приводит к систематической и немедленной записи ложного байта, как было указано выше в описании.

Наконец, как показано на фиг.1d, предпочтительно способ в соответствии с настоящим изобретением включает после любого этапа записи в энергонезависимую память переменной состояния конца срока службы, как показано на этапе G1, этап, обозначенный G2, на котором проверяют значение переменной состояния конца срока службы FdV_R, записанное в оперативной памяти, по истинному значению. Операцию, соответствующую вышеуказанному этапу, обозначают следующим выражением:

FdV_R=OK.

После проверки переменной состояния конца срока службы по истинному значению осуществляют этап выполнения операций перехода к концу срока службы электронного устройства путем вызова этапа C, показанного на фиг.1a.

При отсутствии проверки переменной состояния конца срока службы по истинному значению производят возвращение на этап H.

Кроме того, как показано на фиг.1e, при проверке на этапе D_{21} значения переменной состояния конца срока службы FdV_R по истинному значению, то есть при положительном ответе на вышеуказанный тест D_{21} операцию записи в энергонезависимую память ложного байта OF, показанную на этапе D_{22} фиг.1e, заменяют записью в память EEPROM значения переменной состояния конца срока службы FdV_E путем вызова этапа G, показанного на фиг.1a.

Кроме того, способ в соответствии с настоящим изобретением позволяет применять счетчик ошибок.

Как правило, обновление счетчика ошибок должно соблюдать те же ограничения, что и запись переменной состояния конца срока службы.

Поскольку речь идет о записи в энергонезависимую память типа EEPROM, такую запись можно обнаружить по повышению тока, потребляемого этой памятью во время операции записи.

Предпочтительно в случае обнаружения ошибок, не предполагающих прямого перехода к концу срока службы, способ в соответствии с настоящим изобретением позволяет произвести инкрементацию счетчика до осуществления нормальной записи. После этого значение счетчика регулярно проверяют, и превышение порогового значения позволяет запустить переход к концу срока службы.

Такой рабочий режим показан на фиг.1f и состоит в следующем:

- обнаружение I_1 временной ошибки выполнения команды, отличной от вторжения и непредполагающей перехода к концу срока службы электронного устройства; обнаружение вышеуказанной временной ошибки выполнения обозначено ∃TE?, где TE обозначает вышеуказанную временную ошибку, положительный ответ на тест I_1 вызывает этап I_2 обновления путем инкрементации счетчика ошибок в оперативной памяти.

Обновление на этапе I_2 показано в виде выражения:

TE=TE+1, и за ним следует этап сравнения I_3 значения отсчета обновленных значений с пороговым значением, обозначенным STE.

На этапе теста I_3 операция сравнения обозначена как:

TE>STE?

При превышении порогового значения обновленным значением отсчета ошибки, то есть при положительном ответе на тест I_3, осуществляют запись значения переменной состояния конца срока службы электронного устройства с истинным значением и переход к концу срока службы путем вызова этапа F, затем этапа G, как показано на фиг.1f.

Далее со ссылками на фиг.2 следует описание электронного устройства,

содержащего микропроцессор, обозначенный 1_1, оперативную память, обозначенную 1_2, энергонезависимую память, например, типа EEPROM, обозначенную 1_3, и постоянную память, обозначенную 1_4. Кроме того, как показано на указанной фигуре, устройство содержит входной/выходной порт, обозначенный I/O.

Как показано на фиг.2, электронное устройство во время работы содержит переменную состояния конца срока службы электронного устройства, обозначенную FdV_E, управляемую контрольным модулем CM, который может быть, например, программным модулем, установленным в постоянной памяти 1_4.

Контрольный модуль CM содержит модуль компьютерных программ SCM, обеспечивающий выполнение этапов способа маскировки перехода к концу срока службы электронного устройства, что было описано выше со ссылками на фиг.1a-1f.

Разумеется, модуль компьютерных программ SCM можно установить в энергонезависимой памяти типа EEPROM, которая является носителем для записи информации. Этот модуль компьютерных программ содержит набор команд, выполняемых микропроцессором электронного устройства, и во время выполнения вышеуказанных команд выполняет этапы способа, описанного выше со ссылками на фиг.1a-1f.

Способ маскировки перехода к концу срока службы электронного устройства в соответствии с настоящим изобретением можно применять на электронных картах. Самые тщательные испытания, проведенные на этих электронных картах с использованием независимых блоков проверки надежности, не смогли препятствовать переходу к концу срока службы этих электронных карт в отличие от электронных карт, использующих классические процессы перехода к концу срока службы, при которых можно многократно производить вторжения вплоть до выявления слабого места карты. Следовательно, способ в соответствии с настоящим изобретением не позволяет отличить по времени случай, когда атака обнаружена и должна привести к переходу к концу срока службы электронного устройства, от случая, когда атака не обнаружена или не оказала никакого влияния.

Формула изобретения

1. Способ маскировки перехода к концу срока службы электронного устройства, содержащего микропроцессор, оперативную память, постоянную память и энергонезависимую перепрограммируемую память, содержащую переменную состояния конца срока службы электронного устройства, управляемую контрольным модулем, и входной/выходной порт, отличающийся тем, что, по меньшей мере, во время запуска (ATR) электронного устройства из энергонезависимой памяти в оперативную память загружают (A) значение (FdV_E) указанной переменной состояния конца срока службы; и до выполнения микропроцессором любой текущей команды проверяют (B) по ложному значению значение этой переменной состояния конца срока службы, записанное в оперативную память (FdV_R), и при получении отрицательного ответа на эту проверку выполняют (C) операции перехода к концу срока службы электронного устройства; в противном случае продолжают (D) инициализацию или выполнение микропроцессором электронного устройства текущей команды (COM), поскольку переменная состояния конца срока службы, записанная в оперативную память (FdV_R), является ложным значением, а при обнаружении (E) вторжения задают (F) истинное значение переменной состояния конца срока службы электронного устройства (FdV_R) путем записи только в оперативную память и продолжают инициализацию и/или выполнение текущей команды, при этом

откладывают (G) запись переменной состояния конца срока службы (FdV_E) с истинным значением в энергонезависимую память для выполнения этой записи вместо ближайшей операции записи в энергонезависимую память в команде, что позволяет замаскировать запись указанной переменной состояния конца срока службы.

2. Способ по п.1, отличающийся тем, что ложное значение (FdV_R=NOK) указанной переменной состояния конца срока службы электронного устройства является произвольным цифровым значением, при этом истинное значение (FdV_R=OK) указанной переменной состояния конца срока службы электронного устройства является любым цифровым значением, отличным от указанного произвольного цифрового значения.

3. Способ по п.1 или 2, отличающийся тем, что для всех команд $\left(COM \in \left\{COM_w, COM_{\overline{w}}\right\}\right)$, выполняемых микропроцессором электронного устройства, включая команды (COM_w), содержащие систематическую запись в энергонезависимую память, и команды $\left(COM_{\overline{w}}\right)$, не содержащие записи в энергонезависимую память, независимо от обнаружения или не обнаружения вторжения выполняют запись в энергонезависимую запись ложного байта, что позволяет замаскировать любую запись переменной состояния конца срока службы электронного устройства в энергонезависимую память.

4. Способ по п.3, отличающийся тем, что запись указанного ложного байта в энергонезависимую память выполняют в той же странице памяти, что и запись указанной переменной состояния конца срока службы.

5. Способ по п.3, отличающийся тем, что указанную операцию записи в энергонезависимую память указанного ложного байта выполняют перед любым выполнением операции передачи данных по линии связи входного/выходного порта микропроцессорного электронного устройства.

6. Способ по п.5, отличающийся тем, что после проверки значения указанной переменной состояния конца срока службы (FdV_R) по истинному значению заменяют указанную операцию записи ложного байта в энергонезависимую память операцией записи в энергонезависимую память значения переменной состояния конца срока службы (FdV_E).

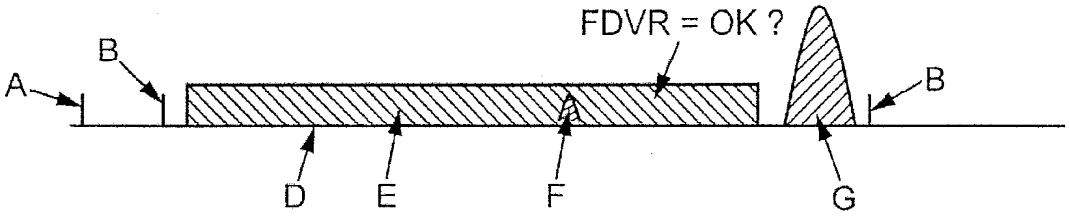
7. Способ по п.3, отличающийся тем, что после любого этапа записи в энергонезависимую память переменной состояния конца срока службы (FdV_E) осуществляют этап проверки значения переменной состояния конца срока службы (FdV_R) по истинному значению и после проверки по истинному значению осуществляют этап выполнения операций перехода к концу срока службы электронного устройства.

8. Способ по п.1, отличающийся тем, что при обнаружении временной ошибки выполнения команды, отличной от вторжения и не предполагающей перехода к концу срока службы электронного устройства, дополнительно обновляют путем инкрементации счетчик ошибок в оперативной памяти; сравнивают значения отсчета ошибок с пороговым значением; и при превышении указанного значения отсчета ошибок над указанным пороговым значением записывают значения указанной переменной состояния конца срока службы с истинным значением и выполняют переход к концу срока службы электронного устройства.

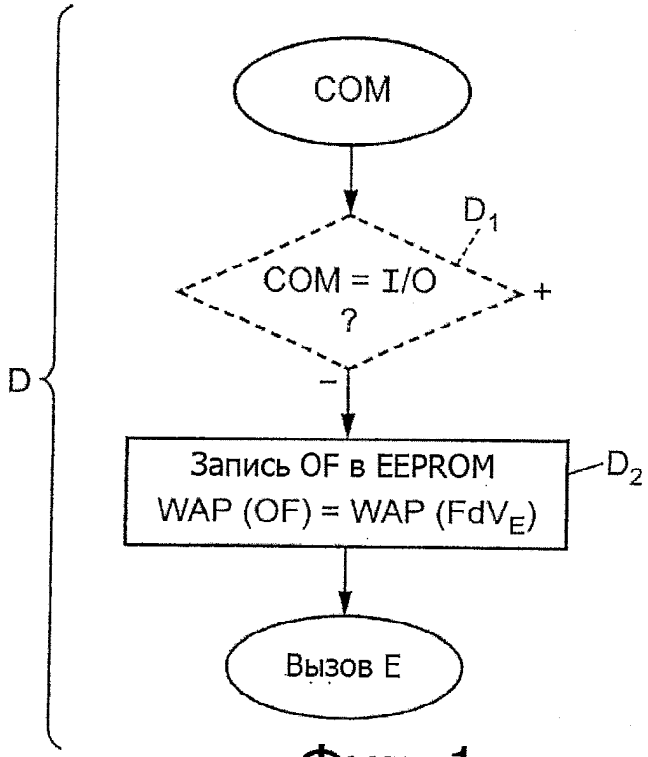
9. Электронное устройство, содержащее микропроцессор, оперативную память, постоянную память и энергонезависимую перепрограммируемую память, содержащую переменную состояния конца срока службы (FdV_E) электронного

устройства, управляемую контрольным модулем, и входной/выходной порт, отличающееся тем, что контрольный модуль содержит модуль компьютерной программы (SCM) для выполнения этапов способа по одному из пп.1-8.

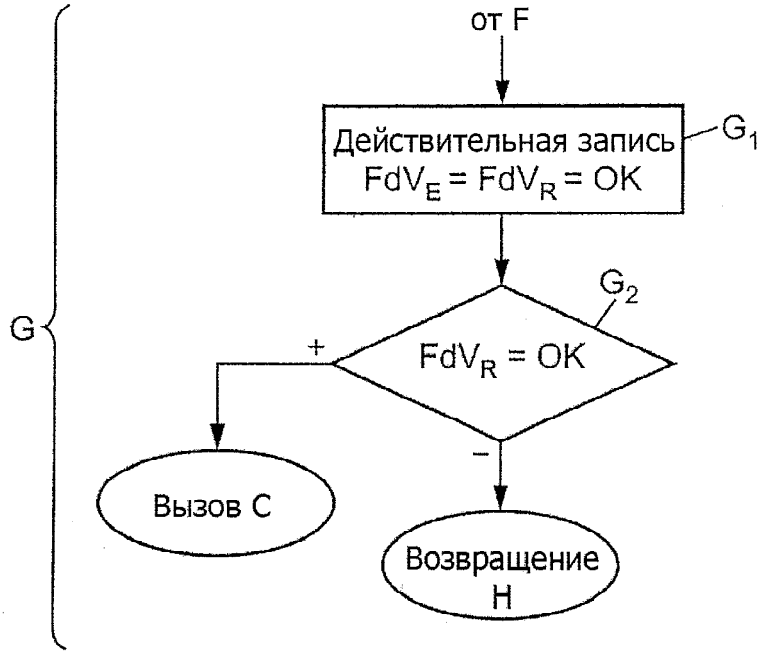
10. Носитель информации с записанным программным компьютерным продуктом, содержащим ряд команд, выполняемых компьютером или микропроцессором электронного устройства, характеризующийся тем, что во время выполнения указанных команд указанная программа выполняет этапы способа по любому из пп.1-8.



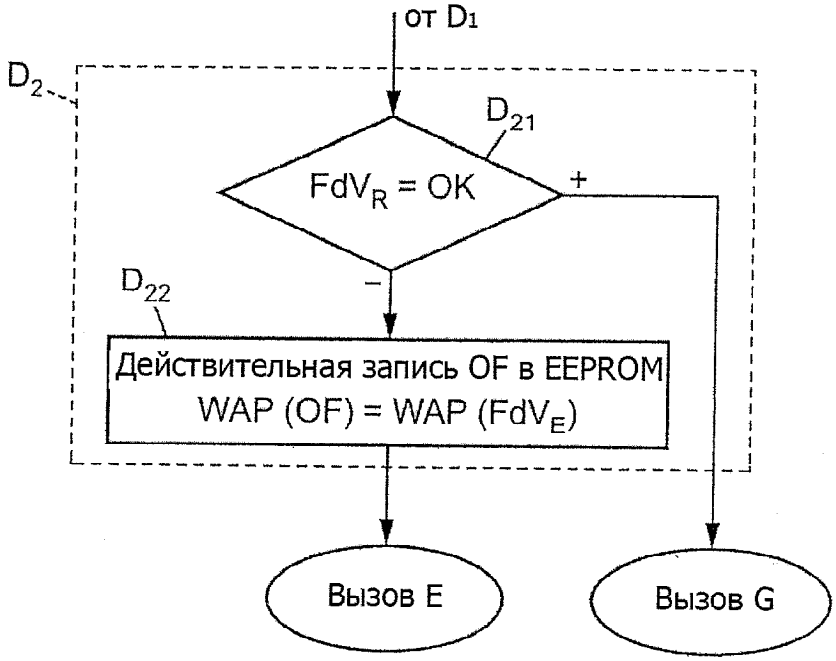
Фиг. 1b



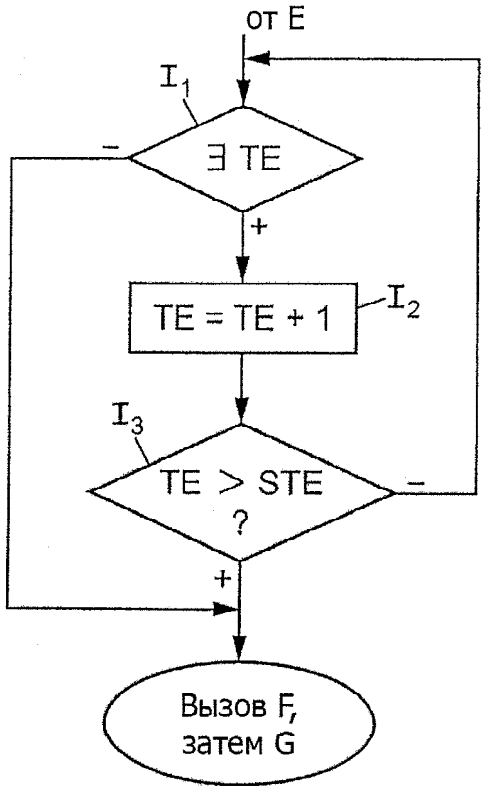
Фиг. 1c



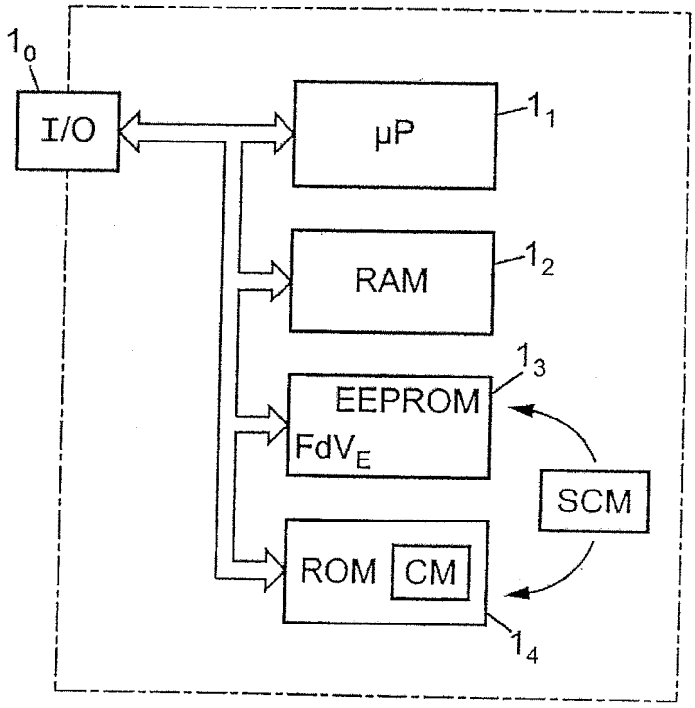
Фиг. 1d


от D1
D2
D21
FdVR = OK
+
–
D22
Действительная запись OF в EEPROM
WAP (OF) = WAP (FdVE)
Вызов E
Вызов G

Фиг. 1e


от E
I1
– ∃ TE
+
TE = TE + 1
I2
I3
TE > STE ?
–
+
Вызов F, затем G

Фиг. 1f



Фиг. 2