



(19) **RU** <sup>(11)</sup> **2 185 657** <sup>(13)</sup> **C2**  
(51) МПК<sup>7</sup> **G 06 F 12/16, 12/14**

РОССИЙСКОЕ АГЕНТСТВО  
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ**

(21), (22) Заявка: 2000111594/09, 10.05.2000

(24) Дата начала действия патента: 10.05.2000

(43) Дата публикации заявки: 10.04.2002

(46) Дата публикации: 20.07.2002

(56) Ссылки: RU 95104292 A1, 20.08.1996. RU 2067313 C1, 27.09.1997. US 5949876 A, 07.09.1999. US 6003135 A, 14.12.1999. US 5361359 A, 01.11.1994.

(98) Адрес для переписки:  
197101, Санкт-Петербург, Большой пр-т П.С.,  
53, кв.14, А.Ю.Щеглову

(71) Заявитель:

Щеглов Андрей Юрьевич

(72) Изобретатель: Щеглов А.Ю.

(73) Патентообладатель:

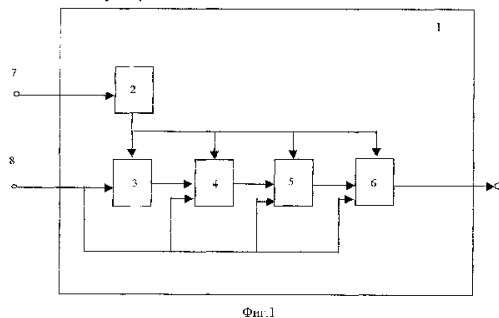
Щеглов Андрей Юрьевич

(54) **СИСТЕМА ЗАЩИТЫ И КОНТРОЛЯ ЦЕЛОСТНОСТИ РЕЗИДЕНТНОЙ ПРОГРАММЫ**

(57)

Изобретение относится к вычислительной технике, а именно к информационным вычислительным системам и сетям, и может быть использовано для защиты информационных ресурсов в рабочих станциях, информационных и функциональных серверах. Техническим результатом является обеспечение непрерывного контроля целостности (корректности функционирования) резидентно запущенной программы, в качестве которой, в частности, может использоваться программный комплекс защиты информации, что приведет к повышению уровня защищенности системы. Поставленная цель достигается тем, что система содержит программную компоненту системы контроля

целостности, аппаратную компоненту системы контроля целостности, содержащую блок аутентификации резидентной программы, блок контроля и управления, блок отключения внешних устройств. 5 ил.





(19) **RU** <sup>(11)</sup> **2 185 657** <sup>(13)</sup> **C2**  
(51) Int. Cl.<sup>7</sup> **G 06 F 12/16, 12/14**

RUSSIAN AGENCY  
FOR PATENTS AND TRADEMARKS

(12) **ABSTRACT OF INVENTION**

(21), (22) Application: 2000111594/09, 10.05.2000  
(24) Effective date for property rights: 10.05.2000  
(43) Application published: 10.04.2002  
(46) Date of publication: 20.07.2002  
(98) Mail address:  
197101, Sankt-Peterburg, Bol'shoj pr-t P.S.,  
53, kv.14, A.Ju.Shcheglovu

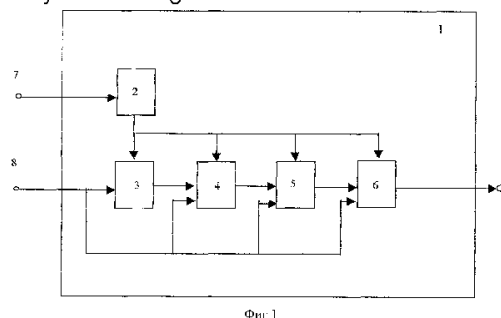
(71) Applicant:  
Shcheglov Andrej Jur'evich  
(72) Inventor: Shcheglov A.Ju.  
(73) Proprietor:  
Shcheglov Andrej Jur'evich

(54) **RESIDENT-SOFTWARE INTEGRITY CONTROL AND PROTECTION SYSTEM**

(57) Abstract:

FIELD: computer engineering; data computing systems and networks. SUBSTANCE: system designed for protecting data resources in workstations, information and functional servers to render continuous integrity control (checking for normal functioning) of resident-run program which may be, for example, data-protection software complex has program component of integrity control system, hardware arrangement of integrity control system incorporating resident-software authentication unit, monitoring and control unit, and turn-off unit for peripheral

devices. EFFECT: enhanced protective level of system. 5 dwg



Изобретение относится к вычислительной технике, а именно к информационным вычислительным системам и сетям, и может быть использовано для защиты информационных ресурсов в рабочих станциях, информационных и функциональных серверах.

Техническим результатом является программно-аппаратный комплекс защиты запущенной на компьютере резидентной программы (в частности программного комплекса защиты информации), при условии, что компьютер может функционировать лишь при корректно функционирующей на нем резидентной программе, в качестве которой, например, может выступать программный комплекс защиты информации, в частности система контроля целостности файлов.

Известен способ контроля целостности информации, реализуемого при загрузке системы. Подобный способ контроля целостности информации реализован, например, в операционной системе Windows NT Server 4.0 (см. кн. Валда Хиллей. Секреты Windows NT Server 4.0. - К.: Диалектика, 1997, с. 14-15). Подобный способ заключается в нахождении контрольных сумм контролируемых файлов при загрузке системы и в сравнении подсчитанных и эталонных контрольных сумм. При несовпадении соответствующих контрольных сумм на экран выводится сообщение о нарушении целостности соответствующей информации.

Наиболее близкой по технической сущности к заявляемой (прототипом) является система защиты информационных ресурсов вычислительной системы и сети Secret Net (см. "Система разграничения доступа Secret Net. Руководство пользователя, 1996"). Она представляет собой программный комплекс, устанавливаемый на автономный компьютер, либо на компьютеры, объединенные в вычислительную сеть. Система решает, в частности, задачу контроля целостности (неискаженности) файлов.

Система представлена на фиг.1. Система (программный комплекс) 1 содержит блок управления 2, блок проверки целостности по длинам файлов 3, по контрольным суммам файлов 4, по прочим параметрам объектов 5, блок выработки результатов 6, управляющий вход запуска контроля 7, вход данных контроля 8, управляющий выход 9, причем вход блока управления 2 соединен с входом запуска контроля 7, выход - с первыми входами блока проверки целостности по длинам файлов 3, по контрольным суммам файлов 4, по прочим параметрам объектов 5, блока выработки результатов 6, третий вход блока проверки целостности по контрольным суммам файлов 4, по прочим параметрам объектов 5, блока выработки результатов 6 соединены со вторым входом блока проверки целостности по длинам файлов 3, с входом данных контроля 8, выход блока проверки целостности по длинам файлов 3 соединен со вторым входом блока проверки целостности по контрольным суммам файлов, выход которого - со вторым входом блока проверки целостности по прочим параметрам объектов 6, выход которого - со вторым входом блока выработки результатов 6, выход которого - с управляющим выходом 9.

Работает система следующим образом. При получении команды на выполнение контроля на вход 7, блок управления 2 передает соответствующие инструкции блокам проверки целостности 3, 4, 5, блоку выработки результатов 6. Блоки 3, 4, 5 сканируют файловую систему и получают со входа 8 информацию о текущем состоянии файловой системы. Затем блоками 3, 4, 5 осуществляется сравнение полученной и соответственно хранимой ими эталонной информации, результаты сравнения передаются в блок выработки результата 6, в котором формируется реакция (команда) на обнаруженное искажение целостности файла, выдаваемая на выход 9.

К недостаткам системы может быть отнесено то, что ею контролируется лишь файловая система и не контролируется целостность (неискаженность) собственно системы контроля 1, запущенной как резидентной программы (сервис). Другими словами прототипом - программным комплексом защиты, не гарантируется контроль, так как данная программа может быть удалена, соответственно с нарушением функций защиты файлов. При этом можно либо удалить программу защиты, либо запустить операционную систему с внешнего носителя без такой программы. Задача контроля целостности резидентно запущенной программы, в частности программного комплекса контроля целостности файлов, не решается, что не может обеспечить высокого уровня защищенности функционирования системы.

Целью изобретения является разработка системы (программно-аппаратного комплекса), обеспечивающей непрерывный контроль целостности (корректности функционирования) резидентно запущенной программы, в качестве которой в частности может использоваться программный комплекс защиты информации, что приведет к повышению уровня защищенности системы.

Поставленная цель достигается тем, что в систему, содержащую программную компоненту системы контроля целостности, содержащую блок управления, причем его вход соединен с управляющим входом запуска контроля, дополнительно введены аппаратная компонента системы контроля целостности, содержащая блок аутентификации резидентной программы, блок контроля и управления, блок отключения внешних устройств, причем первые М выходов блока управления программной компоненты системы контроля целостности соединены с М выходами аутентификации резидентной программы программной компоненты системы контроля целостности, (М+1)-й выход - с выходом контроля целостности, первые М входов блока аутентификации резидентной программы аппаратной компоненты системы контроля целостности соединены с М входами аутентификации резидентной программы аппаратной компоненты системы контроля целостности, (М+1)-й вход - со входом контроля целостности, вторые М входов с М входами задания пароля аппаратной компоненты системы контроля целостности, выход - со вторым входом блока отключения внешних устройств, с первым входом блока контроля и управления, первый выход

которого - с (2M+2)-м входом блока аутентификации резидентной программы, второй вход блока контроля и управления - с первым входом блока отключения внешних устройств, со входом "Сброс (Reset)", третьи L входов - с L входами задания периода контроля, третий вход блока отключения внешних устройств соединен со входом подачи питающего напряжения на внешние устройства, четвертый вход - с третьим выходом блока контроля и управления, второй выход которого - с выходом "Сброс (Reset)", R выходов блока отключения внешних устройств соединены с R выходами подачи питания на внешние устройства, M выходов аутентификации резидентной программы программной компоненты системы контроля целостности соединены с соответствующими M входами аутентификации резидентной программы аппаратной компоненты системы контроля целостности, выход контроля целостности программной компоненты системы контроля целостности соединен со входом контроля целостности аппаратной компоненты системы контроля целостности.

Схема система защиты и контроля целостности резидентной программы представлена на фиг.2. Она содержит программную компоненту системы контроля целостности 1, аппаратную компоненту системы контроля целостности 2, программная компонента системы контроля целостности 1, содержит блок управления 3, причем его вход соединен с управляющим входом запуска контроля 4, первые M выходов блока управления 3 программной компоненты системы контроля целостности 1 соединены с M выходами аутентификации резидентной программы 5 программной компоненты системы контроля целостности 1, (M+1)-й выход - с выходом контроля целостности 6, аппаратная компонента системы контроля целостности 2 блок аутентификации резидентной программы 7, блок контроля и управления 8, блок отключения внешних устройств 9, первые M входов блока аутентификации резидентной программы 7 аппаратной компоненты системы контроля целостности 2 соединены с M входами аутентификации резидентной программы 10 аппаратной компоненты системы контроля целостности 2, (M+1)-й вход - со входом контроля целостности 11, вторые M входов с M входами задания пароля 12 аппаратной компоненты системы контроля целостности 2, выход - со вторым входом блока отключения внешних устройств 9, с первым входом блока контроля и управления 8, первый выход которого - с (2M+2)-м входом блока аутентификации резидентной программы 7, второй вход блока контроля и управления 8 - с первым входом блока отключения внешних устройств 9, со входом "Сброс (Reset)" 14, третьи L входов - с L входами задания периода контроля 13, третий вход блока отключения внешних устройств 9 соединен со входом подачи питающего напряжения на внешние устройства 15, четвертый вход - с третьим выходом блока контроля и управления 8, второй выход которого - с выходом "Сброс (Reset)" 16, R выходов блока отключения внешних устройств 9 соединены с R выходами подачи питания на внешние устройства 17, M

выходов аутентификации резидентной программы 5 программной компоненты системы контроля целостности 1 соединены с соответствующими M входами аутентификации резидентной программы 10 аппаратной компоненты системы контроля целостности 2, выход контроля целостности 6 программной компоненты системы контроля целостности 1 соединен со входом контроля целостности 11 аппаратной компоненты системы контроля целостности 2.

Работает система следующим образом. Программная компонента системы контроля целостности 1 встраивается в ту резидентную программу, контроль целостности которой необходимо контролировать, например в программный комплекс защиты информации. Аппаратная компонента системы контроля целостности 2 реализуется на плате, встраиваемой в слот компьютера. При этом крышка компьютера должна быть надежно закрыта и компьютер опечатан, во избежание удаления платы из слота. Питающее напряжение на все внешние носители (дисковод, сидиром и т.д.), кроме винчестера, подаются на данные устройства с соответствующего выхода 17 аппаратной компоненты системы контроля целостности 2, куда оно подается со входа 15. В функции блока отключения внешних устройств 9 входит обеспечения возможности загрузки системы с того носителя, где располагается контролируемая программа - программная компонента системы контроля целостности 1 (винчестер), остальные внешние носители в исходном состоянии отключены. При включении системы, а также в нормальном режиме ее функционирования на вход 4 программной компоненты системы контроля целостности 1 подается периодический сигнал (например, с использованием встроенных часов) контроля целостности, по которому устройство управления 3 сначала выдает M разрядный код (пароль) на выходы 5, затем сигнал контроля целостности на выход 6. Пароль необходим для того, чтобы функцию контроля целостности не могла перехватить подставленная злоумышленником программа. Пароль со входов 10 поступает на блок аутентификации резидентной программы, куда эталонное значение пароля подается (например, перемычками на плате) с соответствующих входов 12. По сигналу контроля целостности осуществляется аутентификация резидентной программы и при положительном исходе управляющий сигнал передается в блок контроля и управления 8. В функции данного блока входит следующее - осуществлять периодический контроль целостности резидентной программы (поступления от нее сигналов), в случае нарушения целостности - перевод компьютера в нерабочий режим, а также управление внешними устройствами. Получив первый сигнал от блока 7 блок 8 сигнализирует ему, что контроль прошел успешно. Этим же сигналом с блока 7, поступающим на блок 9, разблокируются внешние устройства (на них с соответствующих входов 17 подается питание), компьютер переводится в штатный режим функционирования. Со входов 13 в блок 8 подается период контроля (например, перемычками на плате). Этот период должен превосходить период контроля целостности,

задаваемый со входа 4. Если за период, задаваемый со входов 13, программная компонента системы контроля целостности 1 передала сигнал (с предварительной аутентификацией), компьютер остается в штатном режиме, в противном случае блок контроля и управления 8 формируется сигнал "Сброс (Reset)" на выходе 16 и одновременно размыкает внешние устройства с выхода 17, после чего компьютер может быть включен лишь посредством загрузки операционной системы с винчестера, при условии, что одновременно загружается и контролируемая резидентная программа, в противном случае опять будет выработан сигнал сброса. Входным сигналом "Сброс (Reset)" система штатно переводится в исходное состояние.

Таким образом, заявляемая система обеспечивает защиту и непрерывный контроль целостности резидентной программы, что является необходимым условием функционирования программных комплексов защиты информации, таких как программ шифрования, программ защиты от НСД и т.д., т.к. данная система обеспечивает гарантии невозможности функционирования компьютера без защищаемой программы, при условии, что из компьютера не будет удалена аппаратная компонента системы (платы), противодействие чему достигается уже организационными мероприятиями.

Блоки, используемые в заявляемой системе, могут быть реализованы следующим образом.

Блок 3 представляет собой программу, реализующую передачу пароля и сигнала контроля в заданные интервалы времени.

Блок 7 может быть реализован, например, по схеме, представленной на фиг. 3. Блок 7 содержит регистр 7.1 и схему сравнения 7.2, причем М информационных входов регистра соединены с первыми М входами 7.3 блока 7 (с М входами 10 системы), (М+1)-й вход - с (М+1)-й входом блока 7 (с 11 входом системы), (М+2)-й вход регистра (вход R) - с (2М+2)-м входом 7.7 блока 7 (с первым выходом 8.9 блока 8, см. фиг.4), М выходов регистра 7.1 - с первыми М входами схемы сравнения 7.2, вторые М входов которой - с со вторыми М входами 7.5 блока 7 (с М входами 12 системы), выход схемы сравнения 7.2 соединен с выходом 7.6 блока 7 (с первым входом 8.6 блока 8, см. фиг.4, со вторым входом 9.4 блока 9, см. фиг.5). Работает блок следующим образом. Выставленное на М входов 7.3 значение пароля сигналом со входа 7.4 заносится в регистр 7.1, при его совпадении со значениями, присутствующими на М входах 7.5 схема сравнения 7.2 вырабатывает сигнал на выход 7.6. Сигналом со входа 7.7 содержимое регистра обнуляется.

Блок 8 может быть реализован, например, по схеме, представленной на фиг. 4. Блок 8 содержит генератор 8.1, элемент ИЛИ 8.2, счетчик 8.3, схему сравнения 8.4, элемент ИЛИ 8.5, причем выход генератора 8.1 соединен с первым входом счетчика 8.3, второй вход которого - с первым выходом 8.9 блока 8 (с (2М+2)-м входом 7.7 блока 7, см. фиг.3), с выходом элемента ИЛИ 8.2, первый вход которого - с первым входом 8.6 блока 8 (с выходом 7.6 блока 7, см. фиг. 3), второй вход - со вторым входом элемента ИЛИ 8.5, со вторым входом 8.8 блока 8 (выходом

системы 14), L выходов счетчика 8.3 соединены с первыми L входами схемы сравнения 8.4, вторые L входов которой - с третьими L входами 8.7 блока 8 (L входами системы 13), выход схемы сравнения 8.4 - с третьим выходом 8.11 блока 8 (с четвертым входом 9.5 блока 9, см. фиг.5), выход элемента ИЛИ 8.5 соединен со вторым выходом 8.10 блока 8 (с выходом системы 16). Работает блок следующим образом. Генератор 8.1 выдает меандр импульсов, подсчитываемых счетчиком 8.3. Сигнал со входа 7.6 обнуляет содержимое счетчика (сигнал контроля со схемы сравнения 7.2). Схемой сравнения 8.4 сравнивается текущее содержимое счетчика 8.3 и заданное с L входов 8.7 (13) эталонное значение. При совпадении схемой сравнения 8.4 вырабатывается сигнал, образующий сигнал "Сброс (Reset)" на выходе 8.10 (16) и сигнал для отключения внешних устройств, поступающий на выход 8.11. Входной сигнал "Сброс (Reset)" со входа 8.8 (14) обнуляет счетчик 8.3, с выхода 8.9 подается в блок 7, с выхода 8.10 передается далее. Сигнал со входа 8.6 служит для возвращения блока 7 в исходное состояние в штатном режиме функционирования.

Блок 9 может быть реализован, например, по схеме, представленной на фиг. 5. Блок 9 содержит элемент ИЛИ 9.1, триггер 9.2, реле 9.3, причем первый вход триггера 9.2 соединен со вторым входом 9.4 блока 9 (с первым выходом 7.6 блока 7, см. фиг. 3), второй вход - с уровнем высокого потенциала (логическая "1"), третий вход - 6 с выходом элемента ИЛИ 9.1, первый вход которого - с четвертым входом 9.5 блока 9 (с третьим выходом 8.11 блока 8, см.фиг.4), второй вход - с первым входом 9.6 блока 9 (со входом системы 14), первый вход реле 9.3 соединен с третьим входом 9.7 блока 9 (со входом системы 15), второй вход - с выходом триггера 9.2, R выходов реле 9.3 - с R выходами 9.8 блока 9 (с R выходами системы 17). Работает блок следующим образом. В исходном состоянии триггер 9.2 находится в нулевом состоянии и реле 9.3 разомкнуто, на всех R выходы 9.8 напряжение со входа 9.7 не пропускается. Сигналом со второго входа 9.4 блока (успешно проведена аутентификация резидентной программы) триггер устанавливается в единичное состояние - после подтверждения целостности резидентной программы подключаются внешние устройства - подается напряжение на R выходы 9.8. Сбрасывается в ноль триггер 9.2 (отключаются внешние устройства) при двух условиях - общей командой "Сброс (Reset)" со входа 9.6, либо сигналом со входа 9.5 блока управления и контроля 8, сообщаящим блоку 9 о том, что за заданный интервал времени контроля целостности резидентной программы не осуществлено.

К достоинствам предлагаемой системы может быть отнесено следующее:

1. Система осуществляет непрерывный контроль целостности (в данном случае подтверждаемый работоспособностью) резидентно запущенной программы в процессе всего времени функционирования системы.

2. Система гарантирует невозможность, во-первых, функционирования при снятии

(уничтожении) контролируемой программы, во-вторых, при попытке загрузки без контролируемой программы.

3. За счет реализации аппаратной компоненты системы контроля, при ее встраивании в слот компьютера, система обеспечивает невозможность преодоления защиты без физического удаления аппаратной компоненты (платы) из слота, т.е. без снятия корпуса компьютера.

4. Система отличается универсальностью в том смысле, что ее программная компонента может встраиваться в любую контролируемую резидентную программу, практически без ограничений, в том числе в программные комплексы защиты компьютера от НСД и шифрования данных.

#### Формула изобретения:

Система защиты и контроля целостности резидентной программы, содержащая программную компоненту системы защиты и контроля целостности резидентной программы, содержащую блок управления, причем его вход соединен с управляющим входом запуска контроля, отличающаяся тем, что содержит аппаратную компоненту системы защиты и контроля целостности резидентной программы, содержащую блок аутентификации резидентной программы, блок контроля и управления, блок отключения внешних устройств, причем первые М выходов блока управления программной компоненты системы защиты и контроля целостности резидентной программы соединены с М выходами аутентификации резидентной программы программной компоненты системы защиты и контроля целостности резидентной программы, (М+1)-й выход - с выходом контроля целостности, первые М входов блока аутентификации резидентной программы аппаратной

компоненты системы защиты и контроля целостности резидентной программы соединены с М входами аутентификации резидентной программы аппаратной компоненты системы защиты и контроля целостности резидентной программы, (М+1)-й вход - с входом контроля целостности, вторые М входов - с М входами задания пароля аппаратной компоненты системы защиты и контроля целостности резидентной программы, выход - с вторым входом блока отключения внешних устройств, с первым входом блока контроля и управления, первый выход которого - с (2М+2)-м входом блока аутентификации резидентной программы, второй вход блока контроля и управления - с первым входом блока отключения внешних устройств, с входом "Сброс (Reset)", третьи L входов - с L входами задания периода контроля, третий вход блока отключения внешних устройств - с входом подачи питающего напряжения на внешние устройства, четвертый вход - с третьим выходом блока контроля и управления, второй выход которого - с выходом "Сброс (Reset)", R выходов блока отключения внешних устройств соединены с R выходами подачи питания на внешние устройства, М выходов аутентификации резидентной программы программной компоненты системы защиты и контроля целостности резидентной программы - с соответствующими М входами аутентификации резидентной программы аппаратной компоненты системы защиты и контроля целостности резидентной программы, выход контроля целостности программной компоненты системы защиты и контроля целостности резидентной программы соединен с входом контроля целостности аппаратной компоненты системы защиты и контроля целостности резидентной программы.

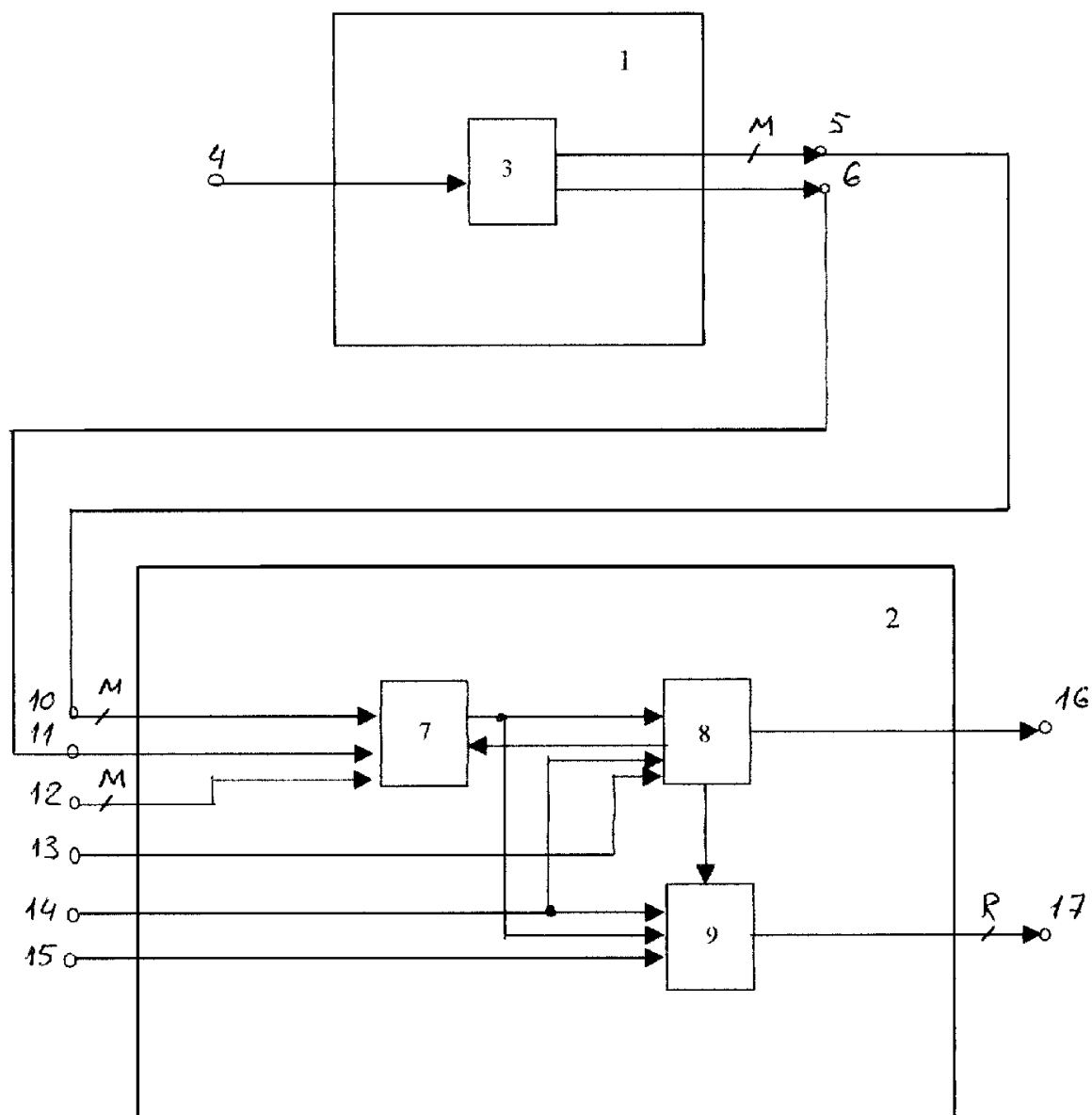
40

45

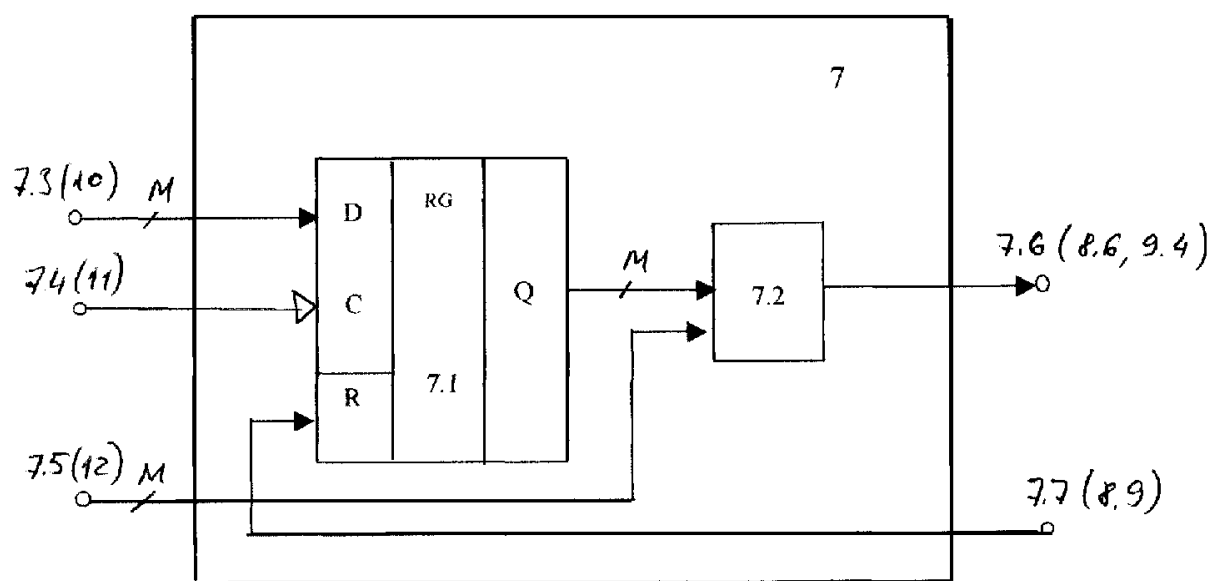
50

55

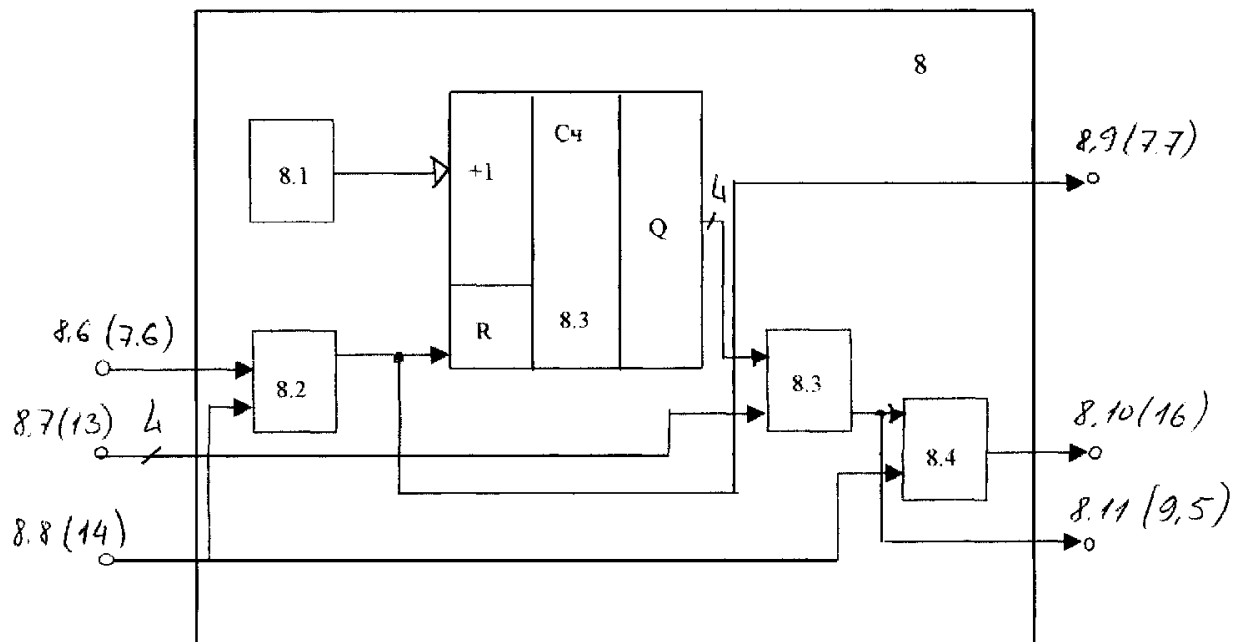
60



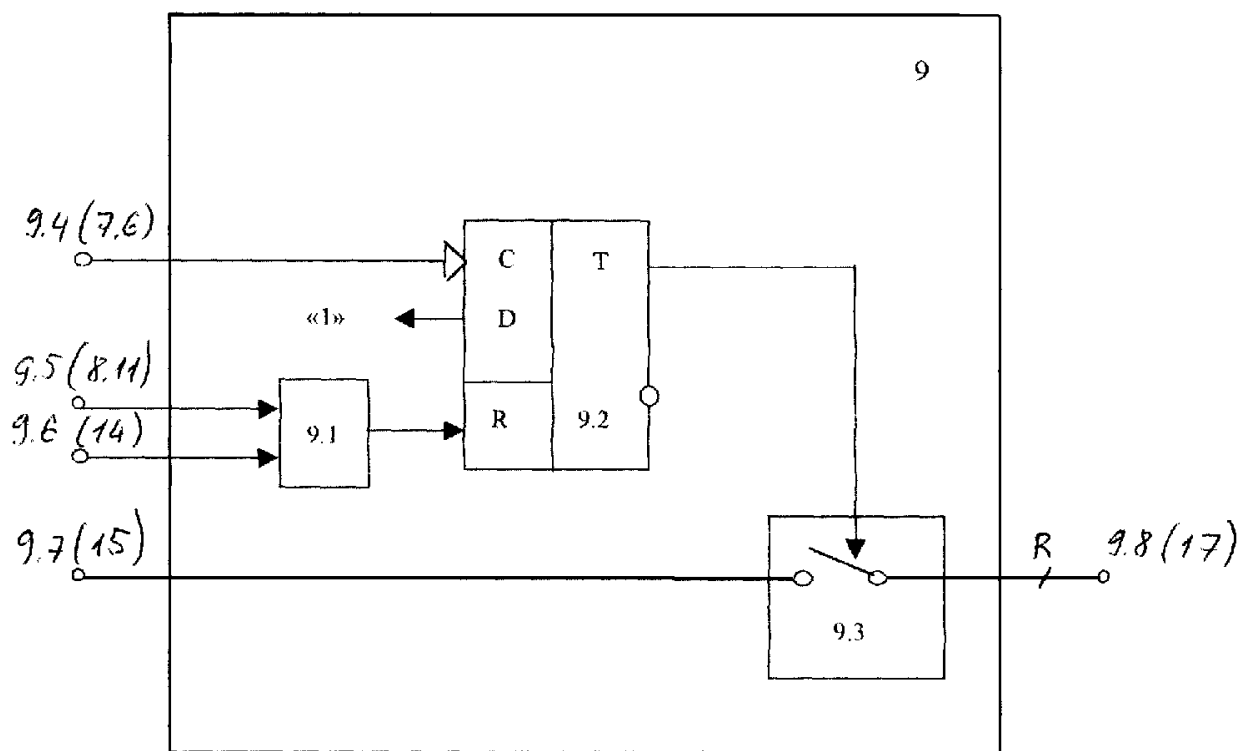
Фиг.2



Фиг.3



Фиг.4



Фиг.5