



(19) **RU** ⁽¹¹⁾ **2 144 737** ⁽¹³⁾ **C1**
(51) МПК⁷ **H 04 L 12/22, H 04 M 17/02**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

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

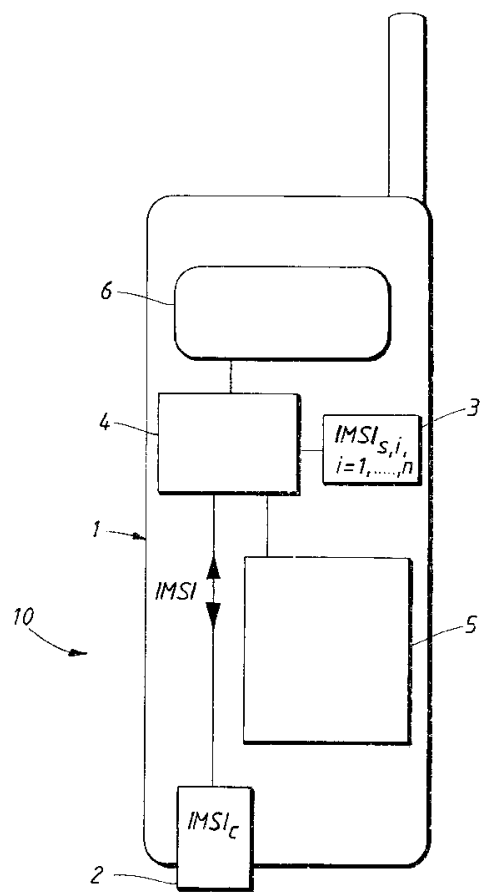
(21), (22) Заявка: 93050169/09, 05.11.1993
(24) Дата начала действия патента: 05.11.1993
(30) Приоритет: 09.11.1992 SE 9203351-3
(46) Дата публикации: 20.01.2000
(56) Ссылки: EP 0301740 A2, 01.02.89. US 5168520 A, 01.12.92. US 4679236 A, 07.07.87. DE 4138861 A1, 01.10.92. SU 1127103 A, 30.11.84.
(98) Адрес для переписки:
129010, Москва, ул.Б. Спасская, 25, стр.3,
ООО "Городисский и партнеры", Емельянову
Е.И.

(71) Заявитель:
Эрикссон Джи-И Мобил Коммьюникейшнз Инк.
(US)
(72) Изобретатель: Матс Олоф Барвестен (SE)
(73) Патентообладатель:
Эрикссон Джи-И Мобил Коммьюникейшнз Инк.
(US)

(54) **УСТРОЙСТВО КОНТРОЛИРУЕМОГО ДОСТУПА К СЛУЖБАМ ОБМЕНА ИНФОРМАЦИЕЙ**

(57) Реферат:
Изобретение относится к устройству для оказания услуг, например, телефонной связи, передачи данных, содержащему терминальный блок и блок доступа, при этом терминальный блок содержит средства (ПИН_t) идентификации терминального блока, который хранится в терминальном блоке, а блок доступа содержит средства (ММИА) идентификации доступа в форме кода или его аналога, причем терминальный блок и блок доступа блокируемы. В терминальном блоке, кроме того, имеются первые средства идентификации доступа для заданного количества блоков доступа (МИА), хранимые в нем при пуске устройства, включающем контакт между терминальным блоком, блоком (МИА) доступа с определенными средствами

(ММИА_c) идентификации доступа к блоку, причем код средств (ММИА_c) идентификации блока доступа сравнивается с хранимым в терминальном блоке кодом (кодами для средств (ММИА_s) идентификации доступа в терминальном блоке, а соответствие между хранимыми средствами (ММИА_s) идентификации доступа и средствами (ММИА_c) идентификации доступа к блоку приводит к разблокированию терминального блока, а при несоответствии между ними соответственно должен быть задан по меньшей мере код (ПИН_t) идентификации терминального блока. Технический результат, достигаемый при реализации данного устройства состоит в обеспечении защиты от злоумышленников и быстрого и легкого доступа для пользователей. 14 з.п. ф-лы, 2 ил.



Фиг. 1



(19) **RU** ⁽¹¹⁾ **2 144 737** ⁽¹³⁾ **C1**
 (51) Int. Cl.⁷ **H 04 L 12/22, H 04 M 17/02**

RUSSIAN AGENCY
 FOR PATENTS AND TRADEMARKS

(12) **ABSTRACT OF INVENTION**

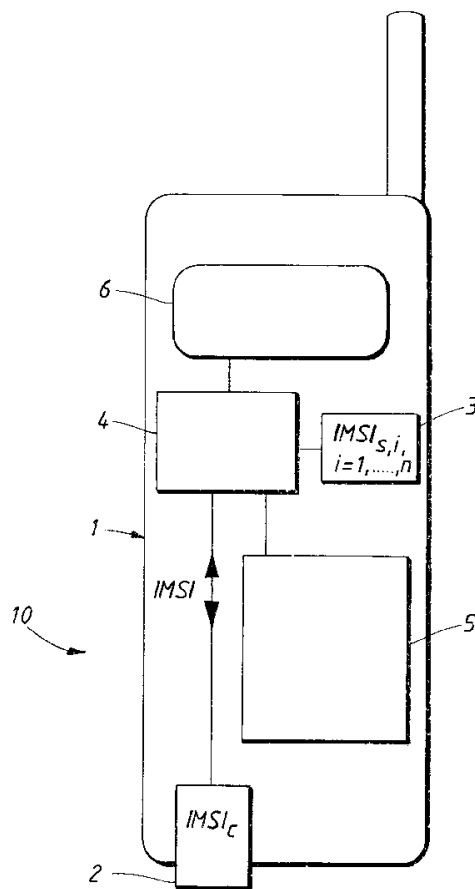
(21), (22) Application: 93050169/09, 05.11.1993
 (24) Effective date for property rights: 05.11.1993
 (30) Priority: 09.11.1992 SE 9203351-3
 (46) Date of publication: 20.01.2000
 (98) Mail address:
 129010, Moskva, ul.B. Spasskaja, 25, str.3,
 OOO "Gorodisskij i partnery", Emel'janovu E.I.

(71) Applicant:
 Ehrikson Dzhi-I Mobil Komm'juniquejshnz Ink. (US)
 (72) Inventor: Mats Olof Barvesten (SE)
 (73) Proprietor:
 Ehrikson Dzhi-I Mobil Komm'juniquejshnz Ink. (US)

(54) **DEVICE FOR AUTHORIZED ACCESS TO INFORMATION EXCHANGE SERVICES**

(57) Abstract:

FIELD: service providers, for example, of telephone communication, data transmission, and so on. SUBSTANCE: device has terminal assembly and access assembly. Terminal assembly has terminal assembly identification units. Access assembly has units for access identification which is provided by a password or a similar mechanism. Access to terminal and access assemblies can be locked. In addition terminal assembly has first access identification units for given number of access assemblies, which are stored in it upon starting device including connection of terminal assembly and access assemblies to specific assembly access identification units. Passwords of specific assembly identification units are compared to password or passwords which are stored in terminal assembly. Matching of stored access identification units to specific access identification units results in unlocking terminal assembly. Otherwise, at least one terminal assembly identification unit password should be entered. EFFECT: protection against malicious access, fast and facilitated access for legal users. 15 cl, 2 dwg



Фиг. 1

RU 2 144 737 C1

RU 2 144 737 C1

Изобретение относится к службам обмена информацией. Подобные устройства могут быть объектом злоупотреблений, имеющих серьезные последствия. Это относится к случаям, когда блоки доступа либо терминальные блоки не блокированы или не имеют блокировки, что делает проблематичным их применение пользователями, которые реально могли бы иметь доступ к одному или другому блокам. Это, например, относится к случаю с мобильными телефонами, когда абонентное обслуживание не связано с конкретным мобильным телефоном или терминальным блоком, но связано с отдельной картой. При этом терминальный блок или телефон могут быть использованы с любой картой. Если, с другой стороны, блок доступа или карта не блокированы, любое лицо может использовать карту и через нее также осуществлять абонентное обслуживание. Одним из путей решения этой проблемы, т.е. защиты терминального блока, а также блока доступа, является использование "запора" в терминальном блоке, а также в блоке доступа, при котором пользователь должен вводить код для "разблокирования" терминального блока и другой код для "заблокирования" карты, таким образом обеспечивая доступ к абонентному обслуживанию. Однако этот путь трудоемок ввиду того, что два различных кода должны быть введены каждый раз при использовании, что очень неудобно, поскольку, помимо прочего, затруднительно запомнить возрастающее количество кодов, которые необходимы для установления связи, и также поскольку ввод двух кодов каждый раз отнимает много времени. Следовательно, велика вероятность того, что пользователь не задействует один или другой код, либо, в худшем случае, оба идентифицирующих кода для возможности получения быстрого доступа к его телефону, в результате чего возникает риск недобросовестного использования или кражи устройства или одного из блоков, содержащихся в устройстве либо установке.

Устройства, рассмотренные выше, известны. Однако, как упоминалось, они подвержены недостатку, заключающемуся в том, что в указанных устройствах должны быть введены два различных кода при каждой активации терминала, либо они должны иметь блокировку терминала, либо карты или блока доступа. Это, например, имеет место в случае с цифровой системой наземного технического обслуживания (НТО) (GSM - ground - support maintenance). В этой системе абонентное обслуживание представлено на отдельной так называемой карте модуля идентификации абонента (МИА) (SIM - Subscriber Identity Module). В этом случае терминальный блок или телефон слабо защищены от злоумышленников, поскольку карта МИА, которая должна иметь доступ к телефону, просто может быть обменена на другую карту МИА и при этом телефон может быть легко использован пользователями, которые не могли бы в этом случае иметь доступа к телефону. Это, в частности, случается, когда терминальные блоки предназначены для использования конкретным пользователем, либо конкретной группой пользователей, или когда терминал достаточно просто украсть. В известном устройстве блок доступа или карта МИА содержит так называемый код

персонального идентификационного номера (ПИН) (PIN - Personal Identification Number), или средство идентификации терминального блока, при этом терминальный блок или телефон, в свою очередь, содержит другой ПИН-код, так что для осуществления полной защиты терминального блока (телефона), а также блока доступа (карты) оба кода должны быть введены при каждой активации терминального блока или телефона. Это приводит соответственно к очень неудобному манипулированию устройством.

С другой стороны в известных аналоговых мобильных телефонных системах абонентное обслуживание запрограммировано внутри телефонного терминала. Это было сделано со специальным оборудованием и управляется авторизованным персоналом, который различался и контролировался оператором, следовательно, аналогичные проблемы не возникают в этом случае.

В основу настоящего изобретения положена задача создания оборудования для служб, в котором терминальный блок, а также блок доступа имеют защиты и не могут быть легко использованы злоумышленниками, с учетом того, что устройство легко использовать и в обычном случае не требуется двойного введения кодов, и в котором главное преимущество заключается в отсутствии необходимости ввода кодов для обеспечения доступа владельца или приватизированного пользователя без ущерба. Устройство призвано также обеспечивать быстрый и легкий доступ для одного или нескольких пользователей в зависимости от ситуации.

Кроме того, устройство призвано обеспечить информацию услуг относительно идентификационного номера (например, телефонного номера) или кодов, принадлежащих блокам доступа, которые имели упрощенный доступ. Эта цель достигалась за счет характеристик, которые даны в пункте 14 формулы изобретения.

Поставленная задача решается совокупностью существенных признаков главного пункта формулы.

В дальнейшем изобретение поясняется описанием вариантов его выполнения со ссылками на чертежи, на которых:

Фиг. 1 изображает схему терминального блока и блока доступа в форме телефона с картой;

Фиг. 2 - пример технологической диаграммы с этапами, которые даны через активацию терминала для "блокирования" терминального блока, а также блока доступа (в иллюстрированном примере телефона и карты).

В предпочтительном примере осуществления, показанном на фиг. 1, показаны устройство или установка 10, в которой терминальный блок содержит мобильный телефон 1, а блок доступа содержит электронную карту 2, имеющую абонентное обслуживание. Устройство далее содержит кнопочный блок 5, память 3 и микропроцессорный блок 4. На дисплее 6 среди других индикаций показаны телефонные номера. В приведенном предпочтительном примере осуществления устройство относится к сотовой так называемой НТО-мобильной телефонной

системе, в частности, к системе CME-20 (фирма Эриксон). В этом контексте также рассматривались рекомендации 11.11 НТО. В приведенном предпочтительном примере осуществления карта 2 с электронной памятью содержит так называемую ММИА-карту (модуль идентификации абонента), далее описанную в рекомендации 02.17 НТО, которая содержит информацию, неоднозначно идентифицирующую абонента. В ММИА-карте 2 хранится так называемый ММИА-код (IMS1-International Mobile Subscriber Identity) (международной мобильной идентификации абонента) или средство идентификации доступа к блоку. Мобильная станция (МС), которая, например, могла бы быть установлена на транспортном средстве, портативная станция либо переносная станция могут быть использованы лишь в случае присутствия значимого ММИА-кода. Для случаев, когда терминальный блок или телефон 1 не заблокированы или не защищены при помощи так называемого регистра оборудования идентификации (ПОИ) (EIR - Equipment Identity Register) (пока не используется), который может быть рассмотрен в качестве альтернативы настоящему изобретению в плане защиты, велика вероятность недобросовестного использования или кроме терминала или телефона. При пуске или активации терминального блока или телефона 1 телефон 1 или терминальный блок и ММИА-карта 2 (блок доступа) связаны один с другим. ММИА-код для ММИА-карты (карт) 2 должен храниться (хранились) в памяти телефона, например, в электрически стираемом и программируемом ПЗУ. В дальнейшем ММИА-код может храниться различными известными способами, например, полностью, частично, не шифрованным или шифрованным, случайно набранным, сформированным калькуляцией остатка либо другим способом. Хранение производится либо автоматически, либо вручную. В соответствии с преимуществами предпочтительного примера осуществления настоящего изобретения возможно, помимо хранения объекта, тождественного собственно ММИА-карте, т. е. ее ММИА-кода, также можно хранить ММИА-коды нескольких других ММИА-карт, которые должны иметь упрощенный или приоритетный доступ к терминальному блоку или телефону 1.

На примере технологической диаграммы, представленной на фиг. 2, в частности, будет описана следующая последовательность операций, при которой в результате хранения одного или нескольких ММИА-кодов в памяти терминального блока, а также, возможно, ПИН- и ПИН_c-кодов, терминал активирован или запущен, причем возможны различные варианты в зависимости от действительного ММИА-кода, хранимого или не хранимого.

При активации телефона, когда либо карта уже присутствует в телефоне 1, либо при введении новой карты действительный ММИА_c-код передается к телефону 1 (в соответствии с рекомендацией НТО) через микропроцессор 4, как указывалось выше, где он сравнивается с хранимым в телефоне 1 ММИА_{Si} - кодом (кодами). Если ММИА_c соответствует любому ММИА_s-коду, хранимому в телефоне 1, телефон начинает работу без необходимости применения любой

другой меры и без запроса любого другого кода. Если, с другой стороны, коды не согласуются, телефон затребует ПИН_f-код для терминального блока или телефона 1.

5 Таким образом, при возникновении любой активации телефона 1 в памяти 3 хранимый код (коды) (ММИА_{Si}) сравнивают с принятым кодом (ММИА_c) действительной ММИА-карты. Так называемый ПИН-код для карты ММИА аналогичным образом хранился в памяти 3 способом, подобным хранению ММИА-кода (кодов). В памяти 3 терминального блока (телефона), помимо одного или нескольких ММИА-кодов, имеется также ПИН_f-код, т.е. хранится персональный идентификационный номер или средство идентификации терминального блока. В соответствии с другим предпочтительным примером осуществления может, кроме того, храниться ПИН_c других карт, хранящих ММИА_c-коды, а также телефонный номер для 10 соответствующего абонентного обслуживания. Это зависит от предъявляемых к системе требований и реализуется в предпочтительных примерах осуществления. Ниже будет продолжено рассмотрение случая, когда действительный ММИА_c-код соответствует хранимому ММИА_s-коду и терминал разблокирован. После этого определяют, что действительный ПИН_c-код карты хранился. Если это 15 соответствует действительности, ПИН_c-код действительной карты считывают из памяти 3, при этом его передают на карту 2, которую после этого разблокируют, после чего разблокируют телефон 1 и карту 2, а устройство 10, заблокированное, рассматривают как готовое к использованию или открытое для связи. В этом случае, 20 соответственно, не требуется введения любого кода пользователем. (Если ПИН_c хранится и активирован, этот код запрашивается и он должен быть затем введен или задан).

Если, однако, действительный ММИА_c-код не соответствует любому хранимому ММИА_s-коду терминального блока 1 или телефона 1, запрашивают ПИН_f-код для терминала. После этого запрашивают, активирован ли ПИН_c-код для карты. Если не активирован, карту разблокируют и таким образом она остается не заблокированной. Если активирован, то запрашивают ПИН_c-код и после его задания карту разблокируют и устройство является готовым к 30 использованию, что касается блокирования. Если, с другой стороны, действительный ММИА-код соответствует хранимому ММИА_s-коду, также вероятно, что ПИН_c-код действительной карты не хранят. Терминал в этом случае, как уже упоминалось выше, был уже разблокирован. Затем проверяется, активирован ли ПИН_c-код для карты. Если активирован, он задан, при этом карта разблокирована. Если нет, карту 35 соответственно не блокируют и, следовательно, она разблокирована, а устройство готово к использованию с точки зрения блокирования. Таким образом, для авторизованного пользователя, т. е. пользователя, который должен иметь доступ к телефону, а также к карте, существует возможность не вводить любой код вовсе, 40 45 50 55 60

однако карта, а также терминал являются автоматически разблокированными. Если, однако, действительный ММИА_с-код не хранят в терминале, возможно получить доступ путем введения ПИН-кодов для терминала и карты. Эти коды могут быть связаны один с другим и, например, содержать один и тот же код.

В соответствии с предпочтительным примером осуществления по меньшей мере один ММИА_с-код, а также ПИН-коды для карты и для терминала крепят в памяти. Для устранения хранения ПИН-кодов карты также возможно, как упоминалось выше, связать их с ПИН-кодом терминала. В соответствии с предпочтительным примером осуществления имеется, однако, ПИН_с-код карты, хранимый в зашифрованной форме в памяти 3. Карты могут, например, содержать карты с электронной памятью, а также карты с магнитной памятью либо возможны другие альтернативы.

В соответствии с предпочтительным примером осуществления возможно, в случае ММИА_с-кода действительной карты, хранимого в памяти 3 терминала 1, показать, например, телефонный номер действительного абонентского обслуживания или МИА-карту, которая может быть полезна, поскольку они другим способом не видны. После разблокирования карты проверяется факт хранения телефонного номера карты в терминале. В этом случае его считывают из памяти и показывают на дисплее 6. Если телефонный номер не хранится в терминале, проверяется, что телефонный номер хранится на карте. Если это имело место, телефонный номер считывают из памяти и демонстрируют на дисплее 6. Если телефонный номер не хранят, отображение не имеет места. Отображение телефонных номеров имеет преимущество, поскольку телефонный номер другим способом не видим ни на терминальном блоке, ни на карте, и если пользователь имеет, например, несколько карт, ему может оказаться затруднительным запомнить номер подобно тому, как трудно запомнить собственный номер. Это справедливо для случая, если один или несколько телефонных номеров связаны с хранимыми ММИА-кодами.

Кроме того, возможно осуществить хранение различных кодов (ММИА, ПИН) в памяти 3 либо вручную, либо автоматически. При ручном хранении могло бы быть эффективным использование, например, так называемого клавишного устройства 5 или его аналога. Более того, существует возможность изменить хранимые коды, а также стирать коды или добавлять коды.

Настоящее изобретение не ограничено приведенными предпочтительными примерами его осуществления и может быть использовано не только в случае мобильного телефона, но и с любым устройством для оказания услуг, например, устройствами для передачи данных или другими, содержащими терминальный блок и блок доступа, например, в случае абонентского обслуживания и т.п., где желательно предохранить блоки, формирующие части устройства от ненадлежащего использования и кражи. Устройство может также содержать более двух блоков.

Формула изобретения:

5 1. Устройство контролируемого доступа к службам телефонной связи и передачи данных, содержащее терминальный блок и блок доступа, при этом терминальный блок содержит средства идентификации терминального блока, хранимые в терминальном блоке, а блок доступа содержит первые средства идентификации блока доступа в форме кода или его аналога, причем терминальный блок и блок доступа блокируемы, отличающееся тем, что 10 терминальный блок дополнительно содержит первые средства идентификации блока доступа для заданного количества (n) блоков доступа, а блок доступа содержит второе средство идентификации блока доступа, пуск терминального блока обеспечивают контактом между терминальным блоком и блоком доступа с первыми и вторым средствами идентификации блока доступа, причем код первых средств идентификации блока доступа сравнивают с кодом первых 20 средств идентификации блока доступа, хранимых в терминальном блоке, и соответствие кодов первых средств идентификации блока доступа и первых средств идентификации блока доступа, хранимых в терминальном блоке, приводит к разблокированию терминального блока, а при несоответствии кодов первых средств идентификации блока доступа и первых средств идентификации блока доступа, хранимых в терминальном блоке, задан по 30 меньшей мере код средств идентификации терминального блока.

2. Устройство по п.1, отличающееся тем, что код второго средства идентификации блока доступа задан вручную пользователем.

3. Устройство по п.1, отличающееся тем, что код второго средства идентификации 35 блока доступа также хранят в терминальном блоке, при этом терминальный блок в случае соответствия между кодом первых средств идентификации блока доступа и кодом первых средств идентификации блока доступа, хранимым в терминальном блоке, автоматически передает код второго средства идентификации блока доступа так, что устройство может быть использовано без кода второго средства идентификации блока 40 доступа, являющегося заданным пользователем.

4. Устройство по п.1, отличающееся тем, что в случае отсутствия хранения кода 45 второго средства идентификации блока доступа и при наличии соответствия между кодом первых средств идентификации блока доступа и кодом первых средств идентификации блока доступа, хранимым в терминальном блоке, блок доступа разблокирован путем ввода кода второго средства идентификации блока доступа. 50

5. Устройство по п.1, отличающееся тем, что при несоответствии между кодом первых 55 средств идентификации блока доступа и кодом первых средств идентификации блока доступа, хранимым в терминальном блоке, терминальный блок, а также блок доступа разблокированы путем задания кода идентификации терминального блока или кода второго средства идентификации блока 60 доступа.

6. Устройство по любому из пп.1, 2 или 4, отличающееся тем, что при несоответствии между кодом первых средств идентификации

блока доступа и кодом первых средств идентификации блока доступа, хранимым в терминальном блоке, код средств идентификации терминального блока, а также код второго средства идентификации блока доступа заданы.

7. Устройство по любому из пп.1 - 6, отличающееся тем, что терминальный блок содержит мобильный телефон.

8. Устройство по любому из пп.1 - 7, отличающееся тем, что блок доступа содержит карту, например, с электронной или магнитной памятью.

9. Устройство по п.8, отличающееся тем, что блок доступа содержит карту модуля идентификации абонента (МИА-карту), определяющую абонентное обслуживание мобильного телефона.

10. Устройство по любому из пп.1 - 9, отличающееся тем, что код первых средств идентификации блока доступа по меньшей мере для абонентного обслуживания, который должен иметь доступ к терминальному блоку, хранят в терминальном блоке, при этом упомянутый код идентификации хранят, например, в электрически стираемом программируемом постоянном запоминающем устройстве (ЭСППЗУ).

11. Устройство по п.10, отличающееся тем, что последующий единичный код или несколько последующих кодов второго

средства идентификации блока доступа хранят в памяти в терминальном блоке, например, в полном объеме, частично или шифрованными известным образом, а по меньшей мере один код второго средства идентификации блока доступа хранят шифрованным в памяти терминального блока.

12. Устройство по п.10 или 11, отличающееся тем, что хранение кода первых средств идентификации блока доступа происходит автоматически.

13. Устройство по п.10 или 11, отличающееся тем, что хранение кода первых средств идентификации блока доступа производят вручную, например, при помощи кнопочного блока или его аналога.

14. Устройство по любому из пп.10 - 13, отличающееся тем, что по меньшей мере код второго средства идентификации блока доступа хранят в памяти терминального блока в основном аналогично хранению кода первых средств идентификации блока доступа.

15. Устройство по любому из пп.7 - 14, отличающееся тем, что по меньшей мере один телефонный номер, относящийся по меньшей мере к одному блоку доступа, хранят либо в памяти терминального блока, либо в памяти блока доступа с возможностью его считывания из упомянутой памяти и демонстрации на дисплее при разблокировании устройства.

5

10

15

20

25

30

35

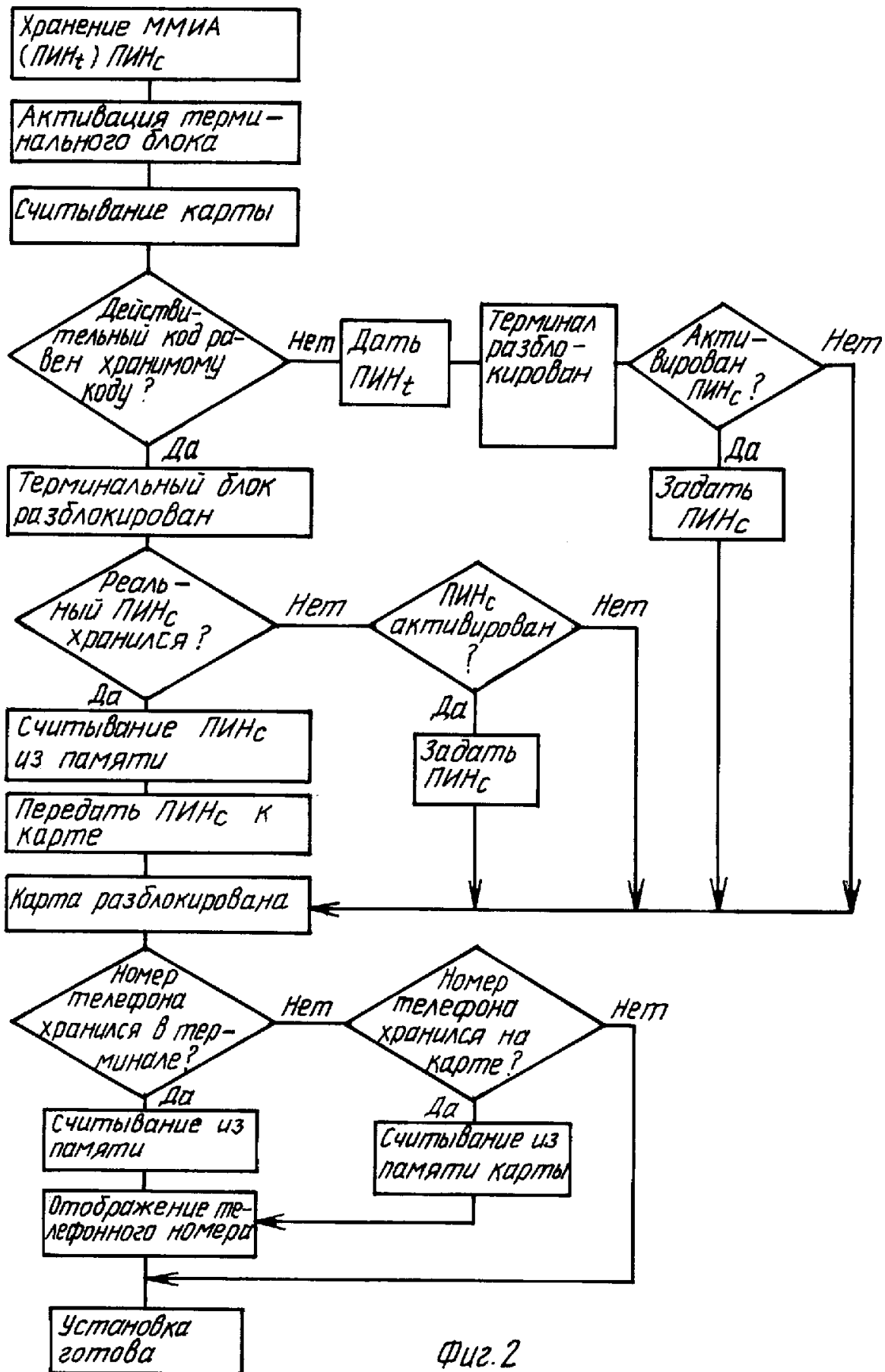
40

45

50

55

60



Фиг. 2