РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 543 935** (13) **C2**

(51) МПК
G07F 7/10 (2006.01)
G06Q 20/20 (2012.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2011148267/08, 01.05.2010**

(24) Дата начала отсчета срока действия патента:
01.05.2010

Приоритет(ы):
(30) Конвенционный приоритет:
03.05.2009 SK PP00032-2009;
27.03.2010 SK PP50009-2010;
08.04.2010 SK PP50012-2010;
19.04.2010 SK PP50016-2010

(43) Дата публикации заявки: **10.06.2013** Бюл. № **16**

(45) Опубликовано: **10.03.2015** Бюл. № **7**

(56) Список документов, цитированных в отчете о поиске: **WO 2007/076456 A2, 05.07.2007. WO 2008/105703 A1, 04.09.2008. WO 2007/081382 A1, 19.07.2007. EP 1390921 B1, 06.09.2006 . RU 2191482 C1, 20.10.2002. RU 2301506 C2, 20.06.2007**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **05.12.2011**

(86) Заявка PCT:
IB 2010/051915 (01.05.2010)

(87) Публикация заявки PCT:
WO 2010/128442 (11.11.2010)

Адрес для переписки:
107078, Москва, а/я 265, ООО "Прозоровский и партнеры"

(72) Автор(ы):
Флорек Мирослав (SK),
Масарык Михал (SK),
Риффелмачер Давид Алан (CZ)

(73) Патентообладатель(и):
ЛОГОМОТИОН, С.Р.О. (SK)

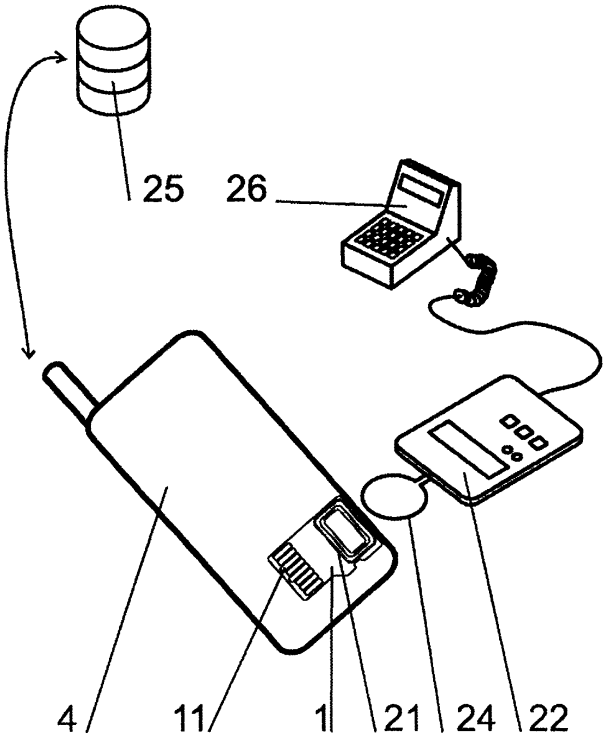
RU 2543935 C2

(54) ПЛАТЕЖНЫЙ ТЕРМИНАЛ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОГО КОММУНИКАЦИОННОГО УСТРОЙСТВА, ТАКОГО КАК МОБИЛЬНЫЙ ТЕЛЕФОН, И СПОСОБ БЕЗНАЛИЧНЫХ ПЛАТЕЖЕЙ

(57) Реферат:

Изобретение относится к платежным устройствам. Технический результат - повышение безопасности при осуществлении платежных операций. Устройство мобильной связи с функцией платежного терминала, содержащее устройство (4) мобильной связи со съемной картой (1) памяти, адаптированной для установки в соответствующий слот устройства (4) мобильной связи и имеющей связанные между собой интерфейс (11), микроконтроллер (12) с внутренней памятью (10) и блоком (9) загрузки операционной системы, элемент (3) безопасности с защищенными областями (31, 32) его памяти, и память (2) карты (1) памяти, разделенную на незащищенную часть и защищенную часть, причем последняя имеет модуль (5) с прикладной

платежной программой платежного терминала, контроллер (17) и модуль (19) управления загрузкой операционной системы, при этом элемент (3) безопасности снабжен размещенными отдельно друг от друга модулем (6) с конфигурационными данными платежного терминала и модулем (7) платежной карточки, а защищенные области памяти (31, 32) элемента (3) безопасности соединены с микроконтроллером (12), который соединен с интерфейсом (11) подключенным к каналу (13) связи карты (1) памяти с возможностью формирования платежной операции при установлении связи между торгово-сервисным предприятием и съемной картой (1) памяти. 4 н. и 28 з.п. ф-лы, 14 ил.



Фиг.6

RU 2543935 C2

RU 2543935 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 543 935**(13) **C2**

(51) Int. Cl.
G07F 7/10 (2006.01)
G06Q 20/20 (2012.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011148267/08, 01.05.2010**

(24) Effective date for property rights:
01.05.2010

Priority:
(30) Convention priority:
03.05.2009 SK PP00032-2009;
27.03.2010 SK PP50009-2010;
08.04.2010 SK PP50012-2010;
19.04.2010 SK PP50016-2010

(43) Application published: **10.06.2013** Bull. № **16**

(45) Date of publication: **10.03.2015** Bull. № **7**

(85) Commencement of national phase: **05.12.2011**

(86) PCT application:
IB 2010/051915 (01.05.2010)

(87) PCT publication:
WO 2010/128442 (11.11.2010)

Mail address:
107078, Moskva, a/ja 265, OOO "Prozorovskij i partnery"

(72) Inventor(s):
Florek Miroslav (SK),
Masaryk Michal (SK),
Riffelmacher David Alan (CZ)

(73) Proprietor(s):
LOGOMOTION, S.R.O. (SK)

RU 2543935 C2

RU 2543935 C2

(54) PAYMENT TERMINAL USING MOBILE COMMUNICATION DEVICE SUCH AS MOBILE TELEPHONE AND NON-CASH PAYMENT METHOD

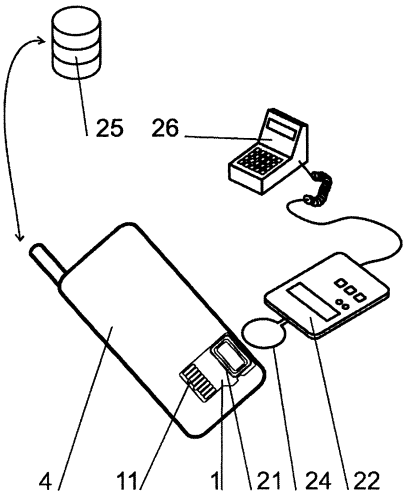
(57) Abstract:

FIELD: physics, computer engineering.

SUBSTANCE: invention relates to payment devices. A mobile communication device having a payment terminal function, comprising a mobile communication device (4) with a removable memory card (1), adapted for installation into a corresponding slot on the mobile communication device (4) and having interconnected interface (11), microcontroller (12) with internal memory (10) and an operating system loading unit (9), a security element (3) with secure regions (31, 32) of the memory thereof, and memory (2) of the memory card (1), divided into an insecure part and a secure part, wherein the latter has a module (5) with a payment application program for the payment terminal, a controller (17) and an operating system loading control module (19), wherein the security element (3) is provided with separately arranged module (6) with configuration data of the payment terminal and payment card module (7), and the secure regions of memory (31, 32) of the security element (3) are connected to the microcontroller (12), which is connected to the interface (11), connected to the communication channel (13) of the memory card (1) to facilitate a payment operation upon establishing communication between a retail and service establishment and the removable memory card (1).

EFFECT: improved security when performing payment operations.

32 cl, 14 dwg



Фиг.6

RU 2543935 C2

RU 2543935 C2

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Изобретение относится к платежным терминалам, которые размещаются в устройствах мобильной связи, в том числе в мобильном телефоне. Платеж осуществляется либо при помощи собственного элемента связи терминала, преимущественно NFC-типа, поддерживающего стандарт беспроводной связи ближнего радиуса действия, либо методом прямого дебетового списания с использованием бесконтактного канала связи и конфигурации для создания временного платежного терминала с упрощенной структурой на основе использования устройства мобильной связи, что удобно, прежде всего, для малых торгово-сервисных предприятий. Данное изобретение направлено на повышение безопасности и удобства при осуществлении платежных операций с использованием мобильного устройства со съемной картой памяти, например, картой micro-SD-типа.

ОБЗОР ПРЕДШЕСТВУЮЩЕГО УРОВНЯ ТЕХНИКИ

Известны платежные терминалы, POS-терминалы (терминалы для производства платежей, расположенные в местах совершения покупки, то есть в торговых точках - Point of Sale), которые стационарно установлены в торговых помещениях. В POS-терминалах перевод денег со счета покупателя на счет оператора торгово-сервисного предприятия защищен в рамках оговоренной системы. До настоящего времени платежный процесс, проводимый через POS-терминал, представлял собой процесс, при котором получатель платежа является владельцем POS-терминала, а клиент-плательщик использует соответствующую карточку в качестве платежного средства. На первом этапе выполняется проверка, верификация (установление личности) владельца карточки. Этот процесс должен обеспечиваться высоким уровнем защиты и исключать необоснованные действия как со стороны торгово-сервисного предприятия, так и со стороны покупателя, осуществляющего платеж. Неоплаченная сумма автоматически записывается на счет оператора торгово-сервисного предприятия.

Ранее для запуска и выполнения прикладной платежной программы (приложения) терминала использовались только карточки, снабженные магнитной полосой. Однако вследствие технических ограничений магнитная полоса с загруженными данными создавала определенный риск для безопасности, поскольку ее можно было легко скопировать или внести в нее изменения при помощи простых технических средств. Технология считывания внутренних данных с магнитной полосы давно устарела.

В связи с вышеизложенным во второй половине девяностых был заключен договор между компаниями-эмитентами карточек Europay, International MasterCard и VISA о создании EMV-стандарта, предусматривающего использование микрочипа, размещенного на платежной карточке. Стандарт EMV (Europay MasterCard Visa) устанавливает порядок взаимодействия между чипом платежной карточки и POS-терминалом с целью обеспечения совместимости на глобальном (мировом) уровне. Использование микрочипа позволяет защитить данные, размещенные на нем, поскольку доступ к этим данным извне невозможен без знания ПИН-кода. Использование чипа на карте также позволяет выполнить Идентификацию Владельца карточки даже без "онлайн" подключения к "процессинговым" центрам (центрам обработки платежных данных). Если магнитные стрипы (полосы) представляли собой пассивные носители данных, то чип, размещенный на карточке, по сути, является мини-компьютером, который обладает определенной вычислительной способностью, с защищенными областями памяти и модулем шифрования данных. Несмотря на упомянутые технические характеристики, присущие современным POS-терминалам, было установлено, что в случае применения мошеннических приспособлений и манипуляций непосредственно

в POS-терминале или в случае использования вставляемого в считывающее устройство вспомогательного средства (адаптера), данные, хранящиеся на карточке, а также ПИН-код могут быть раскрыты. Это происходит без ведома владельца торгово-сервисного предприятия, на территории которого установлен POS-терминал, в случае недостаточно жесткого контроля со стороны обслуживающего персонала или в результате применения других мошеннических способов.

В технических средствах, известных до настоящего времени, не предусмотрена возможность превращения мобильного телефона в такой вид платежного терминала, который, являясь собственностью покупателя, осуществляющего платеж, в то же время обладал бы достаточным уровнем безопасности, удовлетворяющим всех участников платежного процесса (эмитента платежной карточки, процессинговых центров (центров обработки), банка, торгово-сервисного предприятия).

В патенте CN 101351819 описано изобретение, предусматривающее использования мобильного телефона в качестве POS-терминала; однако здесь не показана организация отдельных ключевых элементов системы. Во многих технических решениях, в частности, согласно патентам CN 101339685, CN 101329801, US 2008270246 (A1), SI 22595 (A), US 2008059375 предлагается использование мобильного телефона для выполнения платежей методом прямого дебетового списания, но при этом непосредственно в самом телефоне независимые элементы POS-терминала не размещены. Или, как указано в описании к заявке US 20077241180 (A1), в известных решениях осуществляется взаимодействие мобильного телефона со стационарным (неподвижным) POS-терминалом.

Необходимо такое техническое решение, которое обладало бы высоким уровнем безопасности EMV-платежных прикладных программ и при этом генерировало бы итоговые платежные криптограммы в виде EMV-стандартов или криптограммы аналогичного типа. В частности, при осуществлении платежей через Интернет-сети или при осуществлении платежных операций за пределами обычных магазинов, например, при оплате услуг по загрузке программ, находящихся в распоряжении операторов мобильной связи. Имеющиеся решения обладают недостаточным уровнем безопасности, вследствие чего может произойти раскрытие данных, несанкционированное использование канала связи в процессе пересылки данных с платежной карточки клиента-покупателя на POS-терминал торгово-сервисного предприятия, на виртуальный POS-терминал через Интернет-сети либо при помощи NFC - (беспроводная связь ближнего радиуса действия) или GPRS - (технология пакетной передачи данных) связи. При переходе первоначального непосредственного контакта между POS-терминалом и платежной карточкой в обычном магазине в соединение в среде Интернет угроза безопасности резко возрастает.

Для известных POS-терминалов характерна стабильная (сложившаяся) конструкция, которая, помимо прочего, включает следующие элементы: канал связи, обеспечивающий соединение POS-терминала с центром обработки платежей, принтер (печатающее устройство), ключ шифрования, карт-ридер (устройство чтения карт памяти и др.), который считывает данные с карт разного формата, а также клавиатуру для ввода ПИН-кода. Такая техническая конфигурация требует определенного пространства и является относительно дорогостоящей. Выполнение известных POS-терминалов ориентировано на размещение в стационарных торговых точках, расположенных в капитальных зданиях, где высокие затраты на покупку, установку и работу POS-терминалов уравновешиваются приемлемым уровнем товарооборота.

Известно решение, изложенное в описании к патенту WO 2008063990, где упоминается система, в которой POS-терминал не имеет канала связи с центром обработки платежей,

а использует для этих целей опосредованное соединение при помощи мобильного телефона клиента (покупателя). Данное решение обладает низким уровнем безопасности, поскольку прикладная платежная программа терминала выполняется на удаленном компьютере, а мобильный телефон служит только связующим звеном. Описан также POS-терминал с таким разделением функций, при котором непосредственно в месте осуществления платежа расположена только управляющая часть терминала. Она связана с остальной частью терминала, расположенной на некотором удалении.

В известных решениях и опубликованных патентных описаниях отсутствуют четкие рекомендации в отношении создания недорогого, несложного и одновременно компактного платежного POS-терминала, который будет генерировать платежные криптограммы в соответствии с действующими стандартами, прежде всего, стандартами EMV (стандартами платежных смарт-карт).

Известные решения требуют относительно сложной установки и предполагают использование множества входных и выходных устройств, что увеличивает их стоимость. На данный момент неизвестно о таких устройствах, которые сочетали бы в себе простоту исполнения и высокий уровень безопасности, были компактными и могли применяться даже в небольших торговых точках, например газетных киосках или передвижных лавках, торгующих фаст-фудом.

С расширением использования мобильных устройств, в частности мобильных телефонов, возрастет необходимость в повышении удобства и безопасности проведения платежных процессов для бесконтактных платежных приложений. Устройства мобильной связи имеют возможность устанавливать целенаправленную и одновременно внешне незаметную связь с данными мобильной сети, в момент осуществления которой существует риск проникновения вредоносных программ в среду устройства мобильной связи.

Известно применение специальной платежной кнопки (Pay-button) в соответствии с патентной заявкой, опубликованной под номером WO 2010/011670 A2. Посредством этой кнопки активируется элемент NFC-связи, необходимый для запуска прикладной платежной программы бесконтактным способом. Данная кнопка упрощает запуск платежного приложения, однако ее соединение с элементом NFC-связи не обеспечивает более высокого уровня безопасности в сравнении с предыдущими решениями, согласно которым платежное приложение запускается с помощью виртуальной кнопки, отображаемой в меню на дисплее мобильного устройства связи. Анализ возможных атак (попыток взлома) в отношении платежной карточки, хранящейся внутри устройства мобильной связи, показал, что существует опасность запуска платежного приложения без ведома клиента в результате проникновения нежелательных программ. Платежная карточка в мобильном телефоне постоянно находится в устройстве чтения карт. Ее расположение уже само по себе предполагает вероятность совершения неизменных попыток считывания данных с карточки. Следовательно, имеется опасность, что существующий уровень защиты платежной карточки окажется недостаточным для надежной защиты хранящихся на карточке данных. Проблема актуальна даже для карточек, поддерживающих EMV-стандарт (что до настоящего времени считалось маловероятным), так как платежная карточка в течение продолжительного времени, практически непрерывно, вставлена в устройство чтения карт, например в POS-терминал или в ATM (канал асинхронной передачи данных). По этой причине разработчикам необходимо направлять усилия на повышение не только комфортности, но и безопасности платежной карточки. Имеющиеся на мобильном телефоне специальные (целевые) кнопки, например кнопка для фотографирования, разработаны исключительно

для ускоренного и упрощенного доступа к выбранной функции телефона, при этом не предусмотрена защита от преднамеренного запуска выбранной функции.

Новое устройство, при более высоком уровне безопасности, должно быть также в достаточной степени комфортным для пользователя, что является важным условием увеличения платежей по безналичному расчету при помощи мобильного телефона.

ПРЕДПОСЫЛКИ ДЛЯ СОЗДАНИЯ ИЗОБРЕТЕНИЯ

Указанные недостатки в значительной степени устранены в платежном терминале с использованием устройства мобильной связи, например мобильном телефоне, где платежный терминал содержит память, интерфейс и микроконтроллер. Микроконтроллер соединен с памятью, а также посредством интерфейса с каналом связи мобильного устройства (телефона). Платежный терминал содержит модуль с прикладной платежной программой POS-терминала, а также модуль конфигурационных данных платежного терминала, который хранится в защищенной части памяти. Суть данного изобретения состоит в том, что платежный терминал вместе с соответствующими конфигурационными данными хранится на съемной карте памяти, которая может устанавливаться в слот мобильного устройства связи, предназначенный для подключения дополнительных устройств для расширения функциональных возможностей мобильного устройства связи.

Характерной особенностью предложенного решения является конфигурация, при которой ядро всего процесса для POS-терминала размещается на съемной карте памяти, вставленной в устройство мобильной связи, учитывая, что наиболее вероятно размещение его в слоте общей памяти мобильного телефона. Выполнение всех внутренних прикладных платежных программ POS-терминала может быть реализовано на съемной карте памяти, вставленной в устройство мобильной связи. Исключением могут быть процессы связи с центрами платежных систем, для которых непосредственно используются каналы связи самого мобильного устройства (SMS - система передачи коротких сообщений, GPRS - система пакетной передачи данных, например, через радиоинтерфейс). Для отображения выполнения платежного приложения могут использоваться средства изображения устройства мобильной связи.

Только перенос ядра обработки данных POS-терминала в дополнительную карту памяти мобильного телефона приводит к появлению удивительных технических преимуществ, но при этом также могут возникнуть сложности с загрузкой данных с платежной карточки, поскольку в мобильных телефонах отсутствуют устройства чтения чип-карт (карт с микропроцессором или интеллектуальных карт). Важной особенностью предложенного решения является возможность разместить платежную карточку или даже несколько платежных карточек клиента на одной съемной карте памяти. Технически возможно наличие в съемной карте памяти отдельной защищенной части памяти с данными платежной карточки.

В процессе выполнения платежной прикладной программы (приложения) съемная карта памяти вставлена в слот мобильного устройства, используемый для расширения функциональных возможностей мобильного устройства в дополнение к его основным функциям. Он представляет собой преимущественно, но не исключительно, широко используемый слот, доступ к которому обеспечен на мобильном телефоне, извне. Соответствующий слот разработан для подключения такого технического оборудования, без которого устройство мобильной связи может выполнять свои основные, жизненно важные функции. Следовательно, данный слот непосредственно не оказывает влияния на передачу данных и/или речевой сигнал в сети оператора мобильной связи. В этом отличие данного слота от интерфейса для SIM-карты (SIM - subscriber identity module -

модуль идентификации абонента). Карта памяти, которая является важным элементом настоящего изобретения, не обладает функциональностью SIM-карты мобильного телефона, не зависит от нее и может извлекаться из мобильного телефона или устанавливаться в нем без прерывания регулярных функций телефона.

В случае сужения связи между платежной карточкой и POS-терминалом до функции передачи данных внутри одного аппаратного средства, которое находится (установлено) в мобильном телефоне в процессе выполнения прикладной программы, контролировать и несанкционированно вмешиваться в такую связь с помощью обычных средств невозможно. После выполнения платежа из съемной карты памяти отсылается зашифрованная информация о выполненном платеже. Эта информация характеризуется достаточной степенью защиты в виде EMV-стандарта. При обычной конфигурации устройство мобильной связи может быть представлено мобильным телефоном, который будет обеспечивать поддержку внешних функций связи с центрами обработки платежей для выполнения платежной прикладной программы на съемной карте памяти. Мобильный телефон будет также обеспечивать электропитание съемной карты памяти.

Съемная карта памяти может содержать модуль платежной карточки с платежной прикладной программой, преимущественно EMV-типа (поддерживающей EMV-стандарт). Такой модуль платежной карточки включает аппаратные и программные средства для обеспечения тех же функций, которые выполняет чип (микросхема) в соответствии с EMV-стандартом. Интерфейсы указанного модуля могут отличаться, поскольку он не предназначен для считывания в стандартном считывающем устройстве, но в то же время прочно соединен с держателем съемной карты памяти.

Размещение POS-терминала и платежной карточки в одном неразделяемом аппаратном средстве не имело смысла до настоящего момента, поскольку терминалы фактически устанавливались в торгово-сервисных предприятиях (у получателей платежей). Эти торговые предприятия, как правило, были собственностью банка, платежного центра и т.д.

Предложенное решение подразумевает, что клиент может владеть платежным терминалом на условиях долгосрочной аренды (так называемый "лизхольд"). Следовательно, можно поместить платежный терминал и платежную карточку в одно аппаратное средство. С точки зрения идентичности конфигурации терминал будет оставаться во владении конкретного банка или центра обработки данных, как это имело место до сих пор с терминалами, расположенными на территории торгово-сервисных предприятий. Учитывая, что связь между платежной карточкой и POS-терминалом осуществляется посредством контроллера, при этом микроконтроллер находится в аппаратном устройстве съемной карты памяти, а также имея в виду миниатюрные размеры платежного устройства, ясно, что несанкционированное считывание из внешней среды данных, обмен которыми происходит при реализации такой связи, технически невыполнимо.

Конфиденциальные данные платежного POS-терминала так же, как и ключи шифрования и идентификационные данные, должны храниться в защищенной части памяти, предпочтительно в так называемом Элементе Безопасности. Элемент Безопасности имеет точно заданные характеристики аппаратного устройства и подлежит соответствующей сертификации, благодаря чему участники платежного процесса могут без риска хранить конфиденциальные данные в названном запоминающем устройстве. Указанные данные платежного POS-терминала должны храниться строго отдельно и быть изолированы при доступе к данным платежной карточки, и наоборот. По этой причине на съемной карте памяти должны предусматриваться, по меньшей мере, два

независимых, отдельных защищенных домена памяти. Они могут быть выполнены, например, в виде отдельных секций единого элемента безопасности.

С точки зрения оптимизации процессов, осуществляемых при работе прикладной платежной программы терминала, целесообразно, но не обязательно, наличие на съемной карте памяти двух независимых с точки зрения аппаратного исполнения Элементов Безопасности. Элементы Безопасности могут быть выполнены в виде двух унифицированных чипов, которые размещены независимо на печатной схеме съемной карты памяти. В этом случае первый Элемент Безопасности может быть предназначен для хранения данных POS-терминала или, соответственно, для хранения данных разных POS-терминалов. Второй Элемент Безопасности будет предназначен для хранения данных одной платежной карточки либо данных разных платежных карточек. Таким образом, предложенное решение позволяет размещать POS-терминалы нескольких операторов, а также несколько платежных карточек одного клиента (также платежные карточки разных банков, выданных на имя одного лица) в одном аппаратном устройстве. Поскольку, с точки зрения обеспечения безопасного доступа указанные конфигурация и платежные данные, принадлежащие разным компаниям, должны располагаться обособленно, то Элементы Безопасности будут разделены на несколько независимых доменов, секций. При использовании двух Элементов Безопасности, одновременная передача данных и выполнение двух прикладных программ будут разрешены даже в том случае, если для Элемента Безопасности не предусмотрена функция многозадачности. Использование двух или нескольких Элементов Безопасности увеличивает общую доступную емкость памяти таким образом, что платежная прикладная программ POS-терминала может выполняться непосредственно на Элементах Безопасности. При конфигурации с одним Элементом Безопасности удобнее пользоваться другой, преимущественно дешевой и незащищенной памятью, в которую будет загружаться прикладная платежная программа POS-терминала и в которой будет выполняться программа на протяжении всего платежного процесса.

Помимо наличия общей памяти как таковой, карта памяти может содержать Элемент Безопасности в виде чипа с защищенной памятью, в которой хранится модуль с конфигурационными данными терминала. Этот модуль используется для безопасного хранения данных, необходимых для установления терминалом своей собственной идентичности. Эти данные, по большей части, содержат информацию о том, кто является владельцем терминала и другие подобные данные.

Элемент Безопасности соединен с микроконтроллером. Термин "микроконтроллер" может подразумевать именно контроллер или просто некое понятие в узком смысле аппаратного средства в виде контроллера. Микроконтроллер может быть размещен таким образом, что его функции будут разделены, например контроллерная часть (управляющая) будет отделена от вычислительной части, находящейся в другом чипе. Для запуска платежной прикладной программы POS-терминала микроконтроллер может быть также подключен к памяти карты памяти, в которой хранится модуль с платежной прикладной программой POS-терминала. В частности, прикладная программа может быть выполнена в виде EMV-приложения. Микроконтроллер считывает платежную прикладную программу POS-терминала с соответствующего модуля, вследствие чего терминал становится так называемым общим POS-терминалом (Generic POS Terminal). Это общий платежный POS-терминал, индифферентный в данный момент. Для того чтобы платежный POS-терминал можно было привязать к какому-либо конкретному банку, организации, он должен загрузить конфигурационные данные терминала из выбранного модуля в чипе смарт-карты.

Предложенная конфигурация позволяет установить конфигурированную и адаптированную карту памяти, которая может выполнить платежные операции POS-терминала внутри обычного мобильного телефона со слотом для расширения памяти.

Модуль платежной карточки расположен в защищенной части памяти, отдельно от модуля с конфигурационными данными терминала, предпочтительно на независимых доменах элемента безопасности в специализированном чипе. Подходящей структурой карты памяти, учитывая широкое распространение устройств мобильной связи с SD-слотом, будут карты SD-типа, mini-SD или micro-SD типа, также возможно, M2 (Memory Stick Micro). Поэтому предпочтительно, чтобы интерфейс карты памяти для сопряжения с каналом связи устройства мобильной связи был SD- или M2-типа. Микроконтроллер может соединяться с интерфейсом карты в соответствии со спецификацией, разработанной ассоциацией SD-карт (Технический Комитет Ассоциация SD-карт).

Для повышения коэффициента пропускания данных предлагается платежная карточка, которая содержит двухпроводную, а лучше четырехпроводную шину данных. Предпочтительный вариант исполнения карточки предусматривает максимальный параметр (габарит) менее 24 мм, и второй максимальный параметр менее 14 мм.

Микроконтроллер может быть снабжен защищенной от стирания внутренней памятью, предпочтительно EEPROM-типа. Для достижения приемлемого уровня безопасности микроконтроллер может также содержать модуль загрузки (загрузчик операционной системы) для контроля за несанкционированным вмешательством в загружаемую прикладную платежную программу POS-терминала. Загрузчик операционной системы может размещаться в защищенной части памяти процессора микроконтроллера, предназначенной только для чтения, причем он запускается после каждого сброса терминала в исходное (нулевое) состояние. Загрузчик выполняет функцию контроля, отслеживая, не претерпели ли изменения операционная система или прикладные программы в результате несанкционированного вмешательства. После каждого сброса на нуль загрузчик вычисляет значение хеш-функции (электронно-цифровая подпись) на основе содержимого внешней флэш-памяти программы, в которой хранятся операционная система и прикладные программы. Затем он сравнивает полученный результат со значением, которое хранится во внешней EEPROM-памяти. Если данные совпадают, загрузчик передает управление операционной системе. Если данные не совпадают, загрузчик уменьшает на единицу регистрируемое счетчиком число неудачных попыток, а затем останавливает операцию. В том случае, если счетчик достигает значения нуля, запуск микроконтроллера становится невозможным. В указанной памяти может храниться операционная система (как начало и конец адресуемой области), притом, что значение хеш-функции для емкости памяти (электронно-цифровая подпись) сохраняется в микроконтроллере при первом сохранении операционной системы и приложения (прикладной программы). В дальнейшем произвести изменение этих данных будет невозможно.

Предлагается использовать обычный микроконтроллер на базе микропроцессора разрядностью 32 бита.

Сервисная программа (утилита) терминала может быть значительно расширена при такой конфигурации, когда платежный терминал имеет свой собственный канал связи, то есть не зависит от каналов связи мобильного телефона. Такой вид конфигурации характерен для карты памяти, которая содержит элемент бесконтактной связи, соединенный с элементами безопасности и/или микроконтроллером. Предпочтительным вариантом исполнения предложенного решения является вариант, когда непосредственно на карте памяти размещена антенна, соединенная с элементом

бесконтактной связи. За счет такого конструктивного исполнения достигается функциональная независимость терминала. Элемент бесконтактной связи может иметь функцию детектирования ближнего электромагнитного поля, благодаря чему его каналы связи будут активироваться только в момент обязательного (требуемого) соединения, что приведет к снижению потребляемого терминалом количества энергии. Электропитание терминала будет осуществляться от электромагнитного поля и от блока питания мобильного телефона через соответствующий интерфейс карты памяти. Устройство бесконтактной связи может связываться со всеми блоками, находящимися на элементе безопасности, за исключением блока шифрования, доступ к которому будет открыт только через микроконтроллер для снижения риска несанкционированного взлома кода. С учетом получивших распространение в настоящее время типов связи предпочтительным типом элемента связи является NFC-тип в соответствии с требованиями стандарта ISO14443.

Платежный терминал может содержать несколько индивидуальных (отдельных) модулей с конфигурационными данными разных независимых терминалов в элементе безопасности. Они будут храниться в отдельных доменах элемента безопасности. Такое техническое решение позволит платежному терминалу активироваться в терминал, принадлежащий разным центрам обработки платежей. Указанная способность будет зависеть от клиентского (пользовательского) выбора или от других команд. Таким образом, одна карта памяти может подключать и запускать последовательные функции нескольких независимых платежных терминалов. Данная конфигурация предпочтительна в тех случаях, когда имеет место изменчивость (непостоянство) указанного платежного терминала и отсутствует его привязка к конкретному торгово-сервисному предприятию или в случае целесообразности выбора и идентификатора платежного терминала, и принадлежности платежного терминала.

Платежный терминал может также содержать несколько платежных карточек, для этого в нем предусматривают несколько независимых модулей, в которых находятся независимые платежные карточки с соответствующими им платежными прикладными программами в элементе безопасности. Таким образом, платежный терминал может представлять собой не только множественный (мультиплатежный) терминал, но и множественную (комплексную) карточку. С увеличением числа карточек, владельцем которых является один клиент, предложенное техническое решение будет обеспечивать пространство для удобного и безопасного объединения их в одной карте памяти, которая вставляется в мобильный телефон.

Память карты памяти, предпочтительно выполненной в виде флэш-памяти, может содержать как минимум одну область защищенного объема. В этом случае модуль прикладной платежной программы POS-терминала может храниться в указанной памяти. Такой модуль можно разместить прямо в микропроцессоре или в элементах безопасности. Однако при определенных архитектурах монтажных плат этот вариант технического решения не обеспечивает достаточной гибкости, если необходимо учесть ограничения в отношении требуемого объема области памяти. Кроме того, может потребоваться выполнение поэтапного обновления платежного приложения POS-терминала, что выполняется модулем управления загрузкой, хранящимся в памяти. Карта памяти может быть снабжена модулем обработки контроллера памяти, который предназначен для управления потоком данных. Если существует необходимость в установлении связи между картой памяти и мобильным телефоном через интерфейс, обеспечивающий доступ к web-сети, то в карту памяти включают блок web-сервера (Интернет-сервера).

В соответствии с представленным описанием предложенного технического решения полезность терминала будет расширяться за счет дополнительного введения функций нефинансового характера. Имеющиеся элементы карты памяти, независимый домен элемента безопасности, элемент бесконтактной связи, а также блок шифрования могут использоваться для управления внешними устройствами, например устройством дистанционного управления, электронным ключом для входа (шлюза) и др. В таком случае модуль нефинансовой прикладной программы, который инициализируется через микроконтроллер, может быть расположен в элементе безопасности или в управляющем чипе (микросхеме) смарт-карты.

При конфигурации, описываемой в данном изобретении, карта памяти с функцией платежного терминала может в дальнейшем выполнять даже функцию дополнительной памяти устройства мобильной связи. В таком случае в незащищенной части памяти предусматривается область для данных пользователя, открытых для неограниченного (свободного) доступа, например, таких, как изображения (фото), музыкальные файлы и т.п. Эту часть можно непосредственно просматривать на экране мобильного устройства. В памяти, предназначенной для скрытых от пользователя данных, могут находиться системные данные в виде записей итогов платежных транзакций и т.д.

Система может дополнительно содержать инициатор платежной прикладной программы POS-терминала с целью проведения оплаты в обычном магазине. Инициатор может быть выполнен в виде простого технического элемента либо быть частью контрольно-кассового аппарата. Возможно наличие блока генерирования величин платежных сумм. Торгово-сервисное предприятие вводит сумму, подлежащую оплате, посредством инициатора. Эта же сумма может быть также получена в виде итоговой суммы за покупку на выходе (чек) из контрольно-кассового аппарата. Инициатор может быть соединен с элементом связи или оборудован своим элементом связи, совместимым с элементом связи на съемной карте памяти или с элементом связи ближнего радиуса действия мобильного устройства.

Предлагаемый способ платежа методом прямого дебетового списания с использованием устройства мобильной связи заключается в том, что прикладная платежная программа POS-терминала может выполняться на съемной карте памяти, которая вставлена в слот мобильного телефона, предназначенный для дополнительного оборудования. При этом прикладная программа платежной карточки выполняется на том же аппаратном устройстве.

Для выполнения прикладной платежной программы POS-терминала в известных решениях, характеризующих предшествующий уровень техники, связь платежной карточки с POS-терминалом была временной (в течение выполнения платежа). В настоящем изобретении предусматривается прочное соединение платежной карточки с платежным терминалом. Следовательно, связь между POS-терминалом и платежной карточкой может осуществляться прямо по каналам связи, выполненным в платежной карточке. Многочисленные новые возможности выполнения процедур прикладной платежной программы, вытекающие из настоящего технического решения, как и результат выполнения прикладной платежной программы POS-терминала, могут поддерживать формат, который повсеместно используется сегодня, - EMV - платежную криптограмму.

В одном из вариантов проведения процедуры прикладная платежная программа POS-терминала загружается в микроконтроллер, встроенный в карту памяти, а затем из соответствующего элемента безопасности загружаются конфигурационные данные идентификатора выбранного терминала. Важной особенностью изобретения является

также возможность загрузки данных платежной карточки из элемента безопасности в микроконтроллер, который работает как платежный терминал. Таким образом, данные загружаются из одного вида оборудования, используемого платежной программой POS-терминала, которое он использует для выполнения упомянутой программы. В случае, когда элемент безопасности обладает достаточной вычислительной способностью, прикладная платежная программа POS-терминала может выполняться непосредственно в элементе безопасности. Так происходит при использовании двух элементов безопасности: отдельно для платежного терминала и платежных карточек. Даже при такой конфигурации прикладная платежная программа POS-терминала может быть создана как индифферентная (нейтральная) общая программа для идентификаторов всех платежных терминалов; и идентификационная информация из соответствующего независимого домена элемента безопасности загружается в прикладную платежную программу POS-терминала только после того, как будет выбран платежный терминал. Вариант, в котором предусмотрено использование независимой прикладной платежной программы POS-терминала с уже введенными конфигурационными данными, также возможен.

С целью повышения уровня безопасности предпочтительно, чтобы загрузчик операционной системы осуществлял контроль изменений в прикладной платежной программе POS-терминала перед запуском самой прикладной платежной программы POS-терминала. Управление прикладной платежной программой POS-терминала осуществляется, преимущественно, при помощи входного устройства мобильного телефона, главным образом, посредством кнопочного пульта.

Возможно также создание "POS упрощенного типа" (кассового терминала упрощенного типа) со структурой, позволяющей снизить требования к техническому оборудованию торгового предприятия. Он создается на той же технической основе, что и в случае расположения платежных карточек, или одной платежной карточки на съемной карте памяти и выполнения прикладной платежной программы POS-терминала на той же съемной карте памяти. Суть предложенного решения для данного варианта конфигурации состоит в том, что платежный POS-терминал формируется на съемной карте памяти в момент временного соединения Платежного Модуля (Sales Device) со съемной картой памяти. Платежный Модуль принадлежит торгово-сервисному предприятию или используется им и содержит защищенный модуль с идентификационными данными, которые, в первую очередь, содержат сведения, необходимые для установления соответствия между платежным POS-терминалом и соответствующим банковским счетом торгового предприятия. По сути, таким платежным модулем может служить любое аппаратное средство, которое обеспечивает точную идентификацию временно созданного платежного POS-терминала.

Важной особенностью такого использования общей главной технической идеи является то, что POS-терминал с предварительно заданной структурой создается в период временного соединения двух составляющих одной системы. Это соединение отмечается как временное, поскольку после завершения платежного процесса составные части системы разъединяются, канал связи прерывается, и может быть установлено новое соединение между Платежным Модулем и другой съемной картой памяти. Естественно, что повторное соединение между съемной картой памяти, с которой только что обеспечивалось взаимодействие (соединение), и Платежным Модулем также не исключается. Под временностью соединения подразумевается временная фаза (период времени), которая, на самом деле, ограничивается одним платежным процессом, притом, что в нее может быть включено еще и некоторое время соединения до начала и после

завершения платежного процесса. Возможность создавать пару, представляющую собой всегда новую пару элементов, один - со стороны торгово-сервисного предприятия, а второй - со стороны клиента, осуществляющего оплату, - это решение, при котором всегда можно создать POS-терминал в устройстве мобильной связи плательщика, причем такой POS-терминал, который содержит идентификационные данные соответствующей торговой организации.

Словосочетание «Платежный Модуль» применительно к области платежных POS-терминалов не несет общепринятого смысла. Под таким словосочетанием следует понимать аппаратный элемент любого вида с соответствующим программным обеспечением для реализации функций, приведенных в настоящем патентном описании. Платежный Модуль выполняет функции, свойственные внешнему платежному POS-терминалу, при этом торгово-сервисным предприятиям из практических соображений удобно привлекать его для работы. Однако с точки зрения структуры и выполнения приложения (прикладной программы) Платежный Модуль является существенной, но недостаточной частью платежного POS-терминала в целом. Следовательно, необходимо понимать выражение Платежный Модуль в общем смысле как часть терминала, который, по сути, привязан к торговой точке или к месту совершения покупки и обеспечивает правильный маршрут дебетовых платежных операций.

В платежном POS-терминале, рассматриваемом как одно целое, Платежный Модуль (Sales Device) может иметь две основные функции - хранение идентификационных данных POS-терминала и ввод суммы (стоимости) покупки. В принципе, для этих целей годится даже упрощенный вариант аппаратного средства с минимальными возможностями, в котором сумма платежа (стоимость покупки) вводится при помощи кнопочной панели мобильного устройства. Однако такой вариант неудобен для торгово-сервисного предприятия, поскольку торговая компания будет вынуждена контролировать мобильное устройство клиента или доверить клиенту ввести правильную сумму платежа в прикладную программу платежного терминала. Введенная сумма может также отображаться на дисплее Платежного Модуля, чтобы торговая компания могла проверить ее, однако было бы намного удобнее, если бы оплачиваемая сумма вводилась через устройства, находящиеся в распоряжении торговой компании. В случае введения суммы, подлежащей к оплате, при помощи кнопочной панели мобильного устройства не будет выполняться требование соответствия некоторым стандартам (например, EMV) в части, касающейся порядка проведения операций со стороны торгового предприятия в процессе выполнения дебетового списания, однако данное решение позволяет реализовать и такой вариант.

Платежный Модуль не может независимо выполнить приложение (программу) платежного терминала, кроме того, он не должен иметь каналы связи для установления соединения с центром обработки (процессинговым центром). В предлагаемом комплекте технических средств предусмотрена возможность выполнения всех основных функций широко применяемого платежного POS-терминала только при реализации соединения с Платежным Модулем торгово-сервисного предприятия с помощью съемной карты памяти, вставленной в мобильное устройство клиента. Временное соединение может создаваться для реализации каждого отдельного платежа, притом, что у разных клиентов могут быть разные устройства связи. Именно мобильный телефон способен создать необходимое соединение с расчетным (процессинговым) центром благодаря существующей системе GSM/GPRS (Global System for Mobile Communications - Глобальная система мобильной связи / General packet radio service - система пакетной передачи данных с помощью радиосвязи). Однако такое соединение не является необходимым при каждом

платеже, поскольку предложенное решение способно выполнять обработку как "оффлайн"-, так и "онлайн"-платежей.

Структура съемной карты памяти для соединения с Платежным Модулем подобна вариантам осуществления, которые имели место ранее. Она также содержит элементы аппаратно-программных средств, чтобы комплект, состоящий из Платежного Модуля и мобильного устройства, имел возможность запустить и выполнить прикладную программу платежного терминала, которая с точки зрения процесса формирует ядро дебетовой платежной операции непосредственно на съемной карте памяти. Поскольку комплект, состоящий из Платежного Модуля и мобильного устройства, не должен быть оборудован внешним устройством чтения платежных карточек (карт-ридером), целесообразно размещение защищенной памяти с устройством (чтения) платежных карточек непосредственно на съемной карте памяти. Там же будут размещаться модуль для запуска приложения платежного терминала и элемент связи для соединения с Платежным Модулем. Помимо защищенной памяти с идентификационными данными платежного POS-терминала Платежный Модуль также содержит элемент связи для установления соединения со съемной картой памяти. Благодаря наличию этих элементов платежный POS-терминал создается с помощью обычного мобильного телефона со слотом для карточки, которая служит для расширения памяти. Таким образом, съемная карта памяти может содержать общий платежный терминал, который станет специфическим платежным терминалом с уникальными идентификационными данными только после его соединения с Платежным Модулем. Платежный Модуль будет давать однозначную идентификацию объекта, в чью пользу будет проводиться платеж в ходе этого временного соединения. Поскольку существует заинтересованность в наличии такой функции даже в тех мобильных телефонах, которые не содержат NFC-элемента связи (Near Field Communication - беспроводная связь ближнего радиуса действия), такой NFC-элемент связи может быть помещен прямо на съемной карте памяти. В принципе соединение между мобильным устройством и Платежным Модулем может быть выполнено в виде контактного сопряжения, однако это потребует сложной процедуры стандартизации соединительных устройств (разъемов) и решения проблем, связанных с совместимостью устройств. Следовательно, будет целесообразным, если не единственным, решением выполнение соединения между Платежным Модулем и съемной картой памяти в виде NFC-канала связи, который является в достаточной степени унифицированным.

Благодаря применению данной конфигурации, торговой организации нужно будет иметь в своем распоряжении очень простой Платежный Модуль, который будет содержать информацию об идентификаторе (идентификационных данных), номере терминала, к которому в центре обработки платежей может быть приписан номер счета соответствующей торговой организации. Такой Платежный Модуль будет небольшим и простым устройством. Он может иметь форму небольшого корпуса с дисплеем и клавиатурой, посредством которой торгово-сервисное предприятие будет вводить требуемую сумму платежа. Идентификационные данные могут храниться прямо в соответствующем элементе на печатной схеме Платежного Модуля, на ICC-карте (integrated circuit card - чип-карта или карточка с микропроцессором) или на других носителях, таких как пользующиеся популярностью до настоящего времени SAM-карты (Security Authentication Module - модуль аутентификации в системе защиты) с криптографическим ключом. В данном случае SAM-карта имеет размеры обычной SIM-карты (Subscriber Identity Module - модуль идентификации абонента), доступ к которой обеспечивается снятием крышки Платежного Модуля. SAM-карту вставляют

в Платежный Модуль перед первой активацией.

Клиент подключает свое мобильное устройство к Платежному Модулю. При подключении будет сформирован NFC-канал связи, и информация об идентификационных данных этого временно созданного платежного POS-терминала будет отправлена из Платежного Модуля на съемную карту памяти. Далее, идентификационные данные могут быть зашифрованы Главным Ключом, который хранится внутри Элемента Безопасности, размещенного в Платежном Модуле. Данные, поступающие из Платежного Модуля, будут служить основой для запуска приложения платежного терминала после их считывания на съемной карте памяти. Приложение (программа) платежного терминала может загружаться в индифферентной (нейтральной) форме, без собственной идентификации на съемной карте памяти. По сути, после создания временного соединения между Платежным Модулем и съемной картой памяти общего типа стандартный индифферентный терминал трансформируется в определенный POS-терминал, который привязан к соответствующему торгово-сервисному предприятию в системе. Этот этап является подготовительным при запуске нового одноразового POS-терминала. В дальнейшем, приложение платежного терминала, в частности, для карт, поддерживающих стандарт EMV, может быть запущено, как и в стандартных POS-терминалах, в момент выполнения соединения.

Шифрование идентификационных данных POS-терминала производится с помощью Главного Ключа, отличного от ключей шифрования, которые используются впоследствии приложением (прикладной программой) платежного терминала для создания платежной криптограммы. Главный Ключ может предоставляться, например, поставщиком аппаратных средств Платежного Модуля, а ключи шифрования прикладной программы платежного терминала могут выпускаться банком или платежным центром. На практике отличие ключей шифрования будет обусловлено различными требованиями отдельных юридических лиц, оперирующих в платежной клиринговой системе.

С точки зрения повышения безопасности именно входные данные, содержащие информацию о сумме платежа, могут быть зашифрованы при передаче данных из Платежного Модуля в мобильное устройство. При этом риск уменьшения плательщиком суммы платежа до запуска ядра (операционной системы) прикладной программы платежного терминала существенно снижается. Такой вид изменения суммы будет обнаруживаться при окончательном подтверждении платежной операции со стороны торговой организации в виде отображения на экране оплаченной суммы, однако вследствие невнимательности и при рутинном подходе представитель торговой организации может и не заметить изменения суммы.

Целесообразна конфигурация, при которой связь с модулем выбранной платежной карточки осуществляется прямо на съемной карте памяти в процессе запуска и выполнения прикладной программы платежного терминала. Несколько модулей с независимыми платежными карточками могут храниться на съемной карте памяти, а также на физически разделенных элементах безопасности или независимых доменах одного элемента безопасности. При такой конфигурации приложение платежного терминала может быть запущено прямо на съемной карте памяти, а данные о платежной карточке клиента (покупателя) не отправляются через внешние устройства считывания, а также в Интернет-пространство, что положительно влияет на безопасность проведения платежной операции.

Платежный Модуль может быть выполнен в различных вариантах исполнения. Помимо небольшого корпуса с клавиатурой, который непосредственно содержит

Элемент Безопасности с идентификационными данными, он может быть создан и таким образом, что внутри него будет находиться устройство считывания (карт-ридер) внешних карт, предпочтительно выполненных в стандартном формате ICC-карт. Данные, требующие защиты (например, пароль), можно будет загружать в чип (микросхему) карты такого типа. Чип карты также содержит определенную емкость памяти, которую можно соответствующим образом использовать для ввода данных по выполненным платежным транзакциям. По завершении рабочего дня торговый агент (представитель торгово-сервисного предприятия) может оставить основную часть Платежного Модуля в магазине, например в газетном киоске, а забрать только ICC-карту. Далее, он может подвергнуть данные этой карты обработке в банке или записать их с карты на свой домашний компьютер с помощью карт-ридера. Для нескольких передвижных торговых точек (киосков) необходимы несколько Платежных Модулей, вступающих в соединение с одной ICC-картой с идентификационными данными одного терминала и одним банковским счетом. С другой стороны, один Платежный Модуль может успешно использоваться с несколькими ICC-картами, принадлежащими разным торговым предприятиям в условиях многосменной работы в торговых помещениях одного магазина.

Необходимо предусмотреть в Платежном Модуле собственный интерфейс (устройство сопряжения), например, с USB-портом для подключения периферийных (вспомогательных) устройств, который позволяет распечатывать платежные данные прямо с Платежного Модуля или через соединительное устройство (разъем) подключиться к карт-ридеру, GPRS-модему и другим подобным устройствам.

Можно предположить, что после практического осуществления предложенной системы, мобильные устройства могут стать мишенями для атаки с целью похищения данных платежной карточки, которые находятся в состоянии постоянной готовности для взаимодействия с каналами связи мобильного устройства. В такой момент невозможно указать, в каком направлении будет развиваться ход действий атакующих хакеров, поскольку представленное решение является новым и до настоящего времени не имеет широкого применения. Тем не менее, можно предположить, что будут иметь место тенденции, направленные на злоупотребление такими качествами, как постоянная оперативность, готовность и способность к взаимодействию платежной карточки, платежного терминала или съемной карты памяти. При надлежащей конфигурации возможно снижение риска при наличии двух независимых режимов доступа к съемной карте памяти. Один предназначен и установлен для выполнения обычной функции, характерной для съемной карты памяти, находящейся в ожидании потребности в расширении емкости памяти мобильного устройства связи, например мобильного телефона. Этот режим доступа препятствует доступу к модулю, в котором находится платежная карточка, а также к элементу бесконтактной связи на съемной карте памяти. По сути, при этом режиме доступа, установленном на интерфейсе съемной карты памяти, такая карта выступает в роли обычной съемной карты памяти без элемента безопасности и без элемента связи.

Второй режим доступа предназначен и устанавливается для выполнения платежной функции съемной карты памяти, причем доступ к блоку с платежной карточкой, а также к элементу бесконтактной связи на съемной карте памяти, предоставляется устройством мобильной связи по его каналам связи через интерфейс (устройство сопряжения). В том случае, когда на съемной карте памяти размещен именно модуль с платежным терминалом, то доступ к этому модулю также обеспечивается единственно и исключительно в режиме доступа к платежной функции.

Два режима можно выбирать поочередно, при этом важно, чтобы режим доступа к платежной функции съемной карты памяти становился активным только после физического нажатия платежной кнопки на аппаратном средстве.

Съемная карта памяти, на которой размещен, по меньшей мере, один модуль с платежной карточкой, выполняет функции съемной карты памяти для расширения емкости памяти мобильного устройства через интерфейс до момента нажатия специальной платежной кнопки. После чего съемная карта памяти становится доступной через интерфейс в качестве карты с Элементом Безопасности и, по меньшей мере, с одним модулем платежной карточки.

Съемная карта памяти согласно данному варианту исполнения технического решения имеет архитектуру, предусматривающую наличие общедоступной флэш-памяти, а также аппаратно-программных элементов платежной карточки, в отдельных случаях - платежного терминала. При обычном использовании мобильного устройства съемная карта памяти выполняет функции флэш-памяти, если только в нем предусмотрена флэш-память для расширения емкости имеющейся памяти с соответствующим микроконтроллером (памяти). В этом состоянии чтение и запись файлов в памяти съемной карты памяти разрешены, однако другие элементы, например Элемент Безопасности, элемент NFC-связи, скрыты и обращение к ним и их запуск невозможены в этом режиме доступа.

Наличие специальной «платежной» кнопки на аппаратном средстве позволяет изменить статус съемной карты памяти на ее интерфейсном уровне, который связан исключительно с физическим нажатием платежной кнопки. Необходимость в физическом нажатии кнопки исключает возможность запуска платежного приложения с помощью нежелательных программных средств или сценария (скрипта), имитирующего действия пользователя.

При такой конфигурации исключается риск злонамеренного использования интерфейса съемной карты памяти с целью совершения попыток взлома элементов безопасности без ведома пользователя. Связь между физическим нажатием кнопки и запуском соответствующей прошивки мобильного телефона ("зашитой программы") может храниться в памяти таким образом, что ни при каких обстоятельствах не будет возможна ее перезапись, изменение или обновление или же это будет сделать невозможно без введения соответствующего пароля (кодового слова). Несанкционированная программа, следовательно, не может имитировать инициацию сигнала физическим нажатием кнопки таким образом, чтобы создавалось впечатление, что этот сигнал обусловлен реальным физическим нажатием кнопки, и запустить выполнение остальных команд приложения. Поскольку злоумышленник не будет иметь возможности физически нажать упомянутую кнопку на удаленном мобильном устройстве, удачные попытки неконтролируемого доступа исключены. Съемная карта памяти будет вести себя как стандартная (типовая) карта памяти, и только после физического нажатия платежной кнопки она переключится в режим платежной карточки. Завершение прикладной платежной программы автоматически переведет режим карты в обычный режим для карты - режим расширения емкости памяти карты.

Коррекция (смещение) ранее описанной процедуры запуска платежного процесса в мобильном устройстве базируется на аналогичном принципе двух режимов доступа. Этот вариант процедуры основан на том, что перед запуском платежного процесса съемная карта памяти находится в режиме доступа к обычной функции расширения емкости памяти. При этом модуль с платежной карточкой, элемент бесконтактной связи и модуль с платежным терминалом, размещенные на съемной карте памяти, будут

недоступными со стороны устройства сопряжения (интерфейса). И только исключительно после физического нажатия платежной кнопки, расположенной на аппаратном устройстве, съемная карта памяти переключится в режим доступа платежной функции съемной карты памяти с предоставлением доступа к модулю платежной карточки.

ОПИСАНИЕ ЧЕРТЕЖЕЙ

Предложенное техническое решение в деталях проиллюстрировано фиг.1-14.

На фиг.1 представлена блок-схема отдельных элементов карты памяти и показано соединение между отдельными элементами на карте памяти с одним разделенным на секции элементом безопасности, на котором хранятся защищенные данные платежного POS-терминала, к тому же из нескольких платежных карточек.

На фиг.2 представлено решение, в котором показан мобильный телефон с картой памяти в процессе проведения платежной операции в Интернет-магазине или при выполнении платежа за загруженные файлы из сети мобильной связи.

На фиг.3 представлена съемная карта памяти micro-SD-типа с двумя независимыми Элементами Безопасности и элементом связи, расположенным, как и антенна, непосредственно на карте памяти. Здесь также показана конфигурация с модулем индифферентного (нейтрального) платежного POS-терминала и с четырьмя модулями с независимыми платежными карточками разных банков.

На фиг.4 представлена предоплаченная съемная карта памяти с упрощенной архитектурой в версии с двумя элементами безопасности.

На фиг.5 представлена последовательность задач в рамках запуска прикладной платежной программы на съемной карте памяти в процессе проведения оплаты за файл, выставленный на продажу в сети мобильной связи.

На фиг.6 представлен вариант осуществления изобретения с инициатором платежа, при этом инициатор размещен рядом с контрольно-кассовым аппаратом в реально существующей торговой точке (невиртуальном магазине).

На фиг.7 приведено схематическое изображение (перспективный вид сбоку) устройства мобильной связи в виде обычного мобильного телефона, которое расположено рядом с Платежным Модулем. Размеры, форма и соотношение размеров мобильного устройства и Платежного Модуля не выдержаны, поскольку они приведены исключительно для лучшего понимания структуры системы. На фиг.7 мобильный телефон и Платежный Модуль не перекрываются для большей наглядности, однако в действительности мобильный телефон можно прикладывать прямо к поверхности Платежного Модуля.

На фиг.8 представлена проекция на базовую структуру Платежного Модуля, где видно, что элемент связи, относящийся к мобильному телефону, размещен в съемной карте памяти. Память с идентификационными данными POS-терминала размещена в съемной карте памяти. Память с идентификационными данными POS-терминала размещена в SAM-карте. На фиг.8 также представлен канал NFC-связи между съемной картой памяти и Платежным Модулем.

На фиг.9 дано схематическое представление конструкции Платежного Модуля с конфигурацией, при которой ICC-карта торгово-сервисного предприятия вставлена в корпус считывающего устройства (карт-ридера).

На фиг.10 представлена конфигурация, предусматривающая соединение с контрольно-кассовым аппаратом. Платежный Модуль содержит ICC-карт-ридер, а также имеет мини-USB-коннектор (разъем).

На фиг.11 представлена схема, демонстрирующая порядок осуществления запуска

платежной прикладной программы при нажатии платежной кнопки аппаратного средства, на которой показана локализация отдельных задач и процессов при запуске приложения на аппаратном средстве телефона (встроенной программе-прошивке мобильного телефона, съемной карте памяти).

На фиг.12 представлен вид, который имеет съемная карта памяти с внешней стороны в случае выполнения режима доступа к функции расширения памяти мобильного телефона.

На фиг.13 представлен вид, который имеет съемная карта памяти с внешней стороны в случае выполнения режима доступа к функции платежной карточки. При такой конфигурации предусматривается модуль с платежным терминалом, размещенный на съемной карте памяти.

На фиг.14 приведен пример выполнения мобильного телефона с платежной кнопкой.

ПРИМЕРЫ ОСУЩЕСТВЛЕНИЯ ИЗОБРЕТЕНИЯ

Пример 1

В этом примере демонстрируется описание изобретения с двумя независимыми Элементами Безопасности 31, 32 в соответствии с фиг.3. Применение Элементов Безопасности 31, 32 в отдельном аппаратном исполнении упрощает сертификационные требования, которые устанавливаются индивидуальными участниками платежной системы (банком-эмитентом, выпустившим карточку, оператором клирингового центра) в отношении хранения их конфиденциальных данных на Элементах Безопасности 3, 31, 32. В приведенном примере каждый из Элементов Безопасности 31, 32 также разбивается на независимые домены, которые могут быть предложены разным банкам-эмитентам карт и разным владельцам конфигурационных данных POS-терминала. Элементы Безопасности 31, 32 выполнены в виде независимых чипов на печатной плате, где они соединены с контроллером, который исполняет роль микроконтроллера 12. Взаимодействие Элементов Безопасности (соединение их) с контроллером 12 соответствует требованиям международного стандарта ISO 7816. Съемная карта памяти 1 выполнена в виде micro-SD карты. Прикладная микросхема ASIC (application-specific integrated circuit - специализированная интегральная микросхема), которая установлена для осуществления процессов связи на NFC-платформе и, таким образом, выполняет функцию элемента связи 13. соединена с микроконтроллером 12. Антенна 21, расположенная на корпусе съемной карты памяти 1, сконструирована в соответствии с описанием, приведенным в группе заявок на выдачу патентов, принадлежащих данному патентовладельцу, и подключена к прикладной ASIC микросхеме для обеспечения NFC-связи, которая независима от других аппаратных средств мобильного телефона 4. Съемная карта памяти 1 содержит также обычную флэш-память 2, например, емкостью 2 Гб. Пользователь не может получить доступ к одной из частей 20 памяти 2 через интерфейс мобильного телефона 4, поскольку эта часть памяти используется для архивирования записей по выполненным платежам. Остальная часть памяти 2 используется для обычного хранения музыкальных файлов, фотографий и подобной информации, благодаря чему в целом карта памяти 1 может использоваться пользователем как обычное запоминающее устройство. При размещении POS-терминала и платежной карточки на съемной карте памяти 1 первоначальная функция слота мобильного телефона 4, предусмотренного для расширения емкости памяти, не исчезла.

Процесс оплаты может происходить двумя разными способами. Например, как показано на фиг.6, пользователь мобильного телефона 4 принимает решение купить карту в электронной форме в Интернет-магазине. В этом случае оператор Интернет-магазина может быть производителем мобильного телефона 4. Карту памяти micro-SD

1, изготовленную в соответствии с предложенным техническим решением, вставляют в слот, расположенный сбоку мобильного телефона 4. На элементе безопасности 31 хранятся конфигурационные данные 6 POS-терминала, принадлежащие нескольким людям, в том числе и оператору Интернет-магазина. После выбора товара, который клиент намерен приобрести, на мобильный телефон 4 из Интернет-магазина направляется платежное требование на соответствующую сумму. Пользователь (клиент) нажимает платежную кнопку, которой снабжен мобильный телефон. В соответствии с другим примером проведения оплаты выбор платежа может быть инициирован "программно-реализованной" кнопкой, отображаемой на дисплее мобильного телефона 4. Запрос на запуск прикладной платежной POS-программы отправляется на интерфейс 11. Платежная прикладная программа POS-терминала запускается на карте памяти 1 так же, как при взаимодействии стандартного платежного POS-терминала и платежной карточки, которая вставлена в считывающее устройство (сканер) POS-терминала. Дисплей мобильного телефона 4 используется для управления платежным процессом. Пользователь выбирает платежную карточку, со счета которой он хочет списать требуемую сумму в счет оплаты приобретаемого товара. После активации приложения в соответствующем модуле 7 выбранной платежной карточки можно также управлять процессом проведения платежной операции по предварительно установленным правилам управления рисками, разработанными эмитентом соответствующей карточки. В соответствии с этими правилами потребуется или не потребуется ввести пароль (код) платежной карточки.

После завершения прикладной платежной программы POS-терминала связь между платежным POS-терминалом и платежной карточкой прерывается программой, и итоговая платежная криптограмма отправляется для обработки через GPRS-канал (GPRS - служба пакетной передачи данных через радиоинтерфейс) в Интернет-магазин. После того как Интернет-магазин получит и расшифрует платежный файл, он проверяет сумму проведенной оплаты и в случае положительного результата проверки товар, за который произведена оплата, в данном случае электронная географическая карта, отправляется на мобильный телефон 4.

Пример 2

В данном примере предлагается платежный терминал на платформе съемной платежной карточки micro-SD-типа, которая сопоставима по форме и параметрам со стандартной micro-SD-картой. Платежная карточка 1, как показано на фиг.1, имеет встроенный микроконтроллер 12 в виде микропроцессора разрядностью 32 бита, который работает с многофункциональной операционной системой 8 - в данном примере это Linux. Флэш-память 2, элемент безопасности 3 и SD интерфейс 11 соединены с микроконтроллером 12. Микропроцессор 12 содержит внутреннюю EEPROM-память 10 и блок загрузки операционной системы 9 (загрузчик), который контролирует несанкционированное вмешательство в загруженную прикладную платежную программу POS-терминала.

Флэш-память 2 разделена на защищенную и незащищенную части. В незащищенной части предусмотрены область 15 для широкодоступной и видимой информации пользователя, и область 20 для скрытых системных файлов, в частности, для записей платежных транзакций, которые обрабатываются платежным терминалом. В защищенной части карты памяти находится блок 8, который содержит операционную систему, в данном примере это Linux, и, по большей части, блок с прикладной платежной программой POS-терминала 5, в котором сохраняется прикладная платежная программа POS-терминала, в данном случае это приложение EMV-типа. В приведенном примере

в защищенной части памяти 2 находится также модуль управления загрузкой 19, который используется для сохранения и управления обновлением программных средств на карте памяти 1. В том случае, если необходимо загрузить/обновить приложения, находящиеся в чипе смарт-карты 3, двоичные данные приложения загружаются в незащищенную часть флэш-памяти 2, например в модуль системных данных, в пространство 20, где хранятся скрытые от пользователя данные. Модуль управления загрузкой 19 периодически проверяет наличие новых файлов в модуле системных данных, которые должны загружаться в безопасный элемент 3. Если таковые обнаружены, то запускается соответствующая инсталляция.

В защищенной части памяти 2 имеется также модуль SCWS (Smart Card Web Server - веб-сервер смарт-карт), который используется для управления приложениями, за исключением платежных EMV-приложений, хранящихся в элементе безопасности 3. В микроконтроллере 12 предусмотрено пространство памяти, где хранится операционная система (как начало и конец адресуемой области). Хеш-значение (значение хеш-функции) емкости памяти (электронно-цифровая подпись) сохраняется в микроконтроллере 12 при первом сохранении операционной системы и приложения. Впоследствии изменить эти данные будет уже невозможно, что обеспечивает защиту от несанкционированных изменений программных средств.

В элементе безопасности чипа смарт-карты 3 содержится несколько отдельных доменов. В приведенном патентном описании предлагаются три домена, используемых для хранения модулей с конфигурационными данными трех независимых терминалов 6, которые принадлежат трем различным центрам обработки платежей. Две части элемента безопасности содержат две независимые платежные карточки 7 с соответствующими платежными приложениями EMV-типа. В приведенном примере дается описание изобретения, позволяющее клиенту проводить платежи с двух разных платежных карточек в трех терминалах, принадлежащих разным платежным центрам. Например, одной из этих платежных систем может быть оператор сети, обслуживающей мобильный телефон, который осуществляет передачу данных по каналам дальней связи в службу обработки транзакций при осуществлении платежей методом прямого дебетового списания. На элементе безопасности предусмотрен также модуль RSA-кодирования 14.

Карта памяти 1 содержит также свой собственный NFC-элемент бесконтактной связи 13 с антенной 21, размещенной, соответственно, в пределах карты памяти 1. Такая конфигурация позволяет создавать NFC-соединение между обычным телефоном без NFC-чипа и соответствующим устройством считывания, отвечающим требованиям стандарта ISO 14443.

В элементе безопасности 3 имеется также модуль с приложением (программой) нефинансового характера 16, который в данном примере конфигурирован таким образом, что выполняет функции электронного бесконтактно ключа.

Контроллер 17 флэш-памяти 2 расположен в защищенной части памяти 2 и выполняет функции управления обменом данных между мобильным телефоном и флэш-памятью 2 на карте памяти 1. Контроллер 17 флэш-памяти 2 имеет возможность просмотра данных или записи их в защищенную часть памяти 2, а также обладает возможностью просмотра незащищенной части памяти 2, в которой расположен модуль системных данных (разрешается чтение и запись).

Запуск прикладной платежной программы POS-терминала выполняется на съемной карте памяти 1, которая вставлена в слот 4 мобильного устройства связи, предназначенный для дополнительного оборудования. Прикладная платежная

программа POS-терминала загружается в микроконтроллер 12, встроенный в карту памяти 1, затем происходит загрузка конфигурационных данных идентификатора выбранного терминала из элемента безопасности 3. Выбранные данные платежной карточки загружаются из элемента безопасности 3 в микроконтроллер 12, который действует как платежный терминал. Какие данные платежной карточки будут загружаться, зависит от выбора пользователя.

Загрузчик операционной системы 9 запускает контроль изменений прикладной платежной программы POS-терминала перед запуском самой прикладной платежной программы POS-терминала. Управление прикладной платежной программой POS-терминала производится с помощью кнопочной панели и дисплея мобильного устройства 4. Мобильный телефон имеет графический GUI-интерфейс (Graphic User Interface - графический пользовательский интерфейс), который деблокирует связь между пользователем, картой памяти 1 и HOST-процессором (главным процессором). В телефоне также предусмотрена SMS-технология активизации от нажатия кнопки. Прикладная платежная программа POS-терминала - это приложение SD-микроконтроллера 12, которое дает возможность проводить платежи в режиме онлайн (в реальном времени) и оффлайн (автономном режиме) с использованием платежного приложения, размещенного на micro-SD-карте памяти 1. Платеж осуществляется при условии, что "Карта имеется в наличии", это значительно повышает уровень безопасности - транзакция подписывается криптограммой и при выполнении каждой транзакции ATC-счетчик (счетчик транзакций карты) увеличивается на единицу (число совершенных транзакций), что означает невозможность формирования неограниченного числа транзакций для получения определенных ключей. Клиент управляет прикладной платежной программой POS-терминала через GUI-приложение, которое установлено на его личном телефоне. В данном примере прикладная платежная программа POS-терминала в совокупности с микроконтроллером 12 образует общий POS-терминал (Generic POS terminal). При другой конфигурации общий POS-терминал может быть образован прикладной платежной программой POS-терминала и вычислительным элементом, который расположен непосредственно в чипе с элементом безопасности. Впоследствии вместе с конфигурационными параметрами они будут создавать ВСТРОЕННЫЙ POS-ТЕРМИНАЛ (EMBEDDED POS TERMINAL): Terminal_type 1x = терминал, который принадлежит финансовой организации, 2x = терминал, который принадлежит торговой организации, 3x = терминал, который принадлежит владельцу карточки - терминал владельца карточки (Card holder terminal). Блок с конфигурационными данными терминала 6 содержит ID-номер (идентификационный номер) терминала, PDOL-данные (Processing Option Data Object List - список объектов данных и опций обработки), проверку рисков (Terminal Risk Management), формат командного файла в оффлайн-режиме, SMS-шлюз (канал) на HOST, IP-адрес на главном процессоре (HOST), код для подписи оффлайн-транзакций. Платеж может осуществляться в оффлайн- или онлайн-режиме. Взаимодействие с платежной системой может осуществляться посредством SMS-сообщений или посредством системы GPRS (система пакетной передачи данных с помощью радиосвязи).

Пример 3

В данном примере описывается съемная карта памяти 1, которая содержит только минимальный набор элементов, необходимый для осуществления платежей. Структура такой карты приведена на фиг.4. Этот вид съемной карты памяти специально разработан для продажи в качестве предоплаченной платежной карточки с предварительно введенной денежной суммой, которая предназначена, например, для продажи туристам,

прибывшим из страны, где в обращении находится другая валюта. Съемная карта памяти 1 содержит интерфейс 11 с контактами, выполненными в соответствии со спецификацией для micro-SD-технологий. В пластиковом корпусе съемной карты памяти 1 имеются два Элемента Безопасности 31, 32. В первом Элементе Безопасности 31 содержатся конфигурационные данные POS-терминала, сформированные системным оператором предоплаченной карты. Во втором Элементе Безопасности 32 содержатся данные платежной карточки для осуществления одноразового платежа. Наряду со съемной картой памяти 1 промышленно выпускаемый комплект содержит также бумагоноситель с буфером для временного хранения текста, в котором находится соответствующий PIN-код доступа к платежной карточке. Карта памяти 1 выполняет все операции, которые выполняет обычный POS-терминал, арендуемый торговой точкой, при взаимодействии с платежной карточкой клиента в процессе оплаты. Технические средства, которыми располагает мобильный телефон 4, используются для отображения и обмена информацией.

Пример 4

В данном примере система дополнена инициатором прикладной платежной программы POS-терминала 22. Он может быть выполнен в виде узкоспециализированного устройства с элементом NFC-связи. В приведенном примере инициатор устанавливает связь с выходом контрольно-кассового аппарата, который будет выдавать на выходе информацию об общей сумме платежа, подлежащей к оплате. Инициатор 22 создает файл, который содержит общую стоимость покупки, информацию (реквизиты) о счете получателя платежа (торговой организации) и команду запроса. Инициатор 22 отправляет этот файл на мобильный телефон 4, который прикладывается к инициатору, через элемент связи 24. Получение файла, который поступает на карту памяти 1, приводит к запуску прикладной платежной программы POS-терминала. Этот вариант осуществления изобретения позволяет использовать платежный терминал, имеющийся в мобильном телефоне 4 пользователя, для выполнения платежей методом прямого дебетового списания в обычных магазинах, в распоряжении которых нет своего собственного POS-терминала.

Пример 5

В данном примере, который иллюстрируется фиг.3, 7 и 8, предлагается система, предусматривающая наличие Платежного Модуля 28, находящегося в распоряжении торгово-сервисного предприятия и представляющего собой узкоспециализированное устройство в виде корпуса, который содержит панель с цифровой клавиатурой 36, дисплей 37 и автономный источник питания в виде перезаряжаемого аккумулятора. Платежный Модуль 28 содержит элемент NFC-связи 35 с антенной 21, расположенной под плоскостью верхней крышки, на внешней стороне которой находится центровая точка (отверстие) антенны 21, графически отмеченная ориентирующим целевым знаком 40. В составе аппаратных средств на SAM-карте 42 Платежный Модуль 28 содержит Элемент Безопасности 6, в который загружается идентификатор платежного POS-терминала 27, а также Мастер-ключ (главный ключ) для шифрования данных, передаваемых по сети. В другом варианте исполнения данные могут загружаться непосредственно в защищенную память на печатной схеме Платежного Модуля 28.

Торговый агент использует Платежный Модуль 28 таким образом, что при осуществлении продажи он с помощью клавиатуры 36 вводит сумму, которую он хотел бы получить за товары, отображаемую на дисплее 37. После проверки суммы, высветившейся на дисплее 37, торговый агент нажимает кнопку подтверждения. Затем идентификационные данные платежного POS-терминала 27 шифруются с использованием

главного ключа (Master Key). Таким образом, зашифрованные данные вместе с причитающейся к оплате суммой отсылаются на элемент NFC-связи 35, который, в свою очередь, отправляет зашифрованное сообщение с помощью антенны 41 и ожидает, когда мобильное устройство 4 будет приложено к Платежному Модулю 28. Пользователь мобильного телефона 4 включает запуск платежного приложения либо с помощью специального кнопочного пульта в аппаратном исполнении, либо с помощью программно реализуемой кнопки. После формирования канала NFC-связи зашифрованные данные с Платежного Модуля 28 будут прочтены и расшифрованы, итогом этого будут идентификационные данные POS-терминала 27 и необходимая сумма платежа.

Эта часть передачи данных может быть выражена как

$$3DES[Mk\{Cfg\}] \xrightarrow{NFC} 3DES^{-1}[Mk\{Cfg\}]=Cfg,$$

где 3DES означает шифрование путем трехкратного повторения алгоритма шифрования данных по стандарту DES; Mk - Мастер ключ (Master Key), предоставляемый платежной системой; Cfg означает конфигурационные данные; и NFC представляет канал передачи данных между Платежным Модулем и съемной картой памяти.

Покупатель может проверить оплаченную им сумму на дисплее своего мобильного устройства 4. Идентификационные данные, поступившие с Платежного Модуля 28, пригодны для того, чтобы индифферентный (нейтральный) POS-терминал 27 на съемной карте памяти 1 стал специфическим платежным POS-терминалом 27 данного торгового агента (торгово-сервисного предприятия).

Этот процесс может быть выражен в виде

Cfg + Generic POS=ACg POS,

где Generic POS представляет идентификацию индифферентного, общего платежного терминала (POS), а ACg POS - это POS соответствующей торговой организации.

В дальнейшем прикладная программа платежного терминала выполняется в обычном порядке, например, в соответствии с EMV-стандартом. С учетом предварительно установленных рисков для платежной карточки 7 и в зависимости от размера суммы, подлежащей к оплате, может быть направлен запрос пароля, PIN-кода, которые вводятся покупателем на кнопочной панели его мобильного устройства 4. При этом обеспечивается высокий уровень безопасности, поскольку приложение платежного терминала запускается прямо на съемной карте памяти 1, где хранятся также модули платежных карточек 7, а конфиденциальные данные остаются внутри аппаратного средства, реализующего соединение между Платежным Модулем 28 и съемной картой памяти 1. Результатом выполнения платежного приложения является создание платежной криптограммы, которая отсылается на Платежный Модуль 28, а в случае проведения онлайн-платежа отправляется через интерфейс 11 в мобильное устройство 4, а затем через мобильную сеть связи - в центр обработки платежей. Платежная криптограмма может быть также сформирована и отправлена в соответствии со схемой отношений

$$3DES[Mk\{Transaction\}] \xrightarrow{NFC}$$

применительно к центру обработки платежей как

$$3DES[Mk\{Transaction\}] \xrightarrow{GPRS}$$

Съемная карта памяти в этом случае представляет собой micro-SD-карту.

Пример 6

В данном примере в соответствии с фиг.4 Платежный Модуль 28 представлен в виде

устройства, которое содержит слот для ICC-карты 29 с устройством считывания соответствующего формата. Торговая организация (получатель платежа) может купить Платежный Модуль 28 где угодно, и этот Платежный Модуль 28 не имеет своих собственных идентификационных данных (идентификатора). Торговая организация получает ICC-карту 29 с общепринятыми параметрами согласно ISO 7810 85.60×53.98 мм в банке или центре обработки платежей. Главный ключ (Мастер-ключ), полученный из центра обработки платежей, а также идентификационные данные POS-терминала, присваиваемые соответствующей торговой организации, загружаются в Элемент Безопасности, размещенный на чипе ICC-карты. При размещении ICC-карты 29 в устройстве считывания (карт) образуется Платежный Модуль 28, выполненный в соответствии с приведенным описанием. Платежный Модуль 28 содержит также мини-B USB-разъем 39, через который можно подключить принтер, компьютер и другие входные или выходные устройства при расширенной конфигурации. Обслуживание и работа Платежного Модуля 28 производятся аналогично первому случаю. Однако имеется отличие, которое состоит в том, что после осуществления операции торговый агент извлекает свою ICC-карту 29 и может взять ее, например, в банк для проведения оффлайн-платежей. Не исключается также использование такого вида ICC-карт 29 непосредственно в банкоматах. Кроме того, предложенное решение обладает и другими преимуществами: ICC-карта отличается простотой в обращении, имеет удобные размеры и извлекается из Платежного Модуля 28, что предупреждает ее хищение из торговых помещений, например, в ночное время. ICC-карта 29 также имеет пространство для последующей финансовой операции и создания резервной копии данных в компьютере с простым устройством считывания.

Преимуществом предложенной конфигурации является возможность использования одного Платежного Модуля вместе со считывающим устройством, дисплеем 37 и клавиатурой 36 несколькими торговыми точками, работающими посменно в одних и тех же торговых помещениях, поскольку платежные суммы зачисляются в пользу той торговой организации, чья ICC-карта 29 вставлена в считывающее устройство в данный момент.

Пример 7

Кроме элементов, указанных в предыдущих примерах, Платежный Модуль 28, приведенный на фиг.5, также содержит интерфейс RS232 (Рекомендованного стандарта 232), посредством которого он может подключаться к контрольно-кассовому аппарату 26. В данном примере Платежный Модуль 28 представляет собой расширение (дополнительное устройство) к имеющемуся в наличии кассовому аппарату 26 торговой организации POS-терминала 27, учитывая, что прикладная платежная программа терминала, как и ранее, запускается и выполняется на съемной карте 1, которая наряду с мобильным устройством 4 является собственностью клиента.

Через кабельную линию 38 итоговая сумма с контрольно-кассового аппарата 26 поступает на Платежный Модуль 28, на дисплее 37 которого она высвечивается, и торговая организация подтверждает ее нажатием соответствующей кнопки. Далее процесс протекает точно так же, как если бы сумма к оплате была введена через клавиатуру 36 Платежного Модуля 28. В связи с этим нет необходимости в наличии клавиатуры для ввода суммы, подлежащей оплате в Платежном Модуле 28. Тем не менее, с целью обеспечения широкой применимости Платежного Модуля 28 в различных системах клавиатура 36 включена как часть Платежного Модуля 28 даже в этом примере.

Пример 8

В данном примере в соответствии с фиг.11-14 описывается система, в которой съемная карта памяти 1 представляет собой карту micro-SD-типа. Здесь используются два Элемента Безопасности 3, которые размещаются на карте, причем один Элемент Безопасности 3 предназначен для блока платежной карточки 7, или, соответственно, для нескольких модулей платежных карточек 7 разных банков-эмитентов, а второй Элемент Безопасности 3 содержит модуль платежного терминала 5. В другом примере осуществления изобретения съемная карта памяти 1 содержит один только модуль платежной карточки 7 без модуля платежного терминала 5, местоположение которого установлено.

Съемная карта памяти 1 с общей флэш-памятью 2 имеет интерфейс 11 общего micro-SD-стандарта и вставляется в слот мобильного устройства 4. Это обычный слот, специально предусмотренный для размещения устройств для расширения памяти.

В этом примере элемент NFC-связи 13 с антенной 21 размещен на съемной карте памяти 1. Мобильное устройство 4 снабжено платежной кнопкой 44, расположенной рядом с кнопочным пультом 45 (мобильного устройства). Платежная кнопка 44 соединена с микропереключателем на мобильном устройстве 4. Конкретное исполнение микропереключателя не имеет значения, он может быть выполнен в виде разнообразных устройств, например, в виде мембранного переключателя, емкостного переключателя и других подобных устройств.

Платежная кнопка 44 связана со встроенными программными средствами таким образом, что единственно приемлемая команда для изменения режима доступа к карте памяти 1 может поступать от контакта платежной кнопки 44, по крайней мере, в том случае, если мобильное устройство 4 снабжено такой платежной кнопкой 44. Если же в слот мобильного устройства 4 будет вставлена та же самая съемная карта памяти 1 и не будет предусмотрена выполненная на базе аппаратных средств целевая платежная кнопка 44, то изменение режима доступа будет осуществляться с помощью меню на дисплее 46 мобильного устройства 4. В таком случае съемная карта памяти 1 будет функциональной в обоих режимах доступа, но при этом соединение в целом с устройством мобильной связи 4 будет обладать более низким уровнем безопасности в отношении проведения платежного процесса.

В мобильном телефоне, который снабжен платежной кнопкой 44, доступ к Элементу Безопасности 3 на съемной карте памяти способами, отличными от доступа через предварительно установленную «прошивку» (встроенные программы), связанную с платежной кнопкой 44, будет невозможен. В данном примере такой «прошивкой» будет LGM-приложение (программа лояльности и контроля подлинности товара)

Два режима доступа могут иметь следующие характеристики:

Функция	Режим доступа расширение памяти	Режим доступа к платежной функции
Чтение/запись файлов	ДА	ДА
NFC-связь	НЕТ	НЕТ
Расширенный доступ (SDIO…)	ДА/НЕТ	ДА
	В соответствии с типом телефона	
Доступ к SE (элемент безопасности) из приложения в телефоне	НЕТ	ДА
Файл-кэш (сверхоперативной памяти) во флэш-памяти	ДА/НЕТ	НЕТ
	В соответствии с типом телефона	
Стабильное энергоснабжение	ДА/НЕТ	ДА
Карты	В соответствии с типом телефона	

В режиме доступа к платежной функции функция кэширования (записи в кэш-память) файлов на съемной карте памяти 1 будет отключена, доступ к флэш-памяти 2 и доступ в систему файлов (флэш-памяти) будет поддерживаться.

В случае, когда мобильное устройство 4 поддерживает интерфейс связи (коммуникационный интерфейс) более высокого уровня, например стандарт SDIO (Secure Digital Input Output - стандарт, поддержка которого позволяет использовать со слотом расширения формата SD/MMS соответствующую периферию), McEX, доступ к соответствующему интерфейсу может быть открыт даже в режиме доступа к платежной функции.

ПРОМЫШЛЕННАЯ ПРИМЕНИМОСТЬ

Промышленная применимость изобретения очевидна. Используя данное изобретение, можно на постоянной основе в промышленном масштабе изготавливать и использовать платежные терминалы, встроенные в карты памяти, включая помещение одной или нескольких платежных карточек в одну карту памяти. Кроме того, можно создавать и использовать платежные POS-терминалы, которые создаются временно с целью проведения конкретной платежной операции при установлении связи между Платежным Модулем и устройством мобильной связи. Впоследствии формируются необходимые структуры POS-терминала торговой организации, но только после того, как будет установлена связь со съемной картой памяти, размещенной в мобильном устройстве клиента, выполняющего платеж.

В соответствии с настоящим изобретением можно на постоянной основе в промышленном масштабе изготавливать мобильные устройства связи с дополнительно введенной платежной кнопкой, реализованной на уровне аппаратных средств, которая будет представлять собой селектор текущего режима доступа к съемной карте памяти.

СПИСОК ОБОЗНАЧЕНИЙ

1 - карта памяти
2 - память
3 - элемент безопасности
31 - Элемент Безопасности POS-терминала
32 - Элемент Безопасности платежной карточки
4 - устройство мобильной связи
5 - приложение (прикладная программа) POS-терминала
6 - модуль конфигурационных данных терминала
7 - модуль платежной карточки
8 - модуль (блок) операционной системы
9 - модуль загрузчика (операционной системы)
10 - внутренняя память микроконтроллера
11 - интерфейс
12 - микроконтроллер
13 - элемент связи
14 - блок шифрования (формирования криптограмм)
15 - открытое для доступа пространство пользовательских данных
16 - модуль приложения нефинансового характера
17 - контроллер флэш-памяти
18 - модуль web-сервера
19 - модуль управления загрузкой
20 - пространство скрытых данных
21 - антенна

22 - инициатор
23 - компьютер получателя платежа
24 - элемент связи инициатора
25 - центры обработки платежей (процессинговые центры)
26 - контрольно-кассовый аппарат
27 - платежный POS-терминал
28 - Платежный Модуль
29 - ICC-карта
35 - элемент связи Платежного Модуля
36 - клавиатура
37 - дисплей
38 - соединение с контрольно-кассовым аппаратом
39 - внешний коннектор (разъем)
40 - целевой знак
41 - антенна Платежного Модуля
42 - SAM-карта
43 - временное бесконтактное соединение
44 - платежная кнопка
45 - кнопочная панель мобильного устройства связи
46 - дисплей.

Формула изобретения

1. Устройство мобильной связи с функцией платежного терминала, содержащее устройство (4) мобильной связи со съемной картой (1) памяти, адаптированной для установки в соответствующий слот устройства (4) мобильной связи и имеющей связанные между собой интерфейс (11), микроконтроллер (12) с внутренней памятью (10) и блоком (9) загрузки операционной системы, элемент (3) безопасности с защищенными областями (31, 32) его памяти, и память (2) карты (1) памяти, разделенную на незащищенную часть и защищенную часть, причем последняя имеет модуль (5) с прикладной платежной программой платежного терминала, контроллер (17) и модуль (19) управления загрузкой операционной системы, при этом элемент (3) безопасности снабжен размещенными отдельно друг от друга модулем (6) с конфигурационными данными платежного терминала и модулем (7) платежной карточки, а защищенные области памяти (31, 32) элемента (3) безопасности соединены с микроконтроллером (12), который соединен с интерфейсом (11), подключенным к каналу (13) связи карты (1) памяти с возможностью формирования платежной операции при установлении связи между торгово-сервисным предприятием и съемной картой (1) памяти.

2. Устройство по п.1, отличающееся тем, что элемент (3) безопасности выполнен в виде микросхемы, имеющей модуль (7) платежной карточки и модуль (6) с конфигурационными данными платежного терминала, отделенные друг от друга в защищенных областях (31, 32).

3. Устройство по любому из пп.1 или 2, отличающееся тем, что съемная карта (1) памяти выполнена в формате карты из группы: карта SD-типа, mini-SD-карта, micro-SD- карта или карта M2-типа, а ее интерфейс (11) выполнен в виде интерфейса из группы: интерфейс SD-типа или интерфейс M2-типа.

4. Устройство по любому из пп.1 или 2, отличающееся тем, что внутренняя память (10) микроконтроллера (12) выполнена защищенной от стирания.

5. Устройство по любому из пп.1 или 2, отличающееся тем, что карта (1) памяти

содержит, по меньшей мере, двухпроводную шину (передачи) данных.

6. Устройство по п.5, отличающееся тем, что карта (1) памяти снабжена антенной (21), которая соединена с элементом (13) связи карты (1) памяти.

7. Устройство по любому из пп.1 или 2, отличающееся тем, что элемент (3) безопасности содержит, по меньшей мере, два модуля (6) с конфигурационными данными разных платежных терминалов.

8. Устройство по любому из пп.1 или 2, отличающееся тем, что элемент (3) безопасности содержит, по меньшей мере, два модуля (7) разных платежных карточек.

9. Устройство по любому из пп.1 или 2, отличающееся тем, что блок (9) загрузки операционной системы микроконтроллера (12) выполнен с возможностью контроля вмешательств в платежную программу.

10. Устройство по любому из пп.1 или 2, отличающееся тем, что память (2) карты (1) памяти выполнена в виде флэш-памяти (2) и содержит модуль (18) Интернет сервера.

11. Устройство по любому из пп.1 или 2, отличающееся тем, что память (2) карты (1) памяти имеет в незащищенной части область (20) данных, скрытых от пользователя, и область (15) данных, открытых для доступа пользователя.

12. Устройство по любому из пп.1 или 2, отличающееся тем, что оно снабжено инициатором (22) прикладной платежной программы платежного модуля (28) торгово-сервисного предприятия, содержащего модуль, генерирующий сумму, подлежащую оплате; при этом инициатор (22) снабжен элементом (24) связи, совместимым с элементом (13) связи на съемной карте (1) памяти или с элементом связи мобильного устройства (4) связи.

13. Устройство по любому из пп.1 или 2, отличающееся тем, что устройство (4) мобильной связи снабжено платежной кнопкой (44), а съемная карта (1) памяти выполнена с возможностью реализации режимов:

- режим доступа к функции расширения емкости памяти устройства (4) мобильной связи и блокирования доступа к элементу (3) безопасности и к элементу (13) бесконтактной связи на съемной карте (1) памяти;

- режим доступа к платежной функции съемной карты (1) памяти при нажатии платежной кнопки (44) с разрешенным доступом к элементу (3) безопасности и модулю (5) с прикладной платежной программой платежного терминала, а также с активацией элемента (13) бесконтактной связи на съемной карте (1) памяти.

14. Устройство мобильной связи с функцией платежного терминала, содержащее платежный модуль (28) торгово-сервисного предприятия и устройство (4) мобильной связи со съемной картой (1) памяти, адаптированной для установки в соответствующий слот устройства (4) мобильной связи и имеющей связанные между собой интерфейс (11), микроконтроллер (12), элемент (3) безопасности с защищенными областями (31, 32) его памяти, модуль (5) с прикладной платежной программой платежного терминала и память (2) карты (1) памяти, при этом элемент (3) безопасности снабжен модулем (7) платежной карточки и соединен с микроконтроллером (12), который соединен с интерфейсом (11), подключенным к каналам (13) связи карты (1) памяти с возможностью формирования платежной операции в момент создания временного бесконтактного канала (43) связи между модулем (7) платежной карточки на съемной карте (1) памяти и платежным модулем (28) торгово-сервисного предприятия, снабженным модулем (6) с конфигурационными данными платежного терминала.

15. Устройство по п.14, отличающееся тем, что платежный модуль (28) имеет ключ шифрования и содержит элемент (35) связи с антенной (41) для установления соединения со съемной картой (1) памяти.

16. Устройство по любому из пп.14 или 15, отличающееся тем, что модуль (6) с конфигурационными данными платежного терминала размещен на SAM-карте (42), установленной в платежный модуль (28), или модуль (6) с конфигурационными данными платежного терминала размещен на ICC-карте (29), которая установлена в считывающее устройство платежного модуля (28).

17. Устройство по любому из пп.14 или 15, отличающееся тем, что платежный модуль (28) снабжен клавиатурой (36) для введения суммы, подлежащей оплате, и дисплеем (37).

18. Устройство по любому из пп.14 или 15, отличающееся тем, что элемент (3) безопасности содержит, по меньшей мере, два модуля (7) разных платежных карточек.

19. Устройство по любому из пп.14 или 15, отличающееся тем, что платежный модуль (28) снабжен соединителем (39) для подключения внешних устройств.

20. Устройство по любому из пп.14 или 15, отличающееся тем, что платежный модуль (28) выполнен с соединением (38) с контрольно-кассовым аппаратом (26).

21. Устройство по любому из пп.14 или 15, отличающееся тем, что устройство (4) мобильной связи снабжено платежной кнопкой (44), а съемная карта (1) памяти выполнена с возможностью реализации режимов:

- режим доступа к функции расширения емкости памяти устройства (4) мобильной связи и блокирования доступа к элементу (3) безопасности и к элементу (13) бесконтактной связи на съемной карте (1) памяти;

- режим доступа к платежной функции съемной карты (1) памяти при нажатии платежной кнопки (44), с разрешенным доступом к элементу (3) безопасности и модулю (5) с прикладной платежной программой платежного терминала, а также с активацией элемента (13) бесконтактной связи на съемной карте (1) памяти.

22. Способ осуществления платежной операции, предусматривающий установление временного канала связи между торгово-сервисным предприятием и модулем (7) платежной карточки на съемной карте (1) памяти, установленной в устройство (4) мобильной связи и снабженной модулем (5) с прикладной платежной программой платежного терминала, которая загружается в микроконтроллер (12), размещенный в съемной карте (1) памяти, при этом из элемента (3) безопасности в микроконтроллер (12) загружаются конфигурационные данные платежного терминала и данные о выбранной платежной карточке, а связь с модулем (7) платежной карточки осуществляется по каналам (13) связи съемной карты (1) памяти.

23. Способ по п.22, отличающийся тем, что в процессе или перед инициацией программы платежного терминала осуществляется контроль вмешательств в прикладную платежную программу платежного терминала с помощью блока (9) загрузки операционной системы микроконтроллера (12).

24. Способ по любому из пп.22 или 23, отличающийся тем, что управление запуском прикладной программы платежного терминала осуществляется с помощью входного устройства мобильного устройства (4) связи, преимущественно, в виде кнопочной коммутационной панели.

25. Способ по любому из пп.22 или 23, отличающийся тем, что данные о запрашиваемой сумме платежа вводятся в прикладную программу платежного терминала с помощью инициатора (22), который отсылает данные о требуемой сумме платежа вместе с командой инициирования программы платежного терминала по каналу бесконтактной связи.

26. Способ по п.22, отличающийся тем, что перед осуществлением платежного процесса съемная карта (1) памяти находится в режиме доступа к функции расширения

емкости памяти и модуль (7) платежной карточки недоступен со стороны интерфейса (11), а после физического нажатия платежной кнопки (44) устройства (4) мобильной связи съемная карта (1) памяти переключается в режим доступа к модулю (7) платежной карточки, причем элемент (3) безопасности с модулем (5) с прикладной платежной программой платежного терминала становится доступным после переключения съемной карты (1) памяти в режим доступа к модулю (7) платежной карточки, а после завершения и/или прерывания платежного процесса съемная карта (1) памяти переключается в режим доступа к функции расширения емкости памяти устройства (4) мобильной связи.

27. Способ осуществления платежной операции, предусматривающий установление временного бесконтактного канала (43) связи между платежным модулем (28) торгово-сервисного предприятия, снабженным модулем (6) с конфигурационными данными платежного терминала, и модулем (7) платежной карточки на съемной карте (1) памяти, установленной в устройство (4) мобильной связи и снабженной модулем (5) с прикладной платежной программой платежного терминала, причем конфигурационные данные платежного терминала загружаются на съемную карту (1) памяти из платежного модуля (28) предпочтительно через канал связи с криптографической защитой, а связь с модулем (7) платежной карточки осуществляется по каналам (13) связи съемной карты (1) памяти.

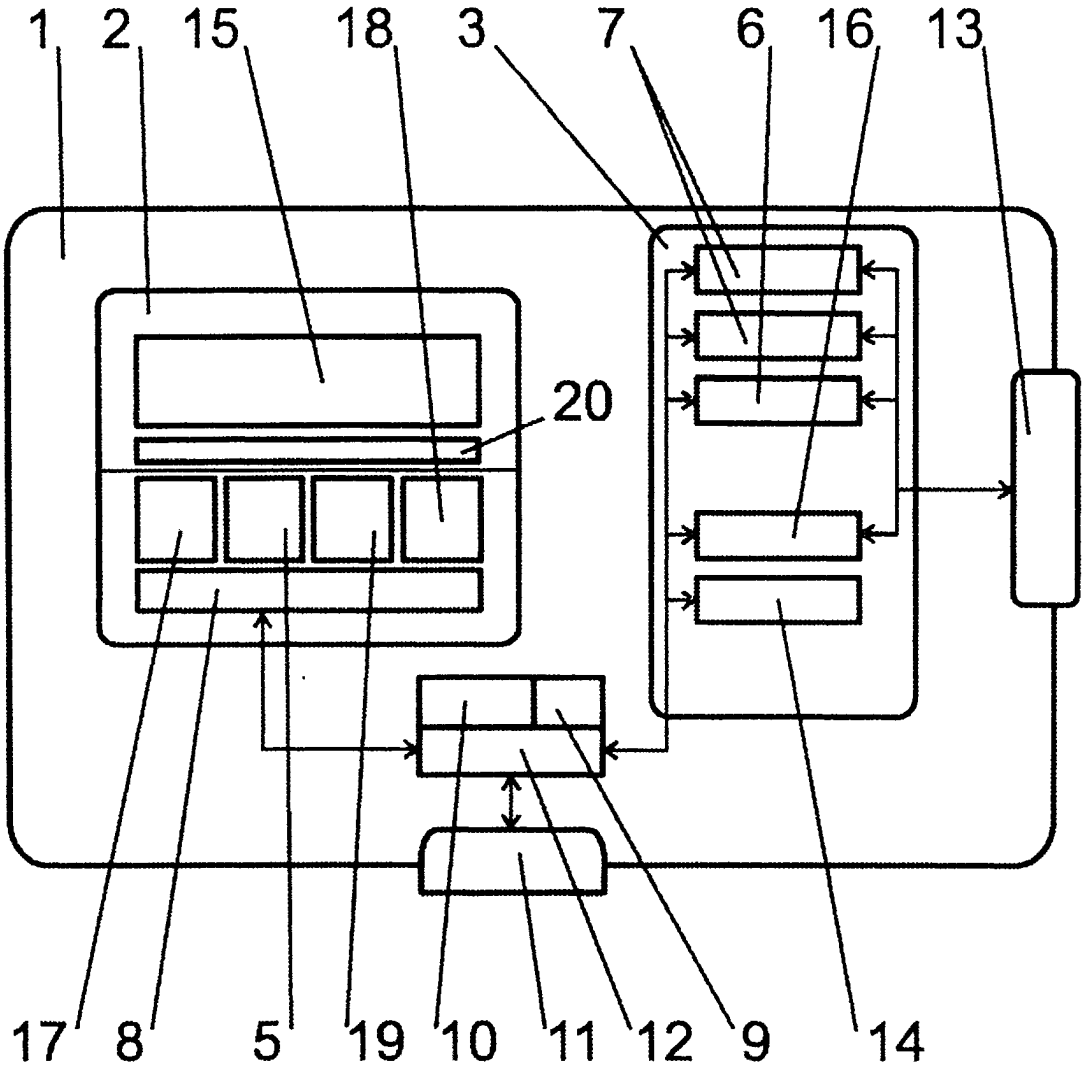
28. Способ по п.27, отличающийся тем, что конфигурационные данные платежного терминала загружаются на съемную карту (1) памяти из платежного модуля (28) предпочтительно через канал связи с криптографической защитой.

29. Способ по п.28, отличающийся тем, что создается платежная криптограмма, которая отсылается в платежный модуль (28), где хранится в памяти архива выполненных платежей.

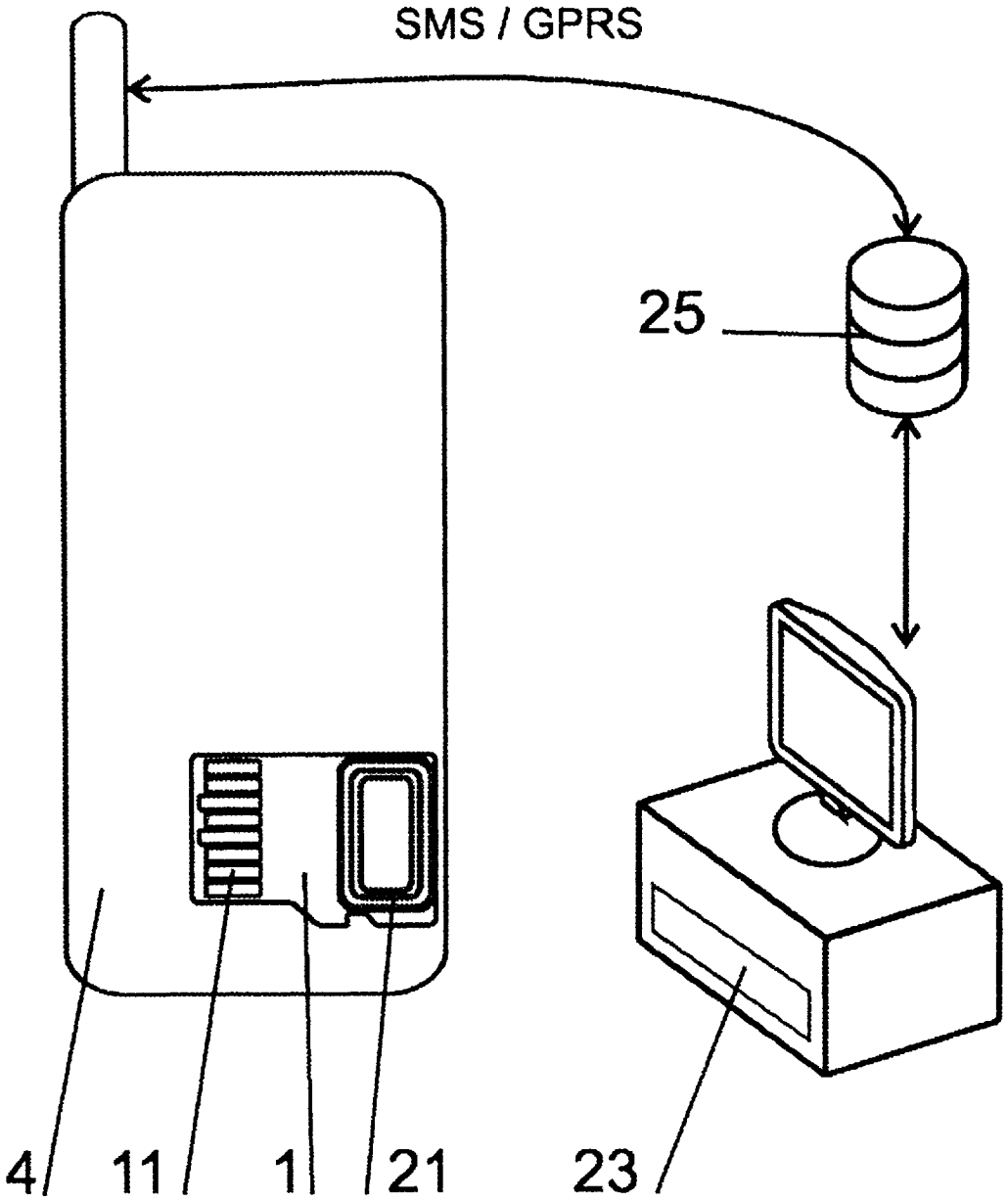
30. Способ по п.29, отличающийся тем, что, после создания платежной криптограммы она отсылается посредством интерфейса (11) и далее при помощи устройства (4) мобильной связи в центр (25) обработки платежей либо носитель с данными о выполненных платежах передается в центр (25) обработки платежей для обработки после его извлечения из платежного модуля (28).

31. Способ по любому из пп.27 или 28, отличающийся тем, что данные о сумме платежа вводятся в съемную карту (1) памяти из платежного модуля (28) путем ручного ввода при помощи клавиатуры (36) или при помощи связи (38) с контрольно-кассовым аппаратом (26).

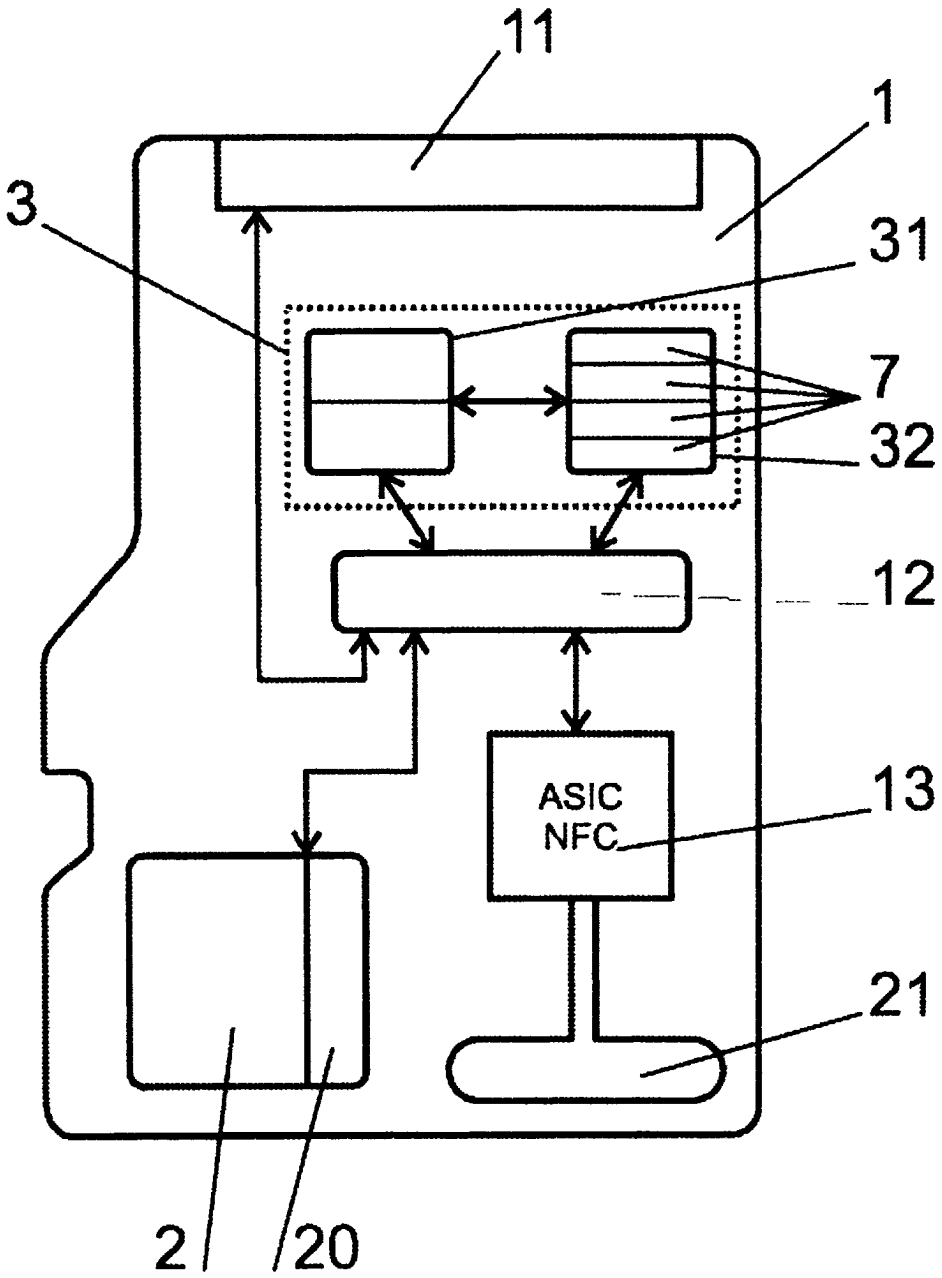
32. Способ по п.27, отличающийся тем, что перед осуществлением платежного процесса съемная карта (1) памяти находится в режиме доступа к функции расширения емкости памяти и модуль (7) платежной карточки недоступен со стороны интерфейса (11), а после физического нажатия платежной кнопки (44) устройства (4) мобильной связи съемная карта (1) памяти переключается в режим доступа к модулю (7) платежной карточки, причем элемент (3) безопасности с модулем (5) с прикладной платежной программой платежного терминала становится доступным после переключения съемной карты (1) памяти в режим доступа к модулю (7) платежной карточки, причем после завершения и/или прерывания платежного процесса съемная карта (1) памяти переключается в режим доступа к функции расширения емкости памяти устройства (4) мобильной связи.



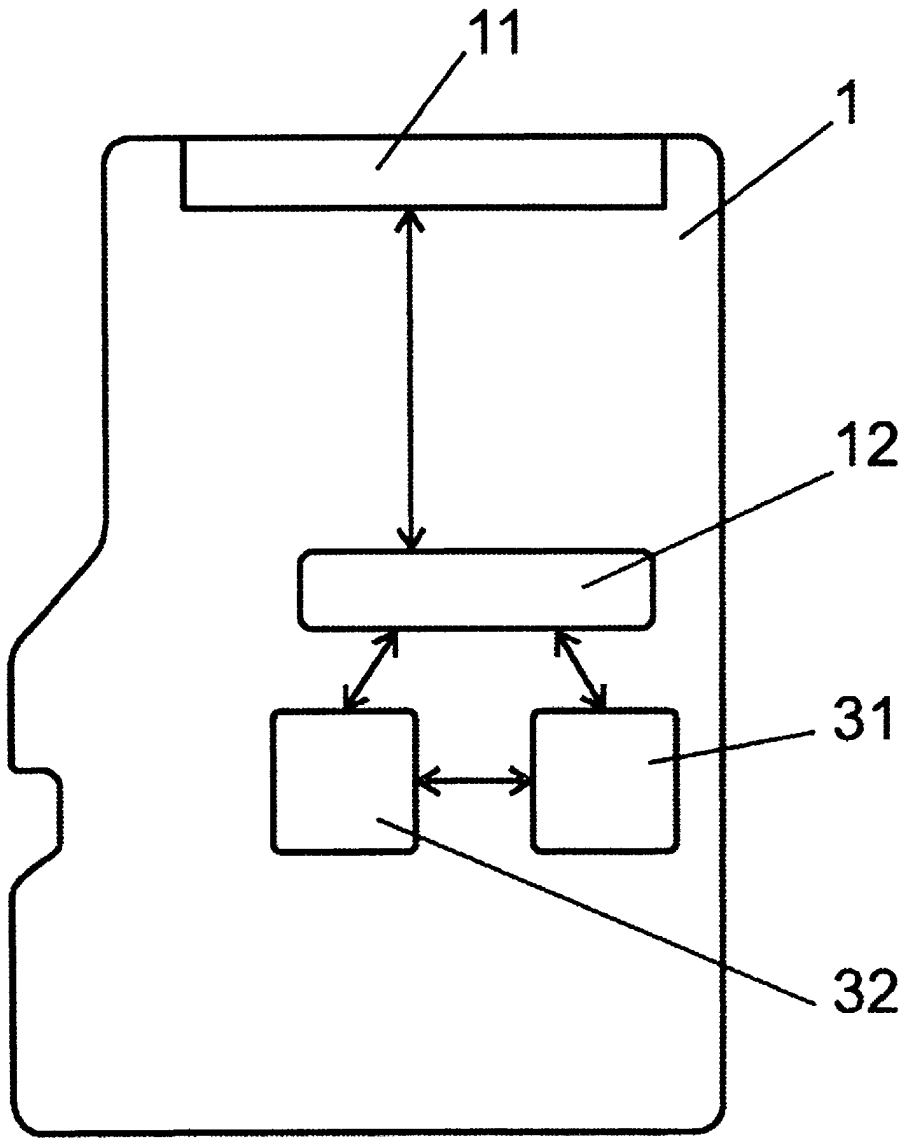
Фиг.1



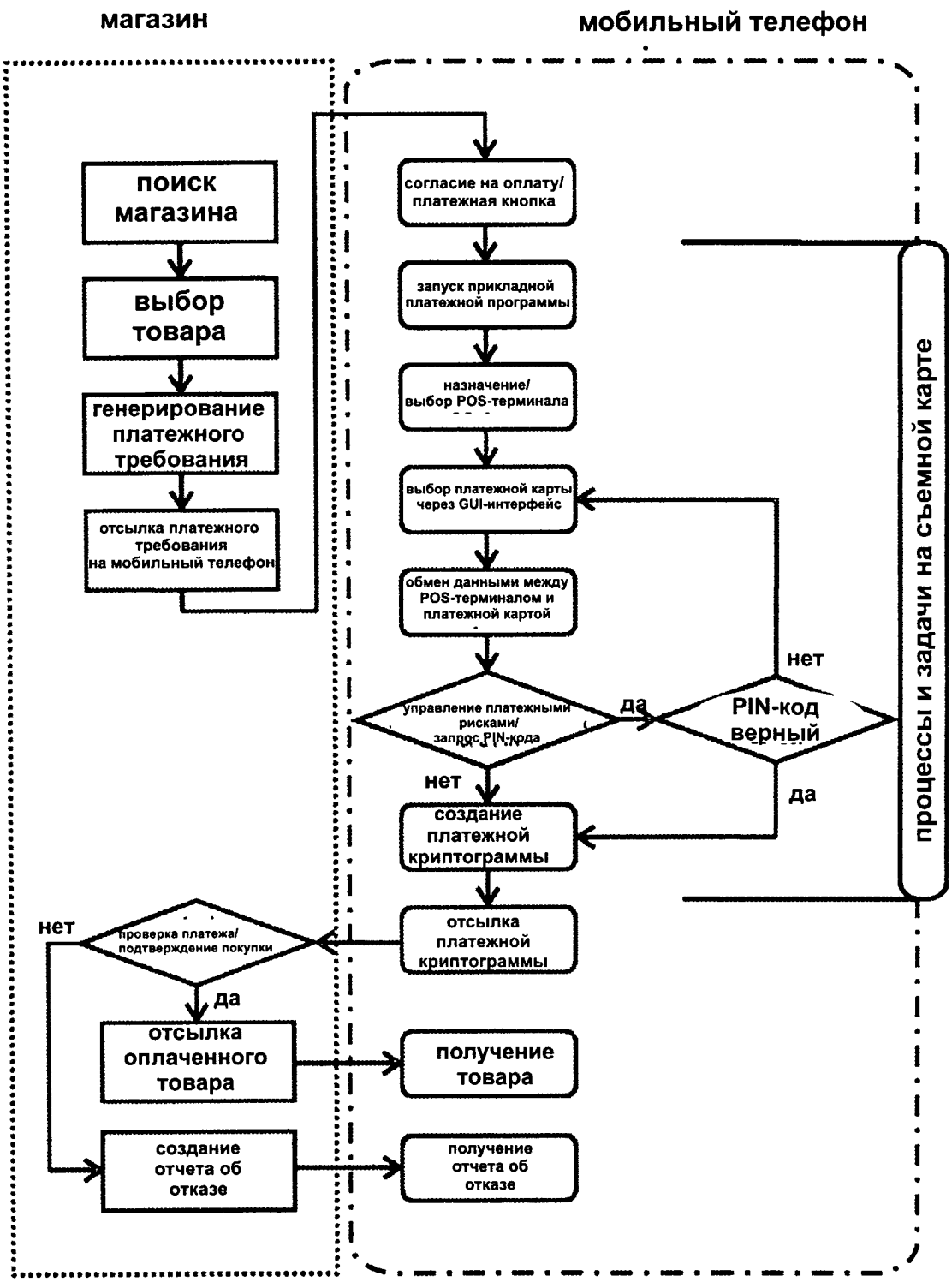
Фиг.2



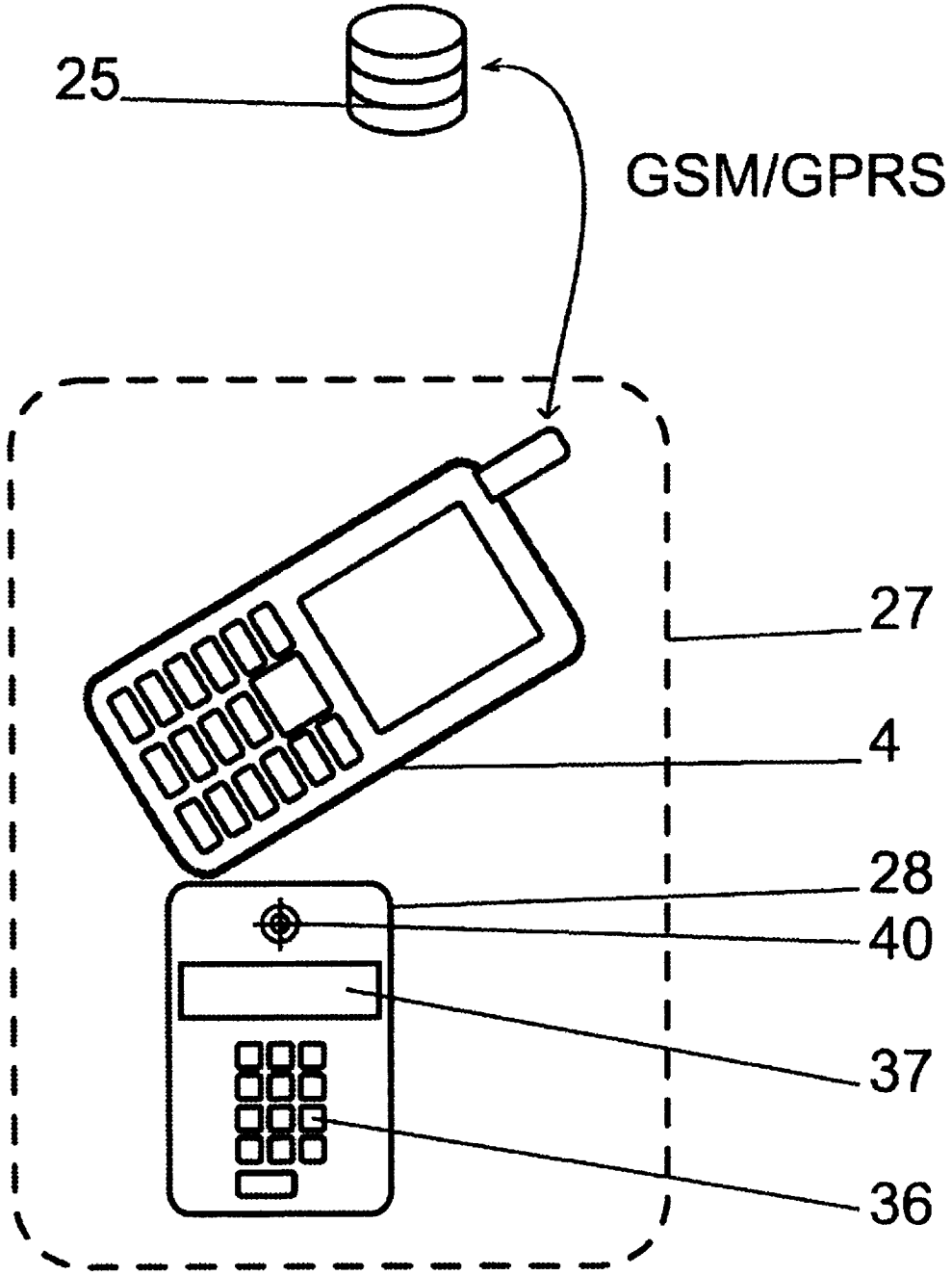
Фиг.3



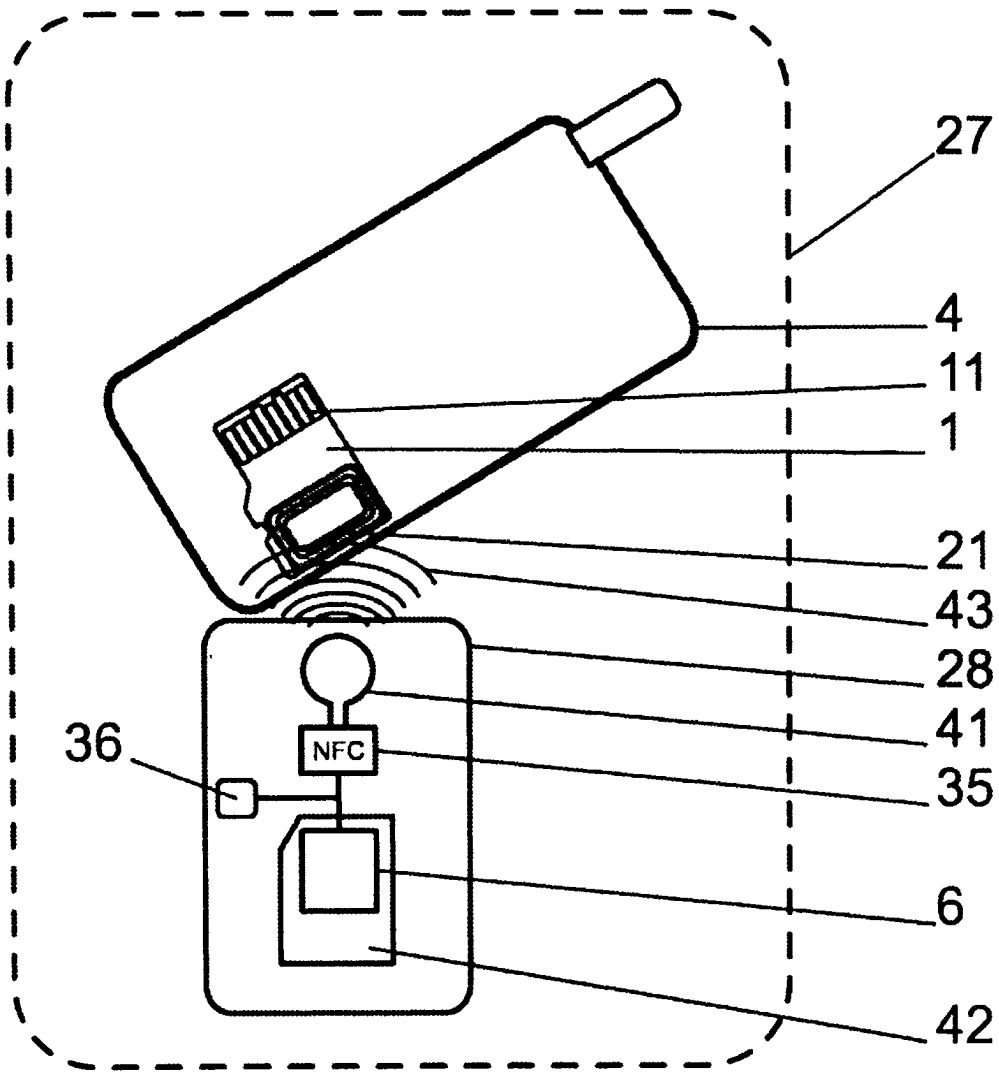
Фиг.4


магазин
мобильный телефон
поиск магазина
выбор товара
генерирование платежного требования
отсылка платежного требования на мобильный телефон
согласие на оплату/ платежная кнопка
запуск прикладной платежной программы
назначение/ выбор POS-терминала
выбор платежной карты через GUI-интерфейс
обмен данными между POS-терминалом и платежной картой
управление платежными рисками/ запрос PIN-кода
да
нет
PIN-код верный
нет
да
создание платежной криптограммы
отсылка платежной криптограммы
проверка платежа/ подтверждение покупки
нет
да
отсылка оплаченного товара
получение товара
создание отчета об отказе
получение отчета об отказе
процессы и задачи на съемной карте

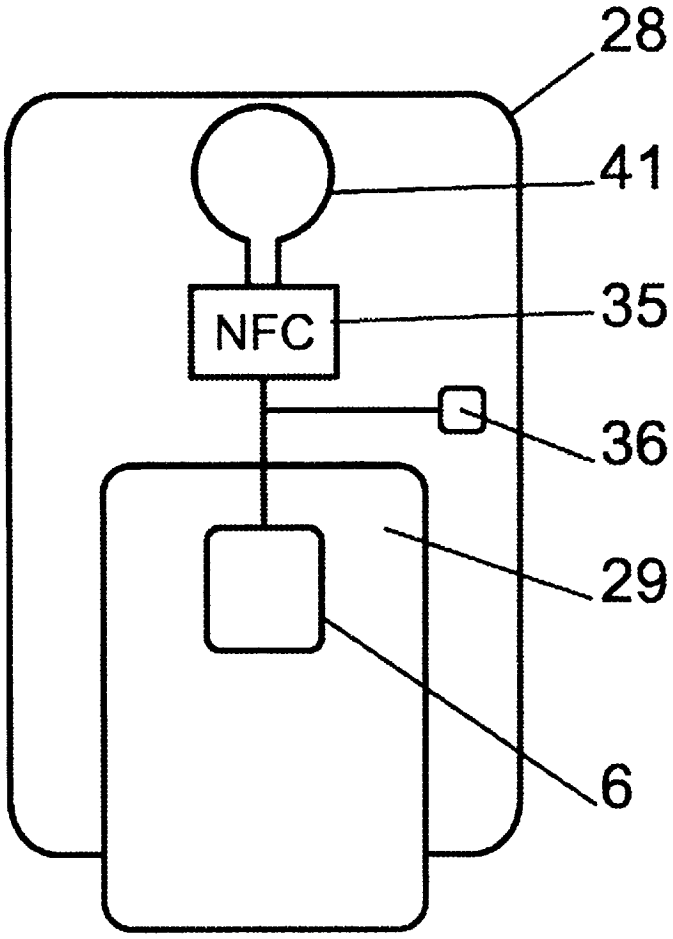
Фиг.5



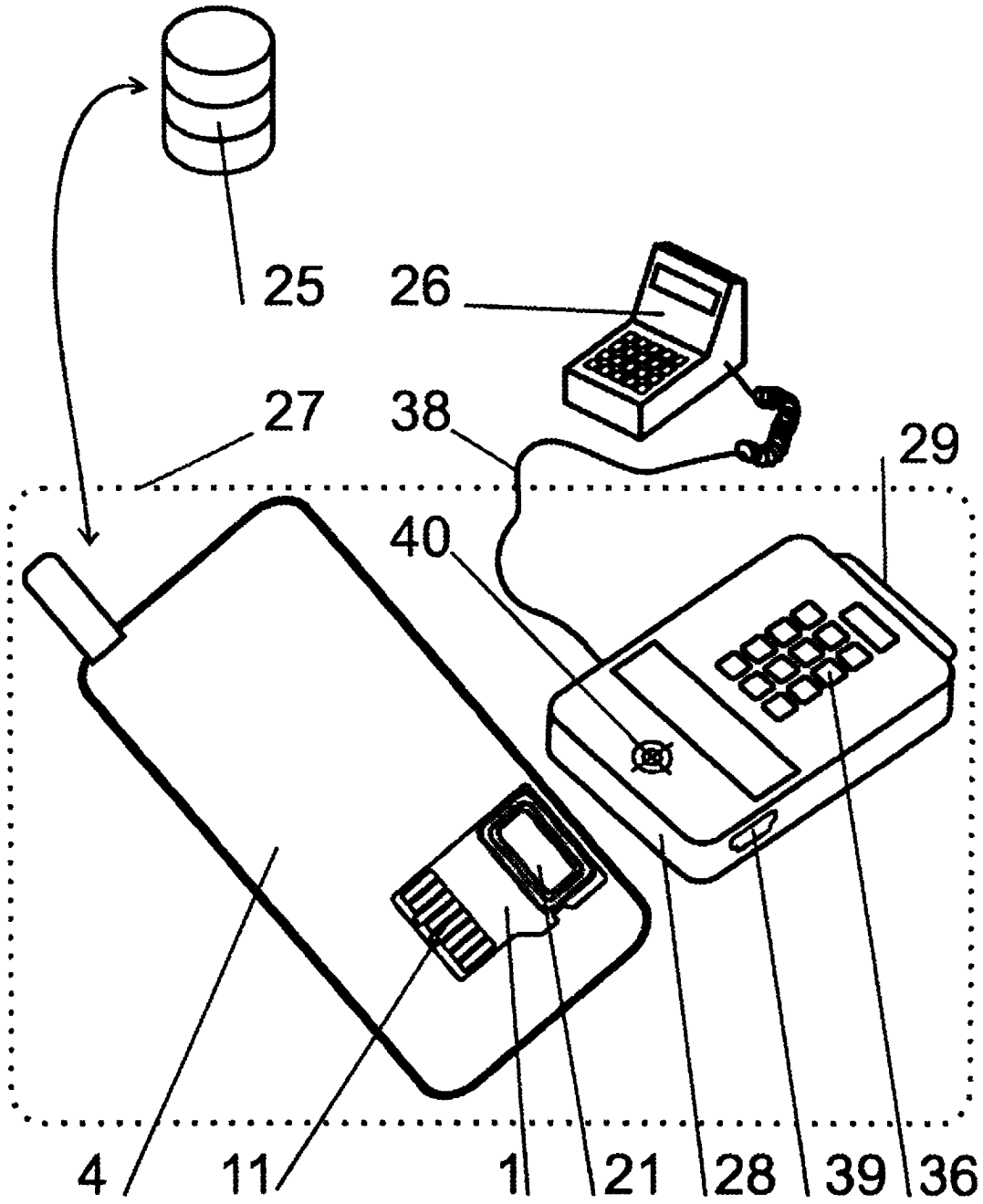
Фиг.7



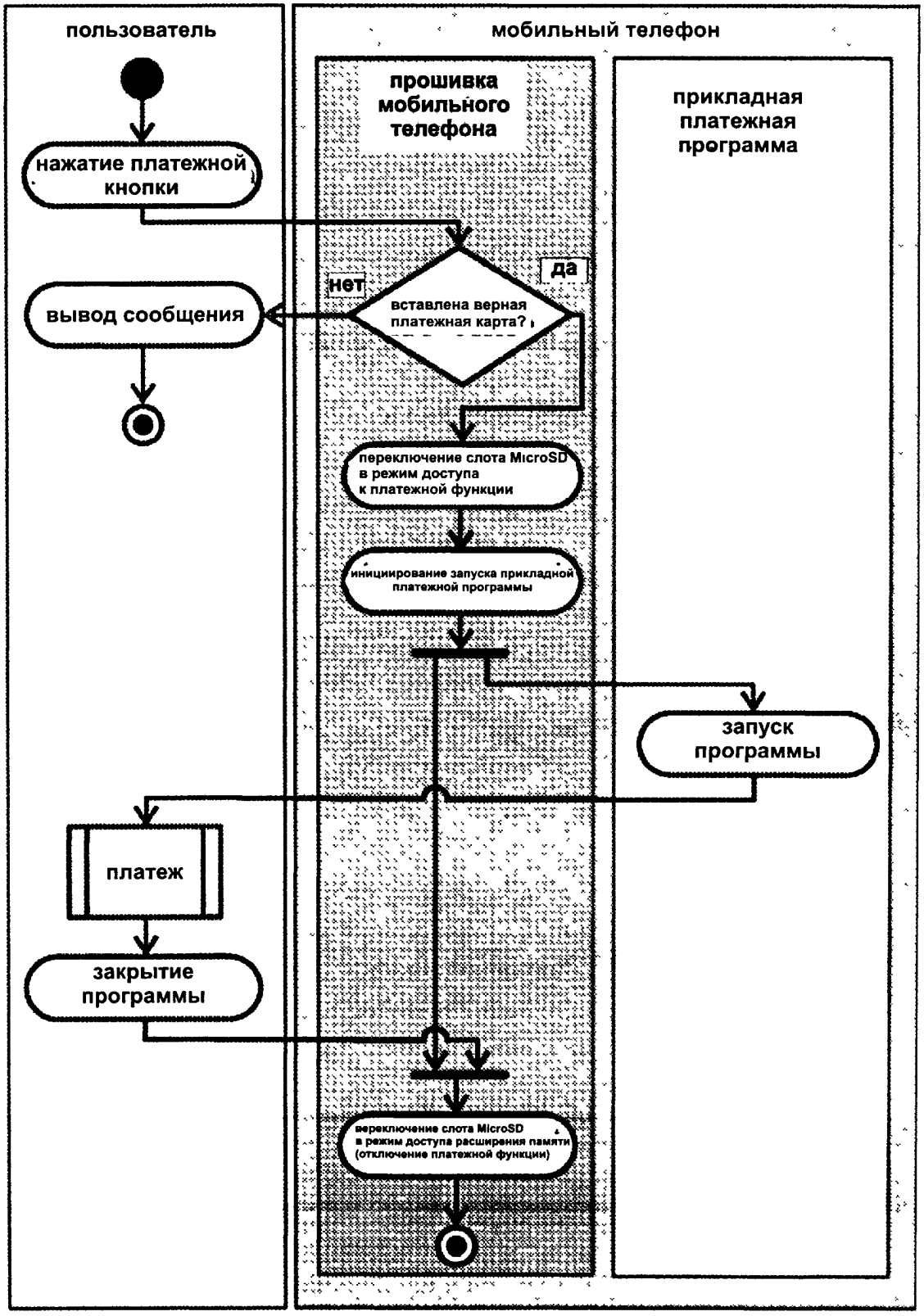
Фиг.8



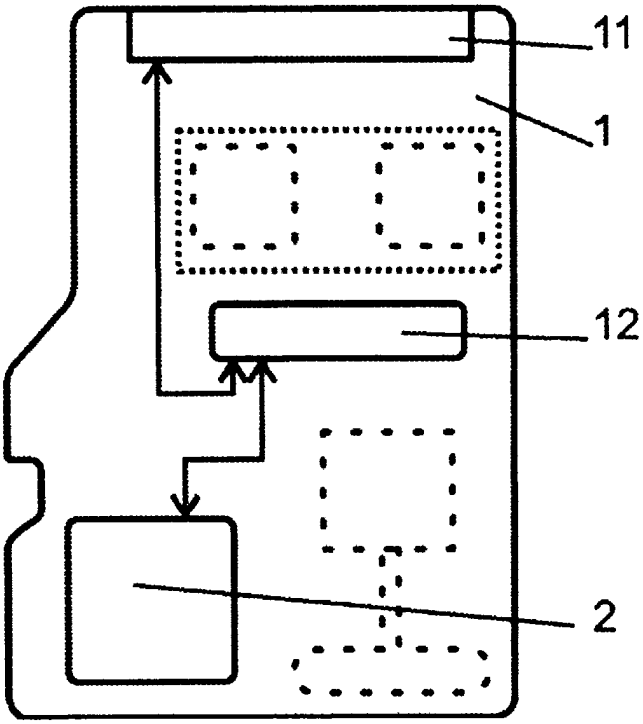
Фиг.9



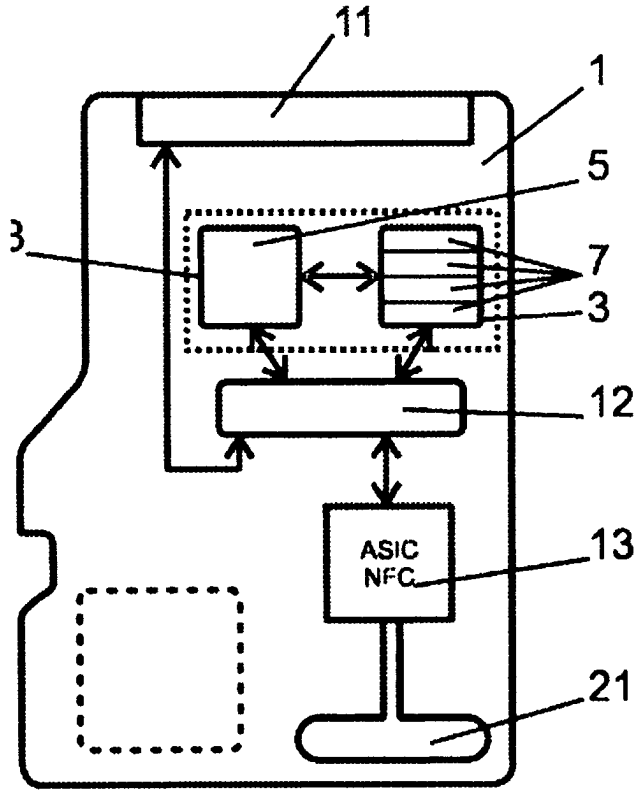
Фиг.10


пользователь
мобильный телефон
прошивка мобильного телефона
прикладная платежная программа
нажатие платежной кнопки
нет
да
вывод сообщения
вставлена верная платежная карта?
переключение слота MicroSD в режим доступа к платежной функции
инициирование запуска прикладной платежной программы
запуск программы
платеж
закрытие программы
переключение слота MicroSD в режим доступа расширения памяти (отключение платежной функции)

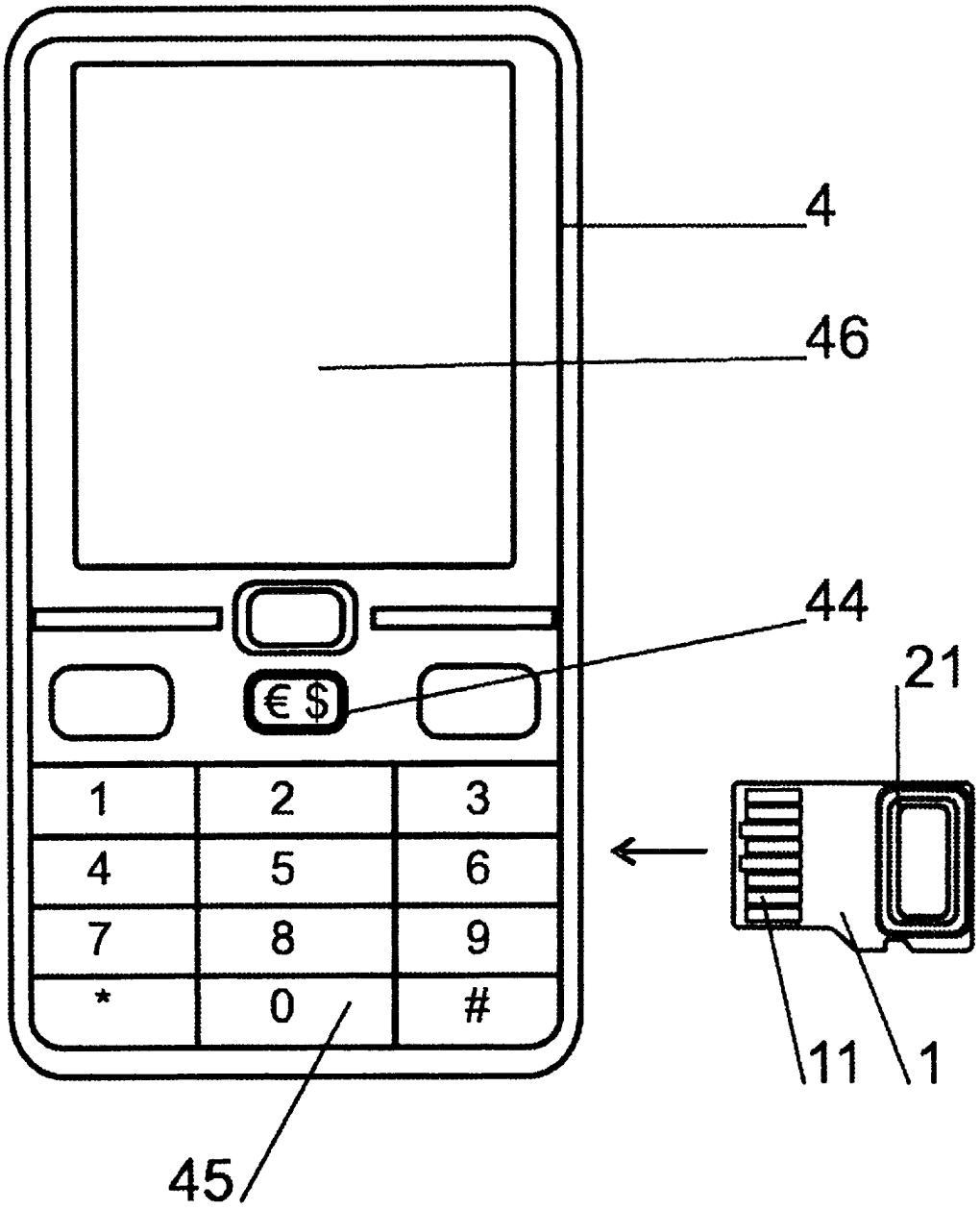
Фиг.11



Фиг.12



Фиг.13



Фиг.14