



(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2022.12.16

(51) Int. Cl. *H04L 9/12* (2006.01)
G06K 19/06 (2006.01)

(22) Дата подачи заявки
2020.05.29

(54) СПОСОБ, УСТРОЙСТВО И СИСТЕМА ДЛЯ ПЕРЕДАЧИ ДАННЫХ

(31) MX/a/2019/006412; 16/886,495

(32) 2019.05.31; 2020.05.28

(33) MX; US

(86) PCT/IB2020/055142

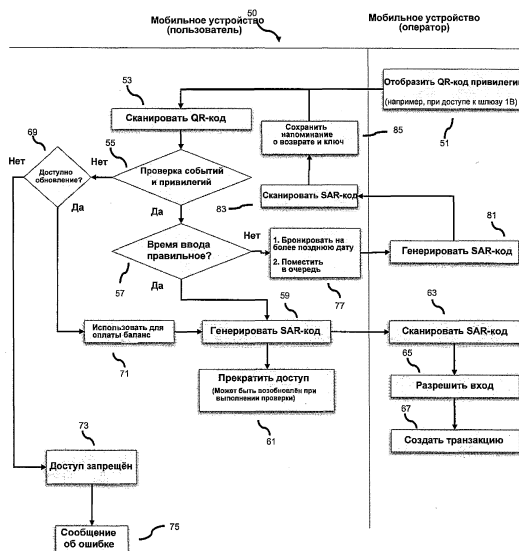
(87) WO 2020/240508 2020.12.03

(71) Заявитель:
МАЙКЭШЛЕСС САПИ ДЕ СИВИ
(MX)

(72) Изобретатель:
Де Пиао Йонг (CN), Бечерра Моралес
Энрико (MX)

(74) Представитель:
Шерстин А.Ю. (RU)

(57) В изобретении предлагается способ и система для передачи шифрованных данных от первого электронного устройства ко второму электронному устройству. Указанный способ включает этап отображения первого зашифрованного двумерного кода на интерфейсе вывода указанного первого электронного устройства, этап считывания указанного первого зашифрованного двумерного кода посредством интерфейса ввода указанного второго электронного устройства и этап дешифрования указанного первого двумерного кода посредством второго электронного устройства, этап генерирования второго зашифрованного двумерного кода посредством второго электронного устройства и этап отображения указанного второго зашифрованного двумерного кода на интерфейсе вывода указанного второго электронного устройства, этап считывания указанного второго двумерного кода, зашифрованного посредством интерфейса ввода указанного первого электронного устройства и этап дешифрования указанного второго двумерного кода посредством первого электронного устройства и этап генерирования действия на указанном первом электронном устройстве на основании указанного второго зашифрованного двумерного кода. При этом указанный второй двумерный код является группой двумерных кодов.



СПОСОБ, УСТРОЙСТВО И СИСТЕМА ДЛЯ ПЕРЕДАЧИ ДАННЫХ

Перекрёстная ссылка

В настоящей заявке испрашивается преимущество в части установления приоритета в соответствии с предварительной заявкой Мексики № MX/a/2019/006412 с датой подачи 31 мая 2019 года, которая включена в материалы настоящей заявки в полном объеме посредством данной ссылки.

Уровень техники, к которому относится изобретение

Настоящее изобретение относится к методам, устройствам и системам для передачи данных без активного соединения, например, соединения с Интернетом, с использованием считывающего устройства мобильного устройства, например, оптического считывающего устройства, и безопасного анимированного кода отклика (SAR-кода).

Предшествующий уровень техники

Компьютерные системы и сети облегчают процессы передачи данных. В данной области техники принято, чтобы передача данных, например, при транзакции, осуществлялась двумя устройствами, например, двумя мобильными устройствами, которые требуют активного соединения, например, подключения к сети, для выполнения операций аутентификации и обеспечения защиты информации, организации доступа к учетным записям пользователей, при проверке данных и обеспечения того, что по меньшей мере одно из двух устройств уполномочено осуществлять передачу данных.

В некоторых случаях, по меньшей мере одно из двух устройств может не иметь подключения к сети передачи данных, такой как сеть Интернет, в то время как все еще желательно осуществлять передачу данных с помощью такого устройства. В данной области техники эта проблема решается с помощью

Перевод первоначального описания

беспроводных технологий, использующих короткие радиоволны, таких как технология *Bluetooth* или технология связи ближнего поля (NFC).

В способах, использующих QR-коды, данные QR-коды генерируются на мобильных устройствах, которые имеют подключение к сети, например, к мобильной сети с подключением к сети Интернет. Пример такого способа приведен в документе US 2015/0178721. В указанном документе US 2013/0111208 представлены способы аутентификации через мобильное устройство.

В уровне техники не существует способа, устройства или системы, способной осуществлять активную автономную связь, например, подключение к сети, которая выполняет операции аутентификации и обеспечения защиты информации, для доступа к учетным записям пользователя для проверки данных, а также для обеспечения того, что по меньшей мере одно из двух устройств авторизовано для осуществления передачи данных.

Поэтому необходимо создать способы, устройства и системы, выполненные с возможностью осуществлять связь без активного подключения, например, к сети или посредством протокола NFC, которые обеспечивают необходимую защиту при передаче данных, при которой требуется высокая степень защиты, например, при выполнении финансовой операции (далее - транзакции).

Краткое описание изобретения

Безопасный анимированный код отклика (SAR-код) представляет собой набор зашифрованных кодов быстрого отклика (QR-кодов) или набор любых иных двумерных кодов, например универсальных товарных кодов (УТК). Данный SAR-код используется для передачи данных, при этом устройства, используемые при передаче данных, проверяются, в то время как узлы устройств не имеют активного подключения к сети, что позволяет безопасно и быстро передавать данные.

Перевод первоначального описания

В противоположность протоколу NFC, использование указанного SAR-кода требует прямой видимости между QR-кодом и оптическим считывающим устройством, например, камерой или считывающим устройством, что позволяет оптическому считывающему устройству получить изображение кода. В результате этого QR-коды не могут прослушиваться сторонними устройствами. Хотя QR-код может быть достаточно защищен путем ограничения времени его показа или демонстрации и контроля QR-кода в пределах прямой видимости, код может быть подвержен дешифрованию. Данный SAR-код, с другой стороны, представляет собой последовательность QR-кодов, в которой по меньшей мере один из QR-кодов является действительным. В настоящем изобретении SAR-код отображается в виде видео, причём оптическое считывающее устройство получает все изображения, а устройство, соединённое с оптическим считывающим устройством, посредством по меньшей мере одного процессора и одной памяти, идентифицирует по меньшей мере один правильный QR-код и расшифровывает информацию, подлежащую передаче.

В предпочтительном варианте, система требует наличия по меньшей мере двух устройств, каждое из которых имеет процессор, флэш-память и память для хранения данных, интерфейс ввода/вывода, такой как, например, экран и камера, клавиатура и т.д., и интерфейс связи. Однако система может понимать и работать с любым из двух полных измерительных устройств, которые могут управлять односторонней связью, например, одно устройство может обеспечивать вывод, например, на экран, а второе устройство может принимать ввод, например, с помощью камеры. Устройство на стороне пользователя может быть заменено чипом, с поддержкой протокола NFC. Для генерирования SAR-кода, в первом устройстве, таком как, напр. первое мобильное устройство, данные, которые должны быть переданы, шифруются с помощью ключа шифрования и с помощью закрытого ключа, набор данных, которые шифруются при помощи алгоритмов шифрования,

Перевод первоначального описания

например таких, как 256-битный симметричный алгоритм блочного шифрования (стандарт AES), тем самым генерируется вышеуказанный код. При этом номер блока добавляется к зашифрованным данным, и генерируется набор QR-кодов, при этом по меньшей мере один QR-код включает зашифрованные данные. Указанный SAR-код отображается на первом устройстве в видеоформате, при этом набор QR-кодов отображается последовательно или в случайном порядке. Считывание SAR-кода осуществляется на втором устройстве, таком как, например, второе мобильное устройство, которое считывает SAR-код с помощью оптического считывающего устройства, такого как, например, камера, захватывая SAR-код в виде изображений. По меньшей мере один правильный код в составе SAR-кода идентифицируется во втором устройстве, при этом зашифрованные данные интегрируются в по меньшей мере один правильный код. Затем по меньшей мере один правильный код расшифровывается с помощью ключа дешифрования, номер блока при этом удаляется и извлекается информация о передаче.

Благодаря этому можно осуществлять различные передачи данных. Например, передача данных, таких как финансовая или товарная операция, может быть осуществлена с помощью способа настоящего изобретения даже без активного подключения к сети, такой как сеть Интернет. Например, в рамках сеанса передачи данных могут быть предусмотрены такие действия как обновление информации, совершение покупки или возврат денежных средств.

Целью настоящего изобретения является создание способа, устройства и системы для передачи данных между по меньшей мере двумя мобильными устройствами без наличия активного сетевого соединения или соединения между этими двумя устройствами.

Ещё одной возможной целью настоящего изобретения является создание способа, устройства и системы для эффективной передачи данных между

Перевод первоначального описания

по меньшей мере двумя электронными устройствами без необходимости задействования для этого внешних устройств и систем.

Другой возможной целью настоящего изобретения является создание способа, устройства и системы для передачи данных между по меньшей мере двумя электронными устройствами в защищенном режиме посредством выполнения операций по аутентификации пользователя и обеспечения защищенного доступа, организации доступа к учетным записям сторон путем проверки данных и обеспечения того, что по меньшей мере одно из двух устройств уполномочено осуществлять передачу данных.

Краткое описание фигур чертежей

Эти и прочие объекты настоящего изобретения будут очевидны при изучении нижеследующего описания изобретения во взаимосвязи с приведенными ниже фигурами сопровождающих чертежей:

На Фиг.1 изображена высокоуровневая блок-схема по меньшей мере одного из двух устройств, например мобильного устройства, в соответствии с настоящим изобретением и предпочтительным вариантом его осуществления.

На Фиг.2 изображена высокоуровневая блок-схема, иллюстрирующая пример устройства/коммуникационной системы, обеспечивающей связь между устройствами посредством функции генерирования двумерного кода в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.3 изображена блок-схема, иллюстрирующая этапы способа, обеспечивающего организацию доступ на сайт, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.3А изображена блок-схема, иллюстрирующая этапы способа, обеспечивающего иную организацию доступа на сайт, в соответствии с

Перевод первоначального описания

предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.4 изображена блок-схема, иллюстрирующая этапы способа для передачи персональной информации от пользователя к оператору, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.4А изображена блок-схема, иллюстрирующая этапы другого способа для передачи персональной информации от пользователя к оператору, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.5 изображена блок-схема, иллюстрирующая этапы способа обновления количественных параметров на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.5А изображена блок-схема, иллюстрирующая этапы другого способа обновления количественных параметров на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.6 изображена блок-схема, иллюстрирующая этапы способа совершения покупок на сайте.

На Фиг.6А изображена блок-схема, иллюстрирующая этапы другого способа совершения покупок на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.7 изображена блок-схема, иллюстрирующая этапы способа возврата денежных средств на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.7А изображена блок-схема, иллюстрирующая этапы другого способа возврата денежных средств на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.8 изображена блок-схема, иллюстрирующая генерирование и

Перевод первоначального описания

шифрование по меньшей мере двух двумерных кодов в виде SAR-кодов, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.9 изображена блок-схема, иллюстрирующая дешифрование ранее зашифрованных двумерных кодов в виде SAR-кодов, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.10 изображена блок-схема, иллюстрирующая этапы способа для проверки транзакции, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.10А изображена блок-схема, иллюстрирующая этапы другого способа для проверки транзакции, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.11 изображена блок-схема, иллюстрирующая этапы способа совершения покупок на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения, при этом в соответствии с альтернативным вариантом осуществления настоящего изобретения указанный способ реализуется онлайн.

На Фиг.11А изображена блок-схема, иллюстрирующая этапы другого способа совершения покупок на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения, при этом в соответствии с альтернативным вариантом осуществления настоящего изобретения указанный способ реализуется онлайн.

На Фиг.12 представлен альтернативный вариант выполнения блок-схемы, отражающей процесс генерирования SAR-кода.

На Фиг.13 представлен альтернативный вариант выполнения блок-схемы, отражающей процесс считывания SAR-кода.

Перевод первоначального описания

На Фиг.14 представлена блок-схема, иллюстрирующая этапы способа аутентификации пользователя на сайте по удостоверению личности, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.14А представлена блок-схема, иллюстрирующая этапы способа иной аутентификации пользователя на сайте по удостоверению личности, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.14В представлена ещё одна блок-схема, иллюстрирующая этапы способа иной аутентификации пользователя на сайте по удостоверению личности, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.15 представлена блок-схема, иллюстрирующая этапы способа аутентификации метода платежа на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.16 представлена блок-схема, иллюстрирующая этапы способа для аутентификации учётных данных на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.16А представлена блок-схема, иллюстрирующая этапы способа аутентификации метода платежа на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.17 представлена блок-схема, иллюстрирующая этапы способа для аутентификации документа о соглашении на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.17А представлена блок-схема, иллюстрирующая этапы способа для другой аутентификации документа о соглашении на сайте, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

Перевод первоначального описания

На Фиг.18 представлена блок-схема, иллюстрирующая этапы способа для автовхода с устройства на сайт, при этом данный вход частично осуществляется в режиме онлайн, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.19 представлена блок-схема, иллюстрирующая этапы способа для использования общего ключа на сайте в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

На Фиг.20 изображена блок-схема, иллюстрирующая этапы ещё одного способа для совершения покупок на сайте с проверкой возраста покупателя и выдачей сведений о специальных предложениях, в соответствии с предпочтительным вариантом осуществления настоящего изобретения.

Подробное описание изобретения

Определения

Устройство: Под «устройством» здесь понимается мобильное устройство любого типа, такое как например смартфон, мобильный компьютер, персональный цифровой помощник (КПК), планшетный компьютер, умные часы или иное электронное 'умное устройство'. Аналогично, данным устройством может служить браслет, содержащий чип, совместимый с протоколом NFC, или фитнес-браслет, снабженный дисплеем или без такового; в случае отсутствия дисплея, является предпочтительным, чтобы фитнес-браслет был снабжен чипом, совместимым с протоколом NFC.

Карта: Подразумеваются карты любого тип, в том числе, но без ограничения, кредитные карты или дебетовые карты, банковские карты, иные виды карт для совершения финансовых операций, водительские права в виде карты, паспорт в виде карты, прочие идентификационные карты, или иные виды карт,

Перевод первоначального описания

которые могут содержать персональную информацию владельца карты.

Двумерный код: В настоящем изобретении используется по меньшей мере один QR-код с информацией, который может быть считан устройствами; кроме того, для реализации способа в соответствии с настоящим изобретением может использоваться группа QR-кодов. Для реализации способа и системы, в соответствии с настоящим изобретением, необходимы один или несколько двумерных кодов.

SAR-код: Представляет собой видеоизображение, содержащее по меньшей мере два QR-кода, причём указанное видеоизображение отображается в формате анимации.

Как правило, и двумерный код, и SAR-код включают данные, необходимые для подтверждения информационного обмена, сведения, которые в иллюстративном, но не ограничивающем порядке могут включать дату, номер или наименование события, имя поставщика, номера заказов, реквизиты заказов и т.д. В общем случае, предпочтительно, чтобы защитная анимация была включена для того, чтобы при касании сенсорного экрана она двигалась бы вместе с движением пальца, чтобы убедиться, что изображение не является снимком экрана или поддельным видеоизображением. Другие системы защиты, которые уже известны и станут известными в данной области техники, также могут считаться включенными в настоящее изобретение неограничивающим образом, но в качестве примеров.

Сигнал данных или сетевое подключение: Понятие «сигнал данных или сетевое подключение» относится к обработке и передаче данных (потока двоичных данных) по двухточечному или многоточечному каналу связи посредством проводных или беспроводных соединений с использованием глобальной вычислительной сети (WAN), общегородской вычислительной сети (MAN) и/или локальной вычислительной сети (LAN), причём в соответствии с одним из вариантов осуществления настоящего изобретения указанное подключение к глобальной

Перевод первоначального описания

вычислительной сети (WAN) может быть подключением к сети Интернет.

В описанных способах могут встречаться подспособы, которые могут быть реализованы при организации коммуникационной связи между двумя устройствами, при этом задействованные для этого устройства снабжены по меньшей мере одной камерой на той же стороне, что и экран, а метод чтения/сканирования осуществляется без вмешательства оператора и/или пользователя, когда соответствующее мобильное устройство перевернуто.

В нижеследующем подробном описании изобретения могут содержаться неявные ссылки на фигуры сопровождающих чертежей. При этом, в нижеследующем подробном описании изобретения несколько конкретных подробностей изобретения раскрыты в качестве примеров, чтобы обеспечить полное понимание соответствующих изобретательских замыслов авторов. В других случаях, способы, процессы, компоненты и/или схемы описаны на относительно высоком уровне, без раскрытия подробностей, во избежание внесения ненужной неясности в изложенные в настоящей заявке сведения.

Несколько описанных в настоящей заявке способов и систем относятся к генерированию двумерных кодов, предпочтительно по меньшей мере двух двумерных кодов, таких как QR-код или SAR-видеоизображение с по меньшей мере двумя QR-кодами и, более предпочтительно, с группой QR-кодов для организации защищенной связи между/с устройствами 13, такими как мобильные устройства.

На Фиг.1 показана блок-схема, иллюстрирующая устройство 13, например мобильное устройство. Указанным мобильным устройством 13 может являться смартфон либо им может быть иное портативное устройство, такое как персональный цифровой помощник (КПК), планшетный компьютер, умные часы, умные наушники /очки, и/или похожие устройства. В соответствии с другим вариантом осуществления настоящего изобретения, указанным мобильным

Перевод первоначального описания

устройством 13 может быть оптимизированное под требования пользователей устройство, такое как смарт-карта со встроенным в неё дисплеем (например, устройство с использованием технологии электронных чернил (e-ink), средств отображения на органических светодиодах (OLED), и.т.д.), процессор, встроенный источник электропитания и/или прочие пригодные элементы. В соответствии с указанным вариантом осуществления изобретения, гарнитура мобильного устройства 13 работает как стандартный цифровой беспроводной телефон. Для этой функции устройство включает микрофон 102, громкоговоритель 104, а также схемы кодирования и декодирования (речевой кодер) 106 для входного и выходного аудиосигнала.

Для осуществления цифровой беспроводной связи устройство 13 также включает по меньшей мере один цифровой приемопередатчик (XCVR) 108, соединенный с антенной 110. Рассмотренные здесь идеи охватывают варианты устройства 13, в которых используется любой цифровой приемопередатчик в соответствии с существующими или будущими стандартами цифровой беспроводной связи. Устройство 13 также может быть выполнено с возможностью функционирования в аналоговом режиме посредством технологии устаревшей сети. Мобильное устройство может также включать несколько приемопередатчиков, сконфигурированных для связи через различные типы сетей, такие как Wi-Fi, Bluetooth, инфракрасные, мобильные или подобные сети.

Устройство 13 содержит экран 122 для отображения сообщений, меню, приложений и т.д., включая двумерные коды, такие как QR-коды и SAR-коды, генерируемые приложениями, работающими на устройстве 13. Клавиатуры 130, сенсорные датчики 126 и сенсорные контроллеры 128 обеспечивают интерфейс ввода данных для получения вариантов выбора и команд от пользователя. Экран 118, клавиатуры 130 и сенсорные датчики 126 являются физическими элементами,

Перевод первоначального описания

которые обеспечивают графический или контекстный пользовательский интерфейс. Другие физические элементы мобильного устройства могут быть включены дополнительно и задействованы в работе устройства 13 и взаимодействии с пользователем, например, датчик инерциальных измерений, биометрические датчики, датчики пространственного изображения и тому подобное. Различные комбинации клавиатуры 120, экрана 118, микрофона 102 и динамика 104 могут быть использованы в качестве элементов вывода графического интерфейса пользователя (ГИП), для мультимедийной связи, например, аудио или видео. Конечно, могут быть использованы и другие элементы интерфейса, например, мышь, как это имеет место в некоторых КПК или смартфонах.

Устройство 13 дополнительно содержит одну или несколько камер 115, которые используются для захвата статических изображений или видеоматериалов. Камера 115, в частности, может использоваться для захвата изображений двумерных кодов, таких как QR-код или SAR-видеоизображение с по меньшей мере двумя QR-кодами, а более предпочтительно с группой QR-кодов, для обработки в приложении для чтения QR-кодов, запущенном на устройстве 13. Камера 115 предоставляет захваченные данные изображения процессору 112 для хранения в памяти 114, 116 и/или обработки.

Помимо стандартной передачи данных и телефонного ввода/вывода, элементы пользовательского интерфейса могут также использоваться для отображения меню и другой информации для пользователя и ввода опций выбора пользователя, включая любую информацию, которая необходима во время динамической генерации QR-кодов.

Микропроцессор 112 действует как программируемый контроллер для устройства 13, при этом он управляет операциями устройства 13 в соответствии с выполняемыми командами, для всех стандартных операций и для операций,

Перевод первоначального описания

связанных с функциональными возможностями, относящимися к двумерным кодам в соответствии с изложенными здесь соображениями. Например, мобильное устройство 13 включает флэш-память 114 для хранения различных процедур программирования и конфигурирования настроек.

Устройство 13 может также содержать оперативное запоминающее устройство (ОЗУ) 116 для рабочей памяти обработки данных. Разумеется, другие запоминающие устройства или конфигурации могут быть добавлены или заменены на те, что приведены в этом примере. В одном варианте реализации настоящего изобретения флэш-память 114 хранит команды, такие как процедуры перезагрузки, информацию о контроллере, операционную систему, процедуру обработки вызова с использованием речевого кодера и процедуру управления, а также множество других приложений, таких как браузеры, службы обмена сообщениями и тому подобное. В памяти 114 и 116 также хранится другая информация, например, телефонные номера и адреса серверов, загруженные данные, такие как мультимедийный контент, и различные данные, введенные пользователем, например, данные о конфигурации учетной записи. Информация, хранящаяся в памяти 114, обычно загружается и обрабатывается в микропроцессоре 112.

Как упоминалось выше, указанные устройства 13 содержат процессор и память 114, которая включает алгоритмы, сконфигурированные таким образом, что процессор устройства способен выполнять различные желаемые функции, в том числе функции, описанные ниже, с двумерными кодами. Как упоминается ниже, данные функции, связанные с генерированием и отображением двумерных кодов через графические пользовательские интерфейсы устройств 13, могут быть реализованы в компьютерах с вышеупомянутыми компонентами. Также могут быть использованы специализированные устройства; такие устройства должны быть способны реализовать процесс аутентификации, о котором пойдет речь ниже, без

Перевод первоначального описания

подключения к сети. В общем случае, функции, связанные с генерированием и отображением двумерных кодов через графический пользовательский интерфейс устройств, могут быть реализованы в любом полнокомплектном поворотном устройстве 13, включающем графический дисплей; причём указанное полнокомплектное поворотное устройство предпочтительно включает ранее упомянутые компоненты.

Способ, в соответствии с настоящим изобретением, может быть реализован на компьютере общего назначения, который может функционировать как сервер приложений и/или который функционирует как устройство 13. В процессе работы этапы указанного способа могут храниться на платформе компьютера общего назначения. Аналогичным образом, этапы способа могут храниться в других местах и/или переноситься для загрузки в соответствующую компьютерную систему общего назначения. Осуществление указанного способа в процессоре компьютера позволяет реализовать методику динамического генерирования и обработки двумерных кодов, таких как QR-коды для организации защищенной связи с устройствами 13 или от них, по существу так, как это излагается и иллюстрируется в настоящей заявке.

На Фиг.2 показана система 10, предоставляющая различные услуги мобильной связи, включая связь для динамического генерирования двумерных кодов для защищенной связи с устройствами 13a, 13b или от них. В данном примере показаны два мобильных устройства 13a и 13b без активного подключения к мобильной беспроводной сети связи 15. Мобильные устройства 13a и 13b (упоминаемые как устройства 13) являются примерами устройств, которые могут быть использованы для функции генерирования двумерного кода. Однако, способ в соответствии с настоящим изобретением может быть осуществлен с помощью аналогичных устройств, имеющих компоненты, упомянутые выше в связи с Фиг.1. В каждом случае устройству не требуется активное подключение к сети, такой как

Перевод первоначального описания

мобильная беспроводная сеть связи 15, сеть Интернет, локальная сеть (LAN) или любой другой тип проводного или беспроводного соединения. При этом, описанная система может использовать и другое устройство 13, которое не является мобильным устройством, например, компьютер общего назначения, браслет 13с снабженный NFC-совместимым чипом, или фитнес-трекер, который может иметь или не иметь дисплей. При отсутствии дисплея, предпочтительно, чтобы фитнес-трекер имел NFC-совместимый чип. Важно подчеркнуть, что во время выполнения способа настоящего изобретения не имеется сети 15 или подключения к сети 15 к устройствам 13, как это может произойти при насыщенных событиях, таких как, например, музыкальный фестиваль. Данные устройства могут быть подключены к сети 15 с помощью уже существующих или будущих стандартов. Как уже упоминалось, одно или оба устройства могут работать в описанных здесь режимах без подключения к сети передачи данных, подключения к телефонной сети и/или к любому подходящему каналу связи вне канала видеосвязи, обеспечиваемого посредством указанной системы и способа, описанных в настоящей заявке. Устройства также могут не иметь активного NFC, а в некоторых вариантах активный NFC может быть отключен, что в некоторых вариантах осуществления изобретения может быть полезно для предотвращения кражи данных, касающихся транзакции. Тем не менее, система и способ передачи данных, описанные в настоящей заявке, могут работать при существующем сетевом соединении. В предпочтительном варианте осуществления изобретения, система и способ передачи данных реализованы без прямой зависимости от беспроводной цифровой связи, хотя она может быть использована при её наличии.

Устройства 13 могут быть выполнены с возможностью осуществления функции генерирования двумерных кодов без активного подключения к сети 15. Пользовательские устройства 13а и 13с характеризуются способностью выполнения

Перевод первоначального описания

функции генерирования двумерных кодов, а также функции выполнения приложений, написанные на разных языках программирования. Аналогичным образом, операторские устройства 13b характеризуются способностью выполнения функции генерирования двумерных кодов, а также функции выполнения приложений, написанные на разных языках программирования. Устройства 13a-13c взаимодействуют друг с другом таким образом, что без NFC они способны сканировать и/или считывать двумерные коды, расположенные в пределах прямой видимости, например, двумерные коды, отображаемые на мобильных устройствах, помещенных в считывающее устройство. Считывающее устройство может представлять собой камеру 115 устройств 13a-13c, устройство для считывания штрих-кодов или любое другое подходящее периферийное устройство. Устройство 13a-13c может включать входящий интерфейс и исходящий интерфейс, используемые для взаимодействия с пользователями, для приема команд и для предоставления уведомлений и другой исходящей информации пользователю/оператору.

Устройствами 13 могут быть мобильные устройства, такие как смартфоны, КПК или компьютеры общего назначения, а также браслеты, содержащие NFC-совместимый чип, или фитнес-трекер. Указанные устройства способны выполнять приложения для реализации функции генерирования двумерного кода, а также для реализации функции считывания двумерного кода, при этом указанные функции генерирования и считывания двумерного кода могут быть написаны на разных языках и выполняться в разных средах, причём некоторые из этих устройств могут использовать многозадачную операционную систему.

Устройства 13 обычно включают в себя камеру 115, которая может использоваться для захвата изображений, включая двумерные коды. Устройство 13, на котором запущено приложение для считывания двумерного кода, может

Перевод первоначального описания

использовать камеру в качестве считывателя двумерного кода для получения или сканирования QR-кода. Устройства 13 также включают в себя исходящий интерфейс, такой как экран 122, для отображения двумерных кодов, которые могут быть считаны считывателем двумерного кода другого устройства.

Приложения для считывания и приложения, генерирующие двумерные коды, которые включают в себя функции считывания и генерирования двумерных кодов, содержат также функции аутентификации, сконфигурированные для аутентификации кодов, сгенерированных и отображенных устройствами 13. Функция аутентификации может также включать функции, связанные с шифрованием, такие как генерирование, распространение и/или аутентификация ключей шифрования, включая пары ключей шифрования/описания.

В настоящей заявке описаны различные способы, реализованные в связи с описанной здесь системой и использующие способ для автономной передачи данных, однако процесс передачи данных и его применение на основе SAR-кодов могут быть адаптированы к другим подходящим типам взаимодействия пользователей, управлению данными, управлению учетной записью, аутентификации и/или подходящим формам координации между двумя устройствами.

На Фиг.3 изображена блок-схема, иллюстрирующая этапы способа 50 для доступа пользователя к сайту, двумерные коды генерируются и считываются устройствами 13. Осуществление способа начинается, когда устройство 13b оператора отображает 51 двумерный код посредством своего экрана 122, который сканируется или захватывается 53 камерой 115 пользовательского устройства 13a. Затем способ обеспечивает проверку события и привилегий 55, которыми обладает пользовательское устройство 13a. Если пользовательское устройство 13a действительно имеет соответствующее событие и привилегии, способ обеспечивает проверку правильно ли указано время ввода 57. Если получено подтверждение, что

Перевод первоначального описания

время ввода является правильным, генерируется группа двумерных кодов 59, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), причём указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), а по меньшей мере один из двумерных кодов включает зашифрованную информацию для проверки операторским устройством 13b. После того как группа двумерных кодов 59 сгенерирована и отображена на экране 122 пользовательского устройства 13a, доступ 61 к событию прекращается, а сгенерированный SAR-код сканируется и/или считывается 63 с помощью камеры 115b операторского устройства 13b. Благодаря функции считывания двумерных кодов, заявляемый способ характеризуется возможностью считывания всех двумерных кодов, представленных в SAR-коде, и возможностью выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция расшифровки позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию, касающуюся двумерного кода, разрешить доступ 65 к пользовательскому устройству 13a и соответствующему пользователю и создать транзакцию 67.

Если подтверждается, что пользователь действительно имеет доступ к событию или соответствующие привилегии 55, в соответствии со способом проверяется доступно ли потенциальное улучшение обслуживания/перевод на более высокий уровень обслуживания 69. Если потенциальное улучшение обслуживания/перевод на более высокий уровень обслуживания 69 доступно, пользователю может быть предоставлен доступ и привилегии 71 и, таким образом, генерируется необходимый SAR-код 59 на пользовательском устройстве 13a. Аналогично, если потенциальное улучшение обслуживания/перевод на более высокий уровень обслуживания 69 доступно, перед предоставлением доступа и привилегий 71 на устройство пользователя 13a может быть отправлена команда на

Перевод первоначального описания

обновление информации на сайте, при этом будет получен новый SAR-код для доступа к предоставленной привилегии. Если потенциальное улучшение обслуживания/перевод на более высокий уровень обслуживания 69 недоступно, производится запрет доступа 73 к мобильному устройству пользователя 13а и пользователю, носящему его, и генерируется при этом сообщение об ошибке 75.

Если время входа 57 неверно, может быть сгенерировано приглашение о возврате 77; приглашение о возврате включает в себя бронирование места на более позднюю дату или время 77 и помещение указанного приглашения в очередь 77, связанную с определенным временем или датой. После генерирования этого приглашения на устройстве оператора 13b генерируется 81 новый SAR-код, включающий время и/или дату возврата денежных средств, то есть SAR-код, который сканируется 83 устройством 13а, а на устройстве пользователя 13а генерируется 85 напоминание о необходимости возврата денежных средств.

На Фиг.3А изображена блок-схема, иллюстрирующая этапы другого способа 50А для доступа пользователя к сайту, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа начинается, когда устройство 13а пользователя выполняет бронирование или покупку доступного интервала 52 доступа к событию. Устройство 13b оператора отображает 54 двумерный код посредством своего экрана 122, который сканируется или захватывается 56 камерой 115 устройства 13а пользователя. Двумерный код 54, отображаемый устройством 13b оператора, может включать среднее время на один билет и/или следующую доступную смену, если требуется цифровая очередь. Затем в соответствии со способом проверяется событие и привилегии 58, которыми обладает пользовательское устройство 13а. Если пользовательское устройство 13а действительно имеет соответствующие событие и привилегии, то может быть проверено является ли время ввода правильным 60. Если в соответствии со способом подтверждается, что время ввода является правильным, генерируется группа

двумерных кодов 62, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), причём указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодами), а по меньшей мере один из двумерных кодов включает зашифрованную информацию для проверки операторским устройством 13b. После того, как группа двумерных кодов 62 сгенерирована и отображена на экране 122 пользовательского устройства 13a, доступ к событию прекращается 64, что может быть осуществлено при выходе, а SAR-код, сгенерированный с помощью камеры 115b операторского устройства 13b, сканируется и/или считывается 66. Указанный подспособ, варьирующийся от отображения 54 двумерного кода до сканирования 66 группы двумерных кодов, может быть осуществлен при организации непосредственной коммуникационной связи между двумя устройствами, при этом мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства. Благодаря наличию функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция расшифровки позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию двумерного кода, разрешить доступ 68 к пользовательскому устройству 13a и соответствующему пользователю и создать транзакцию 70.

Если подтверждается, что пользователь имеет доступ к событию или соответствующие привилегии 58, в соответствии со способом проверяется доступно ли обновление 72. Если обновление доступно 72, в соответствии со способом разрешается оплата баланса 74 и тем самым позволяет бронирование или покупка свободного слота 52 на устройстве пользователя 13a. Если потенциальное обновление 72 недоступно, доступ 76 к мобильному устройству пользователя 13a прекращается, и генерируется сообщение об ошибке 78.

Перевод первоначального описания

Если время входа 60 неверно, то бронируется следующий свободный слот с помещением его в цифровую очередь 80, чтобы впоследствии оператор с помощью своего устройства 13b мог вывести на экран 54 двумерный код.

На Фиг.4 изображена блок-схема, иллюстрирующая этапы способа 150 для передачи персональной информации от пользователя к оператору, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 150 начинается, когда операторское устройство 13b отображает 151 двумерный код посредством своего экрана 122, который сканируется или захватывается 153 камерой 115 пользовательского устройства 13a. Затем, в соответствии со способом пользователю направляется запрос хочет ли он поделиться персональной информацией 155. Если пользователь выбирает на пользовательском устройстве 13a, что он хочет поделиться персональной информацией, в соответствии со способом пользователю направляется запрос какую информацию он хочет отредактировать 157. Если пользователь хочет отредактировать информацию, то способ позволяет пользователю выбрать на устройстве пользователя 13a, какие поля будут переданы 159 оператору. В противном случае, способ предоставляет общий доступ ко всем доступным полям. При выборе полей для совместного использования 159 или при совместном использовании всех полей, генерируется группа двумерных кодов 161, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), в котором указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), при этом по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке операторским устройством 13b.

После того, как группа двумерных кодов сгенерирована 161 и отображена на экране 122 пользовательского устройства 13a, сгенерированный SAR-код сканируется и/или считывается 163 с помощью камеры 115b операторского

Перевод первоначального описания

устройства 13b. С помощью функции считывания двумерных кодов указанный способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию двумерного кода, разрешить доступ к данным 165 на операторском устройстве 13b и создать профиль 167 для пользователя пользовательского устройства 13a.

В случае если пользователь не хочет делиться персональной информацией 155, доступ к данным мобильного устройства пользователя 13a прекращается 169 и выдается сообщение об ошибке 171.

На Фиг.4А изображена блок-схема, иллюстрирующая этапы другого способа 150А для передачи персональной информацией от пользователя к оператору, двумерные коды генерируются и считываются устройствами 13. Осуществление способа 150А начинается, когда устройство 13а пользователя конфигурирует и/или редактирует персональную информацию 152, которая становится доступной для обмена с некоторым устройством 13b оператора. Устройство 13b оператора отображает 154 двумерный код посредством своего экрана 122, который сканируется или захватывается 156 камерой 115 устройства 13а пользователя. Устройство 13а пользователя впоследствии определяет, есть ли персональная информация 158, доступная для обмена, и, если таковая есть, то генерируется группа двумерных кодов 160, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), а по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке устройством 13b оператора. После того как группа двумерных кодов 160 сгенерирована и отображена на экране 122 пользовательского устройства 13а, сгенерированный SAR-код сканируется и/или

Перевод первоначального описания

считывается 162 с помощью камеры 115b операторского устройства 13b. С помощью функции считывания двумерных кодов способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Подспособ, варьирующийся от отображения 154 двумерного кода до сканирования 162 группы двумерных кодов, может быть осуществлен при организации коммуникационной связи между двумя устройствами, причём указанные мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию двумерного кода, создать профиль пользователя 164 на операторском устройстве 13b и получить доступ к данным пользователя 166 на операторском устройстве 13b.

Если будет установлено, что персональная информация 158 отсутствует, доступ к данным мобильного устройства пользователя 13a будет прекращен и будет выдано сообщение об ошибке 168.

На Фиг.5 изображена блок-схема, иллюстрирующая этапы способа 250 обновления количественных параметров на сайте, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 250 начинается, когда пользовательское устройство 13a отображает 251 двумерный код посредством своего экрана 122, и он сканируется или захватывается 253 камерой 115 операторского устройства 13b. Двумерный код может содержать такую информацию, как идентификатор события, имя, код, пол и возраст, среди прочих данных. Затем, в соответствии со способом запрашивается, соответствует ли идентификатор события событию 255, и, если это не так, он отправляет сообщение об ошибке 267 на

Перевод первоначального описания

устройство оператора 13b. Если же оно соответствует, указывается количество, подлежащее обновлению, и потенциальный способ оплаты, такой как, например наличные или дебетовая/кредитная карта, выбираются 257. Группа двумерных кодов 259 генерируется на устройстве 13b оператора, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке пользовательским устройством 13a. После того, как группа двумерных кодов 259 сгенерирована и отображена на экране 122 устройства 13b оператора, сгенерированный SAR-код сканируется и/или считывается 263 с помощью камеры 115a пользовательского устройства 13a. Посредством функции считывания двумерного кода заявленный способ позволяет считывать все двумерные коды, представленные в SAR-коде, и различать по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию двумерного кода и разрешить пополнение выбранного количества 265 на пользовательском устройстве 13a. Благодаря разрешению изменения выбранного количественного параметра 265 на устройстве пользователя, может быть сгенерировано сообщение для подтверждения транзакции, отображающее, например, суммарный баланс денежных средств и новый общий баланс денежных средств, при этом транзакция сохраняется в личном кабинете пользователя. Параллельно с изменением выбранного количественного параметра 265 создается транзакция 261 на операторском устройстве 13b. С учетом Фиг.5 очевидно, что специалист в данной области техники может вывести способ, позволяющий вместо опции обновления количественных параметров на сайте воспользоваться способом обновления количественных параметров после события,

Перевод первоначального описания

т.е. возможностью списания средств после события, при этом данные устройства генерируют и считывают двумерные коды.

На Фиг.5А изображена блок-схема, иллюстрирующая этапы способа 250А обновления количественных параметров на сайте, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 250А начинается, когда операторское устройство 13b выбирает количественный параметр для обновления 252. На пользовательском устройстве 13a двумерный код отображается 254 посредством его экрана 122, который сканируется или захватывается 256 камерой 115 операторского устройства 13b. Способ позволяет впоследствии проверять, соответствует ли событие 258, и, если это не так, он отправляет сообщение об ошибке 260 на устройство 13b оператора. Если же соответствует, на операторском устройстве 13b генерируется 262 группа двумерных кодов, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), в котором указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), при этом по меньшей мере один из двумерных кодов включают в себя зашифрованную информацию, подлежащую проверке пользовательским устройством 13a. После того, как группа двумерных кодов 262 сгенерирована и отображена на экране 122 устройства 13b оператора, сгенерированный SAR-код сканируется и/или считывается 266 с помощью камеры 115a пользовательского устройства 13a. Указанный подспособ, варьирующийся от отображения 254 двумерного кода до сканирования 266 группы двумерных кодов, может быть реализованы при организации коммуникационной связи между двумя устройствами, при котором мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и способ считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства. С помощью функции

Перевод первоначального описания

считывания двумерного кода способ позволяет считывать все двумерные коды, представленные в SAR-коде, и различать по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию двумерного кода и разрешить изменение выбранного количественного параметра 268 на пользовательском устройстве 13a. Благодаря разрешению изменения выбранного количественного параметра 268 на устройстве пользователя, может быть сгенерировано сообщение для подтверждения транзакции, отображающее, например, суммарный баланс денежных средств и новый общий баланс денежных средств, при этом транзакция сохраняется в личном кабинете пользователя. Параллельно с изменением выбранного количественного параметра 268 создается транзакция 264 на устройстве 13b оператора. С учетом Фиг.5 очевидно, что специалист в данной области техники может вывести способ, позволяющий вместо опции обновления количественных параметров на сайте воспользоваться способом обновления количественных параметров после события, т.е. возможностью списания средств после события, при этом данные устройства генерируют и считывают двумерные коды.

На Фиг.6 изображена блок-схема, иллюстрирующая этапы способа 350 совершения покупок на сайте, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 350 начинается, когда пользовательское устройство 13a отображает 351 двумерный код с помощью своего экрана 122, который сканируется или захватывается 353 камерой 115 операторского устройства 13b. Двумерный код может содержать такую информацию, как идентификатор события, имя, код, пол и возраст, среди прочих данных. Затем, в соответствии с заявленным способом, направляется запрос соответствует ли идентификатор события событию 355, и, если это не так, отправляется сообщение об

ошибке 373 на устройство оператора 13b. Если же соответствует, то выбирается заказ(ы)/товар(ы) для покупки 357, и вместе с заказом на покупку генерируется группа двумерных кодов 359. В случае если двумерных кодов несколько, они отображаются в виде безопасного анимированного кода отклика (SAR-кода), в котором по меньшей мере один двумерный код может быть группой кодов быстрого отклика (QR-кодов), при этом по меньшей мере один двумерный код включает зашифрованную информацию, подлежащую проверке пользовательским устройством 13a. Заказ на покупку содержит такую информацию, как идентификатор события, код, количество, номер транзакции, имя пользователя, цена и сумма, среди прочего. После того как группа двумерных кодов 359 сгенерирована и отображена на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 361 с помощью камеры 115a пользовательского устройства 13a. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию двумерного кода. Далее, способ дает возможность проверки баланса 363 и, если проверить баланс 363 не представляется возможным, то система генерирует и отправляет сообщение об ошибке 375. Если баланс может быть проверен 363, генерируется вторая группа двумерных кодов 365 с балансом, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная вторая группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке операторским устройством 13b. Двумерный код с проверенной информацией содержит такую информацию, как идентификатор события, код, количество и номер транзакции,

Перевод первоначального описания

среди прочего. Предпочтительно, когда в этот момент определенное количество денежных средств списывается 367 со счета автономного персонального баланса пользователя. После того, как вторая группа двумерных кодов 365 сгенерирована и отображена на экране 122 пользовательского устройства 13а, сгенерированный SAR-код сканируется и/или считывается 369 камерой 115b операторского устройства 13b. С помощью функции считывания двумерных кодов, способ позволяет считывать всю вторую группу двумерных кодов, представленных в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию двумерного кода. После сканирования и/или считывания SAR-кода 369 с помощью операторского устройства 13b, покупка и запись/передача подтверждаются/закрываются и создается новая транзакция 371.

На Фиг.6А изображена блок-схема, иллюстрирующая этапы другого способа 350А совершения покупок на сайте, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 350А начинается, когда устройство оператора выбирает заказы и/или товары 352. В свою очередь, двумерный код отображается 354 на пользовательском устройстве 13а посредством его экрана 122 и сканируется или захватывается 353 камерой 115 операторского устройства 13b. Двумерный код может содержать такую информацию, как идентификатор события, имя, код, пол и возраст, среди прочих данных. Далее, в соответствии с заявленным способом, генерируется по меньшей мере один двумерный код 356 с выбранными заказами и/или товарами и информацией двумерного кода, отображаемой с пользовательского устройства 13а. Если имеется группа двумерных кодов, они отображаются в виде безопасного анимированного кода отклика (SAR-кода) кода, при этом по меньшей мере один двумерный код может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один двумерный код включает

Перевод первоначального описания

зашифрованную информацию, подлежащую проверке пользовательским устройством 13a. По меньшей мере один двумерный код содержит такую информацию, как идентификатор события, код, количество, номер транзакции, имя пользователя, цена и сумма, среди прочего. После того, как группа двумерных кодов 356 сгенерированы и отображены на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 358 с помощью камеры 115a пользовательского устройства 13a. С помощью функции считывания двумерных кодов, заявленный способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию двумерного кода. Затем, в соответствии с заявленным способом, проверяется событие 360 и, если проверка события 360 невозможна, то генерируется и отправляется сообщение об ошибке 362. Если же проверка события 360 возможна, то проверяется возраст 364. Если проверка возраста 364 невозможна, то генерируется и отправляется сообщение об ошибке 366. Если же проверка возраста 364 возможна, то проверяется баланс 368 и, если проверка баланса 370 невозможна, то генерируется и отправляется сообщение об ошибке 375. Если же баланс может быть проверен 370, то генерируется вторая группа двумерных кодов 372 с балансом, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная вторая группадвумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке операторским устройством 13b. Двумерный код с проверенной информацией содержит такую информацию, как идентификатор события, код, количество и номер транзакции, среди прочего. Предпочтительно, если в этот момент определенное количество денежных средств списывается 378 со счета личного баланса

Перевод первоначального описания

пользователя в автономном режиме. После того, как вторая группа двумерных кодов 374 сгенерирована и отображена на экране 122 пользовательского устройства 13а, сгенерированный SAR-код сканируется и/или считывается 374 камерой 115b операторского устройства 13b. Подспособ, варьирующийся от отображения 254 двумерного кода до сканирования 374 группы двумерных кодов, может быть реализован при организации коммуникационной связи между двумя устройствами, причём указанные мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства. С помощью функции считывания двумерных кодов, способ позволяет считывать всю вторую группу двумерных кодов, представленных в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию двумерного кода. После сканирования и/или считывания SAR-кода 374 с помощью операторского устройства 13b, покупка и запись/передача подтверждаются/закрываются и создается новая транзакция 376.

На Фиг.7 изображена блок-схема, иллюстрирующая этапы способа 450 возврата денежных средств на сайте, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 450 начинается, когда операторское устройство 13b отображает 451 двумерный код с помощью своего экрана 122, который сканируется или захватывается 453 камерой 115 пользовательского устройства 13а. Двумерный код может содержать такую информацию, как идентификатор события, имя и код, пол и возраст, среди прочих данных. Далее, в соответствии с заявленным способом, направляется запрос соответствует ли идентификатор события событию, а также каков баланс 455,

Перевод первоначального описания

подлежащий возврату. Если идентификатор события не соответствует событию, на пользовательское устройство 13а отправляется сообщение об ошибке 467. Если он соответствует, то генерируется группа двумерных кодов 457 с деталями возврата денежных средств, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке операторским устройством 13b. Детали возврата денежных средств, то есть зашифрованная информация, могут содержать такие сведения, как идентификатор события, код, количество возвращаемых денежных средств, номер транзакции, дата первоначальной транзакции, дата возврата, код причины или причина возврата, имя пользователя и прочее. После того как группа двумерных кодов 457 сгенерирована и отображена на экране 122 пользовательского устройства 13а, сгенерированный SAR-код сканируется и/или считывается 459 камерой 115а операторского устройства 13b. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию двумерного кода. После сканирования и/или считывания 459 SAR-кода на операторском устройстве 13b, оператор выбирает способ возврата денег, например, наличными, товаром или на чип с поддержкой протокола NFC. Если возврат осуществляется на чип с поддержкой протокола NFC, оператор, возможно, с помощью устройства 13b, активирует чип NFC пользователя 13с с кодом пользователя и определенным количеством средств. В альтернативном варианте, пользователю может быть дана инструкция как запросить возврат денежных средств на устройстве 13а, добавив данные для возврата, такие как,

Перевод первоначального описания

например, банковский счет для зачисления возвращаемых денежных средств. После выбора метода возврата 461, создается новая транзакция 463. Метод возврата может быть осуществлен несколькими способами, в том числе наличными денежными средствами. Параллельно с созданием новой транзакции 463 на стороне операторского устройства 13b, возврат, например, возвращенное количество денежных средств, удаляется 465 на пользовательском устройстве 13a. Как показано на Фиг.7А, способ 450А, включающий подспособ, варьирующийся от отображения 451 двумерных кодов до сканирования 459 группы двумерных кодов, может быть реализован при организации непосредственной коммуникационной связи между двумя устройствами, причём указанные мобильные устройства имеют по меньшей мере одну камеру, расположенную на той же стороне, что и экран 122, а метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства.

В частном варианте осуществления настоящего изобретения, показанная на фигуре чертежей версия способа может быть скомбинирована со способами, представленными на Фиг. 5 – 7, в замкнутой цепи посредством генерирования и считывания двумерных кодов при помощи устройств 13. В одном из вариантов осуществления настоящего изобретения, эти способы и система эти способы и система дают возможность всем участникам процесса выполнять конфигурацию системы и управлять своими макроэкономическими параметрами, уровнем своего внутреннего потребления с своей продукцией. Данный комбинированный способ можно разделить на три основные части – процесс обновления информации, процесс покупки товара и процесс возврата денежных средств, которые соответствуют способу списания денежных средств, способу совершения покупки и способу возврата денежных средств, описанным выше.

Перевод первоначального описания

На Фиг.10 изображена блок-схема, иллюстрирующая этапы способа 550 для проверки транзакции пользователем, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 550 начинается, когда устройство 13а пользователя привязывается или сопрягается 551 с картой пользователя и, следовательно, с устройством пользователя 13а. В результате привязки или сопряжения 551 карты с пользовательским устройством 13а в системе устанавливается персональный идентификационный номер (ПИН) 553, при этом создается двумерный код, содержащий информацию о пользователе, включая такие данные, как ПИН-код, имя пользователя, дату рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе. Двумерный код отображается 555 на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает его 557. Сканируя или захватывая двумерный код 557 пользовательского устройства 13а, оператор может выбрать конкретную услугу или заказ 581 на операторском устройстве 13b, в результате чего заказ, включающий выбранные товары и/или услуги, а также их количество, может быть сформирован 583 на операторском устройстве 13b, при этом создается двумерный код, включающий по меньшей мере данные, указанные выше. Двумерный код отображается на экране 122 операторского устройства 13b, а камера 115 пользовательского устройства 13а сканирует или захватывает его 585. После сканирования или захвата 585 двумерного кода с операторского устройства 13b, пользовательское устройство 13а генерирует группу двумерных кодов 587, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть подтверждена операторским устройством 13b. После отображения SAR-кода на

Перевод первоначального описания

экране 122 пользовательского устройства 13a, SAR-код сканируется или захватывается 589 камерой 115 операторского устройства 13b, и (b) на пользовательском устройстве 13a генерируется 591 запрос на транзакцию в магазине. В устройстве оператора, когда камера устройства оператора 13b (a) сканирует или захватывает SAR-код 589, устройство оператора 13b запрашивает ПИН-код 559, который должен быть введен 561 пользователем. Операторское устройство 13b проверяет 563 действительность ПИН-кода и, если ПИН-код оказывается неверным, отправляет сообщение об ошибке 565. Если же проверенный ПИН-код 563 действительно верен, то операторское устройство 13b дает возможность создать транзакцию 579, позволяющую пользовательскому устройству 13a получить желаемые товары или услуги 575.

На устройстве пользователя, когда генерируется запрос на транзакцию с магазином 591, пользователь может затем получить желаемые товары или услуги 575 на устройстве пользователя 13a. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция расшифровки позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. В одном из вариантов осуществления настоящего изобретения, после создания ПИН-кода пользователь может использовать номер, связанный с кодом идентификатора пользователя, для подтверждения ПИН-кода и выполнения транзакций без устройства 113a и без чипа с поддержкой протокола NFC.

На Фиг.10А изображена блок-схема, иллюстрирующая этапы другого способа 550А для проверки транзакции пользователем, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа начинается,

Перевод первоначального описания

когда устройство 13а пользователя привязывается или сопрягается 552 с картой пользователя и, следовательно, с устройством пользователя 13а. При привязке или сопряжении 552 карты с пользовательским устройством 13а, в системе устанавливается персональный идентификационный номер (ПИН) 554, в котором в соответствии с заявленным способом проверяется ПИН-код 556, при этом если ПИН-код не может быть проверен 556, генерируется и отправляется сообщение об ошибке 558. Если же ПИН-код может быть проверен 556, генерируется двумерный код, содержащий информацию о пользователе, включая такие данные, как ПИН-код, имя пользователя, дату рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе. Двумерный код отображается 560 на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает его 564. В свою очередь, на операторском устройстве 13b выбирается конкретная услуга и/или заказ на товар 562, поэтому заказ, включающий выбранные товары и/или услуги, а также их количество, может быть затем сформирован операторским устройством 13b, которое, в свою очередь, генерирует двумерный код 564, включающий по меньшей мере данные, указанные выше. Двумерный код отображается на экране 122 операторского устройства 13b, а камера 115 пользовательского устройства 13а сканирует или захватывает его 566. После сканирования или захвата 566 двумерного кода с операторского устройства 13b пользовательское устройство 13а проверяет событие 568 и, если оно не может подтвердить событие 568, генерирует и отправляет сообщение об ошибке 570. Если возможно проверить событие 568, проверяется возраст 572 покупателя. Если подтверждение возраста 572 невозможно, генерируется и отправляется сообщение об ошибке 574. Если способ позволяет осуществить проверку возраста 572, то далее проверяется кредитный лимит 576 или баланс и, если проверка кредитного лимита 576 или баланса невозможна, то генерируется и отправляется сообщение об ошибке

Перевод первоначального описания

578. Если проверка кредитного лимита 576 или баланса в соответствии с указанным способом возможна, то генерируется группа двумерных кодов 580, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена операторским устройством 13b. После отображения SAR-кода на экране 122 пользовательского устройства 13a, SAR-код сканируется или захватывается 586 камерой 115 операторского устройства 13b, и запрос на транзакцию 582 генерируется и сохраняется на пользовательском устройстве 13a. На устройстве оператора, когда камера устройства оператора 13b сканирует или захватывает SAR-код 586, устройство оператора 13b создает транзакцию 588, которая позволяет устройству пользователя 13a получить желаемые товары, заказ или услуги 584. С помощью функции считывания двумерных кодов способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования способна расшифровать по меньшей мере один правильный двумерный код и проверить информацию в по меньшей мере одном двумерном коде. Подспособ, варьирующийся от отображения 560 двумерного кода до сканирования 586 группы двумерных кодов может быть осуществлен при организации непосредственной коммуникационной связи между двумя устройствами, причём мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства. В одном из вариантов осуществления настоящего изобретения, после создания ПИН-кода, пользователь может использовать номер, связанный с кодом

Перевод первоначального описания

идентификатора пользователя, для подтверждения ПИН-кода и выполнения транзакций без устройства 113a и без чипа с поддержкой протокола NFC.

На Фиг.11 изображена блок-схема, иллюстрирующая этапы способа 650 совершения покупок на сайте, в котором двумерные коды генерируются и считываются устройствами 13, причём указанный способ реализуется, в альтернативном варианте осуществления изобретения, в режиме онлайн. Указанный способ 650 начинается, когда устройство 13a пользователя привязывается или сопрягается 652 с картой пользователя и, следовательно, с устройством пользователя 13a. Аналогично, способ может начать осуществляться, когда на пользовательском устройстве 13a производится обновление баланса 654, которое может быть произведено, как описано ранее, в соответствии со способами, проиллюстрированными на Фиг.5 или Фиг.5А, или любым другим известным или будущим известным способом списания денежных средств. Привязка или сопряжение 552 с картой может быть выполнено параллельно или вместо списания денежных средств 654, и аналогично, списание денежных средств 654 может быть параллельно или вместо привязки или сопряжения 652 с картой. При привязке, сопряжении 652 и/или списании денежных средств 654 генерируется двумерный код, содержащий информацию о пользователе, включая такие данные, как ПИН-код, имя пользователя, дата рождения пользователя, идентификационный номер карты, выполненное списание денежных средств или любая другая информация о пользователе. Двумерный код отображается 658 на экране 122 пользовательского устройства 13a, а камера 115 операторского устройства 13b сканирует или фиксирует его. В свою очередь, на операторском устройстве 13b выбирается конкретная услуга заказ на товар и/или заказ 656, поэтому заказ, включающий выбранные товары и/или услуги, а также количество заказанных товаров, может быть затем сформирован операторским устройством 13b, которое, в свою очередь, генерирует двумерный код

Перевод первоначального описания

660, включающий по меньшей мере данные, указанные выше. Двумерный код отображается на экране 122 операторского устройства 13b, а камера 115 пользовательского устройства 13a сканирует или захватывает его 662. После сканирования или захвата 662 двумерного кода операторским устройством 13b пользовательское устройство 13a проверяет баланс 664 и, если нет возможности проверить баланс 664, проверяется кредитный лимит 666. Если подтверждение кредитного лимита невозможно, то проверяется метод оплаты 668 и, если невозможно подтвердить метод оплаты 668, генерируется и отправляется сообщение об ошибке 676, указывающее, что требуется пополнение баланса. Если невозможно проверить баланс 664 или если невозможно проверить кредитный лимит 666, генерируется группа двумерных кодов 678, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена операторским устройством 13b. После отображения SAR-кода на экране 122 пользовательского устройства 13a, SAR-код сканируется или захватывается 682 камерой 115 операторского устройства 13b, и количество товаров и их наименования, которые должны быть получены, выводятся 680 на пользовательском устройстве 13a. На устройстве оператора, когда камера устройства оператора 13b сканирует или захватывает SAR-код 682, устройство оператора 13b создает транзакцию 684, которая позволяет устройству пользователя 13a получить желаемые товары, заказ или услуги 680. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию,

Перевод первоначального описания

хранящуюся в по меньшей мере одном двумерном коде. При невозможности проверки метода оплаты 668, проверяется есть ли сигнал данных 670. Если сигнал данных 670 отсутствует, то снова проверяется наличие сигнала данных 686 и, если сигнал данных отсутствует, посылается сообщение об ошибке 676, требующее, возможно, обновления баланса 654. В случае, если при любой из двух проверок 670, 686 можно подтвердить, что сигнал данных есть, обрабатывается платеж 672, для чего используется платежный процессор 674. Если платеж не может быть обработан 672, отправляется сообщение об ошибке 676, требующее, возможно, обновления баланса 654. Если платеж может быть обработан 672, генерируется группа двумерных кодов 678, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода). как описано выше, для того, чтобы операторское устройство 13b создало транзакцию 684 и предъявителю пользовательского устройства 13a было разрешено получить желаемые товары, заказ или услуги 680. Подспособ, варьирующийся от отображения двумерного кода 658 до получения желаемых товаров, заказа или услуг 680, создания транзакции 684, обработки платежа 672 и проверки сигналов данных 670, 686, может быть осуществлен при организации непосредственной коммуникационной связи между двумя устройствами, при этом мобильные устройства по меньшей мере имеют одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства.

На Фиг.11А изображена блок-схема, иллюстрирующая этапы способа 650А совершения покупок на сайте, в котором двумерные коды генерируются и считываются по меньшей мере одним устройством 1313. Выполнение способа 650А начинается, когда пользовательское устройство 13а привязывается или сопрягается 652 с картой пользователя и, следовательно, есть привязка карты к

пользовательскому устройству 13а. Аналогично, выполнение указанного способа может начаться, когда пользовательское устройство 13а обновляет баланс 654, что может быть выполнено, как описано ранее, в соответствии со способами, проиллюстрированными на Фиг.5 или Фиг.2 или Фиг.5А, или при помощи любых других известных в настоящее время из уровня техники или появившихся в будущем способов обновления информации. Привязка или сопряжение 652 с картой может быть выполнено параллельно или вместо обновления баланса 654, и аналогично, обновление баланса 654 может быть выполнено параллельно или вместо привязки или сопряжения 652 с картой. В свою очередь, количество денежных средств, подлежащее уплате, сообщается 657 оператором, а также количество средств, которое передается на пользовательское устройство; при этом, способ передачи данных может быть любым из известных из уровня техники или из установленных ранее. В процессе выработки предложения по цене, при выполнении привязки карты 652 и/или обновлении баланса счета 654 и установление количества денежных средств, подлежащего оплате 657, генерируется код, который может быть двумерным 655 на устройстве пользователя 13а, который содержит информацию о пользователе, включая такие данные, как ПИН-код, имя пользователя, дата рождения пользователя, идентификационный номер карты, произведенное пополнение или любую другую информацию о пользователе, а также количество, подлежащее уплате, сообщенное оператором. Сгенерированный код 655 хранится на устройстве пользователя 13а, и на устройстве пользователя 13а проверяется баланс 659, и если невозможно проверить баланс 659, то проверяется кредитный лимит 661. Если невозможно проверить кредитный лимит 661, то проверяется способ оплаты 663, и если невозможно проверить способ оплаты 663, то генерируется и отправляется сообщение об ошибке 665, указывающее, что требуется пополнение баланса. Если возможно проверить баланс 659 или если возможно проверить кредитный лимит 661,

Перевод первоначального описания

генерируется группа двумерных кодов 667, которые отображаются как безопасный анимированный код отклика (SAR-код), причём указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), а по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена операторским устройством 13b. После отображения SAR-кода на экране 122 пользовательского устройства 13a, SAR-код подтверждается оператором 669 как актуальный, и количество изделий и товары, которые должны быть получены, списываются 671 на пользовательском устройстве 13a. Подтверждение SAR-кода может осуществляться средствами, известными в данной области техники, например, при касании SAR-кода на сенсорном экране, для перемещения движением пальца SAR-кода, чтобы убедиться, что изображение не является снимком экрана или поддельным видеоизображением. Другие системы защиты, известные и которые станут известными в данной области техники, также могут считаться включенными в настоящее изобретение не ограничивающим образом, но в качестве примера. Когда оператор подтверждает 669 SAR-код, оператор предоставляет товары, заказ или услуги, которые должны быть предоставлены 673 предъявителю пользовательского устройства 13a. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. Если метод оплаты может быть проверен 663, то проверяется наличие сигнала данных 675. Если сигнал данных 675 отсутствует, то отправляется сообщение об ошибке 665, требующее, возможно, обновления баланса 653. Если может быть подтверждено, что при проверке 675 сигнал данных есть, платеж обрабатывается 677, для чего используется платежный

Перевод первоначального описания

процессор 679. Если платеж не может быть обработан 677, то отправляется сообщение об ошибке 665, требующее, возможно, обновления баланса 653. Если платеж может быть обработан 677, генерируется группа двумерных кодов 667, которые отображаются как безопасный анимированный код отклика (SAR), как описано выше, для того, чтобы оператор мог доставить товар, заказ или оказать услуги 673, а предъявителю пользовательского устройства 13а было бы позволено получить желаемые товары, заказ или услуги 671.

На Фиг.14 изображена блок-схема, показывающая этапы способа 1250 аутентификации пользователя на сайте по удостоверению личности, в котором двумерные коды генерируются и считываются устройствами 13. Выполнение указанного способа начинается, когда пользовательское устройство 13а отображает 1255 двумерный код, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дату рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе, на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает его 1257. После сканирования или захвата 1257 двумерного кода 1257 пользовательского устройства 13а, операторское устройство 13b определяет 1259, является ли пользователь законным владельцем удостоверения личности. Если установлено 1259, что пользователь не является законным владельцем удостоверения личности, на операторское устройство 13b отправляется сообщение об ошибке 1261. Если было установлено 1259, что пользователь является законным владельцем удостоверения личности, операторское устройство 13b подтверждает 1263, что удостоверение личности соответствует личности пользователя, и тогда пользователю следует предъявить 1265 удостоверение личности оператору, а оператор должен сфотографировать 1267 удостоверение личности, которое затем зашифровывается, и при этом генерируются двумерные

Перевод первоначального описания

коды 1269 с отображением в виде безопасного анимированного кода отклика (SAR-кода), причём указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), а по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть подтверждена пользовательским устройством 13a. Этап фотографирования 1267 удостоверения личности не является обязательным для выполнения. После генерирования группы двумерных кодов 1269, удостоверение личности проходит проверку подлинности 1271 на устройстве оператора 13b. Кроме того, после того как группа двумерных кодов 1269 сгенерирована и отображена на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 1273 камерой 115 пользовательского устройства 13a. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования SAR-кода 1273 и расшифровки правильного QR-кода на пользовательском устройстве 13a получается аутентификация 1275 пользователя по идентификатору.

На Фиг.14А изображена блок-схема, показывающая этапы способа 1250А иной аутентификации пользователя на сайте по удостоверению личности, при этом двумерные коды генерируются и считываются устройствами 13. Осуществление способа 1250А начинается, когда пользователь предъявляет 1252 удостоверение личности с фотографией, при этом установление личности пользователя может проводиться по официальному документу с фотографией, а оператор выполняет проверку 1254 соответствует ли удостоверение личности указанному пользователю. Оператор делает фотографию 1256 проверенного им удостоверения личности

Перевод первоначального описания

пользователя; причём этап фотографирования 1256 удостоверения личности пользователя не является обязательным для выполнения. В свою очередь, пользователь показывает своё лицо 1258 для создания соответствующего файла, а оператор при помощи операторского устройства 13b фотографирует лицо 1260 для указанного пользователя; на операторском устройстве 13b удостоверение личности пользователя проходит аутентификацию и файл пользователя обновляется 1262. Пользователь, посредством пользовательского устройства 13a, отображает 1264 двумерный код, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе, на экране 122 пользовательского устройства 13a, а камера 115 операторского устройства 13b сканирует или захватывает его. В операторском устройстве 13b генерируется группа двумерных кодов 1266 и отображается в виде безопасного анимированного кода отклика (SAR-кода), при этом группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по крайней мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке пользовательским устройством 13a. После генерирования группы двумерных кодов 1266, указанная группа двумерных кодов отображается на экране 122 операторского устройства 13b, а камера 115 пользовательского устройства 13a сканирует или захватывает их, в результате чего они проходят проверку подлинности на пользовательском устройстве 13a. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования SAR-кода 1268 и расшифровки правильного

Перевод первоначального описания

QR-кода на пользовательском устройстве 13а происходит аутентификация 1270 пользователя по удостоверению личности. Подспособ, варьирующийся от отображения двумерного кода 1264 и генерирования SAR-кода 1266 до сканирования SAR-кода, 1268 может быть выполнен при организации непосредственной коммуникационной связи между двумя устройствами, при этом мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, а метод считывания/сканирования выполняется без вмешательства оператора и/или пользователя относительно переворачивания соответствующего мобильного устройства. После подтверждения 1270 удостоверения личности, полученного на пользовательском устройстве 13а, пользовательское устройство 13а отображает 1272 двумерный код с помощью своего экрана 122, который сканируется или захватывается камерой 115 операторского устройства 13b. Двумерный код 1272, отображаемый устройством 13а пользователя, может включать данные пользователя, такие как его имя, пол, возраст и т.д. Устройство 13b оператора отображает 1274 двумерный код с помощью своего экрана 122, который сканируется или захватывается 1276 камерой 115 устройства 13а пользователя. Затем, способ обеспечивает выполнение проверки события 1278 на пользовательском устройстве 13а. Если пользовательское устройство 13а действительно имеет соответствующее событие и привилегии, способ обеспечивает проверку правильности учетных данных 1282. Если подтверждается, что учетные данные верны, генерируется группа двумерных кодов 1286, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, подлежащую проверке операторским устройством 13b. После того как группа двумерных кодов сгенерирована 1286 и отображена на экране 122 пользовательского устройства 13а, запрос на транзакцию

Перевод первоначального описания

сохраняется 1288 на пользовательском устройстве 13a, и пользователь получает привилегию 1290. В свою очередь, сгенерированный SAR сканируется и/или считывается 1292 с помощью камеры 115b устройства оператора 13b для создания транзакции 1294 на устройстве оператора 13b и для предоставления привилегии 1296 оператором. Подспособ, варьирующийся от отображения 1272 двумерного кода до сканирования 1292 группы двумерных кодов, может быть осуществлен при организации непосредственной коммуникационной связи между двумя устройствами, в котором мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя в отношении переворачивания соответствующего мобильного устройства. Функция считывания двумерных кодов позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция расшифровки позволяет расшифровать по меньшей мере один правильный двумерный код, проверить информацию двумерного кода, разрешить доступ 1290 к пользовательскому устройству 13a и соответствующему пользователю и создать транзакцию 1294. В случае, если при проверке нет доступа к событию 1278 или если учетные данные не могут быть проверены 1282, генерируется и отправляется сообщение об ошибке 1280.

На Фиг.14В изображена блок-схема, показывающая этапы способа 1250В иной аутентификации пользователя на сайте по удостоверению личности, при этом генерирование и считывание двумерных кодов выполняется устройствами 13. Осуществление способа 1250В начинается, когда указанный пользователь предъявляет регистрационные данные или удостоверение личности 1300, причём указанные учётные данные или удостоверение личности могут быть снабжены фоторграфией, и оператор при этом проверяет 1302, что удостоверение личности

Перевод первоначального описания

пользователя соответствует указанному пользователю. Оператор фотографирует 1304 учётные данные пользователя или его удостоверение личности, затем выполняется аутентификация удостоверения личности учётным данным, и происходит обновление 1306 файла пользователя. Пользователь с помощью пользовательского устройства 13а предъявляет 1308 двумерный код, содержащий информацию пользователя, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию пользователя на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает его. В операторском устройстве 13b генерируются двумерные коды 1310 и отображаются в виде безопасного анимированного кода отклика (SAR-кода), где группа двумерных кодов может быть группой кодов быстрого отклика (QR-код), при этом по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена пользовательским устройством 13а. После генерирования группы двумерных кодов 1310, указанная группа двумерных кодов отображается на экране 122 операторского устройства 13b и камера 115 пользовательского устройства 13а сканирует или захватывает 1312 его, производя аутентификацию на пользовательском устройстве 13а. С помощью функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования SAR-кода 1312 и расшифровки правильного QR-кода на пользовательском устройстве 13а происходит аутентификация 1314 по удостоверению личности пользователя. Подспособ, варьирующийся от отображения двумерного кода 1308, генерирования

Перевод первоначального описания

SAR-кода 1266 до сканирования SAR-кода 1312, может быть выполнен при организации непосредственной коммуникационной связи между двумя устройствами, при этом мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования выполняется без вмешательства оператора и/или пользователя в отношении поворота соответствующего мобильного устройства.

На Фиг.15 изображена блок-схема, показывающая этапы способа 1050 аутентификации метода платежа на сайте посредством генерирования и считывания двумерных кодов при помощи устройств 13. Осуществление указанного способа начинается, когда пользовательское устройство 13а отображает 1055 двумерный код, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе, на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает 1057 эту информацию. Сканируя или захватывая двумерный код 1057 пользовательского устройства 13а, операторское устройство 13b определяет 1059, является ли пользователь законным владельцем карты. Если установлено 1059, что пользователь не является законным владельцем карты, на операторское устройство 13b отправляется сообщение об ошибке 1061. Если пользователь был определен 1059 как законный владелец карты, операторское устройство 13b подтверждает 1063, что карта соответствует пользователю, и пользователь должен предъявить карту 1065 оператору, оператор должен сфотографировать карту 1067, которая затем шифруется, и генерируется группа двумерных кодов 1069 и отображается как безопасный анимированный код отклика (SAR-код), где группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), где по крайней мере один из двумерных кодов включает зашифрованную

Перевод первоначального описания

информацию, которая должна быть проверена пользовательским устройством 13a. После генерирования группы двумерных кодов 1069, карта и способ оплаты аутентифицируются 1071 на устройстве оператора 13b. Также, после генерирования группы двумерных кодов 1069 и отображения их на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 1073 камерой 115 пользовательского устройства 13a. При помощи функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования SAR-кода 1073 и расшифровки правильного QR-кода на пользовательском устройстве 13a происходит аутентификация 1075 идентификационных данных пользователя.

На Фиг.16 изображена блок-схема, показывающая этапы способа 1150 аутентификации учётных данных на сайте посредством генерирования и считывания двумерных кодов при помощи устройств 13. Осуществление указанного способа начинается, когда пользовательское устройство 13a отображает 1155 двумерный код, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе на экране 122 пользовательского устройства 13a, а камера 115 операторского устройства 13b сканирует или захватывает 1157 эту информацию. Сканируя или захватывая 1157 двумерный код пользовательского устройства 13a, операторское устройство 13b определяет 1159, является ли пользователь законным владельцем учётных данных. Если определено, что пользователь не является законным владельцем учётных данных, на операторское устройство 13b отправляется сообщение об ошибке 1161.

Перевод первоначального описания

Если установлено, что пользователь 1159 является законным владельцем учётных данных, операторское устройство 13b подтверждает 1063, что учетные данные соответствует пользователю, и пользователь должен предъявить учетные данные 1165 оператору, оператор должен сфотографировать учетные данные 1167, которые затем шифруются, и генерируется группа двумерных кодов 1169 и отображается в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть подтверждена пользовательским устройством 13a. После генерирования группы двумерных кодов 1169, учетные данные подвергаются аутентификации 1171 на устройстве оператора 13b. Также, после генерирования группы двумерных кодов 1169 и отображения их на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 1173 камерой 115 пользовательского устройства 13a. При помощи функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования SAR-кода 1073 и расшифровки правильного QR-кода на пользовательском устройстве 13a происходит аутентификация 1175.

На Фиг.16А изображена блок-схема, показывающая этапы способа 1150А аутентификации метода платежа на сайте, при этом генерирование и считывание двумерных кодов выполняется устройствами 13. Осуществление указанного способа 1150А начинается, когда карта 1152, соответствующая пользователю, отображается или «прокатывается» через считывающее устройство.

Перевод первоначального описания

При предъявлении или прокатывании карты 1152, оператор подтверждает, что карта 1154 соответствует пользователю, передает или фотографирует карту 1156 и аутентифицирует пользователя и платеж 1158. Пользовательское устройство 13а отображает на экране 122 пользовательского устройства 13а двумерный код 1160, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе, и камера 115 операторского устройства 13b сканирует или захватывает его. При сканировании или захвате двумерного кода генерируется группа двумерных кодов 1162 и отображается в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть подтверждена пользовательским устройством 13а. После генерирования группы двумерных кодов 1162 и отображения их на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 1164 камерой 115 пользовательского устройства 13а. При помощи функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования 1164 SAR-кода и расшифровки правильного QR-кода в пользовательском устройстве 13а происходит аутентификация метода оплаты 1166. Подспособ, варьирующийся от отображения двумерного кода 1160, генерирования SAR-кода 1162 до сканирования SAR-кода 1164, может быть выполнен при организации непосредственной коммуникационной связи между двумя устройствами, причём мобильные устройства

Перевод первоначального описания

имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования выполняется без вмешательства оператора и/или пользователя в отношении поворота соответствующего мобильного устройства.

На Фиг.17 изображена блок-схема, показывающая этапы способа 950 аутентификации документа о соглашении на сайте посредством генерирования и считывания двумерных кодов при помощи устройств 13. Осуществление указанного способанабначается, когда документ о соглашении 955 загружается в операторское устройство 13b. После загрузки 955 генерируется 957 и отображается на экране 122 операторского устройства 13b двумерный код, содержащий информацию о пользователе, включая такие данные, как соглашение, идентификация и любая другая необходимая информация, который затем сканируется или захватывается 959 камерой 115 пользовательского устройства 13a. Сканируя или захватывая 959 двумерный код пользовательского устройства 13b, пользовательское устройство 13a определяет 961, было ли аутентифицировано удостоверение личности пользователя. Если установлено 961, что удостоверение личности пользователя не прошло аутентификацию, то отправляется запрос на аутентификацию удостоверения личности пользователя 963 на пользовательском устройстве 13a. Если было установлено 961, что удостоверение личности пользователя прошло аутентификацию, то пользовательское устройство 13a генерирует группу двумерных кодов 965 в виде безопасного кода анимированного отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена операторским устройством 13b. После генерирования группы двумерных кодов 965 определяется, готово ли вышеуказанное соглашение к подписанию 967 сторонами. Если установлено 967, что соглашение еще не готово к подписанию сторонами, то

Перевод первоначального описания

аутентификация соглашения отменяется 969. Если установлено 967, что соглашение готово к подписанию сторонами, то сгенерированный SAR-код 965 отображается на экране 122 устройства 13a, при этом сгенерированный SAR-код сканируется и/или считывается 971 камерой 115 операторского устройства 13b. При помощи функции считывания двумерных кодов, заявленный способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию в по меньшей мере одном двумерном коде. После сканирования 971 SAR-кода и расшифровки правильного QR-кода определяется 973, следует ли добавить другого пользователя или свидетеля в соглашение, и если другой пользователь или свидетель должен быть добавлен в соглашение, сканируется новый SAR-код 971. Если установлено 973, что нет необходимости добавлять другого пользователя или аппаратный ключ (токен) к соглашению, то пользовательское устройство 13a аутентифицирует подписанный документ соглашения 975 и отправляет подписанный аутентифицированный документ 977 сторонам, участвующим в соглашении.

На Фиг.17A изображена блок-схема, показывающая этапы способа 950A иной аутентификации документа о соглашении на сайте посредством генерирования и считывания двумерных кодов при помощи устройств 13. Осуществление указанного способа 950A начинается, когда документ о соглашении 956 загружается в операторское устройство 13b. В свою очередь, пользовательское устройство 13a проверяет подлинность удостоверения личности пользователя 952 и отображает двумерный код, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, пол и возраст пользователя или любую другую информацию о пользователе, при этом код

Перевод первоначального описания

отображается на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает его. При сканировании или захвате двумерного кода и загрузке документа соглашения 956 генерируется двумерный код 958, содержащий информацию подписанного соглашения, включая такие данные, как текст соглашения, идентификационные данные и любая другая необходимая информация, и он отображается на экране 122 операторского устройства 13b, который затем сканируется или захватывается 960 камерой 115 пользовательского устройства 13а. При сканировании или захвате 959 двумерного кода пользовательского устройства 13b пользовательское устройство 13а проверяет 962 учетные данные пользователя. Если определено 962, что учетные данные пользователя не совпадают с истинными, отправляется запрос на аутентификацию удостоверения личности пользователя 964 в пользовательском устройстве 13а и здесь требуется выполнение аутентификации удостоверения личности пользователя 952. Если установлено 962, что учетные данные пользователя соответствуют истинным, пользовательское устройство 13а генерирует группу двумерных кодов 966 в виде безопасного анимированного кода быстрого отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть подтверждена операторским устройством 13b. После генерирования группы двумерных кодов 966, подпись запроса на передачу данных 968 сохраняется в пользовательском устройстве, а сгенерированный SAR-код 966 отображается на экране 122 пользовательского устройства 13а, причём сгенерированный SAR-код сканируется и/или считывается 970 с помощью камеры 115 операторского устройства 13b. При помощи функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который

должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию в по меньшей мере одном двумерном коде. После сканирования SAR-кода 970 и расшифровки правильного QR-кода определяется 972, следует ли добавить другие подписи к соглашению, и если другие подписи должны быть добавлены к соглашению, выдается запрос на проверку подлинности новых идентификационных данных 952. Если определяется 972, что нет необходимости добавлять еще одну подпись, пользовательское устройство 13а аутентифицирует подписанный документ соглашения 974 и отправляет подписанный, аутентифицированный документ 976 сторонам, участвующим в соглашении. Подспособ, выходящий от отображения двумерного кода 954, генерирования SAR-кода 958 с подписанным соглашением до сканирования SAR-кода 970, может быть выполнен при организации непосредственной коммуникационной связи между двумя устройствами, причём указанные мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и способ считывания/сканирования выполняется без вмешательства оператора и/или пользователя в отношении поворота соответствующего мобильного устройства.

На Фиг.18 изображена блок-схема, показывающая этапы способа 850 для автохода с устройства на сайт, причём указанный вход на сайт осуществляется частично в режиме онлайн, а генерирование и считывание двумерных кодов осуществляется при помощи указанных устройств 13. Осуществление указанного способанабначается, когда операторское устройство 13b отображает 851 двумерный код, содержащий информацию о проверке, на экране 122 операторского устройства 13b, а камера 115 пользовательского устройства 13а сканирует или захватывает 853 его. Сканируя или захватывая 853 двумерный код операторского устройства 13b, пользовательское устройство 13а определяет 855, является ли приложение

Перевод первоначального описания

правильным. Если установлено, что приложение является неправильным, пользовательское устройство 13b генерирует и отправляет сообщение об ошибке 857 на пользовательское устройство 13a. Если же в соответствии со способом определяется 855, что приложение является правильным, то пользовательское устройство 13a генерирует группу двумерных кодов 859, которые отображаются в виде безопасного анимированного код отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена операторским устройством 13b. После генерирования группы двумерных кодов 859 и отображения их на экране 122 пользовательского устройства 13a, сгенерированный SAR-код сканируется и/или считывается 863 камерой 115 операторского устройства 13b. При помощи функции считывания двумерных кодов, способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию в по меньшей мере одном двумерном коде. Параллельно со сканированием 863 на пользовательском устройстве 13a регистрируется логин устройства 861. После сканирования SAR-кода 863 и расшифровки действительного QR-кода проверяется наличие сигнала данных 865 на устройстве оператора 13b, и если установлено, что сигнал данных отсутствует, генерируется и отправляется сообщение об ошибке 869. Если установлено наличие сигнала данных, выполняется обработка логина для подключения к данным 867, данные пользователя 871 загружаются с помощью указанного подключения, и подтверждается синхронизация 873 данных. Следует отметить, что на блок-схеме, представленной на Фиг.18, можно увидеть другие варианты применения описанной системы, например,

Перевод первоначального описания

автоматический запуск устройств, а именно вместо входа в систему по логину, что может быть выполнено как показано на блок-схеме, представленной на Фиг. 18, в соответствии с которой могут быть запущены устройства, такие как транспортные средства или рабочие машины, которые могут быть доступны для аренды.

На Фиг.19 изображена блок-схема, показывающая этапы способа 750 для использования общего ключа на сайте при помощи генерирования и считывания двумерных кодов из указанных устройств 13. Осуществление указанного способанабначается, когда пользовательское устройство 13а отображает 755 двумерный код, содержащий информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает 757 эту информацию. Сканируя или захватывая 757 двумерный код пользовательского устройства 13а, операторское устройство 13b определяет 759, имеет ли пользователь правильные учетные данные. Если установлено 759, что пользователь не имеет правильных учетных данных, на операторское устройство 13b отправляется сообщение об ошибке 761. Если установлено 759, что пользователь имеет правильные учетные данные, операторское устройство 13b генерирует группу двумерных кодов 763, которые отображаются в виде безопасного анимированный код отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть подтверждена пользовательским устройством 13а. После генерирования группы двумерных кодов 763 и отображения их на экране 122 операторского устройства 13b, сгенерированный SAR-код сканируется и/или считывается 765 камерой 115 пользовательского устройства 13а. При помощи

Перевод первоначального описания

функции считывания двумерных кодов, способен позволяет считывать все двумерные коды, представленные в SAR-коде , и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в по меньшей мере одном двумерном коде. После сканирования 765 SAR-кода и расшифровки правильного QR-кода, ключ находится внутри QR-кода и затем сканируется на входе в шлюз 759. Затем устанавливается 771, есть ли ключ у пользовательского устройства 13а, и если у пользовательского устройства 13 нет ключа, на пользовательское устройство отправляется сообщение об ошибке 773. Если установлено 771, что у пользовательского устройства есть ключ, то пользовательское устройство 13а генерирует группа двумерных кодов 775, которые отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), где по крайней мере один из двумерных кодов включает зашифрованную информацию, и шлюз открывается 777.

На Фиг.20 изображена блок-схема, показывающая способ 2050 совершения покупок на сайте с проверкой его возраста пользователя и участия в рекламных акциях, при этом генерирование и считывание двумерных кодов выполняется при помощи указанных устройств 13. Реализация указанного способа 2050 начинается, когда пользовательское устройство 13а отображает двумерный код, содержащий такие данные, как возраст, сведения о рекламных акциях, балансы и аппаратные ключи (токены), на экране 122 пользовательского устройства 13а, а камера 115 операторского устройства 13b сканирует или захватывает его 2053. При сканировании или захвате 2053 устройство оператора также проверяет возраст, сведения о рекламных акциях, баланс и требуемые аппаратные ключи (токены).

Перевод первоначального описания

Затем устройство оператора выбирает заказы и/или товары 2055. В свою очередь, пользовательское устройство 13а отображает на экране 122 двумерный код 2057, который сканируется или захватывается 353 камерой 115 операторского устройства 13b. Двумерный код содержит информацию о пользователе, включая такие данные, как имя пользователя, дата рождения пользователя, идентификационный номер карты или любую другую информацию о пользователе. Далее, в соответствии с указанным способом, генерируется по меньшей мере один двумерный код 2059 с выбранными заказами и/или товарами и информацией двумерного кода, отображаемой с пользовательского устройства 13а, а также сведениями о рекламных акциях, балансах и аппаратных ключах (токенах); в случае, если двумерных кодов несколько, они отображаются в виде безопасного анимированного кода отклика (SAR-кода), при этом по меньшей мере один двумерный код может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один двумерный код включает зашифрованную информацию для проверки пользовательским устройством 13а. После генерирования группы двумерных кодов 2059 и отображения их на экране 122 операторского устройства 13b, SAR-код, сгенерированный с помощью камеры 115а пользовательского устройства 13а, сканируется и/или считывается 2061. При помощи функции считывания двумерных кодов, заявленный способ позволяет считывать все двумерные коды, представленные в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию, хранящуюся в двумерном коде. Затем, в соответствии с заявленным способом, проверяется событие 2063, и если указанное событие 2063 не может быть проверено, то генерируется и отправляется сообщение об ошибке 2065. Если же проверка события 2063 возможна, то проверяется возраст 2067 пользователя, а при невозможности проверки указанного возраста 2067, он

Перевод первоначального описания

генерируется и отправляется сообщение об ошибке 2065. Если проверка возраста 2067 возможна, то проверяется баланс 2069, и при невозможности проверки баланса 2069, генерируется и отправляется сообщение об ошибке 2065. Если баланс 2069 может быть проверен, то генерируется вторая группа двумерных кодов 2071 с балансом, отображаемым в виде безопасного анимированного кода отклика (SAR-кода), при этом указанная вторая группа двумерных кодов может быть группой кодов быстрого отклика (QR-кодов), причём по меньшей мере один из двумерных кодов включает зашифрованную информацию, которая должна быть проверена устройством оператора 13b. Двумерный код с проверенной информацией содержит такую информацию, как идентификатор события, код, сумма и номер транзакции, среди прочего. Предпочтительно, когда в этот момент сумма 2073 списывается с оффлайн-ового лицевого счёта пользователя в личном кабинете. После генерирования второй группы двумерных кодов 2071 и отображения их на экране 122 пользовательского устройства 13a, SAR-код, сгенерированный камерой 115b операторского устройства 13b, сканируется и/или считывается 2075. Подспособ, варьирующийся от отображения 2057 двумерного кода до сканирования 2075 группы двумерных кодов, может быть реализован при организации непосредственной коммуникационной связи между двумя устройствами. При этом, указанные мобильные устройства имеют по меньшей мере одну камеру на той же стороне, что и экран 122, и метод считывания/сканирования осуществляется без вмешательства оператора и/или пользователя относительно поворота соответствующего мобильного устройства. При помощи функции считывания двумерных кодов, заявленный способ позволяет считывать все коды из второй группы двумерных кодов, представленных в SAR-коде, и выделить по меньшей мере один правильный двумерный код, который должен быть расшифрован. Функция дешифрования позволяет расшифровать по меньшей мере один правильный двумерный код и проверить информацию в

двумерном коде. После сканирования и/или считывания 2075 SAR-кода с помощью устройства оператора 13b, покупка и регистрация/передача данных подтверждаются/закрываются и создается новая транзакция 2077.

Как показано на Фиг.12, способ генерирования и отображения SAR-кода может включать монтирование информации о данных S110, создание базового набора данных S120, шифрование указанного набора данных S130, создание зашифрованных данных фрейма S140, преобразование зашифрованных данных фрейма в машиночитаемые элементы графики S150 и отображение указанных элементов графики S160. Монтирование информации о данных выполняется с целью сбора данных, которые должны быть переданы, совместно с введенными исходными данными для запуска процесса генерирования SAR-кода. Монтирование информации о данных может включать в себя монтирование информационных данных (например, информационного набора, который должен быть передан $I = \{I_1, I_2, I_3, \dots, I_k\}$, шифровального ключа (K_e), закрытого ключа (K_{priv}) и набора данных о номерах фреймов ($FN = \{FN_0, FN_1, FN_2, \dots, FN_k\}$). Набор номеров фреймов (FN) предпочтительно включает в себя группу номеров фреймов ($\{FN_1, \dots, FN_k\}$, где $k > 1$). Количество номеров фреймов (k) предпочтительно соответствует информации со вторым набором данных (то есть количеству элементов данных во втором наборе данных (где второй набор данных представляет собой $I = \{I_1, I_2, \dots, I_k\}$)). Номера фреймов FN_0 - FN_k являются случайными числами, не дублирующимися от начального числа, $\min(FN_0, \dots, FN_k)$, до конечного числа, $\max(FN_0 - FN_k)$, таким образом, что они отформатированы по меньшей мере при помощи двух цифр. Указанные номера фреймов FN_i и указанный закрытый ключ K_{priv} заносятся в память 114, 116, предпочтительно во флэш-память 114. Создание базового набора данных выполняется для монтирования набора данных из введенных исходных данных. Каждый элемент в указанном базовом наборе данных может включать в себя

Перевод первоначального описания

последовательность случайных данных. При этом, генерируется новый набор данных S_6 , где $S = \{S_0, \dots, S_{\min(FN_0-FN_k)} \dots, S_{\max(FN_0-FN_k)}, \dots S_m\}$, и $0 < \min(FN_0-FN_k) \leq \max(FN_0-FN_k) < M$, и k является количеством наборов данных, которые являются подмножеством S . То есть, для информационного набора $I = \{I_1, \dots, I_k\}$, где I_i обозначает i -й информационный набор внутри I , генерируется соответствующий i -й набор данных $SFN_i = [I_i][RnS]$, который является элементом нового сгенерированного набора данных S_6 . Набор данных S_6 представляет собой случайные данные, не дублирующие начальный и конечный номера, отформатированные по меньшей мере двумя цифрами. Средство обработки информации использует данные длиной не менее 30 байт, предпочтительно не менее 50 байт и наиболее предпочтительно не менее 70 байт. Для нового набора данных S_i он состоит из номера фрейма и случайной строки (RnS), такой, что $S_0 = [FN_0][RnS]$. The FN0 frame data is defined as $SFN_0 = [Kprv][FN_1][FN_2][FN_3] \dots [FN_k][RnS]$. Данные, такие как $FN_1, FN_2, FN_3, \dots, FN_k$, определяются как $SFN_1 = [I_1][RnS]$, $SFN_2 = [I_2][RnS]$, $SFN_3 = [I_3][RnS]$... $SFN_k = [I_k][RnS]$. Шифрование набора данных выполняется для создания зашифрованного набора данных. Является предпочтительным, если S_0 и SFN_0 базового набора данных зашифрованы ключом шифрования Ke , а остальные элементы базового набора данных зашифрованы закрытым ключом $Kprv$. Создание зашифрованного набора данных, помеченного фреймом, позволяет подготовить зашифрованный набор данных для представления данных фрейма. К зашифрованным данным, помеченные фреймами, предпочтительно добавляется (или иным образом суммируется) номер фрейма, соответствующий соответствующему элементу в зашифрованном наборе данных. Например, Ske' будет равен $[FN_k][Sk]$ для каждого из $k = \{0, 1, 2, \dots, (\text{Общее количество фреймов}-1)\}$. Затем осуществляется преобразование зашифрованного набора данных типа "фрейм во фрейме" в набор машиночитаемых графических

Перевод первоначального описания

элементов для создания набора QR-кодов или других машиночитаемых элементов для представления в потоке. Машиночитаемый набор графических элементов предпочтительно представляет собой QR-коды, но в качестве альтернативы это могут быть другие формы двумерных графических кодов или даже одномерные графические коды (например, штрих-коды). Машиночитаемый код графически представляет данные, которые могут быть надежно интерпретированы машиной с возможностями визуализации. В одном из вариантов, набор данных может быть преобразован в средства вывода пользовательского интерфейса, такие как аудио, вибрационные модели (выводятся через тактильную обратную связь), инфракрасные световые модели (используются в проекционных световых камерах) и/или другие подходящие средства вывода пользовательского интерфейса. Графический дисплей может отображать набор машиночитаемой графики. Машиночитаемые графические изображения предпочтительно отображаются в установленном порядке, обозначенном номерами фреймов. В альтернативном варианте машиночитаемая графика может отображаться вне порядка или в постоянно меняющемся порядке. Кроме того, некоторые фреймы, в которых отсутствуют информационные данные или данные для считывания SAR-кода, могут быть опущены. Также могут быть добавлены шумовые фреймы. В одном из вариантов каждый из различных фреймов выбирается и отображается отдельно для имитации видео или анимации. В другом варианте фреймы монтируются в видео, GIF или другой подходящий видеоформат.

На Фиг.8 изображена блок-схема, показывающая генерирование по меньшей мере двух двумерных кодов в виде SAR-кода. Набор данных 2, подлежащий шифрованию в SAR-коде, включает любые желаемые или соответствующие данные. Как упоминалось выше, данные могут включать идентификатор события, имя пользователя, пол пользователя, код, такой как код транзакции и/или код события, возраст пользователя и т.д., среди прочих данных. Набор данных 2 предпочтительно

Перевод первоначального описания

включает ключ шифрования, причём ключ шифрования и набор данных хранятся в памяти 114, 116, предпочтительно во флеш-памяти 114. Как часть Фиг.8 сюда также может быть включено генерирование второго набора данных 4 для шифрования в SAR-коде, второй набор данных 4 включает закрытый ключ K_{prv} для шифрования данных, со случайной и/или псевдослучайной строкой символов, которая может иметь 8 или более байт. Для второго набора данных 4 генерируется фрейм, включающий номер фрейма FN и закрытый ключ K_{prv} . Генерируется группа номеров фреймов FN_k , и количество фреймов FN_i хранится в i раз, когда сохраняется информация I_i . Номера фреймов $FN_0 \sim FN_k$ - это случайные, не дублирующиеся числа от начального номера до конечного, отформатированные по меньшей мере при помощи двух цифр. Номера фреймов FN_k и закрытый ключ K_{prv} хранятся в памяти 114, 116, предпочтительно во флэш-памяти 114. Из первого набора данных 2 и второго набора данных 4 генерируется при помощи алгоритма новый набор данных S_6 , где количество наборов данных S_6 является случайным и не дублируется от начального числа до конечного числа, отформатированного по меньшей мере при помощи двух цифр. Средство обработки информации использует длину данных не менее 30 байт, предпочтительно не менее 50 байт и наиболее предпочтительно не менее 70 байт. Новый набор данных S_6 включает номер фрейма и случайную строку RNS, такую, что $S_0 = [FN_0][RnS]$. Данные фрейма FN_0 определяются как $SFN_0 = [K_{prv}][FN_1][FN_2][FN_3] \dots [FN_k][RnS]$. Данные $FN_1, FN_2, FN_3, \dots, FN_k$ определяются как $SFN_1 = [I_1][RnS]$, $SFN_2 = [I_2][RnS]$, $SFN_3 = [I_3][RnS] \dots SFN_k = [I_k][RnS]$. Чтобы избежать взлома или пиратства, средство обработки информации использует случайные строки в качестве дополнительных данных. Для повышения безопасности средство обработки информации может использовать 8 типов шифрования по стандарту AES-256 и, по меньшей мере, два ключа или другую технологию, использующую аналогичные или более высокие стандарты

Перевод первоначального описания

шифрования, где один ключ (K_e) является открытым ключом, а другой ключ (K_{prv}) – закрытым ключом. При этом, S_0 и SFN_0 шифруются ключом K_{mi} , а другие данные шифруются ключом K_{prv} , таким образом, что:

$$S_{0e} = \text{AES}(S_0, K_e)$$

$$SFN_{0e} = \text{AES}(SFN_0, K_e)$$

$$SFN_{1e} = \text{AES}(SFN_1, K_{prv})$$

$$SFN_{2e} = \text{AES}(SFN_2, K_{prv})$$

...

$$SFN_{29e} = \text{AES}(SFN_{29}, K_{prv})$$

В дополнение к декодированию SAR-кода, выполняется изменение указанного набора данных путём добавления в него номера фрейма 10 перед каждым элементом данных, таким образом что:

$$Ske' = [FNk][Ske], k = (0, 1, 2, \dots, 29)$$

В данном примере для наглядности используется 30 фреймов, но можно использовать любое подходящее количество фреймов или значение k . После добавления номера фрейма 10 генерируется набор двумерных кодов 12, соответствующих каждому из данных, с использованием библиотеки ZXing или тому подобного средства. Размер предпочтительного двумерного кода составляет 300x300 пикселей, и этот набор двумерных кодов хранится в памяти, предпочтительно в формате изображения. В конце этого процесса, SAR-код отображается 14 в способе отображения двумерного кода со скоростью, по меньшей мере, 1 двумерный код каждые 70 мс, предпочтительно 1 двумерный код каждые 40 мс. Для предотвращения взлома, SAR-код не хранится в устройстве 13, он лишь временно хранится в памяти 114, 116.

Как показано на Фиг.13, считывание и дешифрование SAR-кода предпочтительно включает считывание набора машиночитаемых кодов в

Перевод первоначального описания

последовательности S210, расшифровку машиночитаемых кодов в наборе данных S220, помеченных фреймами, извлечение зашифрованного набора данных, созданного путем удаления номеров фреймов из зашифрованного набора данных, S230, помеченных фреймами, извлечение закрытого ключа и набора номеров фреймов S240, монтирование зашифрованного базового набора данных S250, расшифровка зашифрованного базового набора данных с помощью закрытого ключа S260 и извлечение информационных данных S270.

На Фиг.9 изображена блок-схема, показывающая дешифрование ранее зашифрованных двумерных SAR-кодов. Используя камеру, устройство 13 предоставляет захваченные данные изображения 20 процессору 112 для хранения в памяти 114, 116 и/или обработки с помощью библиотеки ZXing или аналогичного средства; при этом процессор извлекает все фреймы 22 (набор двумерных кодов) из SAR-кода и преобразует их в зашифрованный набор данных:

$S=(S_0, S_1, S_2, \dots, S_{29})$.

Перед шифрованием номер фрейма удаляется из каждого элемента данных таким образом, что:

$S'=(S'_0, S'_1, S'_2, \dots, S'_{29})$

Данный набор заносится в память 114, 116 для дешифрования. Каждый зашифрованный элемент данных начинается с префиксного номера фрейма; поэтому средство обработки информации извлекает FN0 из S0' (данные первого фрейма) путем расшифровки 26 по стандарту AES-256 с помощью открытого ключа Ke. Когда S0' расшифровывается с помощью Ke, извлекается FN0. Далее, FN0 заносится в память 114, 116 для извлечения закрытого ключа и других номеров фреймов. Указанный закрытый ключ (K_{grv}) и набор указанных номеров фреймов, FN=(FN1, FN2, FN3 ..., FNk), извлекаются для дешифрования SFN0 (AES-256 with Ke key). Указанные K_{grv} и FN заносятся в память 114, 116 для дешифрования набора данных.

Перевод первоначального описания

Используя набор номеров фреймов (FN), средство обработки информации извлекает необходимые данные 28 из S '(SFN1', SFN2', SFN3', ..., SFNk'). Данные SFN1', SFN2', SFN3', ..., SFN1k' и они расшифровываются с помощью закрытого ключа по стандарту AES-256 (Kprv), таким образом при расшифровке с помощью закрытого ключа Kprv:

SFN1'=> SFN1d

SFN2'=> SFN2d

SFN3'=> SFN3d

...

SFNk'=> SFNkd

Из каждого элемента расшифрованных данных, средство обработки данных извлекает соответствующую информацию 32, например из:

SFN1d=> I1

SFN2d=> I2

SFN3d=> I3

...

SFNkd=> Ik

и, таким образом, что вся информация расшифровывается и извлекается из SAR-кода.

Если в настоящей заявке отсутствуют предварительные определения, используемые в ней понятия и выражения следует понимать в обычном смысле, придаваемом этим понятиям и выражениям применительно к соответствующим областям их употребления, за исключением, как указано выше, тех, которые определены выше. Относительные понятия, такие как выше, ниже, первый, второй и тому подобные, могут употребляться только для того, чтобы отличить один объект или действие от других, что никоим образом не подразумевает взаимосвязь и

Перевод первоначального описания

характер запросов между такими объектами или действиями. Понятия "*содержит*", "*включает*" "*состоит из*" или любые прочие их варианты предназначены для неэксклюзивного включения, так что процесс, способ, изделие, система, устройство или товар, включающий перечень элементов, включает в себя не только эти элементы, но также может включать другие элементы, которые явным образом не перечислены или присущи процессу, способу, изделию, системе, устройству или продукту. Краткое описание изобретения приведено для ознакомления читателя с технической сущностью изобретения, излагаемого в описании. Оно приводится с пониманием того, что оно не будет использоваться для толкования или ограничения объёма или смыслового значения формулы изобретения. Кроме того, в подробном описании возможно обнаружить несколько признаков, которые сгруппированы по различным вариантам осуществления изобретения, чтобы обеспечить правильное понимание того, что изложено в описании изобретения. Такой способ изложения сущности изобретения не должен быть истолкован как отражающий намерение авторов утверждать, что заявленные варианты осуществления изобретения требуют больше характеристик, чем те, которые явным образом указаны в каждом пункте формулы изобретения. С другой стороны, как следует из нижеследующей формулы изобретения, характеризующие настоящее изобретение признаки опираются на меньшее количество характеристик описанного в заявке варианта осуществления изобретения. Поэтому нижеследующие пункты формулы изобретения включены в подробное описание изобретения, при этом каждый пункт формулы приведен отдельно в качестве пункта формулы, в котором заявляется соответствующий объект изобретения. Несмотря на то, что некоторые аспекты заявленного изобретения были описаны в данной заявке в контексте устройства, представляется очевидным, что эти аспекты также представляют собой описание соответствующего способа, где узел или устройство соответствует этапу заявленного способа или характеристике этапа

Перевод первоначального описания

способа. Аналогично, аспекты заявленного изобретения, описанные в контексте этапа способа, представляют собой описание соответствующего или конкретного узла или элемента соответствующего устройства. В зависимости от характера определенных требований к реализации изобретения, варианты осуществления заявленного изобретения могут быть реализованы с использованием для этого соответствующего аппаратного или программного обеспечения. Изобретение может осуществляться с использованием электронных носителей цифровой информации, например с использованием гибких дисков, DVD дисков, компакт-дисков, ПЗУ, ППЗУ, стираемых ППЗУ, электрически стираемых программируемых ПЗУ либо с использованием флэш-памяти, содержащей сохраненные электронно-считываемые управляющие сигналы, которые взаимодействуют (или выполнены с возможностью взаимодействия) с компьютерной программируемой системой таким образом, что происходит реализация соответствующего способа. При этом, некоторые варианты осуществления настоящего изобретения включают носитель информации, характеризующийся наличием электронно-считываемых управляющих сигналов, которые способны взаимодействовать с компьютерной программируемой системой, например, для осуществления одного из описанных в настоящей заявке способов. В целом, варианты осуществления настоящего изобретения могут быть реализованы в виде компьютерного программного продукта с программным кодом, причем программный код является оперативным для реализации одного из способов, когда компьютерная программа выполняется на ЭВМ. Программный код может, например, храниться на машиночитаемом носителе информации. Несмотря на то, что вышеприведенное описание изобретения было составлено с приведением в нём наиболее доступных для понимания пояснений и/или других примеров, подразумевается, что различные модификации могут быть применимы или могут быть внесены в данное изобретение, и что описанный здесь объект изобретения

Перевод первоначального описания

может быть реализован в различных формах и вариантах, и что такие притязания заявителя могут быть реализованы в различных вариантах применения данного изобретения, некоторые из которых были описаны выше. Нижеследующая формула изобретения предназначена для охватывания любых и всевозможных вариантов применения заявляемого изобретения, его всевозможных модификаций и вариаций, которые подпадают под объём изложенных в заявке притязаний заявителя.

Формула изобретения

1. Способ передачи шифрованных данных от первого электронного устройства к второму электронному устройству, при этом каждое из указанных электронных устройств содержит по меньшей мере один интерфейс ввода/вывода, память и процессор, включающий:

отображение по меньшей мере первого зашифрованного двумерного кода на интерфейсе вывода первого электронного устройства;

считывание по меньшей мере первого двумерного кода, шифрованного при помощи интерфейса ввода второго электронного устройства, и расшифровка по меньшей мере одного первого двумерного кода при помощи процессора и памяти второго электронного устройства;

генерирование по меньшей мере одного второго зашифрованного двумерного кода при помощи процессора и памяти второго электронного устройства в ответ на первый расшифрованный двумерный код, и отображение по меньшей мере одного шифрованного двумерного кода на интерфейсе вывода второго электронного устройства;

считывание по меньшей мере одного второго шифрованного двумерного кода при помощи интерфейса ввода первого электронного устройства и расшифровка по меньшей мере второго двумерного кода при помощи процессора первого электронного устройства; и

генерирование действия на первом электронном устройстве на основании второго расшифрованного двумерного кода.

2. Способ по п.1, в котором указанный по меньшей мере один второй двумерный код представляет собой группу двумерных кодов, отображаемых в безопасном видеоформате анимированного отклика с частотой по меньшей мере 1

Перевод первоначальной формулы изобретения

раз в 70 мс, предпочтительно 1 двумерный код каждые 40 мс, и в котором по меньшей мере второй двумерный код не хранится на втором мобильном устройстве,

причём указанные электронные устройства не имеют активного сетевого подключения и/или указанные электронные устройства не имеют между собой активного соединения.

3. Способ по п.1, в котором генерирование по меньшей мере одного первого кода или по меньшей мере второго зашифрованного двумерного кода включает:

генерирование передаваемого набора данных, включающего первый набор данных и второй набор данных со строкой символов, при этом первый и второй наборы данных включают фрейм со случайным и не дублирующимся номером фрейма и ключ для шифрования данных из другого набора данных, причём передаваемый набор данных дополнительно включает номер фрейма и случайную строку,

шифрование передаваемого набора данных с помощью первого открытого ключа и шифрование вторых данных из передаваемого набора данных с помощью второго закрытого ключа, и

создание помеченного зашифрованного набора данных и преобразование указанного помеченного зашифрованного набора данных в считываемый процессором набор графических элементов;

причём расшифровка по меньшей мере одного первого кода или по меньшей мере второго зашифрованного двумерного кода включает:

извлечение всех фреймов из переданного двумерного кода и удаление номера фрейма из каждого набора данных;

преобразование указанных фреймов в зашифрованный набор данных и расшифровка данных фреймов с помощью открытого ключа;

Перевод первоначальной формулы изобретения

извлечение закрытого ключа и набора номеров фреймов, расшифровка наборов данных с помощью закрытого ключа и извлечение информационных данных;

при этом указанный набор данных включает в себя идентификационные данные события, название и уникальный код.

4. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает:

проверка достоверности данных о событиях и привилегиях, полученных в первом двумерном коде на втором мобильном устройстве;

проверка правильности времени ввода в случае, если данные о событии и привилегии являются правильными на втором мобильном устройстве;

размещение второго мобильного устройства в очереди, генерирование двумерного кода на первом мобильном устройстве, который считывается интерфейсом ввода второго мобильного устройства;

генерирование второго двумерного кода в случае, если событие и привилегия, а также время входа, были проверены как правильные во втором мобильном устройстве; и

прекращение доступа на втором мобильном устройстве.

5. Способ по п. 4, дополнительно включающий:

проверку наличия обновлений, если данные о событии и привилегии не достоверны на втором мобильном устройстве;

использование баланса для подтверждения события и привилегий в случае, если обновления доступны на втором мобильном устройстве; и

Перевод первоначальной формулы изобретения

сохранение напоминания и ключа на втором мобильном устройстве.

6. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает:

редактирование и выбор персональной информации для обмена в случае, если пользователь хочет поделиться персональной информацией на втором мобильном устройстве;

генерирование второго двумерного кода по завершении редактирования и выбора информации для совместного использования на втором мобильном устройстве;

разрешение доступа к данным и создание профиля на первом мобильном устройстве.

7. Способ по п.1, в котором первое мобильное устройство соответствует пользователю, а второе мобильное устройство соответствует оператору, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает:

проверку соответствия идентификатора события событию во втором мобильном устройстве;

выбор суммы средств для обновления с генерированием таким образом второго двумерного кода;

создание транзакции на втором мобильном устройстве; и

изменение указанного количественного параметра, определённого на первом мобильном устройстве.

Перевод первоначальной формулы изобретения

8. Способ по п.1, в котором первое мобильное устройство соответствует пользователю, а второе мобильное устройство соответствует оператору, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает:

проверку соответствия идентификатора события событию во втором мобильном устройстве;

выбор заказов и/или товаров;

проверку баланса на первом мобильном устройстве, и при соответствии баланса, генерирование затем второго двумерного кода;

уменьшение суммы средств на первом мобильном устройстве; и

создание транзакции посредством считывания другого двумерного кода на втором мобильном устройстве.

9. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает:

проверку соответствия идентификатора события событию и наличия баланса на втором мобильном устройстве, генерируя таким образом второй двумерный код, если подтверждено соответствие идентификатора события событию и наличие баланса на втором мобильном устройстве;

списание суммы средств на втором мобильном устройстве;

выбор метода возврата денежных средств на первом мобильном устройстве; и

создание транзакции на первом мобильном устройстве.

Перевод первоначальной формулы изобретения

10. Способ по п.1, в котором первое мобильное устройство соответствует пользователю, а второе мобильное устройство соответствует оператору, дополнительно включающий:

привязку карты к первому мобильному устройству, при этом данные, привязанные к карте, включают персональный идентификационный код (ПИН-код);

причём считывание и расшифровка по крайней мере первого двумерного кода с помощью процессора и памяти второго электронного устройства или считывание и расшифровка по крайней мере второго двумерного кода с помощью процессора и памяти первого электронного устройства включает:

выбор заказов/товаров на втором электронном устройстве, таким образом, генерируя второй двумерный код на втором электронном устройстве;

генерирование нового двумерного кода и сохранение запроса на транзакцию на первом электронном устройстве;

считывание и расшифровка нового двумерного кода на втором электронном устройстве;

проверку достоверности данных и создание транзакции в случае, если данные достоверны на втором электронном устройстве; и

получение заказов/товаров в случае, если транзакция создана на втором электронном устройстве или путем сохранения запроса на транзакцию в первом электронном устройстве.

11. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю, в котором считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти первого электронного устройства дополнительно включает:

проверку достоверности двумерного кода с помощью карты,

Перевод первоначальной формулы изобретения

предъявляемой пользователем оператору;

проверку подлинности карты пользователя;

генерирование второго двумерного кода на втором мобильном устройстве и проверка подлинности карты на втором мобильном устройстве; и

считывание второго двумерного кода на первом мобильном устройстве и получение результатов проверки подлинности карты на первом мобильном устройстве.

12. Способ по п.1, в котором первое мобильное устройство соответствует пользователю, а второе мобильное устройство соответствует оператору, метод дополнительно включает:

обновление документа;

при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти первого электронного устройства дополнительно включает:

аутентификацию карты на основе карты пользователя;

генерирование второго двумерного кода на первом мобильном устройстве;

определение на первом мобильном устройстве, готов ли документ к заверению электронной подписью;

генерирование на втором мобильном устройстве третьего двумерного кода, если документ готов к заверению электронной подписью, и определение необходимости добавления другого пользователя или свидетеля к документу; и

аутентификация, на втором мобильном устройстве, документа, включающего второй и третий двумерные коды.

13. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует

Перевод первоначальной формулы изобретения

пользователю, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти первого электронного устройства дополнительно включает:

определение того, был ли документ подписан пользователем;

если документ не был подписан пользователем, определение наличия у пользователя действительной карты;

если документ был подписан пользователем или если пользователь имеет действительную карту, генерирование второго двумерного кода на первом мобильном устройстве;

получение ключа на втором мобильном устройстве; и

открытие аутентифицированного документа с помощью ключа доступа на втором мобильном устройстве.

14. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю, при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти первого электронного устройства дополнительно включает:

определение наличия у пользователя действительной карты;

генерирование второго двумерного кода на первом мобильном устройстве, если установлено, что карта пользователя действительна;

получение ключа на втором мобильном устройстве и сканирование другого двумерного кода, отображаемого на шлюзе;

определение на втором мобильном устройстве, имеет ли пользователь правильный ключ, и генерирование третьего двумерного кода на втором мобильном устройстве, если ключ определен как правильный; и

отображение третьего двумерного кода на шлюзе и открытие шлюза с

Перевод первоначальной формулы изобретения

учетом третьего двумерного кода.

15. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю, дополнительно включающий:

привязку карты и обновление информации при помощи второго мобильного устройства;

при этом считывание и расшифровка по меньшей мере первого двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает в себя:

определение наличия баланса на карте;

определение наличия у карты кредитного лимита;

определение метода оплаты;

уменьшение суммы средств на первом мобильном устройстве;

определение наличия сигнала данных и обработку платежа в связи с сигналом данных; и

при этом считывание и расшифровка по меньшей мере второго двумерного кода с помощью процессора и памяти первого электронного устройства дополнительно включает в себя:

создание транзакции; и

при этом путем определения наличия сигнала данных во втором электронном устройстве определяется наличие сигнала данных в первом электронном устройстве.

16. Способ по п.1, в котором первое мобильное устройство соответствует оператору, а второе мобильное устройство соответствует пользователю,

при этом считывание и расшифровка по меньшей мере первого

Перевод первоначальной формулы изобретения

двумерного кода с помощью процессора и памяти второго электронного устройства дополнительно включает в себя:

определение правильности приложения и правильности генерирования второго двумерного кода; и

при этом чтение и расшифровка по меньшей мере второго двумерного кода с помощью процессора и памяти первого электронного устройства дополнительно включает в себя:

определение наличия сигнала данных, а при наличии сигнала данных обработку логина для входа в систему или запуск устройства с загрузкой данных, соответствующих второму мобильному устройству, с использованием сигнала данных.

17. Система для передачи зашифрованных данных между электронными устройствами, содержащая:

первое электронное устройство с интерфейсом ввода/вывода, памятью и процессором;

второе электронное устройство с интерфейсом ввода/вывода, памятью и процессором;

причём указанные устройства выполнены с возможностью:

отображения по меньшей мере одного первого зашифрованного двумерного кода на выходном интерфейсе первого электронного устройства;

считывания по меньшей мере одного первого двумерного кода с входного интерфейса второго электронного устройства и расшифровки по меньшей мере одного первого двумерного кода с помощью процессора и памяти второго электронного устройства;

генерирования по меньшей мере одного второго двумерного кода, зашифрованного с помощью процессора и памяти второго электронного устройства в

Перевод первоначальной формулы изобретения

ответ на расшифровку первого двумерного кода, и отображения по меньшей мере одного второго двумерного кода на выходном интерфейсе второго электронного устройства; и

считывания по меньшей мере одного второго двумерного кода с помощью интерфейса ввода первого электронного устройства и расшифровки по меньшей мере одного второго двумерного кода с помощью процессора первого электронного устройства.

18. Система по п.14, в которой указанный по меньшей мере по меньшей мере второй двумерный код представляет собой группу двумерных кодов, отображаемых в защищенном видеоформате анимированного отклика с частотой по меньшей мере 1 двумерный код в 70 мс, предпочтительно 1 двумерный код каждые 40 мс, при этом по меньшей мере второй двумерный код не хранится во втором мобильном устройстве и указанные электронные устройства не имеют активного сетевого подключения и/или активного соединения между ними.

19. Машиночитаемый энергонезависимый носитель информации для реализации способа по п.1 для передачи шифрованных данных от первого электронного устройства к второму электронному устройству.

20. Способ обработки шифрованных данных в первом электронном устройстве, содержащем по меньшей мере один интерфейс ввода/вывода, память и процессор, включающий:

генерирование по меньшей мере одного кода в первом электронном устройстве в ответ на информацию, полученную от первого электронного устройства и оператора;

проверка баланса с первого электронного устройства, и в ответ на подтверждение достаточного баланса:

генерирование по меньшей мере одного шифрованного двумерного

Перевод первоначальной формулы изобретения

кода с помощью процессора и памяти первого электронного устройства в ответ на успешную проверку баланса, и отображение по меньшей мере одного зашифрованного двумерного кода на интерфейсе вывода первого электронного устройства;

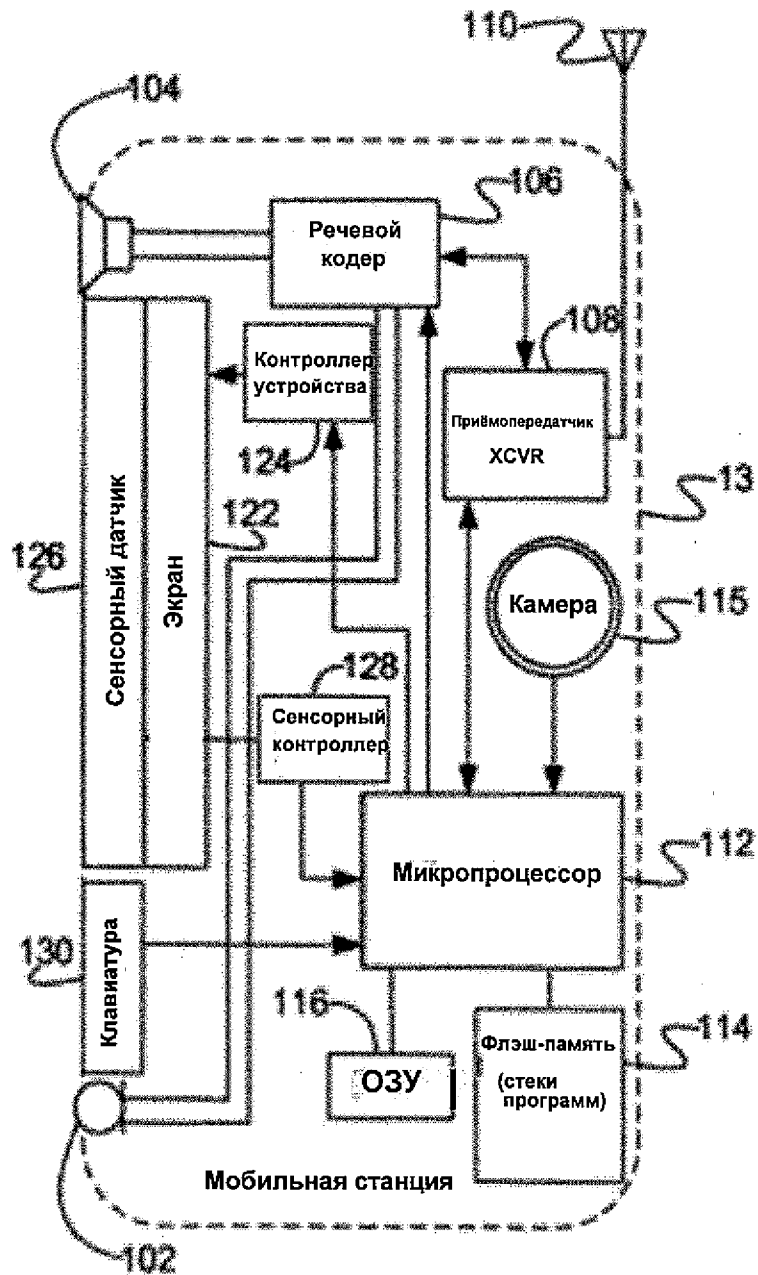
получение подтверждения по меньшей мере одного зашифрованного двумерного кода от оператора;

генерирование действия оператором на основе проверки по меньшей мере одного подтвержденного двумерного кода; и

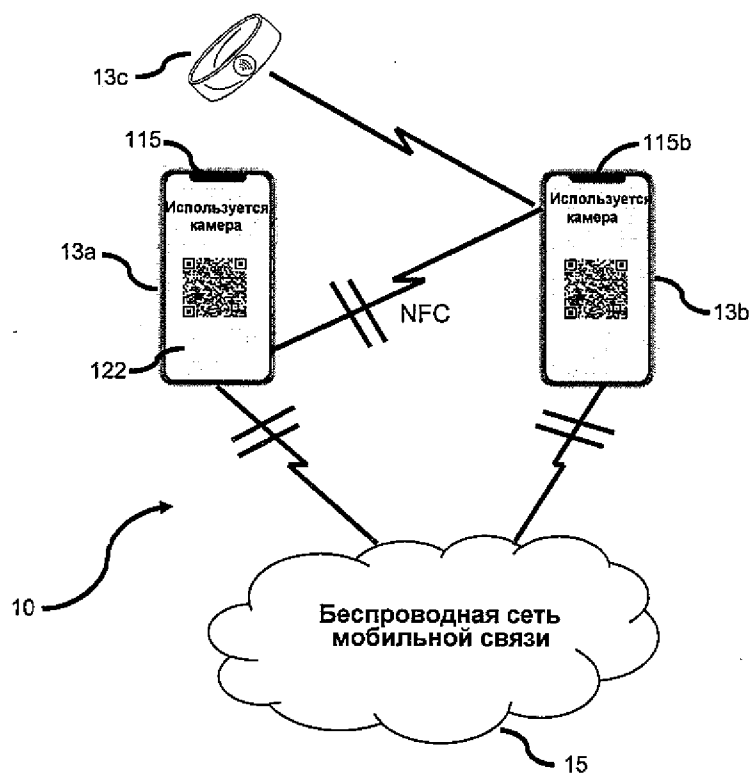
уменьшение баланса первого электронного устройства на сумму средств по указанному действию;

причём первое электронное устройство не имеет активного сетевого подключения.

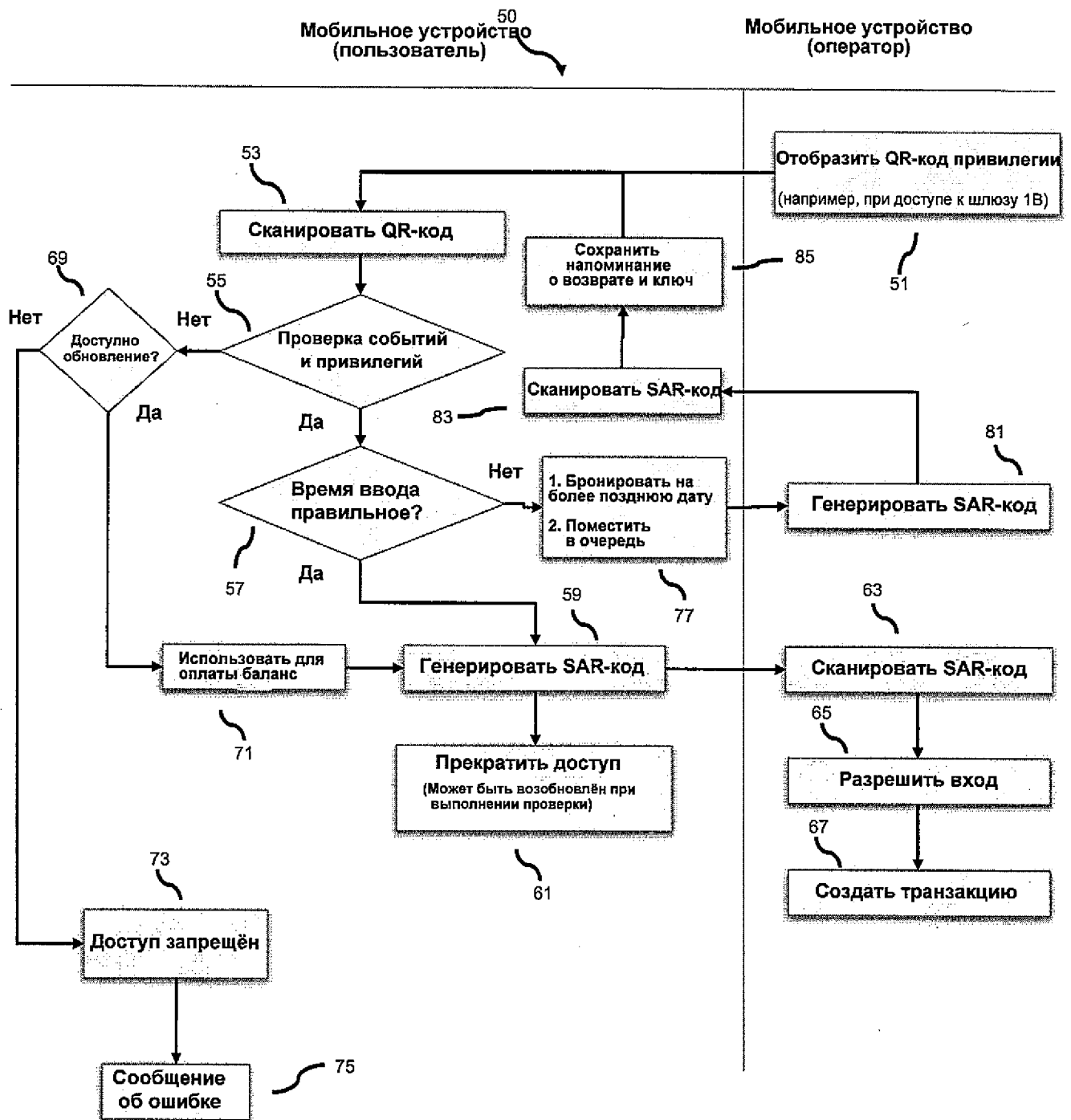
Перевод первоначальной формулы изобретения



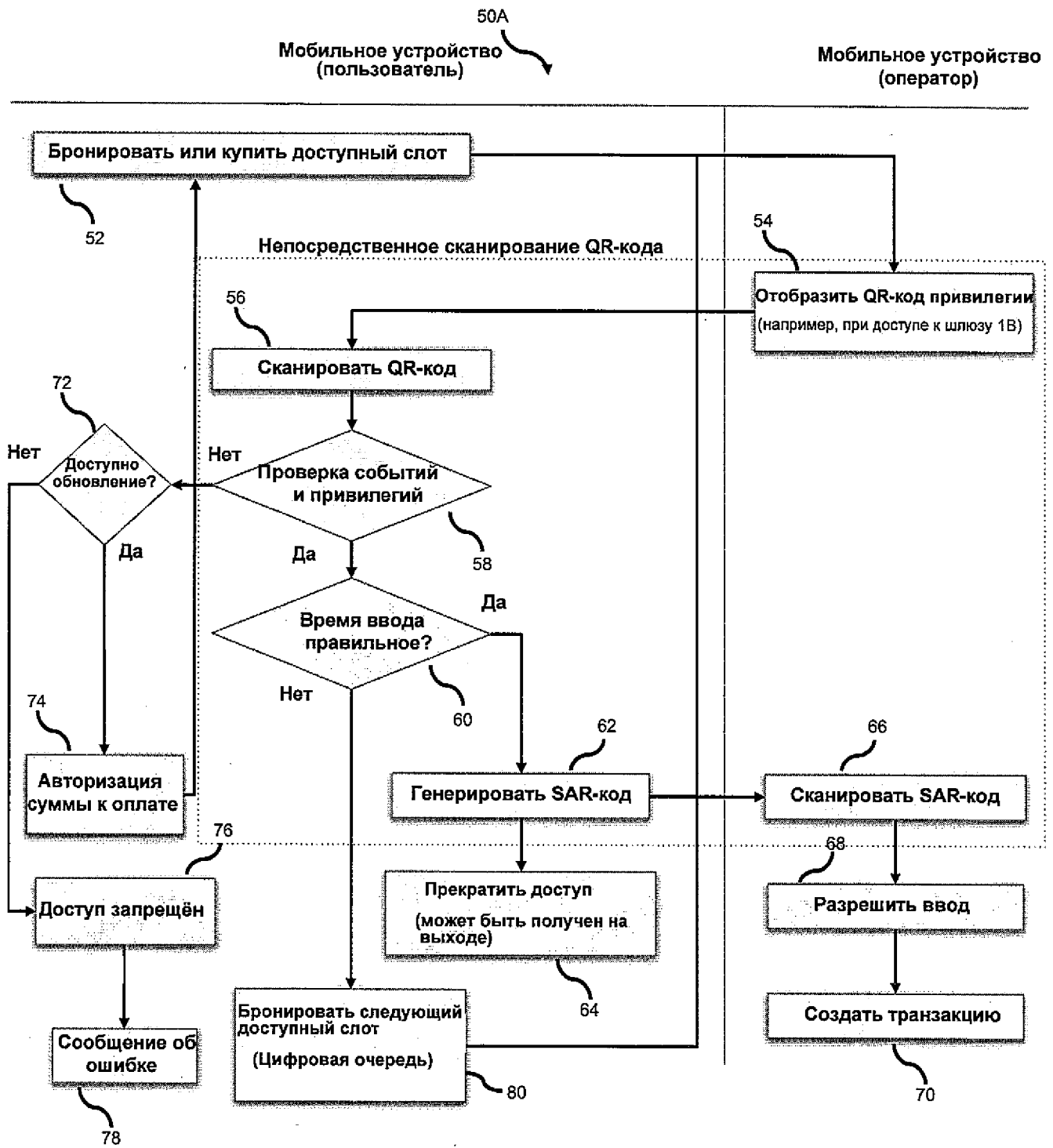
Фиг.1



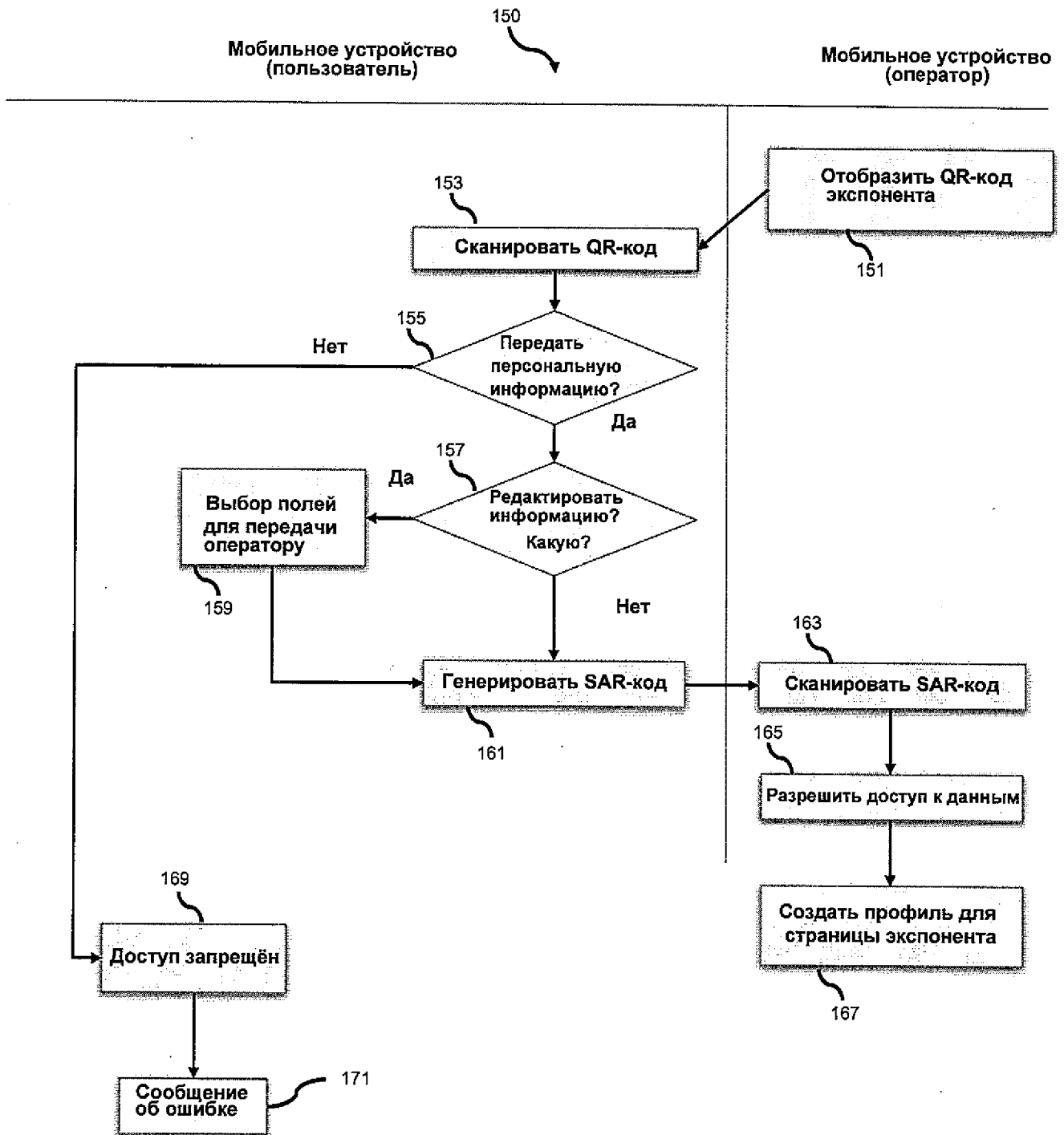
Фиг.2



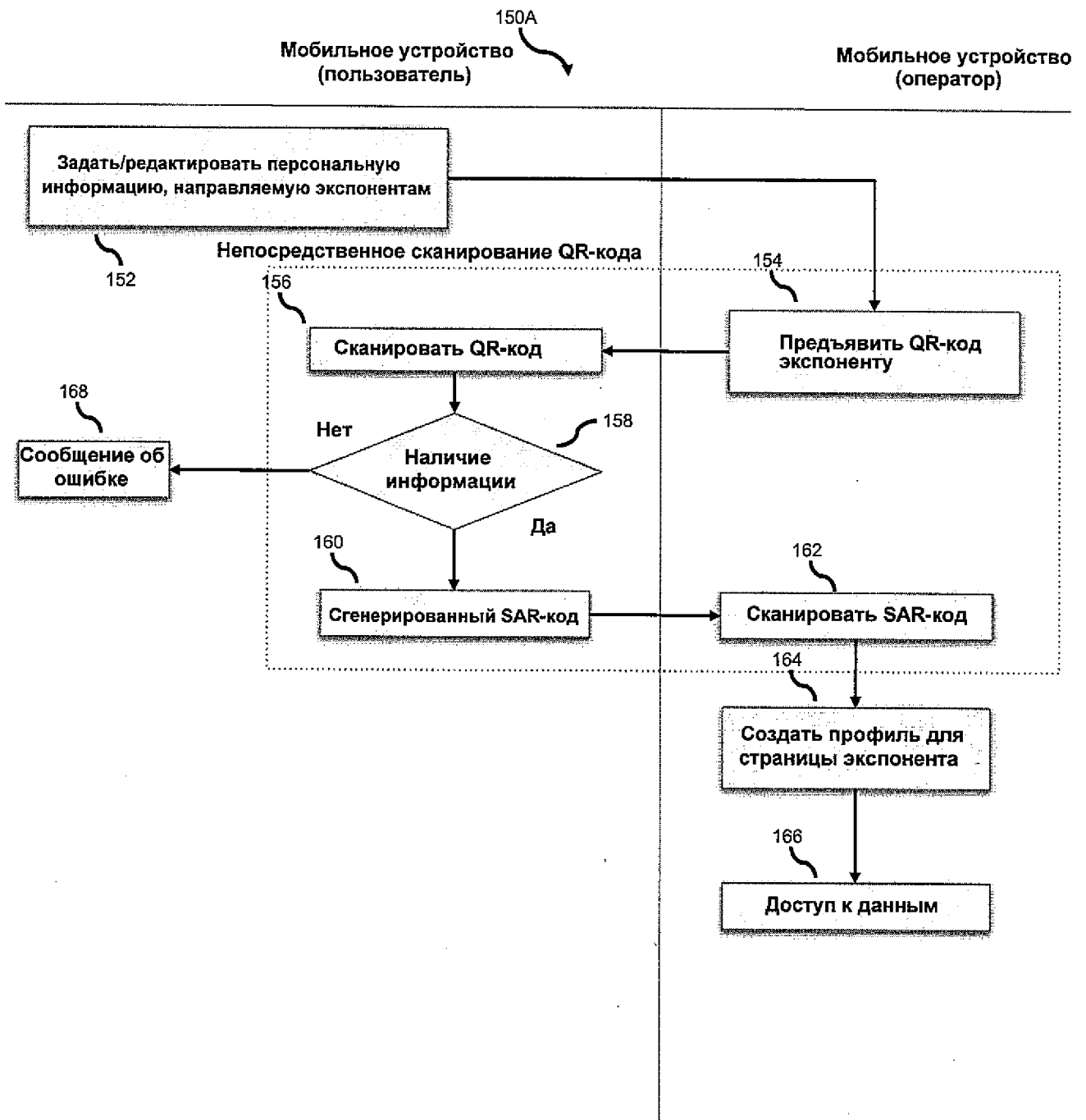
Фиг.3



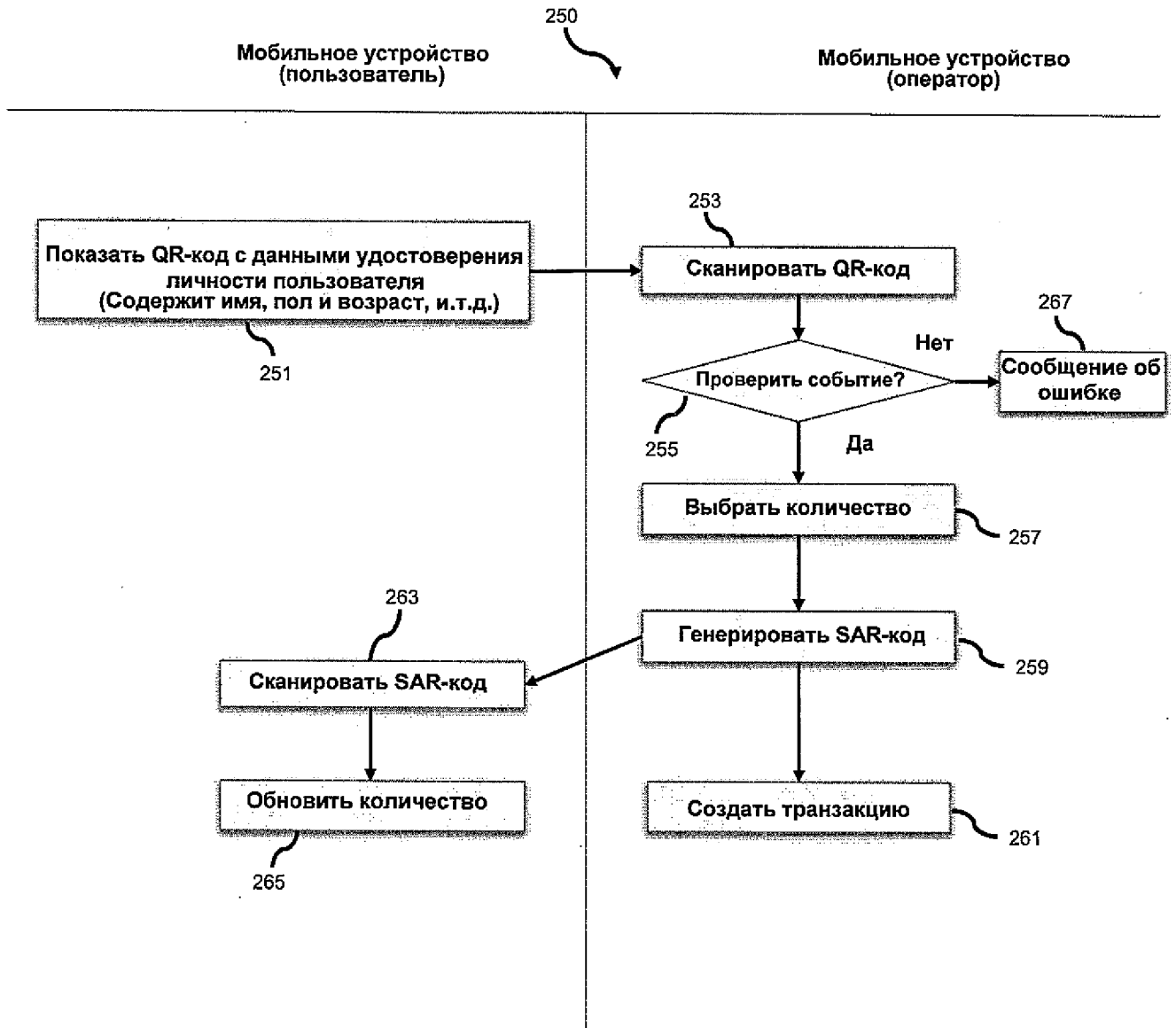
Фиг.3А



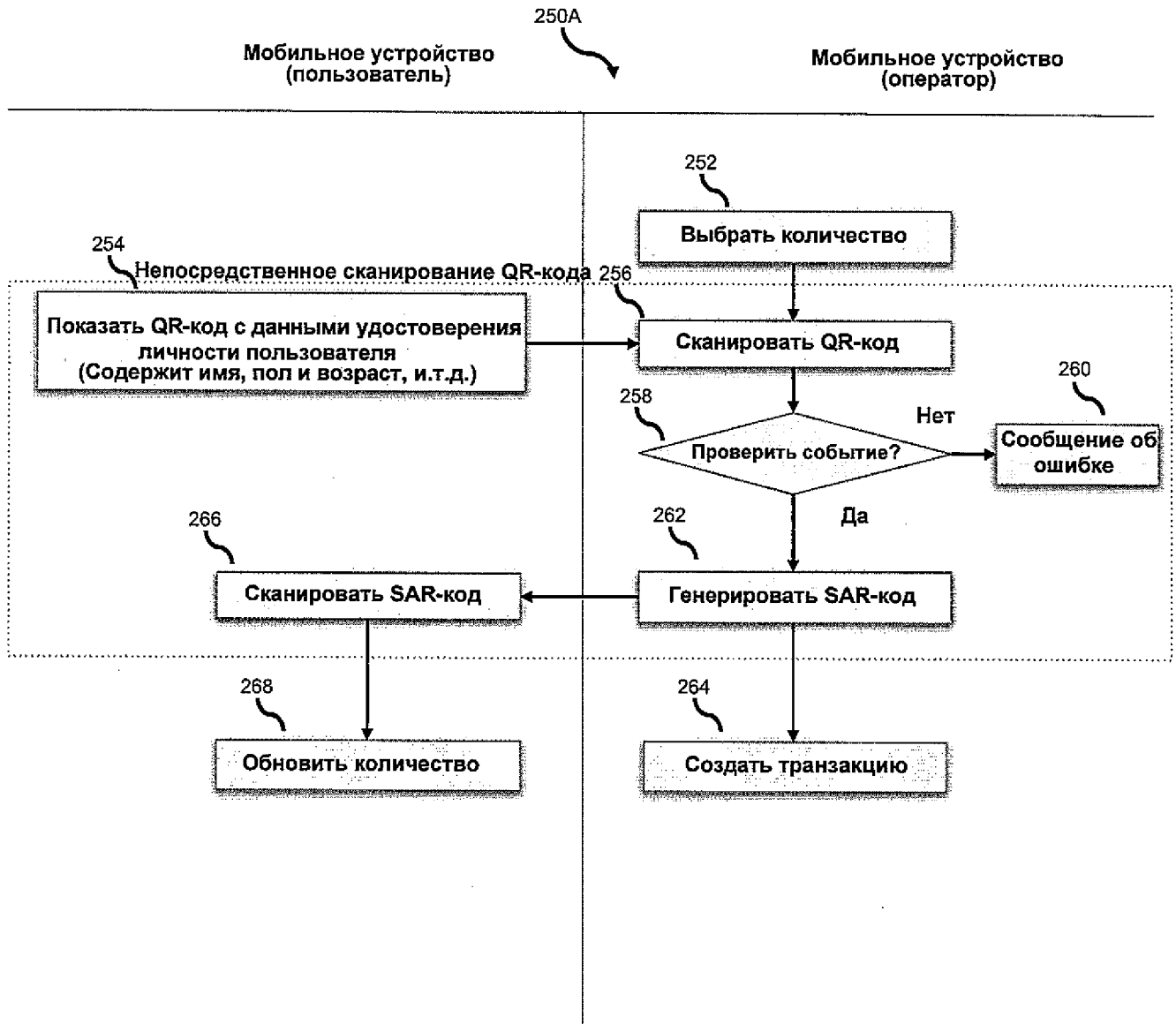
Фиг.4



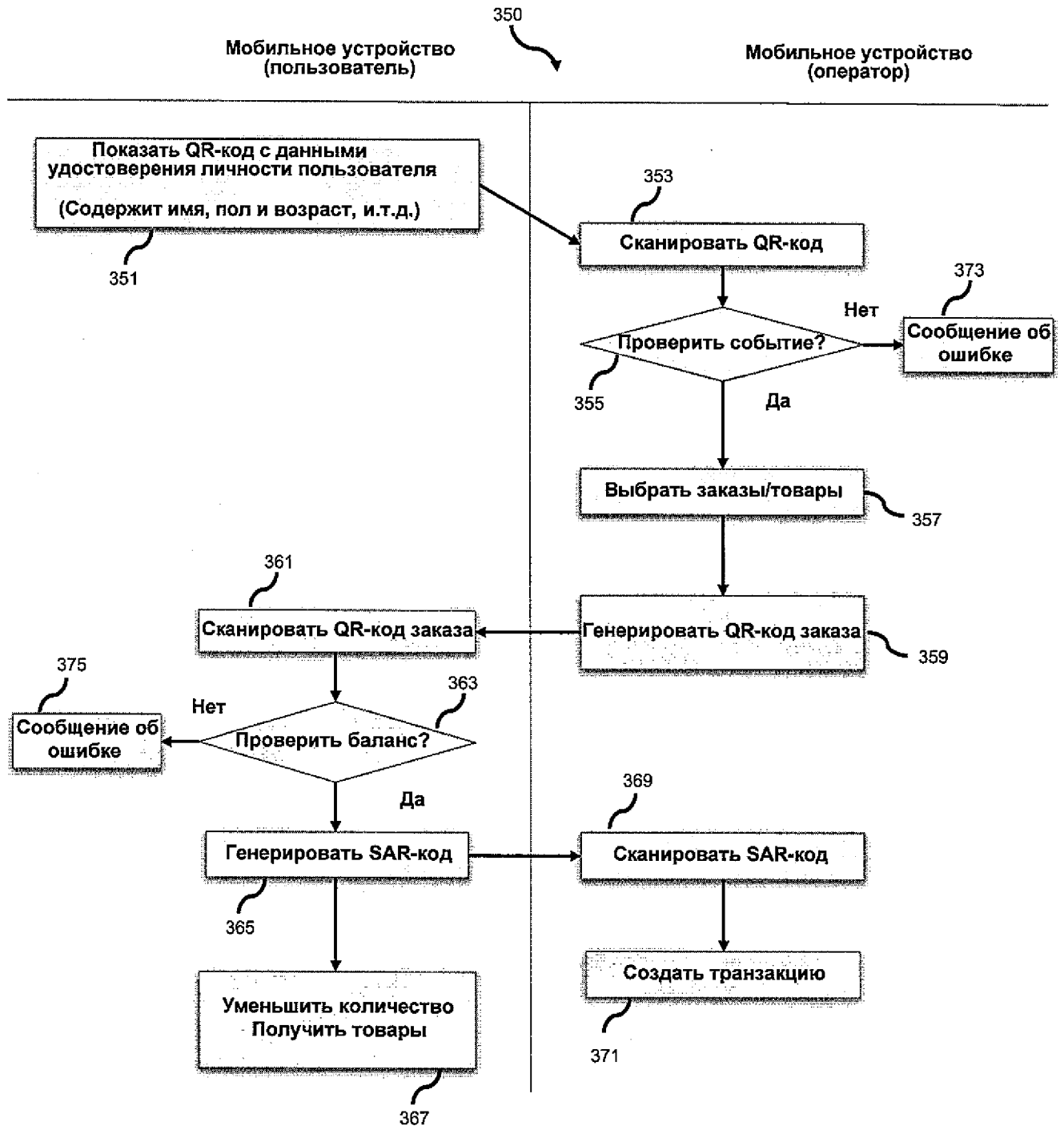
Фиг.4А



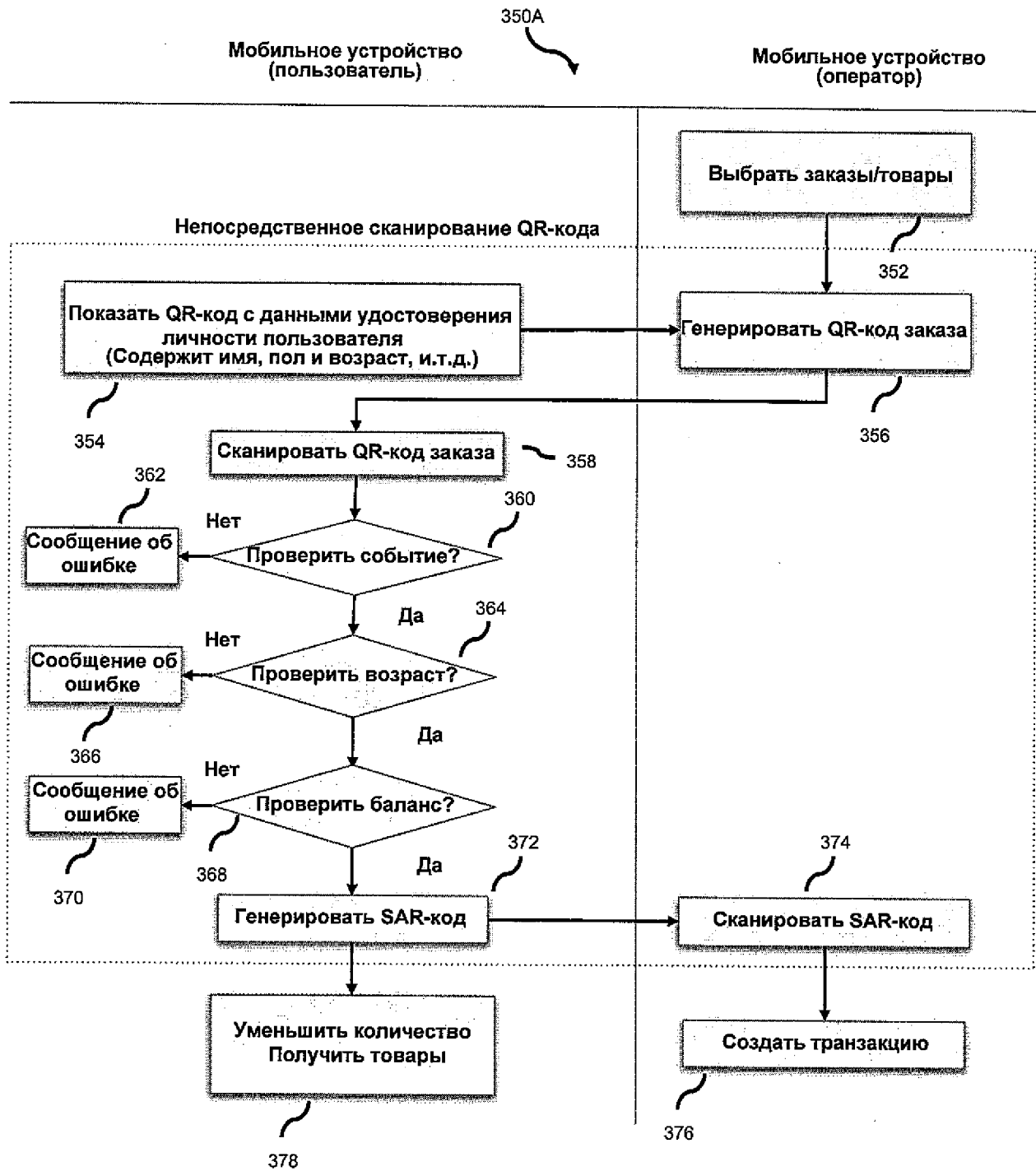
Фиг.5



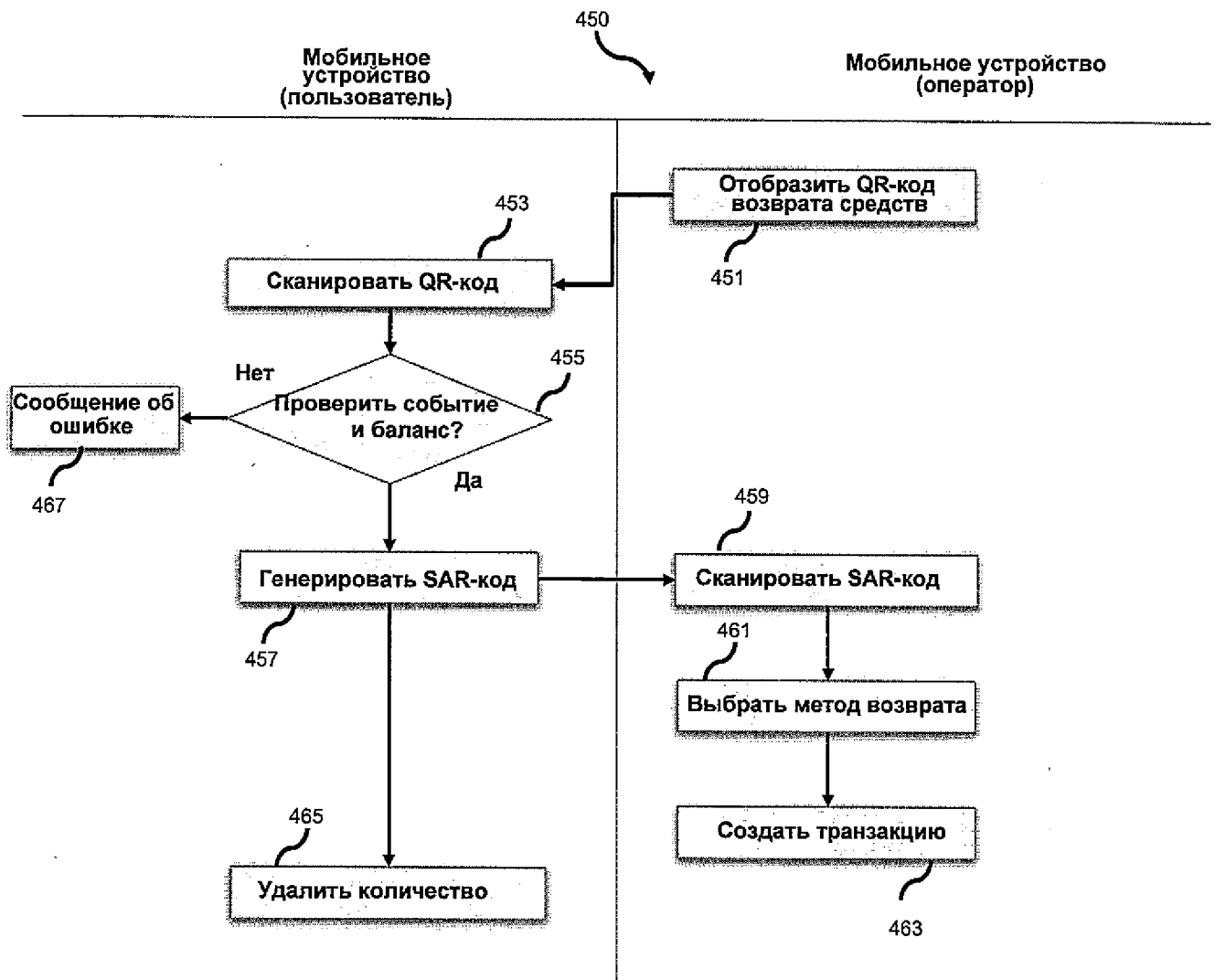
Фиг.5А



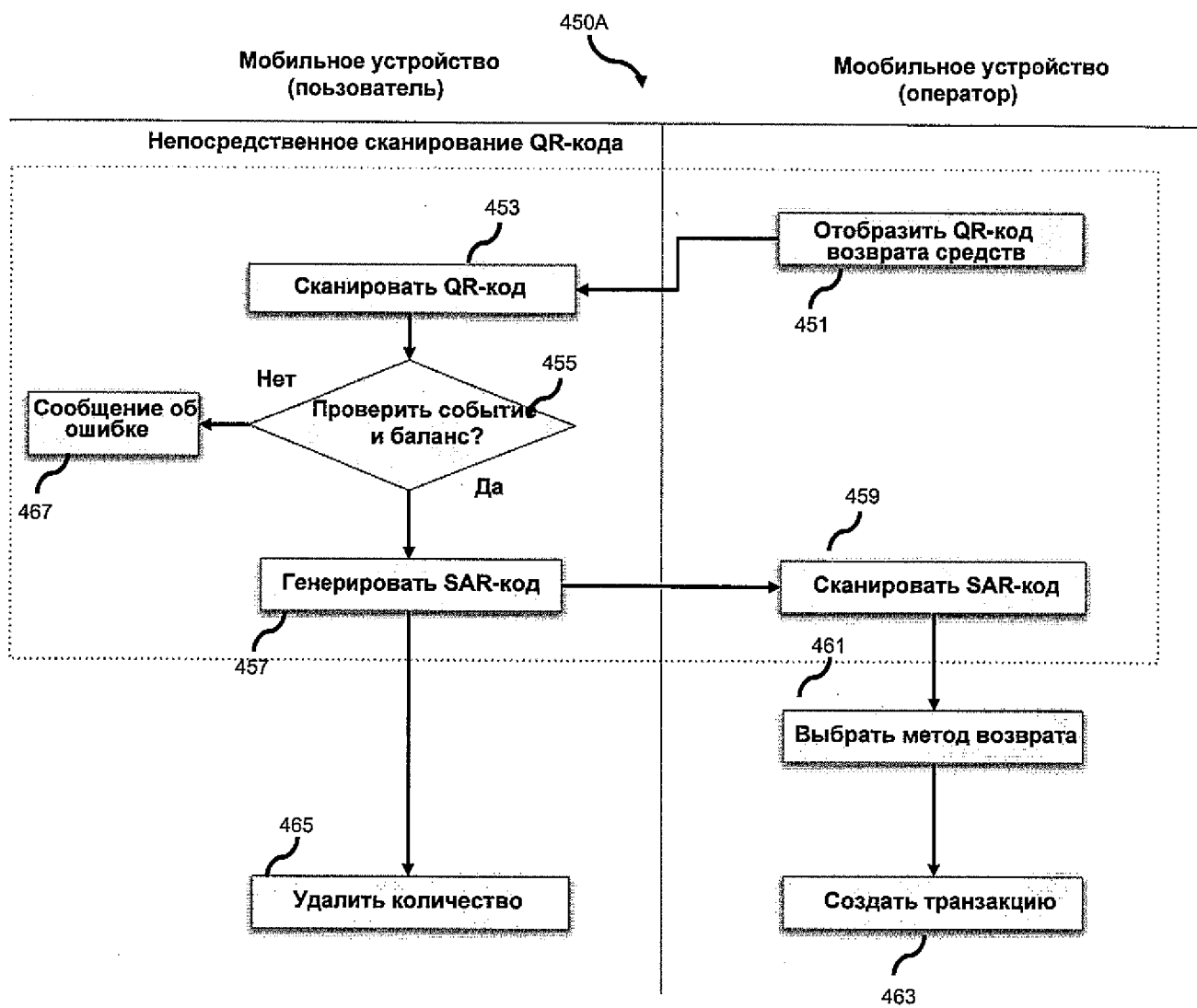
Фиг.6



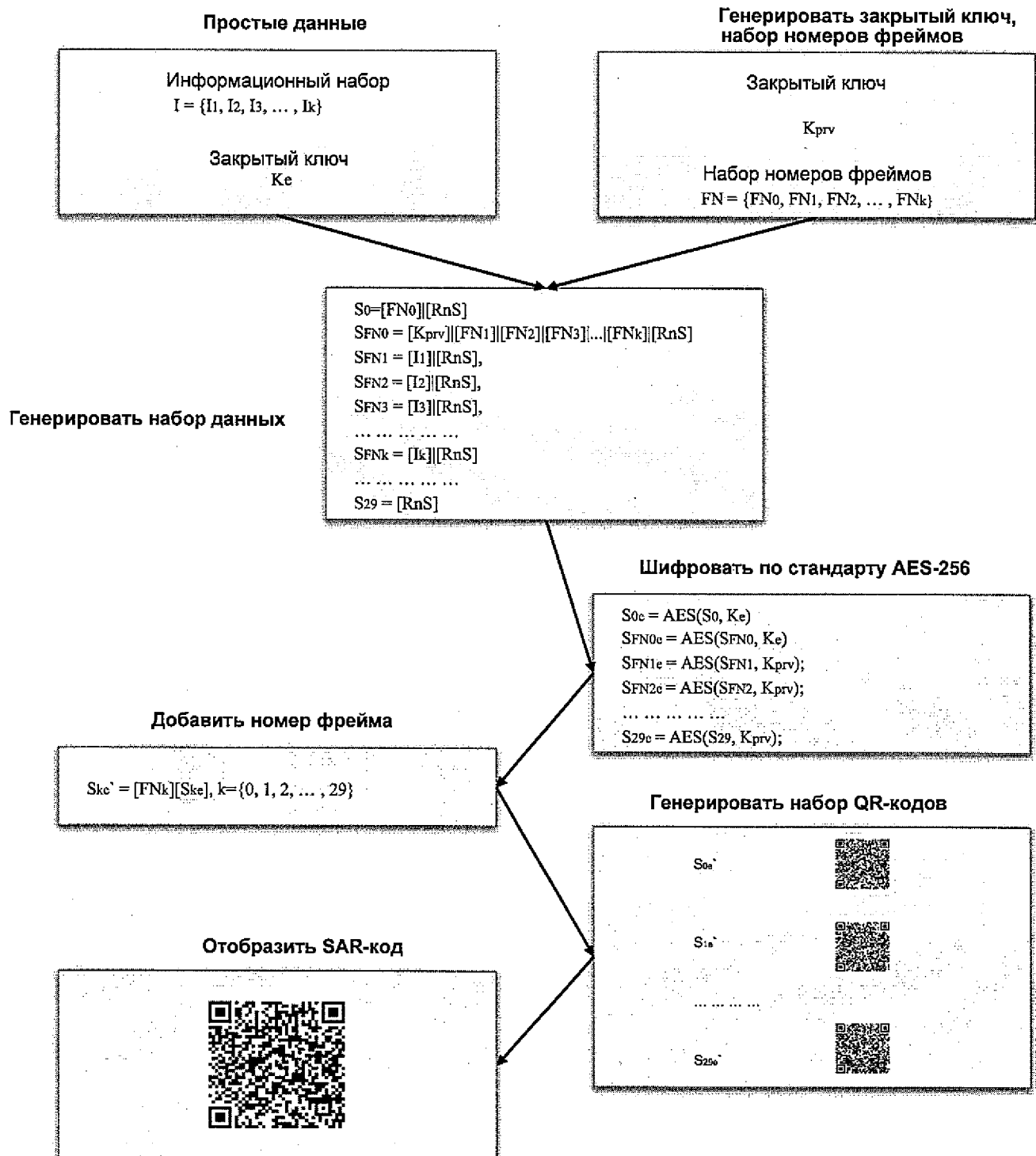
Фиг.6А



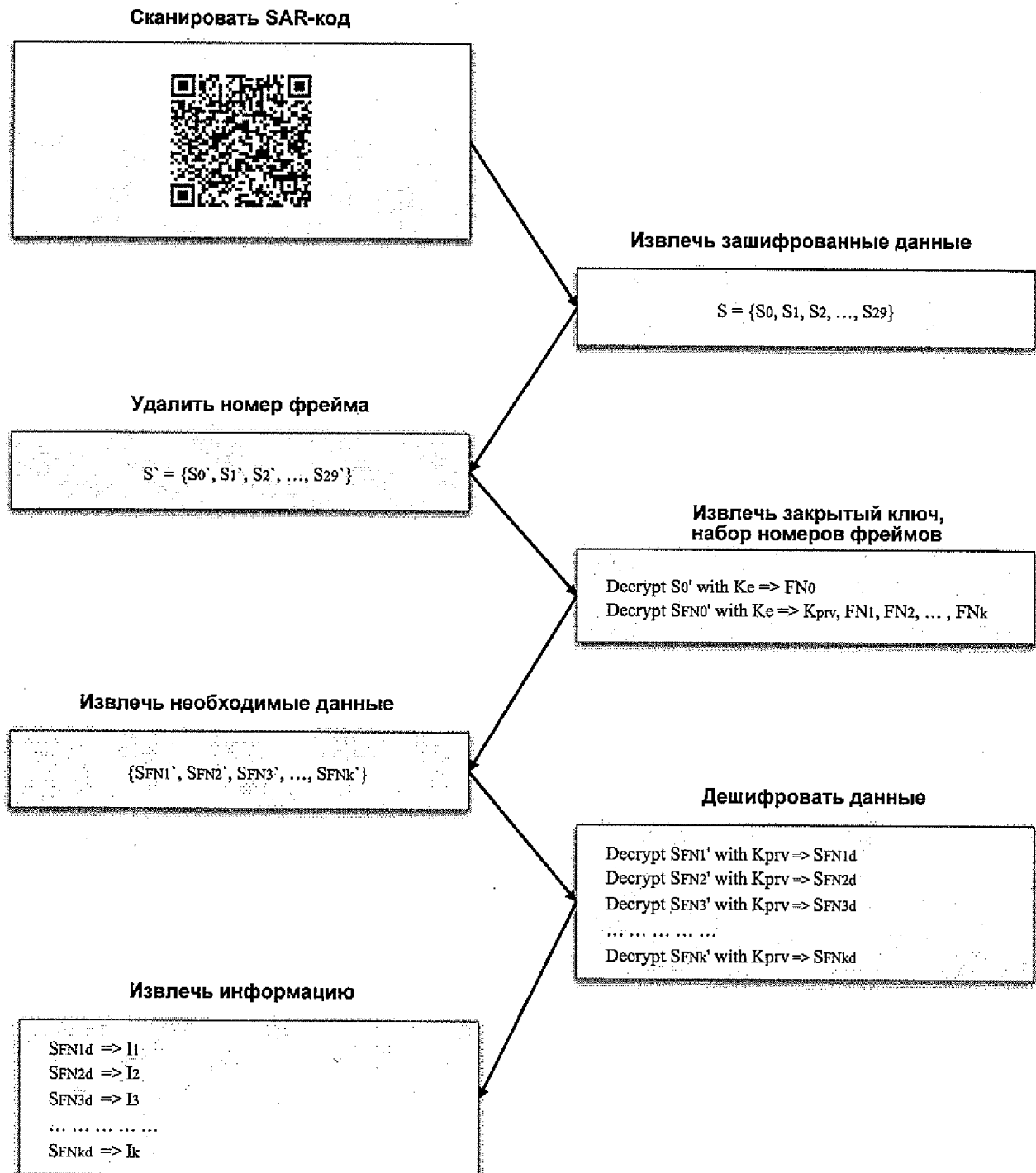
Фиг.7



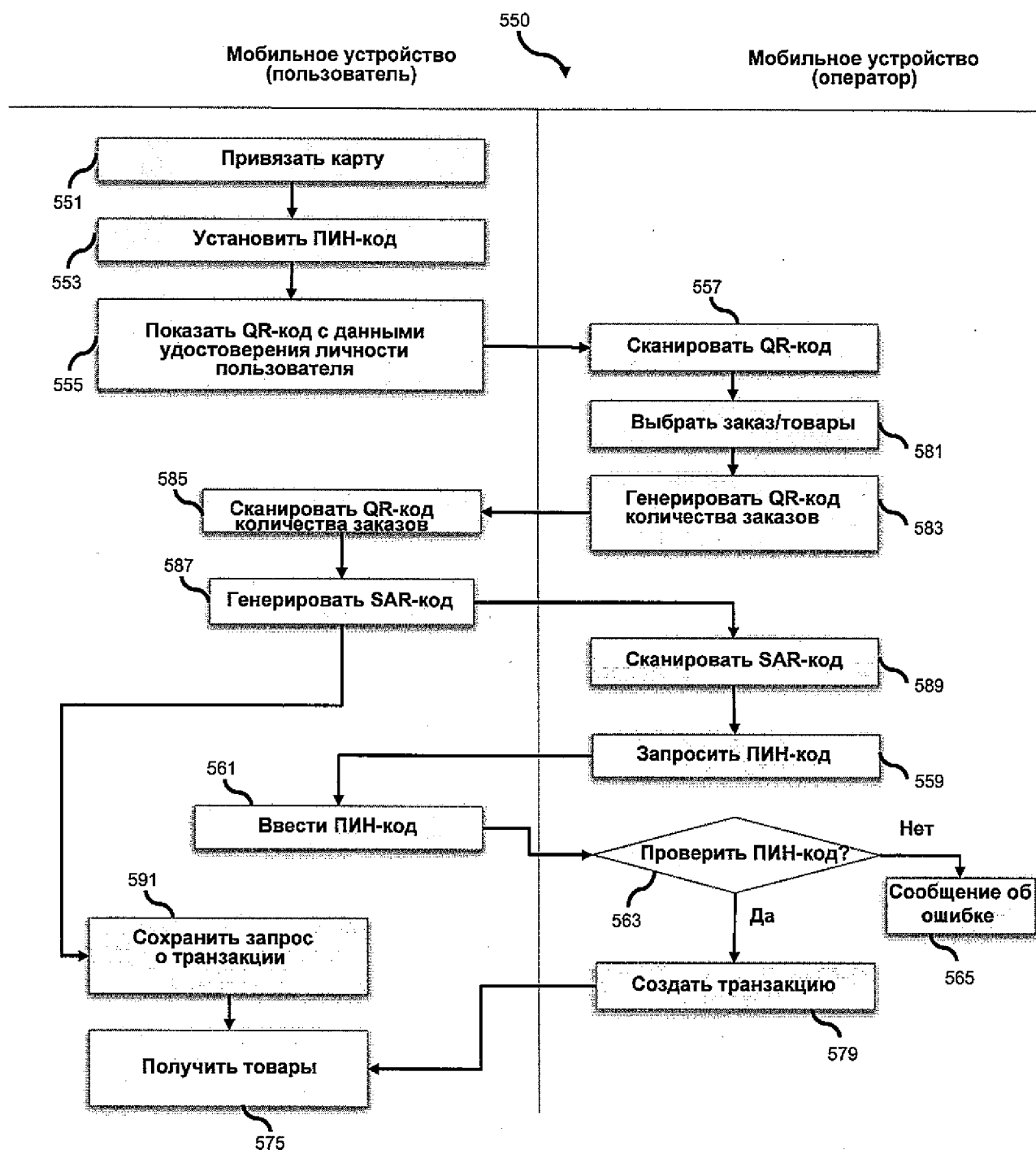
Фиг.7А



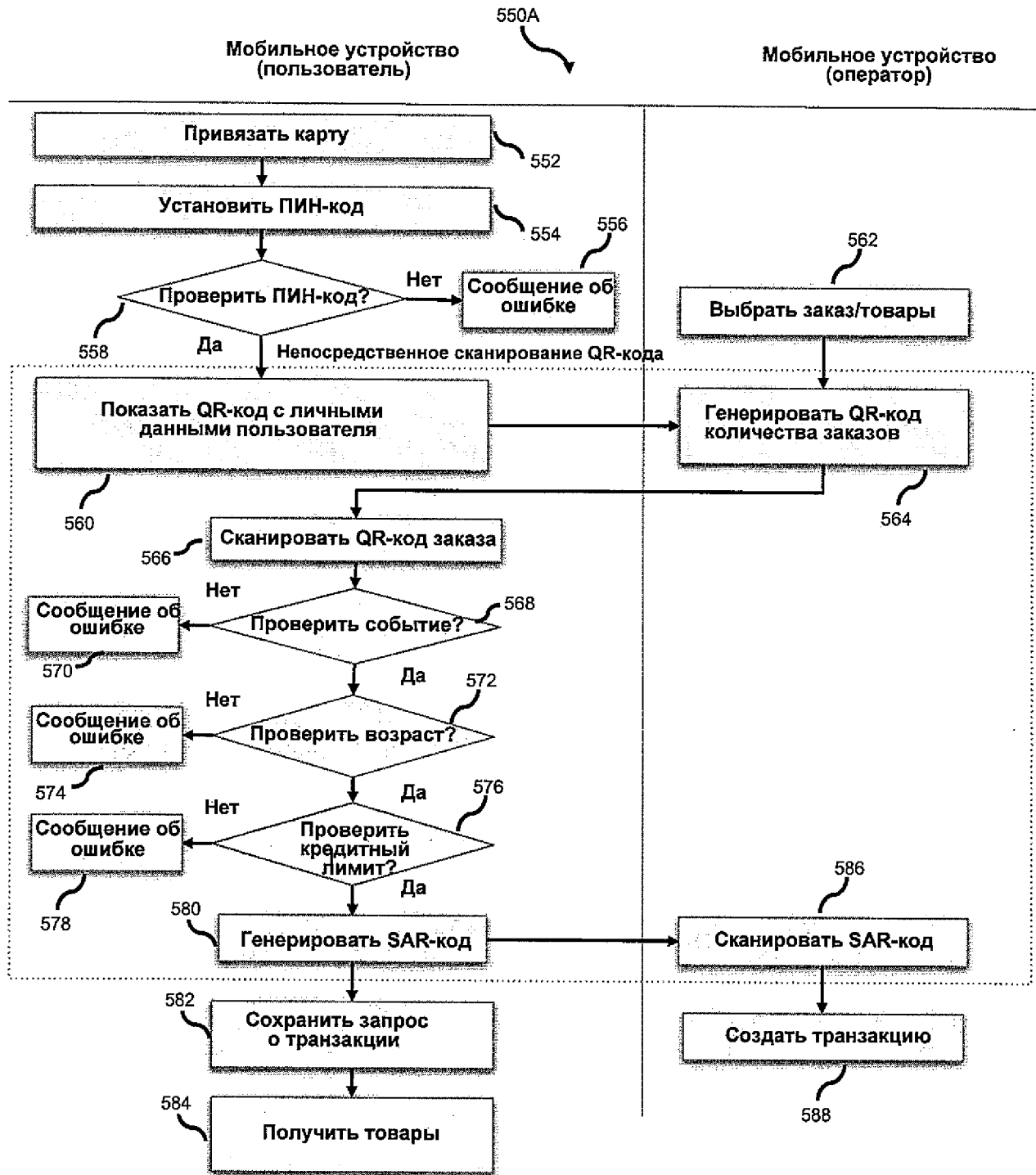
Фиг.8



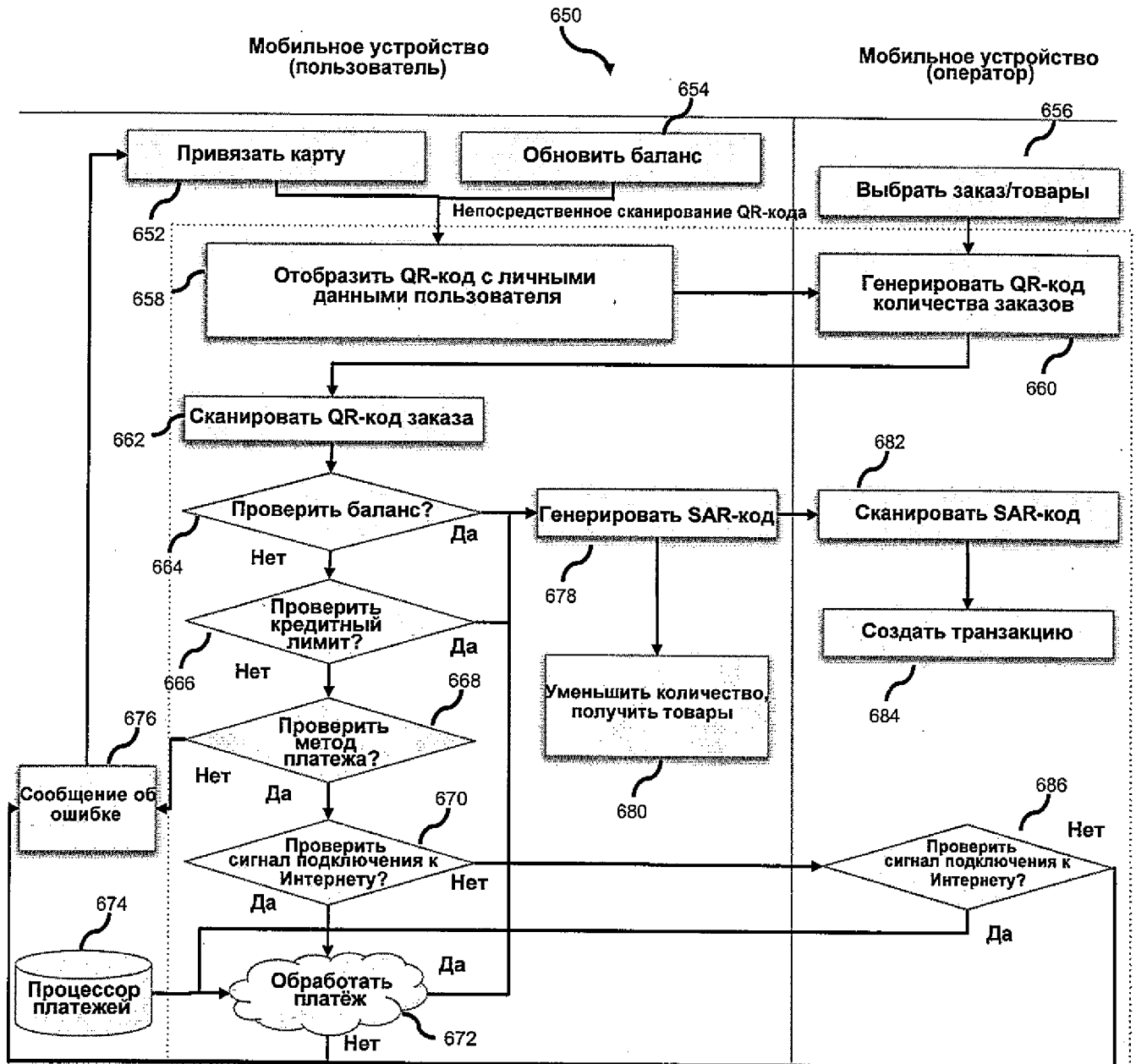
Фиг.9



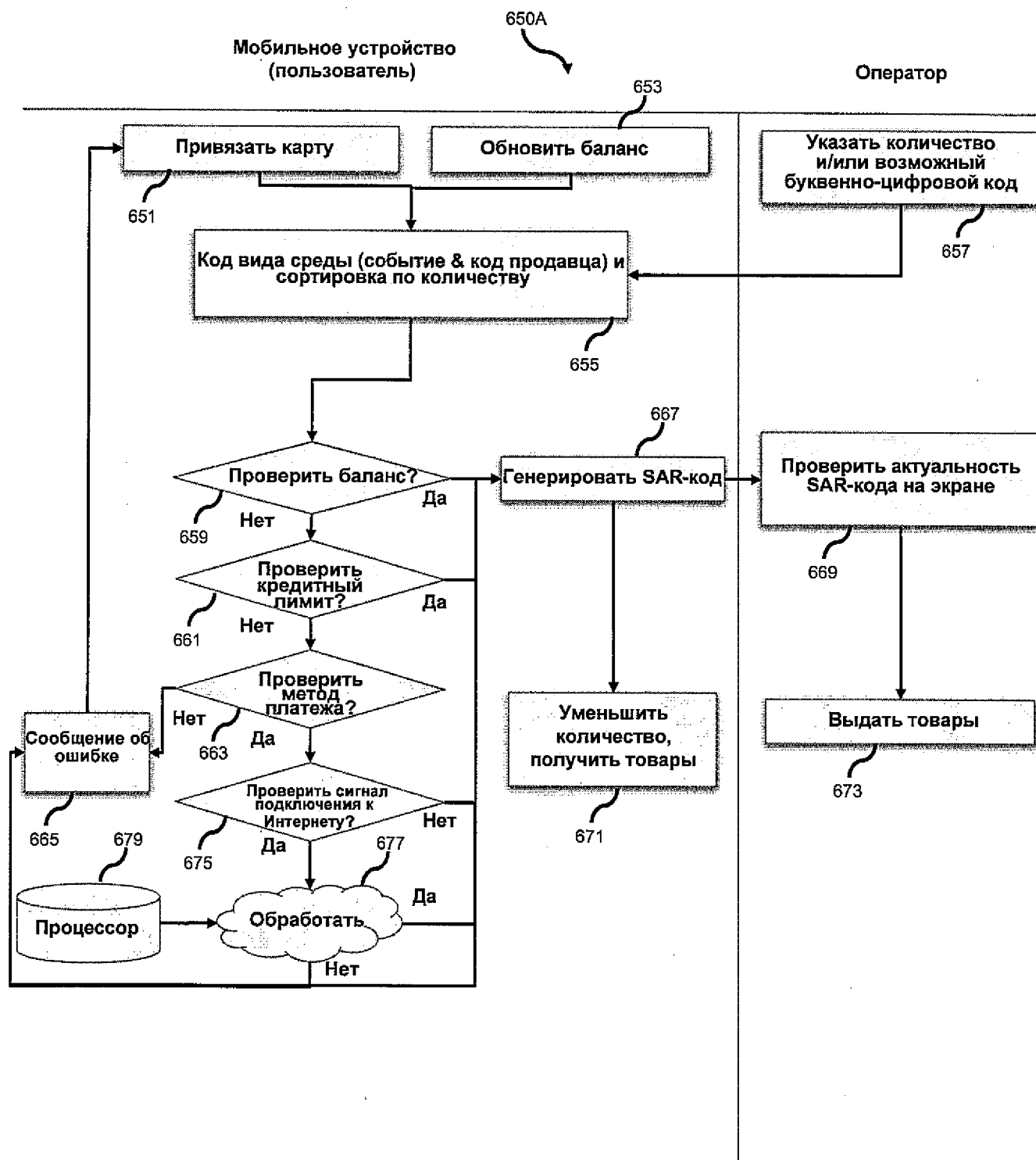
Фиг.10



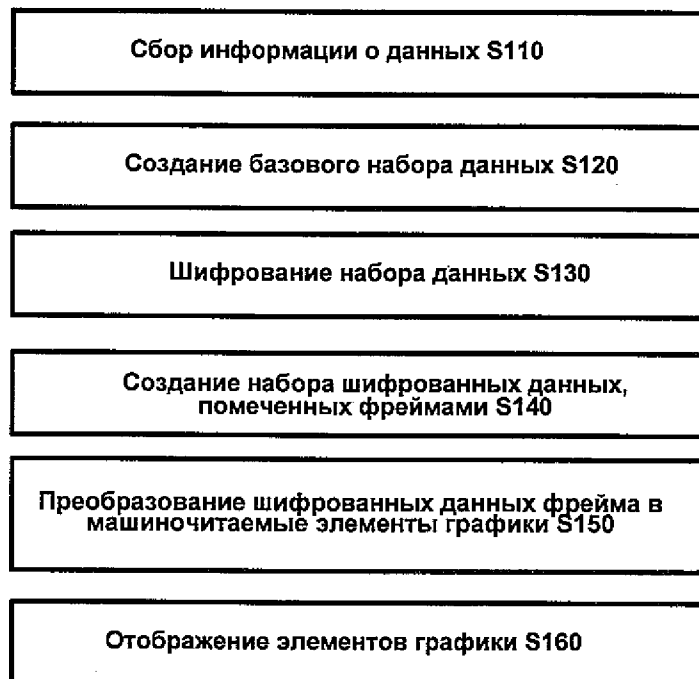
Фиг.10А



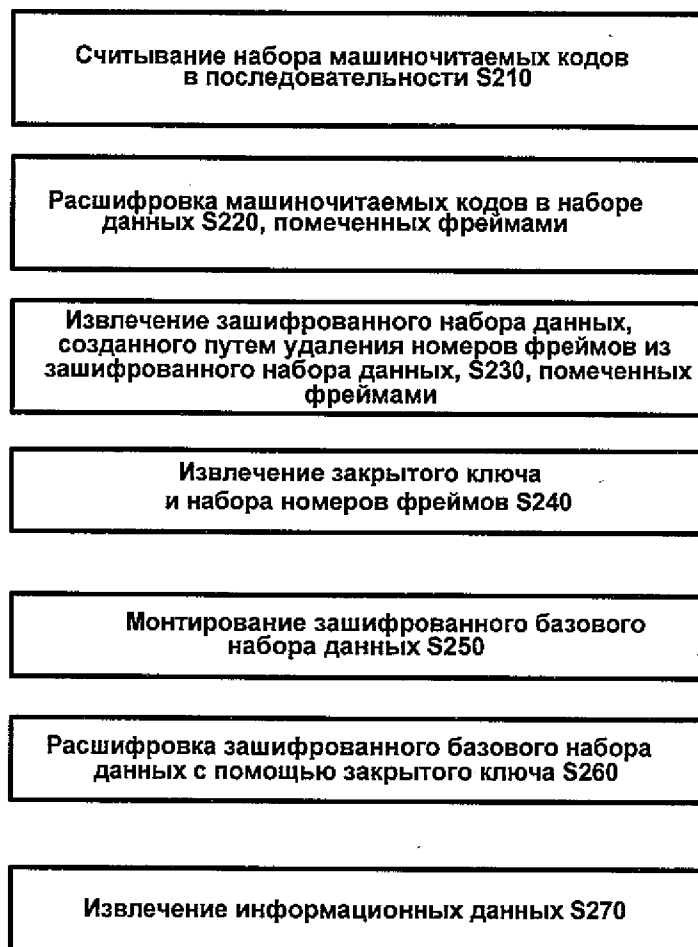
Фиг.11



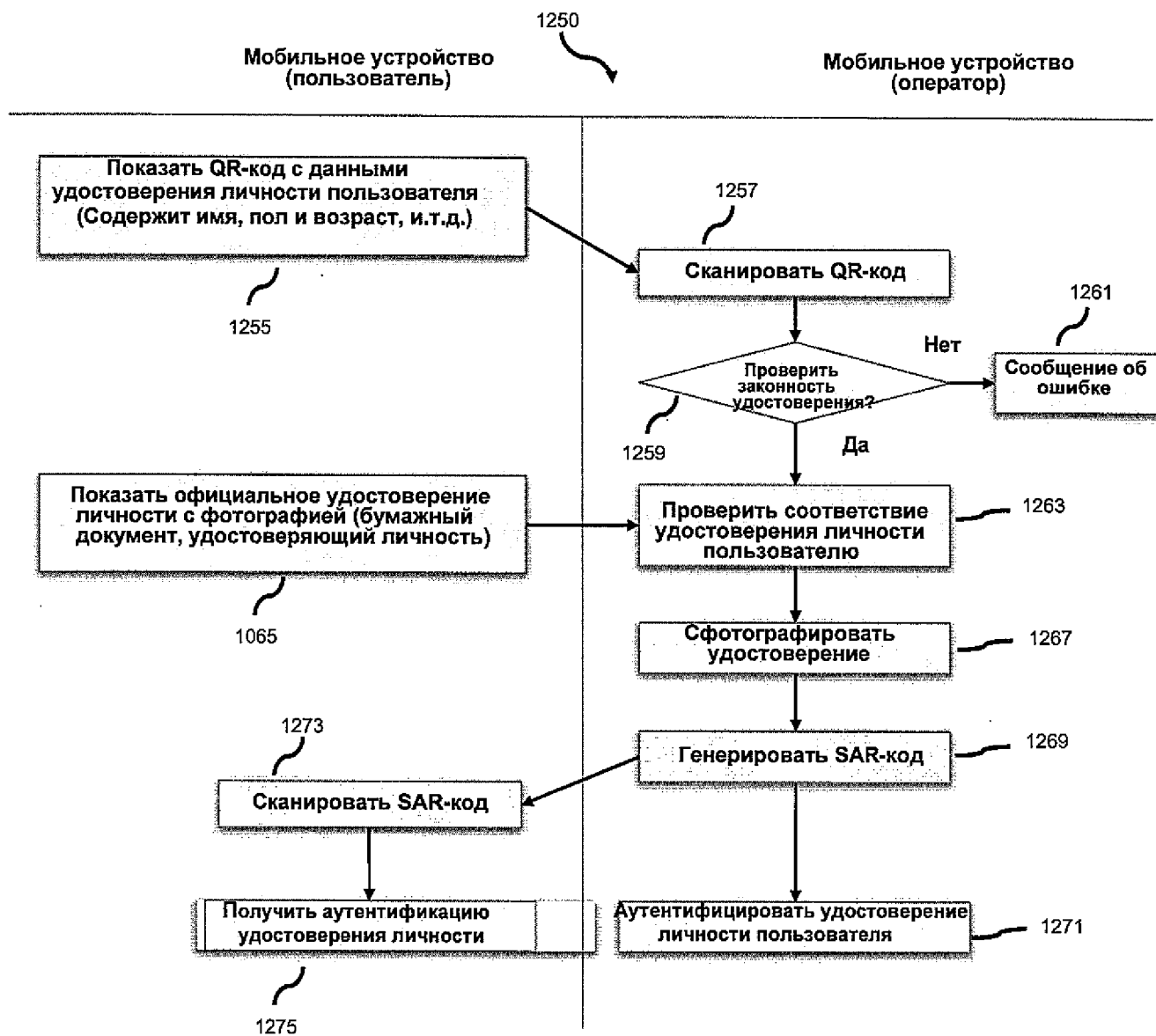
Фиг.11А



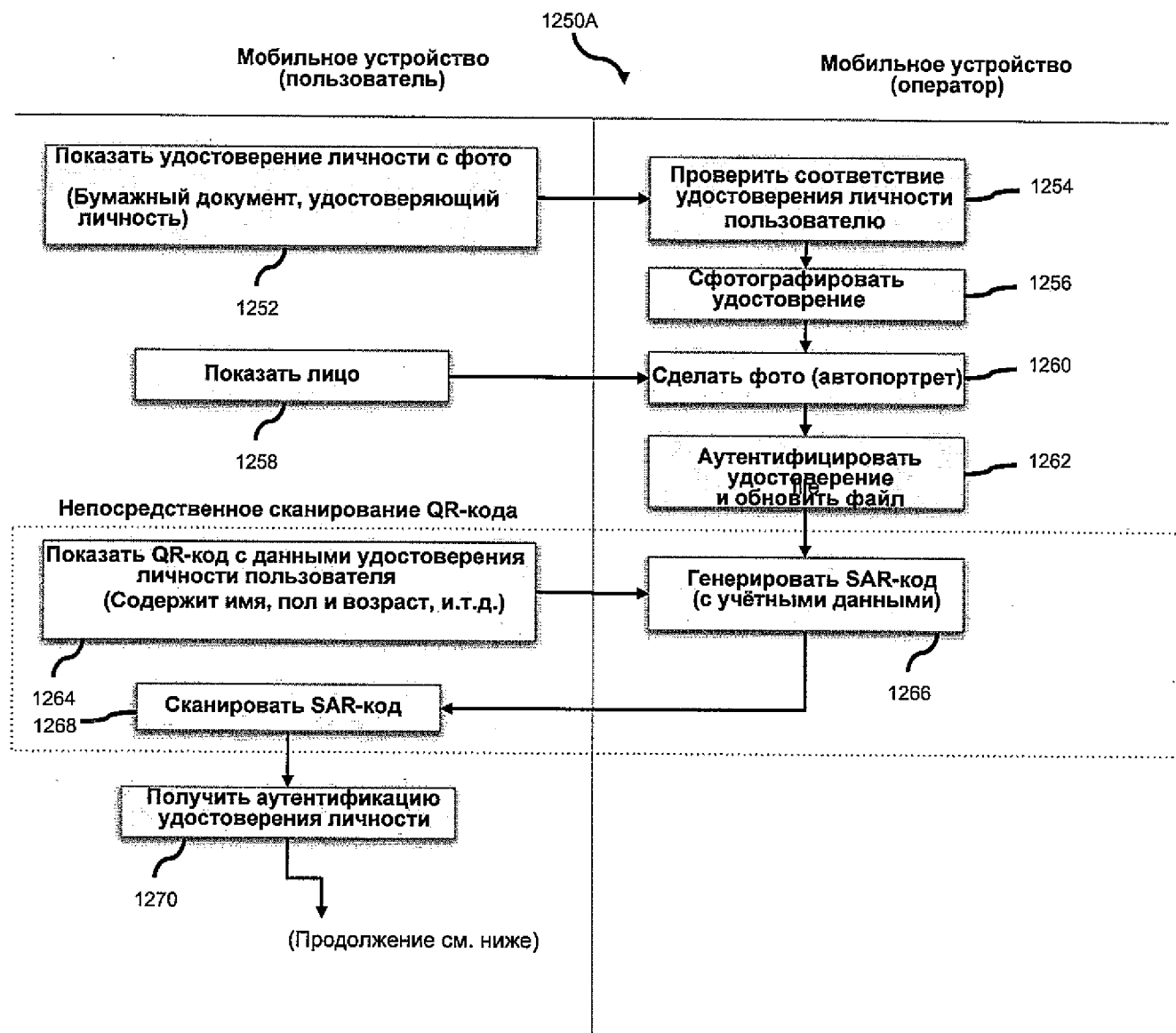
Фиг.12



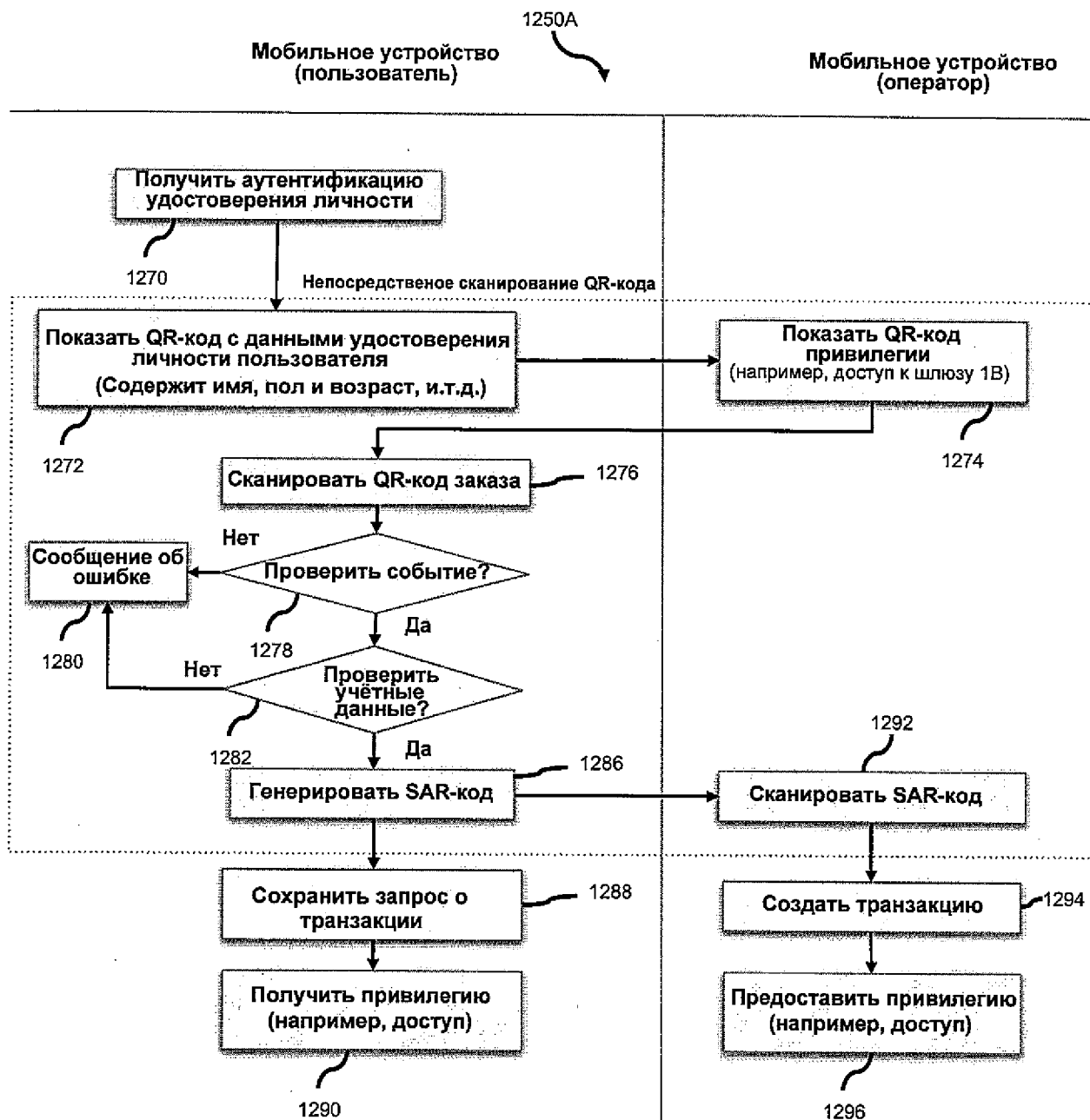
Фиг.13



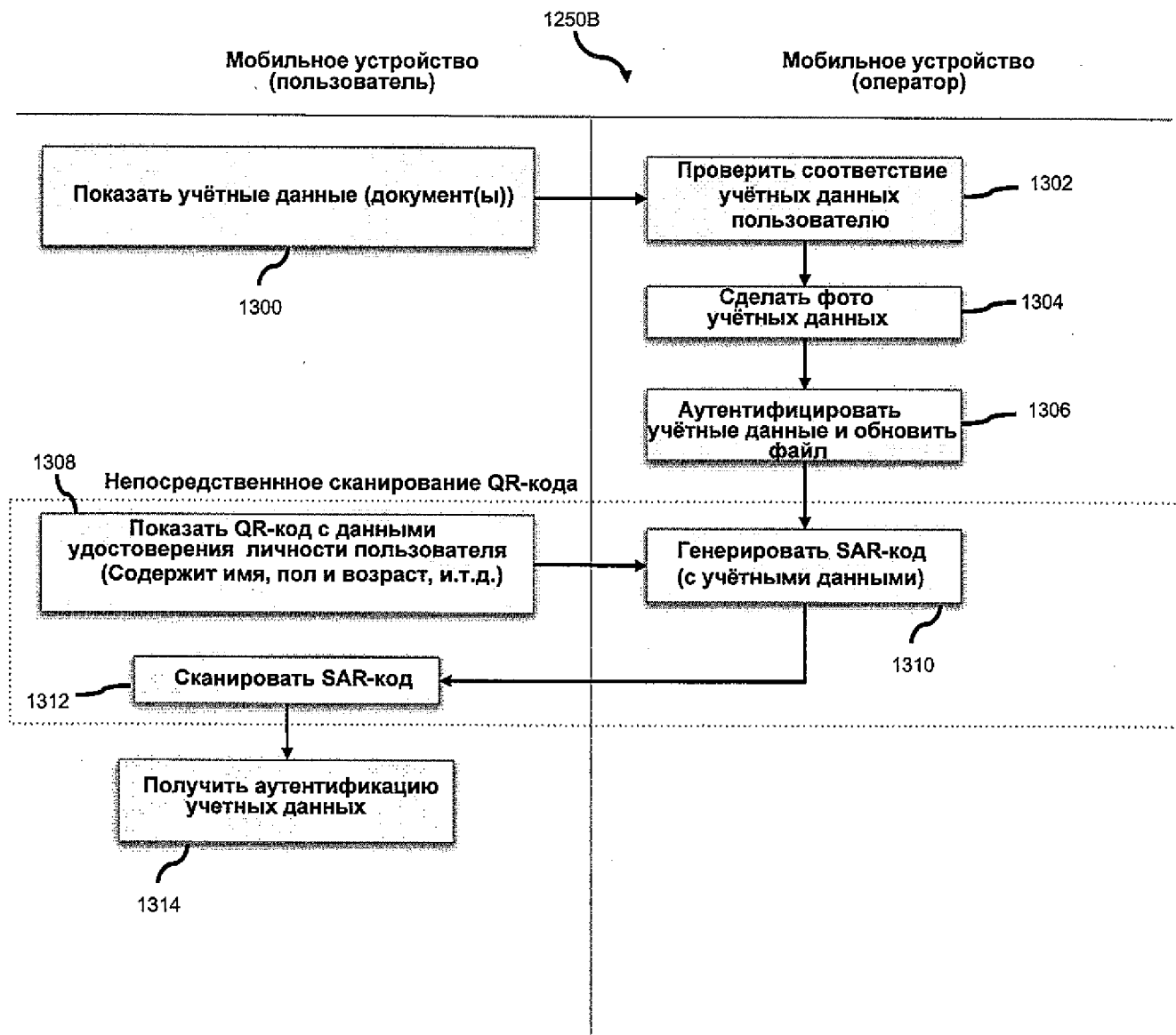
Фиг.14



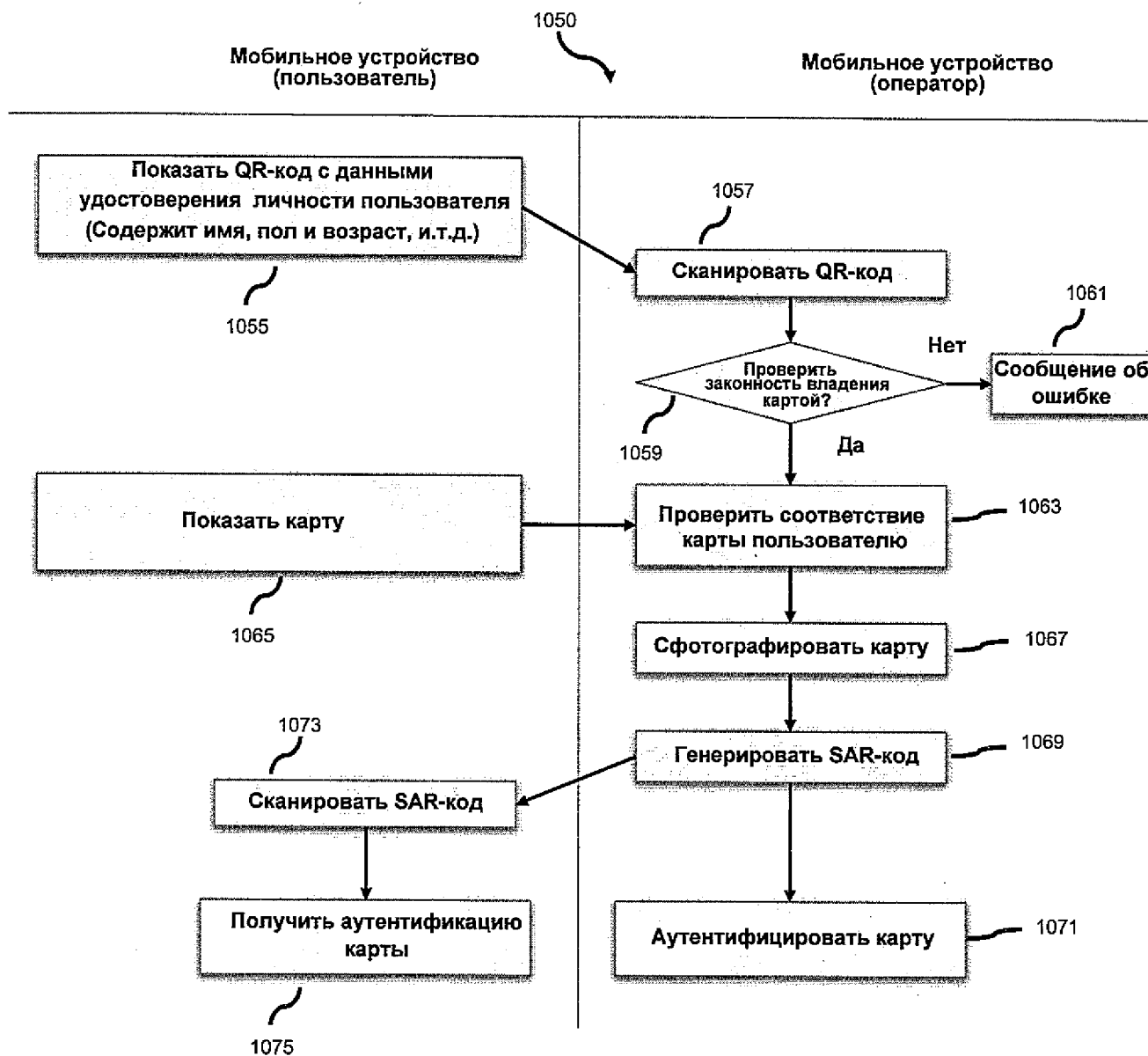
Фиг.14А



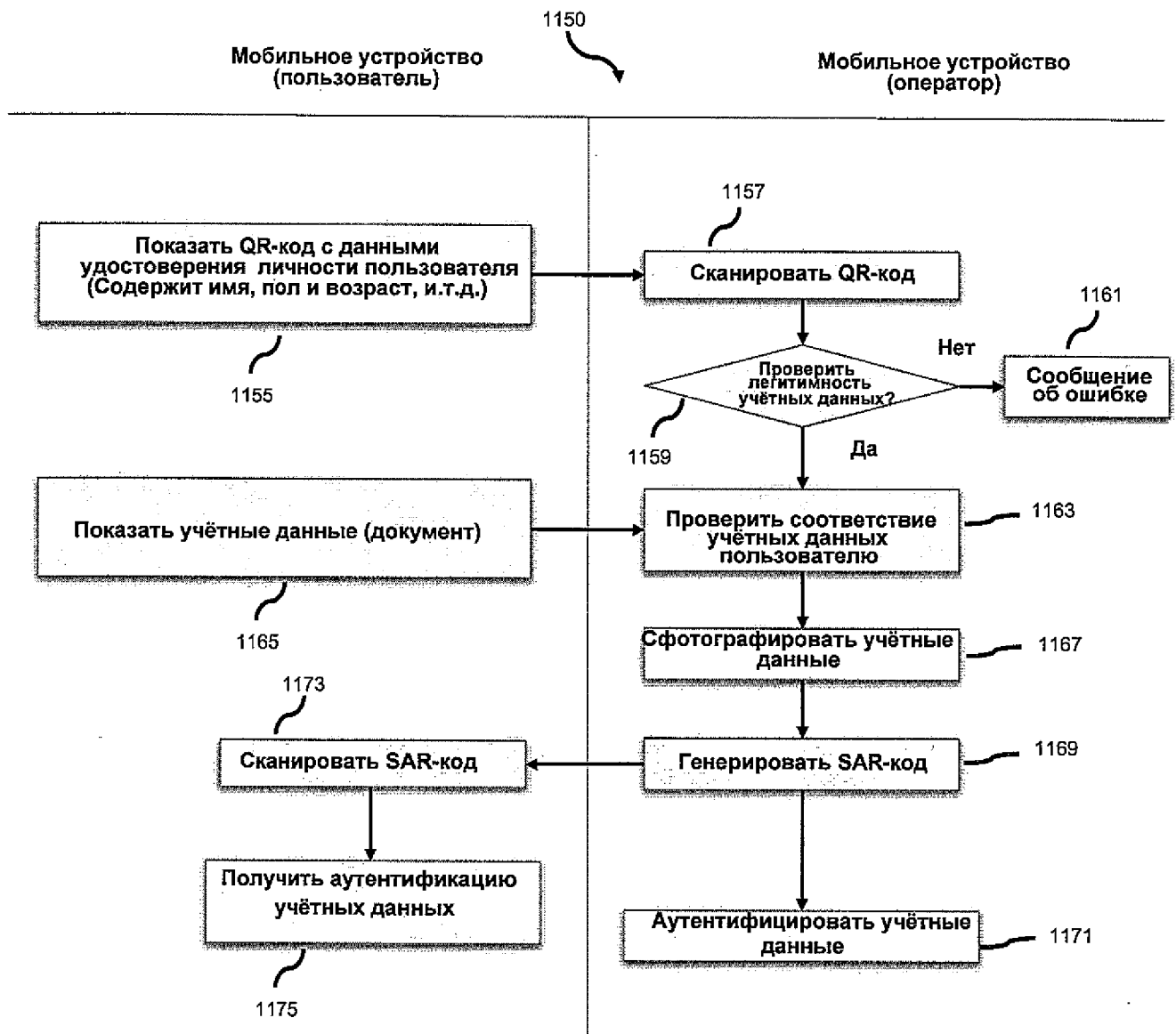
Фиг.14А (продолжение)



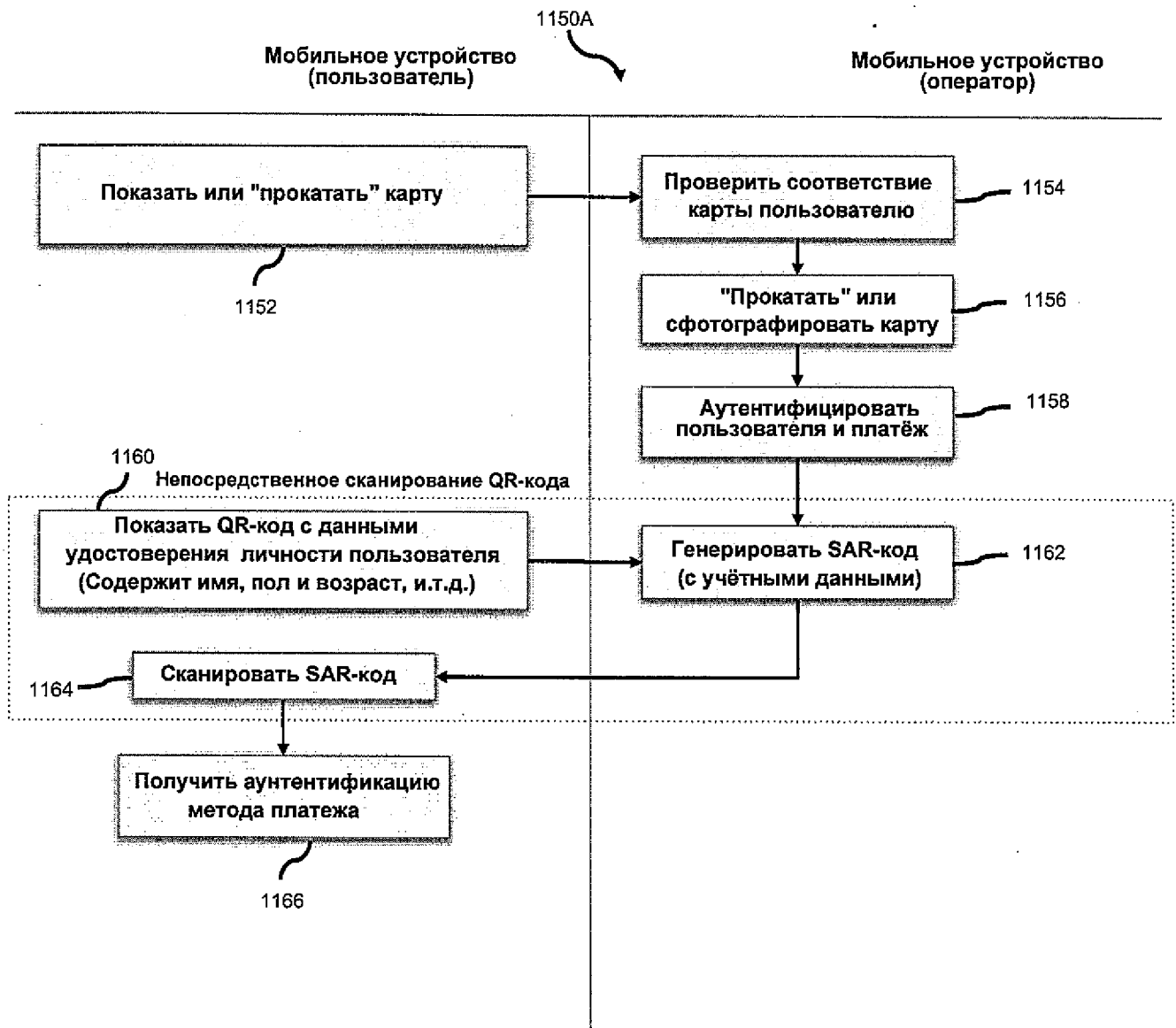
Фиг.14В



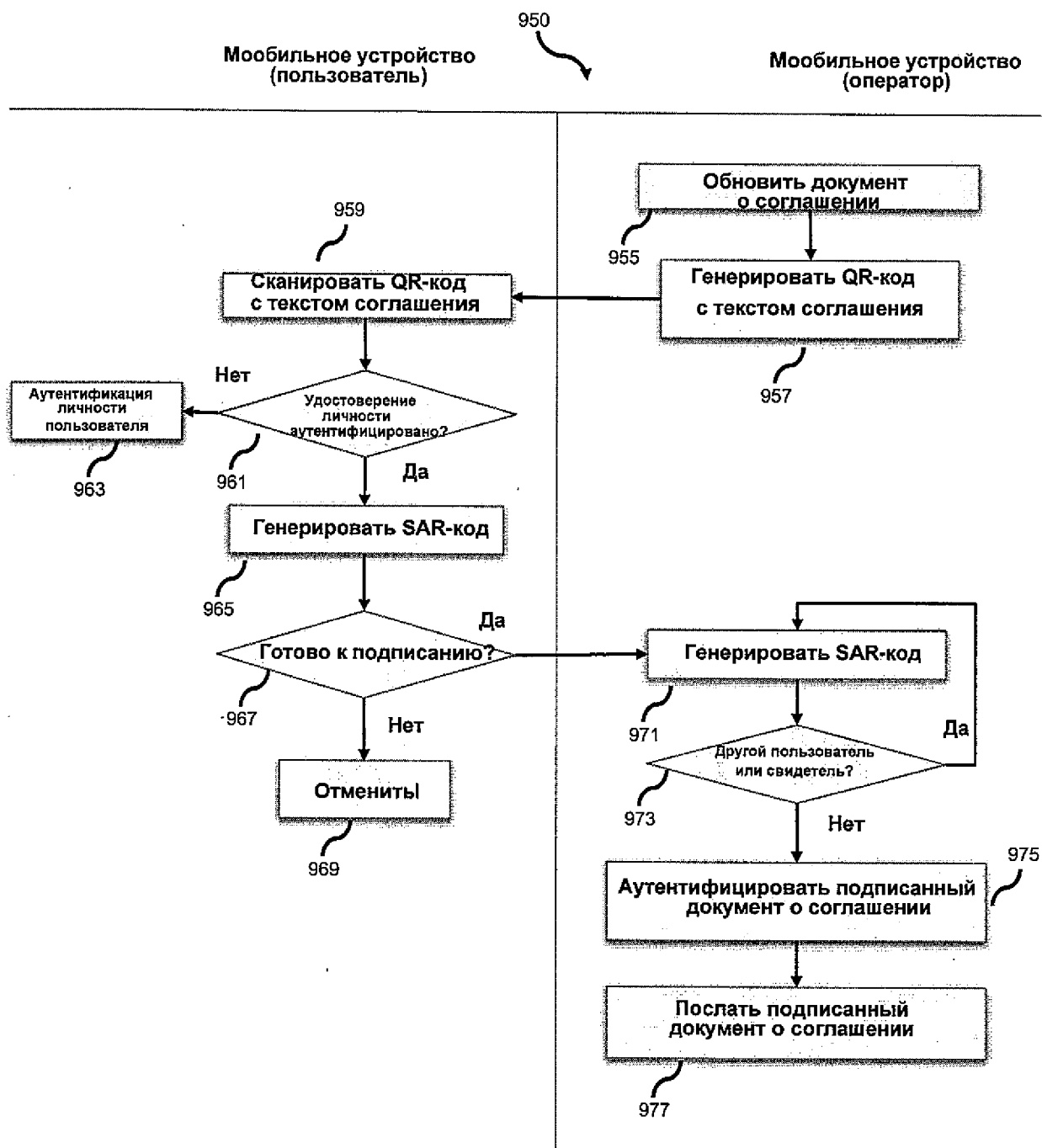
Фиг.15



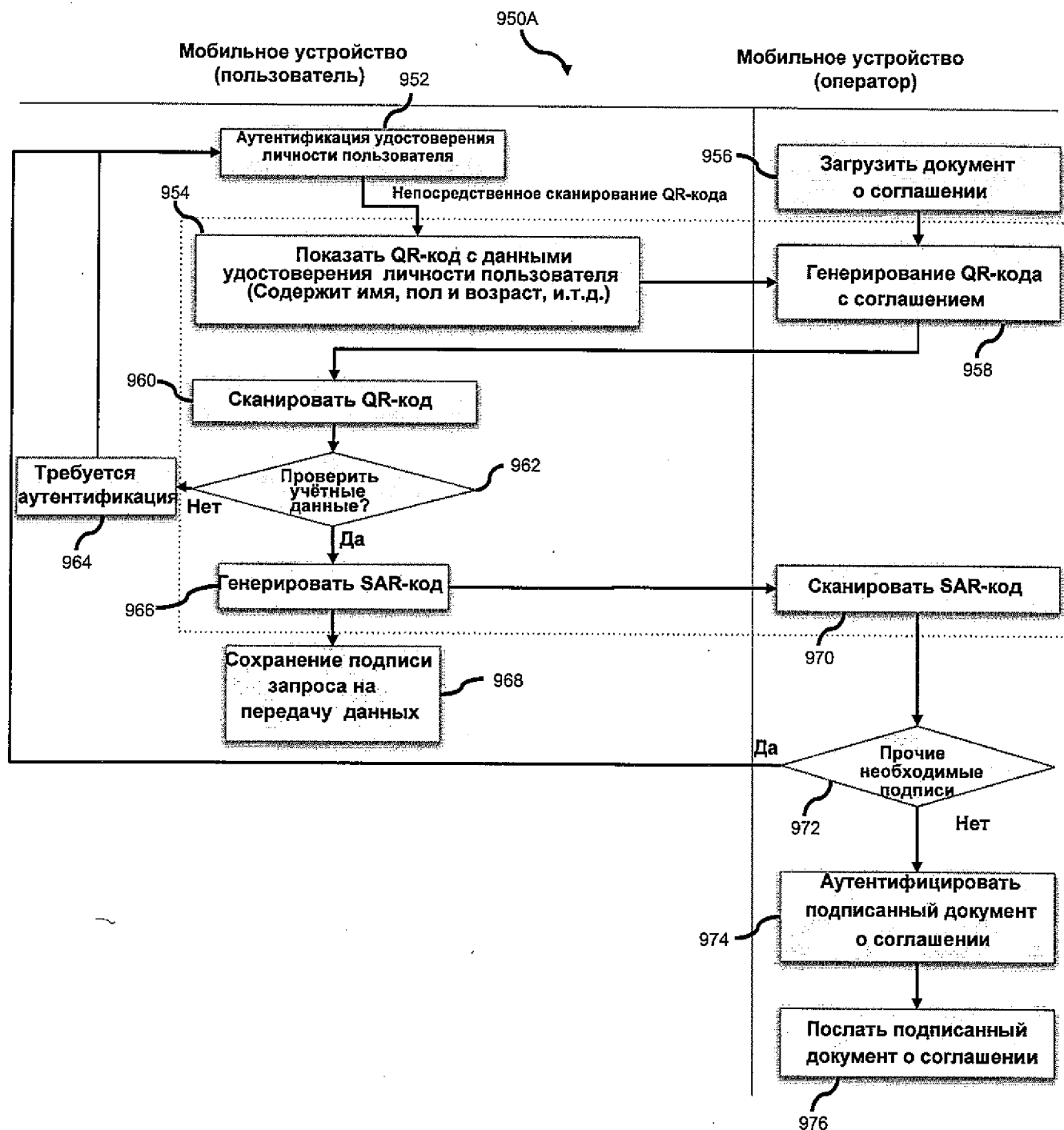
Фиг.16



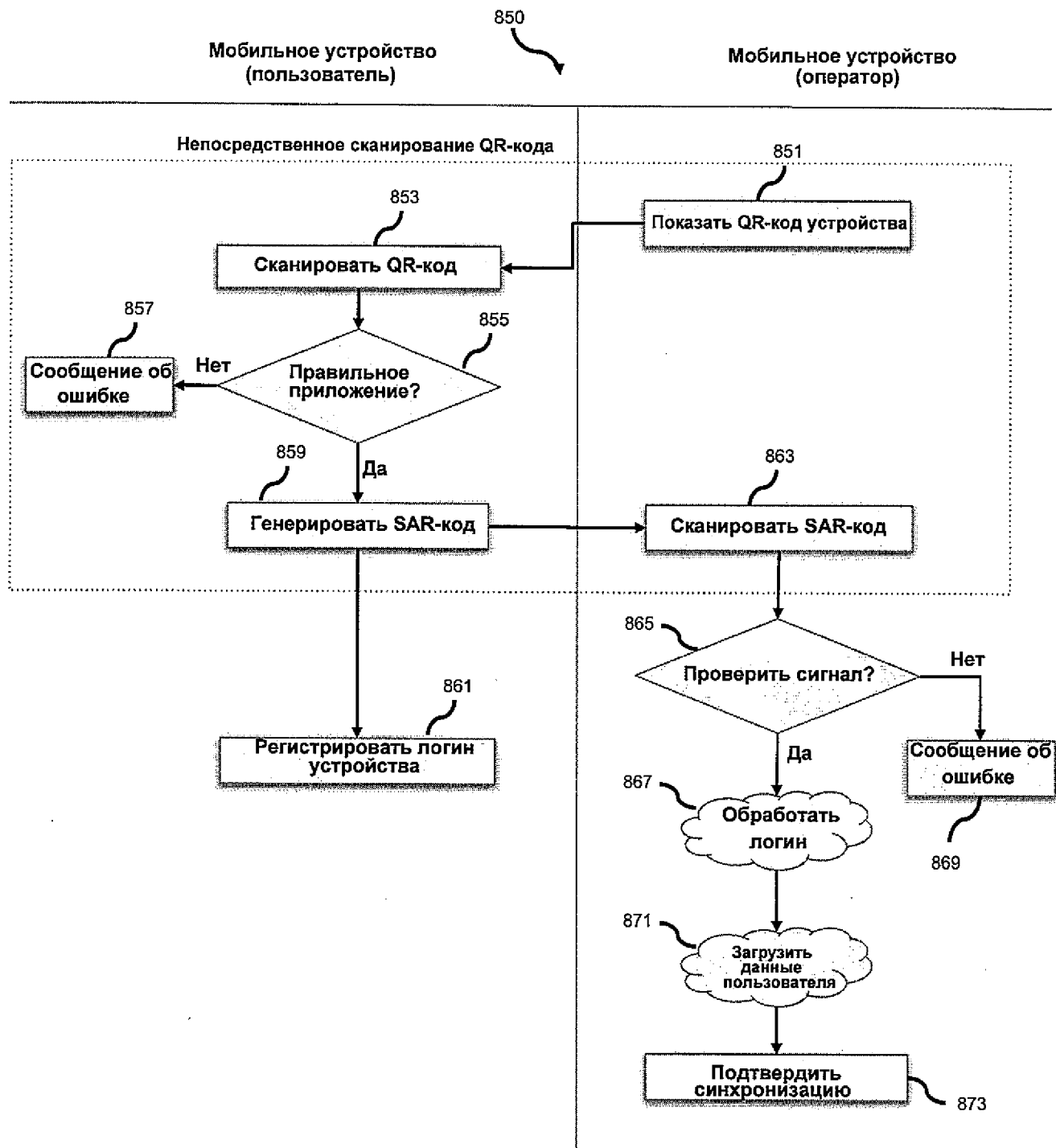
Фиг.16А



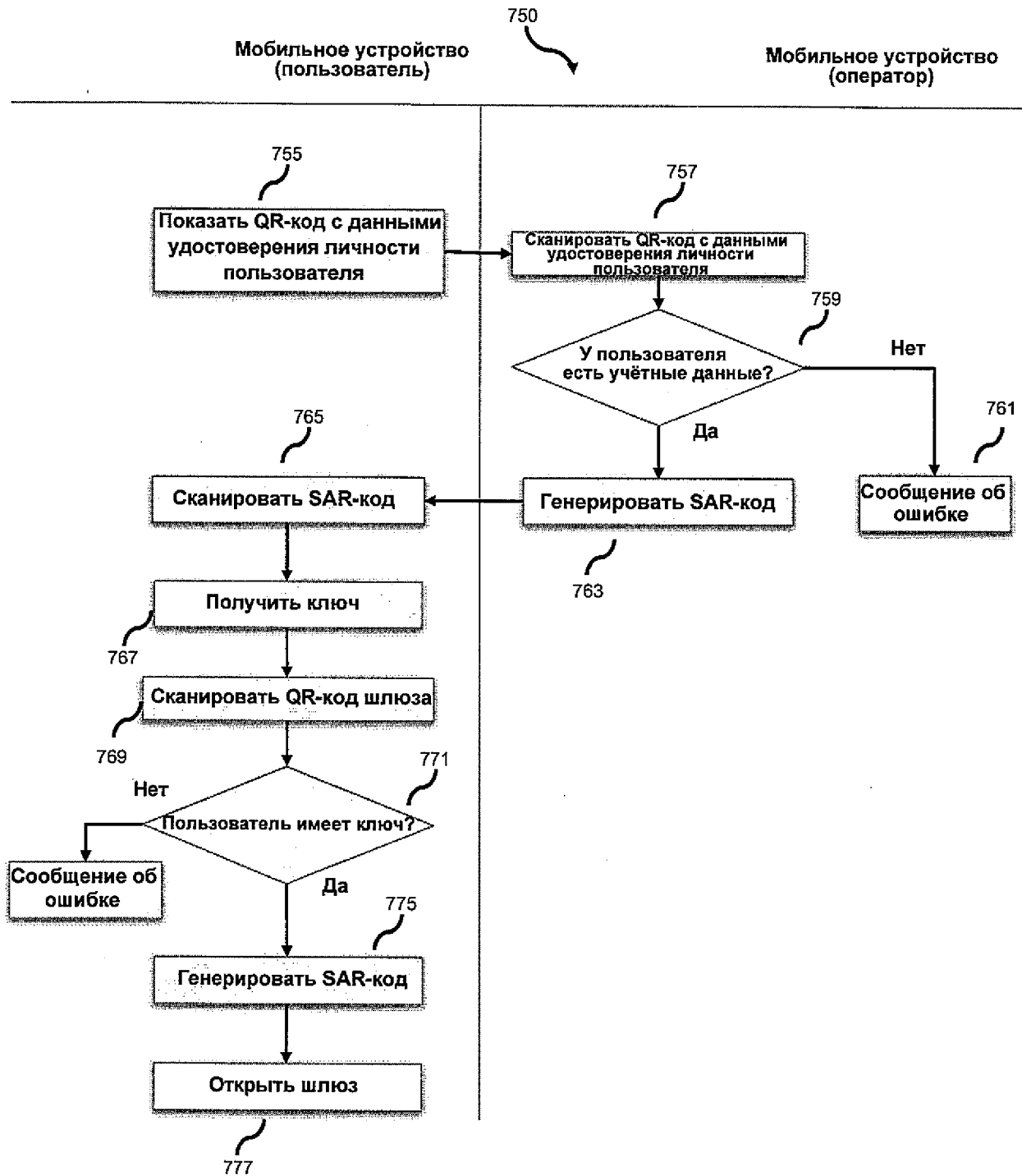
Фиг.17



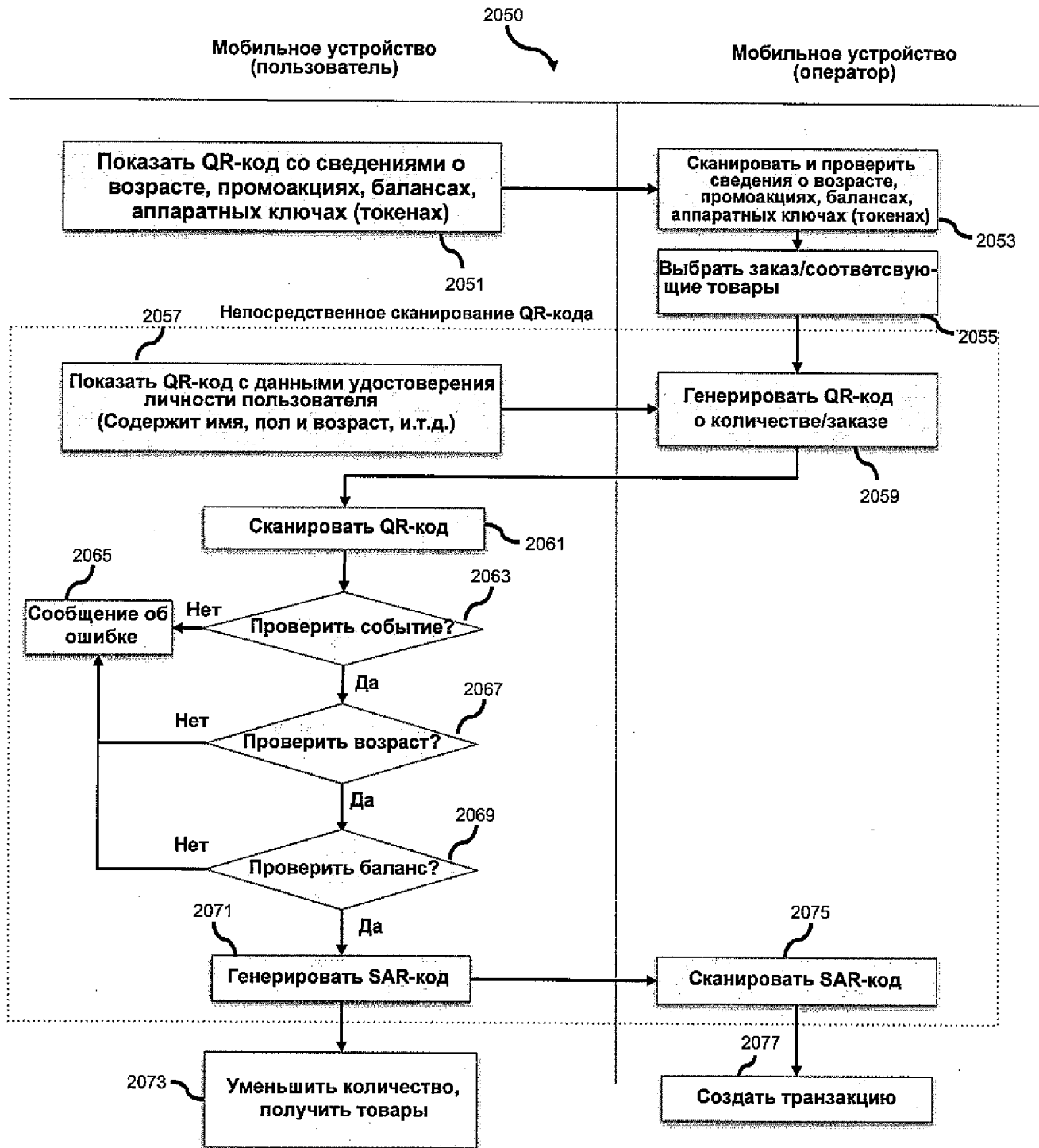
Фиг.17А



Фиг.18



Фиг.19



Фиг.20