(19) Евразийское патентное ведомство

(11) 041305 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.10.06

(21) Номер заявки
202092879

(22) Дата подачи заявки
2020.12.23

(51) Int. Cl. ***G07F 19/00*** (2006.01)
G06Q 20/00 (2006.01)

(54) СПОСОБ И СИСТЕМА ВОЗВРАТА ДЕНЕЖНЫХ СРЕДСТВ ПРИ ОТМЕНЕ ОПЕРАЦИИ ВЗНОСА НАЛИЧНОСТИ В КАНАЛЕ УСТРОЙСТВА САМООБСЛУЖИВАНИЯ

(31) **2020140336**
(32) **2020.12.08**
(33) **RU**
(43) **2022.06.30**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Куликов Дмитрий Владимирович,
Карицкий Александр Андреевич,
Кичаев Сергей Викторович,
Моисейкин Михаил Александрович,
Дорошенко Михаил Юрьевич,
Нецкин Иван Геннадьевич,
Айрапетян Сергей Суренович,
Стадник Дмитрий Фёдорович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-A1-20110068169
RU-C1-2677384
US-A1-20190130389
RU-C2-2715801
US-A1-20070174190

(57) Изобретение относится к области вычислительной техники, в частности, в обработке данных, выполняемой при автоматизированной операции возврата вносимых наличных денежных средств (ДС) при отмене операции взноса наличности в канале устройств самообслуживаний (УС). Техническим результатом является повышение защищенности операции возврата внесенных ДС за счет осуществления процедуры дополнительного подтверждения авторизационных данных клиента. Заявленный технический результат достигается за счет компьютерно-реализуемого способа возврата ДС при отмене операции взноса наличных ДС в канале УС, реализуемый с помощью процессора и содержащий этапы, на которых получают транзакционный запрос клиента по взносу наличных ДС с помощью авторизации клиента посредством получения NFC-токена или биометрической авторизации; осуществляют идентификацию банковской карты клиента; фиксируют процесс внесения ДС; распознают сумму внесенных ДС в канале УС; фиксируют событие отмены операции клиентом на этапе подтверждения внесения суммы распознанных ДС; формируют повторный запрос авторизации клиента, при этом упомянутый запрос является валидным в установленный временной промежуток; получают данные NFC-токена клиента или биометрическую информацию; выполняют сравнение полученных данных авторизации с данными, полученными в упомянутом транзакционном запросе; при этом в случае совпадения данных авторизации выполняют возврат суммы внесенных ДС с помощью перемещения ДС в лоток УС, в противном случае, если данные авторизации отличаются от данных, с помощью которых был сформирован транзакционный запрос, или указанные данные не получены в указанный временной промежуток, то внесенные ДС зачисляются на счет клиента, связанный с номером карты транзакционного запроса.

041305 B1

041305 B1

Область техники

Изобретение относится к области вычислительной техники, в частности, в обработке данных, выполняемой при автоматизированной операции возврата вносимых наличных денежных средств (ДС) при отмене операции взноса наличности в канале устройств самообслуживании (УС).

Уровень техники

В настоящий момент времени при взносе наличности в УС, например банкомат, при последующей отмене операции со стороны клиента после его первичной авторизации ДС выдаются без процесса дополнительного подтверждения со стороны клиента, что может приводить к тому, что внесенные ДС могут быть выданы ненадлежащему клиенту или являться объектом мошеннических операций.

Такой подход известен из уровня техники, например из патентной заявки US 20190130389 A1 (Wayne Fueling Systems LLC, 02.05.2019). В данном решении в случае отмены операции внесения наличности не осуществляется повторная проверка авторизационных данных клиента, которые были первично указаны при создании транзакционной сессии, в частности, с помощью передачи NFC-токена клиента.

Сущность изобретения

Заявленное изобретение позволяет решить техническую проблему, заключающуюся в создании более защищенного способа возврата ДС при отмене операции внесения наличных ДС.

Техническим результатом является повышение защищенности операции возврата внесенных ДС за счет осуществления процедуры дополнительного подтверждения авторизационных данных клиента.

Заявленный технический результат достигается за счет компьютерно-реализуемого способа возврата ДС при отмене операции взноса наличных ДС в канале УС, реализуемый с помощью процессора и содержащий этапы, на которых

получают транзакционный запрос клиента по взносу наличных ДС с помощью авторизации клиента посредством получения NFC-токена или биометрической авторизации;

осуществляют идентификацию банковской карты клиента;

фиксируют процесс внесения ДС;

распознают сумму внесенных ДС в канале УС;

фиксируют событие отмены операции клиентом на этапе подтверждения внесения суммы распознанных ДС;

формируют повторный запрос авторизации клиента, при этом упомянутый запрос является валидным в установленный временной промежуток;

получают данные NFC-токена клиента или биометрическую информацию;

выполняют сравнение полученных данных авторизации с данными, полученными в упомянутом транзакционном запросе;

при этом в случае совпадения данных авторизации выполняют возврат суммы внесенных ДС с помощью перемещения ДС в лоток УС, в противном случае, если данные авторизации отличаются от данных, с помощью которых был сформирован транзакционный запрос, или указанные данные не получены в указанный временной промежуток, то внесенные ДС зачисляются на счет клиента, связанный с номером карты транзакционного запроса.

В одном из частных вариантов осуществления способа NFC-токен формируется мобильным устройством или умным носимым устройством.

В другом частном варианте осуществления способа биометрическая информация получается с помощью камеры УС.

В другом частном варианте осуществления способа дополнительно получают видеоданные клиента при работе с УС.

В другом частном варианте осуществления способа фиксируют наличие событий повторной транзакции клиентом, не сформировавшем транзакционный запрос, и осуществляют зачисление ДС на карту клиента, сформировавшего транзакционный запрос. Заявленное техническое решение также осуществляется с помощью системы возврата ДС при отмене операции взноса наличных ДС в канале УС, которая содержит по меньшей мере один процессор и по меньшей мере одно запоминающее устройство, хранящее машиночитаемые инструкции, которые при их исполнении процессором осуществляют вышеуказанный способ.

Краткое описание чертежей

Фиг. 1А иллюстрирует пример схемы УС,

фиг. 1Б-1В - пример взаимодействия клиента с УС,

фиг. 2 - блок-схему заявленного способа,

фиг. 3 - пример вычислительного устройства.

Осуществление изобретения

Ниже будут описаны понятия и определения, необходимые для подробного раскрытия заявленного изобретения.

Денежные средства (ДС) - специфический товар, обладающий наивысшей ликвидностью, служащий измерителем стоимости других товаров и услуг.

Банковское устройство самообслуживания (УС) - программно-технический комплекс, предназна-

ченный для автоматизированной выдачи и/или приёма наличных ДС как с использованием платёжных карт, так и без, а также выполнения других операций, в том числе оплаты товаров и услуг, составления документов, подтверждающих соответствующие операции. Банковские устройства самообслуживания подразделяются на два типа в зависимости от того, поддерживают ли они функцию выдачи наличных денег или нет. Если функция поддерживается, то УС является ATM (англ. automated teller machine), или банкоматом, иначе - NCS (non-cash systems), или терминалом для безналичных операций.

Программное обеспечение (ПО) - программа или множество программ, используемых для управления УС.

В каждый момент времени УС находится в одном из следующих режимов работы:

Power Up - загрузка;

Offline - нет связи с сервером, осуществляется подключение;

Supervisor - работает инкассатор или сервис-инженер;

Out of service - УС не работает в связи с неисправностью, исчерпанием денежных средств или принудительным переводом УС в указанный режим;

In service - основной режим работы УС.

В режиме In service УС находится в одном из состояний (стейт) с номером от 001 до 999 и 25-символьной строкой-описанием. Первый символ этой строки - тип стейта (обозначаются буквами A…Z, а также a…z и некоторыми символами (,'.?)), который определяет совокупность. Остальные 24 символа - это 8 десятичных 3-значных чисел, каждое из которых является определенной настройкой стейта (номер экрана для показа, условия перехода на стейт, список действий). Стейтов одного типа может быть любое количество.

Заявленное решение реализуется алгоритмом работы УС (100), обеспечивающего функцию внесения наличных ДС пользователем (10). На фиг. 1A приведена примерная схема компонентов УС (100). В качестве УС (100) может выступать банкомат, платежный терминал и любое другое устройство, обеспечивающее прием наличных денежных средств. Как показано на представленной общей схеме УС (100), устройство содержит объединенные с помощью шины (110) компоненты, такие как процессор (101), память (102), средство сетевого взаимодействия (103), дисплей (104), органы управления (105), средство выдачи ДС (106), средство приема ДС (107) и средство чтения карт (108). Процессор УС (101) выполняет все необходимые вычислительные операции при обработке транзакционных запросов. Память (102) может представлять одно или более устройств различного типа, таких как ОЗУ, ПЗУ или их сочетания. В качестве ПЗУ может использоваться HDD, SSD диски, флэш-память и т.п. В памяти (102), как правило, хранится исполняемая процессором (101) программная логика, необходимая для реализации способа работы УС (100), а также операционная система, организующая интерфейс взаимодействия (GUI) и протоколы обработки данных.

В качестве средств сетевого взаимодействия (103) могут применяться устройства, обеспечивающие обмен данными с помощью проводного или беспроводного типа связи, например Ethernet карта (LAN), Wi-Fi модуль, GSM модем (2G, 3G, 4G, 5G) и т.п. Дополнительно могут использоваться средства обмена данными между УС (100) и пользователем (устройством пользователя), например Bluetooth приемопередатчик, NFC-модуль, IrDa и т.п. Дисплей УС (104) служит для отображения графического интерфейса пользователя (GUI), а также при его исполнении в виде сенсорного дисплея, что также обеспечивает взаимодействие с пользователем (10) и получения от него команд управления. Органы управления УС (105) могут представлять собой клавиатуру, сенсорный дисплей, пин-пад, механические и сенсорные кнопки, либо сочетание вышеперечисленных элементов. Средство выдачи ДС (106) представляет собой диспенсер. Диспенсер (106) может быть различного типа, например фрикционным или вакуумным. УС (100) также содержит средство для приема наличных ДС (107) от пользователя, в частности купюроприемник или модуль приема наличности.

УС (100) также содержит считыватель банковских карт (108), обеспечивающий авторизацию клиента (10) и переход на стейт для формирования для исполнения транзакционного запроса. Считыватель (108) может исполняться как карт-ридер или NFC-модуль для бесконтактного считывания карт клиента (10).

УС (100) может дополнительно содержать одно или несколько средств биометрической идентификации (109), например камеру, сенсоры отпечатка пальца, сетчатки глаза, микрофон и т.п. Данные устройства как по отдельности, так и в совокупности, могут применяться для идентификации и верификации пользователя, получая требуемую информацию и обрабатывая с помощью программной логики УС (100), хранимой в памяти (102).

С помощью указанных средств (109) может применяться двухфакторная верификация пользователя с помощью камеры или биометрических сенсоров, например сканера отпечатка пальца, сетчатки глаза, или с помощью анализа голоса пользователя. С помощью камеры может фиксироваться изображение пользователя УС (100) для последующей обработки и сравнения с эталонной идентифицирующей информацией владельца счета при инициации транзакционной операции в УС (100).

УС (100) может также обеспечивать обмен идентификационной информацией в полностью бесконтактном режиме с помощью заранее создаваемого идентификационного токена с помощью устройства

пользователя, например смартфона, планшета или ноутбука, и его последующей передачи по беспроводному каналу обмена информацией, например Bluetooth, Wi-Fi, NFC, RFID и т.п., в УС (100). На фиг. 1Б-1В показана общая схема взаимодействия пользователя (10) с УС (100). Первичный пользовательский запрос на выполнение транзакции может формироваться в памяти УС (100) после выбора клиентом банковской операции.

Банковскую операцию пользователь (10) может выбирать посредством использования графического интерфейса пользователя УС (100), отображаемого на дисплее УС (104). В качестве банковской операции в настоящем решении рассматривается внесение наличных ДС для их последующего зачисления на счет клиента или иной счет.

УС (100) связано посредством сети передачи данных (150), например Интернет, с удаленным сервером (120), который обеспечивает обработку данных, поступающих от УС (100).

Первичный пользовательский запрос формируется с помощью взаимодействия пользователя (10) с УС (100) и содержит, по меньшей мере, информацию о намерении пользователя осуществить транзакцию по доставке ДС с помощью распознавания NFC-токена его мобильного устройства или банковской карты, а также при биометрической аутентификации клиента (10).

Далее с ссылкой на фиг. 2 рассмотрим блок-схему заявленного способа (200) автоматического зачисления внесенных наличных ДС при отмене операции внесения клиентом (10). На этапе (201) формируется первичный пользовательский запрос на выполнение транзакции, который сохраняется в памяти УС (100). Такой запрос содержит, по меньшей мере, информацию, идентифицирующую клиента (10), в частности идентификатор счета для зачисления ДС, связанный с устройством (11) или биометрической информации клиента (10).

Первичная авторизация и формирование транзакционного запроса осуществляется посредством взаимодействия с помощью устройства (11) пользователя, например смартфона, банковской карты с чипом NFC или умного носимого устройства (смарт-часы, браслет), снабженного NFC-модулем, обеспечивающим передачу NFC-токена платежной карты клиента (10), а также с помощью биометрической идентификации. Биометрическая идентификация осуществляется с помощью работы модуля (109), например камеры, захватывающей изображение лица клиента (10), для последующей отправки УС (100) полученного изображения на сервер (120) посредством сети передачи данных (150) в целях подтверждения личности и получения данных о счете клиента (10). Для каждой транзакции создается уникальный идентификатор транзакции (TrID). В некоторых вариантах осуществления идентификатор транзакции является численным или символьным значением. Значение TrID должно быть уникальным для каждого транзакционного запроса (значение TrID обновляется при каждом переходе на транзакционный стейт в сценарии УС). Во все транзакционные запросы добавляется поле "TransactionID", например, с идентификатором "3", состоящее из 12 символов. Для первичного запроса данные поля формируются следующим образом: ГММДДЧЧММNNN (где Г - последняя цифра текущего года, ММ - номер месяца, ДД - день, ЧЧ - час, ММ - минута, NNN - последние 3 цифры текущего значения Accumulated Transaction Count, что обеспечивает уникальность значения TransactionID для данного терминала). Для повторного запроса значение поля "TransactionID" должно повторять значение, сформированное в момент первичного запроса.

На этапе (202) клиент осуществляет внесение наличных ДС через купюроприемник (107) УС (100). После внесения наличных ДС клиент (10) инициирует отмену выполнения транзакционной операции на этапе (204), в связи с чем логика УС (100) фиксирует внесенную сумму ДС (этап 203) и активирует запрос на повторную аутентификацию клиента (этап 205). Следующим этапом (206) является аутентификация клиента (10), первично сформировавшего транзакционный запрос. На этапе (206) выполняется проверка идентификатора клиента (10), полученного при первичном формировании транзакционного запроса с помощью передачи NFC-токена от устройства (11).

На данном этапе на дисплее УС (100) пользователю (10) предлагается повторить авторизацию с помощью прикладывания устройства (11) к считывателю (108) для передачи NFC-токена или пройти повторную биометрическую идентификацию. Если первый и второй токены совпадают, или личность клиента (10) повторно подтверждается, то внесенные ДС возвращаются (этап 207) пользователю (10) путем их выдачи через лоток выдачи наличности (106).

Также при инициировании процедуры отмены операции на этапе (204) активируется таймер, в течение которого необходимо выполнить повторную авторизацию клиента (10). В случае, если в ходе отведенного времени авторизации не происходит, либо же полученный NFC-токен или личность клиента (10) отличается от информации, полученной в ходе формирования первичного транзакционного запроса, то наличные ДС не выдаются, а зачисляются на счет (этап 208), связанный с идентификатором клиента (10), полученного в ходе формирования транзакционного запроса, например, по номеру связанной банковской карты.

Такой подход позволяет исключить неблагоприятные факторы для клиента (10), в частности хищение ДС, в случае завершения операции отмены внесения наличности другим лицом. Разработанный способ позволяет однозначно утверждать о выдаче внесенных ДС клиенту (10), который инициировал транзакционный запрос и процедуру его отмены после внесения наличности.

Также на этапе (206) проверяется факт того, что повторная идентификация клиента (10) осуществ-

ляется тем же устройством (11), с помощью которого первично был сформирован транзакционный запрос на этапе (201). Если клиент (10) на этапе (206) осуществил повторную идентификацию другим устройством (11), то наличные ДС не возвращаются и зачисляются на счет клиента автоматически.

В одном из примеров осуществления настоящего изобретения дополнительно может использоваться информация об обстановке около УС (100), фиксируемая камерой УС (109) в ходе выполнения транзакционного запроса. В данном примере камерой (109) получается не только изображение клиента (10), но и выполняется фиксация событий, происходящих в момент внесения ДС и последующего формирования команды на отмену транзакции. В момент анализа на этапе (206), если камерой (109) фиксируется наличие нестандартного поведения клиента (10) или наличие в кадре других людей, которые могут осуществлять противоправные действия в отношении клиента (10), осуществляющего транзакцию, в частности нападение, выхватывание средства авторизации (11) или авторизация вместо клиента (10), то УС (100) автоматически зачисляет ДС клиенту на счет (10). УС (100) может также блокироваться для дальнейших операций в случае возникновения нестандартных ситуаций вблизи УС (100).

Представленные материалы раскрывают предпочтительные примеры реализации изобретения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

На фиг. 3 представлен общий вид вычислительного устройства (300), пригодного для выполнения способа (200). Устройство (300) может представлять собой часть УС (100), сервер (120), устройство пользователя (11) и иные непредставленные устройства, которые могут участвовать в общей информационной архитектуре заявленного решения.

В общем случае вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (305) и устройство для сетевого взаимодействия (306).

Процессор (301) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. В качестве процессора (301) может также применяться графический процессор, например Nvidia, AMD, Graphcore и пр.

ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнения необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (303) представляет собой одно или более устройств постоянного хранения данных, например жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов устройства (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь, PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п. Для обеспечения взаимодействия пользователя с вычислительным устройством (300) применяются различные средства (305) В/В информации, например клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (306) обеспечивает передачу данных устройством (300) посредством внутренней или внешней вычислительной сети, например Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) может использоваться, но не ограничиваться, Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации в составе устройства (300), например GPS, ГЛОНАСС, BeiDou, Galileo.

Представленные материалы раскрывают предпочтительные примеры реализации изобретения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Компьютерно-реализуемый способ возврата денежных средств (ДС) при отмене операции взноса наличных ДС в канале устройства самообслуживания (УС), реализуемый с помощью процессора и содержащий этапы, на которых

получают транзакционный запрос клиента по взносу наличных ДС с помощью авторизации клиента посредством получения NFC-токена или биометрической авторизации;

осуществляют идентификацию банковской карты клиента;

фиксируют процесс внесения ДС;

распознают сумму внесенных ДС в канале УС;

фиксируют событие отмены операции клиентом на этапе подтверждения внесения суммы распознанных ДС;

формируют повторный запрос авторизации клиента, при этом упомянутый запрос является валидным в установленный временной промежуток;

получают данные NFC-токена клиента или биометрическую информацию;

выполняют сравнение полученных данных авторизации с данными, полученными в упомянутом транзакционном запросе;

при этом в случае совпадения данных авторизации выполняют возврат суммы внесенных ДС с помощью перемещения ДС в лоток УС, в противном случае, если данные авторизации отличаются от данных, с помощью которых был сформирован транзакционный запрос, или указанные данные не получены в указанный временной промежуток, то внесенные ДС зачисляются на счет клиента, связанный с номером карты транзакционного запроса.

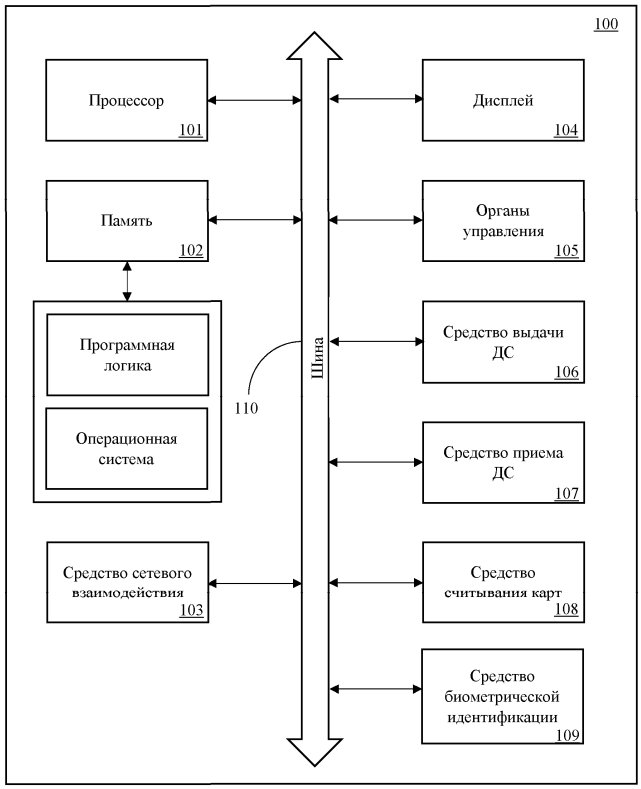
2. Способ по п.1, в котором NFC-токен формируется мобильным устройством или умным носимым устройством.

3. Способ по п.1, в котором биометрическая информация получается с помощью камеры УС.

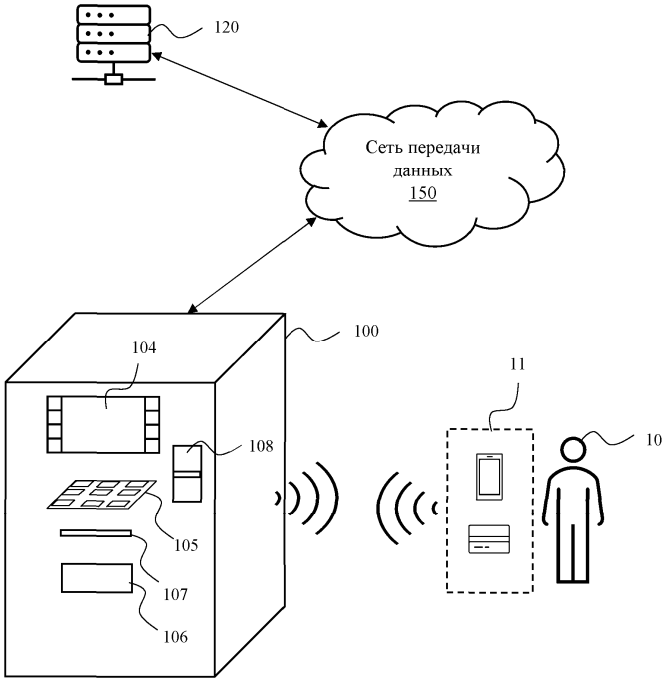
4. Способ по п.3, в котором дополнительно получают видеоданные клиента при работе с УС.

5. Способ по п.4, в котором фиксируют наличие событий повторной транзакции клиентом, не сформировавшем транзакционный запрос, и осуществляют зачисление ДС на карту клиента, сформировавшего транзакционный запрос.

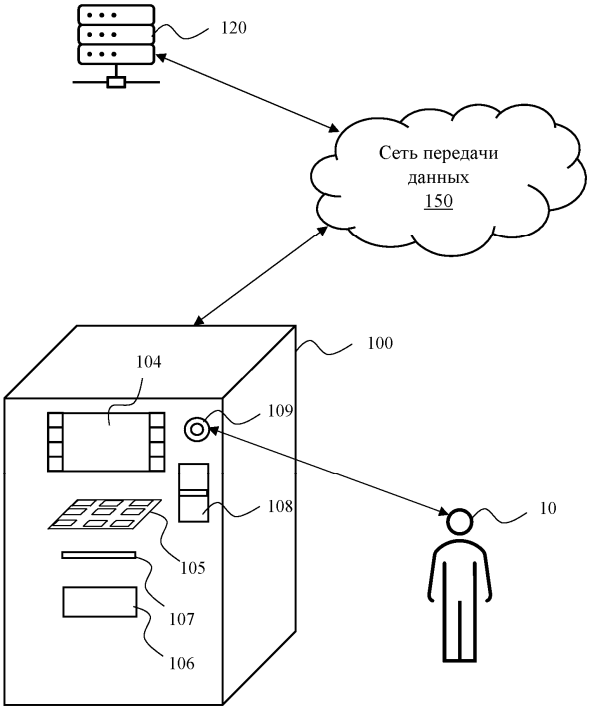
6. Система возврата ДС при отмене операции взноса наличных ДС в канале УС, содержащая по меньшей мере один процессор и по меньшей мере одно запоминающее устройство, хранящее машиночитаемые инструкции, которые при их исполнении процессором осуществляют способ по любому из пп.1-5.



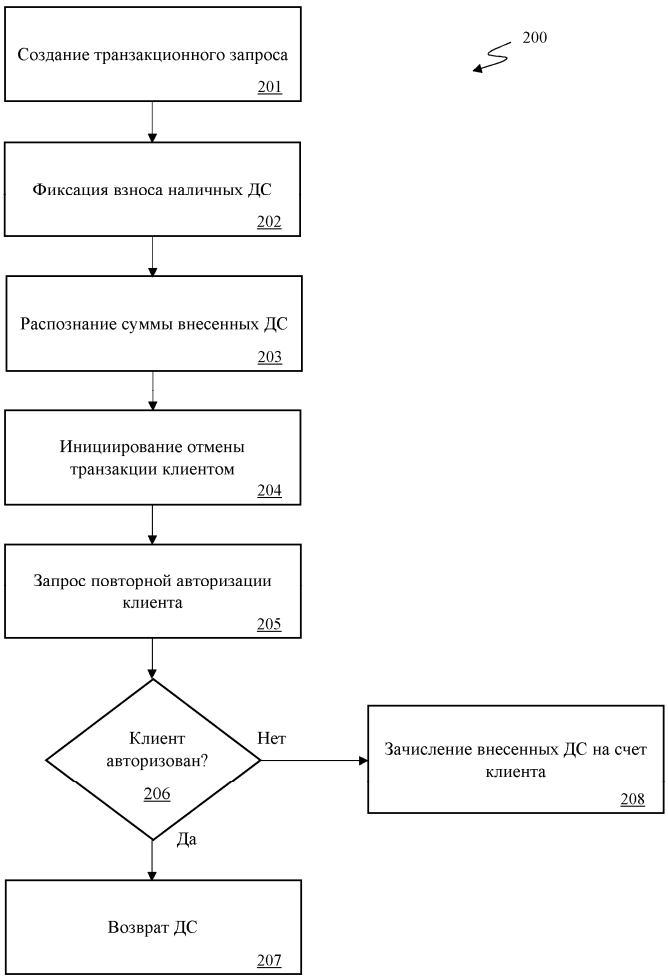
Фиг. 1А


120
Сеть передачи данных
150
100
104
108
105
107
106
11
10

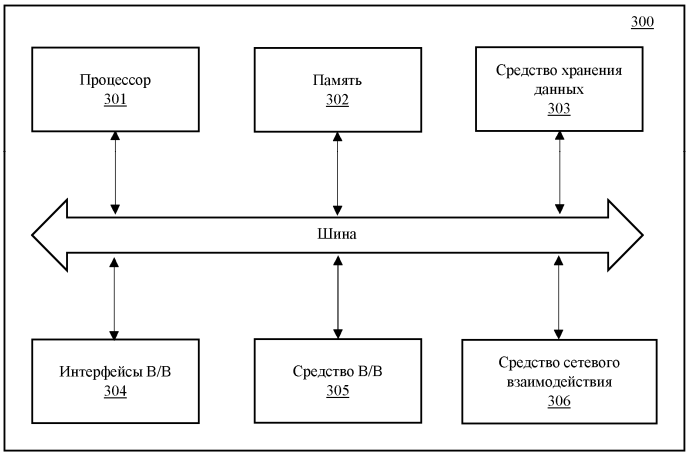
Фиг. 1Б


120
Сеть передачи данных
150
100
104
109
108
105
107
106
10

Фиг. 1В


200
Создание транзакционного запроса
201
Фиксация взноса наличных ДС
202
Распознание суммы внесенных ДС
203
Инициирование отмены транзакции клиентом
204
Запрос повторной авторизации клиента
205
Клиент авторизован?
206
Нет
Зачисление внесенных ДС на счет клиента
208
Да
Возврат ДС
207

Фиг. 2


300
Процессор
301
Память
302
Средство хранения данных
303
Шина
Интерфейсы В/В
304
Средство В/В
305
Средство сетевого взаимодействия
306

Фиг. 3