РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 728 828**(13) **C2**

(51) МПК
*G06F 21/40* (2013.01)
*G06Q 20/40* (2012.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
*G06F 21/40 (2019.05); G06Q 20/40145 (2019.05); G06Q 20/4016 (2019.05); G06Q 20/322 (2019.05); H04L 9/0838 (2019.05); H04L 9/0891 (2019.05); H04L 9/3268 (2019.05)*

(21)(22) Заявка: **2018138709, 02.11.2018**

(24) Дата начала отсчета срока действия патента:
**02.11.2018**

Дата регистрации:
**31.07.2020**

Приоритет(ы):
(30) Конвенционный приоритет:
**03.11.2017 US 15/803,519**

(43) Дата публикации заявки: **19.05.2020** Бюл. № **14**

(45) Опубликовано: **31.07.2020** Бюл. № **22**

Адрес для переписки:
**129090, Москва, ул. Б. Спасская, 25, стр. 3, ООО "Юридическая фирма Городисский и Партнеры"**

(72) Автор(ы):
**ПИЛ Брайан (US)**

(73) Патентообладатель(и):
**МАСТЕРКАРД ИНТЕРНЭШНЛ ИНКОРПОРЕЙТЕД (US)**

(56) Список документов, цитированных в отчете о поиске: **US 2013/0232073 A1, 05.09.2013. US 8572391 B2, 29.10.2013. US 8793777 B2, 29.07.2014. RU 2014138193 A, 20.05.2016.**

## (54) Системы и способы для аутентификации пользователя на основании биометрических данных и данных устройства

(57) Реферат:

Изобретение относится к области вычислительной техники. Техническим результатом является обеспечение аутентификации пользователя. Раскрыта система контроллера данных (DC) для аутентификации пользователя, содержащая одно или более вычислительных устройств контроллера данных (DC), причем одно или более вычислительных устройств DC содержат по меньшей мере один процессор и память, при этом одно или более вычислительных устройств DC выполнены с возможностью: принимать, как часть процесса регистрации пользователя для цифрового кошелька, первые данные криптографического ключа, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства и первый идентификатор счета; сохранять первые данные криптографического ключа в базе данных, которая находится на связи с упомянутыми одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа; принимать сообщение запроса аутентификации для платежной транзакции, включающей в себя вторые данные криптографического ключа, причем вторые данные криптографического ключа включают в себя второй идентификатор устройства и второй идентификатор счета; соотносить вторые данные криптографического ключа с историческими данными криптографического ключа; определять оценку мошенничества для платежной транзакции, при этом оценка мошенничества определяется на основе упомянутого соотнесения данных криптографических ключей; автоматически



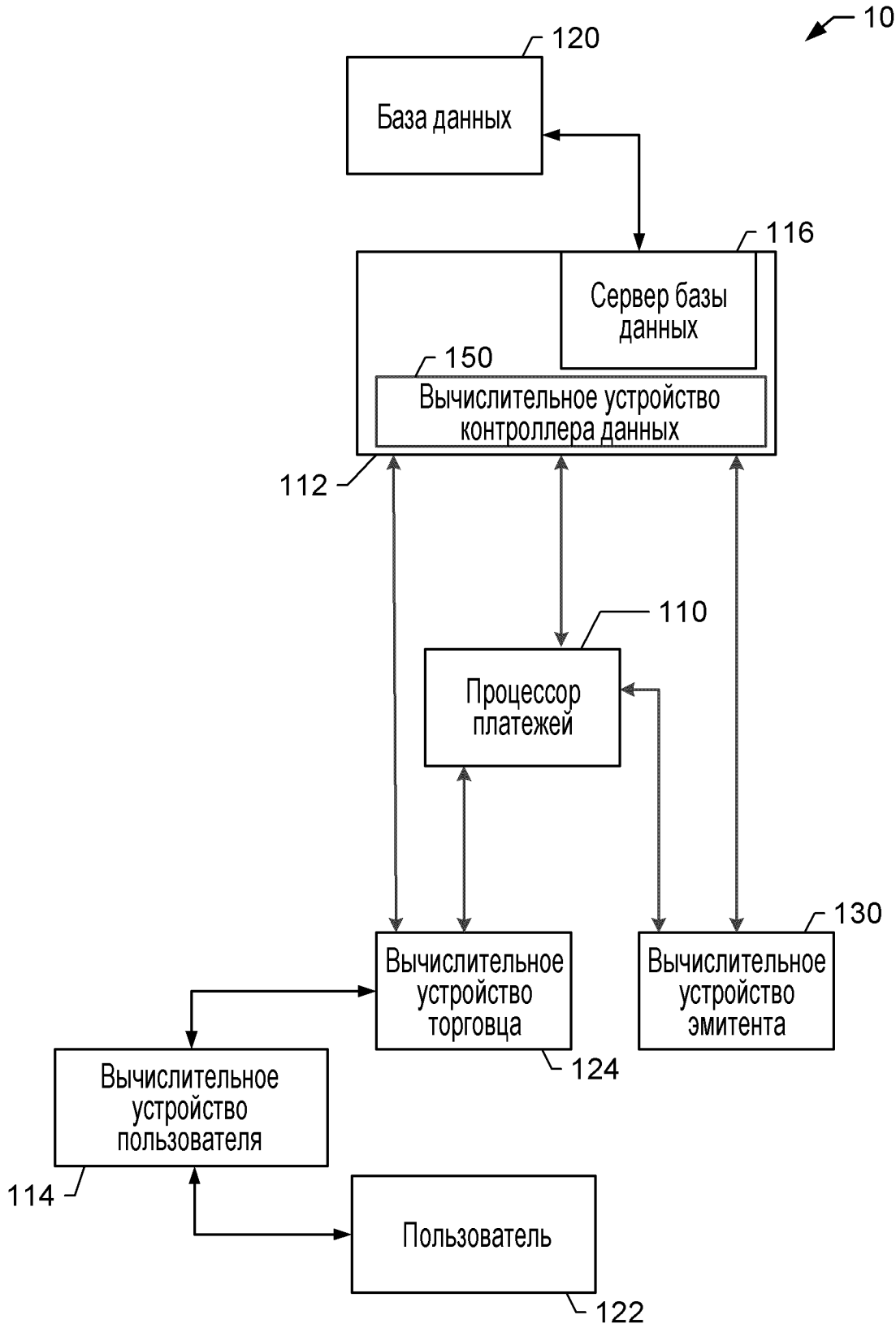
RU 2728828 C2

RU 2728828 C2

генерировать сообщение ответа аутентификации в ответ на сообщение запроса аутентификации, причем сообщение ответа аутентификации включает в себя оценку мошенничества; передавать сообщение ответа аутентификации; принимать третьи данные криптографического ключа, причем третьи данные криптографического ключа относятся к ранее одобренному запросу аутентификации; определять, что третьи данные криптографического ключа не согласуются с историческими данными криптографического ключа из упомянутого процесса регистрации пользователя для цифрового кошелька; и расширять исторические данные криптографического ключа включением в них третьих данных криптографического ключа. 3 н. и 17 з.п. ф-лы, 7 ил.

RU 2728828 C2

RU 2728828 C2




ФИГ. 1

RU 2728828 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 728 828**(13) **C2**

(51) Int. Cl.
*G06F 21/40* (2013.01)
*G06Q 20/40* (2012.01)

## (12) ABSTRACT OF INVENTION

(52) CPC
*G06F 21/40 (2019.05); G06Q 20/40145 (2019.05); G06Q 20/4016 (2019.05); G06Q 20/322 (2019.05); H04L 9/0838 (2019.05); H04L 9/0891 (2019.05); H04L 9/3268 (2019.05)*

(21)(22) Application: **2018138709, 02.11.2018**

(24) Effective date for property rights:
**02.11.2018**

Registration date:
**31.07.2020**

Priority:
(30) Convention priority:
**03.11.2017 US 15/803,519**

(43) Application published: **19.05.2020** Bull. № **14**

(45) Date of publication: **31.07.2020** Bull. № **22**

Mail address:
**129090, Moskva, ul. B. Spasskaya, 25, str. 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"**

(72) Inventor(s):
**PIEL, Brian (US)**

(73) Proprietor(s):
**MASTERCARD INTERNATIONAL INCORPORATED (US)**

RU 2728828 C2

### (54) SYSTEMS AND METHODS FOR USER AUTHENTICATION BASED ON BIOMETRIC DATA AND DEVICE DATA

(57) Abstract:

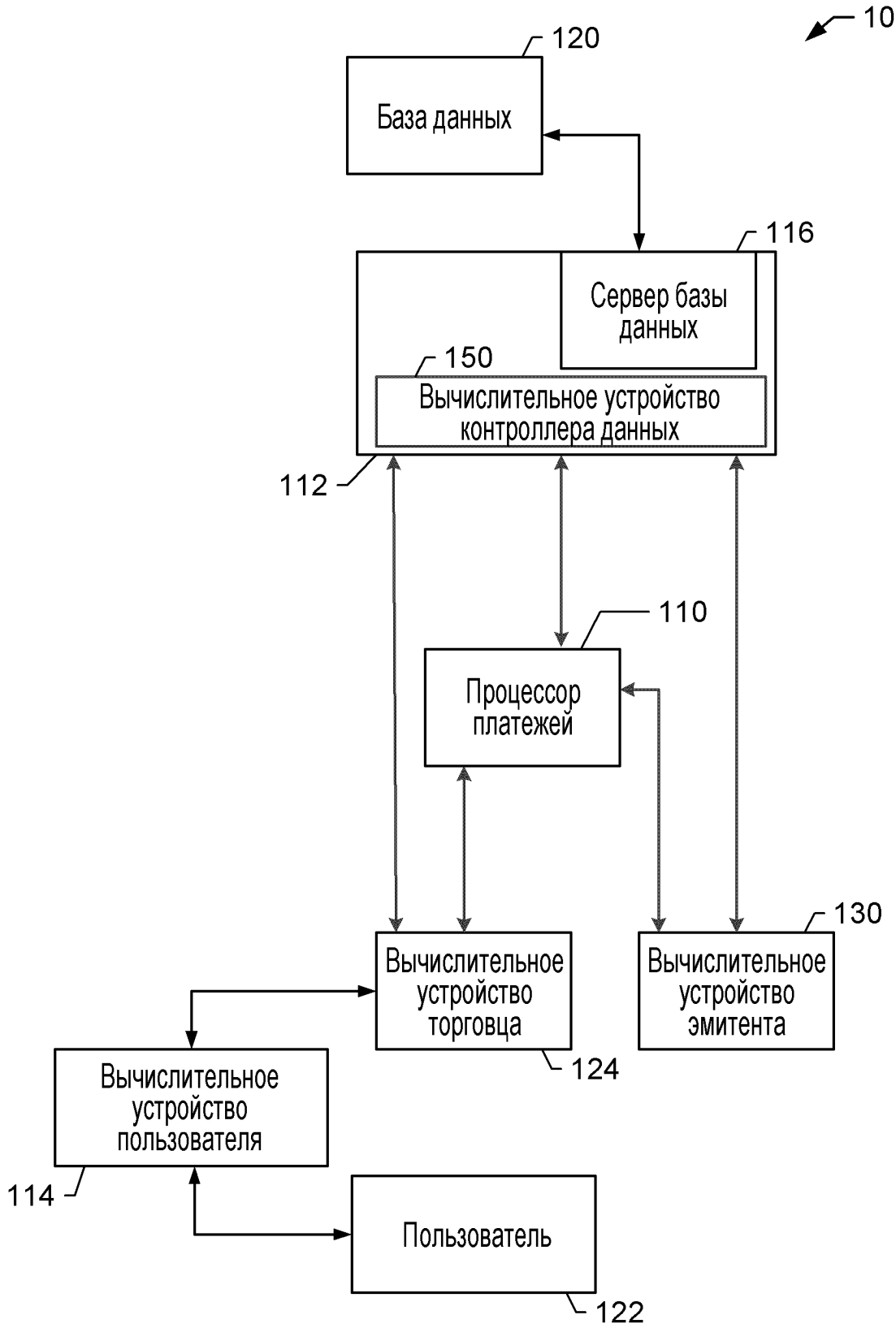
FIELD: computer equipment.

SUBSTANCE: disclosed is a data controller (DC) system for user authentication, comprising one or more data controller (DC) computing devices, wherein one or more DC computing devices comprise at least one processor and memory, wherein one or more DC computing devices are configured to: receive, as part of user registration process for digital wallet, first cryptographic key data including encrypted biometric data on device, a first device identifier and a first account identifier; store first data of cryptographic key in database, which is in communication with said one or more DC computing devices, as historical data of cryptographic key; receive authentication request message for payment transaction, including cryptographic key second data, wherein the second cryptographic key data includes a second device identifier and a second account identifier; correlate second cryptographic key data with cryptographic key historical data; determine a fraud score for a payment transaction, wherein evaluation of fraud is determined based on said correlation of cryptographic keys data; automatically generate an authentication response message in response to the authentication request message, wherein the authentication response message includes a fraud estimate; transmit an authentication response message; receive third cryptographic key data, wherein the third cryptographic key data refer to the previously approved authentication request; determining that the third cryptographic key data are not consistent with the cryptographic key historical data from the user registration process for the digital wallet; and expand cryptographic key historical data by including third cryptographic key data therein.

EFFECT: technical result is providing user authentication.

20 cl, 7 dwg

RU 2728828 C2




ФИГ. 1

RU 2728828 C2

## ПРЕДПОСЫЛКИ СОЗДАНИЯ ИЗОБРЕТЕНИЯ

[0001] Область техники настоящего изобретения относится, в целом, к сетям, и, более конкретно, к системам и сетям для аутентификации пользователя посредством соотнесения зашифрованных биометрических данных на устройстве с контекстными транзакционными данными и данными устройства, ассоциированными с устройством пользователя.

[0002] По меньшей мере, некоторые известные системы обработки платежей включают обмен некоторым числом сообщений сети платежной карты между торговцем, пользователем или держателем карты, эквайером, и эмитентом, зарегистрированными в многосторонней модели сети взаимного обмена. Эти компьютерные сообщения могут включать в себя несколько атрибутов транзакции, такие как, но не ограничивающиеся, авторизации, извещения, сторнирования, возвраты покупок и возвраты платежей, первичные номера счета, суммы транзакции, идентификаторы торговца, идентификаторы эквайера, дата-время транзакции, и верификации адреса.

[0003] Некоторые из этих известных систем обработки платежей могут использовать аутентификацию, основанную на реберном представлении графа, которая использует мандат, такой как биометрические данные, которые хранятся и удостоверяются внутри вычислительного устройства пользователя, чтобы аутентифицировать пользователя как законного держателя карты. Этот мандат может быть зафиксирован, используя биометрическую технологию, такую как устройства чтения отпечатка пальца. Тем не менее, поскольку проверка достоверности происходит вне платежной сети (например, на вычислительном устройстве пользователя), эмитент платежной карты может не иметь возможности видеть результат аутентификаций и ему может быть приписана ответственность за мошенничество в отношении покупки без непосредственной аутентификации пользователя. Таким образом, эмитент действительно не уверен в том, что ему был предоставлен мандат пользователя/держателя карты, и полагается только на третью сторону, такую как торговец, в обеспечении проверки достоверности такого мандата.

[0004] Соответственно, преимущественным будет наличие системы, которая позволяет сторонам, включенным в онлайновую платежную транзакцию, таким как эмитент или любая сторона, заинтересованная в аутентификации онлайнового пользователя, подтверждать то, что биометрическая аутентификация, выполненная посредством вычислительного устройства пользователя, является аутентичной, без запроса предоставления пользователем таких биометрических данных каждый и любой раз, когда пользователь совершает покупку и/или желает осуществить доступ к данным счета пользователя.

## КРАТКОЕ ОПИСАНИЕ

[0005] В одном аспекте, предоставляется система контроллера данных (DC), включающая в себя одно или более вычислительные устройства контроллера данных (DC) для аутентификации пользователя. Одно или более вычислительные устройства DC включают в себя процессор, коммуникативно связанный с памятью. Система DC выполнена с возможностью приема первых данных криптографического ключа, ассоциированных с первой транзакцией, включающих в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства, и первый идентификатор счета, сохранения первых данных криптографического ключа в базе данных, которая находится на связи с одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа, и приема сообщения запроса аутентификации для второй транзакции, включающей в себя вторые данные

криптографического ключа, которые включают в себя второй идентификатор устройства, и второй идентификатор счета. Система DC также выполнена с возможностью соотнесения вторых данных криптографического ключа с историческими данными криптографического ключа. Система DC дополнительно выполнена с возможностью определения оценки мошенничества для второй транзакции, при этом оценка мошенничества определяется на основе соотнесения криптографического ключа и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета, автоматического генерирования сообщения ответа аутентификации в ответ на сообщение запроса аутентификации, включающего в себя оценку мошенничества, и передачи сообщения ответа аутентификации.

[0006] В другом аспекте, предоставляется реализуемый компьютером способ для аутентификации пользователя. Способ выполняется, используя одно или более вычислительные устройства контроллера данных (DC), которые включают в себя, по меньшей мере, один процессор, который находится на связи с, по меньшей мере, одной памятью. Способ включает в себя этапы, на которых: принимают первые данные криптографического ключа, ассоциированные с первой транзакцией, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства, и первый идентификатор счета; сохраняют первые данные криптографического ключа в базе данных, которая находится на связи с одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа; и принимают сообщение запроса аутентификации для второй транзакции, включающей в себя вторые данные криптографического ключа, которые включают в себя второй идентификатор устройства, и второй идентификатор счета. Способ также включает в себя этап, на котором соотносят вторые данные криптографического ключа с историческими данными криптографического ключа. Способ дополнительно включает в себя этапы, на которых: определяют оценку мошенничества для второй транзакции, при этом оценка мошенничества определяется на основе соотнесения криптографического ключа и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета; автоматически генерируют сообщение ответа аутентификации в ответ на сообщение запроса аутентификации, включающее в себя оценку мошенничества; и передают сообщение ответа аутентификации.

[0007] В еще одном другом аспекте, предоставляется не-временный машиночитаемый носитель информации, который включает в себя исполняемые инструкции для аутентификации пользователя. Когда исполняемые компьютером инструкции исполняются посредством одного или более вычислительных устройств контроллера данных (DC), которые включают в себя, по меньшей мере, один процессор, который находится на связи с, по меньшей мере, одним устройством памяти, исполняемые компьютером инструкции предписывают одному или более вычислительным устройствам DC принимать первые данные криптографического ключа, ассоциированные с первой транзакцией, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства, и первый идентификатор счета, сохранять первые данные криптографического ключа в базе данных, которая находится на связи с одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа, и принимать сообщение запроса аутентификации для второй транзакции, включающей в себя вторые данные криптографического ключа, которые включают в себя второй идентификатор устройства, и второй идентификатор счета. Система DC также выполнена с

возможностью соотнесения вторых данных криптографического ключа с историческими данными криптографического ключа. Система DC дополнительно выполнена с возможностью определения оценки мошенничества для второй транзакции, при этом оценка мошенничества определяется на основе соотнесения криптографического ключа и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета, автоматического генерирования сообщения ответа аутентификации в ответ на сообщение запроса аутентификации, включающее в себя оценку мошенничества, и передачи сообщения ответа аутентификации.

## КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0008] Фиг. 1-7 показывают примерные варианты осуществления способов и систем, описываемых в данном документе.

[0009] Фиг. 1 является упрощенной структурной схемой системы контроллера данных (DC), которая включает в себя одно или более вычислительные устройства DC, используемые для построения оценок мошенничества и аутентификации пользователя посредством соотнесения зашифрованных биометрических данных на устройстве с контекстными транзакционными данными и данными устройства в соответствии с одним вариантом осуществления настоящего изобретения.

[0010] Фиг. 2 является упрощенной структурной схемой примерного потока данных, используя систему DC, показанную на Фиг. 1, в соответствии с одним вариантом осуществления настоящего изобретения.

[0011] Фиг. 3 иллюстрирует примерную конфигурацию вычислительного устройства пользователя, показанного на Фиг. 2, в соответствии с одним вариантом осуществления настоящего изобретения.

[0012] Фиг. 4 иллюстрирует примерную конфигурацию серверной системы, показанной на Фиг. 2, в соответствии с одним вариантом осуществления настоящего изобретения.

[0013] Фиг. 5 является блок-схемой, показывающей процесс для построения оценок мошенничества посредством соотнесения зашифрованных биометрических данных на устройстве с контекстными транзакционными данными и данными устройства, используя систему, показанную на Фиг. 2.

[0014] Фиг. 6 является схемой компонентов одного или более вычислительных устройств, которые могут быть использованы в системе, показанной на Фиг. 2.

[0015] Фиг. 7 иллюстрирует примерную конфигурацию вычислительного устройства DC, в соответствии с одним вариантом осуществления настоящего изобретения.

## ПОДРОБНОЕ ОПИСАНИЕ

[0016] Настоящее изобретение относится к системе контроллера данных (DC) для аутентификации пользователя, и, более конкретно, онлайнового пользователя посредством соотнесения зашифрованных биометрических данных на устройстве с контекстными транзакционными данные и данными устройства, ассоциированными с устройством пользователя. В, по меньшей мере, некоторых реализациях, система DC включает в себя, по меньшей мере, одной вычислительное устройство DC и, по меньшей мере, одну базу данных. В одном варианте осуществления, база данных и вычислительное устройство DC являются компонентами серверной системы. Серверная система может быть сервером, сетью нескольких компьютерных устройств, виртуальным вычислительным устройством, или подобным. В некоторых вариантах осуществления, Вычислительное устройство DC находится на связи с вычислительным устройством процессора платежей. В других вариантах осуществления, вычислительное устройство DC интегрировано в или является частью вычислительного устройства процессора платежей. Вычислительное устройство DC также находится на связи с, по меньшей

мере, одним вычислительным устройством торговца и вычислительным устройством эмитента. В некоторых вариантах осуществления, вычислительное устройство DC соединено с, по меньшей мере, одним вычислительным устройством торговца и вычислительным устройством эмитента через процессор платежей. Вычислительное устройство DC также может находиться на связи с вычислительным устройством пользователя через электронную услугу, такую как электронное приложение.

[0017] Система DC не допускает мошеннические платежные транзакции посредством соотнесения зашифрованных биометрических данных на устройстве с контекстными транзакционными данными и данными устройства, ассоциированными с устройством пользователя и, более конкретно, посредством построения профиля счета пользователя, используя контекстные транзакционные данные и данные криптографического ключа, которые могут быть включены в зашифрованные биометрические данные на устройстве, идентификатор вычислительного устройства пользователя, и идентификатор счета (например, первичный номер счета (PAN). Конфигурация системы DC обеспечивает аутентификацию онлайнового пользователя эффективным образом посредством использования технологии для решения связанных с безопасностью вопросов и также вопросов простоты-использования. Например, система DC может использовать технологию простой аутентификации, такую как платежный шлюз, 3D Secure®, цифровой кошелек, контролируемого платежного номера, и онлайновую аутентификацию. Каждая из этих технологий может использовать аутентификацию, основанную на реберном представлении графа, которая использует мандат, такой как биометрические данные, которые хранятся, проверяются на достоверность, и шифруются внутри вычислительного устройства пользователя.

[0018] Даже несмотря на то, что некоторые известные системы обработки платежей пытаются обнаружить и предотвратить мошеннические платежные транзакции посредством использования предсказания или меры мошенничества, также известной как «оценка мошенничества», обнаружение может быть длительным и может не гарантировать предотвращения мошеннических платежных транзакций. При определении оценки предсказания мошенничества, эти известные системы могут использовать, например, биометрические данные пользователя, которые фиксируются и анализируются на вычислительном устройстве пользователя. Несмотря на то, что результаты анализа могут быть предоставлены эмитенту, эмитент может не быть уверен в том, что биометрическая аутентификация на вычислительном устройстве пользователя была выполнена правильно. Эти известные системы обнаружения мошенничества, которые используют биометрическую аутентификацию на вычислительном устройстве пользователя иногда аналогичны сценарию, где человек принимает телефонный вызов от торговца, который просит человека отправить деньги торговца от лица матери человека. Сценарий проходит следующим образом: человек принимает телефонный вызов от торговца, который говорит, «Эй, мне нужно, чтобы вы отправили мне 5000 долларов. Ваша мать стоит здесь передо мной и хочет купить этот предмет. Отправьте мне 5000 долларов». Человек отвечает, «Я хочу поговорить с мамой». Тем не менее, торговец отвечает, «Нет, я уже проверил ее ID. Не беспокойтесь об этом. Она ваша мама. Отправьте мне 5000 долларов». Человек с большой вероятностью положит трубку и не будет отправлять деньги. Сходным образом, в известных системах обнаружения мошенничества, где вычислительное устройство пользователя выполняет биометрическую аутентификацию, эмитент может не одобрить транзакцию. Эмитент предпочтет подтверждать то, что пользователь является аутентичным пользователем счета, с которого торговец пытается получить средства и не полагаться на другую

сторону, выполняющую аутентификацию. Эти системы обладают рядом серьезных ограничений. В виду упомянутого ранее, требуется система, такая как система DC, которая не требует, чтобы несколько сторон подтверждали аутентификацию пользователя или дополнительных данных аутентификации, таких как биометрические данные, при этом гарантируя то, что пользователь является аутентифицированным. Такая система позволяет сторонам, включенным в транзакцию, пользоваться легко интегрируемыми процессами авторизации и аутентификации транзакции.

[0019] Система DC и, более конкретно, вычислительное устройство DC, выполнена с возможностью обмена данными криптографического ключа, как части процесса регистрации пользователя в электронной услуге. Вычислительное устройство DC также выполнено с возможностью построения оценки мошенничества, используя исторические данные транзакции и правила, запрограммированные в вычислительное устройство DC. Вычислительное устройство DC, сходным образом, способно сохранять один или более идентификаторы устройства (например, идентификатор вычислительного устройства пользователя) и один или более идентификаторы счета, используя зашифрованные биометрические данные на устройстве. Зашифрованные биометрические данные на устройстве являются зашифрованными биометрическими данными пользователя, которые сгенерированы вычислительным устройством пользователя. Биометрические данные пользователя могут включать в себя отпечатки пальцев пользователя, лицо, голос, радужную оболочку, или подобное. Вычислительное устройство пользователя может фиксировать биометрические данные пользователя посредством использования устройств чтения отпечатка пальца, средств распознавания лица, сканов радужной оболочки, отпечатков голоса, или сходных устройств обнаружения. Вычислительное устройство DC способно считывать зашифрованные биометрические данные на устройстве, при этом оставляя такие данные зашифрованными.

[0020] Вычислительное устройство DC также выполнено с возможностью приема данных криптографического ключа (например, идентификатора устройства, идентификатора счета пользователя) как части процесса регистрации пользователя в электронной услуге. Дополнительно или в качестве альтернативы, вычислительное устройство DC выполнено с возможностью приема данных криптографического ключа, включенных в сообщение запроса аутентификации. Электронная услуга может включать в себя электронное приложение, такое как цифровой кошелек, приложение торговца, приложение эмитента, или подобное. Пользователь может использовать вычислительное устройство пользователя, такое как интеллектуальный телефон, персональный компьютер, планшетный компьютер, настольный компьютер, лэптоп, или сходное вычислительное устройство, чтобы регистрироваться в электронной услуге. Вычислительное устройство может фиксировать биометрические данные пользователя посредством использования устройств чтения отпечатка пальцев, сканов радужной оболочки, отпечатков голоса, или сходных устройств обнаружения. Вычислительное устройство пользователя проверяет достоверность, шифрует, и сохраняет такие биометрические данные, и авторизует пользователя в отношении доступа к вычислительному устройству. Когда пользователь регистрируется в электронной услуге, вычислительное устройство DC и вычислительное устройство пользователя могут осуществлять обмен данными криптографического ключа. В некоторых вариантах осуществления, вычислительное устройство DC может выполнять данный обмен посредством использования платформы Быстрой Онлайн-Идентификации (FIDO). В других вариантах осуществления, вычислительное устройство DC может использовать

другой тип платформы.

[0021] В некоторых вариантах осуществления, данные криптографического ключа включают в себя зашифрованные биометрические данные на устройстве, идентификатор устройства и счета. Дополнительно или в качестве альтернативы, данные криптографического ключа включают в себя жетон и/или хеш-значение идентификатора счета, и/или биометрических данных. В некоторых вариантах осуществления, данные криптографического ключа ассоциированы с алгоритмом ассиметричного шифрования (например, RSA, шифрование открытого-закрытого ключа), так что данные криптографического ключа дешифруются, используя ключ отличный от ключа шифрования. Дополнительно или в качестве альтернативы, данные криптографического ключа могут включать в себя цифровую подпись (например, шифрование открытого ключа), так что данные криптографического ключа ассоциированы с закрытым ключом. В некоторых вариантах осуществления, данные криптографического ключа шифруются, используя сочетание ассиметричного и симметричного алгоритмов (например, DES, AES). В некоторых вариантах осуществления, данные криптографического ключа могут включать в себя данные подписания, ассоциированные с центром сертификации. Например, данные криптографического ключа могут включать в себя данные, зашифрованные, используя закрытый ключ центра сертификации.

[0022] Вычислительное устройство DC выполнено с возможностью приема и хранения данных криптографического ключа. Вычислительное устройство DC может хранить данные криптографического ключа в базе данных, используя идентификатор счета пользователя. В некоторых вариантах осуществления, вычислительное устройство DC выполнено с возможностью сохранения принятых данных криптографического ключа в качестве опорных данных криптографического ключа. Например, вычислительное устройство DC может сохранять данные криптографического ключа, принятые во время процесса регистрации, в качестве опорных данных криптографического ключа. Дополнительно или в качестве альтернативы, вычислительное устройство DC выполнено с возможностью сохранения журнала регистрации данных криптографического ключа, включая множество экземпляров данных криптографического ключа. Например, вычислительное устройство DC может сохранять журнал регистрации всех экземпляров данных криптографического ключа, принятых на основе идентификаторов платежной карты, так что ведется запись всех данных криптографического ключа, ассоциированных с идентификатором платежной карты. После того, как данные криптографического ключа сохраняются, вычислительное устройство DC может принимать одни или более данные криптографического ключа для одного и того же идентификатора счета. В некоторых вариантах осуществления, вычислительное устройство DC может принимать данные криптографического ключа как часть процесса транзакции. Таким образом, вычислительное устройство DC может принимать данные криптографического ключа наряду с контекстными транзакционными данными (например, информацией торговца, данными единицы учета запасов (SKU), относящимися к товарам или услугам, покупаемым пользователем, или подобное). Вычислительное устройство DC также выполнено с возможностью построения профиля для идентификатора счета пользователя посредством использования принятых данных криптографического ключа, ассоциированных с идентификатором счета пользователя.

[0023] В некоторых вариантах осуществления, вычислительное устройство DC может принимать данные криптографического ключа, которые включают в себя идентификатор вычислительного устройства пользователя, которые не ассоциированы с хранящимися данными криптографического ключа (например, незарегистрированное вычислительное

устройство пользователя). Вычислительное устройство DC может добавлять незарегистрированное вычислительное устройство пользователя в идентификатор счета пользователя и регистрировать такое вычислительное устройство в электронной услуге. В течение процесса регистрации, вычислительное устройство DC может осуществлять обмен данными криптографического ключа с компьютерным устройством пользователя, чтобы верифицировать то, что вычислительное устройство ассоциировано с зарегистрированным пользователем.

[0024] В других вариантах осуществления, данные криптографического ключа являются частью сообщения запроса аутентификации. В данном случае, незарегистрированное вычислительное устройство пользователя может не быть добавлено в идентификатор счета пользователя, и сообщение запроса аутентификации может быть отклонено. В еще одних других вариантах осуществления, вычислительное устройство DC может одобрять сообщение запроса аутентификации, когда зашифрованные биометрические данные на устройстве и идентификатор вычислительного устройства пользователя соотносятся с хранящимися зашифрованными биометрическими данные на устройстве и хранящимся идентификатором вычислительного устройства пользователя.

[0025] В еще одних других вариантах осуществления, вычислительное устройство DC выполнено с возможностью определения оценки мошенничества, указывающей вероятность мошеннической транзакции для сообщения запроса аутентификации. Вычислительное устройство DC может определять оценку мошенничества, используя исторические данные, ассоциированные с данными криптографического ключа пользователя, более конкретно, идентификатором счета пользователя. Исторические данные могут включать в себя исторические оценки мошенничества для таких идентификаторов счета. Вычислительное устройство DC выполнено с возможностью конкатенации исторических оценок мошенничества, чтобы получать единую оценку мошенничества, ассоциированную с идентификатором счета. Вычислительное устройство DC может использовать машину правил, чтобы определять, является ли оценка мошенничества высокой или низкой. Например, если оценка мошенничества для идентификатора счета, ассоциированного с сообщением запроса аутентификации, находится выше предварительно определенной пороговой величины оценки, но данные криптографического ключа, ассоциированные с сообщением запроса аутентификации, согласуются с историческими данными (например, появляются в исторических данных), вычислительное устройство DC может определять, что оценка мошенничества для сообщения запроса аутентификации является низкой, указывая уменьшенный риск мошеннической транзакции. И наоборот, если оценка мошенничества для идентификатора счета, ассоциированного с сообщением запроса аутентификации является низкой, но данные криптографического ключа, ассоциированные с сообщением запроса аутентификации не согласуются с историческими данными, вычислительное устройство DC может определять, что оценка мошенничества для сообщения запроса аутентификации является высокой, указывая высокий риск мошеннической транзакции.

[0026] В некоторых вариантах осуществления, вычислительное устройство DC выполнено с возможностью одобрения или отклонения сообщения запроса аутентификации посредством использования оценки мошенничества сообщения запроса аутентификации и сравнения ее с предварительно определенной пороговой величиной оценки. Вычислительное устройство DC может использовать машину правил, чтобы идентифицировать предварительно определенную пороговую величину оценки. Например, если сообщение запроса аутентификации имеет оценку мошенничества не

в пределах предварительно определенной пороговой величины оценки, вычислительное устройство DC может отклонять такое сообщение, если сообщение не включает в себя зашифрованные биометрические данные на устройстве. В противоположность, если сообщение запроса аутентификации имеет оценку в рамках предварительно определенной пороговой величины оценки, вычислительное устройство DC может одобрять такое сообщение, даже если сообщение не включает в себя зашифрованные биометрические данные на устройстве.

[0027] В некоторых вариантах осуществления, вычислительное устройство DC выполнено с возможностью сохранения данных криптографического ключа, ассоциированных с одобренным запросом аутентификации. В некоторых вариантах осуществления, где сообщение запроса аутентификации, одобренное вычислительным устройством DC, ассоциировано с принятыми данными криптографического ключа, не согласующимися с историческими данными криптографического ключа, вычислительное устройство DC выполнено с возможностью сохранения принятых данных криптографического ключа. Например, запрос аутентификации, ассоциированный с новым устройством, может быть законным, но включенные криптографические данные могут быть несогласующимися с историческими данными криптографического ключа, и вычислительное устройство DC может обновлять и/или расширять хранящиеся исторические данные криптографического ключа, чтобы они включали в себя данные криптографического ключа, ассоциированные с новым устройством так, что будущие запросы аутентификации, ассоциированные с новым устройством, включают в себя криптографические данные, согласующиеся с историческими криптографическими данными.

[0028] В некоторых вариантах осуществления, вычислительное устройство DC выполнено с возможностью одобрения сообщения запроса аутентификации на основе цены покупки (т.е., суммы транзакции). Например, если вычислительное устройство DC определяет, что оценка мошенничества, ассоциированная с идентификатором счета пользователя, является высокой, но сумма транзакции находится ниже предварительно определенной величины (например, 200 долларов США), и сообщение запроса аутентификации включает в себя зашифрованные биометрические данные на устройстве (т.е., данные криптографического ключа), вычислительное устройство DC может одобрять сообщение запроса аутентификации на основе данных криптографического ключа.

[0029] В альтернативных вариантах осуществления, вычислительное устройство DC выполнено с возможностью авторизации транзакции платежной карты, если сообщение запроса авторизации отвечает предварительно определенному набору правил от машины правил. В данном случае, вычислительному устройству DC может не требоваться осуществлять связь с вычислительным устройством эмитента перед авторизацией транзакции платежной карты.

[0030] В других вариантах осуществления, вычислительное устройство DC выполнено с возможностью сохранения оценки мошенничества для сообщения запроса аутентификации как только вычислительное устройство DC определяет такую оценку. В некоторых вариантах осуществления, вычислительное устройство DC сохраняет оценку мошенничества, в базе данных как часть исторических данных, на основе идентификатора счета пользователя, ассоциированного с оценкой мошенничества. В других вариантах осуществления, вычислительное устройство DC сохраняет оценку мошенничества, в базе данных в-памяти как часть исторических данных, на основе идентификатора счета пользователя, ассоциированного с оценкой мошенничества. В

примерном варианте осуществления, вычислительное устройство DC выполнено с возможностью построения таблицы оценок посредством анализа базы данных, нахождения одной или более оценок мошенничества, и добавления оценки в таблицу оценок. В некоторых вариантах осуществления, вычислительное устройство DC может добавлять оценки мошенничества в таблицу оценок посредством идентификатора счета пользователя. В других вариантах осуществления, вычислительное устройство DC может добавлять оценки мошенничества в таблицу оценок посредством любого другого типа идентификатора, хранящегося в базе данных. В альтернативных вариантах осуществления, вычислительное устройство DC может выполнять этапы, выполняемые в базе данных, как описано выше, в любой другой структуре данных, подходящей для хранения данных, такой как база данных в-памяти.

[0031] Вычислительное устройство DC дополнительно выполнено с возможностью приема одного или более запросов оценки мошенничества от одной или более запрашивающих сторон. Запрашивающими сторонами могут быть эмитент карты, поставщик услуги платежей (PSP), торговец, или любая другая запрашивающая сторона, которая может быть авторизована, чтобы принимать оценки мошенничества, ассоциированные с идентификатором счета пользователя. Вычислительное устройство DC может передавать ответ оценки мошенничества в ответ на запрос оценки мошенничества. Ответ оценки мошенничества может включать в себя идентификатор счета пользователя, конкатенированную оценку мошенничества, одну или более оценки мошенничества, соответствующие одному или более сообщениям запроса аутентификации (например, оценку мошенничества, которая была определена для сообщения запроса аутентификации), или любые другие данные счета пользователя, которые могут быть сохранены в таблице оценок и/или в базе данных.

[0032] В некоторых вариантах осуществления, вычислительное устройство DC выполнено с возможностью автоматического генерирования и передачи сообщения ответа аутентификации в ответ на одобренное сообщение запроса аутентификации. Как объяснялось выше, вычислительное устройство DC выполнено с возможностью одобрения сообщений запроса аутентификации на основе разных данных, таких как оценки мошенничества, цена покупки, идентификатор устройства, зашифрованные биометрические данные на устройстве, и данные криптографического ключа. Как только вычислительное устройство DC одобряет сообщение запроса аутентификации, вычислительное устройство DC автоматически генерирует и передает сообщение ответа аутентификации вычислительному устройству пользователя, вычислительному устройству торговца, и/или вычислительному устройству эмитента.

[0033] Способы и системы, описываемые в данном документе, могут быть реализованы используя методики компьютерного программирования или инженерного искусства, включая компьютерное программное обеспечение, встроенное программное обеспечение, аппаратное обеспечение, или любое сочетание или подмножество. Как раскрыто выше, по меньшей мере, одна техническая проблема предшествующих систем состоит в отсутствии улучшенного обнаружения мошенничества или невозможности подтверждения того, что транзакция не является мошеннической без повторного или дублирующего ввода определенной информации (такой как данные криптографического ключа) с каждой транзакцией (например, без запроса у пользователя предоставления биометрической информации каждый раз, когда пользователь совершает покупку или исполняет транзакцию). Системы и способы, описываемые в данном документе, решают эту техническую проблему использования данных криптографического ключа посредством использования его для построения профиля счета пользователя и сравнения

построенного профиля счета пользователя с данными криптографического ключа, принятыми чтобы аутентифицировать пользователя, пытающегося совершить покупку или исполнить транзакцию. Технический результат систем и процессов, описываемых в данном документе достигается посредством выполнения, по меньшей мере, одного из следующих этапов: (a) принимают первые данные криптографического ключа, ассоциированного с первой транзакцией, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства, и первый идентификатор счета; (b) сохраняют первые данные криптографического ключа в базе данных, которая находится на связи с одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа; (c) принимают сообщение запроса аутентификации для второй транзакции, включающее в себя вторые данные криптографического ключа, причем вторые данные криптографического ключа включают в себя второй идентификатор устройства, и второй идентификатор счета; (d) соотносят вторые данные криптографического ключа с историческими данными криптографического ключа; (e) определяют оценку мошенничества для второй транзакции, при этом оценка мошенничества определяется на основе соотнесения криптографического ключа и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета; (f) автоматически генерируют сообщение ответа аутентификации в ответ на сообщение запроса аутентификации, причем сообщение ответа аутентификации включает в себя оценку мошенничества; и (g) передают сообщение ответа аутентификации.

[0034] Используемые в данном документе понятия «карта транзакций», «карта финансовых транзакций», и «платежная карта» относятся к любой подходящей карте транзакций, такой как кредитная карта, дебетовая карта, предоплаченная карта, расчетная карта, членская карта, рекламная карта, карта часто летающего клиента, идентификационная карта, подарочная карта, и/или любому другому устройству, которое может удерживать информацию платежного счета, такому как мобильные телефоны, Интеллектуальные телефоны, персональные цифровые помощники (PDA), брелоки, и/или компьютеры. Каждый тип карты транзакций может быть использован в качестве способа платежа для выполнения транзакции.

[0035] В одном варианте осуществления, предоставляется компьютерная программа, и программа воплощается на машиночитаемом носителе информации. В примерном варианте осуществления, системы исполняется в единой компьютерной системе, не требуя соединения с серверным компьютером. В дополнительном примерном варианте осуществления, система работает в среде Windows® (Windows является зарегистрированным товарным знаком Microsoft Corporation, Редмонд, штат Вашингтон). В еще одном варианте осуществления, система работает в среде мэйфрейм и серверной среде UNIX® (UNIX является зарегистрированным товарным знаком X/Open Company Limited, которая располагается в Рединг, Беркшир, Великобритания). В дополнительном варианте осуществления, система работает в среде iOS® (iOS является зарегистрированным товарным знаком Apple Inc, расположенной в Купертино, штат Калифорния). В еще одном дополнительном варианте осуществления, система работает в среде MAC OS® (MAC OS является зарегистрированным товарным знаком Apple Inc, расположенной в Купертино, штат Калифорния). Приложение является гибким и разработанным для работы в разнообразных отличных средах без ущерба для любой основной функциональности. В некоторых вариантах осуществления, система включает в себя несколько компонентов, распределенных среди множества вычислительных устройств. Один или более компоненты находятся в форме исполняемых компьютером

инструкций, воплощенных на машиночитаемом носителе информации. Системы и процессы не ограничиваются конкретными вариантами осуществления, описываемыми в данном документе. В дополнение, компоненты каждой системы и каждого процесса могут быть воплощены на практике независимо и отдельно от других компонентов и процессов, описываемых в данном документе. Каждый компонент и процесс также может быть использован в сочетании с другими сборочными пакетами и процессами.

[0036] В одном варианте осуществления, предоставляется компьютерная программа, и программа воплощается на машиночитаемом носителе информации и использует Язык Структурированных Запросов (SQL) с клиентской частью интерфейса пользователя для администрирования и web-интерфейсом для стандартного ввода пользователя и отчетов. В другом варианте осуществления система является с web-поддержкой и работает в интрасети коммерческой организации. В еще одном другом варианте осуществления, система является полностью доступной посредством индивидуумов с авторизованным доступом вне брандмауэра коммерческой организации через Интернет. В дополнительном варианте осуществления, система работает в среде Windows® (Windows является зарегистрированным товарным знаком Microsoft Corporation, Редмонд, штат Вашингтон). Приложение является гибким и разработанным для работы в разнообразных отличных средах без ущерба для любой основной функциональности.

[0037] Используемый в данном документе элемент или этап, перечисленный в форме единственного числа, следует понимать как не исключающий множество элементов или этапов, при условии, что такое исключение не сформулировано в явной форме. Кроме того, ссылки на «примерный вариант осуществления» или «один вариант осуществления» настоящего изобретения не следует толковать как исключающие существование дополнительных вариантов осуществления, которые также включают перечисленные признаки.

[0038] Используемое в данном документе понятие «база данных» может относиться к либо совокупности данных, системе администрирования реляционной базы данных (RDBMS), либо как к тому, так и другому. База данных может включать в себя любую коллекцию данных, включая иерархические базы данных, реляционные базы данных, базы данных с двумерным файлом, объектно-реляционные базы данных, объектно-ориентированные базы данных, и любую другую структурированную коллекцию записей или данных, которая хранится в компьютерной системе. Вышеприведенные примеры являются, только для примера, и, таким образом, не предназначены для того, чтобы ограничивать каким-либо образом определение и/или значение понятия база данных. Примеры RDBMS включают в себя, но не ограничиваются включением Oracle® Database, MySQL, IBM® DB2, Microsoft® SQL Server, Sybase®, и PostgreSQL. Тем не менее, может быть использована любая база данных, которая обеспечивает систему и способы, описанные в данном документе. (Oracle является зарегистрированным товарным знаком Oracle Corporation, Редвуд Шорз, штат Калифорния; IBM является зарегистрированным товарным знаком International Business Machines Corporation, Армонк, штат Нью-Йорк; Microsoft является зарегистрированным товарным знаком Microsoft Corporation, Редмонд, штат Вашингтон; и Sybase является зарегистрированным товарным знаком Sybase, Дублин, штат Калифорния).

[0039] Понятие процессор, используемое в данном документе, может относиться к центральным блокам обработки, микропроцессорам, микроконтроллерам, схемам с сокращенным набором инструкций (RISC), проблемно-ориентированным интегральным микросхемам (ASIC), логическим схемам, и любой другой схеме или процессору, выполненному с возможностью исполнения функций, описываемых в данном документе.

[0040] Используемые в данном документе понятия «программное обеспечение» и «встроенное программное обеспечение» являются взаимозаменяемыми, и включают в себя любую компьютерную программу, хранящуюся в памяти для исполнения посредством процессора, включая память RAM, память ROM, память EPROM, память EEPROM, и память энергонезависимой RAM (NRAM). Вышеприведенные типы памяти являются только для примера, и, таким образом, не ограничиваются типами памяти, используемыми для хранения компьютерной программы.

[0041] Фиг. 1 является упрощенной структурной схемой примерной системы 100 контроллера данных (DC), в которой многообразие вычислительных устройств коммуникативно связаны друг с другом через множество сетевых соединений. Эти сетевые соединения могут быть Интернетом, LAN/WAN, или другими соединениями, выполненными с возможностью передачи данных по вычислительным устройствам. Система 100 DC включает в себя вычислительное устройство 150 контроллера данных (DC) и сервер 116 базы данных. В одном варианте осуществления, вычислительное устройство 150 DC и база 116 данных являются компонентами серверной системы 112. Серверная система 112 может быть сервером, сетью из нескольких компьютерных устройств, виртуальным вычислительным устройством, или подобным. Вычислительное устройство 150 DC может быть соединено с, по меньшей мере, одним вычислительным устройством 124 торговца, и вычислительным устройством 130 эмитента через, по меньшей мере, процессор 110 платежей.

[0042] Сервер 116 базы данных соединен с базой 120 данных, которая содержит информацию по целому ряду вопросов, как описывается ниже более подробно. В одном варианте осуществления, база 120 данных хранится в серверной системе 112 и доступ к ней может быть осуществлен посредством потенциальных пользователей серверной системы 112. В альтернативном варианте осуществления, база 120 данных хранится удаленно от серверной системы 112 и может быть нецентрализованной. База 120 данных может включать в себя единую базу данных с отдельными разделами или фрагментами, или может включать в себя несколько баз данных, причем каждая является отдельной друг от друга. База 120 данных находится на связи с вычислительным устройством 150 DC и может хранить данные криптографического ключа и оценки мошенничества, ассоциированные со счетом пользователя 122.

[0043] В других вариантах осуществления, вычислительное устройство 150 DC выполнено с возможностью приема контекстных транзакционных данных от вычислительного устройства 124 торговца, через процессор 110 платежей. Когда пользователь 122 выполняет транзакцию в местоположении торговца, генерируются контекстные транзакционные данные. Контекстные транзакционные данные могут быть переданы по вычислительным устройствам в качестве сообщения запроса аутентификации. В одном варианте осуществления, когда пользователь выполняет транзакцию на вычислительном устройстве 124 торговца, ассоциированном с торговцем, контекстные транзакционные данные применительно к транзакции передаются серверной системе 112. Серверная система 112 обрабатывает контекстные транзакционные данные и также передает их вычислительному устройству 150 DC.

[0044] Контекстные транзакционные данные могут включать в себя сумму транзакции, дату транзакции, данные счета, которые относятся к платежной карте, использованной для выполнения транзакции (например, PAN Ассоциированный с платежной картой, дату окончания срока действия карты, эмитента карты, код безопасности карты, или подобное), идентификатор торговца, данные единицы учета запасов (SKU), которые относятся к товарам и услугам, покупаемым пользователем, и подобное. В некоторых

вариантах осуществления, контекстные транзакционные данные также могут включать в себя данные криптографического ключа. В других вариантах осуществления, вычислительное устройство 150 DC выполнено с возможностью приема данных криптографического ключа как часть процесса регистрации пользователя в электронной услуге. Электронная услуга может включать в себя электронное приложение, такое как цифровой кошелек, приложение торговца, приложение эмитента, или подобное.

[0045] В некоторых вариантах осуществления, данные криптографического ключа включают в себя зашифрованные биометрические данные на устройстве, идентификатор вычислительного устройства 114 пользователя, и идентификатор счета пользователя 122 (например, персональный номер счета (PAN) платежной карты). Дополнительно или в качестве альтернативы, данные криптографического ключа включают в себя жетон и/или хеш-значение идентификатора счета, и/или биометрические данные. В некоторых вариантах осуществления, данные криптографического ключа ассоциированы с алгоритмом ассиметричного шифрования (например, RSA, шифрование открытого-закрытого ключа), так что данные криптографического ключа дешифруются, используя ключ отличный от ключа шифрования. Дополнительно или в качестве альтернативы, данные криптографического ключа могут включать в себя цифровую подпись (например, шифрование открытого ключа), так что данные криптографического ключа ассоциированы с закрытым ключом. Например, вычислительное устройство 150 DC может быть сконфигурировано, чтобы определять идентификатор закрытого ключа, ассоциированного с данными криптографического ключа. В некоторых вариантах осуществления, данные криптографического ключа шифруются, используя сочетание ассиметричного и симметричного алгоритмов (например, DES, AES). В некоторых вариантах осуществления, данные криптографического ключа могут включать в себя данные подписания, ассоциированные с центром сертификации. Например, данные криптографического ключа могут включать в себя данные, зашифрованные, используя закрытый ключ центра сертификации, и вычислительное устройство 150 DC может быть выполнено с возможностью определения идентификатора центра сертификации.

[0046] В некоторых вариантах осуществления, вычислительное устройство 150 DC принимает сообщение запроса аутентификации, которое может включать в себя данные криптографического ключа наряду с контекстными транзакционными данными (например, информацией торговца, данными единицы учета запасов (SKU), которые относятся к товарам и услугам, покупаемым пользователем 122, или подобное). Вычислительное устройство 150 DC также выполнено с возможностью сохранения данных криптографического ключа в базе 120 данных на основе идентификатора счета, ассоциированного с пользователем 122. В некоторых вариантах осуществления, база 120 данных выполнена с возможностью сохранения информации ассиметричного ключа, такой как открытого/закрытого ключей, и/или идентификаторов (например, хеш-значений, порядковых номеров) открытого/закрытого ключей. Вычислительное устройство 150 DC дополнительно выполнено с возможностью приема одного или более сообщений запроса аутентификации, которые могут включать в себя данные криптографического ключа, которые также могут включать в себя идентификатор вычислительного устройства 114 пользователя, и идентификатор счета пользователя 122.

[0047] Вычислительное устройство 150 DC также выполнено с возможностью хранения данных криптографического ключа, включенных в одно или более сообщения запроса аутентификации, и соотнесения хранящихся данных криптографического ключа с данными криптографического ключа, включенными в принятые сообщения запроса

аутентификации. Вычислительное устройство 150 DC может осуществлять поиск по базе 120 данных, используя идентификатор счета пользователя 122, чтобы соотносить хранящиеся данные криптографического ключа с принятыми данными криптографического ключа. В одном варианте осуществления, вычислительное устройство 150 DC выполнено с возможностью определения идентификатора (например, хеш-значения, порядкового номера) ассиметричного ключа, ассоциированного с данными криптографического ключа, и соотнесения идентификатора с хранящимися данными криптографического ключа. Дополнительно или в качестве альтернативы, вычислительное устройство 150 DC выполнено с возможностью определения идентификатора центра сертификации, ассоциированного с данными криптографического ключа, и соотнесения идентификатора с хранящимися данными криптографического ключа. Например, вычислительное устройство 150 DC может определять, что принятые данные криптографического ключа ассоциированы с тем же самым ключом, как и хранящиеся данные криптографического ключа.

[0048] В примерном варианте осуществления, вычислительное устройство 150 DC выполнено с возможностью определения оценки мошенничества для сообщения запроса аутентификации. Вычислительное устройство DC определяет такую оценку мошенничества, используя соотнесение криптографического ключа и исторические данные, ассоциированные с идентификатором счета пользователя 122. Вычислительное устройство 150 DC дополнительно выполнено с возможностью построения таблицы оценок для счета пользователя 122. Вычислительное устройство 150 DC строит таблицу оценок посредством анализа исторических данных для счета пользователя 122, нахождения одной или более оценок мошенничества для счета пользователя 122, и добавления одной или более оценки мошенничества в таблицу оценок. Вычислительное устройство DC также выполнено с возможностью генерирования оценки мошенничества для счета пользователя 122 посредством конкатенации множества оценок мошенничества, хранящихся в таблице оценок, ассоциированной со счетом пользователя 122. Вычислительное устройство 150 DC также выполнено с возможностью сохранения сгенерированной оценки мошенничества в базе 120 данных, и автоматического генерирования сообщения ответа аутентификации в ответ на сообщение запроса аутентификации. Вычислительное устройство 150 DC также может автоматически генерировать сообщение ответа аутентификации если вычислительное устройство 150 DC определяет, что сообщение запроса аутентификации не является мошенническим. Вычислительное устройство 150 DC может определять, что сообщение запроса аутентификации не является мошенническим, посредством сравнения разных данных с предварительно определенными пороговыми величинами. Вычислительное устройство 150 DC может использовать машину правил, чтобы идентифицировать предварительно определенную пороговую величину времени. Такие разные данные могут включать в себя оценки мошенничества, соотнесение криптографического ключа, и/или цену покупки. Вычислительное устройство 150 DC также может определять, что сообщение запроса аутентификации не является мошенническим посредством сравнения идентификатора вычислительного устройства 114 пользователя и зашифрованных биометрических данных на устройстве пользователя 122, включенных в сообщение запроса аутентификации, с хранящимися вычислительным устройством и биометрическими данными на устройстве, ассоциированными с пользователем 122.

[0049] Вычислительное устройство 150 DC дополнительно выполнено с возможностью передачи сообщения ответа аутентификации вычислительному устройству 114 пользователя, вычислительному устройству 124 торговца, вычислительным устройствам

130 эмитента, и/или любым другим вычислительным устройствам, авторизованным для приема сообщения ответа аутентификации.

[0050] В примерном варианте осуществления, вычислительное устройство 150 DC включает в себя специально разработанное компьютерное аппаратное обеспечение, чтобы выполнять этапы, описываемые в данном документе, и включает в себя специально разработанные инструкции компьютерной реализации. Вычислительное устройство 150 DC является специально разработанным и адаптированным вычислительным устройством, построенным чтобы выполнять особую функцию в виде построения оценок мошенничества посредством соотнесения зашифрованных биометрических данных на устройстве с транзакционными данными и данными устройства.

[0051] Фиг. 2 является упрощенной структурной схемой примерного потока 200 данных, использующего систему 100 контроллера данных (DC). Варианты осуществления, описываемые в данном документе, могут относиться к системе карты транзакции, такой как платежная система кредитной и/или дебетовой карты, использующей сеть взаимного обмена Mastercard®. Сеть взаимного обмена Mastercard® является набором собственных стандартов связи, опубликованных Mastercard International Incorporated® для обмена данными финансовой транзакции и расчета по средствам между финансовыми учреждениями, которые являются членами Mastercard International Incorporated®. (Mastercard является зарегистрированным товарным знаком Mastercard International Incorporated, которая располагается в Перчейз, штат Нью-Йорк).

[0052] В типичной системе карты транзакций, финансовое учреждение, именуемое «эмитентом» выпускает карту транзакций или идентификатор счета электронных платежей, такую как кредитная карта, покупателю или пользователю 122, который использует карту транзакций для внесения платежа за покупку через вычислительное устройство 124 торговца, которое может быть терминалом точки продажи (POS). Чтобы одобрить платеж с помощью карты транзакций, вычислительное устройство 124 торговца должно обычно создавать счет в финансовом учреждении, которое является частью финансовой платежной системы. Данное финансовое учреждение обычно именуется «банком торговца», «банком-эквайером», или «эквайером». Когда пользователь 122 вносит платеж за покупку с помощью карты транзакций, вычислительное устройство 124 торговца запрашивает авторизацию у банка торговца на сумму покупки. Запрос может быть выполнен по телефону, но обычно выполняется посредством использования вычислительного устройства 124 торговца, которое считывает информацию счета пользователя 122 с магнитной ленты, чипа, двумерного кода, или тисненых символов на карте транзакций и осуществляет связь электронным образом с компьютерами обработки транзакций банка торговца, ассоциированного с вычислительным устройством 124 торговца. В качестве альтернативы, упомянутый банк торговца может авторизовать третью сторону на выполнение обработки транзакций от его лица. В данном случае, вычислительное устройство 124 торговца будет выполнено с возможностью осуществления связи с третьей стороной. Такая третья сторона обычно именуется «процессором торговца», «процессором-эквайером», или «сторонним процессором».

[0053] Используя процессор 110 платежей, компьютеры банка торговца или процессора торговца будут осуществлять связь с компьютерами банка эмитента, такими как вычислительное устройство 130 эмитента, чтобы определять, находится ли счет пользователя 122 в хорошем состоянии и покрывается ли покупка доступной кредитной линией пользователя 122. На основе этих определений, запрос на авторизацию будет

отклонен или одобрен. Если запрос одобряется, код авторизации выпускается вычислительному устройству 124 торговца.

[0054] Когда запрос на авторизацию одобряется, доступная кредитная линия счета пользователя 122 уменьшается. Обычно, дебетовая запись за транзакцию платежной карты не отправляется сразу на счет пользователя 122, так как ассоциации банковских карт, такие как Mastercard International Incorporated®, имеют опубликованные правила, которые не позволяют вычислительному устройству 124 торговца дебетовать счет, или «фиксировать», транзакцию до тех пор, пока товары не отгружаются или услуги не доставляются. Тем не менее, по отношению к, по меньшей мере, некоторым транзакциям дебетовой карты, дебетовая запись может быть отправлена в момент транзакции. Когда торговец, ассоциированный с вычислительным устройством 124 торговца, отгружает или доставляет товары или услуги, вычислительное устройство 124 торговца фиксирует транзакцию посредством, например, соответствующих процедур ввода данных. Это может включать привязку одобренных транзакций ежедневно применительно к стандартным розничным покупкам. Если пользователь 122 отменяет транзакцию до того, как она фиксируется, генерируется «пустая операция». Если пользователь 122 возвращает товары 122 после того, как транзакция была зафиксирована, генерируется «кредит». Процессор 110 платежей и/или вычислительное устройство 130 эмитента сохраняет информацию карты транзакций, такую как категория торговца, идентификатор торговца, местоположение, где была совершена транзакция, сумму покупки, дату и время транзакции, в базе 120 данных.

[0055] Применительно к транзакциям дебетовой карты, когда запрос на авторизацию персонального идентификационного номера (PIN) одобряется эмитентом, счет пользователя 122 уменьшается. Обычно, дебетовая запись отправляется сразу на счет 122 пользователя. Ассоциация платежной карты тогда передает одобрение процессору-эквайеру для раздачи товаров/услуг или информации, или наличных в случае банкомата (ATM).

[0056] После того как покупка была совершена, происходит процесс клиринга, чтобы пересылать дополнительные контекстные транзакционные данные, которые относятся к покупке, между сторонами транзакции, такими как банк торговца, процессор 110 платежей, и вычислительное устройство 130 эмитента. В частности, во время и/или после процесса клиринга, дополнительные данные, такие как время покупки, имя торговца, тип торговца, информация о покупке, информация о счете пользователя, тип транзакции, информация касательно купленного предмета и/или услуги, и/или другая подходящая информация, ассоциируются с транзакцией и передаются между сторонами транзакции в качестве контекстных транзакционных данных, и могут быть сохранены любой из сторон транзакции.

[0057] В примерном варианте осуществления, данные криптографического ключа генерируются вычислительным устройством 114 пользователя, когда пользователь 122 осуществляет доступ к вычислительному устройству 114 пользователя. Вычислительное устройство 114 пользователя передает данные криптографического ключа приложению 220 в момент, когда пользователь 122 входит в приложение 220. Впоследствии, приложение 220 осуществляет маршрутизацию данных криптографического ключа к вычислительному устройству 150 DC, которое сохраняет данные криптографического ключа в базе 120 данных. Когда пользователь 122 осуществляет покупку данные криптографического ключа передаются в течение процесса клиринга наряду с контекстными транзакционными данными. Когда процессор 110 платежей принимает данные криптографического ключа, процессор 110 платежей осуществляет

маршрутизацию данных криптографического ключа к вычислительному устройству 150 DC, которое сравнивает принятые данные криптографического ключа с хранящимися данными криптографического ключа. В альтернативных вариантах осуществления, приложение 220 находится на связи с вычислительным устройством 124 торговца и/или процессором 110 платежей. Когда пользователь 122 осуществляет покупку используя приложение 220, приложение 220 принимает данные криптографического ключа от вычислительного устройства 114 пользователя и осуществляет маршрутизацию к вычислительному устройству 114 торговца и/или процессору 110 платежей. В некоторых вариантах осуществления, вычислительное устройство 124 торговца может передавать данные криптографического ключа непосредственно вычислительному устройству 150 DC. В других вариантах осуществления, вычислительное устройство 124 торговца может передавать данные криптографического ключа процессору 110 платежей, который затем осуществляет маршрутизацию данных криптографического ключа к вычислительному устройству 150 DC.

[0058] В примерном варианте осуществления, вычислительное устройство 150 DC выполнено с возможностью приема и сохранения данных криптографического ключа, определения оценки мошенничества для сообщения запроса аутентификации, построения таблицы оценок, автоматического генерирования ответа аутентификации, и передачи такого ответа аутентификации.

[0059] В некоторых вариантах осуществления, вычислительное устройство 150 DC принимает сообщение запроса авторизации от вычислительного устройства 124 торговца. В ответ на сообщение запроса авторизации, вычислительное устройство 150 DC передает ответ авторизации вычислительному устройству 130 эмитента и/или вычислительному устройству 124 торговца. В других вариантах осуществления, вычислительное устройство 150 DC передает сообщение запроса авторизации вычислительному устройству 130 эмитента, принимает, в ответ на сообщение запроса авторизации, сообщение ответа авторизации от вычислительного устройства 130 эмитента, и передает сообщение ответа авторизации вычислительному устройству 124 торговца. В альтернативных вариантах осуществления, вычислительное устройство DC принимает запрос в отношении оценки мошенничества для пользователя 122 от запрашивающей стороны, такой как вычислительное устройство 124 торговца и/или вычислительное устройство 130 эмитента. Вычислительное устройство 150 DC извлекает оценку мошенничества для пользователя 122 и передает оценку мошенничества запрашивающей стороне.

[0060] Фиг. 3 иллюстрирует примерную конфигурацию системы 302 пользователя, такой как вычислительное устройство 114 пользователя (показанное на Фиг. 1), выполненной с возможностью передачи данных вычислительному устройству 150 DC (показанному на Фиг. 1). Система 302 пользователя может включать в себя, но не ограничивается, вычислительное устройство 114 пользователя. В примерном варианте осуществления, система 302 пользователя включает в себя процессор 305 для исполнения инструкций. В некоторых вариантах осуществления, исполняемые инструкции хранятся в памяти 310. процессор 305 может включать в себя один или более блоки обработки, например, многоядерная конфигурация. Память 310 является любым устройством, позволяющим сохранять и извлекать информацию, такую как исполняемые инструкции и/или письменные труды. Память 310 может включать в себя один или более машиночитаемые носители информации.

[0061] Система 302 пользователя также включает в себя, по меньшей мере, один компонент 315 вывода мультимедиа для представления информации пользователю 301. Пользователь 301 может включать в себя, но не ограничивается, пользователя 122

(показан на Фиг. 1). Компонент 315 вывода мультимедиа является любым компонентом, выполненным с возможностью переноса информации пользователю 301. Например, компонент 315 вывода мультимедиа может быть компонентом отображения, выполненным с возможностью отображения данных жизненного цикла компонента в форме отчета, панели инструментов, связи, и подобного. В некоторых вариантах осуществления, компонент 315 вывода мультимедиа включает в себя адаптер вывода, такой как видео адаптер и/или аудио адаптер. Адаптер вывода оперативно связан с процессором 305 и может быть оперативно соединен с устройством вывода, таким как устройство отображения, жидкокристаллический дисплей (LCD), дисплей на органических светоизлучающих диодах (OLED), или дисплей с «электронными чернилами», или устройством вывода аудио, громкоговорителем или головными телефонами.

[0062] В некоторых вариантах осуществления, система 302 пользователя включает в себя устройство 320 ввода для приема ввода от пользователя 301. Устройство 320 ввода может включать в себя, например, клавиатуру, указательное устройство, мышь, стилус, сенсорную панель, сенсорную площадку, сенсорный экран, гироскоп, акселерометр, детектор позиции, устройство ввода аудио, устройство чтения/сканер отпечатка пальцев, устройство чтения/сканер отпечатка ладони, устройство чтения/сканер радужной оболочки, устройство чтения/сканер сетчатки, или подобное. Единый компонент, такой как сенсорный экран может функционировать как устройство вывода у компонента 315 вывода мультимедиа, так и устройство 320 ввода. Единый компонент, такой как сенсорный экран, может функционировать как устройство вывода у компонента 315 вывода мультимедиа, так и устройство 320 ввода. Система 302 пользователя также может включать в себя интерфейс 325 связи, который может быть коммуникативно соединен с удаленным устройством, таким как серверная система 112 (показанная на Фиг. 1). Интерфейс 325 связи может включать в себя, например, адаптер проводной или беспроводной сети или беспроводной приемопередатчик данных для использования с мобильной телефонной сетью, Глобальной Системой Связи с Подвижными Объектами (GSM), 3G, или другой мобильной сетью данных или Общемировой Совместимости Широкополосного Беспроводного Доступа (WIMAX).

[0063] Хранящимися в памяти 310 являются, например, машиночитаемые инструкции для предоставления интерфейса пользователя пользователю 301 через компонент 315 вывода мультимедиа и, опционально, приема и обработки ввода от устройства 320 ввода. Интерфейс пользователя может включать в себя, среди прочих возможностей, web-браузер, и клиентское приложение. Web-браузеры позволяют пользователям, таким как пользователь 310, отображать и взаимодействовать с мультимедиа и другой информацией, как правило, встроенной в web-страницу или web-сайт от серверной системы 112. Клиентское приложение позволяет пользователю 301 взаимодействовать с серверным приложением от серверной системы 112.

[0064] Фиг. 4 иллюстрирует примерную конфигурацию серверной системы 401, такой как серверная система 112 (показанная на Фиг. 1), которая включает в себя вычислительное устройство 150 DC (показанное на Фиг. 1). Серверная система 401 может включать в себя, но не ограничивается, сервер 116 базы данных (показан на Фиг. 1) или вычислительное устройство 150 DC. В некоторых вариантах осуществления, серверная система 401 является сходной с серверной системой 112.

[0065] Серверная система 401 включает в себя процессор 405 для исполнения инструкций. Инструкции могут быть сохранены в памяти 410, например. Процессор 405 может включать в себя один или более блоки обработки (например, многоядерная

конфигурация) для исполнения инструкций. Инструкции могут быть исполнены в разнообразии отличных операционных систем в серверной системе 401, таких как UNIX, LINUX, Microsoft Windows®, и т.д. Более конкретно, инструкции могут предписывать разнообразные манипуляции данными над данными, хранящимися в хранилище 434 (например, процедуры создания, считывания, обновления, и удаления). Также следует иметь в виду, что после инициирования основанного на компьютере способа, разнообразные инструкции могут быть исполнены во время инициализации. Некоторые операции могут потребоваться для того, чтобы выполнять один или более процессы, описываемые в данном документе, тогда как другие операции могут быть более общими и/или особыми для конкретного языка программирования (например, C, C#, C++, Java, или других подходящих языков программирования, и т.д.).

[0066] Процессор 405 оперативно связан с интерфейсом 415 связи, так что серверная система 401 выполнена с возможностью осуществления связи с удаленным устройством, таким как система пользователя или другая серверная система 401. Например, интерфейс 415 связи может принимать связь от вычислительного устройства 130 эмитента через множество сетевых соединений, как иллюстрируется на Фиг. 1.

[0067] Процессор 405 также может быть оперативно связана с запоминающим устройством 434. Запоминающее устройство 434 является любым оперируемым компьютером аппаратным обеспечением, подходящим для хранения и/или извлечения данных. В некоторых вариантах осуществления, запоминающее устройство 434 является интегрированным в серверную систему 401. В других вариантах осуществления, запоминающее устройство 434 является внешним по отношению к серверной системе 401 и является сходным с базой 120 данных (показанной на Фиг. 1). Например, серверная система 401 может включать в себя один или более накопители на жестком диске в качестве запоминающего устройства 434. В других вариантах осуществления, запоминающее устройство 434 является внешним по отношению к серверной системе 401 и доступ к нему может быть осуществлен посредством множества серверных систем 401. Например, запоминающее устройство 434 может включать в себя несколько запоминающих блоков, таких как жесткие диски или твердотельные диски в конфигурации массива недорогих дисков с избыточностью (RAID). Запоминающее устройство 434 может включать в себя сеть хранения данных (SAN) и/или систему подключаемого к сети хранилища (NAS).

[0068] В некоторых вариантах осуществления, процессор 405 оперативно связан с запоминающим устройством 434 через интерфейс 420 хранения. Интерфейс 420 хранения является любым компонентом предоставления процессору 405 доступа к запоминающему устройству 434. Интерфейс 420 хранения может включать в себя, например, адаптер Усовершенствованной Технологии Прикрепления (ATA), адаптер Последовательной ATA (SATA), адаптер Интерфейса Малых Вычислительных Систем (SCSI), контроллер RAID, адаптер SAN, сетевой адаптер, и/или любой компонент, предоставляющий процессору 405 доступ к запоминающему устройству 434.

[0069] Память 410 может включать в себя, но не ограничивается, память с произвольным доступом (RAM), такую как динамическая RAM (DRAM) или статическая RAM (SRAM), постоянную память (ROM), стираемую программируемую постоянную память (EPROM), электрически стираемую программируемую постоянную память (EEPROM), и энергонезависимую RAM (NVRAM). Вышеприведенные типы памяти являются лишь примерными, и, таким образом, не ограничиваются типами памяти, используемыми для хранения компьютерной программы.

[0070] Фиг. 5 является примерной блок-схемой, иллюстрирующей поток 500 способа,

посредством которого, по меньшей мере, одно вычислительное устройство 150 DC (показанное на Фиг. 1) соотносит зашифрованные биометрические данные на устройстве с транзакционными данными и данными устройства для аутентификации пользователя (например, онлайнового пользователя). Способ 500 включает в себя прием 505 первых данных криптографического ключа, ассоциированных с первой транзакцией, включающих в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства, и первый идентификатор счета, сохранение 510 первых данных криптографического ключа в базе 120 данных (показанной на Фиг. 1) в качестве исторических данных криптографического ключа, которая находится на связи с одним или более вычислительными устройствами 150 DC, и прием 515 сообщения запроса аутентификации для второй транзакции, включающей в себя вторые данные криптографического ключа, причем вторые данные криптографического ключа включают в себя второй идентификатор устройства, и второй идентификатор счета. Способ 500 также включает в себя соотнесение 520 вторых данных криптографического ключа с историческими данными криптографического ключа. Способ 500 дополнительно включает в себя определение 525 оценки мошенничества для второй транзакции, при этом оценка мошенничества определяется на основе соотнесения криптографического ключа и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета, автоматическое генерирование 540 сообщения ответа аутентификации в ответ на сообщение запроса аутентификации, включающего в себя оценку мошенничества, и передачу 545 сообщения ответа аутентификации.

[0071] Способ 500 также может включать в себя сохранение 530 оценки мошенничества в базе 120 данных как части исторических данных, ассоциированных с первыми данными криптографического ключа. Способ 500 дополнительно включает в себя построение 535 таблицы оценок, которая включает в себя одну или более оценки мошенничества, хранящиеся в базе 120 данных.

[0072] Фиг. 6 показывает примерную конфигурацию базы 600 данных в вычислительном устройстве, наряду с другими связанными вычислительными компонентами, которая может быть использована, чтобы строить оценку мошенничества посредством соотнесения зашифрованных биометрических данных на устройстве с транзакционными данными и данными устройства, ассоциированными с пользователем 122 (показанным на Фиг. 1). В некоторых вариантах осуществления, вычислительное устройство 610 является сходным с серверной системой 112 (показанной на Фиг. 1). Пользователь 602 (такой как пользователь, оперирующий серверной системой 112) может осуществлять доступ к вычислительному устройству 610 для того, чтобы верифицировать записи в таблице данных, соответствующей пользователю 122. В некоторых вариантах осуществления, база 620 данных является сходной с базой 120 данных (показанной на Фиг. 1). В примерном варианте осуществления, база 620 данных включает в себя данные 622 криптографического ключа (например, исторические данные криптографического ключа, опорные данные криптографического ключа, данные журнала регистрации криптографического ключа), данные 624 оценки мошенничества, и контекстные транзакционные данные 626. Данные 622 криптографического ключа могут включать в себя зашифрованные биометрические данные на устройстве пользователя 122, данные вычислительного устройства пользователя 122 (например, данные IP-адреса, данные MAC-адреса), данные счета пользователя (например, PAN), и временную отметку сообщения запроса аутентификации (например, время, когда сообщение запроса аутентификации было принято и/или сохранено в вычислительном устройстве 610). В некоторых вариантах

осуществления, база 620 данных хранит опорные данные криптографического ключа. Например, база 620 данных может хранить записи, включающие в себя данные криптографического ключа и проиндексированные идентификаторы счета, так что данные криптографического ключа являются быстро доступными на основе идентификатора счета. Дополнительно или в качестве альтернативы, база 620 данных хранит данные криптографического ключа, включающие в себя множество экземпляров данных криптографического ключа. Например, база 620 данных может хранить журнал регистрации всех экземпляров данных криптографического ключа, принятых на основе идентификаторов счета, так что поддерживается запись всех данных криптографического ключа, ассоциированных с идентификатором карты счета.

[0073] Данные 624 оценки мошенничества могут включать в себя исторические данные оценки мошенничества (например, исторические оценки мошенничества для одного или более сообщений запроса аутентификации, исторические значения оценки мошенничества), число сообщений запроса отклоненных и/или одобренных, и текущее значение риска. Контекстные транзакционные данные 626 могут включать в себя суммы транзакции, даты/время транзакции, данные счета, которые относятся к платежной карте, использованной для выполнения транзакции (например, PAN, ассоциированный с платежной картой, дата истечения срока действия карты, эмитент карты, код безопасности карты, или подобное), идентификаторы торговца, данные единицы учета запасов (SKU), относящиеся к товарам или услугам, купленным пользователем 122, и подобное.

[0074] Вычислительное устройство 610 включает в себя устройства 630 хранения данных. Вычислительное устройство 610 также включает в себя компонент-построитель 640, который строит таблицу данных, используя оценки мошенничества из сообщений запроса аутентификации, соответствующих контекстным транзакционным данным, ассоциированным с пользователем 122. Компонент-построитель 640 также может выполнять, например, соотнесение первого криптографического ключа и второго криптографического ключа, определение 525 (показанное на Фиг. 5) оценки мошенничества для сообщения запроса аутентификации посредством использования вычисленной дельты и исторических данных, ассоциированных с первыми данными криптографического ключа, и построение 535 (показанное на Фиг. 5) таблицы оценок, которая включает в себя одну или более оценки мошенничества, хранящиеся в базе 120 данных.

[0075] Вычислительное устройство 610 также включает в себя компонент-коррелятор 650, который способствует соотнесению данных, более конкретно, соотнесению 520 (показанному на Фиг. 5) вторых данных криптографического ключа с историческими данными криптографического ключа. В одном варианте осуществления, коррелятор 650 может определять, согласуются ли вторые данные криптографического ключа с историческими данными криптографического ключа. Например, коррелятор 650 может определять, включены в и/или предлагаются ли историческими данными криптографического ключа (например, данными 622 криптографического ключа) вторые данные криптографического ключа. В определенных вариантах осуществления, коррелятор 650 может соотносить данные криптографического ключа на основе жетона и/или хеш-значения идентификатора счета, и/или биометрических данных. Дополнительно или в качестве альтернативы, коррелятор 650 может соотносить данные криптографического ключа на основе включенной цифровой подписи (например, шифрования открытого ключа), ассоциированной с центром сертификации. Например, коррелятор 650 может быть выполнен с возможностью определения идентификатора

центра сертификации, ассоциированного с данными криптографического ключа. В одном варианте осуществления, коррелятор 650 выполнен с возможностью соотнесения вторых данных криптографического ключа с опорным криптографическим ключом, включенным в исторические данные криптографического ключа. Например, коррелятор 650 может определять, что идентификатор, ассоциированный со вторыми данными криптографического ключа, совпадает с опорными данными криптографического ключа. Дополнительно или в качестве альтернативы, коррелятор 650 выполнен с возможностью соотнесения вторых данных криптографического ключа со множеством экземпляров данных криптографического ключа, включенных в исторические данные криптографического ключа. Например, коррелятор 650 может определять, что идентификатор, ассоциированный с вторыми данными криптографического ключа, является согласующимся со множеством идентификаторов, включенных в исторические данные криптографического ключа.

[0076] Вычислительное устройство 610 также включает в себя компонент 660 связи, который используется, чтобы осуществлять связь с вычислительными устройствами эмитента, вычислительными устройствами торговца, и/или другими вычислительными устройствами, используя предварительно определенные сетевые протоколы, такие как TCP/IP (Протокол Управления Передачей/Интернет Протокол) по множеству сетевых соединений.

[0077] В некоторых вариантах осуществления, в том случае, когда вторые данные криптографического ключа не согласуются с историческими данными криптографического ключа, компонент-коррелятор 650 выполнен с возможностью обновления и/или расширения данных 622 криптографического ключа, чтобы они включали в себя, по меньше мере, частично вторые данные криптографического ключа. Например, данные криптографического ключа могут быть ассоциированы с законной транзакцией, несмотря на то, что криптографические данные могут быть не согласующимися с историческими данными криптографического ключа (например, новое устройство), таким образом, компонент-коррелятор 650 может обновлять данные криптографического ключа так, что будущие запросы аутентификации, ассоциированные с новым устройством, включают в себя криптографические данные, согласующиеся с историческими криптографическими данными.

[0078] Фиг. 7 иллюстрирует примерную конфигурацию 700 вычислительного устройства 150 коллектора данных (DC), выполненного с возможностью приема и сохранения данных криптографического ключа, определения оценки мошенничества для сообщения запроса аутентификации, построения таблицы оценок, автоматического генерирования ответа аутентификации, и передачи такого ответа аутентификации. Вычислительное устройство 150 DC может включать в себя, но не ограничивается, процессор 705 для исполнения инструкций. В некоторых вариантах осуществления, процессор 705 является сходным с процессором 405 (показанным на Фиг. 4). В примерном варианте осуществления, вычислительное устройство 150 DC включает в себя исполняемые инструкции, хранящиеся в памяти 710. Хранящиеся исполняемые инструкции могут быть правилами машины, которые могут предварительно определять пороговую величину. Процессор 705 может применять такие правила машины к данным для того, чтобы определять, отвечают ли данные предварительно определенной пороговой величине. В некоторых вариантах осуществления, память 710 является сходной с памятью 410 (показанной на Фиг. 4). Процессор 705 может включать в себя один или более блоки обработки, например, многоядерная конфигурация. Память 710 является любым устройством, обеспечивающим хранение и извлечение информации,

такой как исполняемые инструкции и/или письменные труды. Память 710 может включать в себя один или более машиночитаемые носители информации.

[0079] Вычислительное устройство 150 DC включает в себя процессор 705 для исполнения инструкций. Инструкции могут быть сохранены в памяти 710, например, Процессор 705 может включать в себя один или более блоки обработки (например, в многоядерной конфигурации) для исполнения инструкций. Инструкции могут быть исполнены в разнообразии отличных операционных систем в вычислительном устройстве 150 DC, таких как UNIX, LINUX, Microsoft Windows®, и т.д. Более конкретно, инструкции могут предписывать разнообразные манипуляции данными над историческими данными 720 и таблицей 725 оценок (например, создание, чтение, обновление, и удаление данных). Также следует иметь в виду, что после инициирования основанного на компьютере способа, разнообразные инструкции могут быть исполнены во время инициализации. Некоторые операции могут потребоваться для того, чтобы выполнять один или более процессы, описываемые в данном документе, тогда как другие операции могут быть более общими и/или особыми для конкретного языка программирования (например, C, C#, C++, Java, или других подходящих языков программирования, и т.д.).

[0080] Процессор 705 оперативно связан с интерфейсом 715 связи так, что вычислительное устройство 150 DC выполнено с возможностью осуществления связи с удаленным устройством, таким как процессор 110 платежей (показанный на Фиг. 1). В некоторых вариантах осуществления, интерфейс связи является сходным с интерфейсом 415 связи (показанным на Фиг. 4). В некоторых вариантах осуществления интерфейс 415 связи может быть порталом приложения оценивания, который может принимать связь от и передавать связь к одному или более вычислительным устройствам 735 запрашивающих сторон через множество сетевых соединений, как иллюстрируется на Фиг. 1. Такие запрашивающие стороны могут запрашивать данные оценки мошенничества, ассоциированные с идентификатором счета пользователя и интерфейс связи может передавать ответ таким запрашивающим сторонам в ответ на запрос. Интерфейс 715 связи также может принимать связь от и передавать связь к одному или более электронным приложениям 740, таким как электронный кошелек, приложение торговца, приложение эмитента, или подобного, через множество сетевых соединений. Эти связи могут включать в себя данные криптографического ключа и/или контекстные транзакционные данные. В некоторых вариантах осуществления, одно или более электронные приложения также находятся на связи с вычислительным устройством 745 пользователя, которое может быть сходным с системой 302 пользователя (показанной на Фиг. 3).

[0081] Процессор 705 также может быть оперативно связан с запоминающим устройством 730. Запоминающее устройство 730 является любым оперируемым компьютером аппаратным обеспечением, подходящим для хранения и/или извлечения данных. В некоторых вариантах осуществления, запоминающее устройство 730 является интегрированным в вычислительное устройство 150 DC. В других вариантах осуществления, запоминающее устройство 730 является внешним по отношению к вычислительному устройству 150 DC и является сходным с запоминающим устройством 434 (показанным на Фиг. 4). Например, вычислительное устройство 150 DC может включать в себя один или более накопители на жестком диске в качестве запоминающего устройства 434 (показанного на Фиг. 4). В других вариантах осуществления, запоминающее устройство 730 является внешним по отношению к вычислительному устройству 150 DC и доступ к нему может быть осуществлен посредством множества вычислительных устройств 150 DC. Например, запоминающее устройство 730 может

включать в себя несколько запоминающих блоков, таких как жесткие диски или твердотельные диски в конфигурации массива недорогих дисков с избыточностью (RAID). Запоминающее устройство 730 может включать в себя сеть хранения данных (SAN) и/или систему подключаемого к сети хранилища (NAS). В примерном варианте осуществления, запоминающее устройство 730 включает в себя исторические данные 720 и таблицу 725 оценок. В других вариантах осуществления, вычислительное устройство DC может находиться на связи с несколькими запоминающими устройствами, сходными с запоминающим устройством 730. Множество запоминающих устройств может включать в себя частичные или полные исторические данные 720 и/или таблицу 725 оценок.

[0082] В некоторых вариантах осуществления, процессор 705 оперативно связан с запоминающим устройством 730 через интерфейс 722 хранения. Интерфейс 722 хранения является любым компонентом, выполненным с возможностью предоставления процессору 705 доступа к запоминающему устройству 730. Интерфейс 722 хранения может включать в себя, например, адаптер Усовершенствованной Технологии Прикрепления (ATA), адаптер Последовательной ATA (SATA), адаптер Интерфейса Малых Вычислительных Систем (SCSI), контроллер RAID, адаптер SAN, сетевой адаптер, и/или любой компонент, предоставляющий процессору 705 доступ к запоминающему устройству 730.

[0083] В некоторых вариантах осуществления, процессор 705 выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на прием данных криптографического ключа и контекстных транзакционных данных через интерфейс 715 связи, сохранение данных криптографического ключа и контекстных транзакционных данных в запоминающем устройстве 730 на основе идентификатора счета пользователя 122, и построение таблицы 725 оценок посредством использования исторических данных 720, хранящихся в запоминающем устройстве 730. В других вариантах осуществления, процессор 705 выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на анализ исторических данных 720, чтобы идентифицировать оценку мошенничества исторических сообщений запроса аутентификации, ассоциированных с идентификатором счета. В еще одних других вариантах осуществления, процессор 705 выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на определение оценки мошенничества текущего сообщения запроса аутентификации и сохранение определенной оценки мошенничества в таблице 725 оценок на основе идентификатора счета пользователя. В некоторых вариантах осуществления, процессор 705 выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на конкатенацию одной или более оценок мошенничества, хранящихся в таблице 725 оценок, и передачу конкатенированной оценки одной или более запрашивающим сторонам 735, используя интерфейс 715 связи.

[0084] В некоторых вариантах осуществления, процессор 705 выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на обмен данными криптографического ключа с электронным приложением 740. Процессор 705 может выдавать инструкцию вычислительному устройству 150 DC на дешифрование фрагмента данных криптографического ключа (например, идентификатора вычислительного устройства пользователя, счета пользователя) для того, чтобы идентифицировать идентификатор счета, где могут быть сохранены данные криптографического ключа. Зашифрованные биометрические данные на устройстве остаются зашифрованными, но может быть назначен идентификатор, чтобы способствовать соотнесениям с зашифрованными биометрическими данными на

устройстве, ассоциированными с тем же самым идентификатором счета пользователя.

[0085] В альтернативных вариантах осуществления, процессор 705 выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на одобрение или отклонение сообщения запроса аутентификации на основе конкатенированной оценки мошенничества, ассоциированной с идентификатором счета пользователя, пороговой величины оценки, стоимости покупки, включенной в сообщение запроса аутентификации, и/или соотнесения криптографического ключа, ассоциированного с сообщением запроса аутентификации. Процессор 705 дополнительно выполнен с возможностью выдачи инструкции вычислительному устройству 150 DC на генерирование и передачу сообщения ответа аутентификации с одобрением или отклонением в ответ на сообщение запроса аутентификации. В примерном варианте осуществления, сообщение ответа аутентификации передается электронному приложению 740. В других вариантах осуществления, сообщение запроса аутентификации может быть передано любому другому приложению, услуге, или устройству, авторизованному на прием сообщения ответа аутентификации.

[0086] Память 710 может включать в себя, но не ограничивается, память с произвольным доступом (RAM), такую как динамическая RAM (DRAM) или статическая RAM (SRAM), постоянную память (ROM), стираемую программируемую постоянную память (EPROM), электрически стираемую программируемую постоянную память (EEPROM), и энергонезависимую RAM (NVRAM). Вышеприведенные типы памяти являются лишь примерными, и, таким образом, не ограничиваются типами памяти, используемыми для хранения компьютерной программы.

[0087] Как будет понятно на основе вышеизложенного технического описания, описанные выше варианты осуществления изобретения могут быть реализованы, используя методики компьютерного программирования или инженерного искусства, включая компьютерное программное обеспечение, встроенное программное обеспечение, аппаратное обеспечение или любое их сочетание или подмножество, при этом технический результат состоит в сборе данных цифрового кошелька из транзакции цифрового кошелька, инициированной пользователем, для определения демографических данных пользователя. Любая такая результирующая программа, со средством машиночитаемого кода, может быть воплощена или предоставлена в рамках одного или более машиночитаемых носителей информации, тем самым составляя компьютерный программный продукт, (т.е., изделие), в соответствии с обсуждаемыми вариантами осуществления изобретения. Машиночитаемые носители информации могут быть, например, но не ограничиваются фиксированным (жестким) диском, дискетой, оптическим диском, магнитной лентой, полупроводниковой памятью, такой как постоянная память (ROM), и/или любым передающим/принимающим носителем информации, таким как Интернет или другая сеть связи или линия связи. Изделие, содержащее компьютерный код, может быть выполнено и/или использоваться посредством исполнения кода непосредственно с одного носителя информации или другого носителя информации, или посредством передачи кода через сеть.

[0088] Эти компьютерные программы (также известные как программы, программное обеспечение, приложения программного обеспечения, «мобильные приложения», или код) включают в себя машинные инструкции для программируемого процессора, и могут быть реализованы на высокоуровневом процедурном и/или объектно-ориентированном языке программирования, и/или на ассемблере/машинном языке. Используемые в данном документе понятия «машиночитаемый носитель информации», «читаемый компьютером носитель информации» относятся к любому компьютерному

программному продукту, аппаратуре и/или устройству (например, магнитным дискам, оптическим дискам, памяти, Программируемым Логическим Устройствам (PLD)), используемым для предоставления машинных инструкций и/или данных программируемому процессору, включая машиночитаемый носитель информации, который принимает машинные инструкции в качестве машиночитаемого сигнала. «Машиночитаемый носитель информации» и «читаемый компьютером носитель информации», тем не менее, не включают в себя временные сигналы. Понятие «машиночитаемый сигнал» относится к любому сигналу, используемому для предоставления машинных инструкций и/или данных программируемому процессору.

[0089] Данное описание использует примеры, чтобы раскрывать изобретение, включая предпочтительный вариант его осуществления, и также позволяет любому специалисту в соответствующей области техники реализовать на практике изобретение, включая создание и использование любых устройств или систем и выполнение любых встроенных способов. Патентоспособный объем изобретения определяется формулой изобретения, и может включать в себя другие примеры, которые приходят на ум специалистам в соответствующей области техники. Подразумевается, что такие другие примеры должны находиться в рамках объема формулы изобретения, если они имеют структурные элементы, которые не отличаются от литературного языка формулы изобретения, или если они включают в себя эквивалентные структурные элементы с неосновательными отличиями от литературного языка формулы изобретения.

## (57) Формула изобретения

1. Система контроллера данных (DC) для аутентификации пользователя, содержащая одно или более вычислительных устройств контроллера данных (DC), причем одно или более вычислительных устройств DC содержат по меньшей мере один процессор и память, при этом одно или более вычислительных устройств DC выполнены с возможностью:

принимать, как часть процесса регистрации пользователя для цифрового кошелька, первые данные криптографического ключа, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства и первый идентификатор счета;

сохранять первые данные криптографического ключа в базе данных, которая находится на связи с упомянутыми одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа;

принимать сообщение запроса аутентификации для платежной транзакции, включающей в себя вторые данные криптографического ключа, причем вторые данные криптографического ключа включают в себя второй идентификатор устройства и второй идентификатор счета;

соотносить вторые данные криптографического ключа с историческими данными криптографического ключа;

определять оценку мошенничества для платежной транзакции, при этом оценка мошенничества определяется на основе упомянутого соотнесения данных криптографических ключей;

автоматически генерировать сообщение ответа аутентификации в ответ на сообщение запроса аутентификации, причем сообщение ответа аутентификации включает в себя оценку мошенничества;

передавать сообщение ответа аутентификации;

принимать третьи данные криптографического ключа, причем третьи данные

криптографического ключа относятся к ранее одобренному запросу аутентификации;

определять, что третьи данные криптографического ключа не согласуются с историческими данными криптографического ключа из упомянутого процесса регистрации пользователя для цифрового кошелька; и

расширять исторические данные криптографического ключа включением в них третьих данных криптографического ключа.

2. Система DC по п. 1, при этом зашифрованные биометрические данные на устройстве включают в себя биометрические данные на устройстве, удостоверенные посредством пользовательского вычислительного устройства.

3. Система DC по п. 1, при этом первые данные криптографического ключа ассоциированы с первым пользовательским вычислительным устройством, используемым для выполнения процесса регистрации пользователя для цифрового кошелька, причем третьи данные криптографического ключа ассоциированы со вторым пользовательским вычислительным устройством, отличающимся от первого пользовательского вычислительного устройства.

4. Система DC по п. 1, дополнительно выполненная с возможностью соотносить вторые данные криптографического ключа и исторические данные криптографического ключа посредством, по меньшей мере, выполнения поиска первого идентификатора счета в базе данных и сопоставления первого идентификатора счета со вторым идентификатором счета.

5. Система DC по п. 1, дополнительно выполненная с возможностью:

сохранять оценку мошенничества в базе данных как часть исторических данных, ассоциированных с первыми данными криптографического ключа; и

строить таблицу оценок мошенничества для первого идентификатора счета, при этом таблица оценок мошенничества включает в себя одну или более оценок мошенничества, хранящихся в этой базе данных.

6. Система DC по п. 5, дополнительно выполненная с возможностью генерировать оценку мошенничества, ассоциированную с первым идентификатором счета, посредством конкатенации множества оценок мошенничества, хранящихся в таблице оценок.

7. Система DC по п. 6, дополнительно выполненная с возможностью передавать оценку мошенничества, ассоциированную с первым идентификатором счета, стороне, запрашивающей оценку мошенничества.

8. Система DC по п. 1, при этом исторические данные криптографического ключа включают в себя множество экземпляров принятых данных криптографического ключа.

9. Система DC по п. 1, при этом исторические данные криптографического ключа, ассоциированные с первыми данными криптографического ключа, включают в себя исторические оценки мошенничества.

10. Система по п. 1, дополнительно выполненная с возможностью автоматически генерировать сообщение ответа аутентификации, когда оценка мошенничества удовлетворяет предварительно определенной пороговой величине оценки.

11. Компьютерно-реализуемый способ аутентификации пользователя, причем способ реализуется с использованием одного или более вычислительных устройств контроллера данных (DC), связанных с устройством хранения данных, при этом способ содержит этапы, на которых:

принимают, как часть процесса регистрации пользователя для цифрового кошелька, первые данные криптографического ключа, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства и первый идентификатор счета;

сохраняют первые данные криптографического ключа в базе данных, которая находится на связи с упомянутыми одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа;

принимают сообщение запроса аутентификации для платежной транзакции, включающей в себя вторые данные криптографического ключа, причем вторые данные криптографического ключа включают в себя второй идентификатор устройства и второй идентификатор счета;

соотносят вторые данные криптографического ключа с историческими данными криптографического ключа;

определяют оценку мошенничества для платежной транзакции, при этом оценка мошенничества определяется на основе упомянутого соотнесения данных криптографических ключей и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета;

автоматически генерируют сообщение ответа аутентификации в ответ на сообщение запроса аутентификации, причем сообщение ответа аутентификации включает в себя оценку мошенничества;

передают сообщение ответа аутентификации;

принимают третьи данные криптографического ключа, причем третьи данные криптографического ключа относятся к ранее одобренному запросу аутентификации;

определяют, что третьи данные криптографического ключа не согласуются с историческими данными криптографического ключа из упомянутого процесса регистрации пользователя для цифрового кошелька; и

расширяют исторические данные криптографического ключа включением в них третьих данных криптографического ключа.

12. Способ по п. 11, в котором зашифрованные биометрические данные на устройстве включают в себя биометрические данные на устройстве, удостоверенные посредством пользовательского вычислительного устройства.

13. Способ по п. 11, дополнительно содержащий этап, на котором строят профиль счета пользователя посредством сохранения первых данных криптографического ключа в базе данных в качестве части процесса регистрации пользователя для цифрового кошелька, при этом профиль счета пользователя строится посредством использования первого идентификатора счета, включенного в первые данные криптографического ключа.

14. Способ по п. 11, дополнительно содержащий этап, на котором соотносят вторые данные криптографического ключа и исторические данные криптографического ключа посредством, по меньшей мере, выполнения поиска первого идентификатора счета в базе данных и сопоставления первого идентификатора счета со вторым идентификатором счета.

15. Способ по п. 11, дополнительно содержащий этапы, на которых:

сохраняют оценку мошенничества в базе данных как часть исторических данных, ассоциированных с первыми данными криптографического ключа; и

строят таблицу оценок мошенничества для первого идентификатора счета, при этом таблица оценок мошенничества включает в себя одну или более оценок мошенничества, хранящихся в этой базе данных.

16. Способ по п. 15, дополнительно содержащий этап, на котором генерируют оценку мошенничества, ассоциированную с первым идентификатором счета, посредством конкатенации множества оценок мошенничества, хранящихся в таблице оценок.

17. Способ по п. 16, дополнительно содержащий этап, на котором передают оценку

мошенничества, ассоциированную с первым идентификатором счета, стороне, запрашивающей оценку мошенничества.

18. Способ по п. 11, в котором исторические данные криптографического ключа включают в себя множество экземпляров принятых данных криптографического ключа.

19. Способ по п. 11, дополнительно содержащий этап, на котором автоматически генерируют сообщение ответа аутентификации, когда оценка мошенничества удовлетворяет предварительно определенной пороговой величине оценки.

20. Долговременный машиночитаемый носитель информации, который включает в себя машиноисполняемые инструкции для аутентификации пользователя, при этом машиноисполняемые инструкции, при их исполнении одним или более вычислительными устройствами контроллера данных (DC), содержащими по меньшей мере один процессор, который находится на связи с по меньшей мере одним запоминающим устройством, предписывают одному или более вычислительным устройствам контроллера данных (DC):

принимать, как часть процесса регистрации пользователя для цифрового кошелька, первые данные криптографического ключа, включающие в себя зашифрованные биометрические данные на устройстве, первый идентификатор устройства и первый идентификатор счета;

сохранять первые данные криптографического ключа в базе данных, которая находится на связи с упомянутыми одним или более вычислительными устройствами DC, в качестве исторических данных криптографического ключа;

принимать сообщение запроса аутентификации для платежной транзакции, включающей в себя вторые данные криптографического ключа, причем вторые данные криптографического ключа включают в себя второй идентификатор устройства и второй идентификатор счета;

соотносить вторые данные криптографического ключа с историческими данными криптографического ключа;

определять оценку мошенничества для платежной транзакции, при этом оценка мошенничества определяется на основе упомянутого соотнесения данных криптографических ключей и исторических данных криптографического ключа, ассоциированных с первым идентификатором счета;

автоматически генерировать сообщение ответа аутентификации в ответ на сообщение запроса аутентификации, причем сообщение ответа аутентификации включает в себя оценку мошенничества;

передавать сообщение ответа аутентификации;

принимать третьи данные криптографического ключа, причем третьи данные криптографического ключа относятся к ранее одобренному запросу аутентификации;

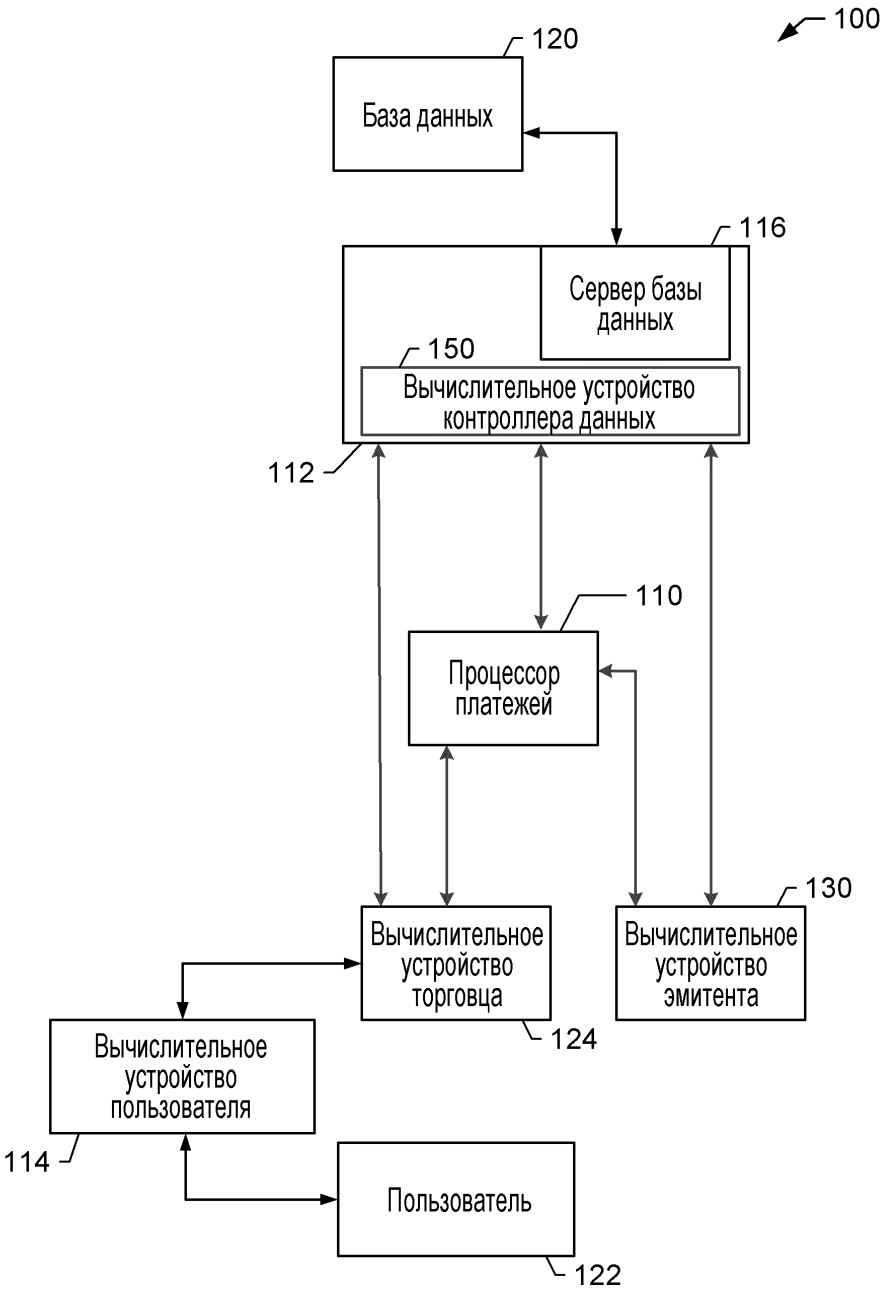
определять, что третьи данные криптографического ключа не согласуются с историческими данными криптографического ключа из упомянутого процесса регистрации пользователя для цифрового кошелька; и

расширять исторические данные криптографического ключа включением в них третьих данных криптографического ключа.

1

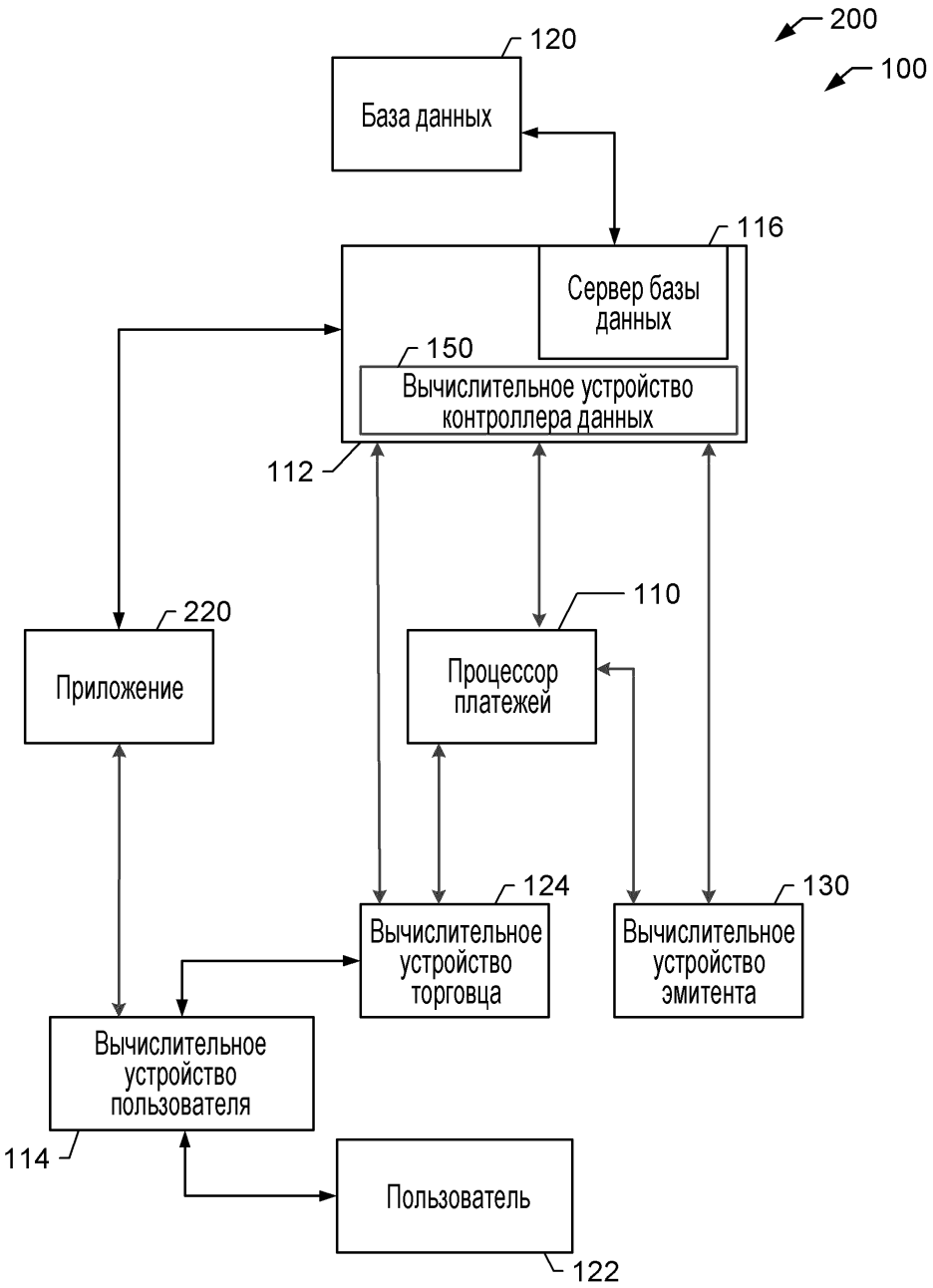


**ФИГ. 1**

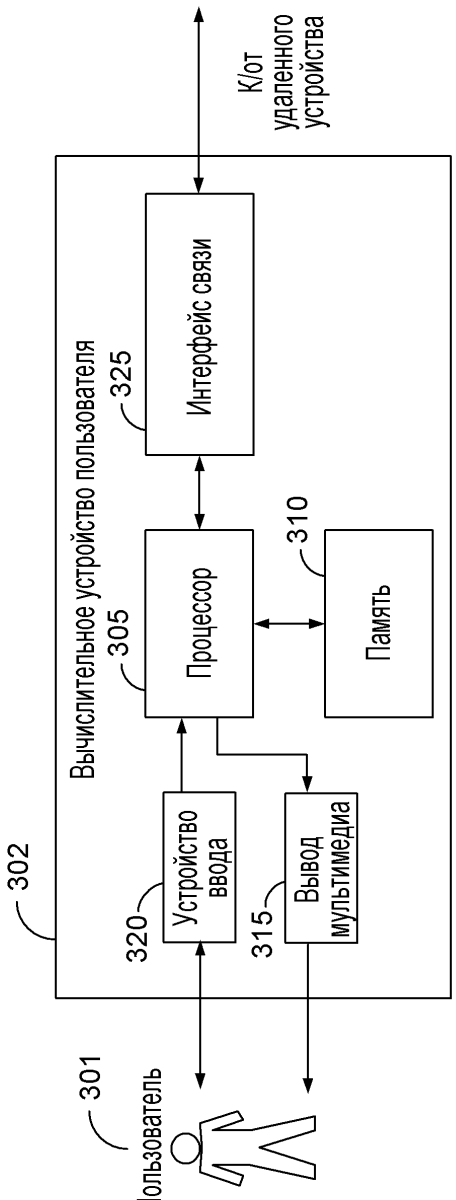

100
120
База данных
116
Сервер базы данных
150
Вычислительное устройство контроллера данных
112
110
Процессор платежей
130
Вычислительное устройство торговца
124
Вычислительное устройство эмитента
Вычислительное устройство пользователя
114
Пользователь
122

2

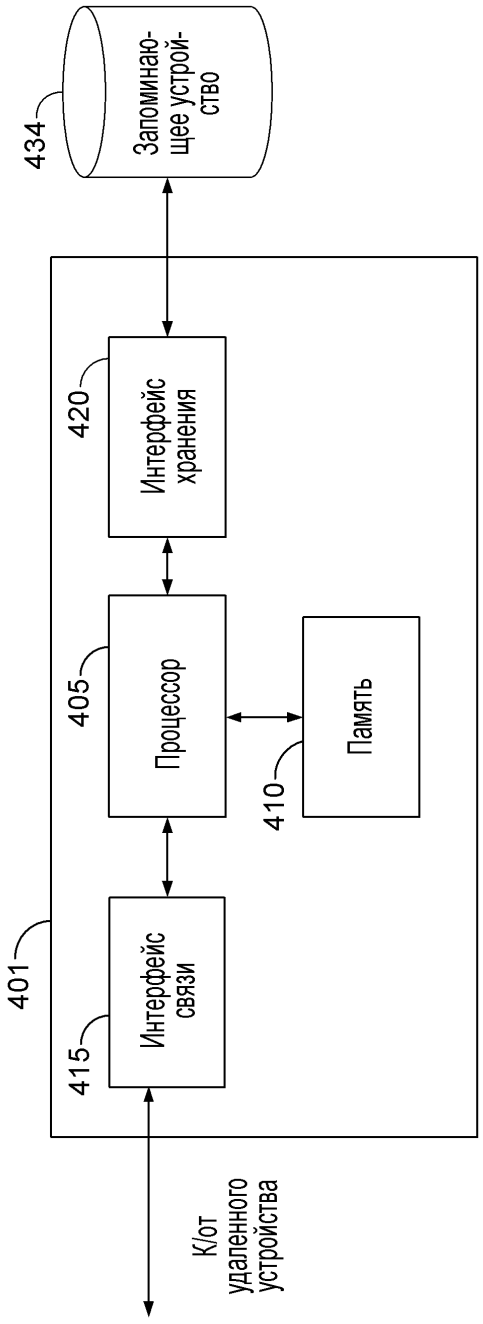
**ФИГ. 2**


200
100
120
База данных
116
Сервер базы данных
150
Вычислительное устройство контроллера данных
112
220
Приложение
110
Процессор платежей
124
Вычислительное устройство торговца
130
Вычислительное устройство эмитента
Вычислительное устройство пользователя
114
Пользователь
122

3

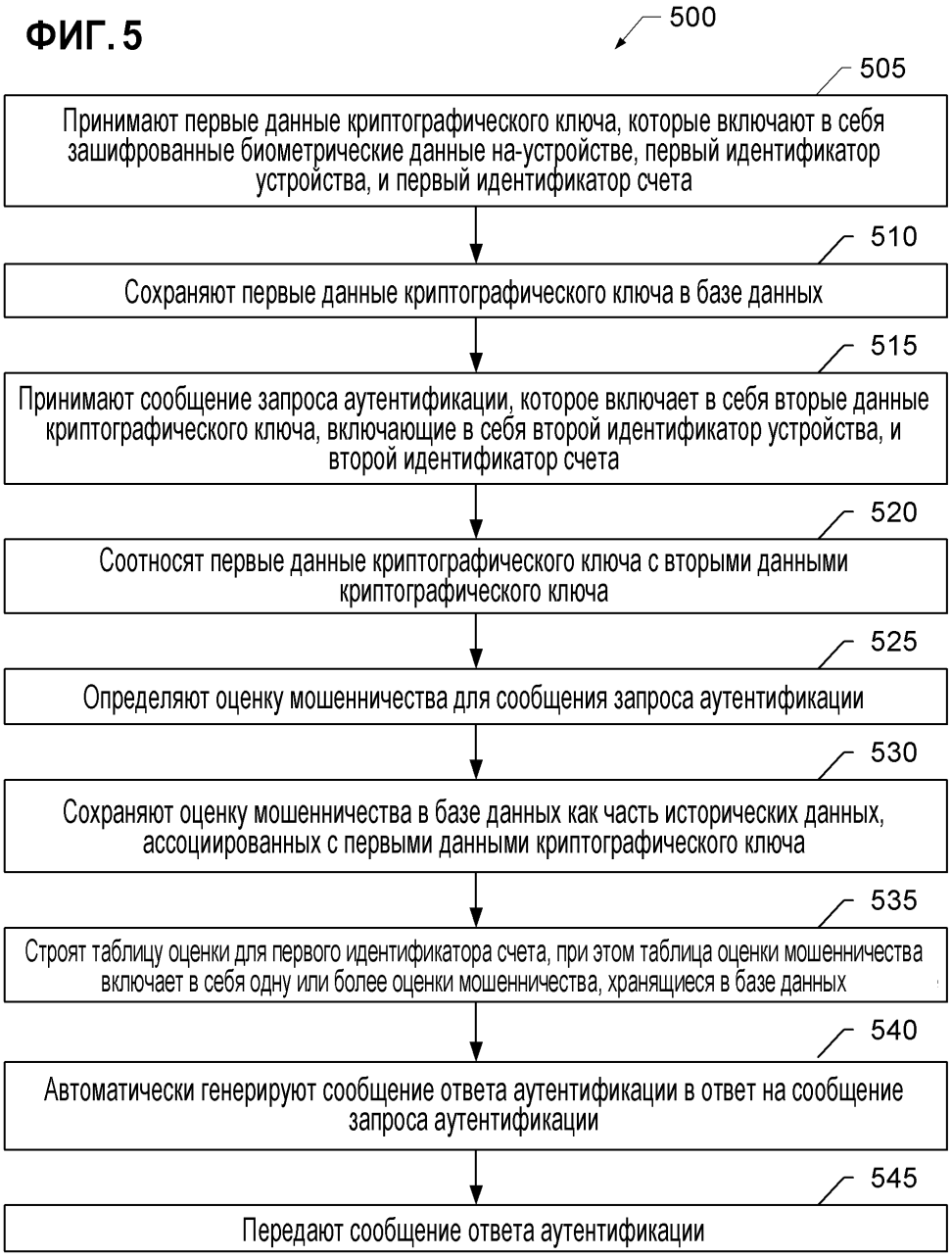

К/от удаленного устройства
Вычислительное устройство пользователя
302
Интерфейс связи
325
Процессор
305
Память
310
Устройство ввода
320
Вывод мультимедиа
315
Пользователь
301

ФИГ. 3

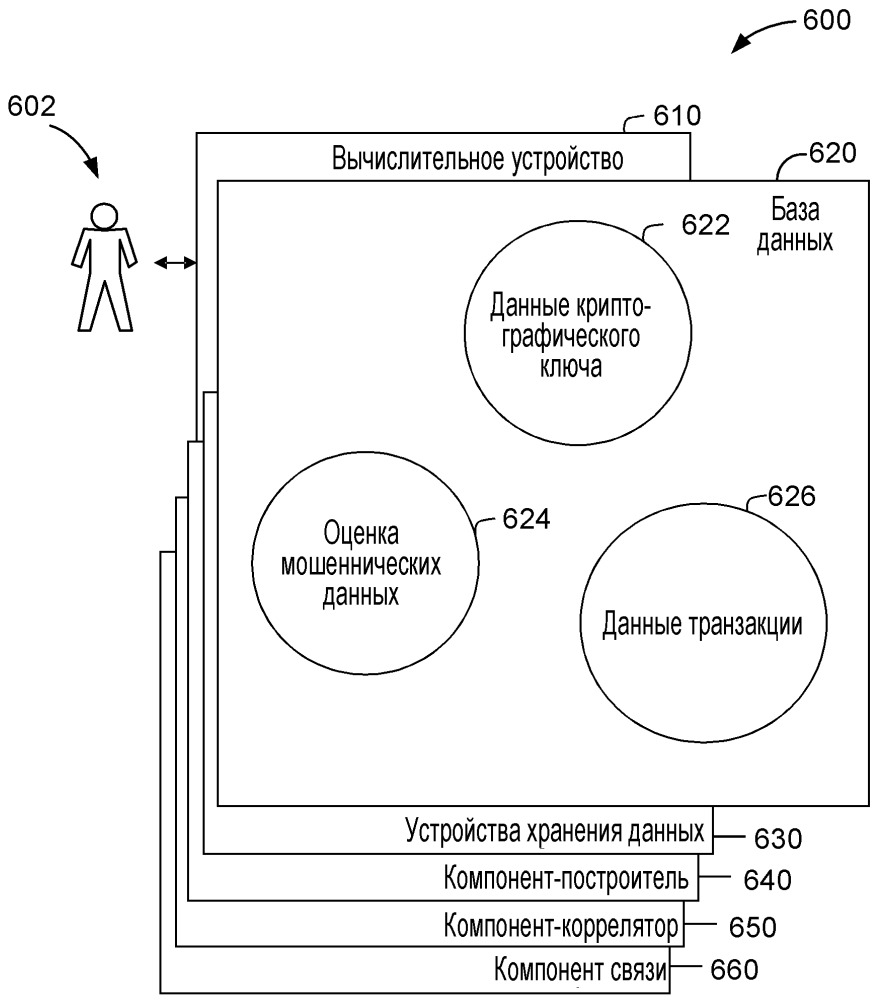

434
Запоминающее устройство
420
Интерфейс хранения
405
Процессор
410
Память
401
415
Интерфейс связи
К/от удаленного устройства

ФИГ. 4

**ФИГ. 5**

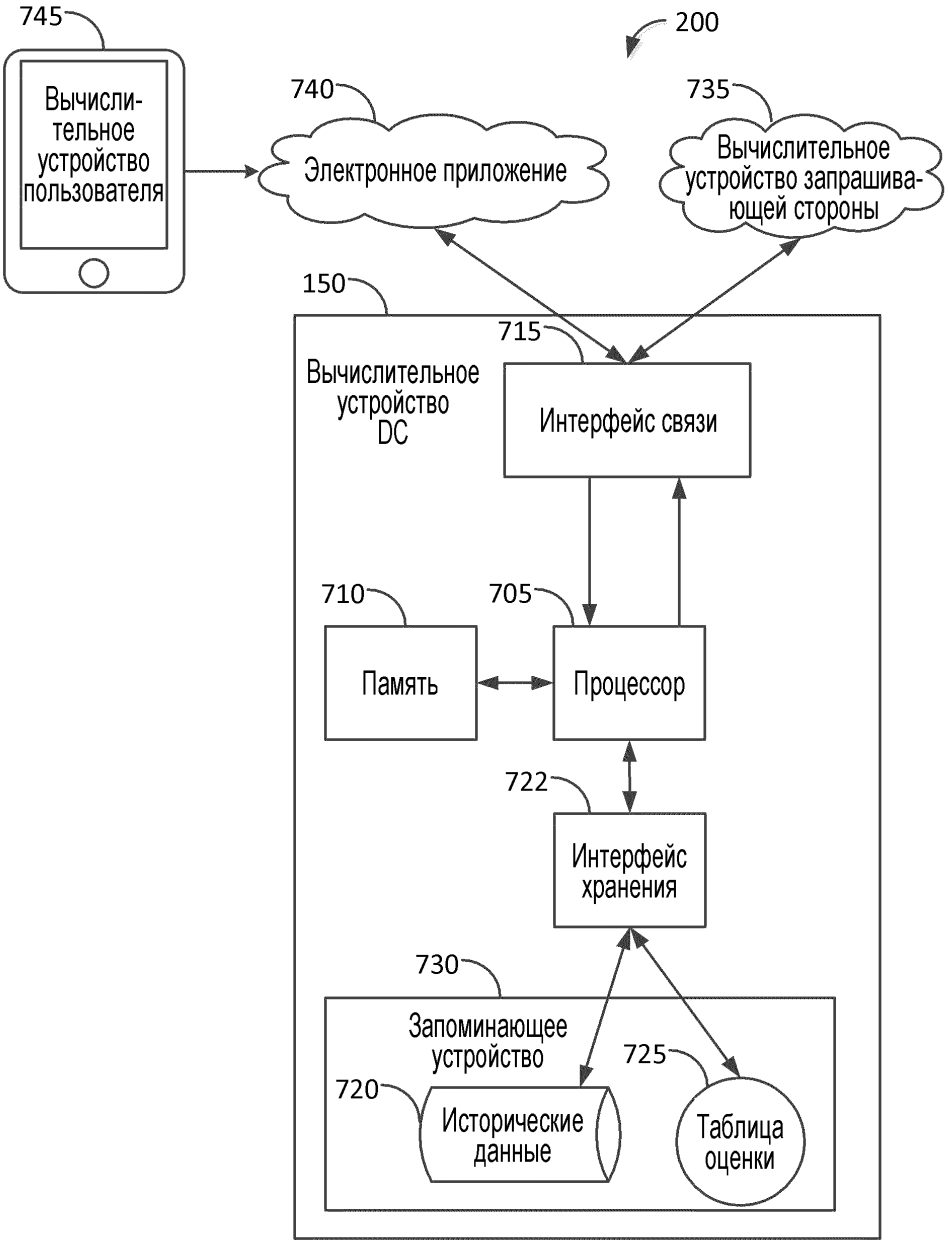

500
505
Принимают первые данные криптографического ключа, которые включают в себя зашифрованные биометрические данные на-устройстве, первый идентификатор устройства, и первый идентификатор счета
510
Сохраняют первые данные криптографического ключа в базе данных
515
Принимают сообщение запроса аутентификации, которое включает в себя вторые данные криптографического ключа, включающие в себя второй идентификатор устройства, и второй идентификатор счета
520
Соотносят первые данные криптографического ключа с вторыми данными криптографического ключа
525
Определяют оценку мошенничества для сообщения запроса аутентификации
530
Сохраняют оценку мошенничества в базе данных как часть исторических данных, ассоциированных с первыми данными криптографического ключа
535
Строят таблицу оценки для первого идентификатора счета, при этом таблица оценки мошенничества включает в себя одну или более оценки мошенничества, хранящиеся в базе данных
540
Автоматически генерируют сообщение ответа аутентификации в ответ на сообщение запроса аутентификации
545
Передают сообщение ответа аутентификации

6


600
602
610
Вычислительное устройство
620
База данных
622
Данные крипто-графического ключа
624
Оценка мошеннических данных
626
Данные транзакции
Устройства хранения данных
630
Компонент-построитель
640
Компонент-коррелятор
650
Компонент связи
660

**ФИГ. 6**

7


745
Вычисли-
тельное
устройство
пользователя
200
740
Электронное приложение
735
Вычислительное
устройство запрашива-
ющей стороны
150
715
Вычислительное
устройство
DC
Интерфейс связи
710
705
Память
Процессор
722
Интерфейс
хранения
730
Запоминающее
устройство
725
720
Исторические
данные
Таблица
оценки

**ФИГ. 7**