(19) Евразийское патентное ведомство

(11) 041505 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.10.31

(21) Номер заявки
201791674

(22) Дата подачи заявки
2017.08.22

(51) Int. Cl. *G06F 21/42* (2013.01)

(54) СПОСОБ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЯ И СИСТЕМА, ЕГО РЕАЛИЗУЮЩАЯ

(43) **2019.02.28**
(96) **2017000074 (RU) 2017.08.22**

(71)(73) Заявитель и патентовладелец:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "СЭЙФТЕК" (RU)

(74) Представитель:
Черняев М.А., Яшмолкина М.Л., Котлов Д.В., Яремчук А.А. (RU)

(56) US-A1-20160112437
US-A1-20060168657

(57) Изобретение относится к области обработки данных, предназначенных для идентификации и аутентификации пользователя. Техническим результатом является обеспечение защищенного процесса аутентификации пользователя и сокращение времени аутентификации пользователя. При этом заявленный способ позволяет организовать разделение (обмен) ключей несколькими способами, использовать как симметричную, так и асимметричную криптографию для подтверждения, а также выполнить необходимые требования по защищенности и секретности в процессе упомянутого разделения. Метод основан на том, что для подтверждения используется устройство (4), в базовом варианте представляющее собой смартфон, который в настоящее время есть у подавляющего большинства пользователей информационных систем. Данное устройство взаимодействует с сервисом подтверждения (3), который выполняет транспортные функции (взаимодействие с устройствами подтверждения (4) пользователей через каналы связи) и функции безопасности (проверку подтверждений), а также обеспечивает взаимодействие с информационными системами (прикладными сервисами) (2).

041505 B1

041505 B1

Область техники

Изобретение относится к области обработки данных, предназначенных для идентификации и аутентификации пользователя.

Уровень техники

Сфера применения данных по идентификации пользователя является достаточно обширной, в частности, аутентификация пользователей распространена на портальных решениях в сети "Интернет", например

подтверждение операции входа на портал;

подтверждение разрешения передачи данных от одного портала другому (например, когда используется "вход через Google Account", "вход через Facebook", "вход через Vkontakte" и др. типы Single Sign-On решений);

подтверждение данных платежных операций

в системах дистанционного банковского обслуживания (онлайн-банкинг) при осуществлении платежных и других операций;

при проведении операций по платежным картам в онлайн-платежах (Card-Not-Present-операции) в качестве способа подтверждения обладания платежной картой (например, при использовании VISA 3D Secure, MasterCard SecureCode);

подтверждение волеизъявлений в системах электронного документооборота

визирование электронных документов с удостоверением личности визирующего и т.п.

В информационных системах, автоматизирующих различные виды документооборота внутри или между организациями и/или физическими лицами, для подтверждения волеизъявлений используются различные виды подтверждений. Подтверждение необходимо для того, чтобы удостоверить личность, выражающую волеизъявление, а также для обеспечения функций безопасности при автоматизации процесса обмена документами.

В критичных с точки зрения безопасности информационных системах, например в системах дистанционного банковского обслуживания, платежных системах, системах сбора решений коллегиальных органов управления и пр., методы подтверждения должны обеспечивать широкий круг функций безопасности, включающий

подтверждение авторства;

возможность обнаружения факта внесения изменений после подтверждения.

Традиционно эти задачи решаются средствами криптографической защиты информации, на основе которых работают системы и средства электронной подписи. То есть для электронного документа или транзакции вырабатывается электронная подпись, которая становится реквизитом документа, описывающего волеизъявление. И она обеспечивает необходимые функции безопасности.

Для выработки электронной подписи и хранения ключа электронной подписи широко применяются различные криптографические программные и аппаратные средства, такие как токены, смарт-карты, например линейка продуктов SafeNet Authenticators, или специализированное программное обеспечение, такое как КриптоПро CSP, Microsoft Base Cryptographic Provider и т.п. При этом данные средства функционируют в среде персонального компьютера и зачастую являются причинами неудобств для пользователя, так как сложны в настройке и использовании.

Чтобы упростить использование средств подтверждения, часто используют генераторы одноразовых паролей, например eToken PASS, которые представляют собой автономные устройства, формирующие одноразовые пароли.

Основным недостатком данных устройств является тот факт, что формируемые ими одноразовые пароли не обеспечивают неизменности электронного документа. Они могут только подтвердить, что определенное лицо обладает данным устройством. То есть если завладеть кодом или несколькими кодами, сформированными данным устройством, то можно подтвердить любой электронный документ независимо от содержания. Это означает, что электронный документ или транзакция могут быть изменены после подтверждения. Следовательно, данные устройства не обеспечивают необходимых функций безопасности.

Другим видом автономных устройств, формирующих подтверждения, являются MAC-вычислители (Message Authentication Code). Их другое название - TAN-генераторы (Transaction Authentication Number). Например, https://www.vasco.com/products/two-factor-authenticators/hardware/card-readers/digipass-836.html

В данный тип устройств вручную или по оптическому каналу вносится ограниченный набор информации (например, последние 6 цифр счета получателя), на основании которых вычисляется код подтверждения операции, привязанный к введенному значению.

Эти устройства предоставляют высокий уровень безопасности, но в использовании являются очень неудобными, так как требуют большого количества ручных операций:

ввод пин-кода на генератор;

ввод значений (обычно до 20 цифр) для вычисления кода;

получение кода;

ввод его в информационную систему.

При этом данное устройство всегда должно быть при себе.

Так как во многих информационных системах, ориентированных на широкий круг неопытных пользователей, одним из решающих факторов успешности является удобство, то широкое распространение получили способы подтверждения, когда некий код подтверждения приходит из информационной системы на мобильный телефон пользователю посредством SMS-сообщения или PUSH-уведомления. И этот код должен быть введен в интерфейс информационной системы для подтверждения. При этом код подтверждения передается посредством незащищенных каналов (SMS или PUSH), т.е. он доступен для прочтения третьим лицам. Следовательно, данный метод также не обеспечивает необходимых функций безопасности, хоть и обладает высоким уровнем удобства. Подтверждением этому являются рекомендации регуляторов (http://iz.ru/news/636249?page=1) в области информационной безопасности и институтов по стандартизации не использовать SMS для передачи кодов подтверждения (https://pages.nist.gov/800-63-3/), а также прямой запрет производителей платформ для смартфонов (Apple, Google, Microsoft) на передачу конфиденциальной информации посредством PUSH-уведомлений.

Сущность изобретения

Заявленное решение направлено на обеспечение функций безопасности, при этом значительно упрощая процесс аутентификации пользователя, повышая удобство организации процесса обмена и обработки информации по сравнению с существующими способами подтверждения.

Техническим результатом является обеспечение защищенного процесса аутентификации пользователя и сокращение времени аутентификации пользователя. При этом заявленный способ позволяет организовать разделение (обмен) ключей несколькими способами, использовать как симметричную, так и асимметричную криптографию для подтверждения, а также выполнить необходимые требования по защищенности и секретности в процессе упомянутого разделения.

Изобретение реализуется за счет осуществления способа подтверждения подлинности данных пользователя, содержащий этапы, на которых

на прикладном сервисе инициируют процедуру проверки подлинности данных, полученных от устройства ввода данных пользователя, в ходе которой осуществляют передачу полученных от устройства ввода данных пользователя данных на сервис подтверждения;

сервис подтверждения передает данные, которые подлежат проверке на подлинность и полученные от прикладного сервиса, на вычислительное устройство пользователя, которое выполнено с возможностью ввода пользователем команды подтверждения подлинности данных, полученных прикладным сервисом от устройства ввода данных пользователя;

после чего вычислительное устройство пользователя в ответ на получение подтверждения подлинности данных, полученных прикладным сервисом от устройства ввода данных пользователя, формирует код подтверждения данных (КПД), который формируется на основании, по меньшей мере,

a) содержания данных, полученных от устройства ввода данных пользователя прикладным сервисом;

b) уникальной секретной последовательности пользователя (УСПП);

после чего выполняют передачу сформированного кода подтверждения данных на сервис подтверждения;

после чего на сервисе подтверждения выполняют проверку сформированного кода подтверждения данных и передают результат проверки прикладному сервису;

в ответ на успешную проверку сформированного кода подтверждения данных считают данные подлинными.

В частном варианте реализации способа КПД формируется дополнительно на основании, по меньшей мере,

времени выработки кода подтверждения данных;

токена вычислительного устройства пользователя.

В другом частном варианте реализации способа УСПП хранится на вычислительном устройстве пользователя.

В другом частном варианте реализации способа токен вычислительного устройства пользователя формируется на основании по меньшей мере одного типа информации, выбираемого из группы

серийный номер устройства;

IMEI устройства;

MAC-адрес;

версия операционной системы устройства;

идентификатор программного обеспечения устройства.

В другом частном варианте реализации способа формирование КПД на вычислительном устройстве пользователя и его проверка на сервисе подтверждения осуществляются криптографическим способом.

В другом частном варианте реализации способа передача данных пользователя от сервиса подтверждения на вычислительное устройство пользователя выполняется через прикладной сервис.

В другом частном варианте реализации способа КПД от вычислительного устройства пользователя передается в сервис подтверждения через прикладной сервис.

В другом частном варианте реализации способа передача КПД через сервис осуществляется в автоматическом режиме с помощью канала передачи данных или с помощью ручного ввода информации в прикладной сервис пользователем.

В другом частном варианте реализации способа вычислительное устройство пользователя представляет собой мобильный телефон, смартфон, планшет, ноутбук, фаблет, портативную игровую приставку или носимое устройство в виде смарт-часов, или смарт-браслета.

В другом частном варианте реализации способа УСПП создается на сервисе подтверждения и передается в вычислительное устройство пользователя.

В другом частном варианте реализации способа УСПП передается по меньшей мере двумя частями в вычислительное устройство пользователя.

В другом частном варианте реализации способа передача одной из частей УСПП осуществляется в виде двумерного графического кода или информации, отображаемой на устройстве отображения информации, или последовательности звуковых сигналов.

В другом частном варианте реализации способа части УСПП передаются по различным каналам передачи данных.

В другом частном варианте реализации способа УСПП передается по защищенному каналу передачи данных.

В другом частном варианте реализации способа передача УСПП от сервиса на вычислительное устройство пользователя осуществляется через прикладной сервис.

В другом частном варианте реализации способа после получения вычислительным устройством пользователя УСПП на нем формируется пара закрытый-открытый ключ.

В другом частном варианте реализации способа на вычислительном устройстве пользователя КПД формируется на основании данных открытого ключа, использующихся в качестве данных, полученных от пользователя и для которых проверяется подлинность.

В другом частном варианте реализации способа КПД вместе с открытым ключом передаются на сервис подтверждения.

В другом частном варианте реализации способа на этапе проверки данных на сервисе подтверждения выполняется проверка подлинности открытого ключа с помощью проверки КПД и, в случае если проверка успешна, то выполняется регистрация открытого ключа для вычислительного устройства пользователя на сервисе подтверждения для дальнейшей проверки КПД.

В другом частном варианте реализации способа при формировании КПД на вычислительном устройстве пользователя в качестве УСПП используется закрытый ключ, а при проверке на сервисе подтверждения - зарегистрированный открытый ключ для данного вычислительного устройства пользователя.

Заявленное решение реализуется также за счет осуществления системы подтверждения пользователем подлинности данных, направленных на прикладной сервис, которая содержит

устройство ввода данных пользователя, с помощью которого данные формируются и передаются по каналу связи на прикладной сервис;

прикладной сервис, выполненный с возможностью проверки подлинности данных, полученных от устройства ввода данных пользователя, в ходе которой осуществляют передачу данных, полученных от устройства ввода данных пользователя на сервис подтверждения;

сервис подтверждения, выполненный с возможностью передачи данных, полученных от устройства ввода данных пользователя и для которых проверяется подлинность, на вычислительное устройство пользователя, которое выполнено с возможностью ввода пользователем команды подтверждения подлинности данных, полученных от устройства ввода данных, причем вычислительное устройство пользователя, выполненное с возможностью в ответ на ввод команды подтверждения подлинности данных, полученных от пользователя, посредством устройства ввода данных пользователя, прикладным сервисом осуществляет формирование кода подтверждения данных, характеризующегося тем, что упомянутый код подтверждения формируется на основании, по меньшей мере, содержания данных, полученных от устройства ввода данных пользователя прикладным сервисом, и уникальной секретной последовательности пользователя (УСПП); и выполнено с возможностью передачи сформированного кода подтверждения данных на сервис подтверждения, который выполнен с возможностью проверки сформированного кода подтверждения данных и передачи результата проверки прикладному сервису, который в ответ на успешную проверку считает данные, полученные от устройства ввода данных пользователя, подлинными.

В частном варианте реализации системы вычислительное устройство пользователя представляет собой мобильный телефон, смартфон, планшет, ноутбук, фаблет, портативную игровую приставку или носимое устройство в виде смарт-часов или смарт-браслета.

В другом частном варианте реализации системы код подтверждения данных формируется дополнительно на основании, по меньшей мере,

времени выработки кода подтверждения данных;

токена вычислительного устройства пользователя.

В другом частном варианте реализации системы УСПП создается на сервисе подтверждения и хра-

нится на вычислительном устройстве пользователя. В другом частном варианте реализации системы токен вычислительного устройства пользователя формируется на основании по меньшей мере одного типа информации, выбираемого из группы

серийный номер устройства;

IMEI устройства;

MAC-адрес;

версия операционной системы устройства;

идентификатор программного обеспечения устройства.

В другом частном варианте реализации системы УСПП передается по меньшей мере двумя частями на вычислительное устройство пользователя.

В другом частном варианте реализации системы передача одной из частей УСПП осуществляется в виде двумерного графического кода или информации, отображаемой на устройстве отображения информации, или последовательности звуковых сигналов.

В другом частном варианте реализации системы части УСПП передаются по различным каналам передачи данных.

В другом частном варианте реализации системы после получения вычислительным устройством пользователя УСПП на нем формируется пара закрытый-открытый ключ.

В другом частном варианте реализации системы на вычислительном устройстве пользователя код подтверждения данных формируется на основании данных открытого ключа, использующихся в качестве данных, полученных от устройства ввода данных пользователя, и для которых проверяется подлинность.

В другом частном варианте реализации системы сформированный код подтверждения данных вместе с открытым ключом передается на сервис подтверждения. В другом частном варианте реализации системы сервис подтверждения осуществляет проверку подлинности открытого ключа с помощью проверки сформированного кода подтверждения данных и, в случае если проверка успешна, то выполняет регистрацию открытого ключа для вычислительного устройства пользователя для последующей проверки сформированного кода подтверждения данных. В другом частном варианте реализации системы при формировании кода подтверждения данных на вычислительном устройстве пользователя в качестве УСПП используется закрытый ключ, а при проверке на сервисе подтверждения - зарегистрированный открытый ключ для данного вычислительного устройства пользователя.

Описание чертежей

Фиг. 1-12 иллюстрируют выполнение заявленного способа,

фиг. 13 - общий вид вычислительного устройства пользователя, предназначенного для реализации заявленного способа (устройства подтверждения).

Детальное описание изобретения

Согласно фиг. 1 метод основан на том, что для подтверждения используется вычислительное устройство пользователя (4), в базовом варианте представляющее собой смартфон, который в настоящее время есть у подавляющего большинства пользователей информационных систем. Данное устройство взаимодействует с сервисом подтверждения (3), который выполняет транспортные функции (взаимодействие с вычислительными устройствами пользователей (4) через каналы связи) и функции безопасности (проверку подтверждений), а также обеспечивает взаимодействие с информационными системами (прикладными сервисами) (2).

Метод подразумевает, что подтверждение данных вырабатывается непосредственно вычислительным устройством пользователя (4) на основе выполнения математических (криптографических) преобразований над данными, полученными от пользователя (1), посредством устройства ввода данных пользователя (электронным документом или транзакцией), что позволяет однозначно определить автора и обнаружить внесение изменений после подтверждения, а также исключить использование недоверенных каналов (мобильная сеть, push-канал) связи для доставки пользователю сформированного кода подтверждения.

На этапе (S101) пользователь (1) посредством устройства ввода данных пользователя формирует данные для прикладного сервиса (2) и выполняет их передачу по выбранному каналу связи. Под каналом связи может пониматься широкий спектр средств и методов для передачи информации, в частности, проводного и/или беспроводного типа, таких как Ethernet, LAN, WLAN, Wi-Fi, оптические каналы (IrDa), NFC, Bluetooth, BLE, сеть "Интернет" и т.п.

Получив данные для подтверждения от пользователя, посредством устройства ввода данных пользователя прикладной сервис (2) инициирует процедуру проверки подлинности данных, полученных от устройства ввода данных пользователя, в ходе которой осуществляют передачу полученных данных на сервис подтверждения (3) на этапе (S102). Далее на этапе (S103) с помощью сервиса подтверждения (3) осуществляется передача данных, полученных от прикладного сервиса (2) на вычислительное устройство пользователя (4), выполненное с возможностью получения от пользователя (1) команды подтверждения правильности данных.

Вычислительное устройство пользователя (4) выполняет взаимодействие (S104) с пользователем

(1), в процессе которого пользователь (1) выполняет ознакомление с данными, которые он подтверждает, и выражает согласие с их содержанием, т.е. даёт команду подтверждения правильности данных.

На этапе (S105) устройство (4) в ответ на получение команды от пользователя (1) осуществляет формирование кода подтверждения данных (КПД) и выполняет его передачу на сервис подтверждения (3). Генерация такой команды может осуществляться с помощью ввода кода подтверждения (например, пароля), взаимодействия с графическим интерфейсом пользователя (GUI) на устройстве (4), ввода голосовой команды с помощью NFC аутентификатора, биометрических средств (сканер отпечатка пальцев, сканер сетчатки глаза) и т.п.

Затем сервис подтверждения (3) выполняет проверку КПД и передает результат проверки прикладному сервису (2) на этапе (S106). В ответ на успешную проверку считают данные, полученные от пользователя посредством устройства ввода данных пользователя, подтвержденными. В ходе успешной проверки формируются данные подтверждения процесса аутентификации пользователя для целей такой проверки, например транзакции или логина на веб-ресурсе.

КПД формируется на основании одного или более типов данных, которые выбираются из группы содержание данных, время выработки КПД, уникальной секретной последовательности пользователя (УСПП) или токена вычислительного устройства пользователя (4). Дополнительно КПД может также формироваться с использованием вычислительных возможностей SIM-карты (Subscriber Identification Module) и процессора устройства (4), в случае, когда в качестве вычислительного устройства пользователя (4) используется смартфон или планшет.

УСПП хранится на вычислительном устройстве пользователя (4).

Токен вычислительного устройства пользователя (4) формируется на основании по меньшей мере одного типа информации, выбираемого из группы

серийный номер устройства;

IMEI устройства;

MAC-адрес;

версия операционной системы устройства;

идентификатор программного обеспечения устройства.

Как показано на фиг. 2, передача данных от сервиса подтверждения (3) в вычислительное устройство пользователя (4) может выполняться через прикладной сервис (2) (S201). При этом способ передачи может быть автоматический с помощью заданного канала связи (S202); автоматизированный с применением средств автоматизации передачи информации при отсутствии канала связи у вычислительного устройства пользователя (4), например оптический, звуковой или радиоканал (фиг. 3), с помощью устройства авторизации пользователя (5), например терминала.

В случае использования устройства авторизации (5) информация сначала передается (S203) на него, после чего считывается (S204) вычислительным устройством пользователя (4). Считывание информации может осуществляться с помощью различных каналов передачи данных, проводного и/или беспроводного типа, оптических, световых, радиоканала, звуковых и т.п.

На фиг. 4 показан пример ручного ввода информации в случае, когда отсутствует соединение между вычислительным устройством пользователя (4) и прикладным сервисом (2). Информация может предоставляться в виде, воспринимаемом человеком, при этом информация передается (S205) на устройство авторизации (5) и вводится пользователем (1) в вычислительное устройство пользователя (4) вручную, например, в виде отображенного на экране устройства (5) кода или записи воспроизводимого звукового сигнала устройством (4).

Как показано на фиг. 5, может использоваться дополнительное устройство (6), канал связи (S207), который используется пользователем (1), например персональный компьютер, смартфон, планшет или терминал, к которому подключается вычислительное устройство пользователя (4).

Согласно фиг. 6, КПД от вычислительного устройства пользователя (4) может передаваться в сервис подтверждения (3) через прикладной сервис (2). Передача КПД может осуществляется в автоматическом режиме с помощью канала передачи данных или с помощью ручного ввода информации в прикладной сервис (2) пользователем (1), как изображено на фиг. 7. Ручной ввод КПД в сервис (2) может (S303) осуществляться с помощью ввода кода или иной информации в интерфейс прикладного сервиса (2) (S304). Процесс персонализации вычислительного устройства пользователя (4) в рамках описанного метода всегда начинается с обмена уникальной секретной последовательностью пользователя (УСПП) между сервисом подтверждения (3) и вычислительным устройством пользователя (4). УСПП формируется на стороне сервиса подтверждения (3), после чего подразумевается несколько способов передачи его в вычислительное устройство (4): передача УСПП полностью (в случае наличия доверенного канала между вычислительным устройством пользователя и прикладным сервисом (2), обычно это означает из-рук-в-руки в печатном виде); передача УСПП двумя частями по разным каналам, когда есть вероятность компрометации одного из каналов передачи (например, один канал - монитор компьютера пользователя; второй - SMS или email); передача УСПП онлайн, если существует защищенный канал между вычислительным устройством пользователя (4) и сервисом подтверждения (3) или между вычислительным устройством пользователя (4) и прикладным сервисом (2).

На фиг. 8 представлен пример передачи УСПП (7) в вычислительное устройство пользователя (4). УСПП (7) формируется сервисом подтверждения (3) и передается (S401) в вычислительное устройство пользователя (4). УСПП (7) может передаваться в виде информации, закодированной визуальным способом, например двухмерный штрих-код, QR-код и т.п., либо в виде физического носителя (распечатка) или путем отображения на устройстве авторизации (5). УСПП (7) вносится (S402) в вычислительное устройство пользователя (4) путем его считывания с помощью соответствующих средств устройства (4).

Как показано на фиг. 9 УСПП (7) может также передаваться по меньшей мере двумя частями на вычислительное устройство пользователя (4), в частности, одна из частей (8) может представлять собой информацию, закодированную визуальным способом, например двухмерный штрих-код; другая часть (9) информацию в человекочитаемом виде, например текст или код.

Части УСПП (8) и (9) могут передаваться по разным каналам передачи данных, например первая часть (8) путем отображения (S403) на устройстве авторизации (5), например мониторе терминала, вторая (9) - путем отправки SMS (Short Message Service) сообщения или PUSH уведомления (S404). УСПП вносится в вычислительное устройство пользователя (4) путем считывания первой части (8) кода и ввода пользователем (1) второй части (9) с последующим их объединением (S405) с помощью программно-аппаратных средств устройства (4).

Согласно фиг. 10 возможен также способ передачи УСПП (7) с помощью защищенного канала передачи данных (S406).

Согласно фиг. 11 УСПП (7) может также передаваться с использованием защищенного канала передачи данных между вычислительным устройством пользователя (4) и прикладным сервисом (2). При этом УСПП (7) передается от сервиса подтверждения (3) в прикладной сервис (2) (S407), после чего по защищенному каналу передается в вычислительное устройство пользователя (4) (S408).

После того как вычислительное устройство пользователя (4) и сервис подтверждения (3) имеют разделенное (одинаковое) значение УСПП, устройство (4) имеет возможность выполнять операции подтверждения в соответствии с методом.

Тем не менее, использование асимметричной криптографии для подтверждения является более предпочтительным из-за своих свойств. В частности, в этом случае выработать подтверждение может только вычислительное устройство пользователя (4), а проверить его может любой желающий, в том числе сервис подтверждения (2). Но для использования асимметричной криптографии необходимо решить задачу сопоставления конкретного устройства (4) с записью на сервисе подтверждения (2). Использование инфраструктуры открытых ключей и цифровых сертификатов является крайне сложным технически и организационно, поэтому метод предполагает для решения этой задачи использовать уже разделенное значение УСПП.

При этом устройство (4) формирует пару закрытый-открытый ключ и предоставляет открытый ключ сервису подтверждения (2) для регистрации. Для удостоверения, что открытый ключ не был подменен в процессе передачи, устройство (4) вырабатывает для открытого ключа подтверждение авторства и неизменности на основе УСПП. И после успешной регистрации открытого ключа дальнейшие подтверждения вырабатываются на основе асимметричной криптографии.

Согласно фиг. 12 после получения вычислительным устройством пользователя (4) УСПП (S409) на нем формируется пара закрытый-открытый ключ с помощью асимметричных криптографических алгоритмов (S410). На устройстве (4) КПД может также формироваться на основании данных открытого ключа, использующихся в качестве содержания данных, полученных от пользователя (S411). КПД также может быть передан вместе с открытым ключом на сервис подтверждения (3) (S412).

На этапе проверки данных на сервисе подтверждения (3) выполняется проверка неизменности открытого ключа с помощью проверки КПД, и в случае если проверка успешна, выполняется регистрация открытого ключа для устройства (4) на сервисе подтверждения (3) для дальнейшей проверки КПД.

При формировании КПД на вычислительном устройстве пользователя (4) в качестве УСПП может использоваться закрытый ключ, а при проверке на сервисе подтверждения (3) - зарегистрированный открытый ключ для данного устройства (4).

Результат асимметричного криптографического преобразования представляет собой длинную (до 512 символов) цифробуквенную последовательность. Поэтому предпочтительно осуществлять такую передачу кода в автоматическом режиме. Использование симметричной криптографии позволяет выполнять "урезание" результата криптографических преобразований до любой длины (обычно 6-10 цифр и букв), что делает возможным передать код подтверждения автоматизировано или вручную. Но при наличии канала связи данное упрощение снижает уровень безопасности процесса подтверждения, так как "урезанный" код, передаваемый с участием человека, менее стоек к перебору, а также подвержен методам социальной инженерии (когда значение кода обманным путем выведывается у пользователя мошенником при общении). Таким образом, метод позволяет организовать максимально удобное разделение (обмен) УСПП (ключей) несколькими способами, использовать как симметричную, так и асимметричную криптографию для подтверждения, а также выполнить необходимые требования по защищенности и секретности в процессе разделения.

Согласно фиг. 13 представлена принципиальная блок-схема вычислительного устройства (200), ко-

торое может использоваться для реализации функциональности вычислительного устройства пользователя (4), прикладного сервиса (2), сервиса подтверждения (3) и других устройств, в частности устройств (5) и (6). С помощью набора вычислительных устройств (200) реализуется система, обеспечивающая программно-аппаратное выполнение заявленного способа.

Система подтверждения данных пользователя реализуется с помощью нескольких вычислительных устройств (200), например персонального компьютера, ноутбука, планшета, сервера, серверного кластера, мейнфрема, носимых смарт-устройств (часы, браслет) и т.п.

В общем случае устройство (200) содержит один или более процессоров (201), выполняющих основную вычислительную работу при реализации этапов способа подтверждения данных.

Оперативную память (ОЗУ) (202), предназначенную для оперативного хранения команд, исполняемых одним или более процессорами (201).

Средство хранения данных (203) может представлять собой жесткий диск (HDD), твердотельный накопитель (SSD), флэш-память (NAND-flash, EEPROM, Secure Digital и т.п.), оптический диск (CD, DVD, Blue Ray), мини-диск или их совокупности.

Интерфейсы ввода/вывода (В/В) (204) представляют собой стандартные порты и средства сопряжения устройств и передачи данных, выбираемые исходя из необходимой конфигурации исполнения системы (200), в частности USB (2.0, 3.0, USB-C, micro, mini), Ethernet, PCI, AGP, COM, LPT, PS/2, SATA, FireWire, Lightning и т.п.

Средства В/В (205) также выбираются из известного спектра различных устройств, например клавиатура, тачпад, сенсорный дисплей, монитор, проектор, манипулятор мышь, джойстик, трекбол, световое перо, стилус, устройства вывода звука (колонки, наушники, встроенные динамики, зуммер) и т.п.

Средства передачи данных (206) выбираются из устройств, предназначенных для реализации процесса коммуникации между различными устройствами посредством проводной и/или беспроводной связи, в частности, таким устройствами могут быть GSM модем, Wi-Fi приемопередатчик, Bluetooth или BLE модуль, GPS модуль, Глонасс модуль, NFC, Ethernet модуль и т.п.

Компоненты устройства (200) сопряжены между собой посредством общей шины передачи данных (210).

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ подтверждения пользователем подлинности данных, направленных на прикладной сервис, содержащий этапы, на которых

на прикладном сервисе (2) инициируют процедуру проверки подлинности данных, полученных от устройства ввода данных пользователя, в ходе которой осуществляют передачу полученных от устройства ввода данных пользователя данных на сервис подтверждения (3);

сервис подтверждения (3) передает данные, которые подлежат проверке на подлинность и полученные от прикладного сервиса (2), на вычислительное устройство пользователя (4), которое выполнено с возможностью ввода пользователем (1) команды подтверждения подлинности данных, полученных прикладным сервисом (2) от устройства ввода данных пользователя;

после чего вычислительное устройство пользователя (4) в ответ на получение подтверждения подлинности данных, полученных прикладным сервисом (2) от устройства ввода данных пользователя, формирует код подтверждения данных, который формируется на основании, по меньшей мере,

содержания данных, полученных от устройства ввода данных пользователя прикладным сервисом (2);

уникальной секретной последовательности пользователя (УСПП);

после чего выполняют передачу сформированного кода подтверждения данных на сервис подтверждения (3);

после чего на сервисе подтверждения (3) выполняют проверку сформированного кода подтверждения данных и передают результат проверки прикладному сервису (2);

в ответ на успешную проверку сформированного кода подтверждения данных считают данные подлинными.

2. Способ по п.1, характеризующийся тем, что код подтверждения данных формируется дополнительно на основании, по меньшей мере,

времени выработки кода подтверждения данных;

токена вычислительного устройства пользователя (4).

3. Способ по п.2, характеризующийся тем, что УСПП хранится на вычислительном устройстве пользователя (4).

4. Способ по п.2, характеризующийся тем, что токен вычислительного устройства пользователя (4) формируется на основании по меньшей мере одного типа информации, выбираемого из группы

серийный номер устройства;

IMEI устройства;

MAC-адрес;

версия операционной системы устройства;

идентификатор программного обеспечения устройства.

5. Способ по п.1, характеризующийся тем, что формирование кода подтверждения данных на вычислительном устройстве пользователя (4) и его проверка на сервисе подтверждения (3) осуществляются криптографическим способом.

6. Способ по п.1, характеризующийся тем, что передача данных, полученных от пользователя, которые подлежат проверке на подлинность, от сервиса подтверждения (3) на вычислительное устройство пользователя (4) выполняется через прикладной сервис (2).

7. Способ по п.1, характеризующийся тем, что сформированный код подтверждения данных от вычислительного устройства пользователя (4) передается в сервис подтверждения (3) через прикладной сервис (2).

8. Способ по п.7, характеризующийся тем, что передача сформированного кода подтверждения данных через прикладной сервис (2) осуществляется в автоматическом режиме с помощью канала передачи данных или с помощью ручного ввода информации в прикладной сервис (2) пользователем с помощью устройства ввода данных пользователя.

9. Способ по п.1, характеризующийся тем, что вычислительное устройство пользователя (4) представляет собой мобильный телефон, смартфон, планшет, ноутбук, фаблет, портативную игровую приставку или носимое устройство в виде смарт-часов или смарт-браслета.

10. Способ по п.3, характеризующийся тем, что УСПП создается на сервисе подтверждения (3) и передается в вычислительное устройство пользователя (4).

11. Способ по п.10, характеризующийся тем, что УСПП передается по меньшей мере двумя частями на вычислительное устройство пользователя (4).

12. Способ по п.11, характеризующийся тем, что передача одной из частей УСПП осуществляется в виде двумерного графического кода или информации, отображаемой на устройстве отображения информации, или последовательности звуковых сигналов.

13. Способ по п.11, характеризующийся тем, что части УСПП передаются по различным каналам передачи данных.

14. Способ по п.10, характеризующийся тем, что УСПП передается по защищенному каналу передачи данных.

15. Способ по п.14, характеризующийся тем, что передача УСПП от сервиса подтверждения (3) на вычислительное устройство пользователя (4) осуществляется через прикладной сервис (2).

16. Способ по любому из пп.10-15, характеризующийся тем, что после получения вычислительным устройством пользователя (4) УСПП в нем формируется пара закрытый-открытый ключ.

17. Способ по п.16, характеризующийся тем, что на вычислительном устройстве пользователя (4) код подтверждения данных формируется на основании данных открытого ключа, использующихся в качестве данных, полученных от пользователя, и для которых проверяется подлинность.

18. Способ по п.17, характеризующийся тем, что сформированный код подтверждения данных вместе с открытым ключом передаются на сервис подтверждения (3).

19. Способ по п.18, характеризующийся тем, что на этапе проверки подлинности данных на сервисе подтверждения (3) выполняется проверка подлинности открытого ключа с помощью проверки сформированного кода подтверждения данных и, в случае если проверка успешна, выполняют регистрацию открытого ключа для вычислительного устройства пользователя (4) на сервисе подтверждения (3) для дальнейшей проверки сформированного кода подтверждения данных.

20. Способ по п.2, характеризующийся тем, что при формировании кода подтверждения данных на вычислительном устройстве пользователя (4) в качестве УСПП используется закрытый ключ, а при проверке на сервисе подтверждения (3) - зарегистрированный открытый ключ для данного вычислительного устройства пользователя (4).

21. Система подтверждения пользователем подлинности данных, направленных на прикладной сервис, содержащая

устройство ввода данных пользователя, с помощью которого данные формируются и передаются по каналу связи на прикладной сервис (2);

прикладной сервис (2), выполненный с возможностью проверки подлинности данных, полученных от устройства ввода данных пользователя, в ходе которой осуществляют передачу данных, полученных от устройства ввода данных пользователя прикладным сервисом (2), подлежащих проверке на подлинность на сервис подтверждения (3);

сервис подтверждения (3), выполненный с возможностью передачи данных, полученных от устройства ввода данных пользователя и для которых проверяется подлинность, на вычислительное устройство пользователя (4), которое выполнено с возможностью ввода пользователем (1) команды подтверждения подлинности данных, полученных от устройства ввода данных, причем вычислительное устройство пользователя (4), выполненное с возможностью в ответ на ввод команды подтверждения подлинности данных, полученных от пользователя (1), посредством устройства ввода данных пользователя, прикладным сервисом (2) осуществляет формирование кода подтверждения данных, характеризующегося тем,

что упомянутый код подтверждения формируется на основании, по меньшей мере, содержания данных, полученных от устройства ввода данных пользователя прикладным сервисом (2), и уникальной секретной последовательности пользователя (УСПП); и выполнено с возможностью передачи сформированного кода подтверждения данных на сервис подтверждения (3), который выполнен с возможностью проверки сформированного кода подтверждения данных и передачи результата проверки прикладному сервису (2), который в ответ на успешную проверку считает данные, полученные от устройства ввода данных пользователя, подлинными.

22. Система по п.21, характеризующаяся тем, что вычислительное устройство пользователя (4) представляет собой мобильный телефон, смартфон, планшет, ноутбук, фаблет, портативную игровую приставку или носимое устройство в виде смарт-часов или смарт-браслета.

23. Система по п.21, характеризующаяся тем, что код подтверждения данных формируется дополнительно на основании, по меньшей мере,

времени выработки кода подтверждения данных;

токена вычислительного устройства пользователя (4).

24. Система по п.23, характеризующаяся тем, что УСПП создается на сервисе подтверждения (3) и хранится на вычислительном устройстве пользователя (4).

25. Система по п.23, характеризующаяся тем, что токен вычислительного устройства пользователя (4) формируется на основании по меньшей мере одного типа информации, выбираемого из группы

серийный номер устройства;

IMEI устройства;

MAC-адрес;

версия операционной системы устройства;

идентификатор программного обеспечения устройства.

26. Система по п.25, характеризующаяся тем, что УСПП передается по меньшей мере двумя частями на вычислительное устройство пользователя (4).

27. Система по п.25, характеризующаяся тем, что передача одной из частей УСПП осуществляется в виде двумерного графического кода или информации, отображаемой на устройстве отображения информации, или последовательности звуковых сигналов.

28. Система по п.27, характеризующаяся тем, что части УСПП передаются по различным каналам передачи данных.

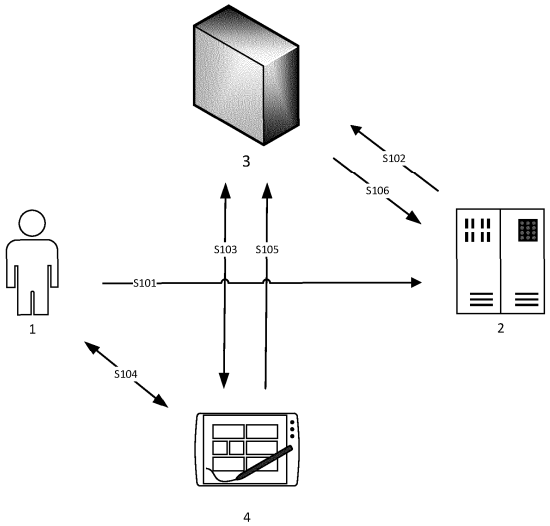
29. Система по п.27, характеризующаяся тем, что после получения вычислительным устройством пользователя (4) УСПП на нем формируется пара закрытый-открытый ключ.

30. Система по п.21, характеризующаяся тем, что на вычислительном устройстве пользователя (4) код подтверждения данных формируется на основании данных открытого ключа, использующихся в качестве данных, полученных от устройства ввода данных пользователя, и для которых проверяется подлинность.

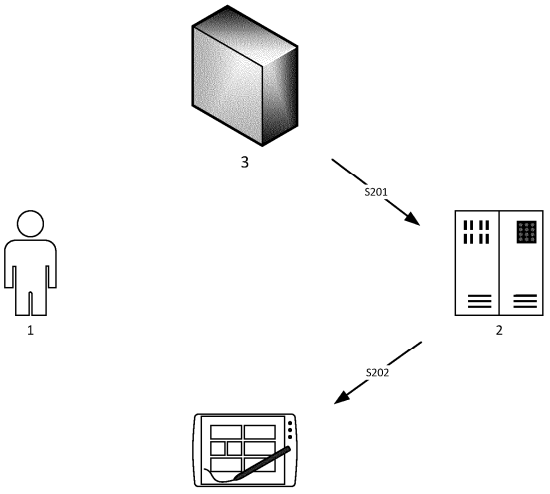
31. Система по п.30, характеризующаяся тем, что сформированный код подтверждения данных вместе с открытым ключом передается на сервис подтверждения (3).

32. Система по п.31, характеризующаяся тем, что сервис подтверждения (3) осуществляет проверку подлинности открытого ключа с помощью проверки сформированного кода подтверждения данных и, в случае если проверка успешна, выполняет регистрацию открытого ключа для вычислительного устройства пользователя (4) для последующей проверки сформированного кода подтверждения данных.

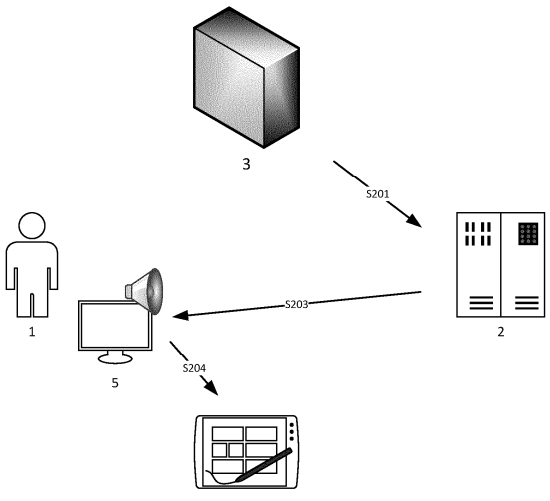
33. Система по п.21, характеризующаяся тем, что при формировании кода подтверждения данных на вычислительном устройстве пользователя (4) в качестве УСПП используется закрытый ключ, а при проверке на сервисе подтверждения (3) - зарегистрированный открытый ключ для данного вычислительного устройства пользователя (4).



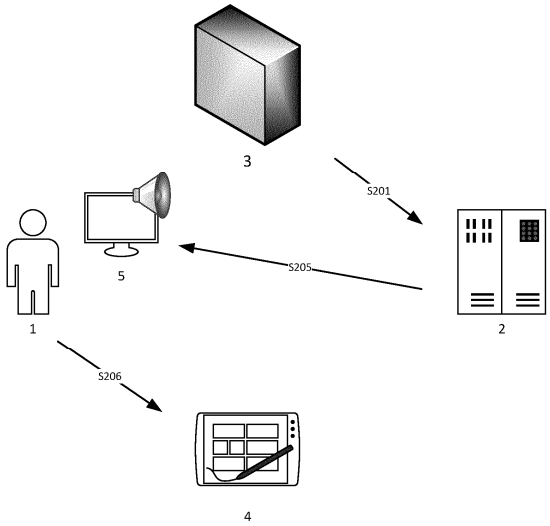
Фиг. 1



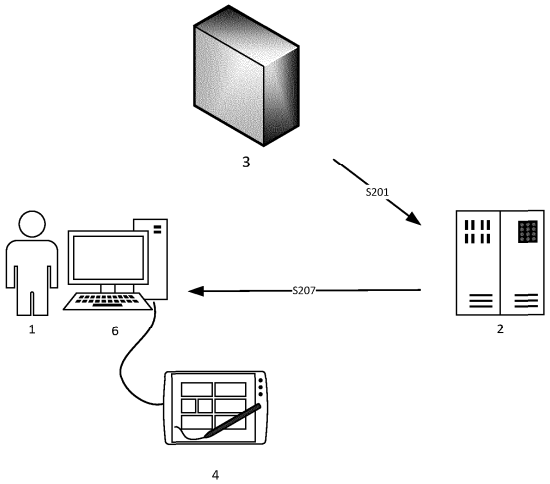
Фиг. 2



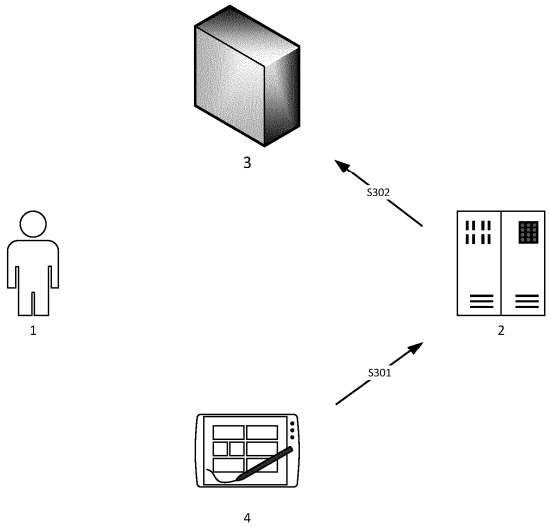
Фиг. 3



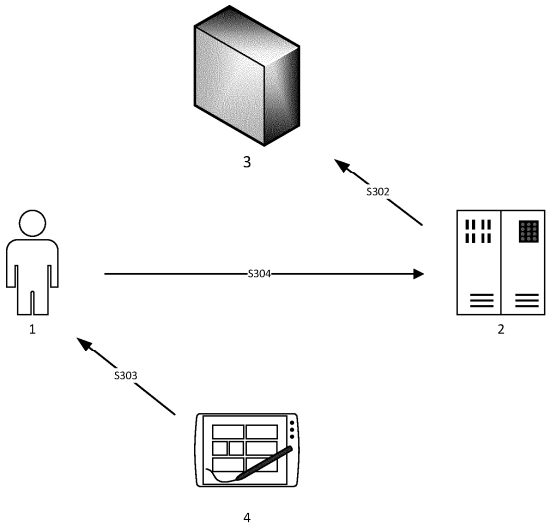
Фиг. 4



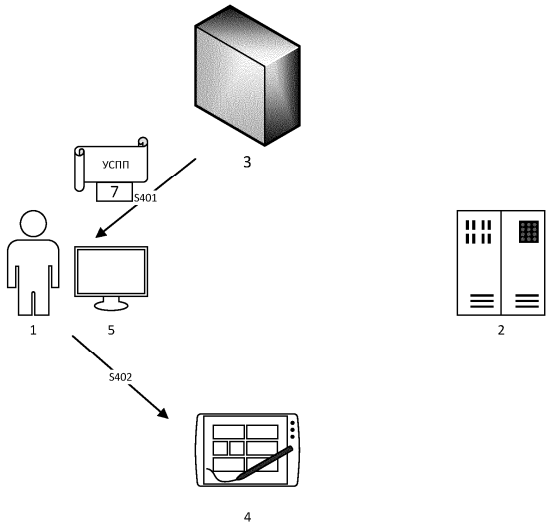
Фиг. 5



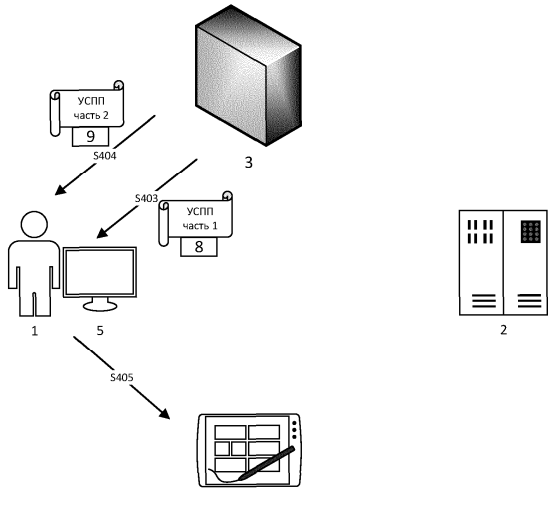
Фиг. 6



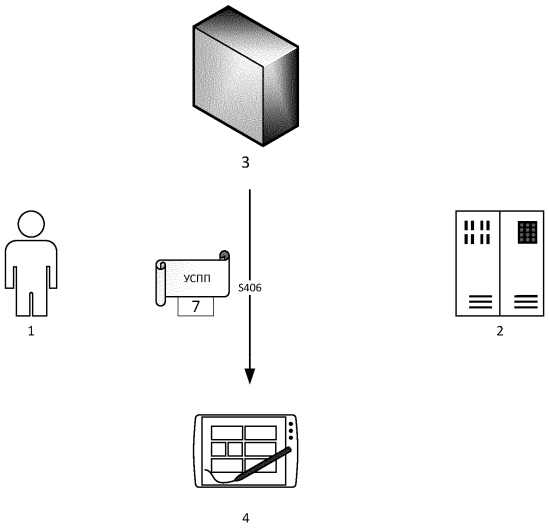
Фиг. 7



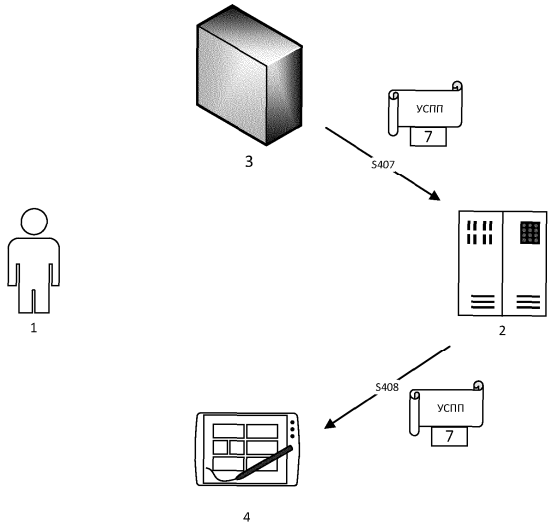
Фиг. 8



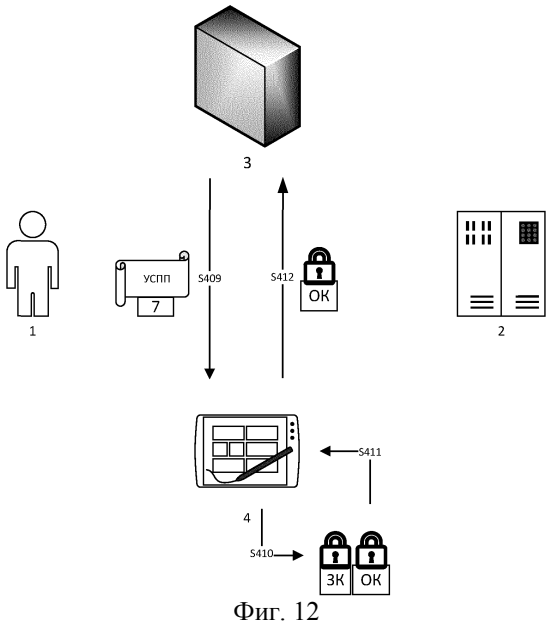
Фиг. 9



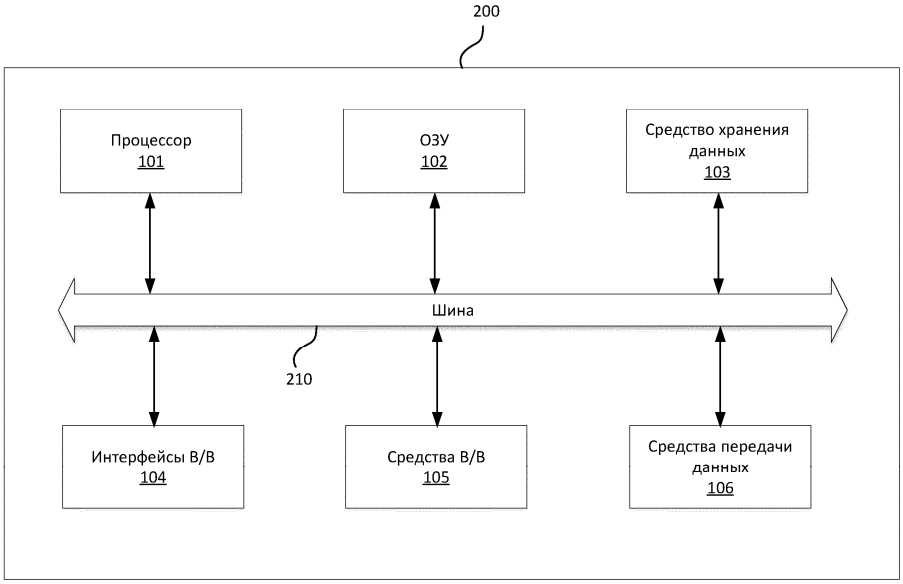
Фиг. 10



Фиг. 11



Фиг. 12


200
Процессор
101
ОЗУ
102
Средство хранения данных
103
Шина
210
Интерфейсы В/В
104
Средства В/В
105
Средства передачи данных
106

Фиг. 13