РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 676 896**(13) **C2**

(51) МПК
G06F 21/31 (2013.01)
G06F 21/45 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/31 (2006.01); G06F 21/45 (2006.01)

(21)(22) Заявка: **2016101134, 07.07.2014**

(24) Дата начала отсчета срока действия патента:
07.07.2014

Дата регистрации:
11.01.2019

Приоритет(ы):
(30) Конвенционный приоритет:
05.07.2013 NO 20130947

(43) Дата публикации заявки: **10.08.2017** Бюл. № **22**

(45) Опубликовано: **11.01.2019** Бюл. № **2**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **05.02.2016**

(86) Заявка PCT:
NO 2014/050123 (07.07.2014)

(87) Публикация заявки PCT:
WO 2015/002545 (08.01.2015)

Адрес для переписки:
119019, Москва, Гоголевский б-р, 11, этаж 3, "Гоулингз Интернэшнл Инк.", Лыу Татьяна Нгоковна

(72) Автор(ы):
ГУЛБРАНДСЕН Магнус Скраастад (NO)

(73) Патентообладатель(и):
СГЭкс АС (NO)

(56) Список документов, цитированных в отчете о поиске: **US 2008/0120707 A1, 22.05.2008. US 20070209054 A1, 06.09.2007. US 2010/0192199 A1, 29.07.2010. US 2013/0061332 A1, 07.03.2013. RU 2332807 C2, 27.08.2008.**

(54) СПОСОБ И СИСТЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К СЕТЯМ ПЕРЕДАЧИ ДАННЫХ

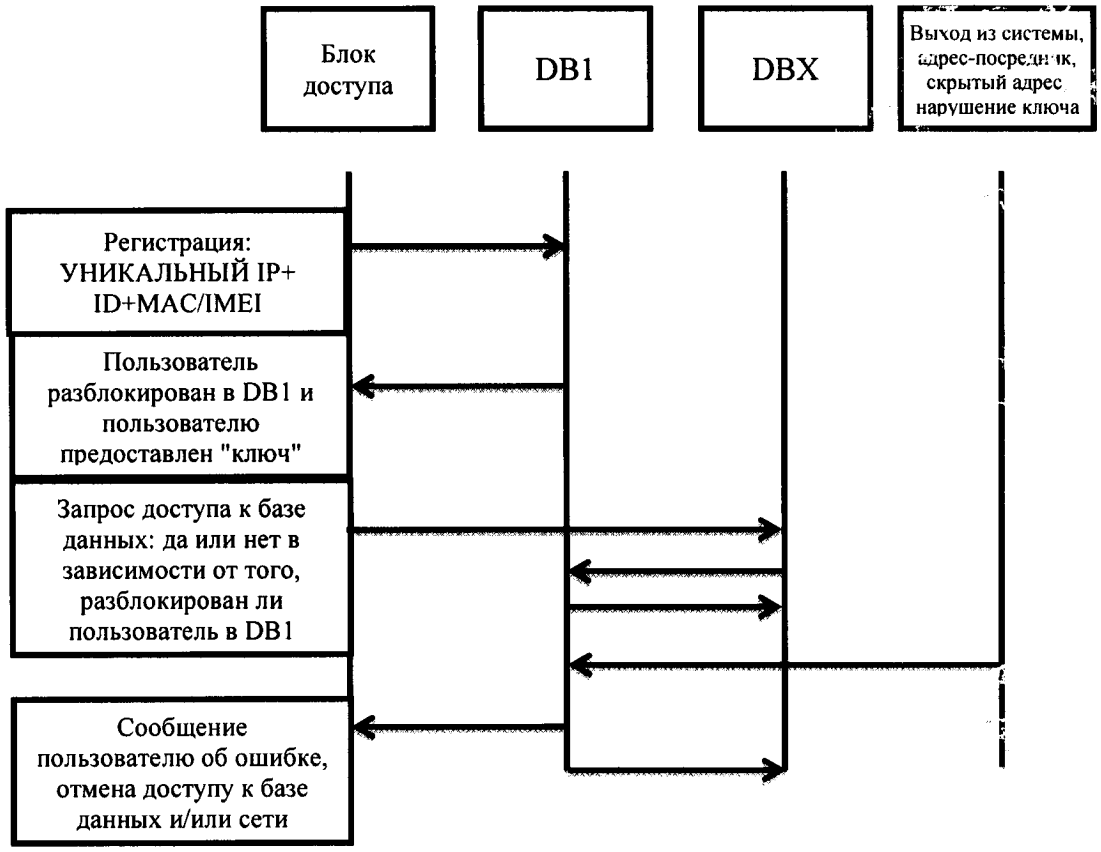
(57) Реферат:

Изобретение относится к доступу к данным, а именно к аутентификации пользователя. Технический результат – повышение эффективности аутентификации пользователей. Способ аутентификации пользователей и/или устройств, баз данных, серверов или другого оборудования, запрашивающих доступ к данным или услугам с ограниченным доступом из базы данных доступа в вычислительной сети, включает этапы: присвоение глобально уникальных связующих адресов всем устройствам в указанной вычислительной сети, причем каждое из устройств уникально привязано к конкретному пользователю, использование по меньшей мере присвоенного уникального связующего адреса, привязанного к пользователю устройства для идентификации пользователя, использование функции регистрации для аутентификации указанного идентифицированного пользователя в первой базе данных доступа в вычислительной

RU 2676896 C2

RU 2676896 C2

сети и генерирование уникального ключа пользователя для доступа к вычислительной сети, предоставление доступа к данным или услугам с ограниченным доступом на запрос пользователя во второй базе данных доступа в вычислительной сети, если присвоенный уникальный связующий адрес или ключ пользователя распознается второй базой данных доступа и указанный пользователь аутентифицирован в первой базе данных доступа, и отклонение доступа пользователя к множеству баз данных доступа и/или к указанной вычислительной сети, если уникальный ключ нарушен или при выходе пользователя из системы для указанного ключа на указанном устройстве. 2 н. и 8 з.п. ф-лы, 9 ил.



ФИГ. 3

RU 2676896 C2

RU 2676896 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 676 896**(13) **C2**

(51) Int. Cl.
G06F 21/31 (2013.01)
G06F 21/45 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/31 (2006.01); G06F 21/45 (2006.01)

(21)(22) Application: **2016101134, 07.07.2014**

(24) Effective date for property rights:
07.07.2014

Registration date:
11.01.2019

Priority:
(30) Convention priority:
05.07.2013 NO 20130947

(43) Application published: **10.08.2017** Bull. № **22**

(45) Date of publication: **11.01.2019** Bull. № **2**

(85) Commencement of national phase: **05.02.2016**

(86) PCT application:
NO 2014/050123 (07.07.2014)

(87) PCT publication:
WO 2015/002545 (08.01.2015)

Mail address:
119019, Moskva, Gogolevskij b-r, 11, etazh 3, "Goulingz Interneshnl Ink.", Lyu Tatyana Ngokovna

(72) Inventor(s):
GULBRANDSEN Magnus Skraastad (NO)

(73) Proprietor(s):
SGX AS (NO)

RU 2676896 C2

RU 2676896 C2

(54) METHOD AND SYSTEM RELATED TO AUTHENTICATION OF USERS FOR ACCESSING DATA NETWORKS

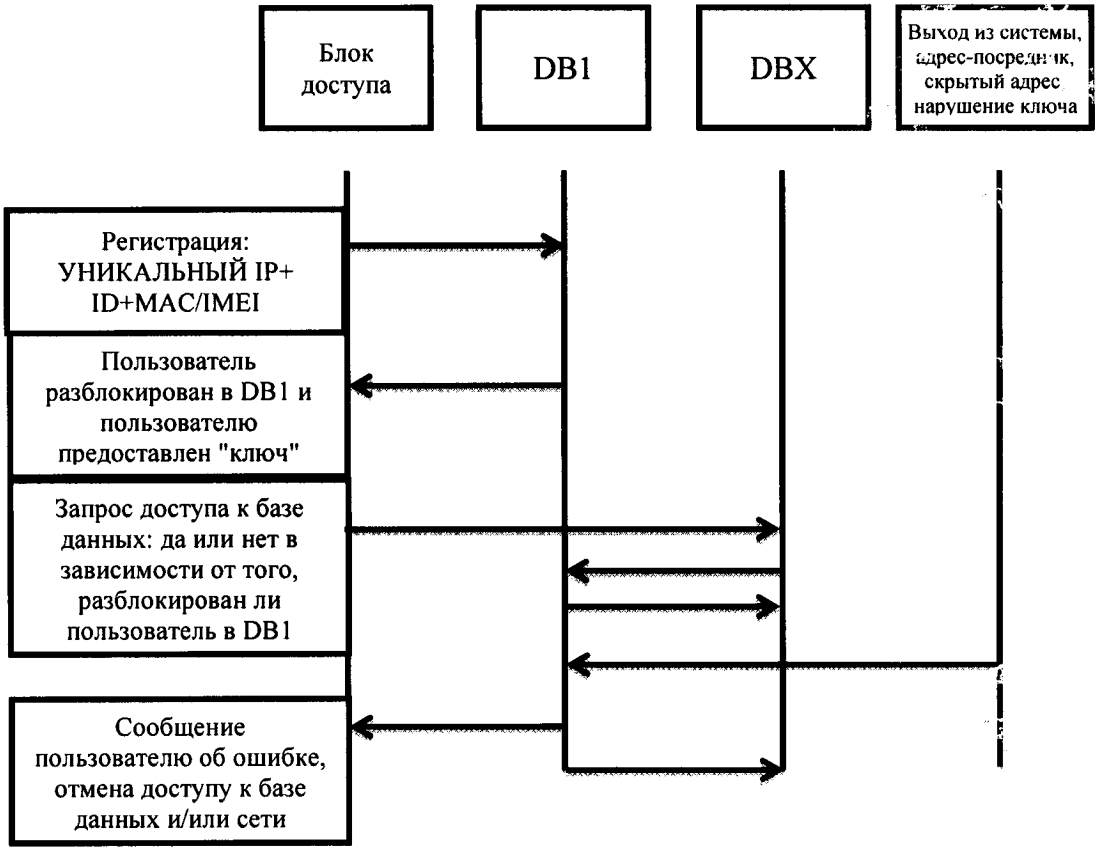
(57) Abstract:

FIELD: electrical communication engineering.

SUBSTANCE: invention relates to data access, in particular to user authentication. Method of authenticating users and/or devices, databases, servers or other equipment requesting access to restricted-access data or services from an access database in a computer network, comprises the steps of: globally assigning unique communication addresses to all devices in said computer network, wherein each of the devices being uniquely associated with particular users, using at least a unique communication address associated with the user for authenticating and identifying the user, using a login function for authenticating the user that is logged in the first access database in the computer network and generating a unique user key for access to the computer network, providing access to data or services with limited access to the user's request in the second access database in the computer network, if the assigned unique link address or user key is recognized by the second access database and said user is authenticated in the first access database, and deviation of user access to the set of access databases and/or to said computer network, if the unique key is broken or when the user logs out the system for said key at said device.

EFFECT: technical result is higher efficiency of user authentication.

10 cl, 9 dwg



ФИГ. 3

RU 2676896 C2

RU 2676896 C2

Область техники

Настоящее изобретение относится в целом к доступу к данным, осуществляемому пользователем с вычислительного устройства, аутентификации пользователя и выставлению счетов пользователю за предоставленный доступ к данным. Данные в этом контексте включают не общедоступные данные, а только данные, доступ к которым связан с определенными ограничениями. Более точно, настоящее изобретение относится способу и системе аутентификации пользователя. Изобретение также относится способу поддержания связи между базовой сетью и рядом внешних устройств и баз данных с ограниченным доступом. Изобретение дополнительно относится к платформе для установления и обеспечения прав и цен, а также для сообщения о них необходимым частям базовой сети.

Уровень техники

Широкий доступ к глобальным вычислительным сетям, который имеют индивидуальные пользователи, породил ряд сложностей, связанных с аутентификацией и авторизацией индивидуальных пользователей. Существует несколько, связанных с как обеспечением безопасности, так и практических сложностей аутентификации пользователей, которые должны аутентифицировать себя. Существование нескольких различных способов аутентификации порождает практические сложности для пользователей, а также технических сложностей в процессе связи между различными областями, клиентами и т.д. с ограниченным доступом. Существует потребность в универсальной системе идентификации и аутентификации.

Существуют разнообразные принципы аутентификации, тремя наиболее распространенными из которых являются однофакторная, двухфакторная и трехфакторная аутентификация. В случае однофакторной аутентификации пользователь аутентифицирует себя с использованием только одного "мандата", такого как мобильный телефон с SIM-картой, например, когда SIM-карта или мобильный телефон передает уникальный аппаратный код, соответствующий конкретному пользователю. Аутентификация этого типа неприемлема в случаях, в которых требуется высокая надежность, таких как транзакции или загрузка объекта с защищенными правами доступа, поскольку важно, чтобы пользователь, который аутентифицирует себя, являлся действительным зарегистрированным владельцем SIM-карты или мобильного телефона. С целью повышения надежности аутентификации обычно вводится дополнительный элемент, используемый при аутентификации, в результате чего используются два фактора. Обычно вторым элементом является что-либо, что помнит пользователь, т.е. используется фактор, отображающий что-либо, чем владеет пользователь, и фактор, отображающий что-либо, что помнит пользователь. Фактором, связанным с тем, что помнит пользователь, может являться ПИН-код, а в случае ручной аутентификации до телефону - это обычно ответ на известный вопрос.

Сложностью с факторами, используемыми для аутентификации, является их изменчивость; как фактор "владения", так и "запоминаемый" фактор могут изменяться, а запоминаемый фактор также может быть забыт.К сожалению, не существует системы, позволяющей осуществлять универсальную самоидентификацию независимо от технических средств идентификации.

В основу настоящего изобретения положена задача создания системы и способа, в который упомянутые недостатки преодолены с использованием изменчивых факторов для аутентификации пользователей услуг, подлежащих защите.

Сущность изобретения

Решение задачи настоящего изобретения достигается за счет способов и систем,

охарактеризованных в прилагаемой формуле изобретения.

В изобретении используется связующий адрес, необходимый для поддержания связи в вычислительной сети в качестве необязательного идентификатора вместе с методом аутентификации любого типа (однофакторной, двухфакторной или трехфакторной), который удостоверяет, что пользователем действительно является надлежащий пользователь. Если требуются несколько факторов, в качестве дополнительного фактора может использоваться, например, аппаратный код/идентификатор устройства доступа. Это подтверждается посредством функции регистрации, которая создает для пользователя/передает пользователю ключ и предоставляет пользователю статус аутентифицированного в регистрационной базе данных, сконфигурированной на поддержание связи. Эта регистрационная база данных может обмениваться ключом с пользователем и/или различными базами данных запросов доступа и/или обработчиками запросов доступа реальной сети.

Изобретение позволяет пользователям использовать связующий адрес (IP) для самоидентификации с обеспечением глобальной универсальной системы идентификации/аутентификации по принципу единственной подписи, которая может использоваться для осуществления любого доступа, платежа и т.п.

Использование IP-адресов гарантирует, что заданный связующий адрес используется надлежащим пользователем. Пользователь не должен иметь возможности доступа к базовой сети и получения посредством этой сети доступа к данным с ограниченным доступом без прохождения надежной авторизации с использованием уникального идентификатора пользователя, такого как, например, присвоенный IP-адрес. В одном из вариантов осуществления изобретения базовая сеть может отклонить запрос со стороны пользователя, если не была осуществлена аутентификация с использованием упомянутого уникального идентификатора. Этим способом личность пользователя может быть непосредственно связана с правами пользователя, и предотвращается получение пользователей доступа к данным с ограниченным доступом, если он не аутентифицировал себя.

За счет применения изобретения пользователь не может осуществлять связь с IP-адреса оператора, в отношении которого не действуют такие же ограничения, как в отношении оператора, предоставившего доступ пользователю. За счет предотвращения доступа пользователя посредством сети, изобретение делает невозможной попытку сохранения анонимности/отказа от идентификации (например, с использованием адреса-посредника, скрытого IP-адреса, другого IP-адреса) с целью доступа, например, к запрещенному контенту или обхода ограничений в базовой сети. Изобретение предотвращает доступ для пользователей к глобальным сетям с использованием инфраструктур других операторов помимо оператора, предоставившего доступ.

Согласно одной из особенностей изобретения предложен способ аутентификации пользователя, запрашивающего доступ к услугам вычислительной сети, включающий использование уникального связующего адреса для аутентификации и идентификации. Способ также может включать присвоение глобально уникальных связующих адресов пользователям и устройствам. Способ может включать использование функции регистрации посредством оборудования или устройства, к которому посредством аппаратного идентификатора, такого как MAC, IMEI IMSI и т.п., может быть привязан уникальный связующий адрес, такой как адрес согласно протоколу IPv6, и которое сконфигурировано на передачу и прием информации по сети. Способ согласно изобретению может включать использование аппаратного идентификатора, т.е. идентификатора, которым является по меньшей мере одно из следующего: связующий

адрес, MAC, IMEI, коде, банковский идентификатор или другое средство идентификации, которое может использоваться для аутентификации пользователя.

В случае утери одного из идентификаторов или выхода пользователя из системы способ может дополнительно включать передачу сигнала базе данных, в которой ведется учет пользователей и их авторизация, и которая сконфигурирована на обеспечение доступа рассматриваемого пользователя к вычислительной сети и удаление такого пользователя из вычислительной сети при отсутствии идентификатора. В соответствии со способом база данных может быть сконфигурирована на регистрацию того, что пользователь больше не владеет всеми идентификаторами, а также на сообщение информации об этом при последующем запросе от базы данных запросов доступа или других внешних устройств на основании запроса пользователя на доступ к ним. В одном из вариантов осуществления изобретения база данных может входить в состав абонентской системы, администрирующей абонентов в телефонной компании.

В изобретении также предложена система аутентификации пользователя, который запрашивает доступ к услугам вычислительной сети, путем использования уникальных связующих адресов для аутентификации и идентификации. В этой системе может быть предусмотрено присвоение глобально уникальных связующих адресов пользователям и устройствам.

В систему может дополнительно входить система регистрации и абонентская система, способная поддерживать связь по меньшей мере с одним из следующего: (а) различными базами данных запросов доступа, (б) обработчиком запросов доступа, (в) ключом пользователя, (г) любыми другими электронными запросами, такими как аутентификация покупки, подписи, сверки, другими внешними устройствами и т.д.

Согласно одной из дополнительных особенностей изобретения предложен способ поддержания связи между базовой сетью и рядом внешних устройств, а также базами данных запросов доступа (ADB), защищающими данные, услуги, информацию, системы, прикладные программы и т.д. с ограниченным доступом, включающий сообщение идентификаторов пользователей, которые имеют доступ, и того, какой доступ они имеют, и определение и сообщение базовой сетью по запросу (абонентской системы/системы выставления счетов) того, произвел ли оплату пользователь/разрешен ли пользователю кредит на предполагаемое использование. Способ может дополнительно включать регистрацию трафика в базовой сети и/или ADB, которая информирует базовую сеть.

Согласно одной из дополнительных особенностей изобретения предложена система поддержания связи между базовой сетью и рядом внешних устройств, а также базами данных запросов доступа (ADB), защищающими данные, услуги, информацию, системы, прикладные программы и т.д. с ограниченным доступом, в которую входит средство сообщения идентификаторов пользователей, которые имеют доступ, и того, какой доступ они имеют, и блок определения и сообщения базовой сетью по запросу (абонентской системы/системы выставления счетов) того, произвел ли оплату пользователь/разрешен ли пользователю кредит на предполагаемое использование. В систему может входить блок регистрации трафика в базовой сети и/или ADB, которая информирует базовую сеть.

Согласно еще одной из дополнительных особенностей изобретения предложен способ поддержания связи между базовой сетью и цифровой платформой, которая предоставляет информацию о контенте, формах платежа, условиях использования, цене распределении цен/доходов среди соответствующих объектов и функциях базовой сети (абонирования, выставления счетов, блокировки, других внешних контактов, платежа

другим сторонам).

Согласно еще одной из дополнительных особенностей изобретения предложена система поддержания связи между базовой сетью и цифровой платформой, которая предоставляет информацию о контенте, формах платежа, условиях использования, цене, распределении цен/доходов среди соответствующих объектов и функциях базовой сети (абонирования, выставления счетов, блокировки, других внешних контактов, платежа другим сторонам).

Дополнительные признаки и преимущества настоящего изобретения станут ясны из зависимых пунктов формулы изобретения.

Краткое описание чертежей

Далее приведено краткое описание чертежей для облегчения понимание изобретения. Настоящее изобретение подробно описано далее со ссылкой на чертежи, на которых:

на фиг. 1 показан заголовок пакета IPv6,

на фиг. 2 показана сеть, в которую входят базы данных, содержащие контент, для доступа к которому требуется аутентификация,

на фиг. 3 показана блок-схема процедуры предъявления пароля/регистрации при аутентификации согласно одному из вариантов осуществления настоящего изобретения,

на фиг. 4 показана блок-схема процедуры предъявления пароля/регистрации при аутентификации согласно одной из разновидностей варианта осуществления, проиллюстрированного на фиг. 3,

на фиг. 5 показана блок-схема способа аутентификации,

на фиг. 6 показана блок-схема способа аутентификации, альтернативного способу, проиллюстрированному на фиг. 5,

на фиг. 7 проиллюстрирован пример поддержания связи между базовой сетью и рядом внешних устройств и баз данных запросов доступа, защищающих данные с ограниченным доступом,

на фиг. 8 проиллюстрирован пример сообщения, альтернативный примеру, проиллюстрированному на фиг. 7, и

на фиг. 9 проиллюстрирован пример платформы для взаимодействия между базовой сетью и системами выставления счетов.

Подробное описание изобретения

Далее сначала описаны общие варианты осуществления настоящего изобретения, а затем конкретные примеры осуществления. Там, где возможно, приведены ссылки на прилагаемые чертежи по возможности с использованием ссылочных позиций, указанных на чертежах. Тем не менее, следует отметить, что на чертежах представлены лишь примеры осуществления, и в объем описанного изобретения могут входить другие подробности и варианты осуществления.

Термином "данные с ограниченным доступом" обозначается любой объект, системы, услуги, прикладные программы, программы, видео, аудио и т.п., охраняемое законами об авторском праве и другими законами, данные, охраняемые основанными на частном праве соглашениями, такими как лицензионные соглашения, соглашения о распространении, агентские соглашения и т.п., а также данные, в отношении которых владелец решает применить ограничения доступа независимо от прав и правовой основы. Поскольку изобретение относится к управлению доступом к данным с ограниченным доступом посредством вычислительных сетей, термин "данные с ограниченным доступом" не включает материальные объекты. Тем менее, он включает любую интерпретацию или представление в цифровой форме охраняемого авторским правом материального объекта. Такой материальный объект может представлять собой

без ограничения фотографии, живопись, а также скульптуры и другие трехмерные объекты, интерпретация которых в цифровой форме может использоваться, например, для производства и эксплуатации трехмерного объекта.

Термином "телефонная компания" в контексте изобретения обозначается любой поставщик услуг доступа к сети, имеющий право выступать в качестве посредника трафика данных, которыми обменивается пользователь, и одновременно способный прямо или опосредованно передавать данные с ограниченным доступом одному или нескольким пользователям.

Термином "правообладатель" обозначается одно или несколько лиц, на законном основаниях владеющих правом на данные и услуги с ограниченным доступом.. В случаях, когда телефонная компания предлагает собственные данные и услуги с ограниченным доступом, правообладателем также может являться телефонная компания. Это могут быть, например, компьютерные программные платформы или прикладные программы, при этом термин "компьютеры" следует интерпретировать согласно данному в описании определению.

Термином "поставщик прав" обозначается одно или несколько лиц, которые могут на законных основаниях действовать в качестве посредника данных с ограниченным доступом. Поставщиком прав может являться телефонная компания.

Термином "компьютер" обозначается любое устройство, которое способно подсоединяться к вычислительной сети и одновременно может быть идентифицировано уникальным идентификатором. Уникальным идентификатором устройства может служить аппаратный идентификатор, такой как, например, MAC-адрес, IMSI или IMEI. В одном из вариантов осуществления изобретения компьютер непосредственно привязан к идентификатору пользователя, который является уникальным и присвоен телефонной компанией или органом сертификации.

Термином "базовая сеть 1" обозначается сеть телефонной компании или поставщика услуг, которая служит носителем трафика данных для пользователей вне зоны обслуживания самого оператора; в некоторых случаях она также называется магистральной сетью.

Термином "IP" обозначается Интернет-протокол, которым является межсетевой протокол на сетевом уровне. Существует несколько межсетевых протоколов на сетевом уровне, наиболее распространенным из которых является IPv4. Протокол IPv4 используется в течение долгого времени, и одним из основных его недостатков является ограниченное число доступных адресов. С резким ростом числа устройств, которым требуются отдельные IP-адреса, в протоколе IPv4 исчерпываются адреса в некоторых диапазонах. Другим недостатком, который также может объясняться тем фактом, что протокол IPv4 вскоре станет устаревшим, является то, что этот протокол не рассчитан на рост потребности в аутентификации, целостности и защите данных, который вызван в основном огромным числом транзакций, доступных в настоящее время в сети, включая как денежные операции, так и не в последнюю очередь транзакции в отношении объектов с охраняемыми правами, таких как игры, музыка, фильмы и книги. С целью преодоления недостатков протокола IPv4 уже в 1994 г. было предложено перейти на протокол с более широким диапазоном адресов и большей гибкостью в целом, и этот протокол был назван IPv6. Протокол IPv6 имеет 128 битов адресного пространства, тогда как протокол IPv4 только 32 бита.

Во многих контекстах адреса IPv6 поделены на две части: 64-битный сетевой префикс и 64-битную часть, определяющую адрес хоста. Последняя часть, являющаяся идентификатором интерфейса, часто автоматически генерируется на основании MAC-

адреса сетевого адаптера. MAC-адрес содержит 48 битов, а преобразование из 48 битов в 64 бита для использования в качестве идентификатора интерфейса описано в разделе 2.5.1 RFC 4291. Адреса IPv6 обычно являются шестнадцатеричными и состоят из восьми групп по четыре шестнадцатеричных цифры, разделенных двоеточием.

Пакет IPv6 состоит из двух частей: заголовка, проиллюстрированного на фиг. 1, и полезной нагрузки. Заголовок содержит 40 первых символов пакета и имеет различные поля. В контексте настоящего изобретения интерес в заголовке в основном представляет поле адреса источника, в котором содержатся адреса источников.

Поскольку, как и протокол IPv4, протокол IPv6 поддерживает глобально уникальные IP-адреса, могут отслеживаться (по меньшей мере, теоретически) действия любого устройства в сети.

Назначением протокола IPv6 является присвоение уникальных адресов каждому устройству, существующему в сети. Следовательно, каждое устройство в сети Интернет будет иметь глобально уникальный адрес, непосредственно адресуемый с любого другого адреса в сети Интернет. Из-за необходимости экономии адресов протокола IPv4 был внедрен протокол трансляции сетевых адресов (NAT) для маскировки устройств, имеющих IP-адреса, находящиеся за сетевым интерфейсом, чтобы такие устройства непосредственно не распознавались извне сетевого интерфейса. В протоколе IPv6 не требуется использовать NAT или самоконфигурирование адресов, хотя возможно самоконфигурирование на основании MAC-адреса. Даже когда адрес не. основан на MAC-адресе, адрес интерфейса будет являться глобально уникальным в отличие от сетей с использованием замаскированного NAT протокола IPv4. Несмотря на возможную критику протокола IPv6 из-за компрометации "секретности", его характеристики, включающие большое адресное пространство и уникальную отслеживаемость, делают его интересным кандидатом для аутентификации.

Задачей настоящего изобретения является создание систем и способов аутентификации, в которых определенный фактор основан на связующем адресе (таком как IPv6). Как указано выше, в качестве одного из факторов, который генерирует код аутентификации, обычно используется MAC-адрес, IMSI или IMEI. Однако, как также указано выше, этому подходу присущи несколько недостатков. Например, аппаратное устройство (фактор владения) может использоваться несколькими пользователями. Если пользователю присвоен глобально уникальный адрес, который является неизменным аналогично номеру карточки социального страхования/телефонному номеру, такой адрес может использоваться в качестве фактора в алгоритме однофакторной, двухфакторной или трехфакторной аутентификации. Таким уникальным адресом может являться адрес IPv6.

Адреса IPv6 могут присваиваться поставщиками интернет-услуг, операторами или сертифицированными органами, уполномоченными выдавать сертификаты, как в существующих системах, в которых отдельные агенты, такие как Symantec, в числе прочих могут подтверждать подлинность и выдавать PKI в качестве центра сертификации (CA). Предполагается, что присвоение адреса IPv6 осуществляется безопасным образом.

Согласно одной из особенностей изобретения после получения персонального и глобально уникального адреса IPv6 пользователь имеет возможность пройти аутентификацию с использованием этого уникального адреса IPv6 в системе однофакторной аутентификации.

Согласно другой особенности изобретения уникальный адрес IPv6 может являться одним из факторов двухфакторной аутентификации, при этом другим фактором может являться MAC-адрес, IMSI или IMEI. Согласно одной из особенностей изобретения

аппаратный код и адрес IPv6 могут вводиться в алгоритм, который генерирует уникальный код аутентификации.

Аналогичным образом, согласно третьей особенности изобретения могут использоваться три фактора.

Если пользователь должен осуществить транзакцию или совершить другие действия, для которых требуется удостоверить личность пользователя, необходима аутентификация.

Предупреждение и автоматическая блокировка ID+IP=проверенного/разрешенного/идентифицированного IP, заданного посредством функции регистрации, в случае утери идентификатора/"разрушения" ключа. Отмена/блокировка доступа к сети и/или защищенному ресурсу (при отсутствии постоянной идентификации происходит отсоединение).

В одном из вариантов осуществления (фиг. 4) в изобретении предусмотрена функция предъявления пароля/регистрации для доступа к сети Интернет/другой сети.

Функция предъявления пароля при использовании двухфакторной аутентификации поддерживает связь с базой данных (DB1), в которой ведется учет связующих адресов и идентификаторов за различными связующими адресами, а также того, как могут быть аутентифицированы идентификаторы. Может использоваться электронное устройство, содержащее приемопередатчик со связным интерфейсом, позволяющим ему иметь связующий адрес, с помощью которого оно может поддерживать связь по сети (IMEI, IMSI, MAC).

Связующий адрес может быть указан в различных базах данных запросов доступа (DBx), подсоединенных к вычислительной сети и защищающих URL, ссылку или конкретный объем данных, услугу или другой объект с ограниченным доступом. Решение о доступе к DBx принимается в зависимости от того, содержится ли связующий адрес в базе данных запросов доступа, и при поступлении в DB1 запроса о том, установлено ли, что адрес разрешен/авторизован правильным пользователем, и, если это так, предоставляется доступ к DBx. В противном случае передается сообщение об ошибке, и доступ отклоняется. Если пользователь выходит из системы, или "ключ" нарушен, об этом может сообщаться DB1, которая передает соответствующим базам данных запросов доступа (DBx) и другим внешним устройствам сообщение о том, что пользователь больше не должен иметь доступа, и передается сообщение об ошибке. В этом случае может проводиться различие между намеренным выходом из системы и срывом вследствие нарушения ключа, за счет чего может уменьшаться величина трафика данных, поскольку о намеренном выходе из системы необязательно сообщать DB1, так как впоследствии снова войти в систему в любом в случае может только правильный пользователь. В случае нарушения ключа DB1 всегда передается сообщение об этом. DB1 регистрирует его и может передать DBx и другим внешним устройствам сообщение о том, что пользователь не идентифицирован. В этом случае будут отклоняться любые последующие попытки доступа со стороны пользователя/связующего адреса, и ADB передается сообщение об ошибке (фиг. 4).

Об ограничении доступа может сообщаться непосредственно обработчику запросов доступа, который предоставляет пользователю доступ и одновременно разблокирует/аутентифицирует пользователя в DB1. Разблокировка происходит при предоставлении правильного идентификатора и правильного IP вместе с MAC, IMEI и т.п. На стороне пользователя создается ключ. Этот ключ уведомляет DB1 о том, нарушен ли он путем изменения/сокрытия/придания анонимности IP или в результате выхода пользователя из системы. DB1 уведомляет обработчика запросов доступа, который доставляет

сообщение об ошибке пользователю.

Пример реализации первой особенности изобретения

Далее описан пример использования аутентификации в процессе связи между базовой сетью и рядом внешних устройств и баз данных с ограниченным доступом. Процесс аутентификации включает пять стадий.

1. Абонент телефонной компании имеет уникальный связующий адрес и использует функцию регистрации, чтобы ввести связующий адрес, и средство аутентификации, которое доказывает, что он в действительности является надлежащим пользователем связующего адреса. Также предусмотрен код, которым снабжаются вычислительные устройства (компьютер, планшет и мобильный телефон) пользователя. После того, как все подтверждено, в абонентской системе оператора регистрируется, что пользователь идентифицирован, и ему присваивается ключ.

Пользователь пытается получить доступ к базе данных, в которой содержится услуга или контент. Если брандмауэр не распознает связующий адрес, доступ не разрешается. Если брандмауэр распознает связующий адрес, доступ разрешается.

2. Если абонентская система (DB1) зарегистрировала выход из системы/нарушение ключа, она может уведомить ADB и внешние устройства.

3. Если пользователь, который зарегистрировался и был идентифицирован, выходит из системы или изменяет IP посредством сервера-посредника, скрывает IP посредством другого программного обеспечения, использует множество IP и т.п., от ключа абонентской функции поступает сообщение, в котором зарегистрировано нарушение ключа.

4. Если пользователь, действует таким образом, что это приводит к нарушению ключа или выходу из системы, эта информация может сообщаться базам данных запросов доступа. Затем пользователю больше не будет разрешен доступ к соответствующим базам данных.

5. Информация о выходе из системы/нарушении ключа может сообщаться непосредственно функции доступа, связанной с базовой сетью, в результате чего может прекращаться доступ соответствующего пользователя.

6. Сервер/база данных, отвечающая за обработку покупки, функция подписи, финансовая функция и т.п.могут принимать сообщение о том, что пользователь не идентифицирован.

Пример реализации второй особенности

Изобретение также относится к платформе для установления и обеспечения прав и цен, а также для сообщения о них необходимым частям базовой сети, которая описана в этом примере со ссылкой фиг. 5.

Поддержание связи между базой данных запросов доступа/брандмауэром (ADB), защищающим контент/услугу/данные и подсоединенным к вычислительной сети, и базовой сетью (CN), в которую входит клиентская и абонентская система (CSS) и система выставления счетов (BS)

Базовая сеть предоставляет информацию о том, каким клиентам следует разрешить доступ и какой доступ следует разрешить. Когда уникальный пользователь запрашивает соответствующий доступ, запрашивается ADB, чтобы определить, следует ли предоставить доступ (предполагается, что указанное использование оплачено клиентом/клиенту разрешен кредит). ADB также запрашивает базовую сеть, чтобы проверить, произведена ли оплата клиентом или ему разрешен кредит. Если доступ предоставлен, такой доступ может осуществляться в согласованных пределах использования. ADB регистрирует трафик и может отчитываться перед базовой сетью.

1. CCS регистрирует в каталоге для каждого пользователя, кем являются клиенты и что они выбирают для получения доступа. Клиентам предоставляется доступ к соответствующим ADB, если указан их уникальный идентификатор в каталоге.

2. BS выставляет счета клиентам в соответствии с тем, какая сумма причитается за указанный доступ. BS принимает информацию о ценах, а также о предполагаемом и/или зарегистрированном трафике. CN поддерживает связь с рядом ADB и внешних устройств.

3. Внутри базовой сети поддерживают связь и согласованно действуют система выставления счетов и клиентская система. Информация о зарегистрированном трафике клиента может извлекаться из различных ADB.

4. При попытке доступа ADB определяет, следует ли разрешить доступ клиенту и, возможно, какой доступ (функция отображения); проверяет в базовой сети, BS, CCS, была ли произведена оплата.

5. Доступ предоставляется, если клиент и соответствующий доступ указаны в ADB, если только в ADB не зарегистрирована поступившая от CN информация о том, что пользователь не произвел оплату или ему не разрешен кредит.

6. ADB регистрирует трафик и затем может отчитываться перед CN. CN может регистрировать использование.

Клиент указывает CN выбранный контент и услуги, а также объем их использования, CN предоставляет эту информацию BS/CN вносит пользователя в различные ADB вместе с объемом использования (функция отображения)/CN передает уведомление, и клиент блокируется в ADB, если он не произвел оплату или ему не разрешен кредит (покупка за наличные, например, может быть все же авторизована (разблокирована/заблокирована в ADB при различных действиях)) или, в качестве альтернативы, ADB запрашивает CN, произвел ли оплату клиент или разрешен ли ему кредит, например, на отдельные покупки вне функции отображения (разблокированной/заблокированной в ADB при различных действиях).

Запрос доступа со стороны пользователя

Существует ли пользователь в ADB? (Входит ли услуга в число услуг, абонированных пользователем? Это также может быть проверено в CCS.)

Тип использования? Например, остаются ли еще данные для загрузки? (функция отображения и регистрации). Если только ADB не была уведомлена CN, предполагается, что клиент произвел оплату или ему разрешен кредит (или он может произвести оплату наличными) (разблокировано/заблокировано в CN)

Получена ли оплата? Разрешен ли кредит? Или произведена ли оплата наличными? (разблокировано/заблокировано в CN)

Отчет перед CN в случае дальнейших действий, за которые должен быть выставлен счет.

ADB регистрирует и предоставляет информацию CN.

Базовая сеть с использованием информации о пользователе и согласованном использовании (абонировании, заданной функции отображения) создает профиль пользователя на основании такой информации в ADB и поддерживает связь с ADB по поводу различных услуг, чтобы в любой заданный момент принять решение о доступе и выставить правильный счет на основании фактического использования (регистрации с задержкой, если был разрешен кредит)

Выбор доступа клиентами

Идентификаторы клиентов регистрируются в соответствующих местоположениях доступа (ADB). Клиенту выставляется соответствующий счет. При запросе доступа

проверяется, зарегистрирован ли клиент, и была ли произведена оплата/разрешен кредит. В случае предоставления доступа согласно требованиям регистрируется его использование клиентом. Эта информация может пересылаться CN.

В изобретении согласно этому примеру решены следующие задачи:

передачи различным ADB сообщений о том, кто к чему имеет доступ;

обеспечения простого решения оплаты, которое не зависит от платформы и может использоваться в сети;

предотвращения избыточной передачи сигналов вследствие осуществляемой в реальном времени проверки того, произвел ли клиент оплату. Может считаться, что пользователь произвел оплату, если от CN не получено уведомление об обратном;

обнаружения по запросу пользователя того, произведена ли оплата индивидуальными пользователями/будет ли разрешен кредит/должна ли быть произведена оплата наличными и за какое использование;

сообщения о регистрации пользователей в базовой сети или ADB (ADB способна легче интерпретировать использование) объекту, который выставляет счет уникальному клиенту/пользователю.

Пример практической реализации одной из особенностей второго примера осуществления изобретения

Уникальный пользователь посредством абонентской системы выбирает доступ к различным услугам предоставления данных и контента.

Базовая сеть, в которую входит абонентская система, уведомляет различные ADB и внешние устройства о том, что пользователю разрешен доступ и том, какие виды доступа должны быть отображены для клиента.

Затем пользователь пытается получить доступ к услугам предоставления контента, которые он запросил. Они находятся за брандмауэром ADB.

Если запрошенный объект находится в предполагаемом использовании, доступ предоставляется, в противном случае доступ не предоставляется. Это также может быть связано с правом на покупку за наличные или разрешением на кредит. ADB может запросить базовую сеть (систему выставления счетов) о том, произвел ли клиент оплату/ разрешен ли клиенту кредит, и доступ предоставляется в соответствии с предполагаемым использованием. Использование регистрируется в ADB, и о нем может поддерживать связь базовой сети. Базовая сеть также может регистрировать использование.

В изобретении согласно второй особенности предусмотрено:

поддержание связи между базовой сетью и рядом внешних устройств и баз данных запросов доступа, защищающих данные, услуги, информацию, системы, прикладные программы и т.д. с ограниченным доступом. Также может быть защищена функция заказа на покупку за наличные;

принятие решения о том, какой доступ следует разрешить, и произвел ли пользователь оплату/будет ли ему разрешен кредит на предполагаемое использование. CN (абонентская функция, функция выставления счетов) уведомляет ADB/внешние устройства, если пользователь не произвел пользователь оплату и ему не будет разрешен кредит. Это может регистрироваться в ADB с целью предотвращения последующих запросов доступа от соответствующего пользователя;

регистрация трафика в базовой сети и/или ADB, которая сообщает об этом базовой сети.

Пример реализации третьей особенности изобретения

Далее со ссылкой на фиг. 6 описан пример осуществления третьей особенности изобретения.

Изобретение относится к платформе для установления и обеспечения прав и критериев доступа, таких как, например, цены, а также для сообщения о них необходимым частям базовой сети, включая комментарии к выставлению счетов (Какова цена; что охраняется правами и блокируется; каково процентное распределение доходов), абонирование, блокировку, регистрацию, внешние контакты.

Электронная платформа площадка с функцией регистрации

Платформа позволяет определять условия, касающиеся прав на цифровой контент/услуги и данные, доступ к которым ограничен правообладателем. Такими условиями могут являться, например, цена, страна и географическое положение, оператор, конкретное распределение платежей пользователей и т.д. Они могут приниматься другой стороной, при этом установленная цена, а также распределение доходов от контента/услуг определяют, как CN следует выставлять счета клиентам, блокировать доступ пользователей к запрещенным аналогичным данным и распределять доходы. Платформа/база данных поддерживает связь с базовой сетью и может предоставлять информацию, необходимую для CN. В системе выставления счетов и клиентской системе определены цены на услуги/контент, правила оплаты и применимый принцип распределения, а также функциональные возможности блокировки запрещенных объектов. Оплата распределяется согласно процентному распределению, указанному для соответствующих услуг/контента.

Регистрация, условия, подтверждение со стороны контрагента, установленная цена, процентное распределение цены/доходов, функции блокировки запрещенных данных

Информация передается абонентской функции, системе выставления счетов, функции блокировки и функции управления денежными потоками.

В изобретении предложена платформа для инициирования, администрирования и реализации соглашений по цифровым авторским правам, которая сообщает базовой сети информацию, необходимую для обеспечения требуемых функциональных возможностей. Это не известно из уровня техники.

Практический пример реализации третьей особенности изобретения

Цифровая платформа

Сторона соглашения регистрируется и принимает условия. При поступлении подтверждения от "контрагента" базовой сети передается информация о том, какой контент/услуги могут быть выбраны пользователем, о применимой стране или регионе, о цене и тем самым о счете, выставляемом пользователю, о том, как распределяется оплата, о сходном запрещенном контенте, который следует заблокировать.

Оператор и правообладатель заключают соглашение, которое дублируется в платформе. Правообладатель на основании регистрируемого им трафика клиентов оператора взимает соответствующую плату с оператора в соответствии с соглашением. Затем оператор удостоверяется в том, что он получил оплату от конечного потребителя, чтобы обеспечить причитающуюся с него оплату правообладателю.

Следовательно, в изобретение согласно третьей особенности обеспечено поддержание связи между базовой сетью и цифровой платформой с целью предоставления информации о контенте, цене, распределении цены среди соответствующих лиц и функциях базовой сети (абонировании, выставлении счетов, блокировке, оплате)

На фиг. 6 показана платформа, содержащая соглашения с различными условиями распределения и использования конечным потребителем, например, что касается цены для конечного потребителя и распределения доходов между правообладателем и дистрибьютором, взаимодействия платформы с базовой сетью и взаимодействий между базовой сетью и системами выставления счетов, платежными системами и разрешенными

версиями. Предотвращается доступ к запрещенным копиям защищенных данных.

Список определений

1	Базовая сеть, управляемая одной или несколькими телефонными компаниями
2, ADB, DBx	База данных, содержащая данные, доступ к которым решил ограничить правообладатель, и имеющая интерфейсы для поддержания связи с несколькими внешними устройствами
3, DB1	База данных, содержащая информацию о правах доступа для индивидуальных пользователей и имеющая интерфейс для поддержания связи с внешними устройствами
4	База данных/сервер, содержащий данные сообщений об ошибках в ответ на запросы от пользователей с уникальными идентификаторами, отклоненных базой (3) данных
5	Обработчик запросов доступа, снабженный связным интерфейсом для приема данных от базовой сети (1), а также связным интерфейсом для поддержания связи с базой (3) данных
6	Один или несколько поставщиков данных, по меньшей мере некоторые из которых защищены авторским правом
7	База данных, содержащая защищенные авторским правом объекты, хранящиеся без разрешения правообладателя(-ей)
8	База данных, содержащая защищенные авторским правом объекты, хранящиеся без разрешения правообладателя(-ей)
9	"Символический" барьер для оператора, который позволяет ему предотвращать доступ к определенным базам данных/адресам (7, 8) в ответ на запрос доступа к защищенные авторским правом объектам, которые хранятся вопреки желанию правообладателя (-ей)
10-14	Примеры компьютеров, которым присвоен постоянный уникальный идентификатор
A-E	Каналы связи, установленные компьютерами (10-14)
DBx	База(-ы) данных запросов доступа

ADB	База(-ы) данных запросов доступа
IMEI	Международный идентификационный номер оборудования подвижной станции – аппаратный номер для идентификации мобильных телефонов стандарта 3GPP или iDEN, таких как телефоны GSM (глобальной системы связи с подвижными объектами), UMTS (универсальной системы подвижной электросвязи), LTE (системы с перспективой развития) и некоторых спутниковых телефонов
IMSI	Международный идентификационный номер оборудования подвижного абонента, используемый для идентификации сети сотовой связи; в сети GSM, UMTS и LTE код присваивается SIM-карте, а в сетях CDMA-2000 код присваивается непосредственно телефоном или в R-UIM-карте (аналоге SIM-карты)
MAC-адрес	Аппаратный адрес
LAN	Локальная сеть для сетевых соединений между устройствами, сконфигурированными на беспроводные или проводные сетевые соединения. Примерами таких устройств могут являться компьютеры, принтеры, мобильные телефоны, PDA и т.д.
LAN MAC	Протокол управления доступом к среде локальной сети, MAC является уникальным аппаратным адресом, присвоенным всем устройствам, сконфигурированным на беспроводные или проводные сетевые соединения
PDA	Персональный цифровой ассистент
IP	Межсетевой протокол, наиболее важный протокол, лежащий в основе сети Интернет
IPv4	Протокол IP версии 4 является фундаментальным протоколом, лежащим в основе сети Интернет. Адресное пространство содержит 32 бита.
IPv6	Протокол IP версии 6 является протоколом сети Интернет. Адресное пространство содержит 128 битов, что в принципе обеспечивает 2^{128} возможных комбинаций адресов. Стандарт

	IPv6 предусматривает самоконфигурирование, что означает, что устройство может присваивать себе собственный уникальный адрес, основанный на MAC-адресе устройства в LAN.
MPLS	Многопротокольная коммутация по меткам является протоколом, посредством которого IP-сети могут принимать решения о пересылке на основании адресов (меток), что позволяет пересылать пакеты от одного сетевого узла следующему сетевому узлу на основании коротких адресов (меток) вместо длинных сетевых адресов, в результате чего может предотвращаться сложный поиск в таблицах маршрутизации.
HTTP	Протокол передачи гипертекстовых файлов
HTTPS	Безопасная версия HTTP, приспособленная для аутентификации и зашифрованной передачи фактически посредством SSL или TLS
FTP	Протокол пересылки файлов является независимым от операционной системы протоколом пересылки файлов в сети на основе TCP/IP. Действует только в среде TCP.
TCP	Протокол управления передачей является сетевым протоколом надежной передачи информации на основе соединений и действует на транспортном уровне модели организации компьютерных сетей по протоколу взаимодействия открытых систем (OSI)
UDP	Протокол передачи дейтаграмм пользователя является ориентированным на обмен сообщениями сетевым протоколом передачи информации без установления соединения и действует на транспортном уровне модели организации компьютерных сетей по протоколу взаимодействия открытых систем (OSI). Он не гарантирует доставку, требует меньших накладных расходов, чем TCP и применим, например, для передачи данных в реальном времени, когда лучше отбрасывать сообщения, чем задерживать их передачу.
SSL	Протокол безопасных соединений

TLS	Протокол безопасности транспортного уровня,
SSH	Безопасная оболочка является компьютерной программой и сетевым протоколом прикладного уровня, то есть верхнего уровня модели взаимодействия открытых систем (OSI). Весь трафик между клиентом SSH и сервером шифруется.
URL	Унифицированный указатель информационного ресурса

(57) Формула изобретения

1. Способ аутентификации пользователей и/или устройств, баз данных, серверов или другого оборудования, сконфигурированного на поддержание связи по сети, запрашивающих доступ к данным или услугам с ограниченным доступом из базы данных доступа в вычислительной сети, причем вычислительная сеть включает по меньшей мере одну базовую сеть, связанную с поставщиком услуг доступа, и множество баз данных доступа, подсоединенных к указанной по меньшей мере одной базовой сети, включающий стадии:

присвоение глобально уникальных связующих адресов всем устройствам в указанной вычислительной сети, причем каждое из устройств уникально привязано к конкретному пользователю,

использование по меньшей мере присвоенного уникального связующего адреса, привязанного к пользователю устройства для идентификации пользователя;

использование функции регистрации посредством указанного устройства указанного пользователя для аутентификации указанного идентифицированного пользователя в первой базе данных доступа (DB1) в вычислительной сети и генерирование уникального ключа пользователя для доступа к вычислительной сети с использованием указанного присвоенного уникального связующего адреса;

предоставление доступа к данным или услугам с ограниченным доступом на запрос пользователя во второй базе данных доступа (DBx) в вычислительной сети, если присвоенный уникальный связующий адрес или ключ пользователя распознается второй базой данных доступа (DBx) и указанный пользователь аутентифицирован в первой базе данных доступа (DB1); и

отклонение доступа пользователя к множеству баз данных доступа и/или к указанной вычислительной сети, если уникальный ключ нарушен или при выходе пользователя из системы для указанного ключа на указанном устройстве.

2. Способ по п. 1, в котором указанным устройствам присвоен уникальный связующий адрес при помощи аппаратного идентификатора, который позволяет устройству отправлять и получать информацию по сети, причем аппаратным идентификатором может являться одно из следующего: MAC-адрес, IMEI или IMSI.

3. Способ по п.1 или 2, включающий дополнительную идентификацию пользователя при помощи идентификатора, включающего по меньшей мере одно из следующего: MAC-адрес, IMEI, IMSI, код, банковский идентификатор.

4. Способ по п. 3, в котором при отсутствии одного из идентификаторов, идентифицирующих пользователя, или при выходе пользователя из системы под ключом на указанном устройстве способ дополнительно включает:

передачу от пользователя сообщения первой базе данных доступа (DB1),

сконфигурированной на предоставление доступа на запрос пользователя к вычислительной сети или удаление пользователя из вычислительной сети при отсутствии идентификатора.

5. Способ по п. 4, в котором первая база данных доступа (DB1) сконфигурирована на регистрацию того, что пользователь больше не владеет всеми идентификаторами, и на сообщение информации об этом автоматически для доступа к базам данных (DBx) или при последующих запросах от других баз данных доступа или других внешних устройств в сети на основании запроса доступа к ним со стороны пользователя.

6. Способ по любому из пп. 1-2, 4-5, в котором первая база данных доступа DB1 входит в состав абонентской системы, администрирующей абонентов телефонной компании.

7. Способ по п. 6, дополнительно включающий передачу из базовой сети и первой базы данных доступа (DB1) в базы данных доступа (DBx) идентификации пользователей, имеющих доступ к вычислительной сети и/или к базам данных доступа (DBx), и того, какой доступ они имеют, и определение и сообщение базовой сетью, произвел ли оплату пользователь/разрешен ли пользователю кредит на использование.

8. Способ по п. 7, включающий регистрацию трафика в базовой сети и/или базах данных доступа (DBx), которые информируют базовую сеть.

9. Способ по любому из пп. 1-2, 4-5, 7-8, в которой базовая сеть дополнительно поддерживает связь с цифровой платформой, которая предоставляет информацию о контенте, формах платежа, условиях использования, цене, распределении цены среди соответствующих объектов и функциях базовой сети.

10. Система для аутентификации пользователей и/или устройств, баз данных, серверов, или другого оборудования, сконфигурированного на поддержание связи по сети, запрашивающих доступ к данным или услугам с ограниченным доступом из базы данных доступа в вычислительной сети, причем вычислительная сеть включает по меньшей мере одну базовую сеть, связанную с поставщиком услуг доступа, и множество баз данных доступа, подсоединенных к указанной по меньшей мере одной базовой сети, включающая:

средство для присвоения глобально уникальных связующих адресов всем устройствам в указанной вычислительной сети, причем каждое из устройств уникально привязано к конкретному пользователю,

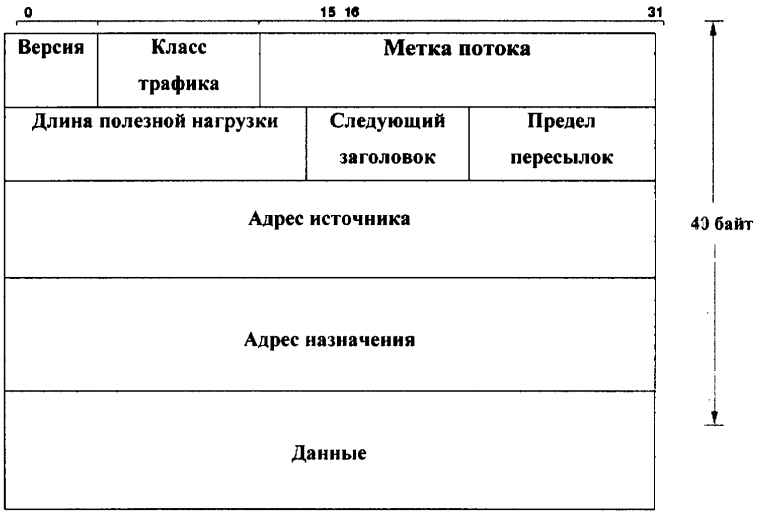
средство для использования по меньшей мере присвоенного уникального связующего адреса, привязанного к пользователю устройства для идентификации пользователя;

средство для использования функции регистрации посредством указанного устройства указанного пользователя для аутентификации указанного идентифицированного пользователя в первой базе данных доступа (DB1) в вычислительной сети и генерирования уникального ключа пользователя для доступа к вычислительной сети с использованием указанного присвоенного уникального связующего адреса;

средство для предоставления доступа к данным или услугам с ограниченным доступом на запрос пользователя во второй базе данных доступа (DBx) в вычислительной сети, если присвоенный уникальный связующий адрес или ключ пользователя распознается второй базой данных доступа (DBx) и указанный пользователь аутентифицирован в первой базе данных доступа (DB1), и

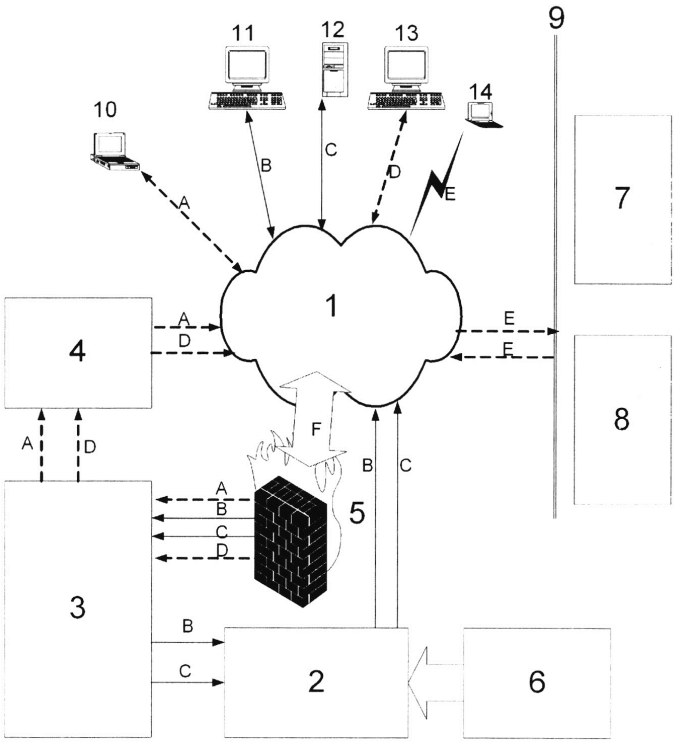
средство для отклонения доступа пользователя к множеству баз данных доступа и/или к указанной вычислительной сети, если уникальный ключ нарушен или при выходе пользователя из системы для указанного ключа на указанном устройстве.

1


0
15 16
31
Версия
Класс трафика
Метка потока
Длина полезной нагрузки
Следующий заголовок
Предел пересылок
Адрес источника
Адрес назначения
Данные
40 байт

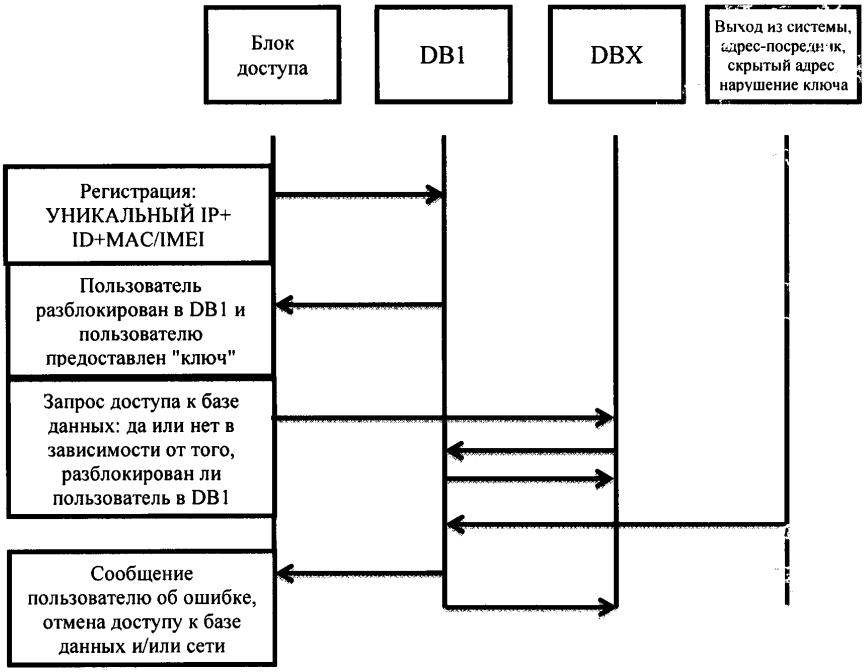
ФИГ. 1

2



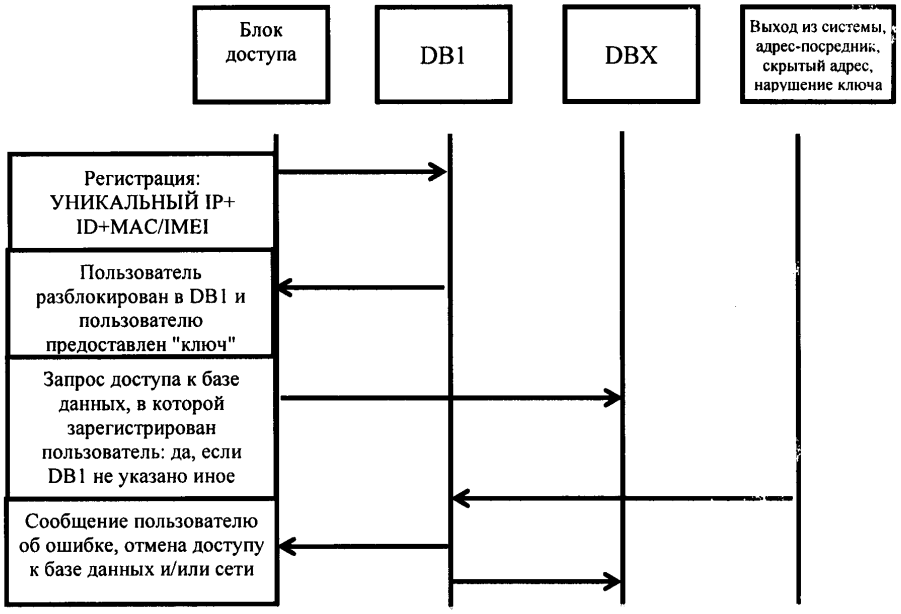
ФИГ. 2

3

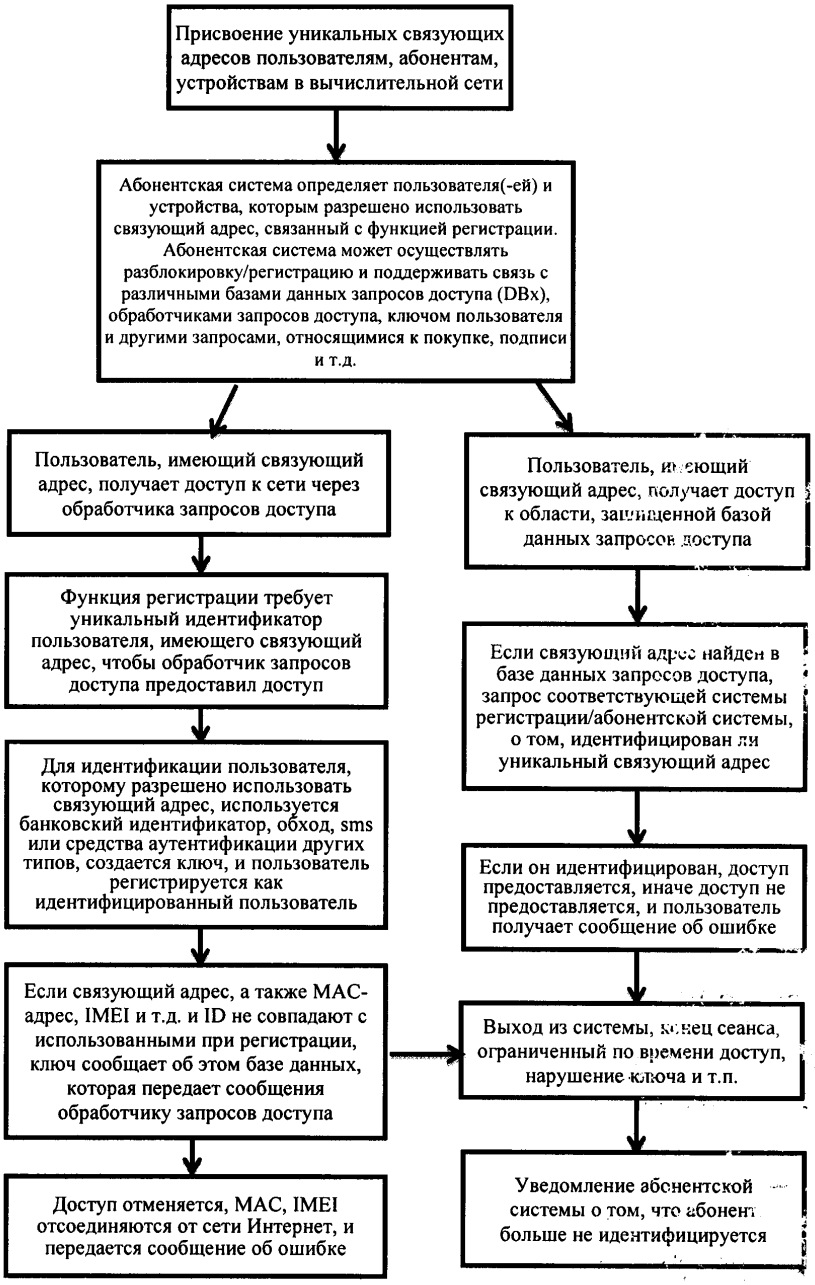

Блок доступа
DB1
DBX
Выход из системы, адрес-посредник, скрытый адрес нарушение ключа
Регистрация: УНИКАЛЬНЫЙ IP+ ID+MAC/IMEI
Пользователь разблокирован в DB1 и пользователю предоставлен "ключ"
Запрос доступа к базе данных: да или нет в зависимости от того, разблокирован ли пользователь в DB1
Сообщение пользователю об ошибке, отмена доступу к базе данных и/или сети

ФИГ. 3

4

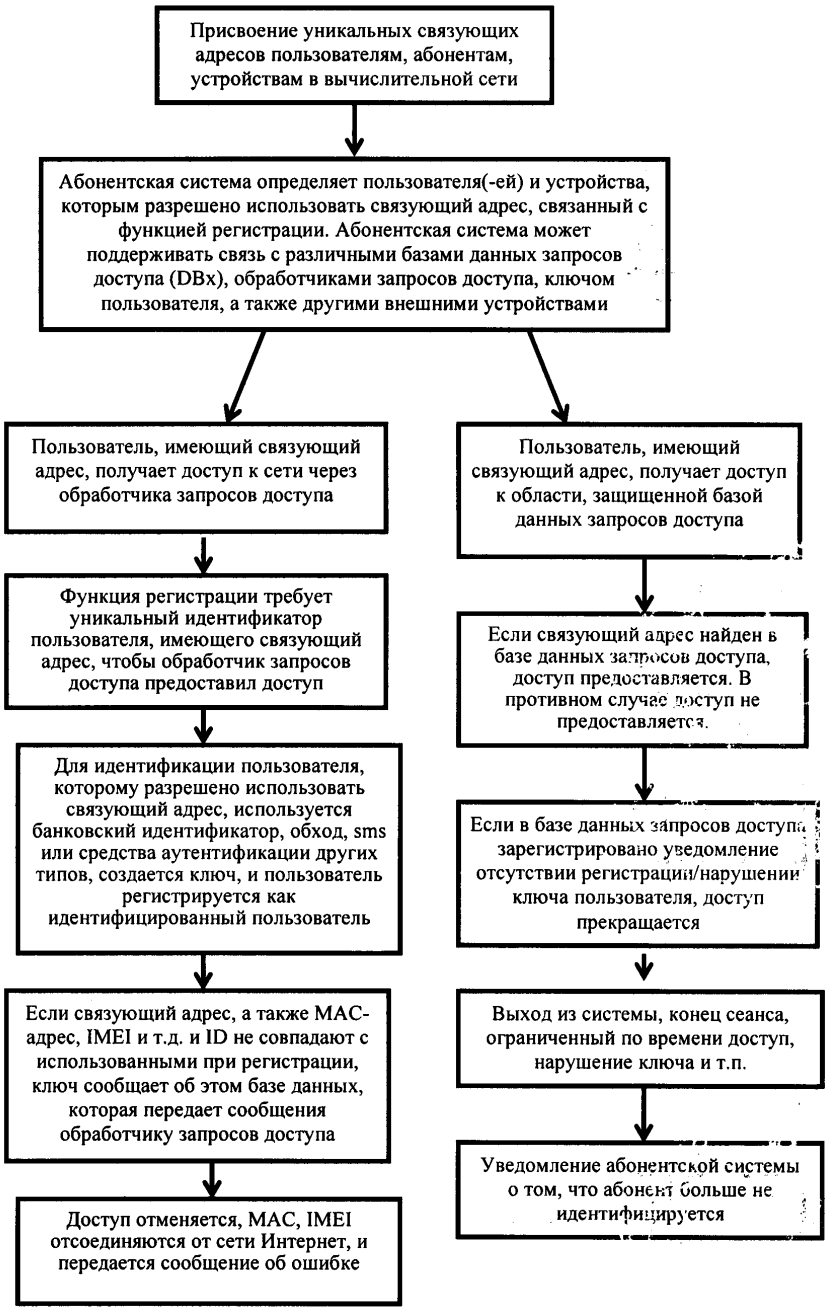

Блок доступа
DB1
DBX
Выход из системы, адрес-посредник, скрытый адрес, нарушение ключа
Регистрация: УНИКАЛЬНЫЙ IP+ ID+MAC/IMEI
Пользователь разблокирован в DB1 и пользователю предоставлен "ключ"
Запрос доступа к базе данных, в которой зарегистрирован пользователь: да, если DB1 не указано иное
Сообщение пользователю об ошибке, отмена доступу к базе данных и/или сети

ФИГ. 4


Присвоение уникальных связующих адресов пользователям, абонентам, устройствам в вычислительной сети
Абонентская система определяет пользователя(-ей) и устройства, которым разрешено использовать связующий адрес, связанный с функцией регистрации. Абонентская система может осуществлять разблокировку/регистрацию и поддерживать связь с различными базами данных запросов доступа (DBx), обработчиками запросов доступа, ключом пользователя и другими запросами, относящимися к покупке, подписи и т.д.
Пользователь, имеющий связующий адрес, получает доступ к сети через обработчика запросов доступа
Функция регистрации требует уникальный идентификатор пользователя, имеющего связующий адрес, чтобы обработчик запросов доступа предоставил доступ
Для идентификации пользователя, которому разрешено использовать связующий адрес, используется банковский идентификатор, обход, sms или средства аутентификации других типов, создается ключ, и пользователь регистрируется как идентифицированный пользователь
Если связующий адрес, а также MAC-адрес, IMEI и т.д. и ID не совпадают с использованными при регистрации, ключ сообщает об этом базе данных, которая передает сообщения обработчику запросов доступа
Доступ отменяется, MAC, IMEI отсоединяются от сети Интернет, и передается сообщение об ошибке
Пользователь, имеющий связующий адрес, получает доступ к области, защищенной базой данных запросов доступа
Если связующий адрес найден в базе данных запросов доступа, запрос соответствующей системы регистрации/абонентской системы, о том, идентифицирован ли уникальный связующий адрес
Если он идентифицирован, доступ предоставляется, иначе доступ не предоставляется, и пользователь получает сообщение об ошибке
Выход из системы, конец сеанса, ограниченный по времени доступ, нарушение ключа и т.п.
Уведомление абонентской системы о том, что абонент больше не идентифицируется

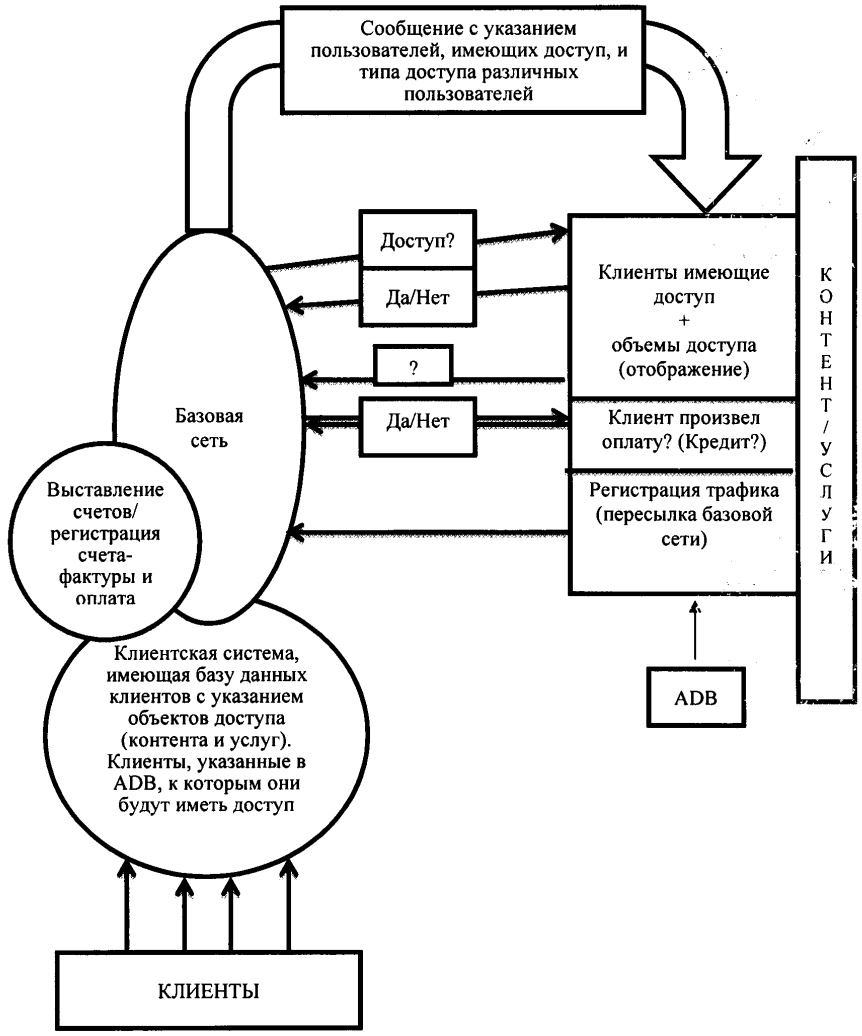
ФИГ. 5

6


Присвоение уникальных связующих адресов пользователям, абонентам, устройствам в вычислительной сети
Абонентская система определяет пользователя(-ей) и устройства, которым разрешено использовать связующий адрес, связанный с функцией регистрации. Абонентская система может поддерживать связь с различными базами данных запросов доступа (DBx), обработчиками запросов доступа, ключом пользователя, а также другими внешними устройствами
Пользователь, имеющий связующий адрес, получает доступ к сети через обработчика запросов доступа
Функция регистрации требует уникальный идентификатор пользователя, имеющего связующий адрес, чтобы обработчик запросов доступа предоставил доступ
Для идентификации пользователя, которому разрешено использовать связующий адрес, используется банковский идентификатор, обход, sms или средства аутентификации других типов, создается ключ, и пользователь регистрируется как идентифицированный пользователь
Если связующий адрес, а также MAC-адрес, IMEI и т.д. и ID не совпадают с использованными при регистрации, ключ сообщает об этом базе данных, которая передает сообщения обработчику запросов доступа
Доступ отменяется, MAC, IMEI отсоединяются от сети Интернет, и передается сообщение об ошибке
Пользователь, имеющий связующий адрес, получает доступ к области, защищенной базой данных запросов доступа
Если связующий адрес найден в базе данных запросов доступа, доступ предоставляется. В противном случае доступ не предоставляется.
Если в базе данных запросов доступа зарегистрировано уведомление отсутствии регистрации/нарушении ключа пользователя, доступ прекращается
Выход из системы, конец сеанса, ограниченный по времени доступ, нарушение ключа и т.п.
Уведомление абонентской системы о том, что абонент больше не идентифицируется

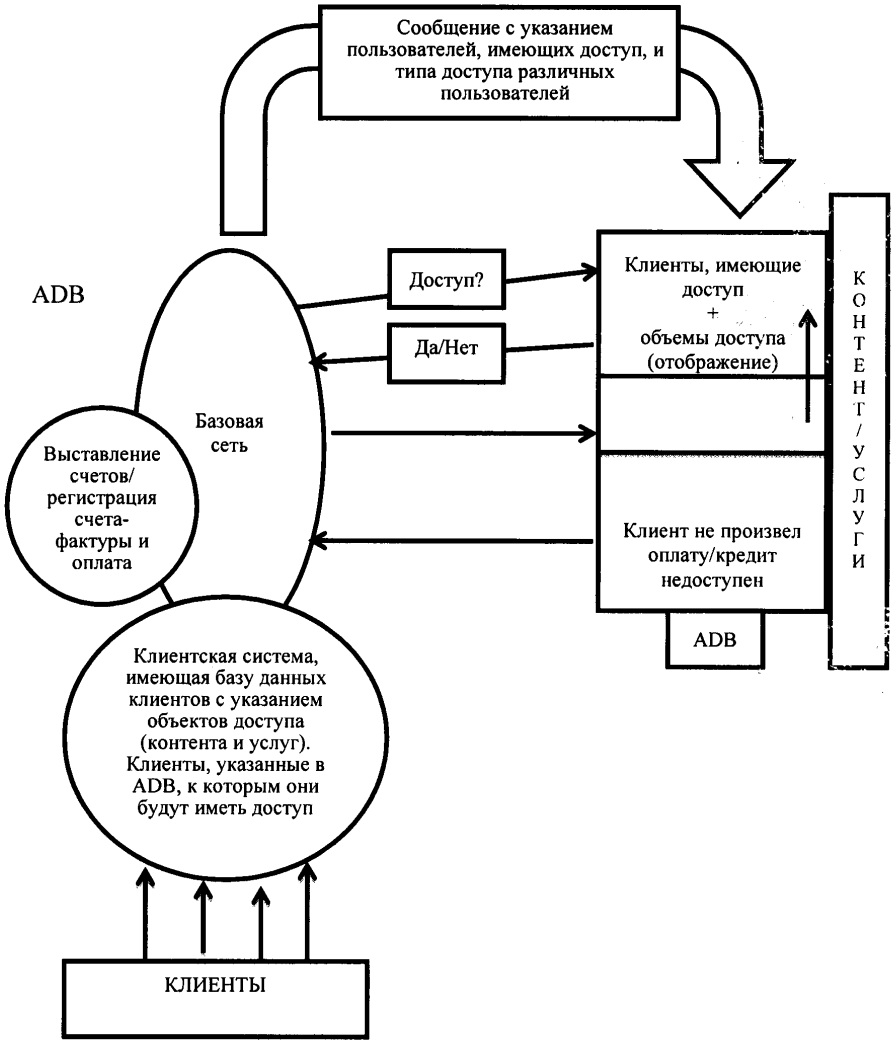
ФИГ. 6

7


Сообщение с указанием пользователей, имеющих доступ, и типа доступа различных пользователей
Доступ?
Да/Нет
?
Да/Нет
Базовая сеть
Выставление счетов/ регистрация счета-фактуры и оплата
Клиентская система, имеющая базу данных клиентов с указанием объектов доступа (контента и услуг). Клиенты, указанные в ADB, к которым они будут иметь доступ
КЛИЕНТЫ
Клиенты имеющие доступ + объемы доступа (отображение)
Клиент произвел оплату? (Кредит?)
Регистрация трафика (пересылка базовой сети)
ADB
КОНТЕНТ/УСЛУГИ

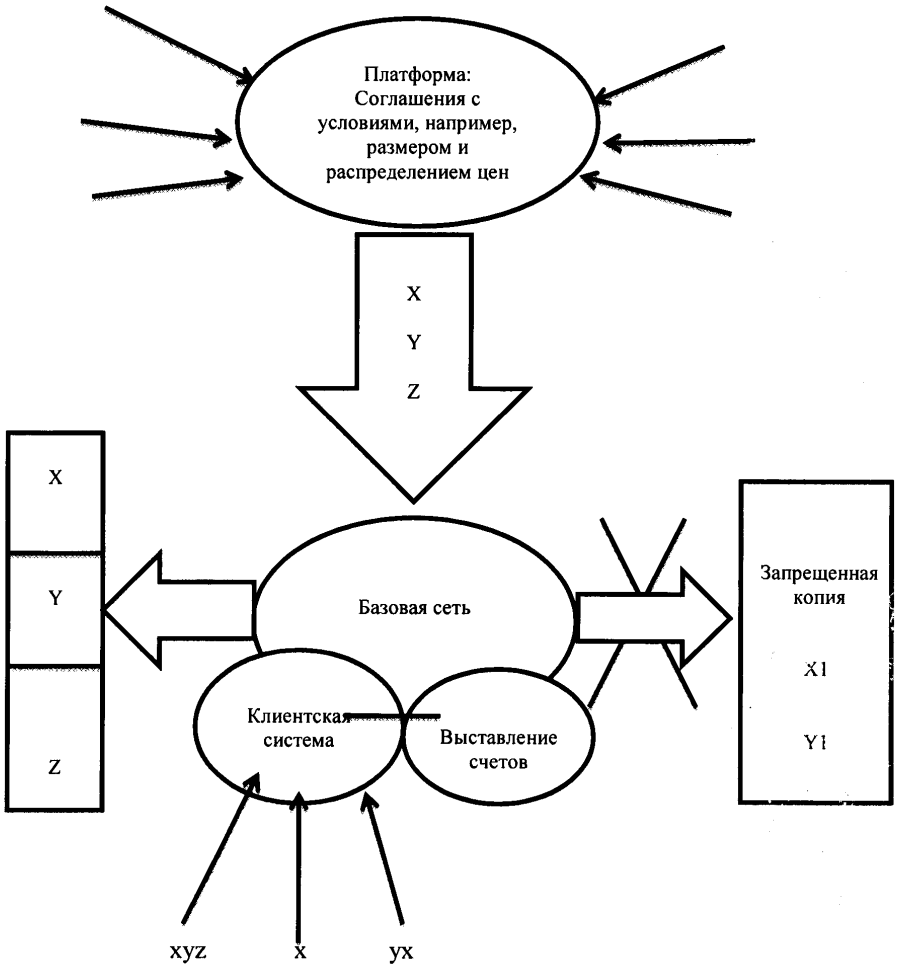
ФИГ. 7

8


Сообщение с указанием пользователей, имеющих доступ, и типа доступа различных пользователей
ADB
Доступ?
Да/Нет
Базовая сеть
Выставление счетов/ регистрация счета-фактуры и оплата
Клиенты, имеющие доступ + объемы доступа (отображение)
Клиент не произвел оплату/кредит недоступен
ADB
КОНТЕНТ/УСЛУГИ
Клиентская система, имеющая базу данных клиентов с указанием объектов доступа (контента и услуг). Клиенты, указанные в ADB, к которым они будут иметь доступ
КЛИЕНТЫ

ФИГ. 8

9


Платформа:
Соглашения с
условиями, например,
размером и
распределением цен
X
Y
Z
X
Y
Z
Базовая сеть
Клиентская
система
Выставление
счетов
Запрещенная
копия
X1
Y1
xyz
x
yx

ФИГ. 9