



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ(21)(22) Заявка: **2008107737/07**, 17.08.2006(24) Дата начала отсчета срока действия патента:
17.08.2006

Приоритет(ы):

(30) Конвенционный приоритет:
31.08.2005 US 11/216,627(43) Дата публикации заявки: **10.09.2009** Бюл. № 25(45) Опубликовано: **20.06.2012** Бюл. № 17(56) Список документов, цитированных в отчете о поиске: **US 2005130641 A1**, 16.06.2005. **EP 1422909 A2**, 26.05.2004. **WO 0103392 A1**, 11.01.2001. **WO 0195063 A2**, 13.12.2001. **WO 0120859 A1**, 22.03.2001. **WO 0042760 A1**, 20.07.2000. **RU 2232478 C2**, 10.07.2004. **RU 2229199 C2**, 20.05.2004. **RU 2003133294 A**, 27.05.2005. **Гольдштейн Б.С. и др. IP ТЕЛЕФОНИЯ, РАДИО И СВЯЗЬ. - М., 2001 Cisco Voice Over IP, Version 4.2, Student Guide, Cisco Systems Inc., 2004.**(85) Дата начала рассмотрения заявки РСТ на национальной фазе: **28.02.2008**(86) Заявка РСТ:
US 2006/032092 (17.08.2006)(87) Публикация заявки РСТ:
WO 2007/027439 (08.03.2007)

Адрес для переписки:

**129090, Москва, ул. Б.Спасская, 25, стр.3,
ООО "Юридическая фирма Городиский и
Партнеры", пат.пов. Ю.Д.Кузнецову,
рег.№ 595**

(72) Автор(ы):

**КРИДДЛ Линда (US),
МИЛСТЕЙН Дэвид (US)**

(73) Патентообладатель(и):

МАЙКРОСОФТ КОРПОРЕЙШН (US)

RU 2 4 5 4 0 1 3 C 2

RU 2 4 5 4 0 1 3 C 2

(54) УПРАВЛЕНИЕ ПЕРЕДАЧЕЙ РЕЧИ ПО ИНТЕРНЕТ-ПРОТОКОЛУ (VoIP)

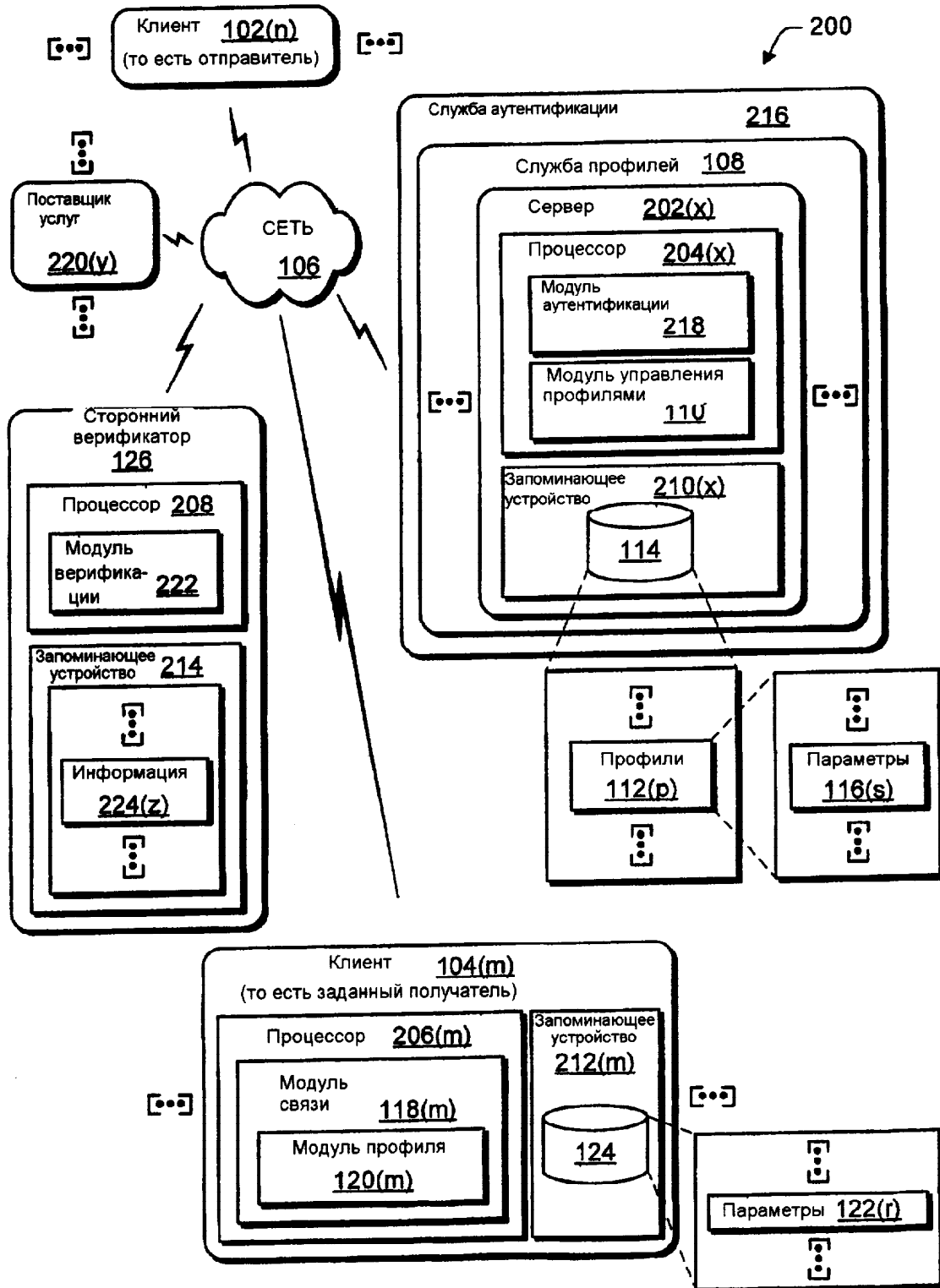
(57) Реферат:

Изобретение относится к области связи и, в частности, к телефонным услугам "VoIP" (передача речи по Интернет-протоколу). Техническим результатом является обеспечение безопасности членов семьи и

конфиденциальности посредством управления маршрутизацией звонков VoIP для конкретных членов семьи. Указанный технический результат достигается тем, что предложен способ управления сообщением по протоколу VoIP, содержащий этапы, на

которых: создают пользовательский профиль на основании параметров безопасности, обеспечивающих меры по обеспечению безопасности, принимают VoIP-сообщение, предназначенное для заданного получателя, доступного по сетевому адресу, определяют, что пользовательский профиль соответствует упомянутому заданному получателю этого VoIP-сообщения; и управляют сообщением VoIP на основе упомянутых

параметров безопасности, заданных в пользовательском профиле, причем управление дополнительно содержит этапы: маршрутизируют VoIP-сообщение к стороннему верификатору, доступному по другому сетевому адресу, который отличается от сетевого адреса заданного получателя, и маршрутизируют VoIP-сообщение, как задано сторонним верификатором. 3 н. и 13 з.п. ф-лы, 6 ил.



ФИГ.2



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(51) Int. Cl.
H04L 12/66 (2006.01)
H04W 8/18 (2009.01)

(12) **ABSTRACT OF INVENTION**

(21)(22) Application: **2008107737/07, 17.08.2006**

(24) Effective date for property rights:
17.08.2006

Priority:

(30) Convention priority:
31.08.2005 US 11/216,627

(43) Application published: **10.09.2009 Bull. 25**

(45) Date of publication: **20.06.2012 Bull. 17**

(85) Commencement of national phase: **28.02.2008**

(86) PCT application:
US 2006/032092 (17.08.2006)

(87) PCT publication:
WO 2007/027439 (08.03.2007)

Mail address:
**129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO
"Juridicheskaja firma Gorodisskij i Partnery",
pat.pov. Ju.D.Kuznetsovu, reg.№ 595**

(72) Inventor(s):
**KRIDDL Linda (US),
MILSTEJN Dehvid (US)**

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

(54) **VOICE OVER INTERNET PROTOCOL (VoIP) MANAGEMENT**

(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to communication and particularly to voice over Internet protocol (VoIP) telephone services. Disclosed is a method of managing VoIP messages, comprising steps for: creating a user profile based on security parameters, which provide security measures; receiving a VoIP message meant for a given recipient, accessible on a network address; determining that the user profile matches said given recipient of said VoIP message; and managing the

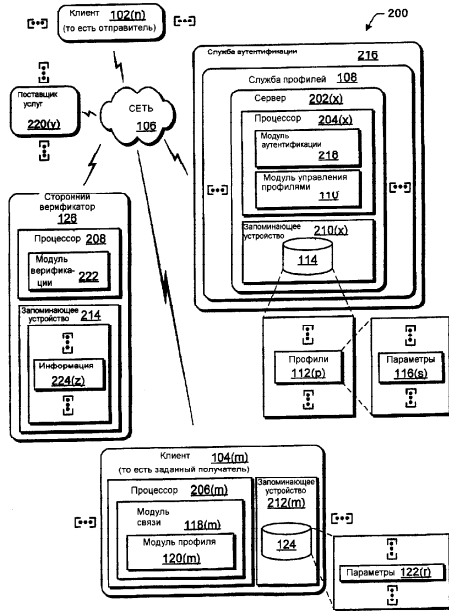
VoIP message based on said security parameters given in the user profile, wherein managing further comprises steps for: routing the VoIP message to a third-party verifier accessible on another network address other than the network address of the given recipient, and the VoIP message is routed as indicated by the third-party verifier.

EFFECT: ensuring safety of family members and confidentiality by managing routing of VoIP calls for specific family members.

16 cl, 6 dwg

RU 2 4 5 4 0 1 3 C 2

RU 2 4 5 4 0 1 3 C 2



ФИГ. 2

RU 2 4 5 4 0 1 3 C 2

RU 2 4 5 4 0 1 3 C 2

Уровень техники

В течение многих лет абоненты общались друг с другом посредством использования традиционных телефонных услуг, известных также под названием традиционной службы телефонной связи (POTS). Поэтому абоненты знают и привыкли к определенным способам осуществления связи посредством традиционных телефонных услуг, таким как набор номера, переадресация вызова и т.д.

Одним способом предоставления телефонных услуг, который завоевывает все большую популярность, является "VoIP", что является сокращением от Voice over Internet Protocol (передача речи по Интернет-протоколу). VoIP обычно осуществляется с использованием Интернета так, чтобы абоненты могли общаться друг с другом так же, как во время обычного телефонного разговора. Однако поскольку абоненты имеют длительное знакомство с традиционными телефонными услугами, компании, предоставляющие услуги VoIP, обычно обеспечивают эти услуги так, чтобы имитировать традиционную службу телефонной связи. Поэтому абонентам этих традиционных телефонных услуг, хотя они предоставляются привычным наглядным образом, не предоставляют дополнительные функциональные возможности, которые могут стать доступными посредством VoIP.

Сущность изобретения

Описаны способы управления передачей речи по интернет-протоколу (VoIP). В одном или нескольких вариантах осуществления способы управления реализуются посредством использования программного обеспечения для предоставления широких функциональных возможностей связи VoIP. Например, способы управления могут обеспечивать безопасность членов семьи и конфиденциальность посредством управления маршрутизацией звонков VoIP для конкретных членов семьи.

Настоящая краткая сущность изобретения предназначена для ознакомления с некоторыми идеями изобретения в упрощенной форме, которые более подробно описаны ниже в подробном описании. Краткая сущность изобретения не предназначена для выявления основных или существенных признаков заявленного изобретения и не предназначена для использования в качестве средства для определения объема заявленного изобретения.

Краткое описание чертежей

На фиг.1 приведен пример реализации среды, которая выполнена с возможностью использования способов для управления связью VoIP.

На фиг.2 приведен пример реализации системы, в котором клиенты, служба профилей и сторонний верификатор, показанные на фиг.1, изображены более подробно.

На фиг.3 приведена блок-схема последовательности действий, изображающая пример реализации процедуры, в которой создается профиль, используемый для управления сообщением VoIP.

На фиг.4 приведена блок-схема последовательности действий, изображающая пример реализации процедуры, в которой используется профиль для управления множеством способов связи, по меньшей мере один из которых включает в себя связь согласно VoIP.

На фиг.5 приведена блок-схема последовательности действий, изображающая пример реализации процедуры, в которой сообщение VoIP, предназначенное определенному получателю, направляется стороннему верификатору перед его получением этим определенным получателем.

На фиг.6 приведена блок-схема последовательности действий, изображающая

пример реализации процедуры, в которой применяются различные способы управления для управления сообщением VoIP.

В описании одинаковые номера позиций используются в примерах осуществления для ссылки на аналогичные структурные элементы.

ПОДРОБНОЕ ОПИСАНИЕ

Общий обзор

Способы традиционной телефонной связи предлагают пользователям ограниченные функциональные возможности. Например, сегодня при осуществлении телефонного соединения по фиксированной линии связи меры по обеспечению безопасности членов семьи и конфиденциальности не предлагаются. Родители, к примеру, не могут в настоящее время управлять тем, кто может связываться с их детьми, в какое время разрешена такая связь (если разрешена) и т.д.

В различных вариантах осуществления описаны способы, которые позволяют управлять связью, осуществляемой посредством передачи речи по интернет-протоколу (VoIP). Может применяться множество других способов управления для предоставления широких функциональных возможностей. Например, в одном способе может использоваться профиль, который задает параметры абонента, например, указывает, каким абонентам разрешено связываться с данным абонентом, куда направлять сообщения VoIP, поступившие от конкретных абонентов, и т.д. Затем, до того как сообщение VoIP будет принято абонентом, может быть осуществлено управление сообщением VoIP, предназначенным абоненту, на основе профиля. Например, управление сообщением на основе профиля до передачи его заданному получателю может осуществлять поставщик услуг VoIP, что будет более подробно рассмотрено ниже со ссылкой на фиг.3.

В другом примере профиль может использоваться для управления способами связи, по меньшей мере один из которых включает в себя связь, согласно VoIP. Например, профиль можно использовать как для управления связью, согласно VoIP, так и электронной почтой, мгновенным обменом сообщениями и т.д. Таким образом, родитель может задать профиль для ребенка, который относится к каждому способу сетевой связи, к которому может прибегнуть ребенок. Более подробное рассмотрение управления различными способами связи приведено ниже со ссылкой на фиг.4.

В другом примере для контроля сообщения, согласно VoIP, может применяться сторонний верификатор. Например, сообщение VoIP от отправителя, который не указан в профиле, может сначала направляться родителю на утверждение. В другом примере может использоваться служба аутентификации, например, посредством использования исполняемого модуля, который автоматически запрашивает автора сообщения VoIP, что более подробно рассмотрено ниже со ссылкой на фиг.5.

В дальнейшем рассмотрении сначала описан пример среды, которая выполнена с возможностью обеспечения управления передачей речи по интернет-протоколу. Затем описаны примеры процедур, которые могут использоваться в этом примере среды, а также в других средах.

Пример среды

На фиг.1 приведен пример реализации среды 100, выполненной с возможностью применения способов управления связью VoIP. Приведенная на чертеже среда 100 включает в себя множество клиентов 102(n), 104(m) (где "n" и "m" могут быть любым целым числом соответственно от одного до "N" и "M"), которые коммуникативно соединены друг с другом посредством сети 106. Клиенты 102(n), 104(m) могут быть сконфигурированы различным образом для связи через сеть 106. Например, один или

несколько клиентов 102(n), 104(m) могут быть сконфигурированы в качестве телефонов, предназначенных для VoIP (например, проводных или беспроводных), что и показано на чертеже вычислительного устройства, такого как настольный компьютер, мобильной станции, развлекательного устройства, телевизионной приставки, коммуникативно связанной с устройством отображения, игровой приставкой и т.д. Таким образом, клиенты 102(n), 104(m) могут представлять собой устройства в диапазоне от устройств, обладающих полноценными ресурсами со значительной памятью и значительными ресурсами для обработки информации (например, существующие беспроводные телефоны, КПК), до устройств, обладающих ограниченными ресурсами с ограниченной памятью и (или) ограниченными ресурсами для обработки информации (например, беспроводные телефоны предыдущего поколения, ручные игровые приставки). Клиенты 102(n), 104(m) могут также иметь отношение к физическому или юридическому лицу, которое управляет клиентами. Иными словами, в дальнейшем описании под одним или несколькими клиентами 102(n), 104(m) могут пониматься логические клиенты, которые включают в себя пользователей, программное обеспечение и(или) устройства.

Хотя в качестве сети 106 приведена сеть Интернет, сеть может принимать самые различные конфигурации. Например, сеть 106 может включать в себя участки, сконфигурированные в виде глобальной сети (WAN), локальной сети (LAN), беспроводной сети, телефонной сети общего доступа, интрасети и т.д. Таким образом, хотя на чертеже показана одна сеть 106, сеть 106 может быть сконфигурирована таким образом, чтобы включать в себя множество сетей.

В приведенной среде клиенты 102(n), 104(m) осуществляют связь друг с другом через сеть 106 при помощи технических средств связи, обеспечивающих передачу речи по интернет-протоколу (VoIP). Технические средства связи VoIP используют пакеты для передачи голосовых сообщений между клиентами 102(n), 104(m) по сети 108.

Например, отправитель (например, клиент) 102(n) может быть выполнен с возможностью преобразовывать аналоговый сигнал в цифровые данные, которые затем передаются получателю, то есть клиенту 104(m), по сети 106 в виде множества пакетов, которые включают в себя эти цифровые данные. Клиент 104(m) может быть выполнен с возможностью упорядочивать принятые пакеты и преобразовывать цифровые данные в аналоговый сигнал, который выдается в клиенте 104(m). Аналогично, связь, согласно VoIP, может выполняться в обратном направлении от клиента 104(m) к клиенту 102(n) посредством пакетов, так что клиенты 102(n), 104(m) могут принимать участие в разговоре. Таким образом, цифровые данные представляют собой полезную нагрузку в пакетах, каждый из которых включает в себя адрес, по которому следует отправлять пакет.

Иллюстрируемая среда 100 включает в себя службу 108 профилей, которая выполнена с возможностью управления связью VoIP между клиентами 102(n), 104(m), и которая поэтому изображена "внутри" сети 106 и "между" клиентами 102(n), 104(m).

Служба 108 профилей включает в себя модуль 110 управления профилями, в котором реализуются функциональные возможности для создания и управления множеством профилей 112(p) (где "p" может быть любым целым числом от единицы до "P"), которые показаны хранящимися в устройстве 114 хранения данных.

Каждый из профилей 112(p) соответствует одному из множества клиентов 102(n), 104(m) и содержит соответствующие параметры 116(s), где "s" может быть любым целым числом от единицы до "S", относящиеся к способам связи для соответствующего клиента из клиентов 102(n), 104(m). Например, клиент 104(m) может

иметь соответствующий профиль 112(p), который включает в себя параметры 116(s) безопасности и конфигурации, которые задают, каким из множества клиентов 102(n) разрешено связываться с клиентом 104(m), в какое время разрешена такая связь, какой способ связи может использоваться для связи с клиентом 104(m) (например, электронная почта, мгновенный обмен сообщениями, VoIP, электронные доски объявлений, блоги и т.д.), настройки для каждого способа связи (например, HTML для электронной почты, версия, поддерживаемая для мгновенного обмена сообщениями) и т.д. Например, профиль 112(p) может быть сконфигурирован в виде списка контактов и включать указание на то, разрешена ли связь с определенными контактами. Модуль 110 управления профилями может затем управлять связью с клиентом 104(m) при помощи соответствующих профилей 112(p).

Для управления VoIP и другими способами связи по сети 106 между клиентами 102(n), 104(m) могут применяться различные способы. Например, родитель может взаимодействовать с модулем 110 управления профилями посредством модуля 118(m) связи (например, сконфигурированного в виде веб-браузера, модуля мгновенного обмена сообщениями и т.д.) для создания профиля 112(p) конкретного ребенка. При создании профиль 112(p) может содержать параметры 116(s), которые задают разрешенную и(или) неразрешенную связь с ребенком, например, каким клиентам 102(n) разрешено или не разрешено связываться с ребенком, в какое время разрешена или не разрешена такая связь и т.д. Модуль 110 управления профилями может затем использовать созданный профиль 112(p) для управления отправленным сообщением даже до того, как такое сообщение будет принято получателем, в данном примере - ребенком. Например, модуль 110 управления профилями может блокировать сообщение, в котором содержится указание (например, идентификатор в заголовке пакета), что оно отправлено от одного из клиентов 102(n), которому не разрешено связываться с ребенком, до того, как это сообщение будет доставлено клиенту 104(m).

В другом примере профиль 112(p) может быть выполнен с возможностью "перемещения" вместе с соответствующим абонентом. Например, ребенок может, как описано выше, использовать для связи посредством сети 106 большое количество клиентских устройств, таких как радиотелефон, КПК, настольный компьютер и т.д. Поэтому служба 108 профилей может быть выполнена с возможностью использовать профиль 112(p) независимо от того, какое клиентское устройство используется ребенком. Например, модуль 118(m) связи может включать в себя модуль 120(m) профиля, который выполнен с возможностью связи через сеть 106 со службой 108 профилей для получения параметров 116(s) от профиля 112(p), который соответствует данному ребенку. Эти параметры 116(s) могут быть переданы через сеть 106 и храниться локально в клиенте 104(m) в виде параметров 122(r) (где "r" может быть любым целым числом от одного до "R") в локальном устройстве 124 хранения данных. В другом примере параметры 116(s) "остаются" в службе 108 профилей, и управление связью осуществляется описанным выше образом, так что клиенту 104(m) не нужно принимать сообщение прежде, чем будет осуществлено управление. В таком случае ребенок может "подключиться" в службе 108 профилей, прежде чем будет получено разрешение на связь с множеством клиентов 102(n). Возможно также множество других примеров, подробное рассмотрение которых приведено со ссылкой на фиг.4.

В еще одном примере служба 108 профилей может также использовать сторонний верификатор 126 для проверки, разрешена ли связь между клиентами 102(n), 104(m). Например, модуль 110 управления профилями может перехватить сообщение VoIP,

предназначенное ребенку, например, клиенту 104(m). Однако отправитель (например, клиент 102(n)) сообщения VoIP может не быть включен в профиль 112(p) для клиента 104(m), а это значит, что сообщения от клиента 102(n) разрешены. В таком случае модуль 110 управления профилями, прежде чем разрешить передачу сообщения клиенту 104(m), может направить сообщение стороннему верификатору 126. Сторонний верификатор 126 может иметь различную конфигурацию, например, он может быть другим клиентом из клиентов 104(m), который является родителем ребенка, сетевой службой сторонней верификации, автоматизированной службой сторонней верификации и т.д. Решение о том, разрешать ли передачу сообщения VoIP клиенту 104(m), может быть затем основано, по меньшей мере частично, на результатах верификации. Дальнейшее описание сторонней верификации приведено ниже со ссылкой на фиг.5.

Хотя было описано управление VoIP, сеть 106 может также поддерживать различные другие способы связи. Например, клиенты 102(n), 104(m) могут связываться по сети 106 при помощи электронной почты, мгновенного обмена сообщениями, электронных досок объявлений, дискуссионных групп и т.д. Поэтому технические средства управления могут быть также выполнены с возможностью обращения с этими другими способами связи для обеспечения единой структуры управления, более подробное обсуждение которой приведено со ссылкой на фиг.4.

Кроме того, хотя описанное управление VoIP осуществлялось посредством службы 108 профилей, управлять VoIP и другими способами связи может также клиент 104(m). Например, модуль 120(m) профиля в процессе выполнения может обеспечивать функциональные возможности, аналогичные тем, что описаны для модуля 128 управления профилями службы 108 профилей. Можно придумать также различные другие примеры.

В целом любые описанные в настоящем описании функции можно реализовать при помощи программного обеспечения, встроенных программно-аппаратных средств (например, при помощи неизменяемых логических схем), ручной обработки или сочетания этих вариантов реализации. Термины "модуль", "функциональные возможности" и "логика", используемые в настоящем документе, обозначают в целом программное обеспечение, программно-аппаратные средства или сочетание программного обеспечения и программно-аппаратных средств. В случае программной реализации модуль, функциональные возможности и логика представляют программный код, который выполняет определенные задачи при его исполнении процессором (например, одним или несколькими ЦПУ). Программный код может храниться в одном или нескольких машиночитаемых запоминающих устройствах, более подробное описание которых приведено ниже со ссылкой на фиг.2. Описанные ниже характеристики способов управления VoIP являются платформо-независимыми, что означает, что эти способы могут быть реализованы на множестве коммерческих вычислительных платформ, имеющих различные процессоры.

На фиг.2 приведен вариант реализации системы 200, где клиенты 104(m), служба 108 профилей и сторонний верификатор 126, изображенные на фиг.1, приведены более подробно. Приведенная служба 108 профилей реализована в виде множества серверов 202(x), где "x" может быть любым целым числом от единицы до "X", а сторонний верификатор 126 и устройства 104(m) показаны в виде устройств. Таким образом, серверы 202(x), клиенты 104(m) и сторонний верификатор 126 включают каждый соответствующий процессор 204(x), 206(m), 208 и соответствующее запоминающее устройство 210(x), 212(m), 214.

Процессоры не ограничены какими-либо определенными материалами, из которых они выполнены, и какими-либо определенными применяемыми в них механизмами обработки данных. Например, процессоры могут содержать полупроводник(и) и (или) транзисторы (например, электронные интегральные схемы (ИС)). В таком контексте выполняемые процессором команды могут быть электронно-выполняемыми командами. В альтернативном варианте, механизмы процессоров или предназначенные для процессоров, и тем самым - вычислительного устройства, или предназначенные для вычислительного устройства могут включать в себя, в частности, квантовые вычисления, оптические вычисления, механические вычисления (например, с использованием нанотехнологии) и т.д. Кроме того, хотя показано одно запоминающее устройство 210(x), 212(m), 214 соответственно для серверов 202(x), клиентов 104(n) и стороннего верификатора 126, можно использовать различные типы и сочетания запоминающих устройств, таких как оперативное запоминающее устройство (ОЗУ), запоминающее устройство на жестком диске, запоминающее устройство на съемном носителе и другие типы машиночитаемых носителей.

Приведенный модуль 110 управления профилями выполнен на процессоре 204(x) и может храниться в запоминающем устройстве 210(x). Как описано выше, модуль 110 управления профилями представляет функциональные возможности, которые управляют способами связи VoIP, а также другими способами связи. Например, модуль 110 управления профилями может использовать параметры 116(s), заданные в профиле 112(p), который соответствует конкретному пользователю, для управления тем, каким образом разрешена связь с данным абонентом. Например, параметры 116(s) могут указывать время дня (например, вечер - от полуночи до шести часов утра и т.д.), определенные дни (например, выходные, праздники и т.д.), число разговоров в день, продолжительность разговоров и т.д.

В процессе управления сообщениями на основе параметров 116(s) могут быть выполнены различные действия. Например, модуль 110 управления профилями может блокировать сообщение, передать сообщения от одного способа связи другому способу связи (например, передать вызов VoIP в электронную почту), направить сообщения (например, стороннему верификатору, голосовой почте, правоохранительным органам при наличии признаков преследования и т.д.), обеспечить соответствующий выходной сигнал на основе личности отправителя (например, персонализированный сигнал вызова, персонализированное сообщение отправителю и т.д.), обеспечивать индикацию "вызова" отправителю, но не получателю (например, в случае звонка ребенку в неурачные часы), уведомлять и записывать конкретные разговоры (например, разговоры, связанные с работой, для их дальнейшего изучения) и т.д.

В системе 200, приведенной на фиг.2, иллюстрируемая служба 108 профилей включена в качестве составной части в службу 216 аутентификации. Служба 216 аутентификации включает в себя модули 218 аутентификации (которые показаны выполняющимися на процессоре 204(x) и хранящимися в запоминающем устройстве 210(x)), которые представляют функциональные возможности, которые обеспечивает служба аутентификации для множества поставщиков 220(y) услуг, где "y" может быть любым целым числом от единицы до "Y".

Например, поставщики 220(y) услуг (например, такие как веб-сайты, поставщики услуг электронной почты, системы мгновенного обмена сообщениями и т.д.) могут "избавиться" от функций аутентификации, передав ее службе 216 аутентификации. Поэтому когда клиент 104(m) регистрируется в (то есть подключается к) службе 216

аутентификации, клиент 104(m) может переходить от одного поставщика 220(y) услуг к другому без предоставления каждый раз своих регистрационных данных. Включение службы 108 профилей в службу 216 аутентификации позволяет модулю 110 управления профилями управлять также связью клиента 104(m) с поставщиками 220(y) услуг, такими как разрешенные веб-сайты и т.д. Таким образом, родитель ребенка может дополнительно управлять взаимодействием ребенка при помощи единого профиля 112(p), не прибегая к созданию отдельного профиля для каждого поставщика 220(y) услуг, клиентского устройства, используемого ребенком, и т.д.

5

10 Более подробное рассмотрение использования профиля 112(p) для множества способов связи приведено со ссылкой на фиг.4.

Как было описано выше, сторонний верификатор 126 может быть реализован различными способами. Например, сторонний верификатор 126 может быть родителем ребенка, к которому первоначально направляется неизвестное сообщение, прежде чем доставить его ребенку. В системе 200, приведенной на фиг.2, сторонний верификатор 126 реализован в виде автономной службы сторонней верификации. Сторонний верификатор 126 включает в себя модуль 222 верификации, который показан выполняемым на процессоре 208 и хранящимся в запоминающем устройстве 214. В процессе выполнения модуль 222 верификации может обеспечивать различные функциональные возможности. Например, модуль 222 верификации может обеспечивать пользовательский интерфейс, который отображает информацию, относящуюся к передаваемому сообщению (например, сообщению VoIP), которое должно быть передано определенному клиенту 104(m), например имя абонента, источник сообщения, параметры 116(s), заданные родителем для ребенка, и т.д.

15

20 Оператор стороннего верификатора 126 может затем послать запрос отправителю (например, клиенту 102(n)) для подтверждения личности отправителя и того, насколько вероятно, что клиент 104(m) желает или ему позволено принимать сообщения от отправителя. В другом варианте осуществления это определение может быть выполнено автоматически, например, посредством сравнения с информацией 224(z) об отправителе. Можно привести множество других примеров, подробное обсуждение которых приведено ниже со ссылкой на фиг.5.

Примеры процедур

Ниже описаны способы управления VoIP, которые могут быть реализованы при помощи ранее описанных систем и устройств. Аспекты каждой из этих процедур могут быть реализованы в аппаратном виде, в виде программно-аппаратных средств или в виде программного обеспечения либо посредством их сочетания. Процедуры изображены в виде набора блоков, которые обозначают операции, выполняемые одним или несколькими устройствами, и не обязательно ограничены изображенным порядком выполнения операций, обозначаемым соответствующими блоками. В различных местах нижеследующего описания сделаны ссылки на среду, приведенную на фиг.1, и систему, приведенную на фиг.2.

35

40

На фиг.3 изображен пример реализации процедуры 300, в которой для управления сообщением VoIP создается и используется профиль. Выдается пользовательский интерфейс, который выполнен с возможностью приема входных данных от пользователя, задающих параметры безопасности (этап 302). Например, пользовательский интерфейс может включать в себя падающие меню для различных параметров, которые можно выбрать для задания разрешенной и (или) неразрешенной связи между пользователем и другим пользователем, определенного времени (например, определенный день, день недели, праздники и т.д.), когда связь

45

50

разрешена, разрешенных способов связи, которые могут применяться (например, электронная почта после 9 вечера) и т.д. Таким образом, при помощи пользовательского интерфейса может быть создан профиль для конкретного пользователя (этап 304), который затем может храниться со множеством других профилей, которые соответствуют множеству других пользователей (этап 306). Например, модуль 120(m) профиля может связываться через сеть 106 с модулем 110 управления профилями для создания и хранения профиля 112(p) в устройстве 114 хранения данных.

Служба 108 профилей принимает сообщение VoIP, предназначенное для указанного получателя (этап 308). Например, сообщение VoIP может задавать конкретного пользователя, группу пользователей и т.д. Затем служба 108 профилей определяет, какой из множества профилей 112(p) соответствует указанному получателю (этап 310). Например, модуль 110 управления профилями может найти и сравнить идентификатор в пакете сообщения VoIP, который указывает, "куда" следует передать пакет, и использует идентификатор для обнаружения соответствующего профиля 112(p).

Затем на основе одного или более параметров безопасности в определенном профиле осуществляется управление сообщением VoIP, прежде чем сообщение VoIP будет принято указанным получателем (этап 312). Например, модуль 110 управления профилем может решить заблокировать сообщение VoIP, направить сообщение VoIP стороннему верификатору, получить персонализированный "сигнал вызова" для выдачи его указанному получателю, получить персонализированный "ответный сигнал вызова" для выдачи его отправителю (например, клиенту 102(n)), отклонить сообщение, но выдать "сигнал" обратно клиенту 102(n), направить сообщение в правоохранительные органы и т.д.

Таким образом, могут быть предоставлены различные функциональные возможности еще до того, как указанный получатель получит сообщение VoIP, хотя в другом варианте осуществления эти функциональные возможности могут быть представлены посредством выполнения модуля 120(m) профиля, который, как было описано выше, расположен локально в клиенте 104(m). Можно также применять множество других способов управления без отступления от сущности и объема этих способов, более подробное описание которых приведено со ссылкой на последующие чертежи.

На фиг.4 изображен пример реализации процедуры 400, в которой используется профиль для управления множеством способов связи, по меньшей мере один из которых включает в себя связь VoIP. Как описано со ссылкой на фиг.3, создается профиль, имеющий множество параметров безопасности, которые применяются к пользователю, когда он взаимодействует с одним или несколькими из множества других пользователей (этап 402). Например, профиль может указывать, что связь с другим определенным клиентом запрещена в любое время, тогда как связь с еще одним конкретным клиентом разрешена в определенное время дня.

Затем при помощи созданного профиля осуществляется управление использованием множества способов связи, по меньшей мере один из которых включает в себя связь VoIP (этап 404). Например, от определенного отправителя может быть принято сообщение VoIP (этап 406). Затем на основе профиля можно осуществлять управление сообщением VoIP (этап 408), например блокировать, направлять, сохранять, выбирать соответствующее сообщение и т.д. Например, сообщение VoIP может быть принято от друга ребенка в "неурочное время", то есть после того времени, когда ребенку разрешено принимать вызовы. Затем может быть

принято другое сообщение от того же конкретного отправителя, отправленное другим способом связи (этап 410), управление которым также осуществляется на основе созданного профиля (этап 412).

5 Например, после сообщения VoIP этот друг может отправить ребенку сообщение по электронной почте. Поскольку сообщения электронной почты можно хранить, и ребенок может прочесть их позже, родитель, создавший профиль, может разрешить такое сообщение. Таким образом, в данном примере параметры безопасности могут быть для конкретного отправителя различными в зависимости от способа связи, 10 используемого этим конкретным отправителем. Можно также придумать множество других примеров. Например, конкретный отправитель может блокироваться вне зависимости от того, какой используется способ сообщения для связи с указанным получателем. Поэтому хотя в данном примере не были указаны различные способы связи, профиль по-прежнему обеспечивает упрощенный и централизованный 15 механизм, посредством которого можно контролировать поступление к ребенку нежелательных сообщений. Хотя в данном примере в качестве способов связи были описаны VoIP и электронная почта, профиль можно использовать для управления множеством других способов связи, таких как доступ к электронным доскам 20 объявлений и размещение в них объявлений, доступ к сетевым журналам (то есть к блогам), к мгновенному обмену сообщениями и т.д. без отступления от сущности и объема изобретения.

На фиг.5 изображен пример реализации процедуры 500, в которой сообщение VoIP, 25 предназначенное для указанного получателя, сначала направляется стороннему верификатору, прежде чем его получит указанный получатель. Сообщение VoIP принимает служба профилей (этап 502). Например, сообщение VoIP, отправленное клиентом 102(n) и предназначенное для клиента 104(m), может быть принято службой 108 профилей, которая выполнена в виде автономной службы. Затем 30 идентифицируется отправитель сообщения VoIP (этап 504). Например, модуль 110 управления профилями в процессе своего выполнения может запросить профили 112(p) для поиска профиля, которые соответствуют указанному получателю, например клиенту 104(m).

Затем определяется, указан ли данный отправитель в профиле (этап 506 принятия 35 решения). Если является "да" от этапа 506 принятия решения, то осуществляется управление сообщением VoIP указанным в профиле образом (этап 508), например направить, заблокировать, сохранить и т.д.

Если отправитель в профиле не указан ("нет" от этапа 506 принятия решения), 40 сообщение VoIP направляется стороннему верификатору (этап 510). Например, сообщение VoIP может быть направлено из службы 108 профилей стороннему верификатору 126 по сети 106. Как было описано выше, сторонний верификатор может быть реализован различными способами, например, это может быть родитель клиента 104(m), автономная служба, которая использует операторов для верификации 45 сообщения, автоматизированная автономная служба, в которой для верификации сообщения выполняется модуль 222 верификации и т.д.

Затем сторонний верификатор указывает действие, которое следует выполнить в отношении сообщения VoIP (этап 512), служба профилей выполняет указанное 50 действие (этап 514). Например, в информации 224(z) может быть указано, что клиент 102(n) вызывает недоверие, и потому указание может заключаться в том, что сообщение от клиента 102(n) следует заблокировать. После этого служба 108 профилей может заблокировать сообщение. В другом примере оператор стороннего

верификатора 126 может задать вопросы клиенту 102(n), например, откуда он знает клиента 104(m) и т.д. Затем оператор может определить, можно ли доверять отправителю (например, клиенту 102(n)), и предоставить результат этого определения службе 108 профилей для дальнейшей обработки. Это определение может быть автоматизировано посредством выполнения модуля 222 верификации, например посредством направления вопросов и анализа ответов на вопросы, представленных клиентом 102(n). Можно придумать также различные другие примеры без отступления от сущности и объема изобретения.

На фиг.6 изображен пример реализации процедуры 600, в которой для управления сообщением VoIP применяется множество различных способов управления. Сообщение VoIP принимает служба профилей (этап 602). Затем определяется, указан ли отправитель сообщения VoIP в профиле (этап 604 принятия решения). Если не указан ("нет" от этапа 604 принятия решения), определяется, имеется ли идентификатор вызывающего абонента (стороны) (C-ID) (этап 606 принятия решения). В зависимости от результата определения загружаются правила для случая неизвестного отправителя с идентификатором вызывающего абонента (этап 608) или правила для случая неизвестного отправителя без идентификатора вызывающего абонента (этап 610) (то есть в зависимости от "да" или "нет" от этапа 606 принятия решения).

Когда отправитель в профиле указан ("да" от этапа 604 принятия решения), загружаются параметры для данного отправителя (этап 612). Например, модуль 110 управления профилями может обнаружить идентификатор, который соответствует отправителю, и загрузить параметры, которые относятся к данному отправителю. Затем определяет, разрешено ли в настоящее время данному отправителю контактировать с указанным получателем (этап 614 принятия решения). Если разрешено ("да" от этапа 614 принятия решения), сообщение VoIP передается указанному получателю (этап 616). Если не разрешено ("нет" от этапа 614 принятия решения), определяется, следует ли передать сообщение в голосовую почту (этап 618 принятия решения).

Когда сообщение не передается в голосовую почту ("нет" от этапа 618 принятия решения), сообщение отклоняется (этап 620). Например, отправитель может быть злоумышленником и потому контакт с отправителем может быть полностью заблокирован. В другом примере сообщение может быть автоматически направлено в правоохранительные органы даже без доставки сообщения указанному получателю.

Когда сообщение передается в голосовую почту ("да" от этапа 618 принятия решения), определяется, доступно ли персонализированное сообщение (этап 622 принятия решения). Если доступно ("да" от этапа 622 принятия решения), загружается персонализированное сообщение (этап 624), а если не доступно ("нет" от этапа 622 принятия решения), загружается стандартное сообщение (этап 626). Затем сообщение VoIP передается в голосовую почту (этап 628 от этапа 624 или 626). Хотя было описано множество способов управления, имеющих конкретный порядок выполнения, должно быть очевидно, что можно также придумать множество других способов и порядков выполнения без отступления от сущности и объема изобретения.

Заключение

Хотя в описании изобретения использована терминология, характерная для конкретных структурных элементов и (или) действий по реализации способов, следует понимать, что изобретение, определяемое прилагаемой формулой, необязательно ограничивается этими описанными элементами или действиями. Вернее, эти

определенные элементы и действия раскрыты в качестве примера реализации заявленного изобретения.

Формула изобретения

5 1. Способ управления сообщением передачи речи по Интернет-протоколу (VoIP),
содержащий этапы, на которых: создают пользовательский профиль на основании
параметров безопасности, обеспечивающих меры по обеспечению безопасности,
принимают VoIP-сообщение, предназначенное для заданного получателя, доступного
10 по сетевому адресу, определяют, что пользовательский профиль соответствует
упомянутому заданному получателю этого VoIP-сообщения; и управляют
сообщением VoIP на основе упомянутых параметров безопасности, заданных в
пользовательском профиле, причем управление дополнительно содержит этапы:
15 маршрутизируют VoIP-сообщение к стороннему верификатору, доступному по
другому сетевому адресу, который отличается от сетевого адреса заданного
получателя, и маршрутизируют VoIP-сообщение, как задано сторонним
верификатором.

2. Способ по п.1, в котором параметры безопасности задают: множество контактов
20 в списке контактов, которым разрешено связываться с заданным получателем;
количество времени, которое заданному получателю разрешено потратить на связь с
одним или более контактами в списке контактов; и время дня, в течение которого
разрешается связь с одним или более контактами в списке контактов.

3. Способ по п.1, в котором этап определения дополнительно включает в себя
25 этапы, на которых: находят идентификатор заданного получателя в по меньшей мере
одном пакете VoIP-сообщения и обнаруживают пользовательский профиль, который
соответствует этому идентификатору; а этап управления включает в себя этап, на
котором управляют каждым пакетом, имеющим идентификатор согласно
30 упомянутому пользовательскому профилю.

4. Способ по п.3, в котором сторонний верификатор включает в себя один или
более дополнительных параметров безопасности, которые используются для
автоматического управления VoIP-сообщением.

5. Способ по п.1, в котором параметры безопасности независимо адресуют
35 множество способов связи.

6. Способ по п.1, в котором пользовательский профиль конфигурируется для
управления посредством идентификатора регистрации, аутентифицированного
службой аутентификации, заданным получателем по множеству различных
40 поставщиков услуг.

7. Способ по п.1, в котором параметры безопасности предоставляются стороной,
отличной от заданного получателя.

8. Способ управления сообщением передачи речи по Интернет-протоколу (VoIP),
содержащий этапы, на которых: создают профиль, который задает параметры
45 безопасности для пользователя при взаимодействии с одним или более из множества
других пользователей, принимают VoIP-сообщение, идентифицируют
отправителя VoIP-сообщения, определяют, указан ли упомянутый отправитель в
одном из множества профилей, в случае, если отправитель указан в определенном
50 профиле: управляют принятым VoIP-сообщением, используя определенный профиль, в
случае, если отправитель не указан в определенном профиле, направляют VoIP-
сообщение стороннему верификатору и используют сторонний верификатор для
выполнения действия на основе одного или более дополнительных параметров

безопасности.

9. Способ по п.8, в котором действие содержит передачу VoIP-сообщения с использованием отличного способа связи, причем упомянутый отличный способ связи включает в себя электронную почту и мгновенный обмен сообщениями.

10. Способ по п.8, в котором этап управления включает в себя аутентификацию отправителя при попытке доступа к одному из множеству поставщиков услуг в сети, при этом аутентификация разрешает отправителю переключаться между множеством поставщиков услуг и множеством клиентских устройств без повторного представления регистрационных данных.

11. Способ по п.8, в котором параметры безопасности независимо адресуют множество способов связи.

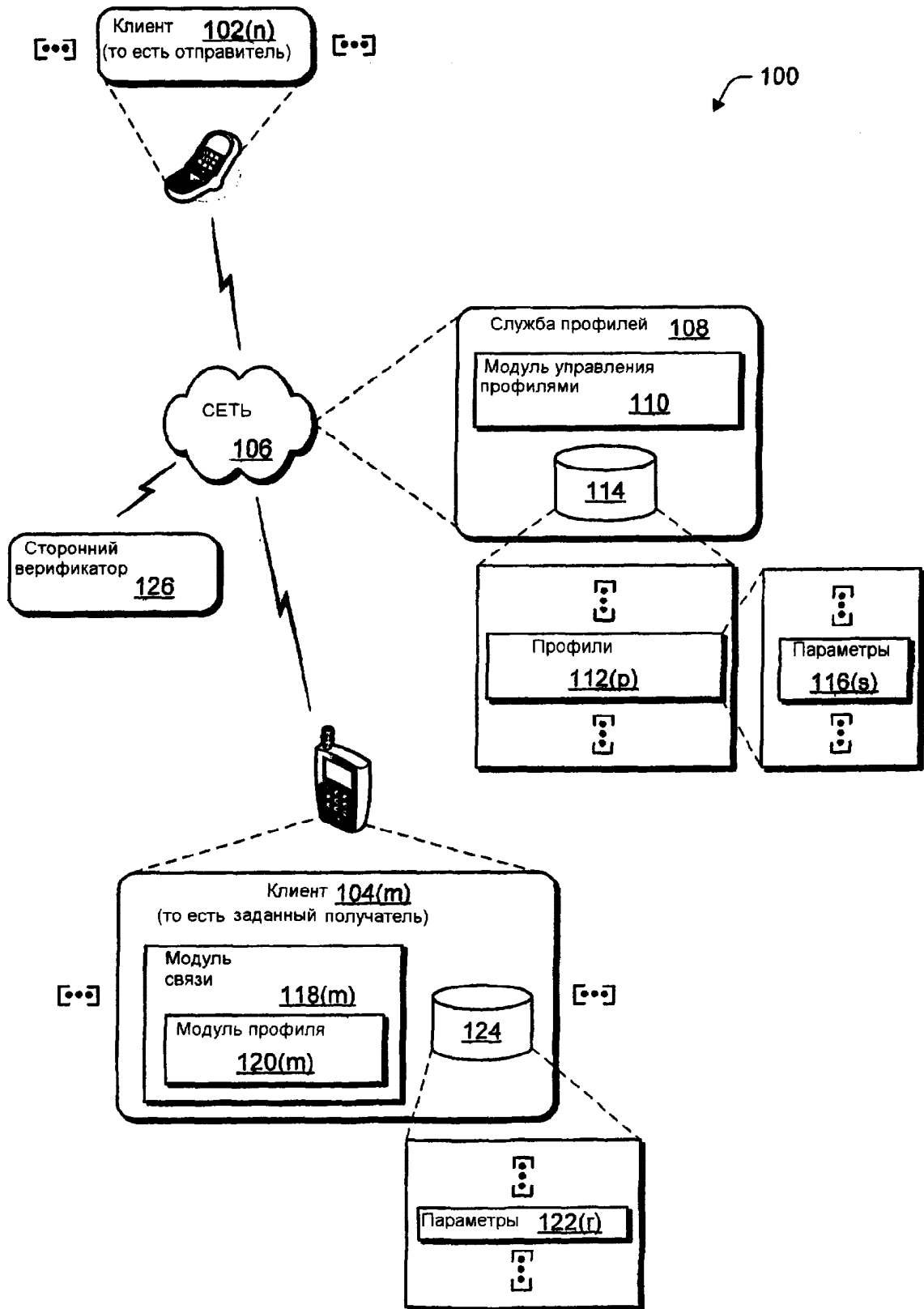
12. Способ по п.8, в котором профиль, указывающий отправителя, конфигурируется для управления посредством идентификатора регистрации, аутентифицированного службой аутентификации, упомянутым получателем по множеству различных поставщиков услуг.

13. Способ по п.8, в котором параметры безопасности предоставляются стороной, отличной от упомянутого отправителя.

14. Способ по п.8, в котором параметры безопасности задают: множество контактов в списке контактов, которым разрешено связываться с пользователем; количество времени, которое пользователю разрешено потратить на связь с одним или более контактами в списке контактов; и время дня, в течение которого разрешается связь с одним или более контактами в списке контактов.

15. Машиночитаемый носитель, содержащий выполняемые компьютером команды, которые при их выполнении предписывают компьютеру выполнять способ управления сообщением передачи речи по Интернет-протоколу (VoIP), содержащий этапы: загружают из сети профиль, который задает параметры безопасности, указывающие меры по обеспечению безопасности для пользователя, когда он связывается с одним или более из множества других пользователей, причем параметры безопасности обеспечиваются стороной, отличной от упомянутого пользователя и упомянутого множества других пользователей, принимают сообщение передачи речи по Интернет-протоколу (VoIP) от пользователя и управляют упомянутым VoIP-сообщением, используя упомянутый профиль, задающий параметры безопасности, причем управление упомянутым VoIP-сообщением посредством выполнения компьютером инструкций дополнительно включает в себя этапы: маршрутизируют VoIP-сообщение к стороннему верификатору, доступному по другому сетевому адресу, который отличается от сетевого адреса, по которому пользователь доступен, и выполняют действие, относящееся к VoIP-сообщению, как задано сторонним верификатором.

16. Носитель по п.15, в котором параметры безопасности задают: множество контактов в списке контактов, которым разрешено связываться с пользователем; количество времени, которое пользователю разрешено потратить на связь с одним или более контактами в списке контактов; и время дня, в течение которого разрешается связь с одним или более контактами в списке контактов.



ФИГ.1

300

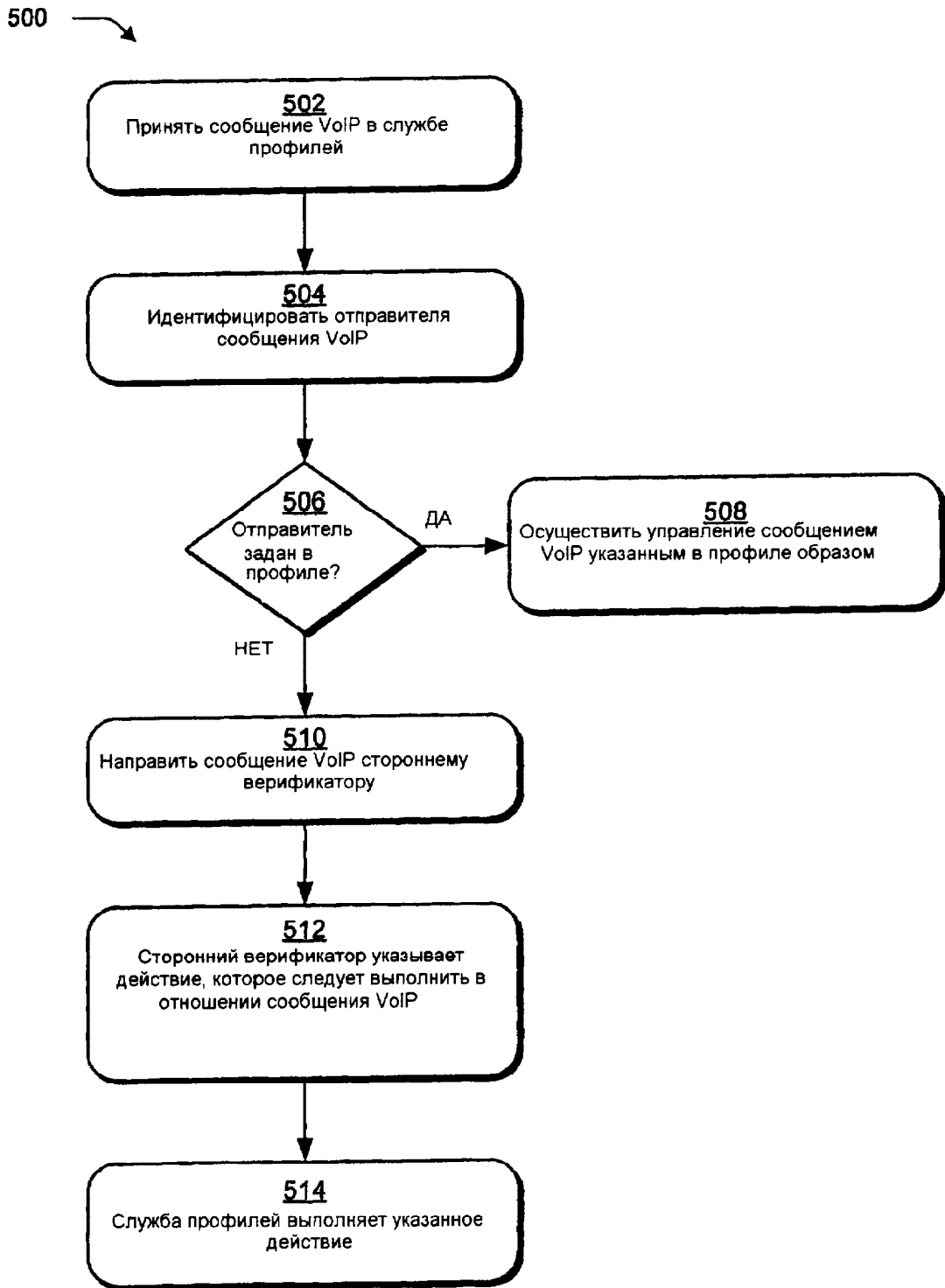


ФИГ.3

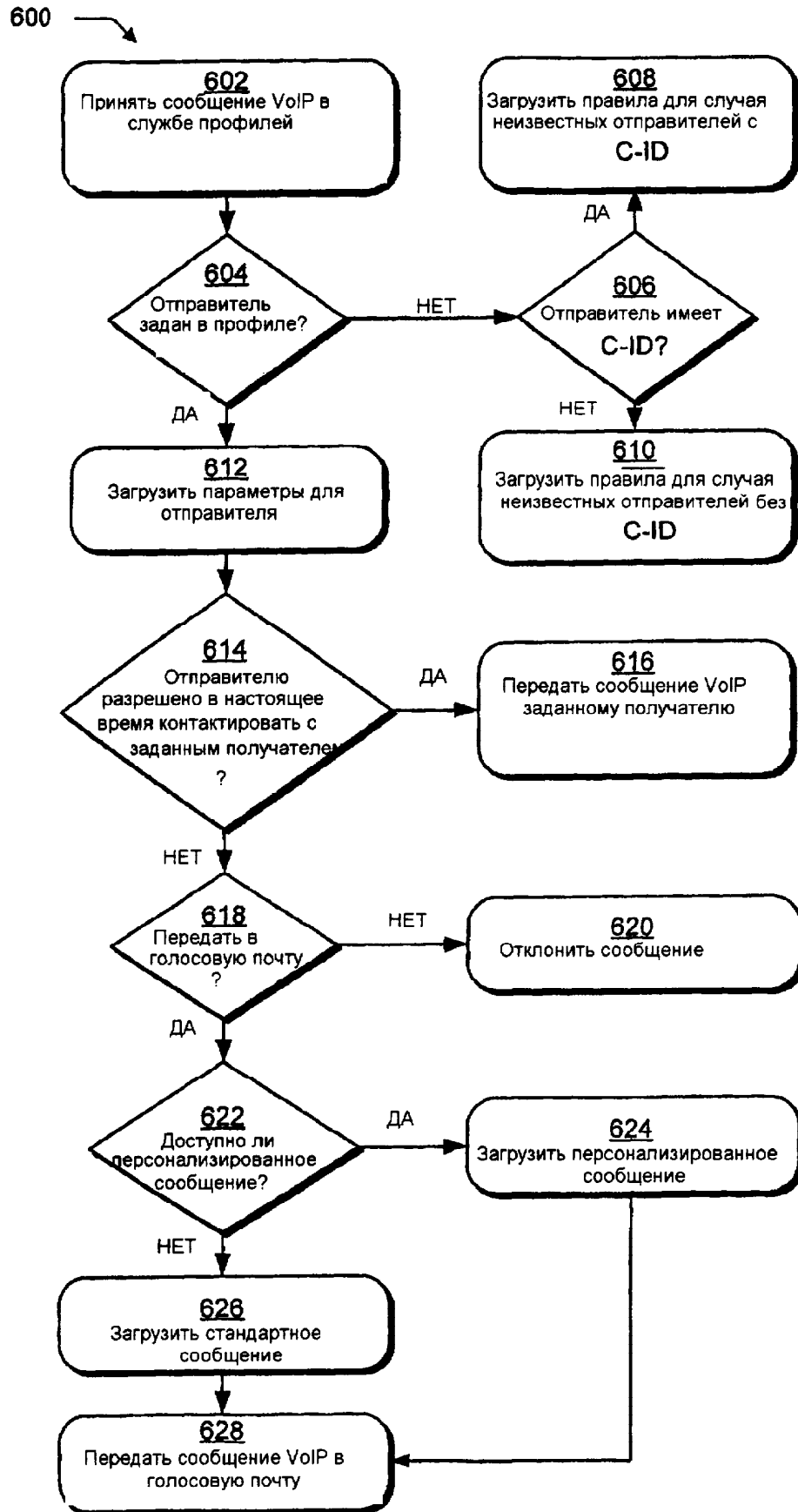
400



ФИГ.4



ФИГ.5



ФИГ.6