РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 419 222** (13) **C2**

(51) МПК
H04L 9/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2007149084/09, 12.05.2006**

(24) Дата начала отсчета срока действия патента:
12.05.2006

Приоритет(ы):
(30) Конвенционный приоритет:
30.06.2005 US 11/172,425

(43) Дата публикации заявки: **10.07.2009** Бюл. № 19

(45) Опубликовано: **20.05.2011** Бюл. № **14**

(56) Список документов, цитированных в отчете о поиске: **US 2004088348 A1, 2004.05.06. US 2004107124 A1, 2004.12.09. WO 2004038565 A2, 2004.05.06. US 2004034773 A1, 2004.02.19. US 2004143738 A1, 2004.07.22. RU 0002178913 C1, 2002.01.27. RU 0002184390 C1, 2002.06.27.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **28.12.2007**

(86) Заявка PCT:
US 2006/018490 (12.05.2006)

(87) Публикация заявки PCT:
WO 2007/005117 (11.01.2007)

Адрес для переписки:
129090, Москва, ул.Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
ШВАРЦ Эйал (US),
ХОЛМС Джон С. (US),
ФОРД Питер С. (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

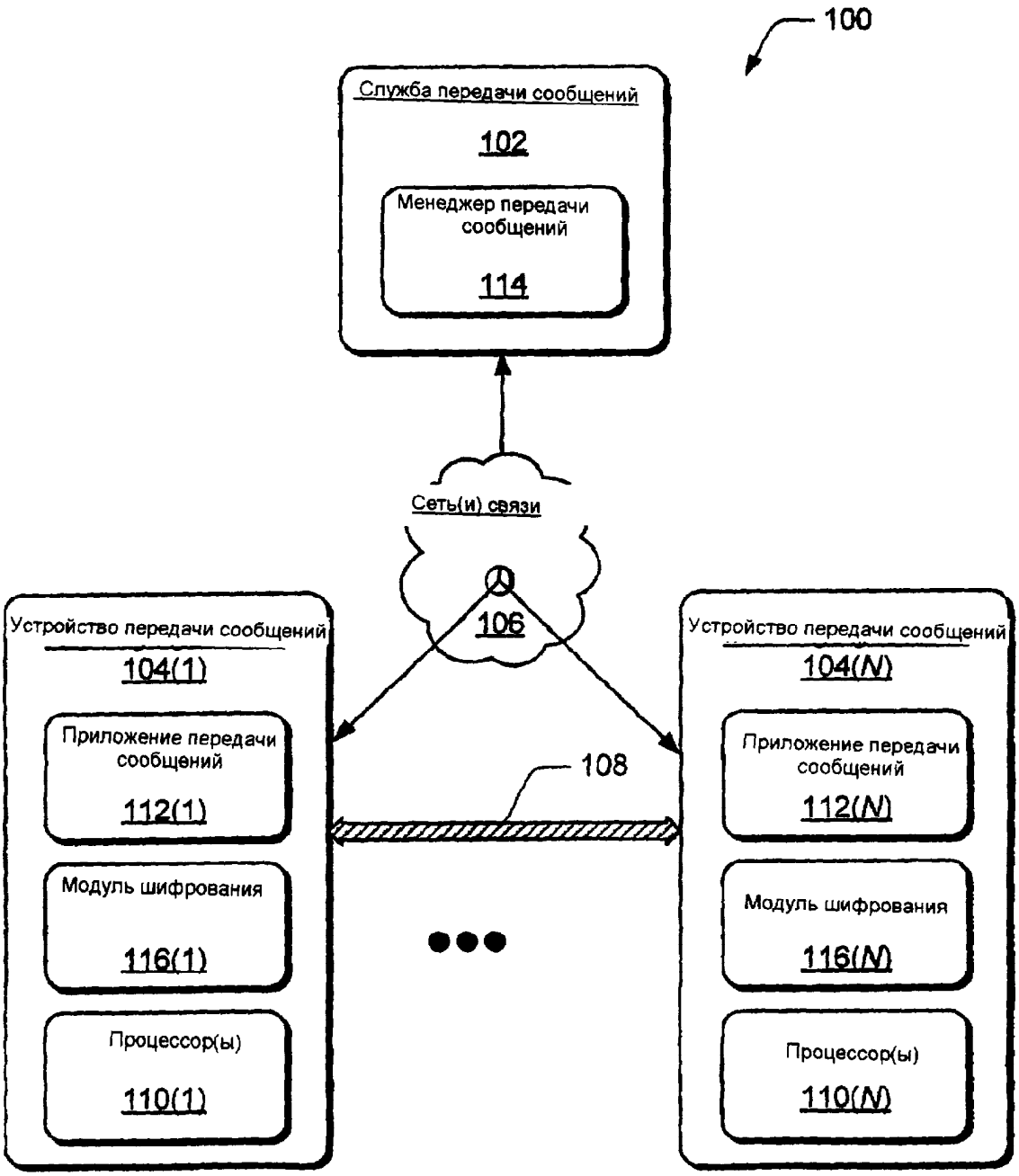
RU 2419222 C2

(54) ЗАЩИЩЕННАЯ МГНОВЕННАЯ ПЕРЕДАЧА СООБЩЕНИЙ

(57) Реферат:

Изобретение относится к радиотехнике, а именно к способу и устройству мгновенной передачи сообщений. Техническим результатом является повышение быстродействия. Технический результат достигается тем, что устройство передачи сообщений шифрует идентификатор вызова, чтобы генерировать зашифрованное сообщение вызова, и передает зашифрованное сообщение вызова через одноранговую линию прямой связи устройству передачи сообщений получателя. Устройство передачи сообщений получателя расшифровывает зашифрованное сообщение вызова и шифрует идентификатор вызова как идентификатор вызова возврата, чтобы генерировать зашифрованный возврат вызова. Устройство передачи сообщений получает зашифрованный возврат вызова от устройства передачи сообщений получателя,

расшифровывает зашифрованный возврат вызова и проверяет, что идентификатор вызова возврата соответствует идентификатору вызова, чтобы установить, что передачи являются защищенными при передаче через одноранговую линию прямой связи. 3 н. и 16 з.п. ф-лы, 7 ил.



ФИГ.1

RU 2419222 C2

RU 2419222 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 419 222** (13) **C2**

(51) Int. Cl.
H04L 9/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2007149084/09, 12.05.2006**

(24) Effective date for property rights:
12.05.2006

Priority:
(30) Priority:
30.06.2005 US 11/172,425

(43) Application published: **10.07.2009** Bull. 19

(45) Date of publication: **20.05.2011 Bull. 14**

(85) Commencement of national phase: **28.12.2007**

(86) PCT application:
US 2006/018490 (12.05.2006)

(87) PCT publication:
WO 2007/005117 (11.01.2007)

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):
ShVARTs Ehjal (US),
KhOLMS Dzhon S. (US),
FORD Piter S. (US)

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

RU 2419222 C2

(54) SECURED INSTANT TRANSFER OF MESSAGES

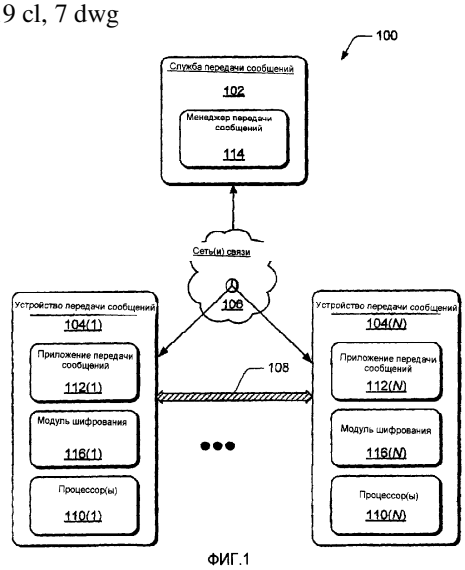
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: device of messages transfer codes a call identifier, to generate a coded call message, and sends the coded call message via a single-range line of direct communication to the device of user's messages communication. The device of user's messages transfer decodes the coded call message and codes the call identifier as an identifier of return call, to generate a coded call return. The device of messages transfer receives the coded call return from the device of user's messages transfer, decodes the coded call return and checks that the call return identifier complies with the call identifier to detect that transfers are secured when sent via a single-range line of direct communication.

EFFECT: improved efficiency.

19 cl, 7 dwg



ФИГ.1

RU 2419222 C2

Область техники, к которой относится изобретение

Мгновенная передача сообщений постоянно увеличивает свою популярность, поскольку пользователи в состоянии осуществлять связь в реальном времени посредством мгновенных сообщений, используя разнообразные устройства, типа компьютеров, беспроводных телефонов, медиа-устройств и т.п. Мгновенная передача сообщений дает возможность двум или более пользователям обмениваться сообщениями через сеть связи во время сеанса мгновенной передачи сообщений. Когда два пользователя находятся в сети в одно и то же время, обмен мгновенными сообщениями между этими двумя пользователями может происходить в реальном времени через соответствующие устройства с поддержкой передачи сообщений. Хотя мгновенные сообщения являются текстовым сеансом связи между этими двумя пользователями, непосредственность обмена сообщениями с помощью мгновенной передачи сообщений подобна участию пользователей в обычном сеансе речевого общения.

Мгновенный обмен сообщениями в реальном времени между двумя (или более) устройствами с поддержкой передачи сообщений может осуществляться через прямую одноранговую линию связи между двумя устройствами с поддержкой передачи сообщений. В альтернативной системе передачи мгновенных сообщений могут маршрутизироваться от устройства клиента на сервер и затем на устройство клиента получателя, в этом случае передачи клиент-сервер и сервер-клиент могут быть защищены. Однако одноранговые передачи данных сеансов мгновенной передачи сообщений не защищены при передаче, при этом нет проверки правильности того, что пользователь, который участвует в сеансе мгновенной передачи сообщений, является фактически тем, кем он себя представляет. Участники мгновенной передачи сообщений подвержены обману и/или раскрытию данных.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Это описание сущности изобретения предоставляется для того, чтобы ввести упрощенные понятия защищенной мгновенной передачи сообщений, которая далее описана в подробном описании. Это описание сущности изобретения не предназначено для того, чтобы идентифицировать основные признаки заявленной сущности изобретения, и при этом оно не предназначено для использования в определении объема формулы изобретения.

В одном варианте воплощения защищенной мгновенной передачи сообщений устройство передачи сообщений шифрует идентификатор вызова для того, чтобы сгенерировать зашифрованное сообщение вызова, и передает зашифрованное сообщение вызова через одноранговую линию связи устройству передачи сообщений получателя. Устройство передачи сообщений получателя расшифровывает зашифрованное сообщение вызова и зашифровывает идентификатор вызова как идентификатор вызова возврата, чтобы сгенерировать зашифрованный возврат вызова. Устройство передачи сообщений принимает зашифрованный возврат вызова от устройства передачи сообщений получателя, расшифровывает зашифрованный возврат вызова и проверяет, что идентификатор вызова возврата соответствует идентификатору вызова, чтобы установить, что связь является защищенной при передаче через одноранговую линию связи.

В другом варианте воплощения защищенной мгновенной передачи сообщений устройство передачи сообщений устанавливает одноранговую линию связи для передачи в реальном времени защищенных передач с устройством передачи сообщений получателя и устанавливает, что зашифрованные передачи защищены при

передаче через одноранговую линию связи с устройством передачи сообщений получателя. Устройство передачи сообщений может затем шифровать передачу, чтобы генерировать зашифрованную передачу, которая содержит политику управления, чтобы ограничивать использование данных передачи, когда принята и расшифрована в устройстве передачи сообщений получателя. Политика управления может определять степень, с которой устройство передачи сообщений получателя, или пользователь в устройстве передачи сообщений получателя, может сохранять данные передачи для будущей ссылки, использовать данные передачи и/или распространять данные передачи после расшифровки. Политика управления может также препятствовать распространению данных передачи наряду с любыми дополнительными данными, связанными с передачей.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Одинаковые ссылочные позиции используются всюду на чертежах для того, чтобы ссылаться на одинаковые признаки и компоненты.

Фиг.1 иллюстрирует примерную систему передачи сообщений, в которой могут быть осуществлены варианты воплощения защищенной мгновенной передачи сообщений.

Фиг.2 иллюстрирует другую примерную систему передачи сообщений, в которой могут быть осуществлены варианты воплощения защищенной мгновенной передачи сообщений и которая содержит компоненты системы передачи сообщений, показанной на фиг.1.

Фиг.3 иллюстрирует другую примерную систему передачи сообщений, в которой могут быть осуществлены варианты воплощения защищенной мгновенной передачи сообщений и которая содержит компоненты систем передачи сообщений, показанных на фиг.1 и 2.

Фиг.4A и 4B иллюстрируют примерный способ для защищенной мгновенной передачи сообщений.

Фиг.5 иллюстрирует другой примерный способ для защищенной мгновенной передачи сообщений.

Фиг.6 иллюстрирует различные компоненты примерного компьютерного устройства, которое может быть осуществлено как одно или более устройств передачи сообщений, которые показаны на фиг.1-3.

Подробное описание

Описана защищенная мгновенная передача сообщений, в которой варианты воплощения обеспечивают способы, чтобы сделать возможными защищенные передачи мгновенной передачи сообщений. Устройство передачи сообщений может установить одноранговую линию связи с устройством передачи сообщений получателя для передачи реального времени защищенных передач типа защищенных мгновенных сообщений. Устройство передачи сообщений может также устанавливать, что зашифрованные передачи типа мгновенных сообщений являются защищенными при передаче через одноранговую линию связи с устройством передачи сообщений получателя.

В одном варианте воплощения используется цифровое управление правами (DRM) для того, чтобы осуществлять защищенную мгновенную передачу сообщений. Цифровое управление правами является протоколом, который был установлен для защиты авторских прав цифровых носителей информации, например для предотвращения незаконного распространения платного содержания по Интернету и предотвращения сетевого пиратства коммерческих выставленных на продажу

продуктов. Цифровое управление правами также обычно используется для того, чтобы шифровать содержание, которое после этого сохраняют в документе. В применении к защищенной мгновенной передаче сообщений цифровой протокол управления правами обеспечивает, по меньшей мере, проверку идентичности, распространения ключа шифрования и интеграцию шифрования для передач реального времени. Дополнительно служба цифрового управления правами, осуществленная с защищенной мгновенной передачей сообщений, обеспечивает то, что идентификационные информации устройств передачи сообщений по сути аутентифицируются. Служба цифрового управления правами выдает лицензии использования и выдачи только известным и аутентифицированным объектам.

Устройство передачи сообщений может устанавливать, что зашифрованные передачи защищены с устройством передачи сообщений получателя посредством сначала шифрования случайно сгенерированного идентификатора вызова, чтобы генерировать зашифрованный вызов. Зашифрованный вызов затем передают на устройство передачи сообщений получателя через одноранговую линию связи, где устройство передачи сообщений получателя расшифровывает вызов. Устройство передачи сообщений получателя шифрует идентификатор вызова в ответе, который затем возвращают на устройство передачи сообщений. Устройство передачи сообщений расшифровывает ответ и проверяет, что полученный идентификатор вызова соответствует идентификатору вызова, который первоначально посылали устройству передачи сообщений получателя. Это устанавливает то, что каждое из устройств передачи сообщений защищено в идентичности других и что передачи могут шифроваться и надежно передаваться через одноранговую линию связи.

В то время как аспекты описанных систем и способов для защищенной мгновенной передачи сообщений могут быть осуществлены в любом количестве различных компьютерных систем, сред и/или конфигураций, варианты воплощения защищенной мгновенной передачи сообщений описаны в контексте следующих примерных системных архитектур.

Фиг.1 иллюстрирует примерную систему 100 передачи сообщений, в которой могут быть осуществлены варианты воплощения защищенной мгновенной передачи сообщений. Система 100 передачи сообщений содержит службу 102 передачи сообщений и любое число устройств 104(1-N) с поддержкой передачи сообщений. Каждое из устройств 104(1-N) передачи сообщений сконфигурировано для связи со службой 102 передачи сообщений через сеть 106 связи типа сети Интранет, Интернет или мобильной сети(ей). Служба 102 передачи сообщений и/или устройства 104(1-N) передачи сообщений может быть осуществлена с любым или комбинацией компонентов, как описано в отношении примерного компьютерного и/или передачи сообщений устройства 600, показанного на фиг.6.

Например, устройство передачи сообщений 104 может быть осуществлено в любом числе вариантов воплощений, чтобы включать в себя компьютерное устройство, мобильное устройство передачи сообщений, устройство прибора, пульт игровой системы, компонент системы развлечения, сотовый телефон, и как любой другой тип устройства передачи сообщений, которое может быть осуществлено в системе передачи сообщений. Устройства 104 (1-N) передачи сообщений могут также представлять логических клиентов, которые могут содержать пользователя в устройстве 104 передачи сообщений, другие устройства и/или программные приложения, которые осуществляют варианты воплощения защищенной мгновенной передачи сообщений.

Сеть(и) 106 связи может быть осуществлена как любая одна или комбинация из глобальной сети (WAN), локальной сети (LAN), беспроводной сети, общественной телефонной сети, интранета и т.п. Хотя показана как единственная сеть связи, сеть(и) 106 может быть осуществлена, используя любой тип топологии сети и любой сетевой протокол связи, и может быть представлена или иначе осуществлена как комбинация двух или более сетей. Цифровая сеть может содержать различные аппаратные и/или беспроводные линии связи, маршрутизаторы, шлюзы, и так далее, для содействия связи между службой 102 передачи сообщений и системами 104(1-N) клиента.

В этом примере устройство 104(1) передачи сообщений и устройство 104(N) передачи сообщений также сконфигурированы для прямой связи через одноранговую сеть 108, через которую устройства 104 (1-N) передачи сообщений могут обмениваться передачами реального времени типа мгновенных сообщений. Одноранговая сеть 108 может быть осуществлена как отдельная и независимая линия связи от сети(ей) 106 связи. Дополнительно одноранговая сеть 108 может быть осуществлена, используя любой тип топологии сети и любой сетевой протокол связи, и может быть представлена или иначе осуществлена как комбинация двух или более сетей.

Каждое из устройств 104(1-N) передачи сообщений содержит один или более процессоров 110(1-N) (например, любой из микропроцессоров, контроллеров, и т.п.), которые обрабатывают различные машинно-исполнимые команды, чтобы управлять работой устройства 104 передачи сообщений, осуществлять связь с другими электронными и компьютерными устройствами и осуществлять варианты воплощения защищенной мгновенной передачи сообщений. Каждое из устройств 104(1-N) передачи сообщений также содержит соответствующее приложение 112(1-N) передачи сообщений, которое является выполнимым на процессоре 110, так что устройство 104(1) передачи сообщений может участвовать в сеансе мгновенной передачи сообщений с другим устройством передачи сообщений типа устройства 104(N) передачи сообщений.

Приложения 112(1-N) передачи сообщений обеспечивают то, что пользователи в каждом из соответствующих устройств 104(1-N) передачи сообщений, участвуя в сеансе мгновенной передачи сообщений, могут осуществлять связь друг с другом посредством мгновенных текстовых сообщений, обмена мультимедиа, голосовой связи, аваторов (например, визуальных представлений) и т.п. Мгновенные сообщения (или другие передачи) обмениваются через одноранговую сеть 108 в реальном времени (или приблизительно реальном времени, поскольку могут быть незначительные задержки в обработке и передаче данных). Мгновенные сообщения обычно передаются в реальном времени, хотя также может использоваться отсроченная доставка, например, посредством регистрации сообщений, когда устройство 104 передачи сообщений находится вне сети или иным образом недоступно.

Служба 102 передачи сообщений содержит менеджер 114 передачи сообщений, который, в некоторых случаях, может быть осуществлен для того, чтобы облегчать сеанс передачи мгновенных сообщений между устройствами 104(1-N) передачи сообщений. В одном варианте осуществления менеджер передачи сообщений может маршрутизировать мгновенные сообщения между устройствами 104(1-N) передачи сообщений, например, когда устройство 104(1) передачи сообщений генерирует мгновенное сообщение для передачи на устройство 104(N) передачи сообщений. Мгновенное сообщение маршрутизируется от устройства 104(1) передачи сообщений через сеть 106 связи менеджеру 114 передачи сообщений, который тогда маршрутизирует мгновенное сообщение на устройство 104(N) передачи сообщений

через сеть 106 связи. Устройство 104(N) передачи сообщений принимает мгновенное сообщение и исполняет приложение 112(N) передачи сообщений для того, чтобы отобразить мгновенное сообщение. Альтернативно мгновенное сообщение может быть передано от устройства 104(1) передачи сообщений напрямую на устройство 104(N) передачи сообщений через одноранговую сеть 108 без использования службы 102 передачи сообщений.

Каждое из устройств 104(1-N) передачи сообщений содержит соответствующий модуль 116(1-N) шифрования для того, чтобы осуществлять варианты воплощения защищенной мгновенной передачи сообщений, как описано далее со ссылкой на примерные системы 200 и 300 передачи сообщений, показанные на фиг.2 и 3. Хотя система 100 передачи сообщений иллюстрирует вариант осуществления защищенной мгновенной передачи сообщений, среда является просто примерной. Признаки защищенной мгновенной передачи сообщений, описанной здесь, независимы от платформы, так что способы мгновенной передачи сообщений могут быть осуществлены на разнообразных коммерческих компьютерных платформах, имеющих разнообразные процессоры, компоненты памяти и различные другие компоненты.

Например, хотя приложение 112 передачи сообщений и модуль 116 шифрования в соответствующем устройстве 104 передачи сообщений, каждое, показаны как независимые приложения, приложение 112 передачи сообщений может быть осуществлено, чтобы содержать модуль 116 шифрования, чтобы формировать многофункциональный компонент устройства 104 передачи сообщений. Дополнительно, хотя каждое из: приложение 112 передачи сообщений и модуль 116 шифрования - в соответствующем устройстве передачи сообщений 104 проиллюстрировано и описано как единственное приложение, сконфигурированное, чтобы осуществлять варианты воплощения защищенной мгновенной передачи сообщений, любое или оба из: приложение 112 передачи сообщений и модуль 116 шифрования - могут быть осуществлены как приложения нескольких компонентов, распределенные каждому для выполнения одной или более функций в устройстве 104 передачи сообщений и/или в системе 100 передачи сообщений.

Фиг.2 иллюстрирует примерную систему 200 передачи сообщений, в которой варианты воплощения защищенной мгновенной передачи сообщений могут быть осуществлены и которая содержит компоненты системы 100 передачи сообщений, показанной на фиг.1. В системе 200 каждое из устройств 104(1-N) передачи сообщений содержит соответствующие приложения 112(1-N) передачи сообщений и модули 116(1-N) шифрования, как описано выше со ссылкой на фиг.1. Дополнительно каждое из устройств 104(1-N) передачи сообщений осуществлено, чтобы передавать и обмениваться передачами реального времени, такими как мгновенные сообщения, через одноранговую сеть 108.

Приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений содержит и/или генерирует различные передачи и данные 202, и, аналогично, приложение 112(N) передачи сообщений содержит и/или генерирует различные передачи и данные 204. В различных вариантах воплощения защищенной мгновенной передачи сообщений, передачи и данные 202, 204, связанные с соответствующими приложениями 112(1-N) передачи сообщений, могут содержать любое одно или комбинацию из: мгновенное сообщение, одноранговую передачу реального времени, передачу файла, передачу изображения, основанную на тексте передачу, передачу аудио, передачу видео, или передачу аудио/видео, любая из которых может быть передана как зашифрованная или иным образом защищенная передача через

одноранговую сеть 108.

В одном варианте воплощения каждый из модулей 116(1-N) шифрования в устройствах 104(1-N) передачи сообщений может содержать соответствующую службу 206(1-N) цифрового управления правами (DRM), которая может использоваться для того, чтобы осуществлять варианты воплощения защищенной мгновенной передачи сообщений. Каждое из устройств 104(1-N) передачи сообщений содержит соответствующую память 208(1-N), чтобы поддерживать контакт(ы) 210(1-N) и данные 212(1-N) шифрования для каждого соответствующего устройства 104(1-N) передачи сообщений. Память 208 может быть осуществлена как любой тип и комбинация машинно-читаемых носителей, как описано со ссылкой на примерное компьютерное и/или передачи сообщений устройство 600, показанное на фиг.6.

Контакт(ы) 210 для конкретного устройства 104 передачи сообщений могут идентифицировать пользователей других устройств 104 передачи сообщений, с которыми пользователь конкретного устройства передачи сообщений осуществляет связь. Например, память 208(1) в устройстве 104(1) передачи сообщений может хранить контакт 210(1), который идентифицирует устройства 104(N) передачи сообщений и/или пользователя в устройстве 104(N) передачи сообщений. Точно так же память 208(N) в устройстве 104(N) передачи сообщений может хранить контакт 210(N), который идентифицирует устройство 104(1) передачи сообщений и/или пользователя в устройстве 104(1) передачи сообщений.

Модуль 116 шифрования в устройстве передачи сообщений (например, устройстве 104(1) передачи сообщений) может быть осуществлен, чтобы подтверждать идентичность устройства передачи сообщений получателя (например, устройства 104(N) передачи сообщений), чтобы устанавливать, что зашифрованные передачи типа мгновенных сообщений являются защищенными, при осуществлении связи через одноранговую сеть 108 с устройством передачи сообщений получателя. В одном варианте воплощения защищенной мгновенной передачи сообщений служба 206 цифрового управления правами используется для того, чтобы шифровать и обмениваться защищенными передачами и мгновенными сообщениями, как описано со ссылкой на фиг.3. Дополнительно служба 206 цифрового управления правами обеспечивает, что идентификационные информации устройств 104(1-N) передачи сообщений аутентифицируются до установления одноранговой линии 108 связи, и выдает лицензии использования и выдачи только известным и аутентифицированным объектам. Другой протокол(ы) управления правами также может аналогично использоваться, чтобы осуществлять варианты воплощения защищенной мгновенной передачи сообщений.

Фиг.3 иллюстрирует примерную систему 300 передачи сообщений, в которой варианты воплощения защищенной мгновенной передачи сообщений могут быть осуществлены и которая содержит компоненты систем 100 и 200 передачи сообщений, показанных на фиг.1 и 2. В системе 300 каждое из устройств 104(1-N) передачи сообщений содержит соответствующие приложения 112(1-N) передачи сообщений и модули 116(1-N) шифрования, как описано выше со ссылкой на фиг.1 и 2. Дополнительно каждое из устройств 104(1-N) передачи сообщений осуществлено, чтобы передавать и обмениваться передачами реального времени типа мгновенных сообщений через одноранговую сеть 108.

В этом примере устройство 104(1) передачи сообщений может проверять идентичность устройства 104(N) передачи сообщений (также упоминаемого здесь как устройство передачи сообщений получателя) и устанавливать, что зашифрованные

передачи 202 являются защищенными, когда они передаются от устройства 104(1) передачи сообщений на устройство 104(N) передачи сообщений получателя через одноранговую сеть 108. В альтернативном варианте воплощения служба 206 цифрового управления правами обеспечивает, что идентичность устройств 104(1-N) передачи сообщений, в сущности, аутентифицируется для защищенных передач мгновенной передачи сообщений.

Модуль 116(1) шифрования в устройстве 104(1) передачи сообщений может шифровать случайно сгенерированный идентификатор 302 вызова, чтобы генерировать зашифрованное сообщение 308 вызова. В одном варианте воплощения, которое использует службу 206 цифрового управления правами, модуль 116(1) шифрования в устройстве 104(1) передачи сообщений может шифровать случайно сгенерированный идентификатор 302 вызова с ключом шифрования 304, который внедрен в лицензию 306 выдачи службы 206(1) цифрового управления правами, чтобы генерировать зашифрованное сообщение 308 вызова. В одном варианте воплощения защищенной мгновенной передачи сообщений ключ 304 шифрования может быть осуществлен как "самодоверительный" ключ, чтобы устанавливать самодоверительную одноранговую систему для передачи сообщений между устройствами 104(1-N) передачи сообщений.

Приложение 112(1) передачи сообщений устройства 104(1) передачи сообщений передает 310 зашифрованное сообщение 308 вызова к приложению 112(N) передачи сообщений в устройстве 104(N) передачи сообщений получателя через одноранговую сеть 108. Модуль 116(N) шифрования в устройстве 104(N) передачи сообщений расшифровывает вызов (то есть зашифрованное сообщение 308 вызова) и, в ответ, зашифровывает идентификатор вызова как идентификатор 312 вызова возврата, чтобы сгенерировать зашифрованный возврат вызова 314. В одном варианте воплощения, который использует службу 206 цифрового управления правами, идентификатор 312 вызова возврата зашифрован с ключом 316 шифрования, который внедрен в собственную версию лицензии 318 выдачи устройства передачи сообщений получателя службы 206(N) цифрового управления правами.

Приложение 112(N) передачи сообщений устройства 104(N) передачи сообщений передает 320 зашифрованный возврат 314 вызова к приложению 112(1) передачи сообщений в устройстве 104(1) передачи сообщений через одноранговую сеть 108. Модуль 116(1) шифрования устройства 104(1) передачи сообщений может расшифровывать ответ (то есть зашифрованный возврат 314 вызова) и проверять, что принятый идентификатор вызова (то есть идентификатор 312 вызова возврата) соответствует идентификатору 302 вызова, который первоначально посылали устройству 104(N) передачи сообщений. Это устанавливает, что каждое из устройств 104(1-N) передачи сообщений защищено в идентичности других и что мгновенные сообщения могут шифроваться и защищенно передаваться через одноранговую сеть 108.

Устройство 104(1) передачи сообщений может теперь доверять устройству 104(N) передачи сообщений, которое в состоянии расшифровывать сообщения, посланные напрямую через одноранговую сеть 108, может расшифровывать сообщения, принятые напрямую от устройства 104(N) передачи сообщений через одноранговую сеть 108 и может доверять установленной идентификационной информации устройства 104(N) передачи сообщений и/или пользователя в устройстве 104(N) передачи сообщений. Устройство 104(1) передачи сообщений может также утверждать, что зашифрованные сообщения, посланные напрямую устройству 104(N) передачи

сообщений, могут быть расшифрованы только в устройстве 104(N) передачи сообщений. Устройство 104(N) передачи сообщений может инициировать ту же самую последовательность проверки достоверности, как описано выше, чтобы гарантировать идентичность устройства 104(1) передачи сообщений, и извлечь лицензию использования, чтобы расшифровывать будущие передачи от устройства 104(1) передачи сообщений.

Например, приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений может генерировать мгновенное сообщение 202 для передачи на устройство 104(N) передачи сообщений. Модуль 116(1) шифрования может зашифровывать мгновенное сообщение 202 с ключом 304 шифрования, внедренным в лицензию 306 выдачи, которая связана с устройством 104(N) передачи сообщений, чтобы сгенерировать зашифрованную передачу. Приложение 112(1) передачи сообщений может затем передать зашифрованную передачу на устройство 104(N) передачи сообщений получателя через одноранговую сеть 108.

Служба 206 цифрового управления правами, связанная с модулем 116 шифрования в устройстве 104 передачи сообщений, может содержать политики 322 управления (также упоминаемые «права использования»), такие как политики 322(1-N) управления в соответствующих устройствах 104(1-N) передачи сообщений. Политики 322(1-N) управления могут определять степень, с которой устройство передачи сообщений получателя или пользователь устройства передачи сообщений получателя, может хранить данные передачи для ссылки в будущем, использовать данные передачи и/или распространять данные передачи, после расшифровки. Политика 322 управления может также препятствовать распространению и/или использованию данных передачи наряду с любыми дополнительными данными, связанными с передачей.

Например, устройство 104(1) передачи сообщений может шифровать мгновенное сообщение 202, чтобы генерировать зашифрованное мгновенное сообщение, которое содержит политику 322(1) управления, чтобы ограничивать использование мгновенного сообщения, принятого и расшифрованного в устройстве 104(N) передачи сообщений получателя. Использование мгновенного сообщения может быть ограничено в том, что устройство 104(N) передачи сообщений получателя не может сохранять данные сообщения вне сети, не может сохранять изображения экрана сообщения или копировать и вставлять содержание сообщения. Политика 322(1) управления может также ограничивать просмотр сообщения и/или чтобы для сообщения истекал срок действия через некоторый промежуток времени и оно было стерто.

Способы для защищенной мгновенной передачи сообщений типа примерных способов 400 и 500, описанных со ссылкой на соответствующие фиг.4А и 4В и 5, могут быть описаны в общем контексте машинно-исполнимых команд. Вообще машинно-исполнимые команды могут содержать подпрограммы, программы, объекты, компоненты, структуры данных, процедуры, модули, функции и т.п., которые выполняют конкретные функции или реализуют конкретные абстрактные типы данных. Способы могут также применяться в распределенной компьютерной среде, где функции выполняются удаленными устройствами обработки, которые связаны через сеть связи. В распределенной компьютерной среде компьютерные выполнимые команды могут быть расположены как в локальных, так и в удаленных компьютерных носителях хранения, включая запоминающие устройства памяти.

Фиг.4А и 4В иллюстрируют примерный способ 400 для защищенной мгновенной передачи сообщений. Порядок, в котором описан способ, не предназначен для того,

чтобы рассматриваться как ограничение, и любое число описанных блоков способа может быть скомбинировано в любом порядке для осуществления способа. Кроме того, способ может быть осуществлен в любых подходящих аппаратных средствах, программном обеспечении, встроенном программном обеспечении или комбинации этого.

На этапе 402 (фиг.4A) идентификатор вызова случайно генерируется и на этапе 404 идентификатор вызова сохраняется в памяти. Например, модуль 116(1) шифрования в устройстве 104(1) передачи сообщений случайно генерирует идентификатор 302 вызова, который может быть сохранен в памяти 208(1) как данные 212(1) шифрования. На этапе 406 идентификатор вызова шифруется, чтобы сгенерировать зашифрованное сообщение вызова. Например, модуль 116(1) шифрования в устройстве 104(1) передачи сообщений шифрует случайно сгенерированный идентификатор 302 вызова, чтобы сгенерировать зашифрованное сообщение 308 вызова. В одном варианте воплощения идентификатор 302 вызова может шифроваться с ключом 304 шифрования, который внедрен в лицензию 306 выдачи службы 206(1) цифрового управления правами, чтобы сгенерировать зашифрованное сообщение 308 вызова.

На этапе 408 лицензия выдачи ассоциируется с устройством передачи сообщений получателя, и на этапе 410 лицензия выдачи сохраняется в памяти, чтобы шифровать передачи, предназначенные для получателя. Например, лицензия 306 выдачи в устройстве 104(1) передачи сообщений связывается с устройством 104(N) передачи сообщений и сохраняется в памяти 208(1) для будущей ссылки. На этапе 412 шифрованное сообщение вызова передается через одноранговую линию связи на устройство передачи сообщений получателя. Например, приложение 112(1) передачи сообщений устройства 104(1) передачи сообщений передает 310 зашифрованное сообщение 308 вызова приложению 112(N) передачи сообщений в устройстве 104(N) передачи сообщений получателя через одноранговую линию 108 связи.

На этапе 414 расшифровывают зашифрованное сообщение вызова. Например, модуль 116(N) шифрования в устройстве 104(N) передачи сообщений получателя расшифровывает зашифрованное сообщение 308 вызова. В одном варианте воплощения устройство 104(N) передачи сообщений получателя расшифровывает зашифрованное сообщение 308 вызова с помощью лицензии использования, которая соответствует лицензии выдачи и которая получена от службы 206(N) цифрового управления правами. На этапе 416 идентификатор вызова шифруется как идентификатор вызова возврата, чтобы сгенерировать возврат зашифрованного вызова. Например, модуль 116(N) шифрования в устройстве 104(N) передачи сообщений шифрует идентификатор вызова как идентификатор 312 вызова возврата, чтобы сгенерировать зашифрованный возврат 314 вызова. В одном варианте воплощения идентификатор 312 вызова возврата может шифроваться с ключом 316 шифрования, который внедрен в собственную версию лицензии 318 выдачи устройства передачи сообщений получателя службы 206(N) цифрового управления правами.

На этапе 418 (фиг.4B) зашифрованный возврат вызова принимается от устройства передачи сообщений получателя. Например, приложение 112(1) передачи сообщений устройства 104(1) передачи сообщений принимает зашифрованный возврат 314 вызова от приложения 112(N) передачи сообщений устройства 104(N) передачи сообщений через одноранговую линию 108 связи. На этапе 420 расшифровывают зашифрованный возврат вызова. Например, модуль 116(1) шифрования устройства 104(1) передачи сообщений расшифровывает зашифрованный возврат 314 вызова, который принят 320

от устройства 104(N) передачи сообщений получателя.

На этапе 422 лицензия использования, соответствующая лицензии выдачи, получается, чтобы расшифровывать передачи, принятые от устройства передачи сообщений получателя. Например, лицензия использования, соответствующая лицензии 318 выдачи, принятой от устройства 104(N) передачи сообщений получателя, получается и сохраняется в памяти 208(1) в устройстве 104(1) передачи сообщений, чтобы расшифровывать будущие передачи, полученные от устройства 104(N) передачи сообщений. На этапе 424 идентификатор вызова возврата проверяется, чтобы соответствовать идентификатору вызова, чтобы установить, что передачи являются защищенными, когда передаются через одноранговую линию связи. Например, модуль 116(1) шифрования устройства 104(1) передачи сообщений проверяет, что идентификатор 312 вызова возврата соответствует идентификатору 302 вызова, который первоначально посылали устройству 104(N) передачи сообщений.

На этапе 426 коммуникацию зашифровывают с лицензией выдачи, связанной с устройством передачи сообщений получателя, чтобы сгенерировать зашифрованную передачу. Например, приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений может генерировать мгновенное сообщение 202 для передачи устройству 104(N) передачи сообщений. На этапе 428 зашифрованная коммуникация передается через одноранговую линию связи на устройство передачи сообщений получателя для передачи реального времени. Например, приложение 112(1) передачи сообщений передает зашифрованную передачу на устройство 104(N) передачи сообщений получателя через одноранговую сеть 108 для передачи (по существу), реального времени. Защищенная передача, переданная через одноранговую линию связи, может содержать любое одно или комбинацию из: мгновенное сообщение, одноранговую передачу реального времени, передачу файла, передачу изображения, основанную на тексте передачу, передачу аудио, передачу видео, или передачу аудио/видео.

На этапе 430 зашифрованная передача принимается от устройства передачи сообщений получателя через одноранговую линию связи. Например, приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений принимает зашифрованную передачу 204 от устройства 104(N) передачи сообщений через одноранговую линию 108 связи. На этапе 432 зашифрованная передача расшифровывается с лицензией использования, соответствующей лицензии выдачи, принятой от устройства передачи сообщений получателя с зашифрованным возвратом вызова. Например, модуль 116(1) шифрования расшифровывает зашифрованную передачу с лицензией пользования, которая соответствует лицензии 318 выдачи, которая принята от устройства 104(N) передачи сообщений.

Фиг.5 иллюстрирует примерный способ 500 для защищенной мгновенной передачи сообщений. Порядок, в котором способ описан, не предназначен для того, чтобы рассматриваться как ограничение, и любое число описанных этапов способа может быть скомбинировано в любом порядке для осуществления способа. Кроме того, способ может быть осуществлен в любых подходящих аппаратных средствах, программном обеспечении, встроенном программном обеспечении или комбинации этого.

На этапе 502 одноранговая линия связи устанавливается для передачи реального времени защищенной передачи с устройством передачи сообщений получателя. Например, приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений устанавливает одноранговую линию 108 связи для передачи (по существу)

реального времени защищенной передачи 204 (например, мгновенных сообщений). На этапе 504 зашифрованные передачи устанавливаются, чтобы быть защищенными при передаче через одноранговую линию связи с устройством передачи сообщений получателя. Это описано со ссылкой на фиг.4A и 4B.

На этапе 506 передача шифруется, чтобы содержать политику управления, чтобы ограничивать распространение и/или использование данных передачи, когда принята в устройстве передачи сообщений получателя. Например, приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений может шифровать мгновенное сообщение 202, чтобы генерировать зашифрованное мгновенное сообщение, которое содержит политику 322(1) управления, чтобы ограничивать распространение и/или использование мгновенного сообщения, когда принято и расшифровано в устройстве 104(N) передачи сообщений получателя.

В этом примере передача может содержать любое одно или комбинацию из: мгновенное сообщение, одноранговую передачу реального времени, передачу файла, передачу изображения, основанную на тексте передачу, передачу аудио, передачу видео или передачу аудио/видео. Политика управления может определять степень, до которой устройство передачи сообщений получателя, или пользователь в устройстве передачи сообщений получателя, может поддерживать данные передачи для будущей ссылки, использовать и/или распространять данные передачи после расшифровки. Политика управления может также препятствовать распространению данных передачи наряду с любыми дополнительными данными, связанными с передачей, и может назначать, чтобы приложение связи в устройстве передачи сообщений получателя проверялось на достоверность службой цифрового управления правами, чтобы принимать и расшифровывать зашифрованную передачу.

На этапе 508 зашифрованная передача передается через одноранговую линию связи на устройство передачи сообщений получателя. Например, приложение 112(1) передачи сообщений в устройстве 104(1) передачи сообщений может генерировать мгновенное сообщение 202, имеющее политику 322 управления для передачи устройству 104(N) передачи сообщений. В одном варианте воплощения модуль 116(1) шифрования может шифровать мгновенное сообщение 202 с лицензией 306 выдачи, которая связана с устройством 104(N) передачи сообщений, чтобы генерировать зашифрованную передачу. Приложение 112(1) передачи сообщений может тогда передавать зашифрованную передачу на устройство 104(N) передачи сообщений получателя через одноранговую сеть 108.

Фиг.6 иллюстрирует различные компоненты примерного компьютерного и/или передачи сообщений устройства 600, в котором могут быть осуществлены варианты воплощения защищенной мгновенной передачи сообщений. Дополнительно компьютерное и/или передачи сообщений устройство 600 может быть осуществлено как любое одно или более устройств 104(1-N) передачи сообщений, описанных со ссылкой на фиг.1-5.

Компьютерное и/или передачи сообщений устройство 600 содержит один или более входов 602 медиасодержания, которые могут содержать входы интернет протокола (IP), по которым потоки медиасодержания принимаются через сеть на основе IP, интранет или Интернет. Устройство 600 дополнительно содержит интерфейс(ы) 604 связи, который может быть осуществлен как любое одно или более из: последовательный и/или параллельный интерфейс, беспроводной интерфейс, любой тип сетевого интерфейса, модем, - и как любой другой тип интерфейса связи. Беспроводный интерфейс позволяет устройству 600 принимать команды ввода

управления и другую информацию от устройства ввода данных, например от устройства дистанционного управления, PDA (личного цифрового помощника), сотового телефона или от другого инфракрасного (IR), 802.11, Bluetooth, или подобного устройства RF ввода данных.

Сетевой интерфейс обеспечивает соединение между компьютерным и/или передачи сообщений устройством 600 и сетью связи (например, сетями 106 связи или одноранговой сетью 108), посредством которой другие электронные, компьютерные, и передающие устройства могут осуществлять связь с устройством 600. Точно так же последовательный и/или параллельный интерфейс обеспечивает передачу данных напрямую между устройством 600 и другим электронным, компьютерным, и/или передачи сообщений устройством. Модем обеспечивает связь устройства 600 с другими электронными и компьютерными устройствами через обычную телефонную линию, соединение DSL, кабель и/или другой тип соединения.

Компьютерное и/или передачи сообщений устройство 600 также содержит один или более процессоров 608 (например, любой из микропроцессоров, контроллеров и т.п.), которые обрабатывают различные машинно-исполнимые команды, чтобы управлять работой устройства 600, осуществлять связь с другими электронными и компьютерными устройствами и осуществлять варианты воплощения защищенной мгновенной передачи сообщений. Устройство 600 может быть осуществлено с машинно-читаемыми носителями 610, такими как один или более компонентов памяти, примеры которых содержат оперативную память (RAM), энергонезависимую память (например, одно или более постоянных запоминающих устройств (ROM), флэш-память, EPROM, EEPROM, и т.д.) и дисковое устройство памяти. Дисковое устройство памяти может содержать любой тип магнитного или оптического запоминающего устройства, накопителя на жестких дисках, записываемый и/или перезаписываемый компакт-диск (CD), DVD, DVD+RW и т.п.

Машинно-читаемые носители 610 обеспечивают механизмы хранения данных, чтобы хранить различную информацию и/или данные, такие как приложения и любые другие типы информации и данных, связанных с операционными аспектами компьютерного и/или передачи сообщений устройства 600. Например, операционная система 612 и/или другие прикладные программы 614 могут поддерживаться как программные приложения с помощью машинно-читаемых носителей 610 и выполняться на процессоре(ах) 608, чтобы осуществлять варианты воплощения защищенной мгновенной передачи сообщений. Например, при осуществлении как устройства передачи сообщений (например, любое из устройств 104(1-N) передачи сообщений) машинно-читаемые носители 610 хранят приложение 112 передачи сообщений и модуль 116 шифрования, чтобы осуществлять варианты воплощения защищенной мгновенной передачи сообщений.

Компьютерное и/или передачи сообщений устройство 600 также содержит аудио- и/или видеовыход 616, который предоставляет аудио- и видеосистеме воспроизведения звука и/или отображения, которая может быть внешней или интегрированной с устройством 600, или другим устройствам, которые обрабатывают, отображают, и/или иначе воспроизводят аудио-, видео- и данные отображения. Видеосигналы и аудиосигналы могут передаваться от устройства 600 к устройству отображения через RF (радиочастотную) линию связи, линию связи S-видео, линию полного видеосигнала, линию раздельного видеосигнала, аналоговое звуковое соединение или другую подобную линию связи. Хотя не показано, пользователь может осуществлять связь с устройством 600 через любое число различных устройств ввода данных, таких

как клавиатура и указательное устройство (например, "мышь"). Другие устройства ввода данных могут содержать микрофон, джойстик, игровую клавиатуру, контроллер, последовательный порт, сканер и/или любой другой тип устройства ввода данных, которое облегчает мгновенную передачу сообщений.

Хотя варианты воплощения защищенной мгновенной передачи сообщений были описаны на языке, конкретном для структурных признаков и/или способов, необходимо понимать, что сущность приложенной формулы изобретения не обязательно ограничена конкретными описанными признаками или способами. Скорее конкретные признаки и способы раскрыты как примерные варианты осуществления защищенной мгновенной передачи сообщений.

Формула изобретения

1. Способ мгновенной передачи сообщений, содержащий этапы, на которых:

шифруют идентификатор вызова, чтобы генерировать зашифрованное сообщение вызова;

передают зашифрованное сообщение вызова через одноранговую линию прямой связи устройству передачи сообщений получателя, которое расшифровывает зашифрованное сообщение вызова и зашифровывает идентификатор вызова как идентификатор вызова возврата, чтобы сгенерировать зашифрованный возврат вызова;

получают зашифрованный возврат вызова от устройства передачи сообщений получателя;

расшифровывают зашифрованный возврат вызова; и

проверяют, что идентификатор вызова возврата соответствует идентификатору вызова, чтобы установить, что передачи являются защищенными при передаче через одноранговую линию прямой связи.

2. Способ по п.1, дополнительно содержащий этапы, на которых:

генерируют случайным образом идентификатор вызова; и

сохраняют идентификатор вызова в памяти.

3. Способ по п.1, дополнительно содержащий этапы, на которых:

ассоциируют лицензию выдачи с устройством передачи сообщений получателя; и

сохраняют лицензию выдачи в памяти для того, чтобы шифровать передачи, предназначенные для устройства передачи сообщений получателя.

4. Способ по п.1, дополнительно содержащий этапы, на которых:

ассоциируют лицензию выдачи с устройством передачи сообщений получателя;

получают лицензию использования, соответствующую лицензии выдачи; и

сохраняют лицензию использования, чтобы расшифровывать передачи, принятые от устройства передачи сообщений получателя.

5. Способ по п.1, дополнительно содержащий этапы, на которых:

генерируют передачу устройству передачи сообщений получателя;

шифруют передачу с помощью ключа шифрования, внедренного в лицензию выдачи, связанную с устройством передачи сообщений получателя, чтобы сгенерировать зашифрованную передачу; и

передают зашифрованную передачу через одноранговую линию прямой связи устройству передачи сообщений получателя, которое расшифровывает зашифрованную передачу.

6. Способ по п.1, дополнительно содержащий этапы, на которых:

принимают зашифрованную передачу от устройства передачи сообщений

получателя через одноранговую линию прямой связи; и

расшифровывают зашифрованную передачу с лицензией использования, которая соответствует лицензии выдачи, которая связана с устройством передачи сообщений получателя.

7. Способ по п.1, в котором защищенные передачи, переданные через одноранговую линию прямой связи, содержат мгновенные сообщения.

8. Способ по п.1, в котором защищенные передачи, переданные через одноранговую линию прямой связи, содержат одноранговые передачи, по существу, реального времени.

9. Способ по п.1, в котором защищенные передачи, переданные через одноранговую линию прямой связи, содержат, по меньшей мере, одно из:

мгновенное сообщение, передачу файла, передачу изображения, основанную на тексте передачу, передачу аудио, передачу видео, или передачу аудио/видео.

10. Система мгновенной передачи сообщений, содержащая:

одноранговую линию прямой связи; и

первое устройство передачи сообщений, сконфигурированное, чтобы устанавливать, что зашифрованные мгновенные сообщения защищены, когда передаются от первого устройства передачи сообщений на второе устройство передачи сообщений через одноранговую линию прямой связи;

причем первое устройство передачи сообщений дополнительно сконфигурировано, чтобы шифровать идентификатор вызова, чтобы генерировать зашифрованный вызов, и передавать зашифрованный вызов через одноранговую линию прямой связи второму устройству передачи сообщений;

второе устройство передачи сообщений сконфигурировано, чтобы расшифровывать зашифрованный вызов, шифровать идентификатор вызова как идентификатор вызова возврата, чтобы генерировать зашифрованный возврат вызова, и передавать зашифрованный возврат вызова через одноранговую линию прямой связи первому устройству передачи сообщений; и

первое устройство передачи сообщений дополнительно сконфигурировано, чтобы расшифровывать зашифрованный возврат вызова и проверять, что идентификатор вызова возврата соответствует идентификатору вызова, чтобы устанавливать, что зашифрованные мгновенные сообщения защищены, когда передаются через одноранговую линию прямой связи.

11. Система мгновенной передачи сообщений по п.10, в которой первое устройство передачи сообщений дополнительно сконфигурировано, чтобы устанавливать, что зашифрованные передачи защищены, когда передаются через одноранговую линию прямой связи, причем зашифрованные передачи содержат, по меньшей мере, одно из: передачу файла, передачу изображения, основанную на тексте передачу, передачу аудио, передачу видео или передачу аудио/видео.

12. Система мгновенной передачи сообщений по п.10, в которой второе устройство передачи сообщений сконфигурировано, чтобы устанавливать, что зашифрованные мгновенные сообщения защищены, когда передаются от второго устройства передачи сообщений на первое устройство передачи сообщений через одноранговую линию прямой связи.

13. Система мгновенной передачи сообщений по п.10, в которой первое устройство передачи сообщений дополнительно сконфигурировано для:

шифрования идентификатора вызова с помощью ключа шифрования, внедренного в лицензию выдачи, связанную со вторым устройством передачи сообщений, чтобы

генерировать зашифрованный вызов;

получения лицензии использования, соответствующей лицензии выдачи; и

расшифровки зашифрованного возврата вызова с лицензией использования.

14. Система мгновенной передачи сообщений по п.10, в которой первое устройство передачи сообщений дополнительно сконфигурировано, чтобы случайным образом генерировать идентификатор вызова.

15. Система мгновенной передачи сообщений по п.10, в которой первое устройство передачи сообщений дополнительно сконфигурировано для:

ассоциации лицензии выдачи со вторым устройством передачи сообщений;

поддержки лицензии выдачи, чтобы шифровать мгновенные сообщения;

шифрования мгновенного сообщения с помощью ключа шифрования, внедренного в лицензию выдачи, чтобы генерировать зашифрованное мгновенное сообщение; и

передачи зашифрованного мгновенного сообщения на второе устройство передачи сообщений через одноранговую линию прямой связи.

16. Система мгновенной передачи сообщений по п.10, в которой первое устройство передачи сообщений дополнительно сконфигурировано для:

получения лицензии использования, соответствующей лицензии выдачи, которая связана со вторым устройством передачи сообщений;

поддержки лицензии использования, чтобы расшифровывать зашифрованные мгновенные сообщения;

приема зашифрованного мгновенного сообщения от второго устройства передачи сообщений через одноранговую линию прямой связи; и

расшифровки зашифрованного мгновенного сообщения с лицензией использования.

17. Машиночитаемый носитель, содержащий машиноисполняемые инструкции, сохраненные на нем, при считывании которых компьютером осуществляется способ согласно п.1.

18. Машиночитаемый носитель по п.17, дополнительно содержащий машиноисполняемые инструкции, которые, при выполнении, направляют устройство мгновенной передачи сообщений, чтобы:

ассоциировать лицензию выдачи с устройством передачи сообщений получателя;

поддерживать лицензию выдачи, чтобы шифровать мгновенные сообщения, предназначенные для устройства передачи сообщений получателя;

получать лицензию использования, соответствующую лицензии выдачи; и

поддерживать лицензию использования, чтобы расшифровывать мгновенные сообщения, принятые от устройства передачи сообщений получателя.

19. Машиночитаемый носитель по п.17, дополнительно содержащий машиноисполняемые инструкции, которые, при выполнении, направляют устройство мгновенной передачи сообщений, чтобы:

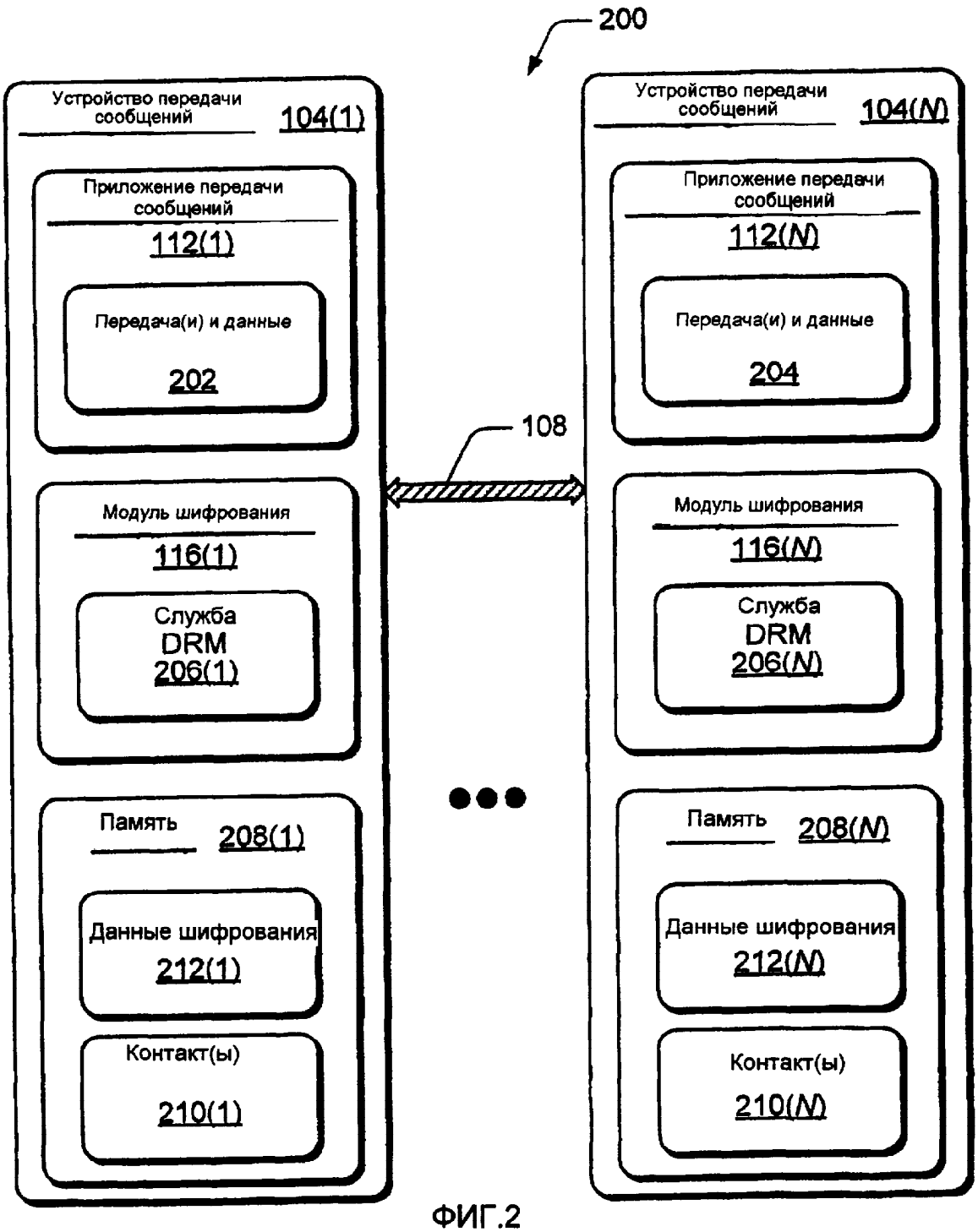
генерировать мгновенное сообщение для передачи на устройство передачи сообщений получателя;

шифровать мгновенное сообщение с помощью ключа шифрования, внедренного в лицензию выдачи, которая связана с устройством передачи сообщений получателя, чтобы генерировать зашифрованное мгновенное сообщение;

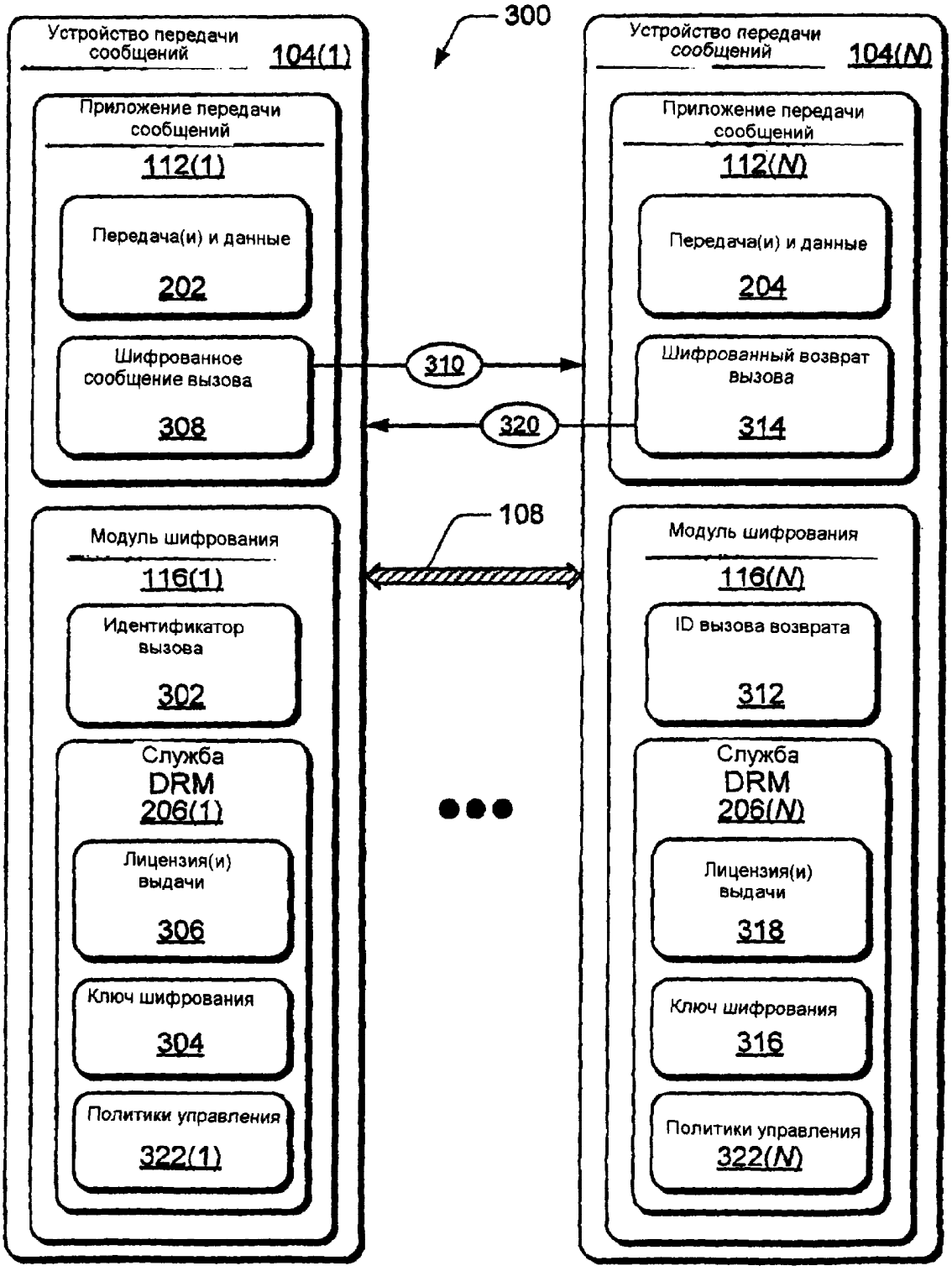
передавать зашифрованное мгновенное сообщение как защищенную передачу на устройство передачи сообщений получателя через одноранговую линию прямой связи;

принимать второе зашифрованное мгновенное сообщение как защищенную передачу от устройства передачи сообщений получателя через одноранговую линию прямой связи; и

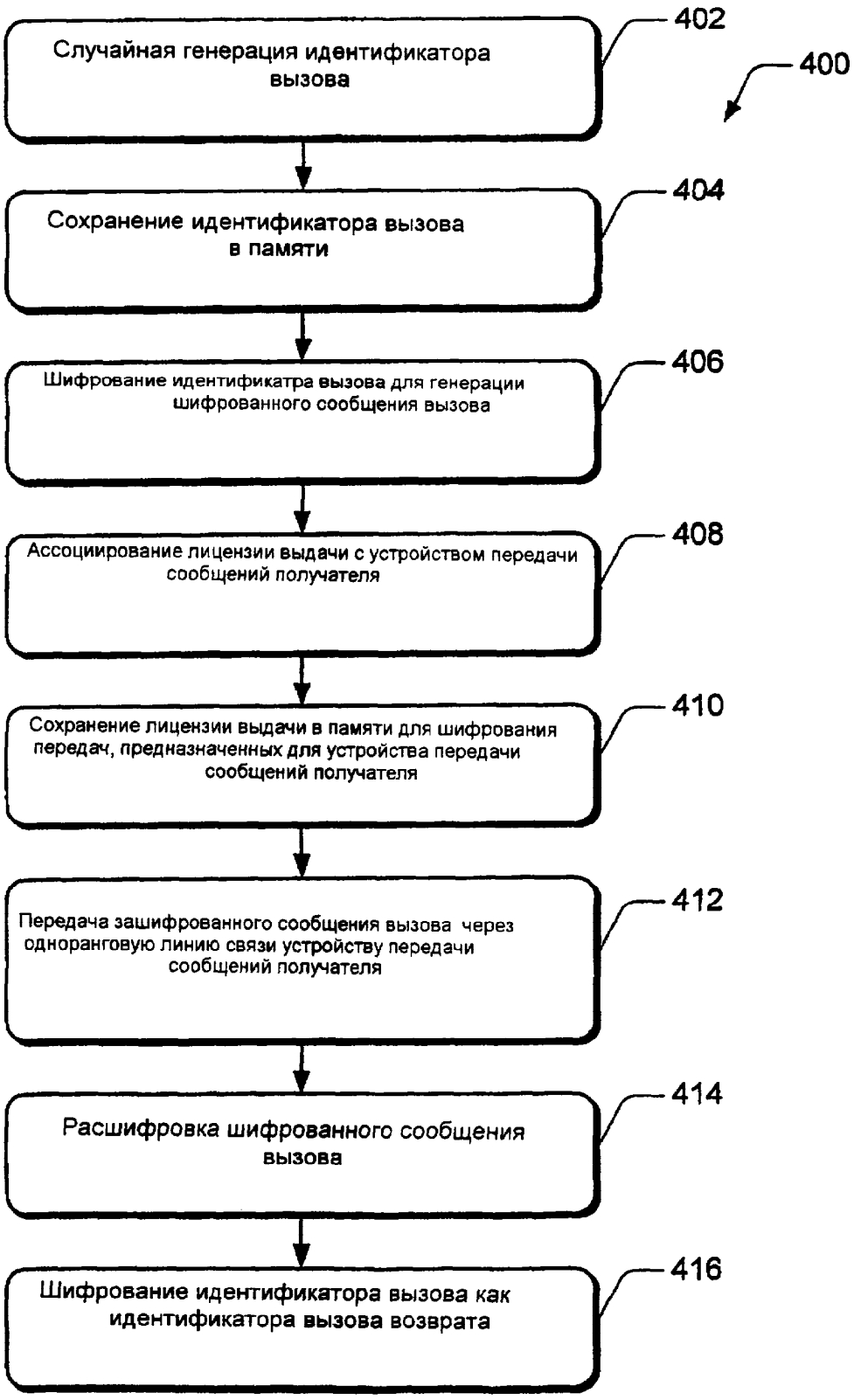
расшифровывать второе зашифрованное мгновенное сообщение с лицензией использования, соответствующей лицензии выдачи, которая связана с устройством передачи сообщений получателя.


200
Устройство передачи сообщений
104(1)
Приложение передачи сообщений
112(1)
Передача(и) и данные
202
Модуль шифрования
116(1)
Служба DRM
206(1)
Память
208(1)
Данные шифрования
212(1)
Контакт(ы)
210(1)
108
Устройство передачи сообщений
104(N)
Приложение передачи сообщений
112(N)
Передача(и) и данные
204
Модуль шифрования
116(N)
Служба DRM
206(N)
Память
208(N)
Данные шифрования
212(N)
Контакт(ы)
210(N)

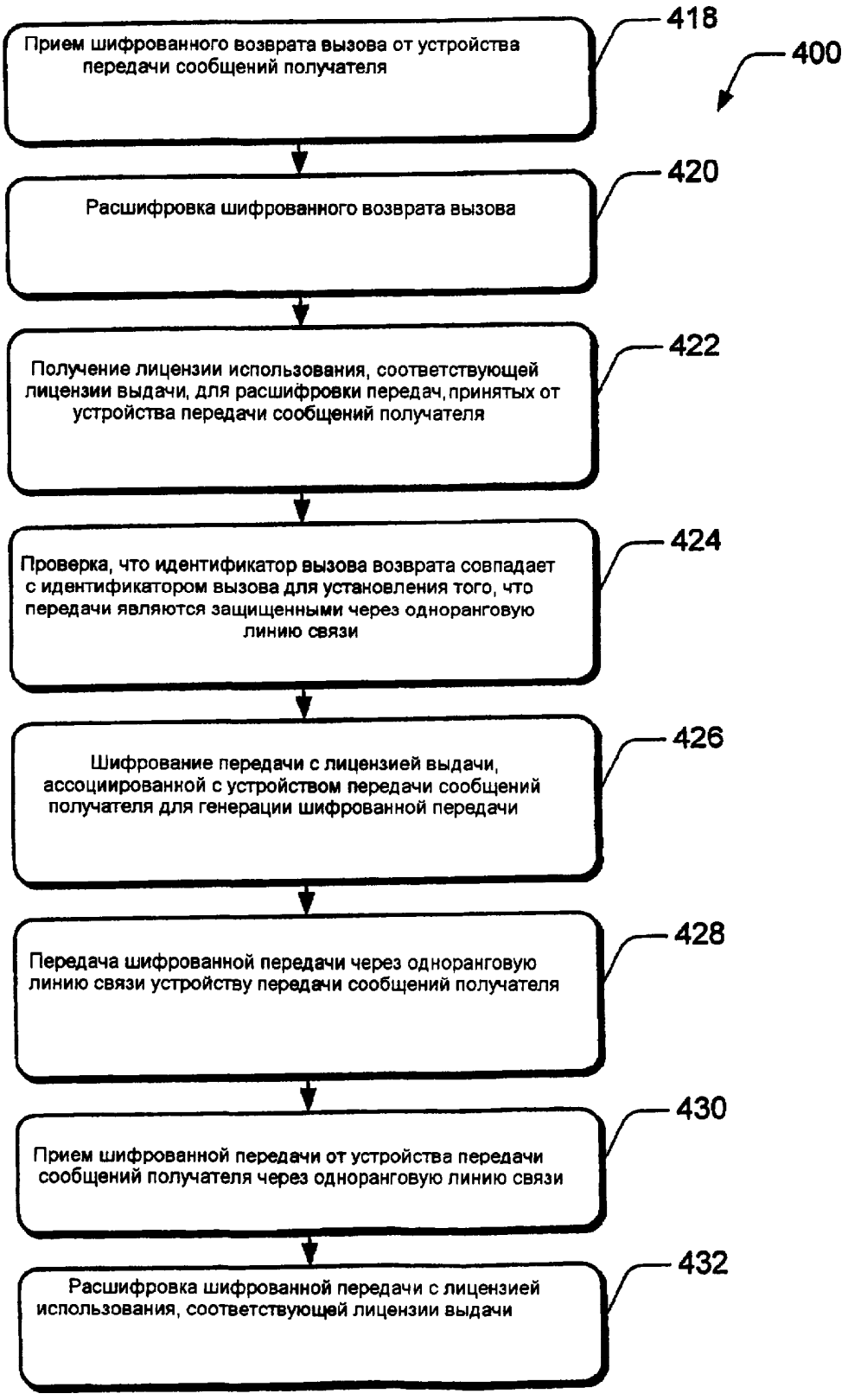
ФИГ.2


300
Устройство передачи сообщений
104(1)
Приложение передачи сообщений
112(1)
Передача(и) и данные
202
Шифрованное сообщение вызова
308
Модуль шифрования
116(1)
Идентификатор вызова
302
Служба DRM
206(1)
Лицензия(и) выдачи
306
Ключ шифрования
304
Политики управления
322(1)
310
320
108
Устройство передачи сообщений
104(N)
Приложение передачи сообщений
112(N)
Передача(и) и данные
204
Шифрованный возврат вызова
314
Модуль шифрования
116(N)
ID вызова возврата
312
Служба DRM
206(N)
Лицензия(и) выдачи
318
Ключ шифрования
316
Политики управления
322(N)

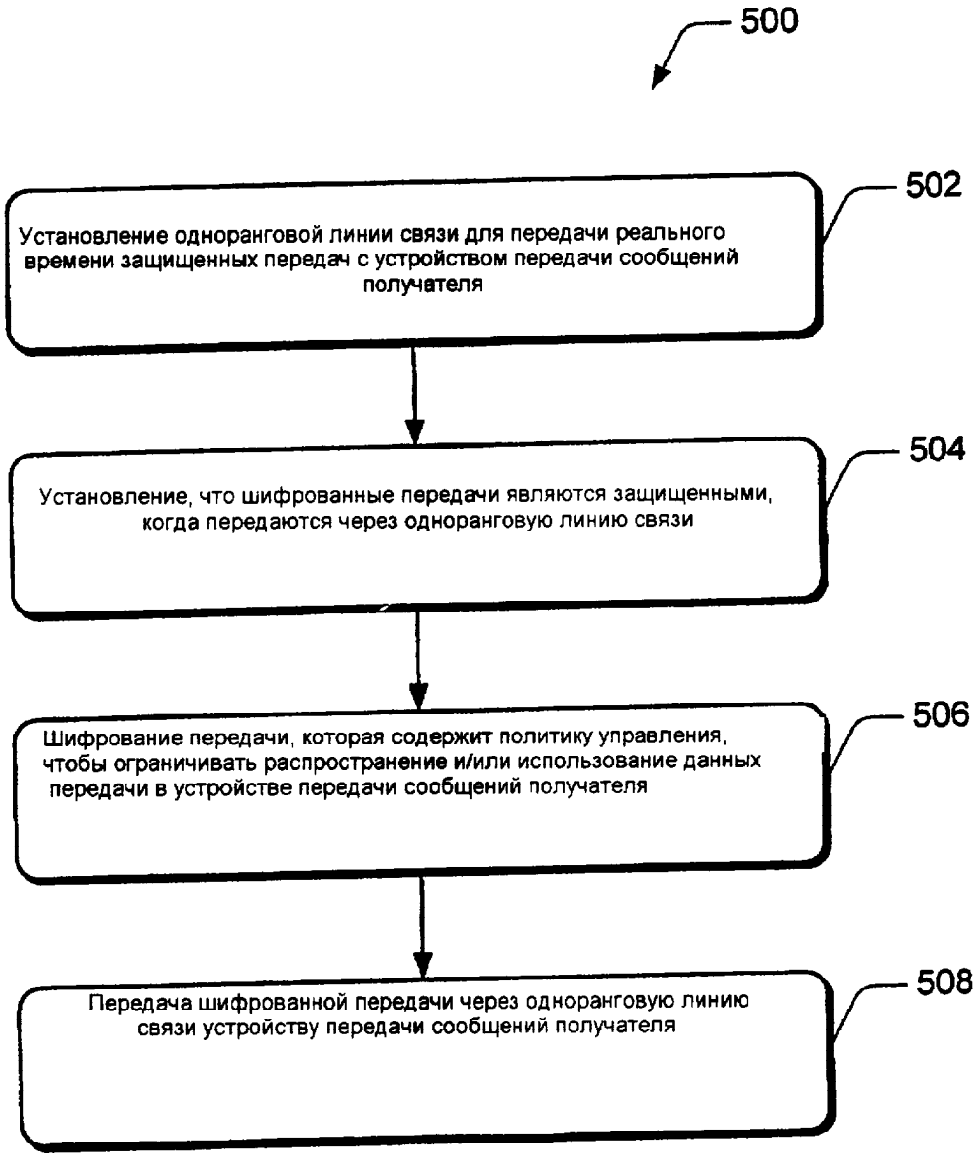
ФИГ.3


400
402
Случайная генерация идентификатора вызова
404
Сохранение идентификатора вызова в памяти
406
Шифрование идентификатра вызова для генерации шифрованного сообщения вызова
408
Ассоциирование лицензии выдачи с устройством передачи сообщений получателя
410
Сохранение лицензии выдачи в памяти для шифрования передач, предназначенных для устройства передачи сообщений получателя
412
Передача зашифрованного сообщения вызова через одноранговую линию связи устройству передачи сообщений получателя
414
Расшифровка шифрованного сообщения вызова
416
Шифрование идентификатора вызова как идентификатора вызова возврата

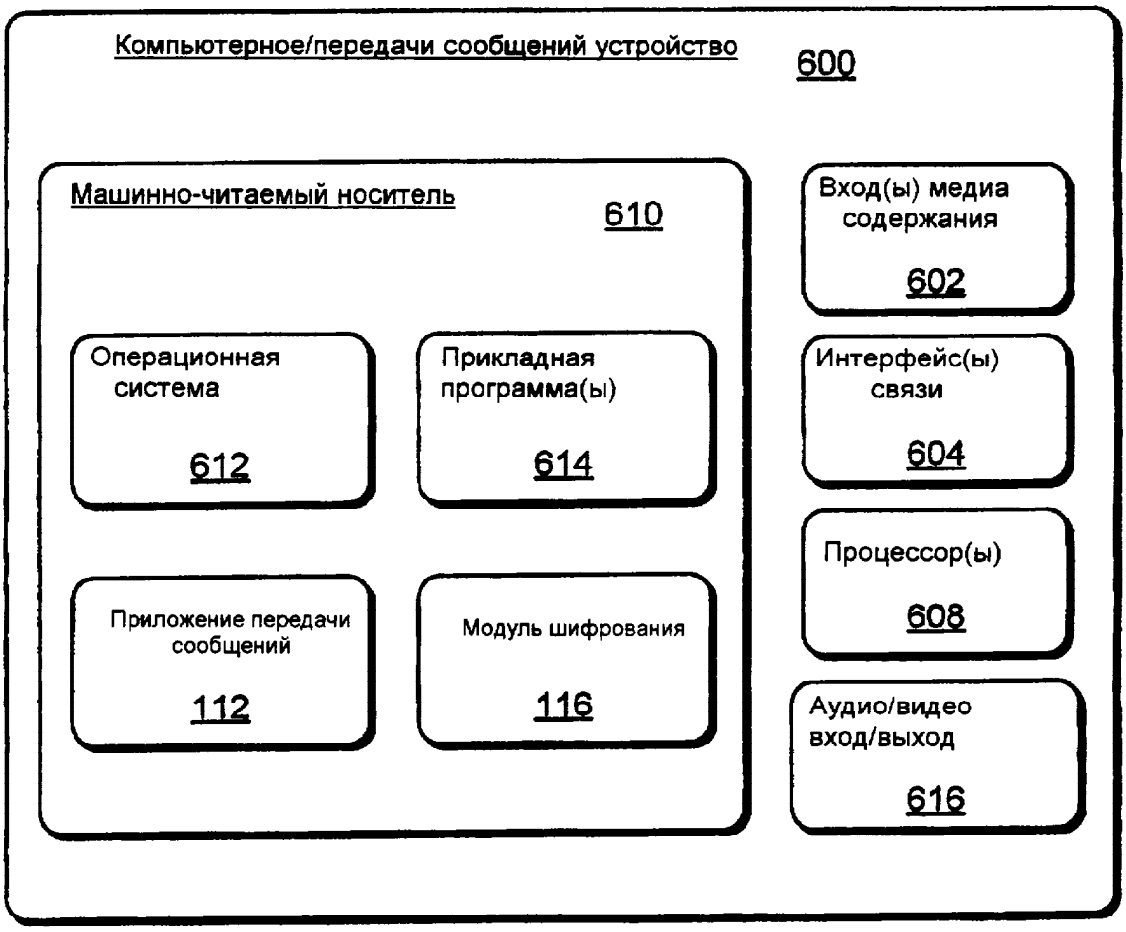
ФИГ.4А


418
400
Прием шифрованного возврата вызова от устройства передачи сообщений получателя
420
Расшифровка шифрованного возврата вызова
422
Получение лицензии использования, соответствующей лицензии выдачи, для расшифровки передач, принятых от устройства передачи сообщений получателя
424
Проверка, что идентификатор вызова возврата совпадает с идентификатором вызова для установления того, что передачи являются защищенными через одноранговую линию связи
426
Шифрование передачи с лицензией выдачи, ассоциированной с устройством передачи сообщений получателя для генерации шифрованной передачи
428
Передача шифрованной передачи через одноранговую линию связи устройству передачи сообщений получателя
430
Прием шифрованной передачи от устройства передачи сообщений получателя через одноранговую линию связи
432
Расшифровка шифрованной передачи с лицензией использования, соответствующей лицензии выдачи

ФИГ.4В


500
502
Установление одноранговой линии связи для передачи реального времени защищенных передач с устройством передачи сообщений получателя
504
Установление, что шифрованные передачи являются защищенными, когда передаются через одноранговую линию связи
506
Шифрование передачи, которая содержит политику управления, чтобы ограничивать распространение и/или использование данных передачи в устройстве передачи сообщений получателя
508
Передача шифрованной передачи через одноранговую линию связи устройству передачи сообщений получателя

ФИГ.5


Компьютерное/передачи сообщений устройство
600
Машинно-читаемый носитель
610
Операционная система
612
Прикладная программа(ы)
614
Приложение передачи сообщений
112
Модуль шифрования
116
Вход(ы) медиа содержания
602
Интерфейс(ы) связи
604
Процессор(ы)
608
Аудио/видео вход/выход
616

ФИГ.6