РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 332 704** (13) **C2**

(51) МПК
G06F 12/14 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004103872/09, 10.02.2004**

(24) Дата начала отсчета срока действия патента:
10.02.2004

(30) Конвенционный приоритет:
11.02.2003 US 10/364,115

(43) Дата публикации заявки: **20.07.2005**

(45) Опубликовано: **27.08.2008 Бюл. № 24**

(56) Список документов, цитированных в отчете о поиске: **WO 01/52021 B1, 19.07.2002. RU 2189119 C2, 10.09.2002. RU 2163056 C2, 10.02.2001. JP 2002229960, 16.08.2002. WO 01/78303 A1, 18.10.2001. JP 2002359616, 13.12.2002. WO 02/101494 A3, 19.12.2002. EP 1128598 A1, 29.08.2001.**

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):
НАРИН Аттила (US),
ВЕНКАТЕШ Чандрамоули (US),
БИРУМ Фрэнк Д. (US),
ДЕМЕЛЛО Марко А. (US),
ВАКСМАН Питер Дэвид (US),
МАЛИК Прашант (US),
МАЛАВИАРАЧЧИ Рушми У. (US),
БОРН Стив (US),
КРИШНАСВАМИ Винай (US),
РОЗЕНФЕЛЬД Евгений Юджин (US)

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

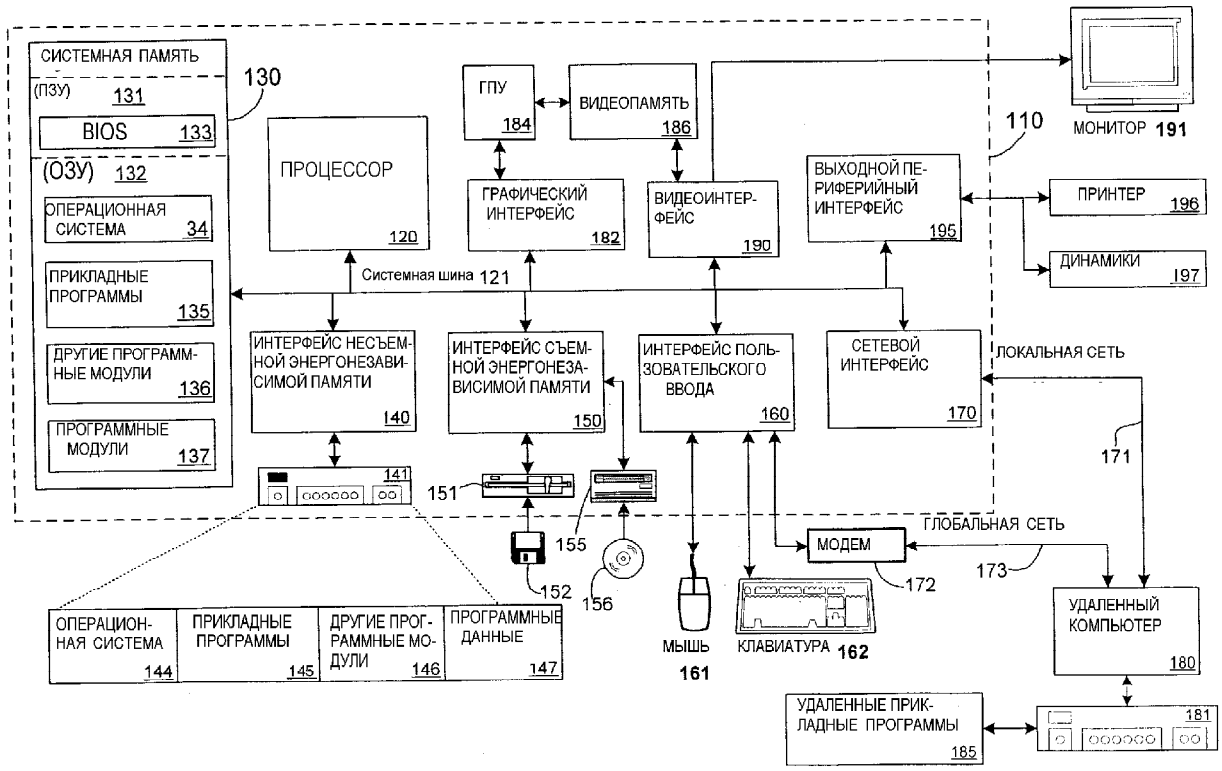
(54) ПУБЛИКАЦИЯ ЦИФРОВОГО СОДЕРЖАНИЯ В ОПРЕДЕЛЕННОМ ПРОСТРАНСТВЕ, ТАКОМ КАК ОРГАНИЗАЦИЯ, В СООТВЕТСТВИИ С СИСТЕМОЙ ЦИФРОВОГО УПРАВЛЕНИЯ ПРАВАМИ (ЦУП)

(57) Реферат:

Изобретение относится к цифровому управлению правами и их исполнением для различных видов цифрового содержания мультимедийных материалов. Техническим результатом является повышение защищенности использования мультимедийных объектов цифровой информации. В способе лицензиар получает от запрашивающей стороны запрос, включающий в себя данные прав, связанные с цифровым содержанием и перечисляющие, по меньшей мере, один идентификатор и набор прав, связанных с ним. Лицензиар выбирает идентификатор и набор связанных с ним прав, которые предполагается изложить в соответствующей цифровой лицензии, а также выбирает на основании идентификатора альтернативный набор прав. Альтернативный набор прав заменяет набор прав из данных прав, и запрашивающей стороне выдается лицензия с альтернативным набором прав, при этом альтернативный набор прав в выданной лицензии излагает условия, которые должна соблюдать запрашивающая сторона в связи с представлением соответствующего содержания. 2 н. и 16 з.п. ф-лы, 14 ил.

RU 2332704 C2

RU 2332704 C2



ФИГ. 1

RU 2332704 C2

RU 2332704 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 332 704** (13) **C2**

(51) Int. Cl.
G06F 12/14 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2004103872/09, 10.02.2004**

(24) Effective date for property rights: **10.02.2004**

(30) Priority:
11.02.2003 US 10/364,115

(43) Application published: **20.07.2005**

(45) Date of publication: **27.08.2008 Bull. 24**

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):
NARIN Attila (US),
VENKATESh Chandramouli (US),
BIRUM Frehnk D. (US),
DEMELLO Marko A. (US),
VAKSMAN Piter Dehvid (US),
MALIK Prashant (US),
MALAVIARAChChI Rushmi U. (US),
BORN Stiv (US),
KRIShNASVAMI Vinaj (US),
ROZENFEL'D Evgenij Judzhin (US)

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

(54) PUBLICATION OF DIGITAL CONTENT IN CERTAIN SPACE SUCH AS ORGANISATION ACCORDING TO DIGITAL RIGHTS MANAGEMENT SYSTEM (DRM)

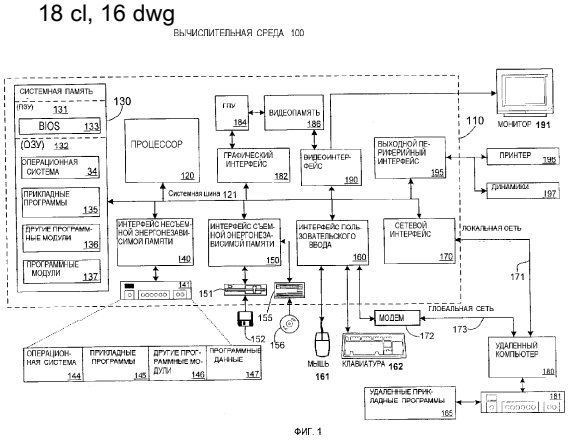
(57) Abstract:

FIELD: information technology.

SUBSTANCE: according to proposed method, the licenser receives an inquiry from the requester, including the rights data connected with digital content and specifying at least one identifier and a set of rights connected therewith. The licenser chooses one identifier and a set of rights connected therewith, witch are supposed to be described in a corresponding digital license, and also chooses an alternative set of rights based on the identifier. The alternative set of rights substitutes for the set of rights from present rights and the requester receives a license with the alternative set of rights. The alternative set of rights in the issued license lays down conditions that must be fulfilled by the requester in connection with presentation of corresponding content.

EFFECT: increased protection of the multimedia digital information objects usage.

18 cl, 16 dwg



ФИГ. 1

RU 2332704 C2

RU 2332704 C2

Ссылки на родственные заявки

Следующие заявки на патент США раскрывают объект изобретения, который связан с объектом изобретения настоящей заявки, и поэтому они включены в нее в полном объеме в качестве ссылки:

Заявка на патент США № 10/185527, поданная 28.06.2002 г. (№ MSFT-1330 в реестре поверенного), на изобретение "Получение подписанной метки прав (ПМП) для цифрового содержания и получение цифровой лицензии, соответствующей содержанию, на основании ПМП в системе цифрового управления правами";

Заявка на патент США № 10/185278, поданная 28.06.2002 г. (MSFT-1333 в реестре поверенного), на изобретение "Использование шаблона прав для получения подписанной метки прав (ПМП) для цифрового содержания в системе цифрового управления правами"; и

Заявка на патент США № 10/185511, поданная 28.06.2002 г. (№ MSFT-1343 в реестре поверенного), на изобретение "Системы и способы выдачи лицензий на использование цифрового содержания и услуг".

Область техники

Настоящее изобретение относится к системе цифрового управления правами (ЦУП). Более конкретно, изобретение относится к использованию системы ЦУП для публикации цифрового содержания в определенном пространстве, например организации, учреждении, корпорации или т.п., таким образом, чтобы представление и использование содержания в данном пространстве можно было ограничить согласно соответствующим условиям использования или лицензии.

Описание известного уровня техники

Цифровое управление правами и их исполнением очень желательно для таких видов цифрового содержания (содержимого) как цифровой звук, цифровое видео, цифровой текст, цифровые данные, цифровые мультимедийные материалы и т.п., в тех случаях, когда это цифровое содержание необходимо распространять одному или более пользователям. Цифровое содержание может быть статичным, например, текстовый документ, или потоковым, например, потоковый звук/видео при вещании в прямом эфире. Типичные способы распространения включают в себя материальные устройства, такие как магнитный (гибкий) диск, магнитная лента, оптический (компактный) диск (CD) и т.п., и нематериальные носители, например, электронная доска объявлений, электронная сеть, Интернет и т.п. После получения цифрового содержания пользователь осуществляет его представление или "воспроизведение" с помощью соответствующего воспроизводящего устройства, например, устройство воспроизведения мультимедийных данных в персональном компьютере или т.п.

В одном сценарии владелец содержания или владелец прав, например, автор, издатель, распространитель и т.д., желает распространять такое цифровое содержание каждому из множества пользователей или получателей в обмен на лицензионную плату или какое-то другое вознаграждение. В таком сценарии содержание может быть музыкальным произведением, альбомом музыкальных произведений, кинофильмом и т.п., и целью его распространения является получение лицензионных платежей. Владелец такого содержания, вероятно, при возможности пожелает ограничить действия, которые пользователь может совершать с таким распространяемым цифровым содержанием. Например, владелец содержания может пожелать воспрепятствовать возможности копирования и дальнейшего распространения такого содержания пользователем другому пользователю, по меньшей мере, таким образом, при котором владелец содержания не сможет получить лицензионную плату от этого другого пользователя.

Кроме того, владелец содержания может пожелать предоставить пользователю гибкость, позволяющую покупать лицензии различного вида за различные лицензионные платы, и в то же время удерживать пользователя в рамках условий, соответствующих фактическому виду купленной лицензии. Например, владелец содержания может пожелать, чтобы воспроизведение распространяемого цифрового содержания осуществлялось только

ограниченное количество раз, только в течение определенного общего времени, только на устройстве определенного типа, только устройством воспроизведения мультимедийных материалов определенного типа, только определенным типом пользователя, и т.д.

В другом сценарии разработчик содержания, например, работодатель или член организации, может пожелать, чтобы цифровое содержание распространялось одному или нескольким работникам или членам организации, или лицам вне организации, без возможности осуществления его представления другими лицами. В этом случае распространение содержания будет более сродни совместному конфиденциальному или ограниченному использованию содержания в рамках организации в отличие от широкого распространения в обмен на лицензионную плату иди другое вознаграждение.

В таком сценарии содержание может быть представлением документа, электронной таблицей, базой данных, электронной почтой или т.п., которыми можно обмениваться внутри учреждения, и разработчик содержания может пожелать, чтобы это содержание оставалось внутри организации или учреждения без возможности его воспроизведения несанкционированными лицами, например, конкурентами или противниками. И в этом случае разработчик содержания также может пожелать ограничить действия, которые получатель сможет совершать с таким распространяемым цифровым содержанием. Например, владелец содержания может пожелать ограничить пользователя от копирования и дальнейшего распространения такого содержания другому пользователю, по меньшей мере, таким образом, при котором содержание станет открытым за рамками тех лиц, которым может быть разрешено воспроизведение этого содержания.

Кроме того, разработчик содержания может пожелать, чтобы разным получателям предоставлялись различные уровни прав на воспроизведение. Например, разработчик содержания может пожелать, чтобы одному классу лиц было разрешено просматривать охраняемое цифровое содержание без возможности его распечатки, а другому классу лиц было разрешено и просматривать его, и распечатывать.

Но после факта распространения в любом из этих сценариев владелец/разработчик содержания имеет очень малую возможность, если вообще ее имеет, управлять этим цифровым содержанием. Это особенно проблематично с учетом того факта, что практически любой персональный компьютер имеет программные и аппаратные средства, позволяющие получить точную цифровую копию такого цифрового содержания и загрузить эту точную цифровую копию на записываемый магнитный или оптический диск, или послать такую точную цифровую копию по сети, например, Интернет, любому адресату.

Конечно, в рамках сделки по распространению содержания владелец/разработчик содержания может потребовать, чтобы пользователь/получатель цифрового содержания дал обещание не распространять это цифровое содержание нежелательным способом. Однако такое обещание легко дается и легко нарушается. Владелец/разработчик содержания может попытаться предотвратить такое дальнейшее распространение с помощью некоторых хорошо известных устройств, обычно требующих шифрования и дешифрования. Однако мало вероятно, что это помешает достаточно решительному пользователю расшифровать зашифрованное цифровое содержание, сохранить такое цифровое содержание в незашифрованной форме в памяти, а затем распространять его дальше.

Таким образом, существует потребность в создании архитектуры и способа для цифрового управления правами (ЦУП) и их исполнением, которые бы обеспечили управляемое представление или воспроизведение произвольных форм цифрового содержания, и чтобы такое управление было гибким и могло определяться владельцем/разработчиком цифрового содержания. Более конкретно, существует потребность в такой архитектуре, которая бы позволила и облегчила осуществление управляемого представления, особенно в среде учреждения или организации или т.п., где документы должны использоваться совместно определенной группой или классом людей.

Краткое изложение сущности изобретения

Перечисленные выше потребности удовлетворяются, по меньшей мере, частично, с

помощью настоящего изобретения, в котором лицензиар выдает цифровую лицензию запрашивающей стороне, разрешающую ей осуществлять представление соответствующего цифрового содержания.

Согласно изобретению лицензиар получает от запрашивающей стороны запрос, содержащий связанные с содержанием (содержимым) данные прав, перечисляющие, по меньшей мере, один идентификатор и набор прав, связанных с ним. Лицензиар выбирает идентификатор и набор связанных с ним прав, которые предполагается изложить в выданной лицензии, а также выбирает на основании идентификатора альтернативный набор прав. Альтернативный набор прав заменяет набор прав из данных прав, и лицензия выдается запрашивающей стороне с альтернативным набором прав, причем в альтернативном наборе прав в выданной лицензии излагаются условия, которые должна соблюдать запрашивающая сторона в связи с представлением соответствующего содержания.

Краткое описание чертежей

Краткое описание сущности изобретения, а также последующее подробное описание вариантов осуществления настоящего изобретения станут более понятны при их чтении со ссылками на прилагаемые чертежи. Для целей иллюстрации изобретения на чертежах представлены варианты, которые могут являться предпочтительными в настоящее время. Однако понятно, что изобретение не ограничено точными изображенными компоновками и средствами. На чертежах

фиг.1 изображает структурную схему, представляющую примерный неограничительный вариант вычислительной среды, в которой может быть реализовано настоящее изобретение,

фиг.2 изображает структурную схему, представляющую примерную сетевую среду, содержащую множество вычислительных устройств, в которой может быть реализовано настоящее изобретение,

фиг.3 изображает функциональную структурную схему одного варианта системы и способа согласно изобретению для публикации цифрового содержания,

фиг.4 иллюстрирует алгоритм выполнения одного варианта способа согласно изобретению для публикации управляемого правами цифрового содержания,

фиг.4А изображает структурную схему, показывающую структуру подписанной метки прав, созданной способом, проиллюстрированным на фиг.4,

фиг.5 изображает структурную схему одного варианта системы и способа согласно изобретению для выдачи лицензии на управляемое правами цифровое содержание,

фиг.6А и 6В иллюстрируют алгоритмы выполнения одного варианта способа согласно изобретению для выдачи лицензии на управляемое правами цифровое содержание,

фиг.7 изображает алгоритм, показывающий основные этапы, которые выполняются при переиздании метки прав в соответствии с одним вариантом настоящего изобретения,

фиг.8 изображает структурную схему, изображающую сертификат, выданный пользователю сервером ЦУП, чтобы разрешить ему выполнять автономную публикацию в соответствии с одним вариантом изобретения,

фиг.9 изображает структурную схему, иллюстрирующую шаблон прав, определяющий информацию, которая должна быть включена в метку прав, согласно одному варианту настоящего изобретения,

фиг.10 изображает алгоритм выполнения основных операций при создании шаблона прав по фиг.9 и создании подписанной метки прав по фиг.4А на основании шаблона прав, согласно одному варианту изобретения,

фиг.11 изображает структурную схему, изображающую архитектуру исполнения в примерном варианте системы, основанном на доверительных отношениях,

фиг.12 изображает структурную схему, показывающую как лицензиар обрабатывает запрос на лицензию согласно одному варианту изобретения,

фиг.13 изображает алгоритм, показывающий операции, выполняемые лицензиаром по фиг.12 в связи с каталогом при выдаче лицензии, и

фиг.14 изображает алгоритм, показывающий операции, выполняемые лицензиаром по фиг.12 при введении стратегии в лицензию, которую предстоит выдать.

Подробное описание изобретения

Вычислительная среда

На фиг.1 и в последующем описании представлена и кратко описана подходящая вычислительная среда, в которой можно реализовать изобретение. Однако при этом следует понимать, что в связи с настоящим изобретением можно использовать карманные, портативные и другие вычислительные устройства всех видов. Хотя в дальнейшем будет описан универсальный компьютер, это всего лишь один пример, и настоящее изобретение требует наличия только "тонкого" клиента, имеющего возможность взаимодействия с сетевым сервером. Таким образом, настоящее изобретение можно реализовать в среде услуг с сетевыми хост-узлами, в которой используются очень небольшие или минимальные клиентские ресурсы, например, в сетевой среде, в которой клиентское устройство служит только в качестве браузера или интерфейса для взаимодействия с «Всемирной паутиной».

Хотя это и не является необходимым, изобретение можно реализовать через интерфейс прикладного программирования (ИПП) для использования разработчиком, и/или включить его в программное обеспечение сетевого браузера, которое будет описано в общем контексте выполняемых компьютером команд, таких как программные модули, исполняемые одним или несколькими компьютерами, например, клиентскими рабочими станциями, серверами или другими устройствами. Программные модули обычно содержат подпрограммы, программы, объекты, компоненты, структуры данных и т.п., которые выполняют определенные задачи или реализуют определенные типы абстрактных данных. Обычно, функциональные возможности программных модулей можно объединять или распределять, в зависимости от потребности, в различных средах. Кроме того, специалистам будет понятно, что изобретение можно реализовать и с другими конфигурациями вычислительной системы. Другие хорошо известные вычислительные системы, среды и/или конфигурации, которые могут быть пригодны для использования с изобретением, включают в себя, не ограничиваясь перечисленным, персональные компьютеры (ПК), автоматические банковские терминалы, серверы, карманные или портативные компьютеры, многопроцессорные системы, системы на базе микропроцессора, программируемые потребительские электронные устройства, сетевые ПК, миникомпьютеры, универсальные вычислительные машины и т.д. Изобретение можно также реализовать в распределенных вычислительных средах, в которых задачи выполняются удаленными устройствами обработки, связанными между собой коммуникационной сетью или другой средой передачи данных. В распределенной вычислительной среде программные модули могут находиться в среде для хранения информации как локального, так и удаленного компьютера, включая запоминающие устройства.

На фиг.1 показан примерный вариант пригодной конфигурации 100 вычислительной системы, в которой можно реализовать изобретение, хотя, как пояснялось выше, конфигурация 100 является только примером пригодной вычислительной среды и не предполагает какого-либо ограничения объема использования или функциональных возможностей изобретения. Также не следует рассматривать конфигурацию 100 вычислительной системы как имеющую какую-либо зависимость или требования, относящиеся к любому компоненту или их комбинациям, показанным в примерной операционной конфигурации 100.

Изображенная на фиг.1 примерная система для реализации изобретения включает в себя универсальное вычислительное устройство в форме компьютера 110. Компоненты компьютера 110 могут включать в себя, без ограничения перечисленным, процессор 120, системную память 130 и системную шину 121, связывающую между собой различные компоненты системы, включая системную память с процессором 120. Системная шина 121 может быть любого из нескольких типов шинных структур, включая шину памяти или контроллер памяти, периферийную шину и локальную шину с использованием любой из

множества шинных архитектур. Например, такие архитектуры включают в себя, без ограничения перечисленным, шину промышленной стандартной архитектуры (ISA), шину микроканальной архитектуры (MCA), шину расширенной промышленной стандартной архитектуры (EISA), локальную шину Ассоциации по стандартам видеооборудования (VESA) и шину межсоединения периферийных компонентов (PCI) (также известную как шина расширения).

Компьютер 110 типично содержит множество машиночитаемых носителей. Машиночитаемый носитель может быть любым имеющимся носителем, к которому может осуществлять доступ компьютер 110, и включает в себя как энергозависимые, так и энергонезависимые носители, как съемные, так и несъемные носители. Например, машиночитаемый носитель может содержать, без ограничения перечисленного, запоминающую среду и среду связи. Запоминающая среда включает в себя энергозависимые и энергонезависимые носители, съемные и несъемные носители, реализованные согласно любой методике или технологии, для хранения информации, такой как машиночитаемые команды, структуры данных, программные модули или другие данные. Запоминающая среда включает в себя, без ограничения перечисленным, ОЗУ, ПЗУ, ЭППЗУ, флэш-память или другую память, диски CD-ROM, DVD или другие оптические диски, магнитные кассеты, магнитную ленту, магнитные диски или другие магнитные запоминающие устройства, или любые другие носители, которые можно использовать для хранения требуемой информации и к которым может осуществлять доступ компьютер 110. Среда связи обычно включает в себя машиночитаемые команды, структуры данных, программные модули или другие данные в модулированном сигнале данных, таком как несущая, или другом транспортном механизме, и включает в себя любую среду передачи информации. Термин "модулированный сигнал данных" означает сигнал, одна или несколько характеристик которого установлены или изменены таким образом, чтобы закодировать информацию в сигнал. Например, среда связи включает в себя, без ограничения перечисленным, проводную среду, такую как проводная сеть или прямое проводное соединение, и беспроводную среду, такую как акустическая, ВЧ, инфракрасная или другая беспроводная среда. В объем понятия машиночитаемой среды также входят комбинации любых из перечисленных выше средств.

Системная память 130 включает в себя машиночитаемый носитель в виде энергозависимой и/или энергонезависимой памяти, такой как постоянное запоминающее устройство (ПЗУ) 131 и оперативное запоминающее устройство (ОЗУ) 132. Базовая система ввода-вывода (БСВВ) 133, содержащая основные программы, которые помогают передавать информацию между элементами компьютера 110, например, при включении, обычно хранится в ПЗУ 131. ОЗУ 132 обычно содержит данные и/или программные модули, доступ к которым может производиться немедленно и/или которые в данный момент обрабатываются процессором 120. Например, без ограничения показанным, на фиг.1 изображена операционная система 134, прикладные программы 135, другие программные модули 136 и программные данные 137.

Компьютер 110 может также содержать съемное/несъемное, энергонезависимое/энергозависимое запоминающее устройство вычислительной машины. Только в качестве примера фиг.1 иллюстрирует накопитель 141 на жестких дисках, который осуществляет считывание или запись на несъемный, энергонезависимый магнитный носитель, накопитель 151 на магнитных дисках, который осуществляет считывание или запись на съемный энергонезависимый магнитный диск 152 и накопитель 155 на оптических дисках, который осуществляет считывание или запись на съемный, энергонезависимый оптический диск 156, такой как CD-ROM или другой оптический носитель. Другие съемные/несъемные, энергозависимые/энергонезависимые запоминающие устройства вычислительной машины, которые можно использовать в данной примерной операционной среде, включают в себя, без ограничения перечисленным, кассеты магнитной ленты, карты флэш-памяти, диски DVD, цифровую видеоленту, полупроводниковые ОЗУ, полупроводниковые ПЗУ и т.п. Накопитель 141 на

жестких дисках обычно подключен к системной шине 121 через интерфейс несъемного запоминающего устройства, такой как интерфейс 140, а накопитель 151 на магнитных дисках и накопитель 155 на оптических дисках обычно подключены к системной шине 121 через интерфейс съемного запоминающего устройства, такой как интерфейс 150.

Эти накопители и связанные с ними запоминающие среды для вычислительной машины, обсуждавшиеся выше и проиллюстрированные на фиг.1, обеспечивают хранение машиночитаемых команд, структур данных, программных модулей и других данных для компьютера 110. Например, показанный на фиг.1 накопитель 141 на жестких дисках хранит операционную систему 144, прикладные программы 145, другие программные модули 146 и программные данные 147. Следует отметить, что эти компоненты могут быть либо такими же, либо отличаться от операционной системы 134, прикладных программ 135, других программных модулей 136 и программных данных 137. Операционная система 144, прикладные программы 145, другие программные модули 146 и программные данные 147 здесь обозначены разными ссылочными номерами, чтобы проиллюстрировать, что они, как минимум, являются различными копиями. Пользователь может вводить команды и информацию в компьютер 110 через устройства ввода данных, такие как клавиатура 162 и указательное устройство 161, обычно именуемое мышью, трекбол или сенсорную панель. Другие устройства ввода (не показаны) могут включать в себя микрофон, джойстик, игровую приставку, спутниковую тарелку, сканер и т.п. Эти и другие устройства ввода часто подсоединены к процессору 120 через интерфейс 160 пользовательского ввода, который подключен к системной шине 121, но может быть подключен другим интерфейсом и шинными структурами, такими как параллельный порт, игровой порт или универсальная последовательная шина (USB).

Монитор 191 или другой вид устройства отображения также подключен к системной шине 121 через такой интерфейс, как видеоинтерфейс 190. Графический интерфейс 182, такой как Northbridge (Северный мост), может быть также подключен к системной шине 121. Northbridge - это микропроцессорный набор, который сообщается с ЦПУ или главным процессором 120 и отвечает за связь через ускоренный графический порт (AGP). Одно или несколько графических процессорных устройств (ГПУ) 184 могут сообщаться с графическим интерфейсом 182. При этом ГПУ 184 обычно включают в себя встроенное в кристалл запоминающее устройство, такое как регистровая память, и ГПУ 184 сообщается с видеопамятью 186. Однако ГПУ 184 являются всего лишь одним примером сопроцессора, и в состав компьютера 110 может входить множество различных сопроцессорных устройств. Монитор 191 или другой тип отображающего устройства также подключен к системной шине 121 через интерфейс, такой как видеоинтерфейс 190, который может, в свою очередь, сообщаться с видеопамятью 186. В дополнение к монитору 191 компьютеры могут также содержать другие периферийные устройства вывода, такие как динамики 197 и принтер 196, которые можно подключить через выходной периферийный интерфейс 195.

Компьютер 110 может работать в сетевой среде с использованием логических соединений с одним или несколькими удаленными компьютерами, такими как удаленный компьютер 180. Удаленный компьютер 180 может быть персональным компьютером, сервером, маршрутизатором, сетевым ПК, одноранговым узлом сети или обычным общим сетевым узлом и обычно включает в себя многие или все элементы, описанные выше в связи с компьютером 110, хотя на фиг.1 проиллюстрировано только запоминающее устройство 181. Логические соединения, показанные на фиг.1, включают в себя локальную вычислительную сеть (ЛВС) 171 и глобальную вычислительную сеть (ГВС), но могут также включать в себя и другие сети. Такие сетевые среды обычно применяются в учрежденческих, корпоративных вычислительных сетях, внутренних сетях и Интернет.

При использовании в сетевой среде ЛВС компьютер 110 подключен к ЛВС 171 через сетевой интерфейс или адаптер 170. При использовании в сетевой среде ГВС компьютер 110 обычно содержит модем 172 или другие средства для установления связи через ГВС 173, такой как Интернет. Модем 172, который может быть внешним или внутренним, может быть подсоединен к системной шине 121 через интерфейс 160 пользовательского ввода

или другой соответствующий механизм. В сетевой среде программные модули, показанные в связи с компьютером 110, или их части могут храниться в удаленном запоминающем устройстве. Например, что не является ограничением, на фиг.1 показаны удаленные прикладные программы 185, находящиеся в запоминающем устройстве 181. Понятно, что показанные сетевые соединения являются примерными и можно использовать другие средства для установления каналов связи между компьютерами.

Специалистам будет понятно, что компьютер 110 или другое клиентское устройство можно использовать как часть вычислительной сети. В этом отношении настоящее изобретение относится к любой вычислительной системе, имеющей любое количество запоминающих устройств, и любое количество приложений и процессов, происходящих на любом количестве запоминающих устройств или емкостей. Настоящее изобретение может применяться в среде с серверами и клиентскими компьютерами, используемыми в сетевой среде, имеющей удаленное или локальное запоминающее устройство. Настоящее изобретение можно также применять в изолированном вычислительном устройстве, имеющем функциональные возможности языка программирования, а также возможности интерпретации и исполнения.

Распределенная обработка данных облегчает совместное использование вычислительных ресурсов и услуг за счет прямого обмена между вычислительными устройствами и системами. Эти ресурсы и услуги включают в себя обмен информацией, кэш-память и накопители на дисках для файлов. Распределенная обработка данных использует сетевые соединения, позволяя клиентам использовать их общие вычислительные возможности на благо всего предприятия. При этом многие устройства могут иметь приложения, объекты или ресурсы, которые способны взаимодействовать между собой для реализации методов аутентификации согласно настоящему изобретению для надежного графического конвейера (конвейеров). На фиг.2 показана схема примерной сетевой или распределенной вычислительной среды. Распределенная вычислительная среда содержит вычислительные объекты 10a, 10b и т.д. и вычислительные объекты или устройства 110a, 110b, 110c и т.д. Эти объекты могут содержать программы, методы, информационные склады, программируемые логические схемы, и т.д. Объекты могут содержать части тех же самых или других устройств, например, персональных цифровых ассистентов, телевизионных приемников, MP3-плееров, персональных компьютеров и т.п. Каждый объект может сообщаться с другим объектом через коммуникационную сеть 14. Эта сеть, как таковая, может содержать другие вычислительные объекты и вычислительные устройства, которые обеспечивают услуги для системы на фиг.2. Согласно одному аспекту изобретения каждый объект 10 или 110 может содержать приложение, которое может требовать применения способов аутентификации согласно настоящему изобретению для надежного графического конвейера (конвейеров).

Понятно, что объект, такой как 110c, может быть размещен на другом вычислительном устройстве 10 или 110. Следовательно, хотя изображенная физическая среда может показывать соединенные устройства в виде компьютеров, такая иллюстрация является только примером, и физическая среда может быть альтернативно изображена или описана как содержащая различные цифровые устройства, такие как персональные цифровые ассистенты, телевизионные приемники, MP3-плееры, и т.п., а также программные объекты, такие как интерфейсы, COM-объекты и т.п.

Существует широкий спектр систем, компонентов и сетевых конфигураций, которые поддерживают распределенные вычислительные среды. Например, вычислительные системы могут быть соединены между собой проводными и беспроводными системами, локальными сетями или глобальными сетями. В настоящее время многие сети подключены к Интернет, который обеспечивает инфраструктуру для глобальных вычислений и охватывает множество различных сетей.

В домашней сетевой среде существует по меньшей мере четыре отдельные сетевые транспортные среды, каждая из которых может поддерживать уникальный протокол, а именно, линия электропитания, среда передачи данных (беспроводная и проводная), среда

передачи речи (например, телефон) и среда развлечений. Большинство домашних приборов управления, например, выключатели света и бытовые приборы, могут использовать для соединения линию электропитания. Службы данных могут поступать в дом через широкополосную сеть (например, DSL или кабельный модем), а доступ к ним в доме возможен с помощью либо беспроводной (например, HomeRF или 802.11b), либо проводной (например, Home PNA, Cat 5 или даже линии электропитания) связи. Речевой трафик может поступать в дом либо по проводам (например, Cat 3), либо по беспроводному каналу связи (например, сотовые телефоны) и может распространяться в доме с помощью проводки Cat 3. Развлекательная среда может поступать в дом через спутник или кабель и обычно распределяется в доме с помощью коаксиального кабеля. Также разрабатываются цифровые межсоединения IEEE 1394 и DVI для множества мультимедийных устройств. Все эти сетевые среды, а также другие, которые возможно возникнут в будущем как стандарты протоколов, могут быть соединены между собой с образованием внутренней сети, которую можно связать с внешним миром через Интернет. Короче, существует множество различных источников для хранения и передачи данных, и поэтому вычислительные устройства, по мере их развития, будут требовать защиты содержания во всех частях конвейера обработки данных.

Понятие "Интернет", в общем, относится к набору сетей и шлюзов, которые используют протоколы типа TCP/IP, хорошо известные в области вычислительных сетей. TCP/IP сокращенно обозначает "Протокол управления передачей/межсетевой протокол". Интернет можно описать как систему географически распределенных удаленных вычислительных сетей, связанных между собой компьютерами, выполняющими сетевые протоколы, которые позволяют пользователям взаимодействовать и совместно использовать информацию через эти сети. Из-за такого широко распространенного совместного использования информации удаленные сети, такие как Интернет, в общем превратились в открытую систему, для которой разработчики могут создавать программные приложения для выполнения специальных операций или услуг, по существу без ограничения.

Таким образом, сетевая инфраструктура позволяет использовать массу сетевых топологий, таких как клиент/сервер, соединение равноправных узлов ЛВС, или гибридные архитектуры. Под "клиентом" подразумевается член класса или группы, пользующийся услугами другого класса или группы, к которой он не относится. Это значит, что в вычислениях клиентом является процесс, т.е., грубо говоря, набор команд или задач, который запрашивает услугу, предоставляемую другой программой. Клиентский процесс использует запрошенную услугу, "не зная" никаких рабочих деталей о другой программе или самой услуге. В архитектуре клиент/сервер, особенно сетевой системы, клиентом обычно является компьютер, который осуществляет доступ к совместно используемым ресурсам, предоставляемым другим компьютером, например, сервером. В примере на фиг.2 компьютеры 110a, 110b и т.д. можно считать клиентами, а компьютеры 10a, 10b можно считать серверами, при этом сервер 10a, 10b и т.д. содержит данные, которые затем копируются в клиентских компьютерах 110a, 110b и т.д.

Сервером обычно является удаленная вычислительная система, доступ к которой возможен по удаленной сети, такой как Интернет. Клиентский процесс может быть активным в первой вычислительной системе, а серверный процесс может быть активным во второй вычислительной системе, при этом они сообщаются друг с другом через средства связи, что обеспечивает распределенные функциональные возможности и позволяет множеству клиентов воспользоваться возможностями сервера по сбору информации.

Клиент и сервер сообщаются друг с другом с помощью функциональных возможностей, обеспечиваемых протокольным уровнем. Например, протокол передачи гипертекста (HTTP) является общим протоколом, используемым в связи с Всемирной паутиной (WWW). Обычно используется сетевой адрес компьютера, такой как унифицированный адрес ресурса (URL), или адрес Интернет- протокола (IP) используется для идентификации серверного или клиентского компьютеров друг другу. Сетевой адрес можно назвать

унифицированным адресом ресурса (URL). Например, связь можно обеспечить по среде связи. В частности, клиент и сервер могут связываться друг с другом через соединения TCP/IP для обеспечения обмена с высокой пропускной способностью.

Таким образом, на фиг.2 показана примерная сетевая или распределенная среда, в которой сервер осуществляет связь с клиентскими компьютерами через сеть/шину, в которой можно использовать настоящее изобретение. Более подробно, несколько серверов 10a, 10b, и т.д. соединены через коммуникационную сеть/шину 14, которая может быть ЛВС, ГВС, внутренней сетью, Интернет и т.п., с несколькими клиентскими или удаленными вычислительными устройствами 110a, 110b, 110c, 110d, 110e и т.д., такими как портативный компьютер, карманный компьютер, тонкий клиент, сетевой бытовой прибор или другое устройство, такое как видеомагнитофон, телевизионный приемник, печь, осветительный прибор, нагревательный прибор, и т.п., в соответствии с настоящим изобретением. Понятно, что настоящее изобретение можно применить в любом вычислительном устройстве, в котором желательно обрабатывать, хранить или осуществлять представление защищенного содержания из надежного источника.

В сетевой среде, в которой коммуникационной сетью/шиной 14 является Интернет, например, серверы 10 могут быть Web-серверами, с которыми клиенты 110a, 110b, 110c, 110d, 110e и т.д. осуществляют связь через любой из известных протоколов, такой как HTTP. Серверы 10 могут обслуживать клиентов 110, как обычно бывает в распределенной вычислительной среде. Связь может быть проводной и беспроводной, в зависимости от случая. Клиентские устройства 110 могут сообщаться между собой через коммуникационную сеть/шину 14 или могут иметь независимые каналы связи, связанные с ними. Например, в случае телевизионного приемника или видеомагнитофона сетевой аспект для управления им может присутствовать или нет. Каждый клиентский компьютер 110 и серверный компьютер 10 может быть оборудован различными модулями или объектами 135 программных приложений, а также иметь связь или доступ к различным типам запоминающих элементов или объектов, в которых могут храниться файлы или в которые может загружаться или мигрировать часть (части) файлов. Таким образом, настоящее изобретение можно использовать в среде вычислительной сети, имеющей клиентские компьютеры, 110a, 110b и т.д., которые могут осуществлять доступ или взаимодействовать с сетью/шиной 14, и серверные компьютеры 10a, 10b и т.д., которые могут взаимодействовать с клиентскими компьютерами 110a, 110b и т.д. и другими устройствами 111 и базами данных 20.

Обзор цифрового управления правами (ЦУП)

Как известно и проиллюстрировано на фиг.11, цифровое управление правами (ЦУП) и их исполнением очень желательно в отношении цифрового содержания 12, такого как цифровой звук, цифровое видео, цифровой текст, цифровые данные, цифровые мультимедийные материалы, и т.д., в тех случаях, когда такое цифровое содержание 12 должно распространяться пользователям. После получения цифрового содержания пользователь осуществляет его представление или "воспроизведение" с помощью соответствующего представляющего устройства, такого как мультимедийный плеер, на персональном компьютере 14 или т.п.

Обычно, владелец или разработчик содержания (далее именуемый как "владелец"), распространяющий такое цифровое содержание 12, желает ограничить действия, которые пользователь сможет осуществлять с таким распространяемым цифровым содержанием 12. Например, владелец содержания может пожелать воспрепятствовать тому, чтобы пользователь мог копировать и дальше распространять содержание 12 другому пользователю, или может пожелать, чтобы можно было проигрывать распространенное цифровое содержание 12 только ограниченное количество раз, только в течение определенного общего времени, только на определенном типе устройства, только на определенном типе мультимедийного плеера, только определенным типом пользователя и т.д.

Однако после того как произошло распространение цифрового содержания 12, его

владелец имеет очень малую возможность управлять им, если вообще ее имеет. И тогда система ЦУП 10 обеспечивает управляемое представление или воспроизведение произвольных форм цифрового содержания 12, причем такое управление является гибким и определяется владельцем этого цифрового содержания. Обычно содержание 12 распространяется пользователю в форме пакета 13 по любому соответствующему каналу распространения. Распространяемый пакет 13 цифрового содержания может включать в себя цифровое содержание 12, зашифрованное симметричным ключом шифрования/дешифрования (КД) (т.е. КД (СОДЕРЖАНИЕ)), а также другую информацию, идентифицирующую содержание, описывающую, как получить лицензию на такое содержание, и т.д.

Основанная на доверительных отношениях система 10 ЦУП позволяет владельцу цифрового содержания 12 определять правила лицензии, которые должны быть удовлетворены прежде, чем будет разрешено представить цифровое содержание 12 на пользовательском вычислительном устройстве 14. Такие правила лицензии могут включать в себя вышеупомянутое временное требование и могут быть включены в цифровую лицензию или документ об использовании (далее именуемый как "лицензия") 16, который пользователь/пользовательское вычислительное устройство 14 (в дальнейшем эти термины используются как взаимозаменяемые, если только обстоятельства не требуют иного) должно получать от владельца содержания или его агента. Такая лицензия 16 также включает в себя ключ дешифрования (КД) для дешифрирования цифрового содержания, возможно зашифрованного согласно ключу, который может быть дешифрован пользовательским вычислительным устройством.

Владелец содержания должен верить в отношении цифрового содержания 12, что пользовательское вычислительное устройство 14 будет подчиняться правилам и требованиям, указанным владельцем содержания в лицензии 16, т.е. что представление цифрового содержания 12 не будет осуществляться, если не будут удовлетворены правила и требования, установленные в лицензии 16. Для этого пользовательское вычислительное устройство 14 предпочтительно имеет доверенный механизм или компонент 18, который будет осуществлять представление цифрового содержания 12 только в соответствии с правилами, указанными в лицензии 16, связанной с цифровым содержанием 12 и полученной пользователем.

Доверенный компонент 18 обычно имеет блок 20 оценки лицензии, который определяет, действительна ли данная лицензия 16 просматривает правила лицензии и требования в такой действительной лицензии 16 и определяет на основании просмотренных правил лицензии и требований, помимо всего прочего, имеет ли запрашивающий пользователь право осуществлять представление запрашиваемого цифрового содержания 12 так, как он желает. Понятно, что блок 20 оценки лицензии пользуется доверием в системе ЦУП 10 для выполнения пожеланий владельца цифрового содержания 12 согласно правилам и требованиям в лицензии 16, и пользователь не должен иметь возможности легко изменить такой доверенный элемент с любой целью, будь она злоумышленная или нет.

Понятно, что правила и требования в лицензии 16 могут определять, имеет ли данный пользователь право осуществлять представление цифрового содержания 12, на основании любого из нескольких факторов, включая следующие: кто является пользователем, где находится пользователь, какой тип вычислительного устройства использует пользователь, какое представляющее приложение вызывает систему ЦУП, дату, время и т.п. Кроме того, правила и требования лицензии 16 могут ограничить лицензию 16, например, заданным количеством проигрываний или заданным временем проигрывания.

Правила и требования могут быть определены в лицензии 16 в соответствии с любым подходящим языком и синтаксисом. Например, этот язык может просто определять атрибуты и значения, которые должны быть удовлетворены (например, ДАТА должна быть позже, чем X), или может требовать выполнения функций согласно определенному сценарию (например, ЕСЛИ ДАТА больше, чем X, ТО СДЕЛАТЬ ...).

После того, как блок 20 оценки лицензии определит, что лицензия 16 действительная и

что пользователь удовлетворяет правилам и требованиям в ней, цифровое содержание 12 можно будет представить. В частности, для представления содержания 12 ключ дешифрования (КД) получается из лицензии 12 и применятся к (КД(СОДЕРЖАНИЕ)) из пакета 13 содержания, чтобы получить действительное содержание 12, которое затем фактически представляется.

Публикация цифрового содержания

На фиг.3 представлена функциональная структурная схема одного варианта осуществления системы и способа согласно изобретению для публикации цифрового содержания. Под "публикацией" в данном контексте подразумевается процесс, который выполняется приложением или службой для установления с доверенным объектом набора прав и условий, которые данный объект может предоставить для данного содержания, а также кому эти права и условия могут быть предоставлены. Согласно изобретению процесс публикации включает в себя шифрование цифрового содержания и связывание с ним перечня постоянных осуществляемых прав, которые автор содержания предназначил для всех пользователей содержания. Этот процесс можно выполнять защищенным образом, чтобы воспрепятствовать доступу к любому из прав или к содержанию, если это не предполагается автором содержания.

В одном варианте изобретения могут, в частности, использоваться три объекта для публикации защищенного цифрового содержания: приложение 302 подготовки содержания, которое выполняется на клиентском устройстве 300 и готовит содержание к публикации; интерфейс 306 прикладной программы (ИПП) цифрового управления правами (ЦУП), который также находится на клиентском устройстве 300, и сервер 320 ЦУП, который связан с возможностью обмена данными с клиентом 300 через коммуникационную сеть 330. В одном варианте изобретения коммуникационной сетью 330 является Интернет, хотя понятно, что коммуникационная сеть 330 может быть любой локальной или глобальной сетью, например, внутренней корпоративной сетью.

Приложение 302 подготовки содержания может быть любым приложением, которое создает цифровое содержание. Например, приложение 302 может быть текстовым процессором или другим сервером публикаций, который создает цифровые текстовые файлы, цифровую музыку, видео или другое содержание такого рода. Это содержание также может быть потоковым содержанием, например, потоковым аудио/видео сигналом передаваемого прямо или записанного на пленку события. Согласно изобретению приложение подготовки содержания предлагает пользователю зашифровать содержание с помощью ключа, который предоставляет пользователь. Приложение 302 использует этот ключ для шифрования цифрового содержания, чтобы создать файл 304 зашифрованного цифрового содержания. Клиентское приложение также предлагает пользователю предоставить данные прав для файла 304 цифрового содержания. Данные прав включают в себя идентификационную информацию для каждого объекта, который обладает правами на цифровое содержание.

Таким объектом может быть, например, человек, класс людей или устройство. Для каждого такого объекта данные прав также включают в себя перечень прав, которыми обладает данный объект на содержание, и любые условия, которые могут налагаться на все или на любое из этих прав. Такие права могут включать в себя право на чтение, редактирование, копирование, распечатку и т.п. цифрового содержания. Кроме того, права могут быть включительными или исключительными. Включительные права указывают, что определенный пользователь имеет определенное право на содержание (например, пользователь может редактировать цифровое содержание). Исключительные права указывают, что определенный пользователь имеет все права на содержание за исключением тех, которые указаны (например, пользователь может делать с цифровым содержанием все, кроме копирования).

Согласно одному варианту изобретения клиентский ИПП 306 может передать зашифрованное цифровое содержание и данные прав в сервер 320 ЦУП. С помощью процесса, подробно описанного ниже, сервер 320 ЦУП определяет, может ли он исполнять

права, которые предоставлены пользователю, и если да, то сервер 320 ЦУП подписывает данные прав для создания подписанной метки 308 прав (ПМП). Однако обычно любой доверенный объект может подписать данные прав, предпочтительно используя ключ, доверенный сервером 320 ЦУП. Например, клиент может подписать данные прав, используя ключ, предоставленный ему сервером 320 ЦУП. Метка 308 прав может включать в себя данные, представляющие описание прав, зашифрованный ключ содержания и цифровую подпись на описании прав и зашифрованном ключе содержания. Если сервер ЦУП подписывает метку прав, он передает подписанную метку 308 прав обратно клиенту через клиентский ИПП 306, который сохраняет подписанную метку 308 прав в клиентском устройстве 300. Затем приложение 302 подготовки содержания связывает подписанную метку 308 прав с файлом 304 зашифрованного цифрового содержания. Например, ПМП 308 может быть объединена с файлом зашифрованного цифрового содержания для создания файла 310 управляемого правами содержания.

Однако обычно не требуется объединять данные прав с цифровым содержанием. Например, данные прав могут храниться в известном месте, а с зашифрованным цифровым содержанием может быть объединена ссылка на сохраненные данные прав. Эта ссылка может включать в себя идентификатор, который указывает, где хранятся данные прав (например, информационный склад, который содержит данные прав), и идентификатор, который соответствует этим конкретным данным прав в этом конкретном месте хранения (например, который идентифицирует файл, содержащий конкретные, представляющие интерес данные прав). Управляемое правами содержание 310 можно затем передать любому объекту в любое место, и только те объекты, которые имеют права на потребление этого содержания, могут делать это и только в соответствии с правами, которые им предоставлены.

На фиг.4 представлен алгоритм выполнения примерного способа 400 согласно изобретению для публикации управляемого правами цифрового содержания, в котором метку прав подписывает сервер ЦУП. Однако следует понимать, что этот вариант является всего лишь примером и что метку прав может подписывать в общем любой доверенный объект. Обычно способ согласно изобретению для публикации цифрового содержания может включать в себя следующие операции: шифрование цифрового содержания с использованием ключа содержания (КС), формирование описания прав, связанного с цифровым содержанием, шифрование ключа содержания (КС) согласно открытому ключу для сервера ЦУП (ОК-ЦУП), чтобы получить (ОК-ЦУП(КС)), и создание цифровой подписи на основании личного ключа (ЛК-ЦУП), соответствующего (ОК-ЦУП) для комбинации описания прав и (ОК-ЦУП(КС)).

На этапе 402 приложение 302 формирует ключ содержания (КС), который используется для шифрования цифрового содержания. Ключ содержания (КС) предпочтительно является симметричным ключом, хотя в общем можно использовать любой ключ для шифрования цифрового содержания. Алгоритмы симметричного ключа, которые иногда называют "алгоритмами секретного ключа", используют тот же самый ключ для дешифрирования сообщения, которым они шифруют сообщение. По этой причине предпочтительно, чтобы (КС) был секретным. Совместное использование (КС) отправителем и получателем должно осуществляться с большой осторожностью, чтобы исключить несанкционированный перехват такого (КС). Так как (КС) используется совместно шифратором и дешифратором, (КС) предпочтительно передается до того, как будут переданы какие-либо зашифрованные сообщения.

Хорошо известно несколько алгоритмов формирования симметричного ключа. В одном варианте используется стандарт шифрования данных (СШД, DES), хотя понятно, что можно использовать любой симметричный алгоритм. Примеры таких алгоритмов симметричного ключа включают в себя, не ограничиваясь перечисленным, AES, Triple-DES, Международный алгоритм шифрования данных (IDEA), Cast, Cast-128, RC4, RC55 и SkipJack.

На этапе 404 приложение 302 шифрует цифровое содержание симметричным ключом

содержания (КС) для образования зашифрованного цифрового содержания 304, которое может быть записано с использованием нотации (СК(содержание)). Автор, использующий приложение 302, может также формировать данные прав, связанные с цифровым содержанием. Данные прав могут включать в себя перечень объектов, которым будет предоставлено право потребления содержания, и конкретные права, которыми обладает каждый из объектов в отношении этого содержания, вместе с любыми условиями, которые могут налагаться на эти права. Такие права могут, например, включать в себя просмотр содержания, распечатку содержания и т.п. Приложение 302 передает данные прав в ИПП (API) 306. В Приложении 1 представлен пример данных прав в формате XML/XrML.

На этапе 406 ИПП 306 формирует второй ключ шифрования (СШД1), который используется для шифрования ключа содержания (КС). Предпочтительно (СШД1) также является симметричным ключом. На этапе 408 ИПП 306 шифрует (КС) с помощью (СШД1), чтобы получить (СШД1(КС)). На этапе 410 ИПП 306 отбрасывает (КС), в результате чего (КС) теперь можно будет получить только с помощью дешифрирования (СШД1(КС)). Чтобы гарантировать, что (СК(содержание)) защищено в центральном сервере 320 ЦУП и что все "запросы на лицензию" для данного содержания делаются централизованно в соответствии с данными прав, ИПП 306 на этапе 412 контактирует с предоставленным сервером 320 ЦУП и извлекает его открытый ключ (ОК-ЦУП). На этапе 414 ИПП 403 шифрует (СШД1) с помощью (ОК-ЦУП), чтобы получить (ОК-ЦУП(СШД1)). Таким образом, (КС) может быть защищен (ОК-ЦУП), чтобы гарантировать, что сервер 320 ЦУП является единственным объектом, который сможет получить доступ к (КС), когда он потребуется для расшифровки (КС(содержание)). На этапе 416 ИПП 306 шифрует данные прав (т.е. перечень санкционированных объектов и соответствующие права и условия, связанные с каждым санкционированным объектом в перечне) с помощью (СШД1), чтобы получить (СШД1(данные прав)).

В альтернативном варианте (КС) можно использовать для прямого шифрования данных прав, чтобы получить (СК(данные прав)), а (ОК-ЦУП) можно использовать для прямого шифрования (КС), чтобы получить (ОК-ЦУП(КС)), тем самым предшествуя использованию (СШД1) полностью. Однако использование (СШД1) для шифрования данных прав и (КС) позволяет такому (СШД1) соответствовать любому конкретному алгоритму, который может быть доступен для сервера ЦУП, тогда как (КС) может быть указан объектом независимо от сервера ЦУП и может быть не доступен для него.

На этапе 418 приложение 302 защиты содержания может послать (ОК-ЦУП(СШД1)) и (СШД1(данные прав)) в сервер 320 ЦУП как метку прав для подписания. Альтернативно, сам клиент может подписать данные прав. Если данные прав посылаются в сервер для подписания, то на этапе 420 сервер ЦУП 320 осуществляет доступ к данным прав и проверяет, может ли он осуществлять права и условия в представленной метке прав. Для проверки, что он может осуществить данные прав, ЦУП сервер 320 применяет (ЛК-ЦУП) к (ОК-ЦУП(СШД1)), чтобы получить (СШД1), и затем применяет (СШД1) к (СШД1(данные прав)), чтобы получить открыто данные прав. Затем сервер 320 может применить любую стратегию проверки, чтобы проверить, подпадают ли пользователи, права и условия, указанные в данных прав, под стратегию, осуществляемую сервером 320. Сервер 320 подписывает первоначально представленную метку прав, включающую (ОК-ЦУП(СШД1)) и (СШД1(данные прав)), чтобы получить подписанную метку 308 прав (ПМП), в которой подпись основана на личном ключе сервера 320 ЦУП (ЛК-ЦУП), и возвращает ПМП 308 обратно в ИПП 306, который затем передает возвращенную ПМП 308 в клиентское приложение 302.

ПМП 308 представляет собой документ с цифровой подписью, которая защищает его от подделки. Кроме того, ПМП 308 не зависит от действительного типа ключа и алгоритма, использованного для шифровки содержания, но сохраняет точное однозначное отношение к содержанию, которое она защищает. Как изображено на фиг.4А, в одном варианте настоящего изобретения ПМП 308 может включать в себя информацию о содержании, которое является основой ПМП 308, включая, возможно, идентификатор (ИД) содержания,

информацию о сервере ЦУП, который подписывает ПМП 308, включая (ОК-ЦУП(СШД1)), и ссылочную информацию, такую как URL, для определения места сервера ЦУП в сети и информацию об отказе в случае отказа URL, информацию, описывающую саму ПМП 308, (СШД1(данные прав)):(СШД1(КС)), и С(ЛК-ЦУП), помимо всего прочего. В Приложении 2 представлен образец ПМП 308 в формате XML/XrML.

Посредством гарантии того, что доверенный объект подписывает данные прав для создания подписанной метки 308 прав, сервер ЦУП обеспечивает выдачу лицензий на содержание в соответствии с условиями, выдвинутыми сервером публикаций, которые описаны в данных прав метки 308 прав. Понятно, что пользователь должен получить лицензию на представление содержания, особенно в силу того, что лицензия содержит ключ содержания (КС). Когда пользователь желает получить лицензию на зашифрованное содержание, он может представить запрос на лицензию, включающий в себя ПМП 308 для данного содержания и сертификат, подтверждающий мандат пользователя серверу ЦУП 320 или другому выдающему лицензию объекту. Тогда выдающий лицензию объект может дешифровать (ОК-ЦУП(СШД1)) и (СШД1(данные прав)), чтобы получить данные прав, список всех прав, предоставленных автором (если таковой имеется) запрашивающему лицензию объекту, и сформировать лицензию только с этими конкретными правами.

Предпочтительно, приложение 302 после получения ПМП 308 соединяет подписанную метку 308 прав с соответствующим (СК(содержание)) 304 для формирования управляемого правами цифрового содержания. Альтернативно, данные прав можно сохранить в известном местоположении со ссылкой на это местоположение, передаваемой вместе с зашифрованным цифровым содержанием. Таким образом, представляющее (визуализирующее) приложение, приводимое в действие ЦУП, может обнаружить подписанную метку 308 прав через часть содержания, которое оно пытается представить. Это обнаружение запускает представляющее приложение, которое инициирует запрос на лицензию к выдавшему лицензию серверу ЦУП 320. Публикующее приложение 302 может, например, хранить URL в выдавшем лицензию сервере 320 ЦУП, или выдавший лицензию сервер 320 ЦУП может ввести свой собственный URL как часть метаданных в метку прав до ее цифрового подписания, так что ИПП 306 клиента ЦУП, вызванный представляющим приложением, может идентифицировать правильный выдавший лицензию сервер 320 ЦУП. Предпочтительно, чтобы в метку прав до ее подписания вводился, например, глобально уникальный идентификатор (ГУИД).

В одном варианте изобретения можно использовать простой протокол доступа к объекту (ППДО) для связи между приложением 302 защиты содержания или представляющим приложением и сервером 320 ЦУП. Кроме того, могут быть предусмотрены библиотеки ИПП, такие как ИПП 306, так что приложения, такие как приложение 302, не будут должны реализовывать клиентскую сторону протокола ЦУП, а будут только делать вызовы локального ИПП. Предпочтительно, для описания прав, лицензий и меток прав для цифрового содержания используется язык XrML, XML, хотя понятно, что можно использовать любой пригодный формат для описания прав и других данных.

Получение лицензии на опубликованное содержание

На фиг.5 представлена функциональная структурная схема одного варианта системы и способа согласно изобретению для получения лицензии на управляемое правами цифровое содержание. Под "получением лицензии" в данном контексте подразумевается процесс, которому следуют приложение или служба для запроса и получения лицензии, которая позволит объекту, названному в лицензии, потреблять содержание в соответствии с условиями, определенными в лицензии. Входные данные процесса получения лицензии могут включать в себя подписанную метку прав (ПМП) 308, связанную с содержанием, на которое запрашивается лицензия, и сертификат(ы) открытого ключа объекта, для которого запрашивается лицензия. Следует отметить, что объект, запрашивающий лицензию, не обязательно должен быть объектом, для которого запрашивается лицензия. Обычно лицензия включает в себя описание прав из ПМП 308, зашифрованный ключ, который может расшифровать зашифрованное содержание, и цифровую подпись на описании прав

и зашифрованном ключе. Цифровая подпись подтверждает, что названные объекты и права являются законными.

Один путь использования приложением 302 управляемого правами содержания 310 заключается в передаче клиентским ИПП 306 подписанной метки 308 прав управляемого правами содержания 310 в сервер 320 ЦУП через коммуникационную сеть 330. Местонахождение сервера ЦУП 320 можно найти, например, в ссылочной информации в ПМП 308. В таком варианте осуществления выдающий лицензию сервер 320 ЦУП, посредством процесса, который будет подробно описан ниже, может использовать описание прав в метке прав, чтобы определить, может ли он выдать лицензию, и если да, получить описание прав для включения его в лицензию.

Как было описано выше, метка 308 прав содержит ключ содержания (КС), зашифрованный согласно открытому ключу сервера ЦУП 320 (ОК-ЦУП), (т.е. (ОК-ЦУП(КС)). В процессе выдачи лицензии сервер 320 ЦУП защищенным образом дешифрирует это значение для получения (КС). Затем он использует открытый ключ (ОК-ОБЪЕКТ) в сертификате открытого ключа, который передан в запросе на лицензию, для повторного шифрования (КС) (т.е.(ОК-ОБЪЕКТ(КС))). Вновь зашифрованный (ОК-ОБЪЕКТ(КС)) является тем, который сервер 320 помещает в лицензию. Таким образом, лицензия может быть возвращена запросившему без риска открытия (КС), поскольку только держатель связанного с нею личного ключа (ЛК-ОБЪЕКТ) сможет восстановить (КС) из (ОК-ОБЪЕКТ(КС)). Клиентский ИПП 306 затем использует (КС) для расшифровки зашифрованного содержания, чтобы получить расшифрованное цифровое содержание 312. После этого клиентское приложение может использовать расшифрованное цифровое содержание 312 в соответствии с правами, которые предоставляются в лицензии.

Альтернативно, клиент, такой как публикующий клиент, может, например, выдать собственную лицензию на использование содержания. В таком варианте защищенный процесс может выполняться на клиентском компьютере, который предоставляет клиенту ключ(и), необходимый для расшифровки цифрового содержания, при соответствующих обстоятельствах.

На фиг.6А и 6В представлен алгоритм выполнения одного варианта способа 600 согласно изобретению для выдачи лицензии на управляемое правами цифровое содержание. Согласно изобретению запрашивающий объект может подать запрос на лицензию от имени одного или нескольких потенциальных лицензиатов. Запрашивающий объект может быть одним из потенциальных лицензиатов. Потенциальным лицензиатом может быть человек, группа, устройство или любой такой объект, который может использовать содержание любым способом. Способ 600 будет в дальнейшем описан со ссылкой на вариант, в котором сервер ЦУП обрабатывает запрос на лицензию, хотя понятно, что обрабатывать запрос на лицензию и прямо выдавать лицензию может клиент.

На этапе 602 выдающий лицензию объект, например, такой как сервер ЦУП, получает запрос на лицензию. Запрос на лицензию предпочтительно содержит либо сертификат открытого ключа, либо именование для каждого из одного или более запрашивающих лицензиатов.

На этапе 604 аутентифицируется запрашивающий объект (т.е. объект, сделавший запрос на лицензию). Согласно одному варианту изобретения выдающий лицензию объект может быть сконфигурирован для использования протокольной (например, "оклик-отзыв") аутентификации для определения идентичности запрашивающего объекта, или он может быть сконфигурирован так, чтобы не требовать аутентификацию запрашивающего объекта ("разрешающий анонимную аутентификацию"). Когда требуется аутентификация, может использоваться любой тип схемы аутентификации (например, упомянутая выше схема "оклик-отзыв", схема "идентификатор и пароль пользователя", такая как MICROSOFT.NET, PASSPORT, авторизация WINDOWS, x509, и т.п.). Предпочтительно, разрешается анонимная аутентификация, а также поддержка любой схемы протокольной аутентификации, поддерживаемой комплексными информационными системами. В результате этапа аутентификации будет получена идентификационная информация, такая

как "анонимная" идентификационная информация (при анонимной аутентификации) или, например, именование личного счета. Если запрос на лицензию невозможно аутентифицировать по любой причине, то возвращается ошибка и лицензия не выдается.

На этапе 606 санкционируется объект аутентификации, т.е. определяется, разрешено ли объекту, аутентифицированному на этапе 608, запрашивать лицензию (от себя или от имени другого объекта). Предпочтительно, выдающий лицензию объект хранит список объектов, которым разрешено (или не разрешено) запрашивать лицензию. В одном варианте идентификационная информация в этом списке объектов является идентификационной информацией объекта, сделавшего запрос, а не идентификационной информацией объекта, для которого запрашивается лицензия, хотя она может быть идентификационной информацией любого из них. Например, идентификационной информации личного счета может быть не разрешено прямо делать запрос на лицензию, но процесс доверенного сервера может сделать запрос на лицензию от имени такого объекта.

Согласно изобретению запрос на лицензию может включать в себя либо сертификат открытого ключа, либо идентификационную информацию для каждого потенциального лицензиата. Если лицензия запрашивается всего для одного лицензиата, называется всего один сертификат или идентификационная информация. Если лицензия запрашивается для нескольких лицензиатов, сертификат или идентификационная информация могут быть названы для каждого потенциального лицензиата.

Предпочтительно, выдающий лицензию объект имеет сертификат открытого ключа для каждой действительной лицензии. Однако приложение 302 может пожелать сформировать лицензию для данного пользователя, но оно может не иметь доступа к сертификату открытого ключа для данного пользователя. В такой ситуации приложение 302 может указать идентификационную информацию пользователя в запросе на лицензию, и в результате выдающий лицензию объект сможет вызвать зарегистрированный интегрированный (встраиваемый) модуль сертификатов, который выполняет просмотр в службе каталога и возвращает соответствующий сертификат открытого ключа пользователя.

Если на этапе 608 выдающий лицензию объект определяет, что сертификат открытого ключа не включен в запрос на лицензию, то он использует указанную идентификационную информацию для выполнения просмотра в службе каталога или базе данных для соответствующего сертификата открытого ключа. Если на этапе 610 выдающий объект определит, что сертификат присутствует в каталоге, то на этапе 612 извлекается этот сертификат. В одном варианте встраиваемый модуль сертификатов используется для извлечения сертификатов открытого ключа из службы каталога с помощью протокола доступа к каталогу. Если сертификат для данного потенциального лицензиата невозможно найти ни в запросе, ни в каталоге, то сервер лицензий не формирует лицензию для этого потенциального лицензиата, и на этапе 614 запросившему объекту возвращается ошибка.

Предполагая, что выдающий лицензию объект имеет сертификат открытого ключа для по меньшей мере одного потенциального лицензиата, тогда на этапе 616 выдающий лицензию объект подтверждает доверие сертификатам лицензиата. Выдающий лицензию объект предпочтительно сконфигурирован с набором сертификатов доверенного выдающего сертификаты объекта, и он определяет, есть ли выдающий сертификаты лицензиата в списке доверенных выдающих сертификаты объектов. Если на этапе 616 выдающий лицензию объект определит, что выдающий сертификаты лицензиата объект отсутствует в списке доверенных выдающих объектов, то запрос на эту лицензию отклоняется, и формируется ошибка на этапе 614. Таким образом, потенциальный лицензиат, сертификат которого не выдан доверенным выдающим лицензию объектом, не получит лицензию.

Кроме того, выдающий лицензию объект предпочтительно выполняет подтверждение цифровой подписи на всех объектах в цепи сертификата, идущей от сертификатов доверенного выдающего объекта до сертификатов открытого ключа отдельных

лицензиатов. Процесс подтверждения цифровых подписей в цепи является известным алгоритмом. Если не подтвержден сертификат открытого ключа для данного потенциального лицензиата или не подтвержден сертификат в цепи, то потенциальный лицензиат не получает доверия и поэтому ему не выдается лицензия. В противном случае на этапе 618 может быть выдана лицензия. Процесс повторяется на этапе 620 до тех пор, пока не будут обработаны все объекты, для которых была запрошена лицензия.

Как видно на фиг.6В, выдающий лицензию объект приступает к подтверждению подписанной метки 308 прав, которая принята в запросе на лицензию. В одном варианте выдающий лицензию объект может использовать встраиваемый модуль метки прав и вспомогательную базу данных для хранения на сервере эталона каждой метки прав, подписанной данным выдающим лицензию объектом. Метки прав идентифицированы ГУИД, помещенным в них при публикации. Во время выдачи лицензии (на этапе 622) выдающий объект просматривает метку прав, введенную в запрос на лицензию, и извлекает ее ГУИД. Затем он передает ГУИД в встраиваемый модуль метки прав, который выдает запрос к базе данных для извлечения копии основной метки прав. Основная метка прав может быть более современной, чем копия метки прав, посланная в запросе на лицензию, и эта метка прав будет использоваться в запросе на следующих этапах. Если метка прав не обнаружена в базе данных на основе ГУИД, то выдающий лицензию объект проверяет свою стратегию на этапе 624, чтобы определить, разрешено ли ему еще выдавать лицензию на основе метки прав в запросе. Если стратегия этого не позволяет, запрос на лицензию будет отклонен на этапе 626 и будет возвращена ошибка в ИПП 306 на этапе 628.

На этапе 630 выдающий лицензию объект подтверждает метку 308 прав. При этом подтверждается цифровая подпись на метке прав, и если выдающий лицензию объект не является объектом, выдавшим метку прав (объектом, который ее подписал), то он определяет, не является ли объект, выдавший метку прав, другим доверенным объектом (например, объектом, с которым выдающий лицензию объект может совместно использовать материал ключа). Если метка прав не подтверждена или если она не выдана доверенным объектом, то запрос на лицензию отклоняется на этапе 626 и на этапе 628 возвращается ошибка в ИПП 306. После того, как произойдут все подтверждения, выдающий лицензию объект преобразует метку 308 прав в лицензию для каждого подтвержденного лицензиата. На этапе 632 выдающий лицензию объект формирует соответствующее описание прав для лицензии, подлежащей выдаче каждому лицензиату. Для каждого лицензиата выдающий лицензию объект оценивает идентификационную информацию, названную в сертификате открытого ключа этого лицензиата по сравнению с идентификационными данными, названными в описании прав в метке прав. Описание прав присваивает каждому праву или набору прав набор идентификационных данных, которые могут осуществлять это право или набор прав в лицензии. Для каждого права или набора прав, с которым связана данная идентификационная информация лицензиата, это право или набор прав копируется в новую структуру данных для данной лицензии. Полученная структура данных является описанием прав в лицензии для конкретного лицензиата. Как часть этого процесса выдающий лицензию объект оценивает любые предварительные условия, которые могут быть связаны с любым правом или набором прав в описании прав в метке прав. Например, это право может быть временным предусловием, связанным с ним, которое не разрешает выдающему лицензию объекту выдавать лицензию после истечения определенного времени. В этом случае выдающий лицензию объект должен будет проверять текущее время, и если прошло время, указанное в предусловии, выдающий лицензию объект не сможет предоставить это право лицензиату, даже если бы именование лицензиата было связано с этим правом.

На этапе 636 выдающий лицензию объект принимает (ОК-ЦУП(СШД1)) и (СШД1(КС)) из метки 308 прав и применяет (ЛК-ЦУП) для получения (КС). Выдающий лицензию объект затем снова шифрует (КС), используя (ОК-ОБЪЕКТ) сертификата открытого ключа лицензиата, для получения (ОК-ОБЪЕКТ(КС)). На этапе 638 выдающий лицензию объект

соединяет сформированное описание прав с (ОК-ОБЪЕКТ(КС)) и делает цифровую подпись на полученной структуре данных, используя (ЛК-ЦУП). Эта подписанная структура данных является лицензией для данного конкретного лицензиата.

На этапе 640 выдающий лицензию объект определяет, нужно ли еще формировать лицензии для данного конкретного запроса, и соответственно не формирует больше лицензий или формирует еще. Сформированные лицензии возвращаются запрашивающему объекту на этапе 643 вместе с цепью сертификата, связанной с этими лицензиями (например, сертификат собственного открытого ключа сервера, а также сертификат, который выдал этот сертификат и т.д.).

В одном варианте системы согласно изобретению может быть использовано множество ключей лицензиара. В таком варианте ключ содержания (КС), который проходит зашифрованным через метку 308 прав и в лицензию, может в действительности быть представлен любыми произвольными данными. Один особенно полезный вариант заключается в том, чтобы использовать множество отдельных зашифрованных ключей содержания (КС), связанных соответственно с различными правами или различными принципалами (пользователями или процессами, имеющими учетную запись) в описании прав. Например, цифровая версия музыкальных произведений в альбоме может быть вся зашифрована различными ключами (КС). Эти ключи (КС) будут включены в одну и ту же метку прав, но один принципал может иметь право воспроизводить одно из музыкальных произведений (например, он может иметь право получить только один ключ в его лицензии), а другой принципал может иметь право воспроизводить все музыкальные произведения (он будет иметь право получить все ключи в его лицензии).

Предпочтительно, система согласно изобретению позволяет публикующим приложениям/пользователям именовать группы или классы лицензиатов в метке 308 прав. В таком варианте выдающий лицензию объект будет оценивать любые группы/классы, названные в метке прав, чтобы определить, является ли текущая идентификационная информация лицензиата членом этих групп/классов. Если членство в названной группе/классе обнаружено, выдающий лицензию объект может добавить права или группу прав, связанных с данной группой/классом, к структуре данных описания прав, использованной для лицензии.

В одном варианте изобретения интерфейсы протоколов публикации и выдачи лицензии в сервере ЦУП поддерживают аутентификацию и авторизацию вызывающего приложения или пользователя, и административный пульт сервера ЦУП позволяет администратору формировать список управления доступом для интерфейсов выдачи лицензии и публикации. Это позволяет потребителю сервера применять стратегию, при которой пользователям/приложениям разрешено либо публиковать, либо выдавать лицензию, либо и то и другое.

Изменение или переиздание подписанной метки 308 прав

В одном варианте настоящее изобретение ПМП 308 может быть "переиздана", если пользователь содержания получил на это разрешение. То есть, если это позволено, пользователь может изменить данные прав в ПМП 308. Конечно, такое разрешение на изменение данных прав следует выдавать сдержанно и осторожно, особенно потому, что пользователь с разрешением изменить данные прав может, по существу, присвоить себе широкие права на соответствующее содержание. Понятно, что такой пользователь может даже предоставить себе право на открытие содержания и передачи его для открытого пользования.

В данном случае разрешение на изменение обозначается путем включения вместе с данными прав в ПМП 308 индикации, что конкретный пользователь или класс пользователей может фактически изменить или "переиздать" данные прав и метку 308 прав. Когда сервер 320 ЦУП получает ПМП 308 с таким разрешением в связи с запросом на лицензию, он включает в запрашиваемую лицензию для пользователя симметричный ключ (СШД1), зашифрованный согласно открытому ключу пользователя (т.е. ОК-ОБЪЕКТ), чтобы получить (ОК-ОБЪЕКТ(СШД1)).

Таким образом, чтобы отредактировать данные прав в ПМП 308, как проиллюстрировано на фиг.7, пользователь извлекает (ОК-ОБЪЕКТ(СШД1)) из лицензии (этап 701), применяет (ЛК-ОБЪЕКТ) к нему, чтобы получить (СШД1) (этап 703), извлекает (СШД1(данные прав)) из ПМП 308 (этап 705) и применяет к нему (СШД1), чтобы получить данные прав (этап 707). После этого пользователь изменяет данные прав, как он желает (этап 709), и передает измененные данные прав в сервер 320 ЦУП, как было описано выше в связи с фиг.4, чтобы получить подписанную метку 308 прав (этап 711). Конечно, при этом подписанная метка 308 прав фактически является переизданной ПМП 308, и соответственно после получения ПМП 308 (этап 713) пользователь удаляет первоначальную ПМП 308, присоединенную к соответствующему содержанию (этап 715), а затем присоединяет переизданную ПМП 308 к этому содержанию (этап 717).

Таким образом, можно понять, что переиздание ПМП 308 позволяет пользователю обновить данные прав в ПМП 308, включая права, условия и пользователей, без изменения связанного с ними содержания. В частности, переиздание не требует повторного шифрования связанного с нею содержания новым (КС). Также переиздание не требует создания новой ПМП с нуля, особенно, поскольку первоначальная ПМП 308 содержит множество элементов, которые можно скопировать в новую ПМП 308.

Самостоятельная публикация подписанной метки 308 прав

В одном варианте настоящего изобретения ПМП 308 может быть подписана самим запрашивающим пользователем. Соответственно, пользователю не надо контактировать с сервером 320 ЦУП для получения ПМП 308 для соответствующего содержания. В результате самостоятельную публикацию можно также назвать автономной публикацией. В таком варианте от пользователя может потребоваться контакт с сервером 320 ЦУП, чтобы запросить лицензию на основе такой самостоятельно опубликованной ПМП 308. Понятно, что публикующему объекту может быть предоставлена возможность выдавать свои собственные лицензии.

В частности, как показано на фиг.8, в этом варианте пользователю сначала предоставляется возможность самостоятельной публикации путем получения из сервера 320 ЦУП сертификата 810 ЦУП, включающего в себя открытый ключ (ОК-СЕРТ) и соответствующий личный ключ (ЛК-СЕРТ), зашифрованный согласно открытому ключу пользователя (ОК-ОБЪЕКТ), чтобы получить (ОК-ОБЪЕКТ(ЛК-СЕРТ)). Сертификат должен быть подписан личным ключом сервера 320 ЦУП (ЛК-ЦУП), чтобы сервер 320 ЦУП мог проверить его, как будет более подробно описано ниже. Понятно, что сертификат 810 ЦУП разрешает пользователю самостоятельную публикацию. Также понятно, что пара ключей (ОК-СЕРТ, ЛК-СЕРТ) является отдельной от (ОК-ОБЪЕКТ, ЛК-ОБЪЕКТ) и используется специально для самостоятельной публикации. Следует отметить, что можно обойтись без пары ключей (ОК-СЕРТ, ЛК-СЕРТ), в этом случае сертификат 810 ЦУП включает в себя только открытый ключ пользователя (ОК-ОБЪЕКТ) и подписан личным ключом сервера 320 ЦУП (ЛК-ЦУП), так что сервер 320 ЦУП может его проверить.

Самостоятельная публикация отличается от публикации, показанной на фиг.4, тем, что пользователь по существу занимает место сервера 320 ЦУП в отношении выполняемых им операций. Что важно, пользователь подписывает представленную метку прав, включающую (ОК-ЦУП(СШД1)) и (СШД1(данные прав)), с помощью (ОК-СЕРТ), полученного из сертификата 810 ЦУП (т.е. С(ЛК-СЕРТ)), чтобы получить подписанную метку 308 прав (ПМП). Понятно, что пользователь получает (ЛК-СЕРТ) из сертификата 810 ЦУП путем получения (ОК-ОБЪЕКТ(ЛК-СЕРТ)) из такого сертификата 810 ЦУП и применения к нему (ЛК-ОБЪЕКТ). Следует отметить, что пользователь не может проверить, что сервер 320 ЦУП может осуществить права в представленной метке прав, особенно, поскольку пользователь не должен иметь (ЛК-ЦУП) для применения к (ОК-ЦУП(СШД1)). Соответственно, сам сервер 320 ЦУП должен выполнить проверку в то время, когда запрашивается лицензия на основании самостоятельно опубликованной ПМП 308.

После того, как пользователь осуществит самостоятельную публикацию ПМП 308, он присоединяет такую самостоятельно опубликованную ПМП 308 и сертификат 810 ЦУП,

использованный для ее получения, к содержанию, и такое содержание с ПМП 308 и сертификатом 810 распространяется другому пользователю. После этого другой пользователь запрашивает и получает лицензию на содержание от сервера 320 ЦУП практически таким же образом, как показано на фиг.6А и 6В. Но при этом запрашивающий лицензию пользователь передает в сервер 320 ЦУП как самостоятельно опубликованную ПМП 308, так и сертификат 810 ЦУП, присоединенный к содержанию. Затем сервер 320 ЦУП проверяет С(ЛК-ЦУП) в сертификате 810 ЦУП на основании соответствующего (ОК-ЦУП) и получает (ОК-СЕРТ) из сертификата 810 ЦУП. После этого сервер 320 ЦУП проверяет С(ЛК-СЕРТ) в ПМП 308 на основании полученного (ОК-СЕРТ) и продолжает описанную выше процедуру. Следует отметить, что поскольку пользователь не проверяет, может ли сервер 320 ЦУП осуществлять права в ПМП 308, как было указано выше, в это время сервер 320 ЦУП сам должен выполнять проверку.

Шаблон прав

Как указано выше, пользователю предоставлена свобода в формировании большей части данных прав в метке прав путем определения пользователей или классов пользователей, определения прав для каждого определенного пользователя или класса пользователей, и определения любых условий использования. Однако, что важно, может быть обременительным многократно определять данные прав для множества меток прав, особенно когда одни и те же пользователи или классы пользователей, права и условия определяются многократно для различных содержаний. Такая ситуация может, например, иметь место в корпоративной или учрежденческой среде, где пользователь многократно публикует различные содержания, которые должны использоваться совместно с конкретно определенной группой пользователей. В такой ситуации согласно одному варианту настоящего изобретения создается шаблон прав, который пользователь может многократно использовать в связи с созданием меток прав, при этом шаблон прав уже включает в себя заранее определенный набор пользователей или классов пользователей, заранее определенные права для каждого определенного пользователя или класса пользователя и заранее определенные условия использования.

В одном варианте настоящего изобретения, проиллюстрированном на фиг.9, шаблон 900 прав имеет практически такие же самые данные прав, как и метка прав. Однако, так как (СШД1) не известен до тех пор, пока не будет опубликовано содержание, данные прав невозможно зашифровать с помощью (СШД1), как в случае метки прав. При этом в одном варианте настоящего изобретения шаблон 900 прав с незашифрованными данными прав предоставляется в ходе шифрования данных прав с помощью (СШД1) на этапе 416 на фиг.4 для получения (СШД1(данные прав)). Конечно, данные прав извлекаются из предоставленного шаблона 900 прав перед тем, как они будут шифроваться.

Сервер 320 ЦУП и открытый ключ (ОК-ЦУП) могут быть известны или неизвестны в то время, когда создается шаблон прав. Кроме того, даже если они известны, может возникнуть ситуация, при которой имеется несколько серверов 320 ЦУП, каждый из которых имеет свой собственный (ОК-ЦУП). Тем не менее, и в случае, когда сервер 320 ЦУП и открытый ключ (ОК-ЦУП) известны в то время, когда создается шаблон, и в случае, когда используется всего один сервер 320 ЦУП, или всего один сервер 320 ЦУП должен использоваться в связи с шаблоном 900 прав, такой шаблон прав может также включать в себя информацию о сервере ЦУП, который должен подписывать метки прав, полученные с помощью шаблона 900 прав, включая его открытый ключ (ОК-ЦУП). Хотя такой (ОК-ЦУП) появляется в ПМП 308 как шифрующий (СШД1), чтобы получить (ОК-ЦУП(СШД1)), следует также понимать, что (СШД1) не известен до тех пор, пока содержание не будет опубликовано, и поэтому (ОК-ЦУП) в шаблоне 900 прав не может зашифровать такой (СШД1), как в случае метки прав. В одном варианте настоящего изобретения шаблон 900 прав с незашифрованным (ОК-ЦУП) предоставляется в ходе шифрования (СШД1) с помощью (ОК-ЦУП) на этапе 414 на фиг.4, чтобы получить (ОК-ЦУП(СШД1)). Конечно, (ОК-ЦУП) извлекается из предоставленного шаблона 900 прав перед его применением.

Кроме того, в упомянутом выше случае другая информация о сервере ЦУП, которая

может быть включена в шаблон прав, может также включать в себя ссылочную информацию, такую как URL, для определения места сервера ЦУП в сети, и информацию об отказе, если URL откажет. В любом случае шаблон прав может также включать в себя, помимо прочего, информацию, описывающую сам шаблон 900 прав. Следует отметить, что шаблон 900 прав может также предусматривать место для информации, релевантной для содержания, которое должно быть опубликовано, например, информацию, которая появляется в метке прав, относящейся к данному содержанию и/или шифровальным ключам (КС) и (СШД1), хотя такое место не требуется, если реализация шаблона прав действительно не преобразуется в метку прав.

Хотя шаблон 900 прав, описанный выше, в основном предназначен для удобства пользователя, понятно, что в некоторых обстоятельствах пользователь не должен иметь неограниченную свободу в определении прав в метке прав, и шаблон 900 прав можно использовать для ограничения объема или типа меток прав, которые могут быть созданы. Например, особенно в случае корпоративной или учрежденческой среды, может быть заранее определено в качестве стратегии, что конкретный пользователь должен всегда публиковать содержание только для конкретного класса пользователей, или что пользователь не должен никогда публиковать содержание для конкретного класса пользователей. В любом случае, согласно одному варианту изобретения такая стратегия реализуется в виде заранее определенных данных прав в одном или более шаблонах 900 прав, и пользователь может быть ограничен применением таких шаблонов прав для создания меток прав при публикации содержания. Примечательно, что шаблон 900 прав или группа шаблонов 900 прав, предоставленная пользователю для определения стратегии публикации для пользователя, может указывать любой конкретный тип стратегии публикации, не выходя при этом за рамки объема притязаний изобретения.

Для определения шаблона 900 прав для ограниченного пользователя или т.п., как проиллюстрировано на фиг.10, администратор или т.п. фактически создает шаблон 900 прав путем определения заранее определенных данных прав (этап 1001) и определения любых других данных, которые могут быть необходимы и существенны, например, информации, относящейся к конкретному серверу ЦУП (этап 1003). Важно, что для реализации шаблона прав для использования пользователем с ограниченным доступом или т.п. шаблон 900 прав должен быть сделан официальным. То есть, шаблон 900 прав должен быть распознаваемым как шаблон прав, который может использовать пользователь с ограниченным доступом или т.п. Соответственно, в одном варианте изобретения шаблон прав, созданный администратором или т.п., передается в сервер 320 ЦУП для подписания им, и такая подпись делает шаблон прав официальным (этап 1005).

Следует отметить, что подписывающий сервер 320 ЦУП является сервером 320 ЦУП, информация о котором находится в шаблоне 900 прав, если такая информация действительно фактически присутствует в шаблоне 900 прав. Также следует отметить, что сервер 320 ЦУП может подписать шаблон 900 прав только после выполнения любых необходимых проверок или может подписать его без каких-либо проверок вообще. И наконец, заметим, что подпись шаблона С(ЛК-ЦУП-Т) (где Т означает, что подпись предназначена для ОШП 900) из сервера 320 ЦУП должна быть основана, по меньшей мере, на заранее определенных данных прав в шаблоне 900 прав, но может быть также основана на другой информации, не выходя при этом за рамки объема изобретения. Как будет описано ниже, подпись С(ЛК-ЦУП-Т) будет введена в метку прав и проверяться в связи с нею, и соответственно, независимо от того, на чем основана подпись, она также должна быть введена в метку прав в неизмененной форме.

После подписания сервером 320 ЦУП шаблона 900 прав и возвращения его администратору или т.п. администратор получает подписанный и теперь официальный шаблон 900 прав с С(ЛК-ЦУП-Т) (этап 1007) и передает официальный шаблон прав (ОШП) 900 одному или нескольким пользователям для использования ими (этап 1009). Соответственно, чтобы опубликовать содержание на основании ОШП 900, пользователь извлекает ОШП 900 (этап 1011) и создает метку прав на основании ОШП 900 (этап 1013)

путем предоставления необходимой информации, такой как информация о содержании, информация о соответствующем ключе, данные прав из ОШП 900, зашифрованные с помощью (СШД1), чтобы получить (СШД1(данные прав)), и любая другая информация из ОШП 900. Важно то, что пользователь также включает вместе с меткой прав подпись С(ЛК-ЦУП-Т) из ОШП 900.

После этого, как и раньше, пользователь передает метку прав в сервер 320 ЦУП для подписания (этап 1015). Но при этом сервер 320 ЦУП не будет подписывать представленную метку прав без проверки С(ЛК-ЦУП-Т) в ней. То есть сервер 320 ЦУП требует, чтобы пользователь обосновал представленную метку прав на ОШП 900, отказываясь подписать представленную метку прав, если она не включает в себя подпись С(ЛК-ЦУП-Т) из ОШП 900. В частности, сервер 320 ЦУП извлекает такую С(ЛК-ЦУП-Т), и на какой бы информации не была основана такая подпись из представленной метки прав, проверяет такую подпись на основании (ОК-ЦУП). Следует отметить, что данные прав в представленной метке прав зашифрованы согласно (СШД1), т.е. (СШД1(данные прав)). Соответственно, сервер 320 ЦУП должен сначала получить (СШД1) и расшифровать (СШД1(данные прав)) с его помощью, как было указано в связи с фиг.7, чтобы можно было проверить подпись на основании данных прав в представленной метке прав.

После проверки сервер 320 ЦУП подписывает представленную метку прав с помощью С(ЛК-ЦУП-Л), чтобы получить ПМП 308, как и прежде (где Л означает, что подпись предназначена для ПМП 308). При этом С(ЛК-ЦУП-Л) может заменить С(ЛК-ЦУП-Т) или может быть дополнением к нему. Если она является дополнением, то С(ЛК-ЦУП-Л) может быть основана частично на С(ЛК-ЦУП-Т). Следует отметить, что (ЛК-ЦУП) можно использовать для получения и С(ЛК-ЦУП-Т) и С(ЛК-ЦУП-Л), или различные (ЛК-ЦУП) можно использовать для каждой из С(ЛК-ЦУП-Т) и С(ЛК-ЦУП-Л). После того, как сервер 320 ЦУП подпишет метку прав и возвратит ПМП 308 пользователю, пользователь получает ПМП 308 с С(ЛК-ЦУП-Л) (этап 1017) и приступает к соединению его с публикуемым содержанием, как и прежде.

Если подпись С(ЛК-ЦУП-Т) ОШП 900 основана, по меньшей мере частично, на заранее определенных данных прав в ОШП 900, то такие данные прав, когда они появляются в ПМП 308 (в СШД1(данные прав)), нельзя изменить. В противном случае С(ЛК-ЦУП-Т) не будет подтверждена. Тем не менее, в одном варианте настоящего изобретения данные прав в ОШП 900 можно изменять в рамках установленных правил, которые также включены в ОШП 900. Например, эти правила могут указывать один из двух наборов данных прав, подлежащий включению в ПМП 308, или могут позволять сделать выбор из нескольких альтернатив. Понятно, что правила могут быть любыми конкретными правилами, изложенными в соответствующем синтаксисе, не выходя за объем настоящего изобретения. При этом правила интерпретируются соответствующим интерпретатором для пользователя в то время, когда создается метка прав. Хотя данные прав могут изменяться, правила не изменяются подобным образом, и соответственно подпись шаблона С(ЛК-ЦУП-Т) для ОШП 900 основана, по меньшей мере частично, на правилах, а не на самих данных прав. В результате, правила, включенные в ОШП 900, должны быть также включены в ПМП 308.

В одном варианте настоящего изобретения заранее определенные данные прав в ОШП 900 являются частично постоянными и неизменными, и частично изменяемыми и управляемыми правилами, как пояснялось выше. При этом подпись шаблона С(ЛК-ЦУП-Т) для ОШП 900 основана, по меньшей мере частично, на постоянной части правил и на правилах для изменяемой части данных прав.

Понятно, что ОШП 900, которым владеет пользователь, может устареть. Это значит, что ОШП 900 может отражать через данные прав, содержащиеся в нем, стратегию, которая устарела, не подходит для данного случая или просто больше не применяется. Например, один или несколько пользователей или классов пользователей, указанных в данных прав в ОШП 900, могут больше не находиться в данной среде с такой стратегией, или конкретный пользователь или класс пользователей, указанных в данных прав ОШП 900, может больше

не иметь те же самые права в среде с такой стратегией. В таком случае администратор может выпустить пересмотренную ОШП 900, а пользователь продолжать использовать предыдущую, устаревшую версию ОШП 900.

В такой ситуации, согласно одному варианту настоящего изобретения сервер 320 ЦУП после подписания представленного шаблона 900 прав для создания ОШП 900 сохраняет копию ОШП 900, причем каждый ОШП 900 имеет уникальные идентификационные указатели, и каждая метка прав, созданная на основании ОШП 900, включает в себя идентификационные указатели ОШП 900. Соответственно, после получения представленной метки прав, как было описано в связи с фиг.10, сервер 320 ЦУП находит идентификационные указатели ОШП 900 в метке прав, извлекает самую новую копию такого ОШП 900 на основании найденных идентификационных указателей, удаляет данные прав из представленной метки прав, вводит данные прав из извлеченного ОШП 900 и затем подписывает метку прав на основании, по меньшей мере, частично, введенных данных прав. Конечно, сервер ЦУП также выполняет любое необходимое шифрование и дешифрирование, необходимое и обязательное в описанном процессе, включая дешифрирование и повторное шифрование (СШД1(данные прав)). Следует отметить, что если сервер ЦУП выполнен с возможностью замены данных прав в представленной метке прав, то такая метка прав и ОШП 900, из которого создана такая метка прав, не обязательно должны включать в себя данные прав. Вместо этого данные прав должны быть только резидентными на сервере 320 ЦУП. Однако включение данных прав с меткой прав и ОШП 900, из которого создана такая метка прав, может быть полезным для пользователя, а значит быть полезным в некоторых ситуациях.

Выдача лицензии с помощью каталога

При выдаче лицензии на защищенное содержание выдающий лицензию объект (далее именуемый как "лицензиар") обращается к присланной ПМП 308 из содержания, чтобы определить, каким пользователям/группам/совокупностям/подразделениям/платформам/и т.п. (далее именуемым как "объекты") следует предоставить права, и к присланному сертификату, чтобы идентифицировать сторону, запрашивающую лицензию. На этом основании лицензиар определяет, какие права из перечисленных в ПМП 308 следует предоставить запрашивающей стороне. По замыслу, лицензиар проверяет объекты, перечисленные в ПМП 308, и сравнивает их с запрашивающей стороной. Таким образом, если ПМП 308 указывает, что конкретная группа должна получить лицензию и что запрашивающая сторона является членом такой группы, то запрашивающей стороне предоставляется лицензия с правами, установленными для данной группы в ПМП 308. Аналогично, если ПМП 308 указывает, что конкретный пользователь должен получить лицензию и запрашивающая сторона является этим пользователем, то запрашивающей стороне предоставляется лицензия с правами, установленными для такого пользователя в ПМП 308. Понятно, что конкретная ПМП 308 может перечислять несколько объектов и права для них, и конкретная запрашивающая сторона может получить лицензию на основании того, что она является членом одного или нескольких объектов.

В одном варианте настоящего изобретения, проиллюстрированного на фиг.12, запрашивающая сторона идентифицируется в присланном сертификате 1202 с помощью идентификатора 1204, где идентификатор 1204 может быть, например, псевдонимом, которым запрашивающая сторона идентифицирована в организационном каталоге 1206. Соответственно, ПМП 308 перечисляет каждый обладающий правами объект согласно такому идентификатору 1204. Таким образом и как часть обработки запроса на лицензию 1208, лицензиар 1210 получает идентификатор 1204 запрашивающей стороны из сертификата 1202 и сравнивает полученный идентификатор 1204 со всеми идентификаторами 1204, перечисленными в присланной ПМП 308. Если обнаруживается совпадение, то лицензиар 1210 выдает лицензию 1208 запрашивающей стороне с правами, указанными в ПМП 308 для идентификатора 1204 такой запрашивающей стороны.

Более того, при доступности каталога 1206 лицензиар 1210 может также определить, является ли данная запрашивающая сторона членом любого другого объекта,

перечисленного в ПМП 308, так как предполагается, что каталог 1206 содержит соответствующую перекрестно-ссылочную информацию, которая отражает статус членства запрашивающей стороны в таком другом объекте. Обычно каталог 1206 перечисляет для каждой запрашивающей стороны не только идентификатор 1204, но также идентификатор 1208 каждой группы/совокупности/подразделения/платформы/другого объекта/т.п., членом которого является запрашивающая сторона. Следует отметить, что каталог 1206 может включать в себя такие идентификаторы 1208, как почтовый адрес, альтернативный почтовый адрес, ИД, альтернативный ИД, членство в группе, исторический идентификатор и/или т.п.

Как показано на фиг.13, при получении сертификата 1202 от запрашивающей стороны с ее идентификатором 1204 в нем и данных прав из ПМП 308, полученной от запрашивающей стороны, лицензиар 1210 выдает лицензию 1208 запрашивающей стороне следующим образом. Сначала лицензиар 1210 получает идентификатор 1204 запрашивающей стороны из полученного сертификата 1202 (этап 1301) и находит полученный идентификатор 1204 в каталоге 1206 (этап 1303). После этого лицензиар 1210 находит на основании найденного идентификатора 1204 в каталоге 1206 идентификатор 1204 каждого объекта, членом которого является запрашивающая сторона 1204 (этап 1305). Таким образом, для каждого найденного идентификатора 1204 запрашивающей стороны и всех найденных идентификаторов 1204 объекта лицензиар 1210 сравнивает такой идентификатор 1204 со всеми идентификаторами 1204, перечисленными в присланной ПМП 308 (этап 1307). И снова, если обнаружено совпадение, лицензиар 1210 выдает лицензию 1208 запрашивающей стороне с правами, указанными в ПМП 308 для совпадающего идентификатора 1204 (этап 1309a).

Следует отметить, что поскольку с ПМП 308 сравнивается множество идентификаторов 1204, может возникнуть случай, что будет найдено множество совпадающих идентификаторов 1204 в ПМП 308. В этом случае лицензиар 1210 выбирает соответствующий совпадающий идентификатор 1204 в ПМП 308 и выдает лицензию 1208 запрашивающей стороне с правами, указанными в ПМП 308 для совпадающего идентификатора 1204 (этап 1309b). Например, лицензиар может выбрать совпадающий идентификатор 1204, который предоставляет максимум прав запрашивающей стороне (этап 1309b-1). Следует отметить, что лицензиар может быть способен определить, какой совпадающий идентификатор 1204 предоставляет максимум прав, или может основываться на некотором виде приоритетных индикаторов 1212 в ПМП 308. В последнем случае каждый совпадающий идентификатор (пользователь) 1204 в ПМП 308 имеет соответствующий индикатор 1212 приоритета, и более высокий индикатор 1212, например, указывает на более широкий объем предоставляемых прав. Следовательно, если лицензиар 1210 обнаруживает множество совпадающих идентификаторов 1204 в ПМП 308, он выбирает совпадающие идентификаторы 1204, имеющие самый высокий индикатор 1212 приоритета (этап 1309b-2).

Следует отметить, что при ссылке на каталог 1206 для формирования дополнительных идентификаторов 1204, релевантных для запрашивающей стороны, лицензиар 1210 повышает вероятность того, что совпадение будет обнаружено даже в ситуации, когда, например, почтовый адрес или идентификатор запрашивающей стороны изменился со времени создания ПМП 308. В целом, каталог 1206 обеспечивает преобразование из одного идентификатора 1204 запрашивающей стороны в другой возможный идентификатор 1204 запрашивающей стороны, так что можно использовать все идентификаторы 1204 в попытке найти совпадение с идентификатором 1204 в ПМП 308.

Выдача лицензии группе

В одном варианте настоящего изобретения присланный сертификат 1202, предоставленный запрашивающей стороной, может представлять группу или множество, или некоторую другую совокупность людей (далее именуемую как "группа"), которая соответствующим образом представлена в каталоге 1206. Такая группа может быть группой, доступной по почте, например, списком распределения или почтовым

псевдонимом, или защищенной группой, например, определенной в связи с сетевой операционной системой, или т.п. Соответственно, лицензиар 1210 после получения присланного "группового" сертификата 1203 поступает по существу так, как было описано прежде. Но следует отметить, что поскольку присланный сертификат 1202 представляет конкретную группу, может возникнуть ситуация, когда выданная лицензия 1208 от лицензиара 1210 будет предназначена для группы, идентифицированной в сертификате 1202, а не для запрашивающей стороны конкретно. Альтернативно, лицензиар 1210 может определить из каталога 1206, что данная запрашивающая сторона является частью группы, идентифицированной в сертификате 1202, и в этом случае выданная лицензия 1210 будет предназначена для запрашивающей стороны.

В первом случае выданная лицензия 1208 может включать в себя ключ содержания, зашифрованный согласно открытому ключу группы, и поэтому запрашивающей стороне надо будет получить соответствующий личный ключ группы. Соответственно, запрашивающая сторона может иметь сертификат членства в группе с таким личным ключом, возможно зашифрованным согласно открытому ключу запрашивающей стороны, который можно дешифрировать согласно соответствующему личному ключу запрашивающей стороны.

Во втором случае, чтобы включить ключ содержания, зашифрованный согласно открытому ключу запрашивающей стороны в выданной лицензии 1208, лицензиар 1210 может дополнительно получить сертификат от запрашивающей стороны с таким открытым ключом. Альтернативно, лицензиар 1210 может иметь такой сертификат в наличии (см., например, этапы 608-612 на фиг.6А и 6В) и использовать открытый ключ в нем после определения из каталога 1206, что запрашивающая сторона является частью группы, идентифицированной в присланном групповом сертификате 1202.

Следует отметить, что указание прав в ПМП 308 и выдача лицензий 1208 для группы позволяет реализовать цифровое управление правами на предприятии или в организации. Например, документ или электронная почта может быть защищена ЦУП таким образом, что все члены данного отдела будут иметь право прочесть данный документ или электронную почту. Допустим, что группа (например, псевдоним в электронной почте) такого отдела существует в каталоге 1206 организации, что является наиболее распространенным случаем, тогда автор документа или электронной почты будет предоставлять права на основании группы, а не отдельным лицам. Понятно, что такая групповая выдача прав облегчает автору работу при определении классов лиц, которые обладают правами. Кроме того, при определении прав согласно группе указанные права не "устаревают", когда новые члены присоединяются к группе, а старые члены покидают группу. Вместо этого все текущие члены группы способны осуществлять права, поскольку членство такой группы поддерживается в организационном каталоге 1206 в соответствии с текущим состоянием.

Введение стратегии во время выдачи лицензии

В одном варианте настоящего изобретения, упоминаемом выше в связи с ОШП 900 на фиг.9, сервер ЦУП/лицензиар 1210 может быть способен изменять или заменять данные из представленной ПМП 308 по время выдачи лицензии 1208 на основании такой ПМП 308. В частности, могут возникать некоторые ситуации, когда данные прав в представленной ПМП 308 явно не учитываются, и лицензиар 1210 вместо них подставляет или "вводит" альтернативную стратегию при создании лицензии 1208 на основании такой ПМП 308. Следует отметить, что, несмотря на описание нескольких конкретных ситуаций, в которых лицензиар 1210 вводит стратегию в лицензию 1208, лицензиар 1210 может также ввести стратегию в лицензию 1208 в ситуации любого другого типа, не выходя при этом за рамки объема притязаний настоящего изобретения.

В первой ситуации, проиллюстрированной на фиг.14, лицензиар 1208 ведет (поддерживает) список 1214 (фиг.12) специальных объектов (пользователей, групп и т.п.), которым предоставляются специальные права. Например, специальными объектами могут быть, помимо прочего, определенные лица, имеющие более высокое положение в организации, определенные контролирующие лица, определенные лица, которые должны

иметь возможность осуществлять представление всего содержания, и группы вышеупомянутых лиц. Такой список 1214 может быть фактически введен в организационный каталог 1206 как идентифицирующая информация в списке каталога для каждого специального объекта, или проще - просто путем создания одной или более групп таких специальных объектов. Поэтому такие специальные объекты смогут осуществлять представление содержания, даже если ПМП 308 для них в противном случае запрещает такое представление.

После того, как объект предоставил ПМП 308 как часть запроса на лицензию 1208, как проиллюстрировано на фиг.14, лицензиар 1210 проверяет каталог 1206 соответствующим образом, чтобы определить, можно ли предоставивший объект охарактеризовать как специальный объект (этап 1401), и если да, то лицензиар 1210 создает лицензию 1208 для специального объекта со специальными правами, которые отличаются от данных прав, присутствующих в предоставленной ПМП (этап 1403). Следует отметить, что эти специальные права могут быть любыми правами, не выходя при этом за рамки объема изобретения. Например, специальные права могут заключаться в том, что все специальные объекты могут полностью иметь доступ к соответствующему содержанию и осуществлять его представление, что все специальные объекты из конкретной группы могут полностью осуществлять доступ к содержанию и его представление, что конкретный специальный объект получает расширенные права, например, большее количество воспроизведений или более длительный период до того, как истечет лицензия 1208, и т.д. Следует отметить, что если специальные права являются конкретными для человека или группы, то такие права можно указать в записи каталога 1206 для лица или группы, такая запись в каталоге может иметь соответствующую ссылку на место, где расположены специальные права, лицензиар 1210 может найти специальные права в базе данных на основании идентификатора 1204 этого человека или группы, или т.п.

Во второй ситуации, проиллюстрированной на фиг.15, лицензиар 1208 ведет (поддерживает) список 1216 (фиг.12) объектов (пользователей, групп и т.п.) с ограниченными полномочиями, в отношении которых права ограничены или отказаны. Например, объектами с ограниченными полномочиями могут быть, помимо прочего, лица которые покинули организацию; лица, состоящие в организации, которые нормально не имеют права на какое-либо содержание, например, технический или служебный персонал; лица, имеющие только ограниченный статус в организации, например, работающие по контрактам и временные служащие, а также группы вышеупомянутых лиц. Подобно упомянутому выше "специальному" списку 1214 ограниченный список 1216 может быть также введен в организационный каталог 1206 в качестве идентифицирующей информации в списке каталога для каждого объекта с ограниченными полномочиями, или проще - путем создания одной или более групп таких объектов с ограниченными полномочиями. Следовательно, таким объектам с ограниченными полномочиями не предоставляется возможность представления содержания, даже если ПМП 308 для них в противном случае разрешает такое представление.

После того, как объект предоставил ПМП 308 как часть запроса на лицензию 1208, как показано на фиг.14, лицензиар 1210 сверяется с каталогом 1206 соответствующим образом, чтобы определить, может ли предоставивший объект быть охарактеризован как объект с ограниченными полномочиями (этап 1405), и если да, то лицензиар 1210 создает лицензию 1208 для данного объекта с ограниченными правами, которые отличаются от прав, присутствующих в предоставленной ПМП 308 (этап 1407). Следует отметить, что ограниченные права могут быть любыми правами, не выходя за рамки объема притязаний настоящего изобретения. Например, ограниченные права могут состоять в том, что все объекты с ограниченными полномочиями не смогут осуществлять доступ к соответствующему содержанию и его представление любым способом, что все объекты с ограниченными полномочиями из конкретной группы смогут осуществлять доступ к содержанию и его представление только в непродолжительной форме, что конкретный объект с ограниченными полномочиями сможет распечатать всего одну копию части

содержания, и т.д. Кроме того, ограниченные права могут заключаться в том, что объект с ограниченными полномочиями не сможет получить лицензию вообще. Как и в случае специальных прав, если ограниченные права являются конкретными для человека или группы, то они могут быть указаны в записи каталога для этого человека или группы в каталоге 1206, такой каталог может иметь соответствующую ссылку на местоположение, где находятся ограниченные права, лицензиар 1210 может найти ограниченные права в базе данных на основании идентификатора 1204 данного человека или группы, или т.п.

В третьей ситуации лицензиар 1208 может ввести стратегию в лицензию 1208, указывающую минимальные системные требования к вычислительному устройству 14 (фиг.11), которое будет осуществлять представление (воспроизведение) соответствующего содержания (этап 1409). Такие минимальные системные требования обычно относятся к достоверности и защищенности вычислительного устройства 14, хотя такие требования могут также относиться к любому другому материалу, не выходя за рамки объема изобретения.

Основным примером достоверности и защищенности, которые будут касаться лицензиара 1210, является вопрос, является ли доверенный компонент 18 вычислительного устройства 14 или его защищенная часть подлинными. Понятно, что такая подлинность может быть представлена номером версии, датой выпуска, или т.п. и отражать возраст доверенного компонента 18 или его части. Также понятно, что доверенный компонент 18 или его часть по мере их старения становятся все более подвержены атакам со стороны недобросовестных объектов. Соответственно, лицензиар 1210 может решить, что доверенный компонент 18 или его часть, превосходящая определенный возраст, не заслуживает доверия и может ввести стратегию в выдаваемую им лицензию 1208, которая будет требовать, чтобы такой не вызывающий доверия компонент 18 или его часть были обновлены прежде, чем на нем будет разрешено осуществлять представление соответствующего содержания.

Другой пример достоверности и защиты, которая может касаться лицензиара 1210, заключается в определении, является ли достоверным приложение, которое должно осуществлять представление содержания. Понятно, что может возникнуть случай, когда одному приложению можно доверить представление содержания в рамках лицензии 1208, например, не разрешая при этом сохранять содержание в незащищенном виде, а другому приложению нельзя доверить то же самое. Соответственно, лицензиар 1210 может решить, что можно использовать только определенные приложения для представления соответствующего содержания, и может ввести стратегию в выданную им лицензию 1208, которая потребует, чтобы использовалось только такое приложение для представления данного содержания.

Конечно, существует великое множество других ситуаций введения стратегии. Обычно стратегию можно вводить для прибавления дополнительных прав или изъятия прав из данных прав в ПМП 308, возможно, на основе запрашивающей стороны (этап 1411), и также для добавления условий или изъятия условий из таких данных прав, снова, возможно, по просьбе запрашивающей стороны (этап 1413).

Выводы

Программирование, необходимое для реализации способов, выполняемых в связи с настоящим изобретением, является относительно простым и должно быть очевидным для программистов. Поэтому такие программы не прикладываются к данному описанию. Можно использовать любые конкретные программы для реализации настоящего изобретения, не выходя за рамки объема притязаний изобретения.

Понятно, что в описанные выше варианты можно внести изменения, не выходящие за рамки изобретательского замысла. Следует отметить, что хотя настоящее изобретение было описано в контексте определенного «пространства» (генеральной совокупности), такого как организация, оно может быть также реализовано в рамках ограниченного пространства, например, части организации, или охватывать множество организаций, - все это подпадает под объем изобретения. Следовательно, настоящее изобретение не

ограничено конкретными описанными выше вариантами, а охватывает модификации в рамках притязаний, охарактеризованных в прилагаемой формуле изобретения.

ПРИЛОЖЕНИЕ 1

Образец данных прав

```
<?xml версия ="1.0"?>
<XrML версия="1.2">
 <ТЕЛО тип = "Шаблон прав">
  <ДЕСКРИПТОР>
   <ОБЪЕКТ>
    <ИД тип=ГУИД">c43..</ИД>"
    <ИМЯ>$$411$11имя$11опис</ИМЯ>
   </ОБЪЕКТ>
  </ДЕСКРИПТОР>
  <РАБОТА>
   <ОБЪЕКТ>
    <ИД/)
  <ОБЪЕКТ>
  <ГРУППА ПРАВ имя="ОСНОВНЫЕ ПРАВА">
   <СПИСОК ПРАВ>
    <ПРОСМОТР>
     <СПИСОК УСЛОВИЙ>
      <ДОСТУП>
       <ПРИНЦИПАЛ>
        <ОБЪЕКТ>
         <ИД/>
         <ИМЯ>test@company.com</ИМЯ>
        </ОБЪЕКТ>
       </ПРИНЦИПАЛ>
      </ДОСТУП>
     </СПИСОК УСЛОВИЙ>
  </ПРОСМОТР>
```

```
      <ПРАВО имя ="родовое">
       <СПИСОК УСЛОВИЙ>
        <ДОСТУП>
         <ПРИНЦИПАЛ>
          <ОБЪЕКТ>
           <ИД/>
            <ИМЯ>test@company.com</ИМЯ>
           </ОБЪЕКТ>
          </ПРИНЦИПАЛ>
         </ДОСТУП>
        <СПИСОК УСЛОВИЙ>
       </ПРАВО>
      </СПИСОК ПРАВ>
     </ГРУППА ПРАВ>
    </РАБОТА>
   </ТЕЛО>
  <ПОДПИСЬ>
    <АЛГОРИТМ>RSA PKCS#1-V1.5</АЛГОРИТМ>
    <ДАЙДЖЕСТ>
     <АЛГОРИТМ>SHA1<АЛГОРИТМ>
     <ПАРАМЕТР имя="тип кодирования">
      <ЗНАЧЕНИЕ кодирование="цепь">поверх.кодирование</ЗНАЧЕНИЕ>
     </ПАРАМЕТР>
     <ЗНАЧЕНИЕ кодирование="base64"размер="160">Mwl…=</ЗНАЧЕНИЕ>
    </ДАЙДЖЕСТ>
    <ЗНАЧЕНИЕ кодирование="base64"размер="1024">Msi…=</ЗНАЧЕНИЕ>
   </ПОДПИСЬ>
  </XrML>
```

ПРИЛОЖЕНИЕ 2

Образец подписанной метки прав (ПМП) 308

```
<?xml версия ="1.0"?>
<XrML версия="1.2">
 <ТЕЛО тип = "Шаблон прав" версия="3.0">
  <ВРЕМЯ ВЫДАЧИ>2002-01-01_12:00:00</ВРЕМЯ ВЫДАЧИ>
  <ДЕСКРИПТОР>
   <ОБЪЕКТ>
    <ИД/>
    <ИМЯ>$$409$...ИМЯ>
   </ОБЪЕКТ>
  </ДЕСКРИПТОР>
 <ВЫДАВШИЙ>
  <ОБЪЕКТ тип="ЦУП-Сервер">
   <ИД тип="ГУИД">{d81...}</ИД>
  <ИМЯ>Тест ЦУП Сервер</ИМЯ>
 <АДРЕС тип="URL">http://licensing.dev.com<|АДРЕС>
</ОБЪЕКТ>
<ОТКРЫТЫЙ КЛЮЧ>
 <АЛГОРИТМ>RSA</АЛГОРИТМ>
 <ПАРАМЕТР имя="открытый экспонент">
  <ЗНАЧЕНИЕ кодирования="целое32">65537<ЗНАЧЕНИЕ>
 </ПАРАМЕТР>
 <ПАРАМЕТР имя="модуль">
  <ЗНАЧЕНИЕ кодирования="основа64"размер="1024">NcO...=</ЗНАЧЕНИЕ>
  </ПАРАМЕТР>
 </ОТКРЫТЫЙ КЛЮЧ>
 <ОТПИРАЮЩИЕ БИТЫ тип="закрытый ключ">
  <ЗНАЧЕНИЕ кодирования="основа64"размер="1024">tFg...=</ЗНАЧЕНИЕ>
```

```
    </ОТПИРАЮЩИЕ БИТЫ>
    <УРОВЕНЬ ЗАЩИТЫ имя="Сервер-Версия"значение="2.0"/>
    <УРОВЕНЬ ЗАЩИТЫ имя="Сервер-SKU"значение="22222-3333"/>
  </ВЫДАВШИЙ>
  <ПУНКТ РАСПРОСТРАНЕНИЯ>
   <ОБЪЕКТ тип=="URL ПОЛУЧЕНИЯ ЛИЦЕНЗИИ">
     <ИД тип="ГУИД">{0F4…}</ИД>
     <ИМЯ>КЛАСТЕР СЕРВЕР ЦУП</ИМЯ>
     <АДРЕС тип="URL">http://localhost/Licensing<|АДРЕС>
   </ОБЪЕКТ>
   </ПУНКТ РАСПРОСТРАНЕНИЯ>
   <РАБОТА>
    <ОБЪЕКТ тип="ТЕСТ-ФОРМАТ">
     <ИД ТИП="MYID>FDB-1</ИД>
    </ОБЪЕКТ>
   <МЕТАДАННЫЕ>
    <SKU тип="PIDTYPE">PID</SKU>
   </МЕТАДАННЫЕ>
   <СПИСОК ПРЕДУСЛОВИЙ>
    <ВРЕМЯ/>
  </СПИСОК ПРЕДУСЛОВИЙ>
 </РАБОТА>
 <АВТ ДАННЫЕ имя="Зашифрованные данные прав">PAB…</АВТ ДАННЫЕ>
</ТЕЛО>
<ПОДПИСЬ>
 <АЛГОРИТМ>RSA PKCS#1-V1.5</АЛГОРИТМ>
 <ДАЙДЖЕСТ>
  <АЛГОРИТМ>SHA1</АЛГОРИТМ>
  <ПАРАМЕТР имя="тип кодирования">
```

```
        <ЗНАЧЕНИЕ кодирования ="цепь">поверх-кодирование</ЗНАЧЕНИЕ>
      </ПАРАМЕТР>
    <ЗНАЧЕНИЕ кодирования ="основа64"размер="160">Prc...=</ЗНАЧЕНИЕ>
  </ДАЙДЖЕСТ>
  <ЗНАЧЕНИЕ кодирования ="основа64"размер="1024">EHd...=</ЗНАЧЕНИЕ>
 </ПОДПИСЬ>
</XrM>
```

Формула изобретения

1. Способ выдачи лицензиаром запрашивающей стороне цифровой лицензии, чтобы разрешить запрашивающей стороне осуществлять представление соответствующего цифрового содержания, заключающийся в том, что

получают от запрашивающей стороны запрос, включающий в себя данные прав, связанные с содержанием, причем данные прав перечисляют, по меньшей мере, один идентификатор и набор прав, связанных с ним, выбирают идентификатор и набор связанных с ним прав, которые предполагается изложить в выданной лицензии, выбирают на основании идентификатора альтернативный набор прав, заменяют альтернативным набором прав набор прав из данных прав, выдают запрашивающей стороне лицензию с альтернативным набором прав,

при этом альтернативный набор прав в выданной лицензии излагает сроки и условия, которые должна соблюдать запрашивающая сторона в связи с представлением соответствующего содержания.

2. Способ по п.1, в котором лицензиар имеет доступ к каталогу, содержащему список для данного идентификатора, причем список ссылается на альтернативный набор данных прав, и в котором при выборе альтернативного набора данных прав находят идентификатор в каталоге и находят альтернативный набор прав на основании ссылки на него в списке для данного идентификатора в каталоге.

3. Способ по п.1, в котором определяют на основании идентификатора, что запрашивающая сторона является специальной запрашивающей стороной, имеющей расширенный набор прав по сравнению с набором прав запрашивающей стороны, и выбирают на этой основе альтернативный набор прав, который предоставляет более широкие права, чем набор прав из данных прав.

4. Способ по п.3, в котором выбирают альтернативный набор прав, который позволяет специальной запрашивающей стороне полностью осуществлять доступ к соответствующему содержанию и его представление.

5. Способ по п.1, в котором определяют на основании идентификатора, что запрашивающая сторона является запрашивающей стороной с ограниченными полномочиями, и выбирают на этой основе альтернативный набор прав, который предоставляет меньшие права, чем набор прав из данных прав.

6. Способ по п.5, в котором выбирают альтернативный набор прав, не позволяющий запрашивающей стороне с ограниченными полномочиями осуществлять доступ к соответствующему содержанию и его представление.

7. Способ по п.1, в котором выбирают на основании идентификатора альтернативный набор прав, налагающий минимальные системные требования на вычислительное устройство, на котором должно осуществляться представление соответствующего содержания.

8. Способ по п.1, в котором выбирают на основании идентификатора альтернативный набор прав, добавляющий права к набору прав из данных прав.

9. Способ по п.1, в котором выбирают на основании идентификатора альтернативный набор прав, исключающий права из набора прав из данных прав.

10. Машиночитаемый носитель, имеющий хранящиеся на нем исполняемые компьютером команды для выполнения способа выдачи лицензиаром запрашивающей стороне цифровой лицензии, чтобы разрешить запрашивающей стороне осуществлять представление соответствующего цифрового содержания, причем способ заключается в том, что получают от запрашивающей стороны запрос, включающий в себя данные прав, связанные с содержанием, причем данные прав перечисляют, по меньшей мере, один идентификатор и набор прав, связанных с ним, выбирают идентификатор и набор связанных с ним прав, которые предполагается изложить в выданной лицензии, выбирают на основании идентификатора альтернативный набор прав, заменяют альтернативным набором прав набор прав из данных прав, выдают запрашивающей стороне лицензию с альтернативным набором прав, при этом альтернативный набор прав в выданной лицензии излагает условия, которые должна соблюдать запрашивающая сторона в связи с представлением соответствующего содержания.

11. Носитель по п.10, в котором лицензиар имеет доступ к каталогу, содержащему список для данного идентификатора, причем список ссылается на альтернативный набор данных прав, и в котором при выборе альтернативного набора данных прав находят идентификатор в каталоге и находят альтернативный набор прав на основании ссылки на него в списке для данного идентификатора в каталоге.

12. Носитель по п.10, в котором способ включает в себя определение на основании идентификатора, что запрашивающая сторона является специальной запрашивающей стороной, имеющей расширенный набор прав по сравнению с набором прав запрашивающей стороны, и выбор на этой основе альтернативного набора прав, который предоставляет более широкие права, чем набор прав из данных прав.

13. Носитель по п.12, в котором способ включает в себя выбор альтернативного набора прав, позволяющего специальной запрашивающей стороне полностью осуществлять доступ к соответствующему содержанию и его представление.

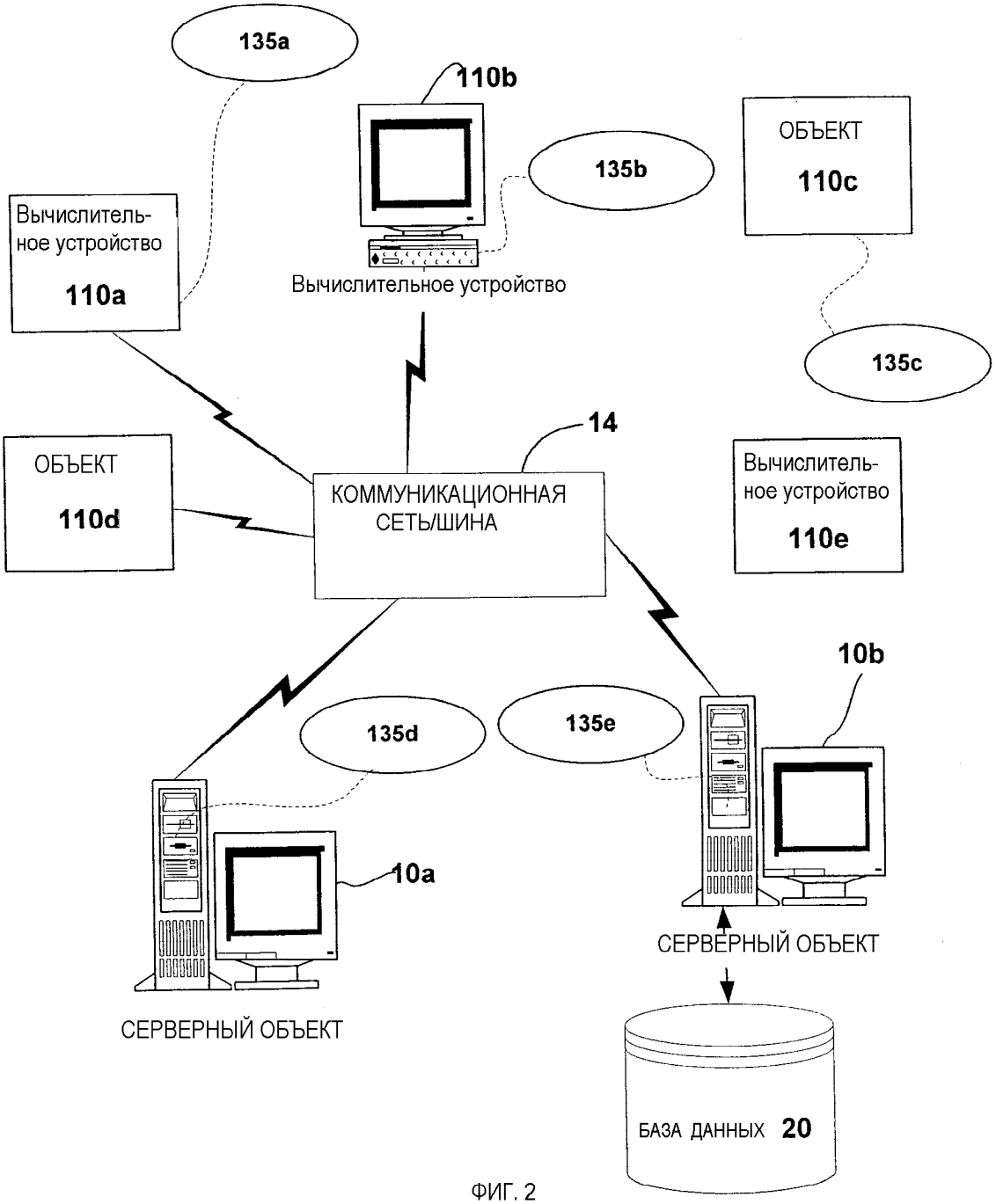
14. Носитель по п.10, в котором способ включает в себя определение на основании идентификатора, что запрашивающая сторона является запрашивающей стороной с ограниченными полномочиями, и выбор на этой основе альтернативного набора прав, который предоставляет меньшие права, чем набор прав из данных прав.

15. Носитель по п.14, в котором способ включает в себя выбор альтернативного набора прав, не позволяющего запрашивающей стороне с ограниченными полномочиями осуществлять доступ к соответствующему содержанию и его представление.

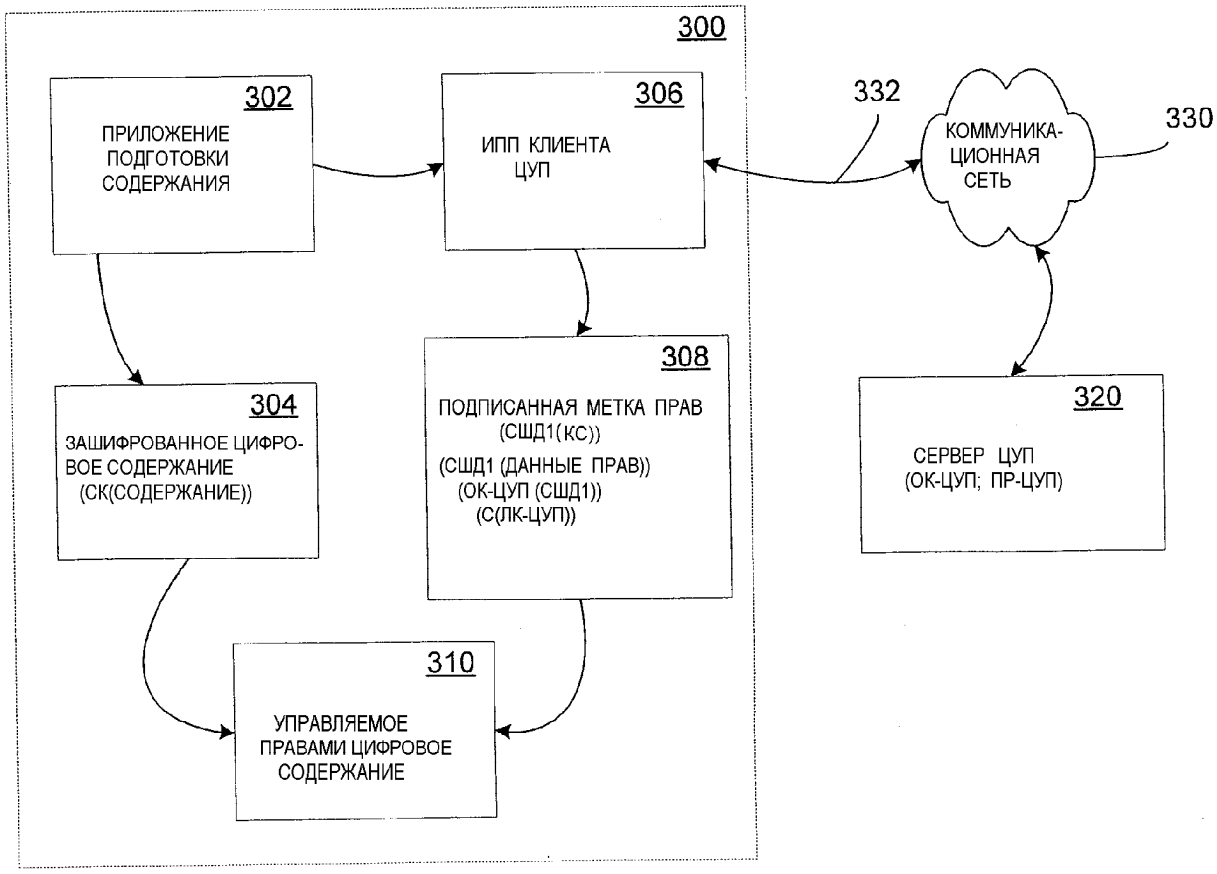
16. Носитель по п.10, в котором способ включает в себя выбор, на основании идентификатора, альтернативного набора прав, налагающего минимальные системные требования на вычислительное устройство, на котором должно осуществляться представление соответствующего содержания.

17. Носитель по п.10, в котором способ включает в себя выбор, на основании идентификатора, альтернативного набора прав, добавляющего права к набору прав из данных прав.

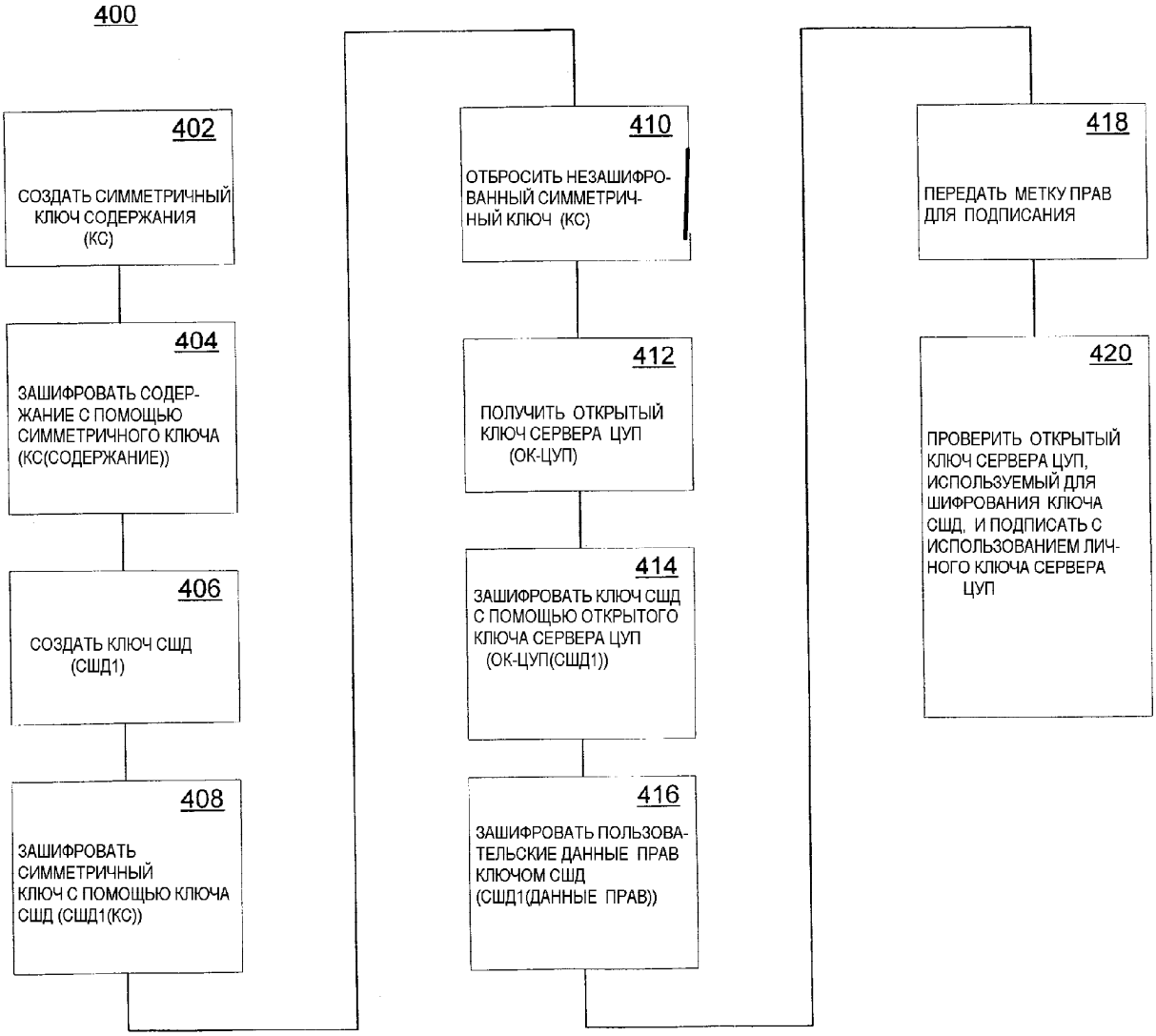
18. Носитель по п.10, в котором способ включает в себя выбор, на основании идентификатора, альтернативного набора прав, исключающего права из набора прав из данных прав.


135a
110b
135b
ОБЪЕКТ
110c
Вычислитель-
ное устройство
110a
Вычислительное устройство
135c
14
ОБЪЕКТ
110d
КОММУНИКАЦИОННАЯ
СЕТЬ/ШИНА
Вычислитель-
ное устройство
110e
10b
135d
135e
10a
СЕРВЕРНЫЙ ОБЪЕКТ
СЕРВЕРНЫЙ ОБЪЕКТ
БАЗА ДАННЫХ 20

ФИГ. 2


300
302
ПРИЛОЖЕНИЕ ПОДГОТОВКИ СОДЕРЖАНИЯ
306
ИПП КЛИЕНТА ЦУП
332
КОММУНИКА-ЦИОННАЯ СЕТЬ
330
304
ЗАШИФРОВАННОЕ ЦИФРОВОЕ СОДЕРЖАНИЕ (СК(СОДЕРЖАНИЕ))
308
ПОДПИСАННАЯ МЕТКА ПРАВ (СШД1(КС)) (СШД1 (ДАННЫЕ ПРАВ)) (ОК-ЦУП (СШД1)) (С(ЛК-ЦУП))
320
СЕРВЕР ЦУП (ОК-ЦУП; ПР-ЦУП)
310
УПРАВЛЯЕМОЕ ПРАВАМИ ЦИФРОВОЕ СОДЕРЖАНИЕ

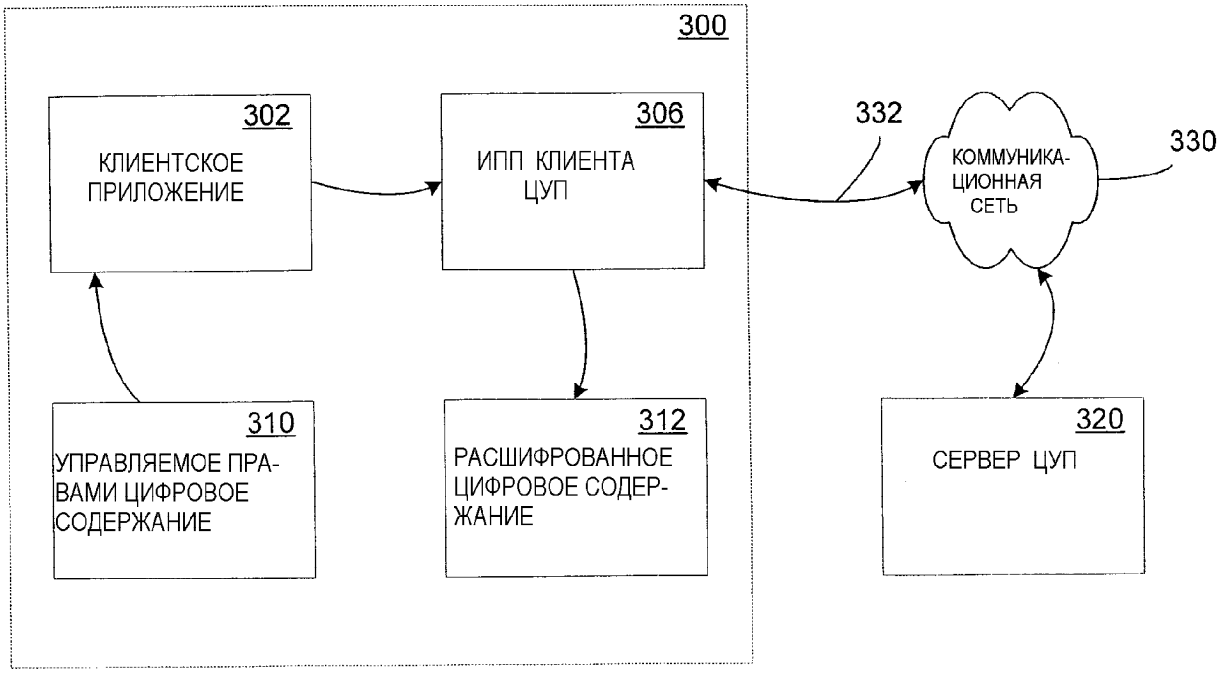
ФИГ. 3


400
402
СОЗДАТЬ СИММЕТРИЧНЫЙ КЛЮЧ СОДЕРЖАНИЯ (КС)
404
ЗАШИФРОВАТЬ СОДЕРЖАНИЕ С ПОМОЩЬЮ СИММЕТРИЧНОГО КЛЮЧА (КС(СОДЕРЖАНИЕ))
406
СОЗДАТЬ КЛЮЧ СШД (СШД1)
408
ЗАШИФРОВАТЬ СИММЕТРИЧНЫЙ КЛЮЧ С ПОМОЩЬЮ КЛЮЧА СШД (СШД1(КС))
410
ОТБРОСИТЬ НЕЗАШИФРОВАННЫЙ СИММЕТРИЧНЫЙ КЛЮЧ (КС)
412
ПОЛУЧИТЬ ОТКРЫТЫЙ КЛЮЧ СЕРВЕРА ЦУП (ОК-ЦУП)
414
ЗАШИФРОВАТЬ КЛЮЧ СШД С ПОМОЩЬЮ ОТКРЫТОГО КЛЮЧА СЕРВЕРА ЦУП (ОК-ЦУП(СШД1))
416
ЗАШИФРОВАТЬ ПОЛЬЗОВАТЕЛЬСКИЕ ДАННЫЕ ПРАВ КЛЮЧОМ СШД (СШД1(ДАННЫЕ ПРАВ))
418
ПЕРЕДАТЬ МЕТКУ ПРАВ ДЛЯ ПОДПИСАНИЯ
420
ПРОВЕРИТЬ ОТКРЫТЫЙ КЛЮЧ СЕРВЕРА ЦУП, ИСПОЛЬЗУЕМЫЙ ДЛЯ ШИФРОВАНИЯ КЛЮЧА СШД, И ПОДПИСАТЬ С ИСПОЛЬЗОВАНИЕМ ЛИЧНОГО КЛЮЧА СЕРВЕРА ЦУП

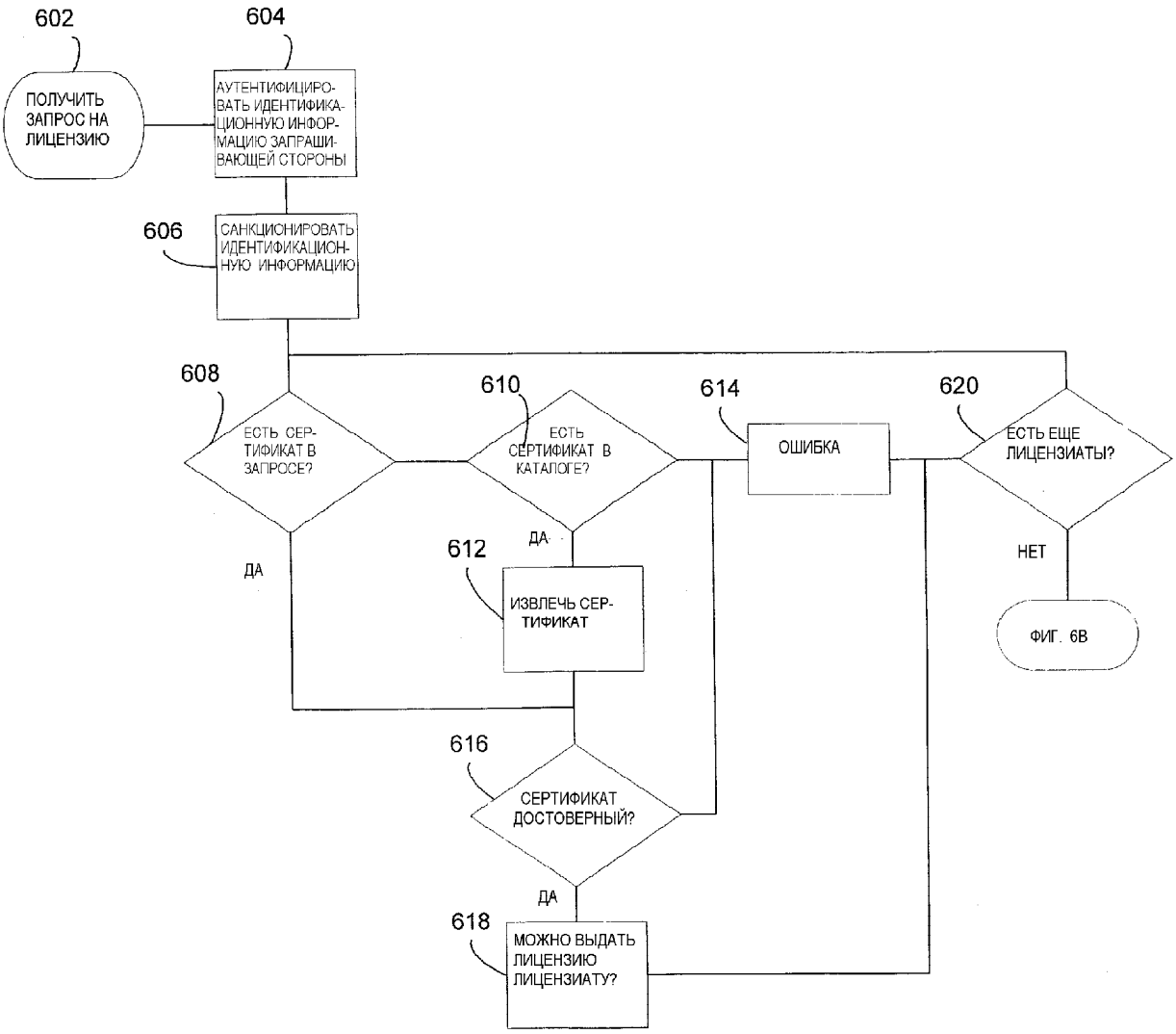
ФИГ. 4

ПМП 308
ИНФОРМАЦИЯ О СОДЕРЖАНИИ
ИНФОРМАЦИЯ О СЕРВЕРЕ ЦУП
- (ОК-ЦУП(СШД1))
- ССЫЛОЧНАЯ ИНФОРМАЦИЯ
- - URL
- - ОТКАЗ
ИНФОРМАЦИЯ О МЕТКЕ ПРАВ
(СШД1(ДАННЫЕ ПРАВ))
(СШД1(КС))
С (ЛК-ЦУП)

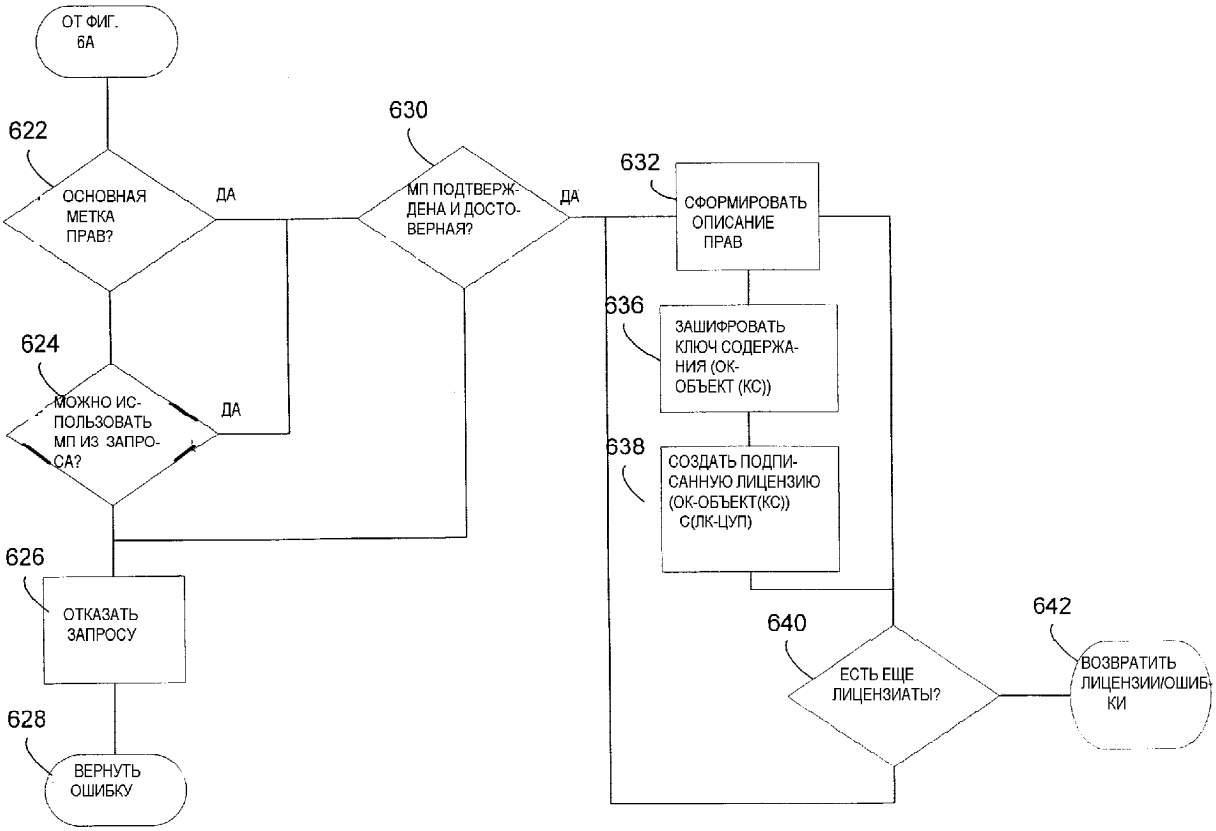
ФИГ. 4А



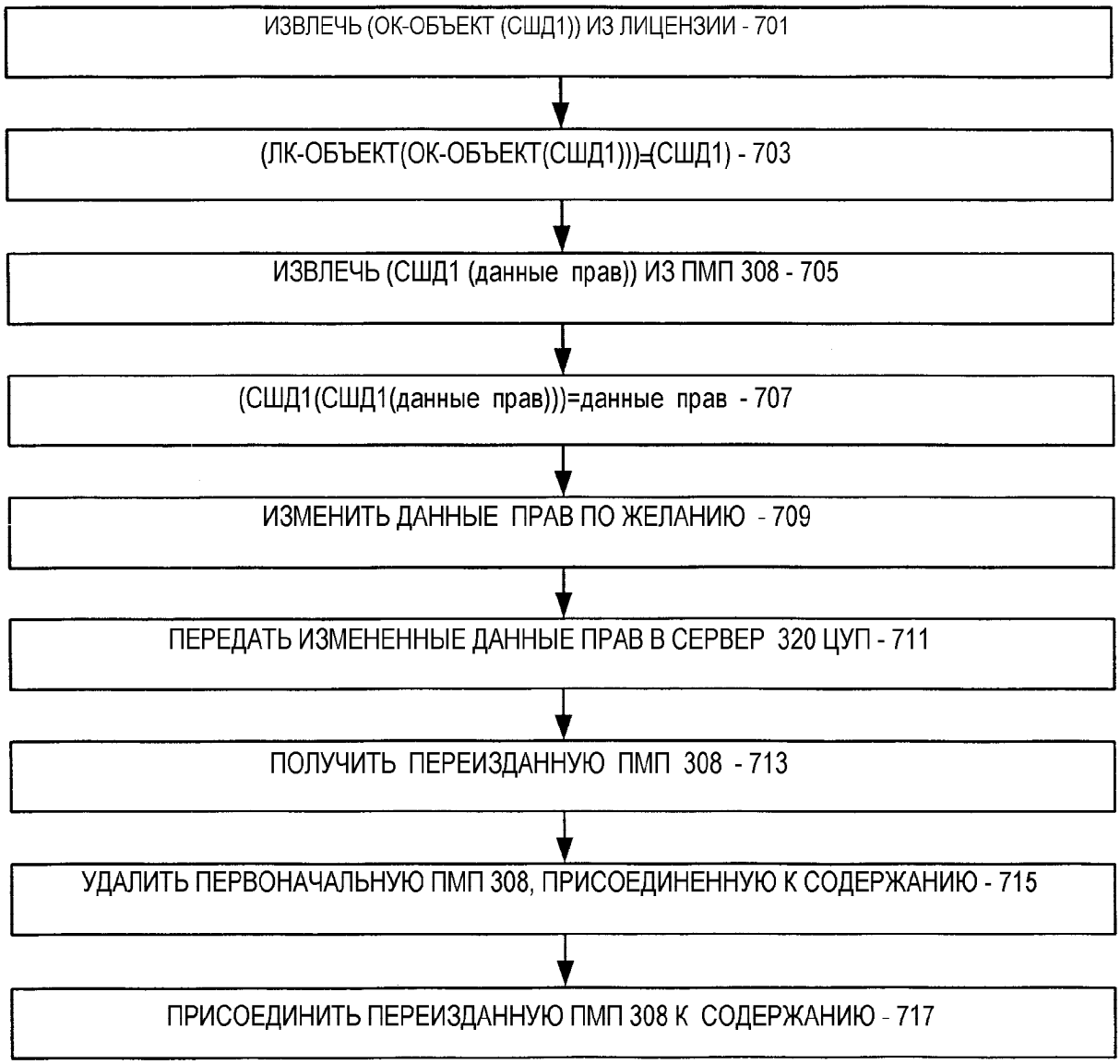
ФИГ. 5


602
604
ПОЛУЧИТЬ ЗАПРОС НА ЛИЦЕНЗИЮ
АУТЕНТИФИЦИРОВАТЬ ИДЕНТИФИКАЦИОННУЮ ИНФОРМАЦИЮ ЗАПРАШИВАЮЩЕЙ СТОРОНЫ
606
САНКЦИОНИРОВАТЬ ИДЕНТИФИКАЦИОННУЮ ИНФОРМАЦИЮ
608
ЕСТЬ СЕРТИФИКАТ В ЗАПРОСЕ?
610
ЕСТЬ СЕРТИФИКАТ В КАТАЛОГЕ?
614
ОШИБКА
620
ЕСТЬ ЕЩЕ ЛИЦЕНЗИАТЫ?
ДА
ДА
НЕТ
612
ИЗВЛЕЧЬ СЕРТИФИКАТ
ФИГ. 6В
616
СЕРТИФИКАТ ДОСТОВЕРНЫЙ?
ДА
618
МОЖНО ВЫДАТЬ ЛИЦЕНЗИЮ ЛИЦЕНЗИАТУ?

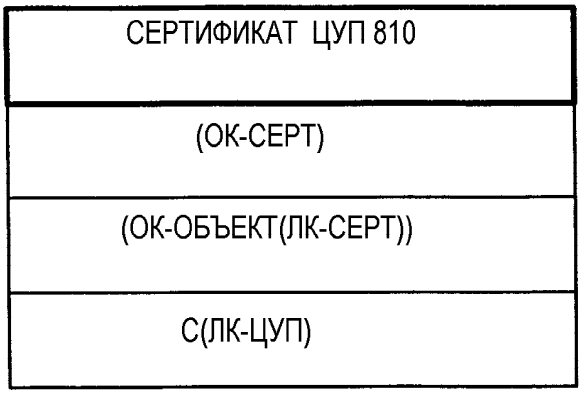
ФИГ. 6А


ОТ ФИГ. 6А
622
ОСНОВНАЯ МЕТКА ПРАВ?
ДА
630
МП ПОДТВЕРЖДЕНА И ДОСТОВЕРНАЯ?
ДА
632
СФОРМИРОВАТЬ ОПИСАНИЕ ПРАВ
624
МОЖНО ИСПОЛЬЗОВАТЬ МП ИЗ ЗАПРОСА?
ДА
636
ЗАШИФРОВАТЬ КЛЮЧ СОДЕРЖАНИЯ (ОК-ОБЪЕКТ (КС))
638
СОЗДАТЬ ПОДПИСАННУЮ ЛИЦЕНЗИЮ (ОК-ОБЪЕКТ(КС)) С(ЛК-ЦУП)
626
ОТКАЗАТЬ ЗАПРОСУ
640
ЕСТЬ ЕЩЕ ЛИЦЕНЗИАТЫ?
642
ВОЗВРАТИТЬ ЛИЦЕНЗИИ/ОШИБКИ
628
ВЕРНУТЬ ОШИБКУ

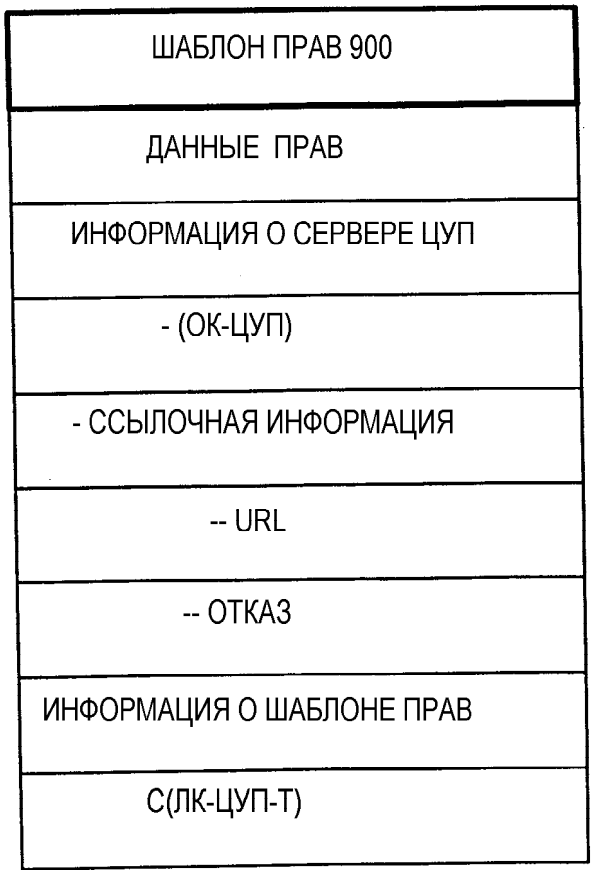
ФИГ. 6В


ИЗВЛЕЧЬ (ОК-ОБЪЕКТ (СШД1)) ИЗ ЛИЦЕНЗИИ - 701
(ЛК-ОБЪЕКТ(ОК-ОБЪЕКТ(СШД1)))=(СШД1) - 703
ИЗВЛЕЧЬ (СШД1 (данные прав)) ИЗ ПМП 308 - 705
(СШД1(СШД1(данные прав)))=данные прав - 707
ИЗМЕНИТЬ ДАННЫЕ ПРАВ ПО ЖЕЛАНИЮ - 709
ПЕРЕДАТЬ ИЗМЕНЕННЫЕ ДАННЫЕ ПРАВ В СЕРВЕР 320 ЦУП - 711
ПОЛУЧИТЬ ПЕРЕИЗДАННУЮ ПМП 308 - 713
УДАЛИТЬ ПЕРВОНАЧАЛЬНУЮ ПМП 308, ПРИСОЕДИНЕННУЮ К СОДЕРЖАНИЮ - 715
ПРИСОЕДИНИТЬ ПЕРЕИЗДАННУЮ ПМП 308 К СОДЕРЖАНИЮ - 717

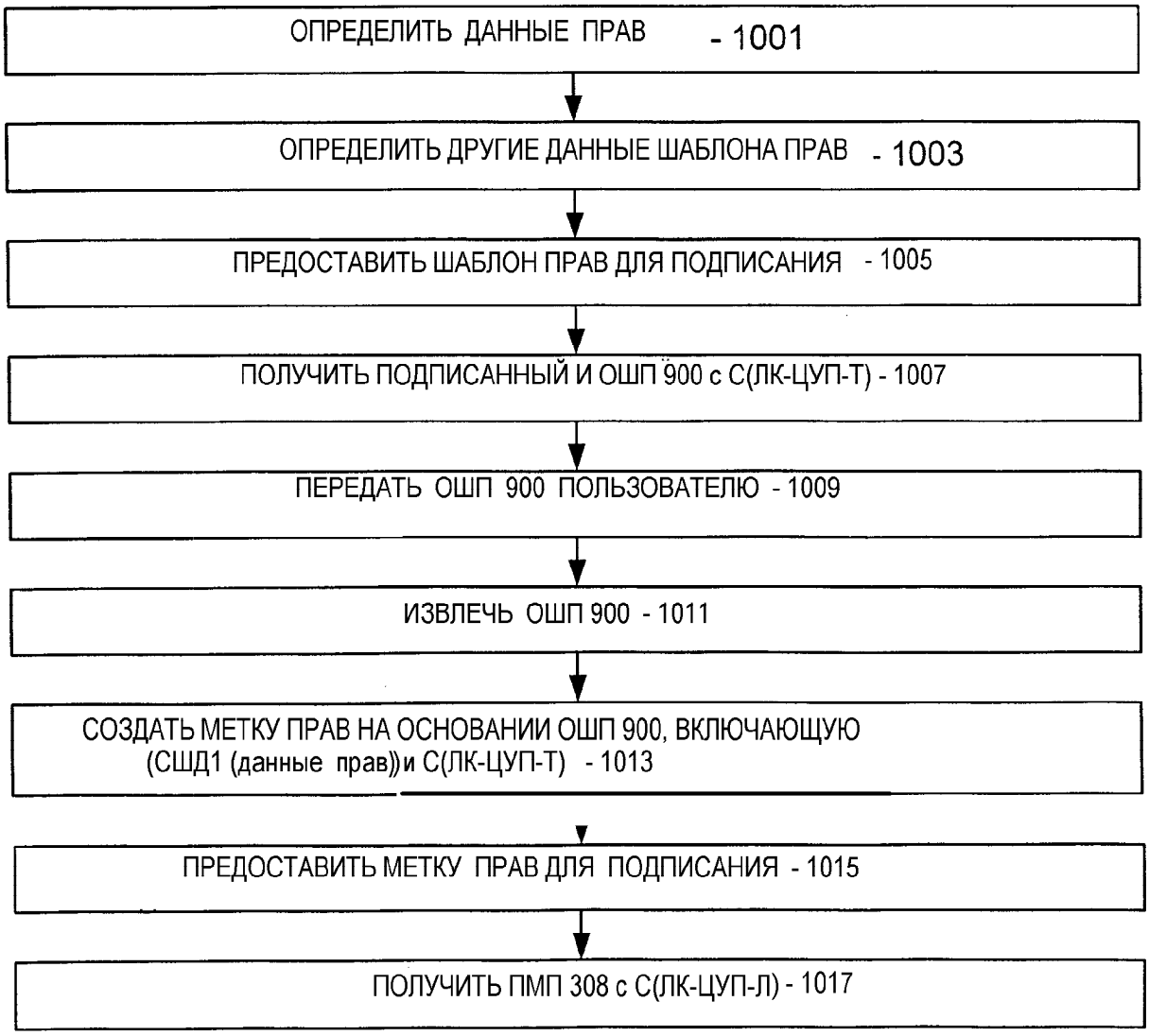
ФИГ. 7


СЕРТИФИКАТ ЦУП 810
(ОК-СЕРТ)
(ОК-ОБЪЕКТ(ЛК-СЕРТ))
С(ЛК-ЦУП)

ФИГ. 8

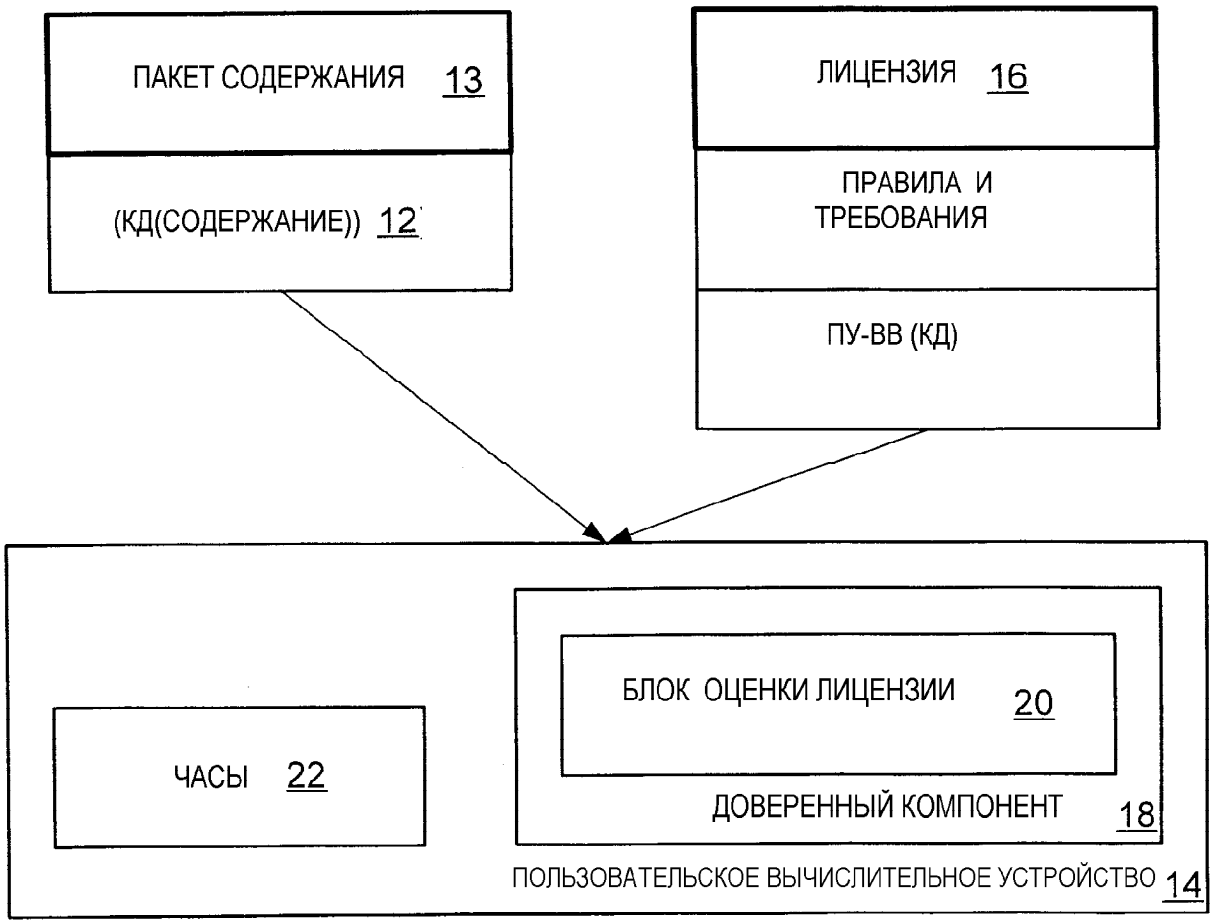

ШАБЛОН ПРАВ 900
ДАННЫЕ ПРАВ
ИНФОРМАЦИЯ О СЕРВЕРЕ ЦУП
- (ОК-ЦУП)
- ССЫЛОЧНАЯ ИНФОРМАЦИЯ
-- URL
-- ОТКАЗ
ИНФОРМАЦИЯ О ШАБЛОНЕ ПРАВ
С(ЛК-ЦУП-Т)

ФИГ. 9

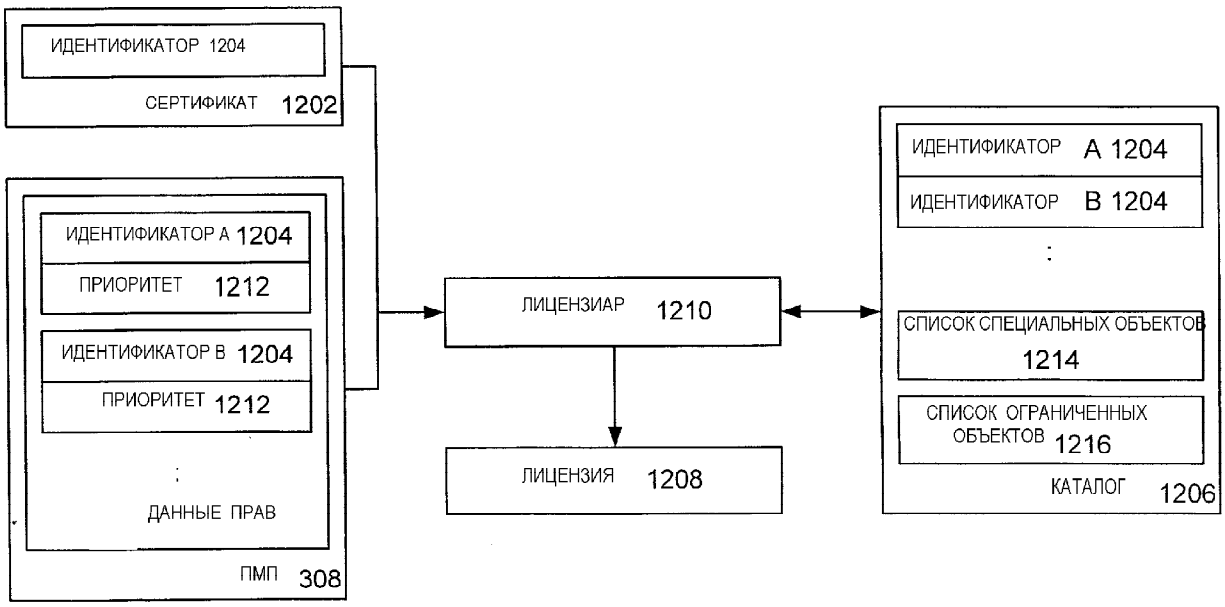

ОПРЕДЕЛИТЬ ДАННЫЕ ПРАВ - 1001
ОПРЕДЕЛИТЬ ДРУГИЕ ДАННЫЕ ШАБЛОНА ПРАВ - 1003
ПРЕДОСТАВИТЬ ШАБЛОН ПРАВ ДЛЯ ПОДПИСАНИЯ - 1005
ПОЛУЧИТЬ ПОДПИСАННЫЙ И ОШП 900 с С(ЛК-ЦУП-Т) - 1007
ПЕРЕДАТЬ ОШП 900 ПОЛЬЗОВАТЕЛЮ - 1009
ИЗВЛЕЧЬ ОШП 900 - 1011
СОЗДАТЬ МЕТКУ ПРАВ НА ОСНОВАНИИ ОШП 900, ВКЛЮЧАЮЩУЮ (СШД1 (данные прав))и С(ЛК-ЦУП-Т) - 1013
ПРЕДОСТАВИТЬ МЕТКУ ПРАВ ДЛЯ ПОДПИСАНИЯ - 1015
ПОЛУЧИТЬ ПМП 308 с С(ЛК-ЦУП-Л) - 1017

ФИГ. 10

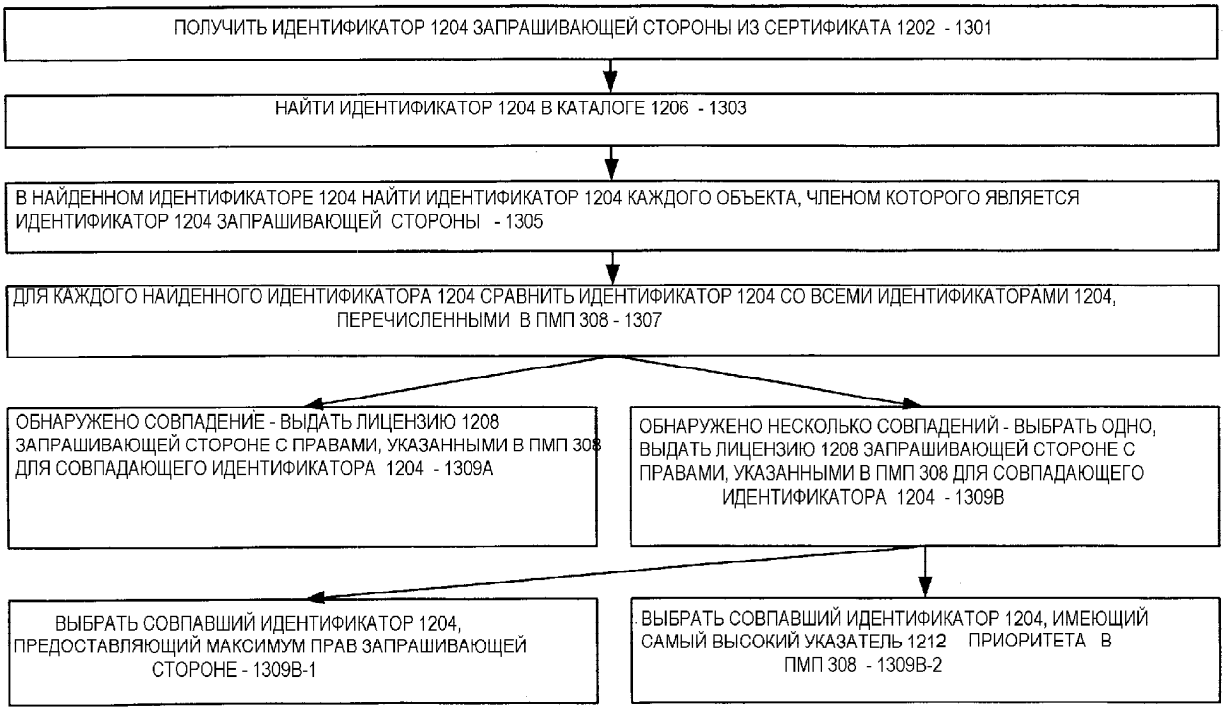
СИСТЕМА ЦУП 10



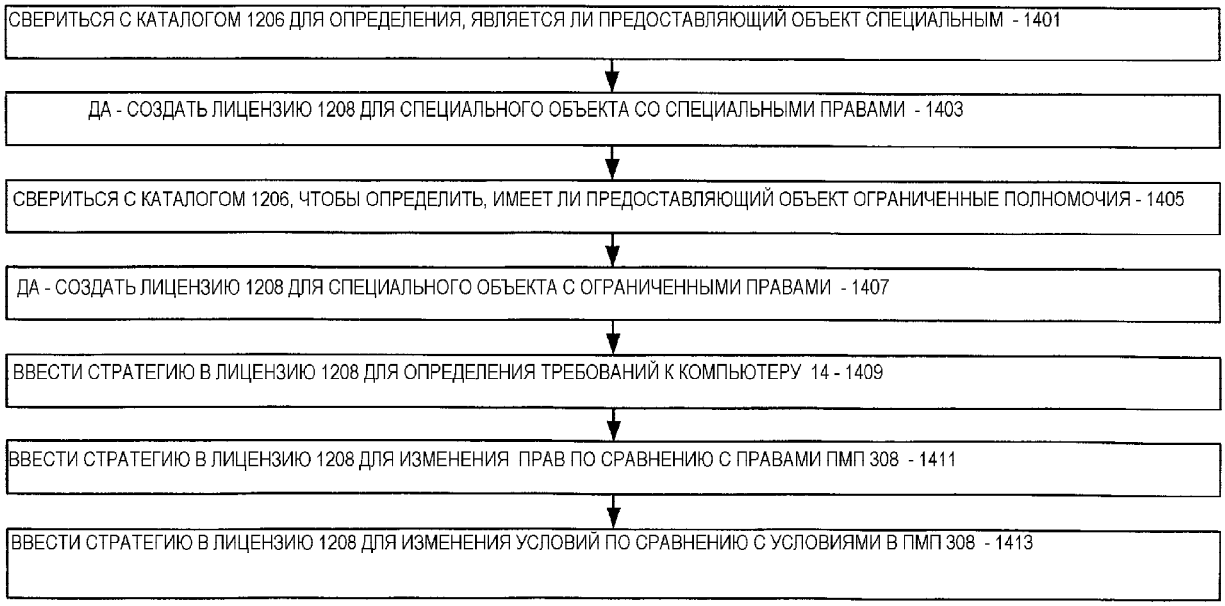
ФИГ. 11



ФИГ. 12


ПОЛУЧИТЬ ИДЕНТИФИКАТОР 1204 ЗАПРАШИВАЮЩЕЙ СТОРОНЫ ИЗ СЕРТИФИКАТА 1202 - 1301
НАЙТИ ИДЕНТИФИКАТОР 1204 В КАТАЛОГЕ 1206 - 1303
В НАЙДЕННОМ ИДЕНТИФИКАТОРЕ 1204 НАЙТИ ИДЕНТИФИКАТОР 1204 КАЖДОГО ОБЪЕКТА, ЧЛЕНОМ КОТОРОГО ЯВЛЯЕТСЯ ИДЕНТИФИКАТОР 1204 ЗАПРАШИВАЮЩЕЙ СТОРОНЫ - 1305
ДЛЯ КАЖДОГО НАЙДЕННОГО ИДЕНТИФИКАТОРА 1204 СРАВНИТЬ ИДЕНТИФИКАТОР 1204 СО ВСЕМИ ИДЕНТИФИКАТОРАМИ 1204, ПЕРЕЧИСЛЕННЫМИ В ПМП 308 - 1307
ОБНАРУЖЕНО СОВПАДЕНИЕ - ВЫДАТЬ ЛИЦЕНЗИЮ 1208 ЗАПРАШИВАЮЩЕЙ СТОРОНЕ С ПРАВАМИ, УКАЗАННЫМИ В ПМП 308 ДЛЯ СОВПАДАЮЩЕГО ИДЕНТИФИКАТОРА 1204 - 1309A
ОБНАРУЖЕНО НЕСКОЛЬКО СОВПАДЕНИЙ - ВЫБРАТЬ ОДНО, ВЫДАТЬ ЛИЦЕНЗИЮ 1208 ЗАПРАШИВАЮЩЕЙ СТОРОНЕ С ПРАВАМИ, УКАЗАННЫМИ В ПМП 308 ДЛЯ СОВПАДАЮЩЕГО ИДЕНТИФИКАТОРА 1204 - 1309B
ВЫБРАТЬ СОВПАВШИЙ ИДЕНТИФИКАТОР 1204, ПРЕДОСТАВЛЯЮЩИЙ МАКСИМУМ ПРАВ ЗАПРАШИВАЮЩЕЙ СТОРОНЕ - 1309B-1
ВЫБРАТЬ СОВПАВШИЙ ИДЕНТИФИКАТОР 1204, ИМЕЮЩИЙ САМЫЙ ВЫСОКИЙ УКАЗАТЕЛЬ 1212 ПРИОРИТЕТА В ПМП 308 - 1309B-2

ФИГ. 13


СВЕРИТЬСЯ С КАТАЛОГОМ 1206 ДЛЯ ОПРЕДЕЛЕНИЯ, ЯВЛЯЕТСЯ ЛИ ПРЕДОСТАВЛЯЮЩИЙ ОБЪЕКТ СПЕЦИАЛЬНЫМ - 1401
ДА - СОЗДАТЬ ЛИЦЕНЗИЮ 1208 ДЛЯ СПЕЦИАЛЬНОГО ОБЪЕКТА СО СПЕЦИАЛЬНЫМИ ПРАВАМИ - 1403
СВЕРИТЬСЯ С КАТАЛОГОМ 1206, ЧТОБЫ ОПРЕДЕЛИТЬ, ИМЕЕТ ЛИ ПРЕДОСТАВЛЯЮЩИЙ ОБЪЕКТ ОГРАНИЧЕННЫЕ ПОЛНОМОЧИЯ - 1405
ДА - СОЗДАТЬ ЛИЦЕНЗИЮ 1208 ДЛЯ СПЕЦИАЛЬНОГО ОБЪЕКТА С ОГРАНИЧЕННЫМИ ПРАВАМИ - 1407
ВВЕСТИ СТРАТЕГИЮ В ЛИЦЕНЗИЮ 1208 ДЛЯ ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ К КОМПЬЮТЕРУ 14 - 1409
ВВЕСТИ СТРАТЕГИЮ В ЛИЦЕНЗИЮ 1208 ДЛЯ ИЗМЕНЕНИЯ ПРАВ ПО СРАВНЕНИЮ С ПРАВАМИ ПМП 308 - 1411
ВВЕСТИ СТРАТЕГИЮ В ЛИЦЕНЗИЮ 1208 ДЛЯ ИЗМЕНЕНИЯ УСЛОВИЙ ПО СРАВНЕНИЮ С УСЛОВИЯМИ В ПМП 308 - 1413

ФИГ. 14