



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ(21), (22) Заявка: **2005120234/09, 29.07.2004**(24) Дата начала отсчета срока действия патента:
29.07.2004(30) Конвенционный приоритет:
23.10.2003 US 10/693,516(43) Дата публикации заявки: **20.01.2006**(45) Опубликовано: **20.11.2009** Бюл. № 32(56) Список документов, цитированных в отчете о
поиске: **RU 2157596 C2, 10.10.2000. RU 2170454**
C2, 10.07.2001. US 2003177178 A1, 18.09.2003.
US 5812776 A, 22.09.1998.(85) Дата перевода заявки РСТ на национальную
фазу: **27.06.2005**(86) Заявка РСТ:
US 2004/024341 (29.07.2004)(87) Публикация РСТ:
WO 2005/045741 (19.05.2005)

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

(72) Автор(ы):

САТАГОПАН Мерли (US),
КАМЕРОН Ким (US)

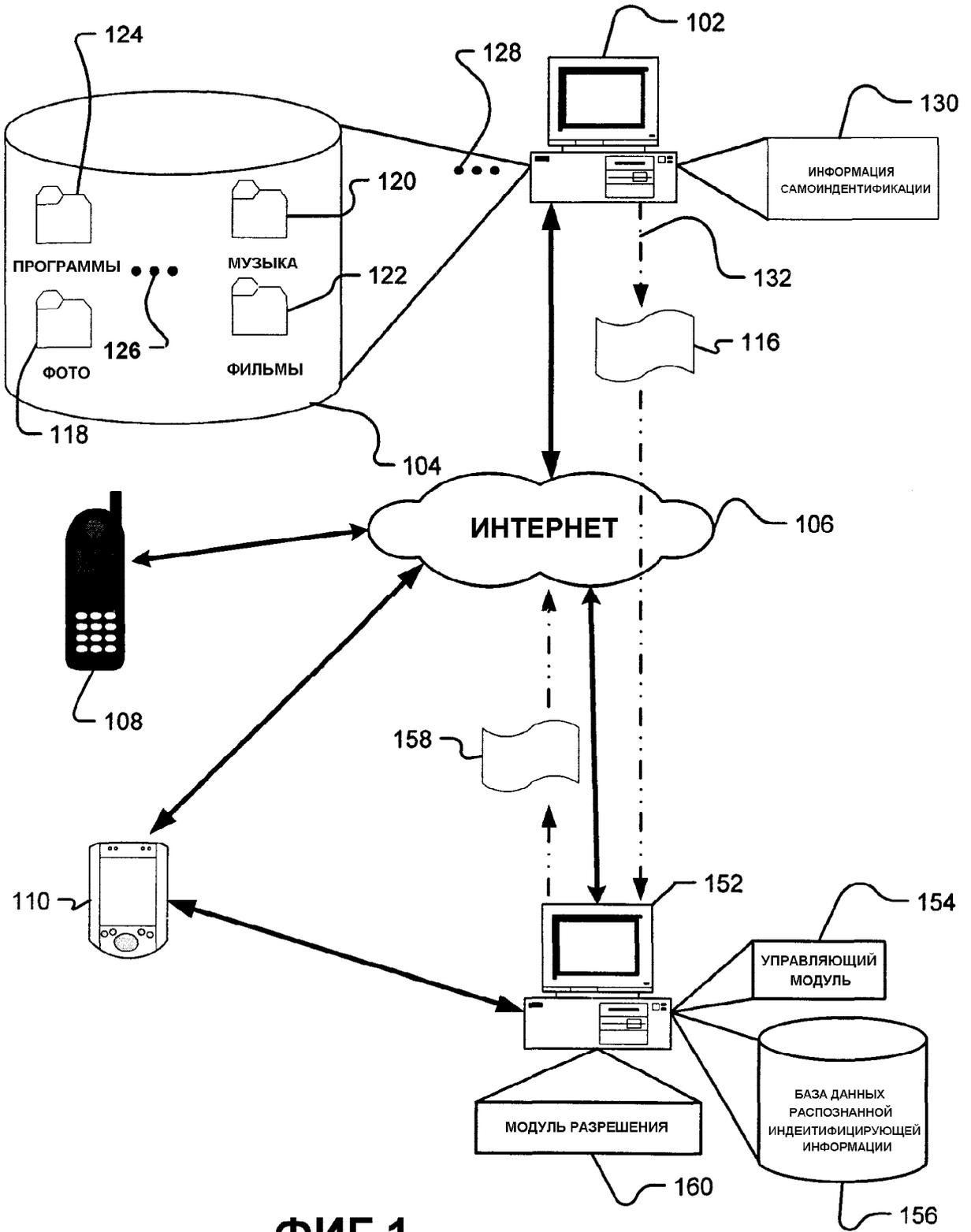
(73) Патентообладатель(и):

МАЙКРОСОФТ КОРПОРЕЙШН (US)**(54) СИСТЕМА И СПОСОБ ДЛЯ РАЗРЕШЕНИЯ ИМЕН**

(57) Реферат:

Изобретение относится к доступу и публикации документов между двумя компьютерными системами или узлами, которые соединены между собой в сетевой среде. Техническим результатом является расширение функциональных возможностей за счет облегчения нахождения местоположения машин. Система и способ для разрешения имен предусматривают сохранение документа идентифицирующей информации, содержащего удобный для пользователя дескриптор, обозначающий идентификационные данные,

например, адрес электронной почты, местоположение машины, например, IP-адрес, для публикующей компьютерной системы, где сохранены документы. Затем система и способ предусматривают перехват первоначального запроса на доступ к документам, если первоначальный запрос содержит удобный для пользователя дескриптор. А также замену удобного для пользователя дескриптора местоположением машины, так что сетевые пользователи могут легко получать доступ к этим документам, зная только удобный для пользователя дескриптор. 5 н. и 37 з.п. ф-лы, 7



ФИГ.1

RU 2373572 C2

RU 2373572 C2



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2005120234/09, 29.07.2004**
 (24) Effective date for property rights:
29.07.2004
 (30) Priority:
23.10.2003 US 10/693,516
 (43) Application published: **20.01.2006**
 (45) Date of publication: **20.11.2009 Bull. 32**
 (85) Commencement of national phase: **27.06.2005**
 (86) PCT application:
US 2004/024341 (29.07.2004)
 (87) PCT publication:
WO 2005/045741 (19.05.2005)
 Mail address:
129090, Moskva, ul. B.Spaskaja, 25, str.3, OOO
"Juridicheskaja firma Gorodisskij i Partnery",
pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
SATAGOPAN Merli (US),
KAMERON Kim (US)
 (73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

(54) SYSTEM AND METHOD FOR RESOLUTION OF NAMES

(57) Abstract:
 FIELD: information technologies.
 SUBSTANCE: invention is related to access and publication of documents between two computer systems or units, which are combined to each other in network environment. System and method for resolution of names provide for storage of identification information document, which contains user-friendly descriptor that indicates identification data, for instance email address, car location, for instance, IP-address, for publishing

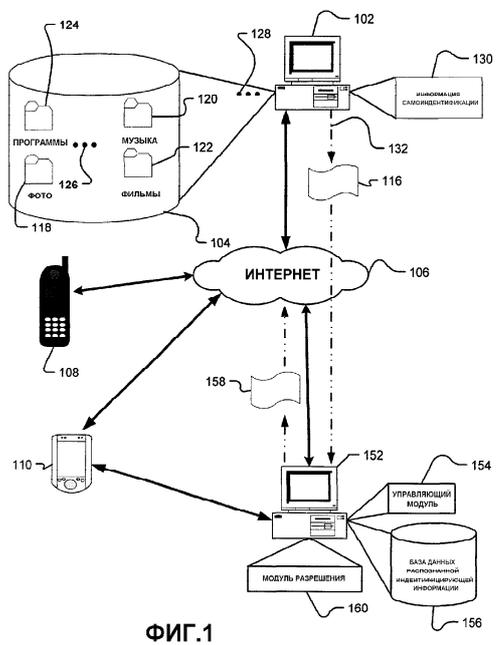
computer system, where documents are stored. Then system and method provide for wiretap of initial query for access to documents, if initial query contains user-friendly descriptor. And also for replacement of user-friendly descriptor with car location, so that network users may easily get access to these documents, knowing only user-friendly descriptor.

EFFECT: expansion of functional resources, due to facilitation of car location detection.

42 cl, 7 dwg

RU 2 373 572 C2

RU 2 373 572 C2



Область техники

Настоящее изобретение относится к публикации документов и информации, сохраненных на отдельных машинах или узлах в распределенной сети, и к использованию этих документов совместно с другими узлами в сети. Более конкретно, настоящее изобретение относится к системам и способам для обеспечения другого пользовательского доступа к таким опубликованным документам.

Предшествующий уровень техники

В распределенных сетях или системах, имеющих множество соединенных узлов или процессов, важной является возможность совместного использования файлов, документов и информации узлами в сети.

Существуют различные традиционные способы, которыми пользователи могут совместно использовать файлы и документы, включая посылку документов на web-серверы, где доступ может быть открыт любому или ограничен предварительно разрешенными пользователями посредством системы защиты с помощью пароля. Проблема с такой системой является двойкой. Во-первых, в типовом случае она требует участия третьей стороны, такой как web-сервис, для поддержки документов на компьютере-сервере, что требует в общем случае первоначальной платы за установку и периодической платы за поддержку. Во-вторых, участие третьей стороны очевидным образом снижает пользовательский контроль над файлами и документами, сохраненными на web-сервере.

Другим способом совместного использования файлов пользователями распределенной сети является тот, когда пользователь, желающий совместно использовать файлы («издатель») с другим пользователем («получающий доступ», «аксессуар»), снабжает «аксессуара» данными местоположения своей машины и именем пути на машине, где сохранены документы. «Аксессуар» получает доступ к документам «издателя» путем ввода местоположения машины и имени пути в web-браузер или другую программу доступа, чтобы попасть на машину «издателя». В этой ситуации машина «издателя» в типовом случае обеспечивает систему защиты, которая разрешает доступ только утвержденным обращающимся за доступом пользователям.

Для того чтобы ввести местоположение машины, пользователь должен знать его. Один из способов ввода местоположения машины связан с вводом адреса протокола Интернет (IP). IP-адрес является уникальной последовательностью чисел, которая идентифицирует компьютер в сети Интернет. IP-адреса содержат 32 бита, упорядоченные в четыре набора из трехразрядных чисел между 0 и 255, разделенных точками, например: 123.123.023.002. Все машины в Интернет должны иметь IP-адрес, и никакие две компьютерные системы не могут иметь одинаковый IP-адрес в одно и то же время. IP-адреса могут быть динамическими и статическими. Статический IP-адрес представляет собой адрес, постоянно назначенный компьютерной системе, - это единственный IP-адрес, используемый данной системой. Динамический IP-адрес является адресом, который присваивается «на лету» из группы IP-адресов, присвоенных, например, организации. Хотя ни один IP-адрес не может использоваться для двух компьютерных систем в одно и то же время, каждая компьютерная система может использовать множество различных IP-адресов. IP-адреса не удобны для пользователя, поскольку они содержат только числа, без легко понятного значения. По этой причине для пользователей практически невозможно запомнить их собственные IP-адреса, не говоря уже об IP-адресах машин, принадлежащих другим пользователям.

Система имен доменов (DNS) облегчает нахождение местоположений машин, позволяя использовать знакомую последовательность букв («доменное имя») вместо скрытого IP-адреса. Так, вместо запоминания и печатания последовательности 66.201.69.207 пользователи могут ввести `www.microsoft.com`.

5 Доменные имена также используются для нахождения адресов электронной почты и для других Интернет-приложений. Доменные имена разрешаются, т.е. преобразуются из доменного имени в IP-адрес, с помощью сервиса, размещенного на ряде серверов, расположенных в сети Интернет. Однако система DNS имеет, по меньшей мере, два
10 ограничения. Во-первых, она требует использования оборудования третьей стороны, то есть DNS-серверов, для реализации обработки разрешения имен. Во-вторых, она недостаточно защищенная, так как почти любой может определить конкретное имя машины и местоположение для любой компьютерной системы. Поэтому обычная
15 система DNS не обеспечивает достаточно эффективного метода для публикации ресурсов в компьютерной системе.

Другим способом получения местоположения машины является использование открытого ключа. Открытые ключи ассоциированы с конкретным лицом и состоят из длинной последовательности байтов, например, из 32 цифр и букв, такой
20 как `KP12JSP2345L1298FE23CLKSERQOC38S`. Открытые ключи в типовом случае используются для обеспечения возможности пользователям незащищенной сети общего пользования, такой как Интернет, обмениваться данными защищенным и конфиденциальным образом путем использования пары ключей, состоящей из
25 открытого и секретного ключей, получаемой и совместно используемой через доверительный орган. Криптография на основе открытого ключа является наиболее широко распространенным методом в Интернет для аутентификации отправителя сообщения или шифрования сообщения. Открытые ключи могут быть получены
30 рядом способов. Например, открытый ключ может быть создан и присвоен операционной системой, когда некоторое лицо создает пользовательскую учетную запись в компьютерной системе. Альтернативно, в криптографии открытых ключей открытый ключ и секретный ключ создаются одновременно с использованием одного и того же алгоритма органом распределения сертификатов.

Открытые ключи связаны с местоположениями машин за счет использования
35 протокола PNRP (протокол разрешения имени группы), который сохраняет открытый ключ каждого лица с его текущим местоположением в общедоступной таблице или в некоторой другой структуре данных, в которой может быть проведен поиск. Таким образом, если известен открытый ключ лица, то можно использовать протокол PNRP
40 для определения ассоциированного текущего местоположения машины, которое обычно представляется в форме IP-адреса. Однако, подобно IP-адресу, открытый ключ является последовательностью из множества битов, которые не имеют смыслового содержания и которые еще труднее запоминать, чем сам IP-адрес.

Еще один способ определения местоположения машины связан с получением
45 (например, посредством электронной почты) связи (ссылки), которая воплощает в себе или содержит местоположение машины. Когда эта связь выбрана, браузер автоматически вводит IP-адрес или открытый ключ, ассоциированный со связью, в браузер. Однако, к сожалению, лицо, получающее доступ, должно сохранять
50 электронную почту, находить и открывать ее всякий раз, когда обращающийся за доступом узел желает получить доступ к ресурсам публикующего узла. Эта процедура требует затрат времени, является громоздкой и напрасно расходует емкость памяти на машине пользователя обращающегося за доступом узла.

Изобретение может быть реализовано как компьютерный процесс, вычислительная система или как продукт производства, такой как компьютерный программный продукт или машиночитаемый носитель. Компьютерный программный продукт может представлять собой компьютерный носитель для хранения данных, считываемый компьютерной системой и кодирующий компьютерную программу команд для исполнения компьютерной обработки. Компьютерный программный продукт может, таким образом, представлять собой распространяющийся сигнал на носителе, считываемом вычислительной системой, и кодировать компьютерную программу команд для исполнения компьютерной обработки.

Эти и различные другие признаки, а также преимущества, которые характеризуют настоящее изобретение, поясняются в нижеследующем детальном описании, иллюстрируемом чертежами.

Сущность изобретения

Настоящее изобретение относится к доступу и публикации документов между двумя компьютерными системами или узлами, которые соединены между собой в сетевой среде, в частности, к системе и способу для разрешения имен между удобным для пользователя дескриптором, обозначающим идентичность с местоположением машины, где сохранены документы, так что сетевые пользователи могут легко получать доступ к этим документам через знание удобного для пользователя дескриптора. Иными словами, к документам пользователя может быть обеспечен доступ за счет использования удобного для пользователя дескриптора, идентифицирующего пользователя, и имени пути, которое описывает документы, представляющие интерес, которые разрешаются с использованием местоположения машины, где документы сохранены. Адрес электронной почты является примером удобного для пользователя дескриптора, а IP-адрес или открытый ключ являются примерами местоположений машины. Компьютерная система или узел, где сохранены документы, упоминаются далее как публикующая компьютерная система или узел, а компьютерная система, которая запрашивает доступ к документам, сохраненным на публикующем узле, упоминается как обращающаяся за доступом компьютерная система или узел.

В соответствии с конкретными аспектами способ доступа к документам, сохраненным на первой публикующей компьютерной системе, через вторую обращающуюся за доступом компьютерную систему начинается, когда документ идентифицирующей информации с первой компьютерной системы сохраняется на второй компьютерной системе. Документ идентифицирующей информации имеет, как минимум, удобный для пользователя дескриптор, идентифицирующий лицо и местоположение машины для первой компьютерной системы. Когда делается первоначальный запрос для доступа к документам, содержащим удобный для пользователя дескриптор, он принимается (перехватывается) второй компьютерной системой. Вторая компьютерная система заменяет удобный для пользователя дескриптор местоположением машины и посылает измененный запрос в местоположение машины первой компьютерной системы. Этот способ позволяет второй компьютерной системе получать доступ к документам на первой компьютерной системе, зная только удобный для пользователя дескриптор. Знание местоположения машины, IP-адреса или открытого ключа для первой компьютерной системы не обязательно.

В соответствии с другими аспектами настоящее изобретение относится к способу публикации документов между множеством узлов, соединенных в сетевой среде.

Способ начинается с посылки документа идентифицирующей информации от публикующего узла к обращающемуся за доступом узлу. Документ идентифицирующей информации включает в себя, по меньшей мере, удобный для пользователя дескриптор, идентифицирующий главного пользователя, и местоположение машины для публикующего узла. Документ идентифицирующей информации после этого сохраняется в обращающемся за доступом узле. Когда первоначальный запрос на доступ к документам делается из обращающегося за доступом узла к публикующему узлу, удобный для пользователя дескриптор разрешается с использованием местоположения машины. Затем измененный запрос для доступа к документам посылается из обращающегося за доступом узла в местоположение машины публикующего узла.

В соответствии с еще одним аспектом настоящее изобретение относится к компьютерной системе, содержащей модуль хранения для хранения документа идентифицирующей информации, принятого от второй компьютерной системы, и модуль разрешения имени, соединенный с модулем хранения. Модуль разрешения имени принимает запросы для доступа к документам, сохраненным соответственно удобному для пользователя дескриптору документа идентифицирующей информации, и изменяет запрос для замены удобного для пользователя дескриптора местоположением машины из документа идентифицирующей информации.

В соответствии с другими аспектами настоящее изобретение относится к машиночитаемому носителю, кодирующему компьютерную программу команд для исполнения компьютерным процессом разрешения имен. Процесс начинается с операции сохранения, сохраняющей документ идентифицирующей информации из публикующей компьютерной системы. Затем операция перехвата (приема) перехватывает первоначальный запрос на доступ к документам, сохраненным в публикующей компьютерной системе, если первоначальный запрос содержит удобный для пользователя дескриптор. Наконец, операция изменения изменяет запрос путем замены удобного для пользователя дескриптора местоположением машины.

Краткое описание чертежей

Фиг.1 - иллюстрация коммуникационной системы или распределенной сети узлов, воплощающей аспекты настоящего изобретения.

Фиг.2 - компьютерная система, которая может быть использована в соответствии с конкретными аспектами настоящего изобретения.

Фиг.3 - структура документа идентифицирующей информации согласно конкретным аспектам настоящего изобретения.

Фиг.4 - представление программной среды в соответствии с аспектами настоящего изобретения.

Фиг.5 - блок-схема рабочих характеристик настоящего изобретения по отношению к обращающемуся за доступом узлу.

Фиг.6 - блок-схема операционных характеристик альтернативного варианта осуществления настоящего изобретения по отношению к публикующему узлу.

Фиг.7 - блок-схема операционных характеристик другого альтернативного варианта осуществления настоящего изобретения по отношению к обращающемуся за доступом узлу и публикующему узлу.

Детальное описание предпочтительного варианта осуществления

Распределенная среда 100, воплощающая аспекты настоящего изобретения, показана на фиг.1. Среда 100 содержит, по меньшей мере, одну компьютерную систему 102 и потенциально другие компьютерные системы, такие как 108, 110 и 152,

причем различные компьютерные системы упоминаются как «узлы» и как «машины». В том виде как используется в настоящем описании, термин «компьютерная система» должен пониматься в широком смысле и определяется как «одно или более устройств или машин, которые выполняют программы для отображения и обработки текста, графики, символов, аудио, видео и/или цифровых данных». Узлы в сети могут представлять собой компьютерную систему любого типа, включая, без ограничения указанным, телефон в виде узла 108, PDA (цифровой персональный помощник) в виде узла 110, настольный компьютер в виде узлов 102 и 152, компактный портативный компьютер (не показан) и многие другие устройства. Кроме того, хотя узлы 102, 108, 110 и 152 показаны как компьютерные системы, альтернативно они могут представлять собой компьютерные процессы в компьютерной системе. Альтернативно, узлы 102, 108, 110 и 152 могут образовывать комбинацию из отдельных компьютерных систем, распределенных в локальной сети, глобальной сети или комбинацию отдельных сетевых коммуникаций.

Как указано, каждая из компьютерных систем 102, 108, 110 и 152 рассматривается как узел в среде 110, имеющий возможность информационного обмена с другими узлами в среде 100 и использующий документы, информацию и ресурсы совместно с другими узлами. Кроме того, узлы могут осуществлять связь с использованием отдельных протоколов, таких как TCP/IP (протокол управления передачей/межсетевой протокол) или другие сетевые и/или коммуникационные протоколы, реализуемые в сетях, таких как Интернет. То есть, хотя отдельные узлы 102, 108, 110 и 152 показаны как соединенные видимым образом прямыми стрелками, в действительности они могут быть соединены с другими узлами посредством не прямых путей. На самом деле соединения, представленные в среде 100, просто показывают, что узел может связываться с другим узлом.

Связь между машинами 102, 108, 110 и 152 может осуществляться, как указано, посредством множества коммуникационных протоколов. Определение связи (информационного обмена), используемое в настоящем описании, может относиться к передаче сообщения, события или любой другой информации от одного узла к другому. В одном варианте осуществления узлы в среде 100 могут иметь возможность связываться со всеми другими узлами в сети 100, но такое требование не является обязательным. Для того чтобы передать информацию от первого узла к второму узлу, первому узлу необходимо местоположение или некоторая другая идентификационная информация для доступа к узлу. Используя местоположения машины, передающий узел может послать информацию с использованием любого протокола передачи.

Хотя на фиг.1 показаны только четыре узла 102, 108, 110 и 152, сетевая среда может включать в себя другие узлы. На самом деле, число узлов для среды 100 может быть весьма большим, порядка тысяч и до десятков тысяч и более. Следовательно, настоящее изобретение имеет преимущество, состоящее в возможности масштабирования среды 100 в соответствии с потребностями, так что практически любое количество узлов может передавать информацию в соответствии с настоящим изобретением.

Настоящее изобретение относится к удобной для пользователя системе и способу для публикации или совместного использования ресурсов, сохраненных на одном сетевом узле, называемом «публикующим узлом», с другим сетевым узлом, называемым «обращающимся за доступом узлом». Компьютерная система 102 является примером публикующего узла и включает в себя базу 104 данных, в которой данные организованы в одной или более директорий или папок, таких как папки

118, 120, 122 и 124. База 104 данных относится к типовой файловой системе или другой организованной системе данных для хранения и извлечения электронных документов. Как таковая база 104 данных может включать в себя любой тип данных или файла, которые упоминаются как «документы». Термин «документы» должен пониматься в широком смысле и может включать в себя, без ограничения указанным, фотоснимки, видеоклипы, аудиоклипы, текстовые файлы, презентации, программный код или любые другие персональные ресурсы, сохраненные на компьютерной системе. Документы могут быть организованы в базе данных любым способом, включая, без ограничения указанным, папки и подпапки с описательными именами. Например, папка 118 может содержать «jpeg»-файлы и именоваться как «фото», папка 120 может содержать аудиоклипы и обозначаться как «музыка», папка 122 может содержать «mpeg»-файлы и обозначаться как «видео», и папка 124 может содержать исполняемый код и обозначаться как «программы». Трехточие 126 указывает, что в общем случае может иметься любое количество папок в базе 104 данных, содержащей любые типы документов.

Хотя показана только одна база 104 данных, трехточие 128 указывает, что машина 102 может иметь более одной базы данных, организованных тем же или иным способом, по сравнению с базой 104 данных. Например, база 104 данных может предназначаться для главного пользователя машины и сохраняться в профиле главного пользователя, размещенном на машине. Термин «главный пользователь», в том виде как он используется в настоящем описании, должен пониматься в широком смысле и определяться как любой объект, способный выполнять цифровые операции. Главные пользователи включают в себя, без ограничений указанным, индивидуальных людей, группы или множества людей, понимая под этим индивидуумов, домашние хозяйства, организации, явно выраженные группы, и людей в обычной их роли или людей, совместно использующих атрибуты некоторого рода, а также различные электронные устройства, посредством которых эти индивидуумы действуют. Другой главный пользователь может иметь другую базу данных, сохраненную на машине 102, доступную только для данного главного пользователя.

Компьютерная система 102 дополнительно поддерживает набор информации 130 самоидентификации, которая включает в себя различную информацию о главном пользователе, представленном или использующем компьютерную систему 102. Эта информация, например, может включать в себя имя, адрес электронной почты, URL (универсальный указатель ресурса) web-сайта, физический почтовый адрес, местоположение машины для компьютерной системы главного пользователя и другую персональную информацию, а также стратегию использования, описывающую, каким образом эта информация может быть использована. Каждый из этих различных идентифицирующих элементов упоминается далее как идентификационная заявка. Важно, что набор идентификационных заявок включает в себя, по меньшей мере, удобный для пользователя дескриптор, идентифицирующий компьютерную систему 102 и местоположение машины.

Компьютерная система 102 может создавать документ 116 идентифицирующей информации, содержащий некоторую или всю информацию 130 самоидентификации, и посылать документ 116 идентифицирующей информации в любой другой узел в среде 100, как показано пунктирными стрелками 132 на фиг.1. Как использовано в настоящем описании, термин «документ идентифицирующей информации» должен означать подмножество идентифицирующей информации для главного пользователя, передаваемое от одной машины к другой машине таким образом, чтобы позволить

устройству, принимающему документ идентифицирующей информации, распознать главного пользователя и цифровые события, связанные с главным пользователем. Детальные особенности возможного формата для документа 116 идентифицирующей информации описаны ниже со ссылкой на фиг.3. Однако, вообще говоря, документ 116 5 идентифицирующей информации может быть в формате, подходящем для передачи информации между неравноправными системами, по каналам различных типов. Каналы, используемые для передачи документа 116 идентифицирующей информации от компьютерной системы 102 к принимающей системе, такой как компьютерная 10 система 152, могут быть любыми возможными средами передачи. Например, электронная почта, мгновенная передача сообщений, направленная передача и многие другие механизмы могут использоваться в качестве каналов. Кроме того, каналы могут быть защищенными или незащищенными.

Компьютерная система 152 является примером обращающегося за доступом узла и 15 содержит управляющий модуль 154, который считывает входящий документ 116 идентифицирующей информации и принимает его или отклоняет его в зависимости от различных переменных. Например, если документ 116 идентифицирующей информации исходит от известного главного пользователя, то компьютерная 20 система 152 примет и сохранит документ 116 идентифицирующей информации. Однако если документ 116 идентифицирующей информации поступает от неизвестного главного пользователя или если имеется опасение того, что у мошенников имелась достаточная мотивация открыть и модифицировать или фальсифицировать документ 116 идентифицирующей информации, то компьютерная система 152 может 25 отклонить документ 116 идентифицирующей информации или предпринять попытку дополнительной верификации его аутентичности.

В одном варианте осуществления, после того как документ 116 идентифицирующей информации принят, заявки идентификации, которые он содержит, добавляются к 30 базе 156 данных распознанной идентифицирующей информации, которая может использовать эту информацию для верификации и аутентификации компьютерной системы 102 в будущем и использовать каналы взаимодействия с тем главным пользователем, достоверность которого иным путем не может быть установлена. Главный пользователь, представленный документом 116 идентифицирующей 35 информации, может затем, например, быть верифицированным и получать доступ к ресурсам на компьютерной системе 152, таким как документы, сохраненные в базе данных, подобной базе 104 данных компьютерной системы 102.

Дополнительно, после того как компьютерная система 152 приняла и сохранила 40 документ 116 идентифицирующей информации в своей базе 156 данных, она может использовать заявки идентификации для главного пользователя компьютерной системы 102, чтобы более просто и быстро получить доступ к документам, содержащимся в базе 104 данных компьютерной системы 102, как пояснено ниже со ссылками на фиг.4-6.

Однако в общем случае компьютерная система 152 содержит модуль 160 45 разрешения, который перехватывает запросы на доступ к документам на компьютерной системе 102, которые могут поступить от главного пользователя компьютерной системы 152 или могут возникнуть автоматически. Первоначальный 50 запрос от главного пользователя включает в себя удобный для пользователя дескриптор, например, заявку идентификации удобного для пользователя дескриптора от компьютерной системы 102. Модуль 160 разрешения преобразует удобный для пользователя дескриптор в местоположение машины, также полученное от

компьютерной системы 102, и вводит соответствующую информацию в web-браузер компьютерной системы 152, который, в свою очередь, получает доступ к запрошенным данным на компьютерной системе 102. Вследствие операции разрешения модуля 160 разрешения главному пользователю компьютерной системы 252 нет необходимости запоминать местоположение машины, IP-адрес или открытый ключ для компьютерной системы 102, а вместо этого нужно только запомнить удобный для пользователя дескриптор (и ассоциированный путь).

В одном варианте осуществления настоящего изобретения компьютерная система 152 также содержит информацию самоидентификации (не показана), а компьютерная система 102 также содержит управляющий модуль (не показан) и базу данных распознанной идентифицирующей информации (не показана). Для того чтобы главному пользователю компьютерной системы 152 получить доступ к документам в базе 104 данных компьютерной системы 102, главный пользователь компьютерной системы 152 должен послать свой собственный документ 158 идентифицирующей информации компьютерной системе 102, прежде чем он получит доступ к документам в базе 104 данных. Иными словами, должен иметь место взаимный обмен документами 116 и 158 идентифицирующей информации для главного пользователя компьютерной системы 152, чтобы простым способом запросить и получить доступ к документам в базе 104 данных. Альтернативно, компьютерная система 102 может не потребовать никакого процесса верификации или аутентификации и может разрешить любому обращающемуся за доступом главному пользователю доступ к документам, содержащимся в базе 104 данных. В этом случае только компьютерной системе 102 необходимо послать документ 116 идентифицирующей информации компьютерной системе 152, чтобы система 152 получила доступ к базе 104 данных. То есть требуется только односторонний обмен документами идентифицирующей информации от публикующего узла к обращающемуся за доступом узлу.

Фиг.2 показывает компьютерную систему 200, которая может представлять один из узлов, такой как 102 или 152, показанных на фиг.1, который получает и распространяет информацию и публикует и совместно использует документы в соответствии с настоящим изобретением. Система 200 имеет, по меньшей мере, один блок 202 обработки (процессор) и память 204. Процессор 202 использует память 204 для хранения документов в базах данных, таких как база 104 данных, информация 130 самоидентификации и база 156 данных распознанной идентифицирующей информации.

В наиболее базовой конфигурации вычислительная система 200 показана на фиг.2 пунктирной линией 206. Дополнительно система 200 может включать в себя дополнительные устройства хранения данных (съёмные и/или несъёмные), такие как, например, магнитные диски, оптические диски, магнитную ленту. Такие дополнительные устройства хранения показаны на фиг.2 съёмным устройством 208 хранения данных и несъёмным устройством 210 хранения данных. Компьютерные носители (среды) для хранения данных могут включать в себя энергозависимые и энергонезависимые, съёмные и несъёмные носители, реализованные любым способом или технологией для хранения информации, такой как машиночитаемые команды, структуры данных, программные модули и другие данные. Память 204, съёмное устройство 208 хранения данных и несъёмное устройство 210 хранения данных являются примерами компьютерных носителей для хранения данных. Компьютерные носители для хранения данных включают в себя, без ограничения указанным, RAM, ROM, EEPROM (электронно-стираемую программируемую постоянную память), флэш-память или другую технологию памяти, CD-ROM, DVD (цифровые

многофункциональные диски), или другие оптические устройства хранения данных, устройства хранения на магнитных кассетах, магнитных лентах, магнитных дисках и другие магнитные устройства хранения данных, или любые другие носители, которые могут быть использованы для хранения необходимой информации и доступ к которым может быть обеспечен с помощью системы 200. Любой такой носитель для хранения данных может представлять собой часть системы 200. В зависимости от конфигурации и типа вычислительного устройства память 204 может быть энергозависимой, энергонезависимой или некоторой комбинацией этих двух типов.

Система 200 может также содержать коммуникационные соединения 212, которые позволяют устройству осуществлять связь с другими устройствами, такими как другие узлы 108, 110 или 152, показанные на фиг.1. Дополнительно система 200 может иметь устройства 214 ввода, такие как клавиатура, мышь, перо, устройство голосового ввода, устройство сенсорного ввода и т.д. Также могут быть включены устройства 216 вывода, такие как дисплей, динамики, принтер и т.д. Все эти устройства хорошо известны в технике и не требуют дополнительного описания.

Компьютерная система 200 в типовом случае включает в себя, по меньшей мере, некоторую форму машиночитаемого носителя (среды). Машиночитаемая среда может представлять собой любую доступную среду, к которой система 200 может иметь доступ. Машиночитаемые носители описаны выше. Среда передачи может в типовом случае быть реализована посредством машиночитаемых команд, структур данных, программных модулей или других данных в модулированном сигнале данных, таком как несущее колебание или другой транспортный механизм, и включает в себя любую среду доставки информации. Термин «модулированный сигнал данных» означает сигнал, который имеет одну или более характеристик, установленных или изменяющихся таким образом, чтобы кодировать информацию в сигнале. Например, но не в качестве ограничения, среда передачи включает в себя проводную среду, такую как проводная сеть или непосредственное проводное соединение, и беспроводную среду, такую как акустическая, радиочастотная, инфракрасная и другие беспроводные среды передачи. Комбинации вышеприведенных типов также должны быть включены в объем машиночитаемого носителя (среды).

Фиг.3 иллюстрирует примерный формат документа 300 идентифицирующей информации, который может представлять один или оба из показанных на фиг.1 документов 116 и 158 идентифицирующей информации. В качестве структуры данных документ 300 идентифицирующей информации представляет собой набор заявок идентификации и других заявок атрибутов/свойств, которые могут быть связаны с открытым ключом и управляться заложенной стратегией использования. Язык XML может использоваться в качестве языка кодирования для документа идентифицирующей информации. Однако другие форматы также рассматриваются в качестве пригодных для использования. Элементы документа 300 идентифицирующей информации могут быть дополнительно зашифрованы, если они содержат информацию, которая должна поддерживаться конфиденциальной.

Данные в документе 300 идентифицирующей информации могут быть разделены на две категории, включая набор логических компонентов 302 и набор тегов (дескрипторов) 316 атрибутов. Документ 300 идентифицирующей информации имеет шесть логических компонентов главного пользователя: 1) идентификатор 304 главного пользователя; 2) одну или более заявок 306 идентификации главного пользователя; 3) имя дисплея и нуль или более селективно раскрытых атрибутов 308 главного пользователя; 4) один или более ключей 310 для главного пользователя,

скомпонованных в любых приемлемых форматах (например, открытые ключи в сертификатах X509v3); 5) использование стратегии 312, которая выражает требования конфиденциальности главного пользователя; и б) цифровая подпись 314 для всего содержимого идентифицирующей информации, которая защищает целостность
5 данных и аутентифицирует отправителя в случае обновлений идентифицирующей информации. Каждый из этих шести логических компонентов 302 описан ниже.

Идентификатор 304 главного пользователя представляет собой удобный для
10 пользователя дескриптор, который идентифицирует главного пользователя, который является главным пользователем заявок идентификации, содержащихся в документе 300 идентификационной информации. Предпочтительный идентификатор 304 главного пользователя является адресом электронной почты главного пользователя, если главный пользователь является лицом. Однако
15 идентификатор главного пользователя должен трактоваться в широком смысле как любой тип удобного для пользователя дескриптора, который уникальным образом идентифицирует главного пользователя и может включать в себя, без ограничений указанным, адреса электронной почты, номера телефонов, номера мобильных телефонов и т.д.

20 Заявки 306 идентификации включают в себя дополнительную структурированную информацию, относящуюся к главному пользователю, который является субъектом документа идентифицирующей информации. Заявки 306 идентификации должны рассматриваться в широком смысле как описательная информация, касающаяся
25 главного пользователя, которая может включать в себя, без ограничения указанным, физические почтовые адреса, номера телефонов и факсимильных аппаратов, информацию работодателя, дату рождения и т.д. Более конкретно, «заявки идентификации» уникальным образом действительны для одного объекта (лица, организации и т.д.). Таким образом, в некоторых случаях номер телефона может быть
30 действительной заявкой идентификации для одного лица. Например, номер сотового телефона, номер рабочего телефона прямого вызова или домашний номер телефона может быть действительной заявкой идентификации для некоторого индивидуума, который индивидуально использует сотовый телефон или номер прямого вызова или
35 который живет один. В других случаях телефон не может быть действительной заявкой идентификации для одного лица, если домашний номер телефона совместно используется членами семьи. В таком случае домашний номер телефона мог бы быть заявкой идентификации для представления домашнего хозяйства, но не индивидуального лица.

40 Местоположение 308 машины обеспечивает уникальный адрес для компьютерной системы главного пользователя и может включать в себя, без ограничения указанным, IP-адрес или открытый ключ. Подобно физическому адресу с указанием улицы, местоположение машины необходимо для определения местоположения, установления соединения и коммуникации с компьютерной системой в
45 распределенной сети. Местоположение 308 машины может в действительности включать в себя список местоположений машины, если главный пользователь 308 имеет более одной компьютерной системы или если компьютерная система является мобильной, например, такой как компактная портативная компьютерная система или
50 персональный цифровой помощник (PDA). В одном варианте осуществления каждое местоположение машины может содержать список документов, сохраненных в данном местоположении машины. Например, если главный пользователь имеет первую компьютерную систему, в которой сохранены jpeg-файлы под именем пути

«фото», и вторую компьютерную систему, в которой сохранены звукозаписи под именем пути «музыка», местоположение 308 машины может включать в себя IP-адрес для каждой из первой и второй компьютерных систем и указание того, что файлы «фото» сохранены в местоположении машины для первой компьютерной системы и что файлы «музыка» сохранены в местоположении машины для второй компьютерной системы.

Компонент 310 ключей содержит один или более ключей, таких как открытые ключи, инкапсулированные в формате сертификата (например, сертификатов X509v3). Ключи 310 могут быть открытыми ключами и могут быть включены в идентификационную информацию как информация распознавания или субъект идентификационной информации. Если используется сертификат, он может быть подписанным самостоятельно или выданным органом распределения сертификатов.

Стратегия 312 использования передает инструкции главного пользователя относительно разрешенных использований содержимого документа 300 идентифицирующей информации. Например, стратегия 312 использования может указывать, что содержимое идентифицирующей информации не должно разглашаться другим сторонам. База данных распознанной идентифицирующей информации получателя, такая как база 156 данных на фиг.1, должна сохранять стратегию использования вместе с остальной информацией, определяющей главного пользователя.

Цифровая подпись 314 обеспечивает главному пользователю возможность подписывать данные в документе идентифицирующей информации. XML-подписи имеют три способа связывания подписи с документом: она является охватывающей, или охватываемой, или отсоединенной. В соответствии с одним вариантом осуществления настоящего изобретения документ идентифицирующей информации использует охватываемую XML-подпись при подписании содержания идентифицирующей информации.

Документ 300 идентифицирующей информации может содержать шесть или более тегов 316 атрибутов, относящихся к собственно документу 300 идентифицирующей информации. Хотя не показано, однако теги атрибутов могут включать в себя значения идентификатора (ИД) для документа 300 идентифицирующей информации, информацию версии для документа 300 или тип главного пользователя, который представляет документ 300, например, лицо, компьютер или организация. Другие теги атрибутов также могут использоваться.

В одном варианте осуществления документ идентифицирующей информации сохранен обобщенным способом на основной компьютерной системе, такой как системы 102 и 402, описанные выше со ссылками на фиг.1 и 4 соответственно.

На фиг.4 показаны функциональные компоненты, связанные с доступом и совместным использованием или публикацией документов между двумя или более компьютерными системами 402 и 450. То есть фиг.4 представляет компоненты или модули программного обеспечения согласно аспектам настоящего изобретения. В частности, фиг.4 иллюстрирует публикующий узел или компьютерную систему 402 и обращающийся за доступом узел или компьютерную систему 452 и связанные с ними модули, используемые для публикации и доступа к документам согласно настоящему изобретению. Компьютерная система 402 имеет в числе других модулей, которые не показаны, следующие компоненты: 1) базу данных 404; 2) модуль 414 документов идентифицирующей информации; 3) модуль 416 пользовательского интерфейса; 4) модуль 418 верификации и публикации; 5) модуль 420 доступа к памяти; 6)

коммуникационный модуль 422 и (7) базу 424 данных информации самоидентификации.

Подобно базе 104 данных, показанной на фиг.1, база 404 данных содержит документы, которые могут быть организованы в папки 406, 408, 410 и 412. В этом примере эти документы представляют документы, подлежащие публикации для системы 452, следовательно, к которым получает доступ система 452.

Модуль 416 пользовательского интерфейса позволяет главному пользователю компьютерной системы 402 получать доступ и управлять любыми другими модулями, включая, без ограничения указанным, модуль 420 доступа к памяти, модуль 414 идентифицирующей информации и коммуникационный модуль 422. Хотя настоящее изобретение и, в частности, пример, представленный на фиг.4, предусматривает пользовательское взаимодействие на системе 402, оно не является обязательным для реализации аспектов настоящего изобретения.

Модуль 420 доступа к памяти позволяет компьютерной системе 402 и/или главному пользователю получать доступ к данным, сохраненным в системе, таким как данные, содержащиеся в базе 402 данных, и/или данные, содержащиеся в базе 424 данных информации самоидентификации.

Альтернативно, компьютерная система 402 может получать доступ к модулю 420 доступа к памяти через другие модули, такие как модуль 414 документов идентифицирующей информации или модуль 418 верификации и публикации. Главный пользователь использует модуль 416 пользовательского интерфейса для управления модулем 420 доступа к памяти.

Модуль 414 документов идентифицирующей информации создает документы идентифицирующей информации, такие как документ 300 идентифицирующей информации, показанный на фиг.3, с использованием считывания из модуля 414 доступа к памяти для извлечения данных из базы 424 данных информации самоидентификации. Модуль 414 документов идентифицирующей информации может создать документ идентифицирующей информации по команде от главного пользователя через модуль 416 пользовательского интерфейса или может альтернативно создавать документы идентифицирующей информации через стандартизованную процедуру без непосредственной команды от главного пользователя. Модуль 414 документов идентифицирующей информации передает документ идентифицирующей информации к коммуникационному модулю 422 для передачи к другим узлам в сети. В других вариантах осуществления документ идентифицирующей информации просто сохраняется в памяти, и по запросу документ передается к другой системе через коммуникационный модуль 422.

Коммуникационный модуль 422 управляет передачами между компьютерной системой 402 и другими узлами сети, включая как передачу информации к другим узлам сети, так и прием информации от других узлов сети, таких как компьютерная система 452. В общем случае главный пользователь управляет коммуникационным модулем 422 через модуль 416 пользовательского интерфейса и может посредством этого процесса выдать команду, чтобы послать документ идентифицирующей информации к другим компьютерным системам, таким как компьютерная система 452. Коммуникационный модуль 422 также позволяет главному пользователю посылать другие типы информации, такие как электронная почта, к другим узлам сети.

Модуль 418 верификации и публикации принимает запросы на доступ и публикацию документов, таких как находящиеся в базе 404 данных, от других узлов сети через коммуникационный модуль 422. В одном варианте осуществления модуль 418 верификации и публикации выполняет функцию «сторожа» и пытается проверить,

имеет ли обращающаяся за доступом компьютерная система разрешение от главного пользователя на прием публикуемых документов. Если разрешение имеется, то модуль 418 верификации и публикации использует модуль 420 доступа к памяти для извлечения запрошенных документов и публикует документы путем посылки их в коммуникационный модуль 422 для передачи обращающейся за доступом компьютерной системе. Если разрешения нет, то модуль 418 верификации и публикации отклоняет запрос на публикацию, который пересылается «ассессору» через коммуникационный модуль 422. В альтернативном варианте осуществления модуль 418 верификации и публикации не выполняет функцию «сторожа», а просто извлекает и публикует все запрашиваемые документы.

Компьютерная система 452 является примером обращающегося за доступом узла, подобно узлу 152 на фиг.1, и содержит следующие компоненты: 1) коммуникационный модуль 454, 2) модуль 460 верификации; 3) модуль 458 хранения; 4) модуль 456 разрешения имен и 5) модуль 462 пользовательского интерфейса.

Подобно модулю 416 пользовательского интерфейса, модуль 462 пользовательского интерфейса позволяет главному пользователю компьютерной системы 452 получать доступ и управлять любыми из других модулей, включая, без ограничения указанным, коммуникационный модуль 454. Так, например, главный пользователь системы 452 может использовать модуль 462 пользовательского интерфейса для выдачи команды коммуникационному модулю 454 послать запрос на публикацию документов к публикующему узлу 402.

Подобно коммуникационному модулю 422, коммуникационный модуль 454 управляет коммуникациями между компьютерной системой 452 и другими узлами сети, включая как посылку, так и прием информации от других узлов, таких как компьютерная система 402. Коммуникационный модуль 454 обеспечивает передачу документов идентифицирующей информации, которые он принимает от других узлов сети, в модуль 460 верификации.

Модуль 460 верификации обеспечивает преобразование документов идентифицирующей информации и определение, исходят ли они из достоверного источника, достоверного канала или могут быть аутентифицированы иным образом. Если документ идентифицирующей информации принят, модуль верификации передает документ идентифицирующей информации в модуль 458 хранения. По существу модуль 460 верификации связан с некоторыми функциями модуля 154 управления по фиг.1 в том, что он считывает поступающий документ 116 идентифицирующей информации и принимает или отклоняет его в зависимости от различных переменных.

Модуль 458 хранения сохраняет документ идентифицирующей информации для последующих использований компьютерной системой 452. Как в случае модуля 460 верификации, модуль 458 хранения также выполняет некоторые из функций модуля 154 управления, показанные и описанные со ссылками на фиг.1, заключающиеся в том, что он сохраняет принятые документы идентифицирующей информации.

Наконец, модуль 456 разрешения имен обеспечивает перехват запроса на доступ к опубликованным документам от другого узла сети в форме удобного для пользователя дескриптора от коммуникационного модуля 454. Как описано выше, запрос наиболее вероятно приходит от главного пользователя через модуль 462 пользовательского интерфейса. Модуль 456 разрешения имен дополнительно обеспечивает поиск в модуле 458 хранения документов идентифицирующей информации с идентификатором главного пользователя (такого как ИД 304 главного

пользователя на фиг.3), который согласуется с перехваченным удобным для пользователя дескриптором, изменяя запрос путем подстановки или замены удобного для пользователя дескриптора на местоположение машины, содержащееся в документе идентифицирующей информации, и посылает запрос на публикацию документов в форме местоположения машины назад в коммуникационный модуль 454. Модуль 456 разрешения имен подобен модулю 160 разрешения по фиг.1 в том, что он перехватывает запросы на доступ к документам от обращающегося за доступом узла, преобразует удобный для пользователя дескриптор в местоположение машины для публикующего узла и вводит соответствующую информацию в web-браузер компьютерной системы 152, которая, в свою очередь, получает доступ к запрошенным данным на публикующем узле.

Фиг.5 иллюстрирует способ публикации документов, находящихся на публикующей компьютерной системе, такой как компьютерная система 102 по фиг.1 или 402 по фиг.4, для обращающейся за доступом компьютерной системы, такой как компьютерная система 152 по фиг.1 или 452 по фиг.4. Поток обработки 500 в основном относится к процессу, выполняемому обращающимся за доступом узлом.

Поток обработки 500 начинается с операции 502 сохранения, в которой документ идентифицирующей информации, такой как документ с публикующего узла, сохраняется в определенном местоположении на обращающейся за доступом компьютерной системе, например, в базе 156 данных распознанной идентифицирующей информации по фиг.1. Подобно документу 300 идентифицирующей информации, показанному на фиг.3, принятый документ идентифицирующей информации будет содержать, как минимум, удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующей системы, такой как адрес электронной почты, и местоположение машины для компьютерной системы главного пользователя, такое как IP-адрес. Спустя некоторое время после этого операция 504 перехвата осуществляет перехват первоначального запроса на доступ к опубликованным документам, которые сохранены на публикующем узле. Запрос может инициироваться главным пользователем обращающегося за доступом узла, может инициироваться другими модулями в обращающейся за доступом компьютерной системе или представлять собой автоматический запрос. Запрос будет иметь форму удобного для пользователя дескриптора или содержать этот дескриптор, идентифицирующий главного пользователя публикующего узла или собственно публикующий узел. Например, запрос может представлять собой запрос на доступ к документам, находящимся по определенному адресу электронной почты.

Затем операция 506 поиска отыскивает ранее принятые и сохраненные документы идентифицирующей информации для определения того, совпадает ли идентификатор главного пользователя с удобным для пользователя дескриптором, принятым в операции 504 запроса. Если система не может отыскать согласующийся документ идентифицирующей информации на этапе 506, поток обработки 500 ответвляется на этап 507, соответствующий решению «нет», на котором главный пользователь или другой модуль уведомляется, что запрос был безуспешным. После уведомления главного пользователя, что запрос был безуспешным, процесс обработки 500 заканчивается. В этом случае главный пользователь может снова ввести данный запрос или другой подобный запрос для повторного запуска процесса обработки.

В противном случае, если в операции 506 поиска найден согласующийся документ идентифицирующей информации, то есть документ, в котором ИД главного

пользователя совпадает с адресом электронной почты, полученным на этапе 504, поток обработки 500 ответвляется на этап 504, соответствующий решению «да», для реализации операции 508 определения. Операция 508 определения осуществляет определение местоположения машины, которое включено в документ

5 идентифицирующей информации, найденный на этапе 506. Вслед за операцией 508 определения в операции 510 разрешения осуществляется замена удобного для пользователя дескриптора, например, адреса электронной почты, местоположением машины, например, IP-адресом 123.123.023.002. Затем в

10 операции 512 передачи осуществляется передача запроса на публикацию документа в форме местоположения машины, вместо удобного для пользователя дескриптора, к публикующему узлу. Этапы 506 и 508-512 реализуются в фоновом режиме и не раскрываются главному пользователю. Напротив, главному пользователю представляется, что его запрос на

15 доступ к опубликованному документу доставляется в форме удобного для пользователя дескриптора, т.е. адреса электронной почты, а не в не имеющей смысла форме данных местоположения машины. Таким путем главный пользователь может получить доступ к документам, находящимся на другой компьютерной системе, зная

20 только удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующей компьютерной системы. Главному пользователю обращающейся за доступом системы не требуется знать или запоминать громоздкие номера, такие как IP-адрес, для получения доступа к этим документам. На фиг.6 аналогичным образом иллюстрируется способ публикации документов, находящихся на публикующей компьютерной системе, но показаны процессы

25 обработки, выполняемые как публикующим узлом, таким как компьютерная система 102 или 402, так и обращающимся за доступом узлом, таким как компьютерная система 152 или 452. Поток обработки 600 начинается с операции 602 доставки, в которой на другой

30 узел, такой как обращающийся за доступом узел, доставляется имя пути для определения местоположения одного или более документов и удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующего узла. Например, операция доставки может включать в себя сообщение электронной

35 почты от главного пользователя публикующего узла, имя которого Боб, которое сообщает следующее: «проверь мои фото в bob@xyz.com/photos». Альтернативно главный пользователь может послать имя пути и удобный для пользователя дескриптор на обращающийся за доступом узел или главному пользователю

40 посредством телефонного вызова, факсового документа или некоторого другого средства. Поток обработки 600 переходит к операции 604 приема, где получающая доступ машина принимает имя пути для документов и удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующей машины. Затем

45 в операции 606 передачи осуществляется передача получающей доступ машине документа идентифицирующей информации для главного пользователя публикующей машины, в данном примере документа идентифицирующей информации пользователя по имени Боб. В операции 608 приема осуществляется прием документа

50 идентифицирующей информации пользователя по имени Боб, и затем в операции 609 сохранения документ идентифицирующей информации сохраняется в базе данных распознанной идентифицирующей информации, подобной базе 156 данных, описанной выше и показанной на фиг.1.

В альтернативном варианте осуществления после операции 608 приема и перед

операцией сохранения осуществляется операция верификации (не показана). В операции верификации осуществляется попытка аутентификации главного пользователя, представленного документом идентифицирующей информации, и принятие решения о том, следует ли принять и сохранить документ

5 идентифицирующей информации.

Спустя некоторое время после этого в операции 610 перехвата осуществляется перехват первоначального запроса на доступ к документам. Первоначальный запрос может исходить от главного пользователя или некоторого другого источника и имеет

10 целью получить доступ к документам в местоположении, определяемом удобным для пользователя дескриптором/именем пути, например, «bob@xyz.com/photos». Затем в операции 612 разрешения осуществляется разрешение первоначального запроса для создания измененного запроса путем подстановки данных местоположения машины вместо удобного для пользователя дескриптора с использованием процесса, детально

15 описанного со ссылкой на фиг.5, а именно отыскание согласующегося документа идентифицирующей информации, определяющего местоположение машины, и подстановку этого местоположения машины вместо удобного для пользователя дескриптора.

В альтернативном варианте осуществления в операции синтаксического анализа (не показана) осуществляется разделение удобного для пользователя дескриптора и имени пути и поиск совпадения только по компоненту первоначального запроса, соответствующему удобному для пользователя дескриптору. Например, операция синтаксического анализа игнорирует компонент «/photos» и осуществляет поиск ИД

20 главного пользователя по адресу электронной почты Боба «bob@xyz.com».

Еще в одном альтернативном варианте осуществления документ идентифицирующей информации главного пользователя включает в себя более одного местоположения машины и дополнительная операция поиска (не показана)

30 осуществляет поиск каждого из местоположений машин в документе идентифицирующей информации для определения того, какое местоположение машины содержит имя пути, включенное в перехваченный запрос. Операция 612 разрешения затем осуществляет подстановку данных местоположения машины, которое соответствует имени пути, указанному в первоначальном запросе.

После завершения операции 612 разрешения в операции 614 передачи осуществляется передача измененного запроса на опубликованные документы с использованием местоположения машины вместо удобного для пользователя дескриптора. Если при этом применяется имя пути, то операция 614 передачи

35 дополнительно включает запрос на доступ к документам, расположенным соответственно этому пути.

В этот момент поток обработки 600 возвращается к осуществляемой на публикующей машине операции 616 приема, принимающей измененный запрос на доступ к документам по указанному пути, в данном случае к папке «фото», такой как

45 папка 118 на фиг.1. Затем в операции 618 верификации определяется, авторизован ли главный пользователь обращающегося за доступом узла просматривать запрашиваемые документы. Если обращающийся за доступом главный пользователь не авторизован, то поток обработки ответвляется к операции 620 отклонения

50 соответственно принятому решению «нет», в которой запрос на доступ к документам отклоняется, и процедура обработки завершается.

Если обращающийся за доступом главный пользователь авторизован, то поток обработки 600 ответвляется к операции 622 определения местоположения,

соответствующей принятому решению «да», в которой определяется местоположение запрашиваемых документов с использованием имени пути, включенного при осуществлении операции 614 передачи. Наконец, в операции 624 публикации запрашиваемые документы публикуются, и поток обработки 600 завершается.

5 В одном варианте осуществления настоящего изобретения операция 618 верификации осуществляет проверку для определения того, содержится ли
обращающийся за доступом главный пользователь в базе данных распознанной
идентифицирующей информации, то есть послал ли обращающийся за доступом
10 главный пользователь ранее свой документ идентифицирующей информации
публикующему узлу. Если ответ положителен, то операция 619 верификации
ответвляется к соответствующей принятому решению «да» операции 622 определения
местоположения. Таким образом, в этом варианте осуществления требуется взаимный
15 обмен информацией документами идентифицирующей информации, для того чтобы
документы могли быть опубликованы одной машиной для другой машины. Это
наиболее защищенный способ публикации документов.

В альтернативном варианте осуществления настоящего изобретения операция 618
верификации не требует, чтобы обращающийся за доступом главный пользователь
20 посылал свой документ идентифицирующей информации. Вместо этого операция 618
верификации может учитывать другую переменную при определении того, следует ли
разрешить доступ к запрашиваемым документам, или операция 618 разрешения и
операция 620 отклонения могут быть совсем исключены из потока 600 обработки.
Вместо этого поток 600 обработки в этом случае переходит от операции 616 приема
25 непосредственно к операции 622 определения местоположения. Иными словами,
публикующая машина может принять решение, что она разрешит любому
пользователю с его документом идентифицирующей информации доступ к
документам на ее системе. Хотя этот способ проще, чем последний из указанных
30 выше, он не настолько защищен, как способ, требующий взаимного обмена
документами идентифицирующей информации.

Еще в одном альтернативном варианте осуществления операция уведомления
уведомляет обращающийся за доступом узел о том, что запрос на доступ к
документам был отклонен. После уведомления в другой операции передачи (не
35 показана) публикующему узлу может быть передан документ идентифицирующей
информации, представляющий обращающийся за доступом узел или его главного
пользователя, и процедура обработки запускается с операции 610 перехвата. Если
публикующий узел принял документ идентифицирующей информации обращающегося
40 за доступом узла, то поток 600 обработки может с большей вероятностью ответить
к операции 622 определения местоположения, соответствующей принятому решению
«да», чем к операции 620 отклонения, соответствующей принятому решению «нет».

Еще в одном альтернативном варианте осуществления настоящего изобретения
компонент определения местоположения машины документа идентифицирующей
45 информации может содержать открытый ключ вместо IP-адреса. Как использовано в
настоящем описании, термин «открытый ключ» должен пониматься в широком
смысле и определяться как код, уникальный для главного пользователя, состоящий из
чисел и/или букв и не имеющий распознаваемого смыслового значения.
50 Вышеописанная система и способы будут в этом случае работать, как описано выше,
с одним только исключением, описанным ниже.

Когда открытый ключ используется в качестве данных определения
местоположения в документе идентифицирующей информации, открытый ключ

используется для поиска текущего местоположения машины главного пользователя, которое может представлять собой IP-адрес, использующий протокол разрешения имен группы (PNRP). Протокол PNRP обычно состоит из распределенной системы знаний, включая хеш-функции открытых ключей и текущие местоположения машин.

5 Таким образом, открытый ключ используется для нахождения «текущего» местоположения машины главного пользователя. Как используется в настоящем описании, термин «текущее местоположение машины» должен пониматься в широком смысле как обозначающий местоположение машины в заданный момент времени.

10 Например, если компьютерная система использует динамический IP-адрес, для нее текущее местоположение машины может изменяться с соответствующего первому моменту времени на соответствующее второму, более позднему моменту времени. Использование открытого ключа и протокола PNRP обеспечит возможность
15 обращающемуся за доступом узлу получать доступ к документам из публикующего узла, даже если публикующий узел использует динамический IP-адрес.

Альтернативно, текущее местоположение машины может изменяться, если машина является мобильной, такой как компактная портативная компьютерная система или PDA. Протокол PNRP также может отслеживать текущие местоположения
20 машины для мобильных машин. Кроме того, использование открытого ключа и протокола PNRP позволит обращающемуся за доступом узлу получать доступ к документам из публикующего узла, даже если публикующий узел является мобильным.

Если открытый ключ используется в качестве местоположения машины, обращающийся за доступом узел должен знать открытый ключ публикующего узла,
25 чтобы получить доступ к документам публикующего узла. Единственный путь для обращающегося за доступом узла, чтобы получить открытый ключ публикующего узла, заключается в том, что публикующий узел посылает свой ключ обращающемуся за доступом узлу. Таким путем публикующий узел способен эффективным образом
30 контролировать тех, которые способны получать доступ к его ресурсам, путем контролирования тех, кому он посылает свой открытый ключ.

На фиг.7 показан еще один вариант осуществления настоящего изобретения, заключающегося в способе публикации документов, находящихся на публикующей
35 компьютерной системе, такой как компьютерная система 102 или 402, для обращающейся за доступом компьютерной системы, такой как компьютерная система 152 или 452.

Поток 700 обработки начинается с операции регистрации, заключающейся в регистрации зашифрованного имени машины, домена хоста и ассоциированного
40 местоположения регистрируемой машины в обычном DNS-сервере. DNS-сервер обычно хранит таблицу с именами машин, присоединенными к доменам хостов, вместе с соответствующими зарегистрированными местоположениями машин, такими как IP-адреса. Сетевые пользователи используют DNS-сервер для поиска зарегистрированных IP-адресов для конкретных машин. Как используется в
45 настоящем описании, термин «зашифрованное имя машины» должен обозначать открытый ключ, который преобразован в секретный код, который невозможно понять или использовать на обычном оборудовании. Возможным путем создания зашифрованного имени машины является применение некоторого алгоритма к
50 открытому ключу.

Затем в операции 706 доставки осуществляется доставка имени пути для местоположения одного или более документов и удобного для пользователя дескриптора, идентифицирующего главного пользователя публикующего узла.

Поток 700 обработки переходит к операции 706 приема, где обращающаяся за доступом машина принимает имя пути для документов и удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующей машины. Спустя некоторое время в операции 708 обращающемуся за доступом узлу передается документ идентифицирующей информации для главного пользователя публикующей машины. Документ идентифицирующей информации включает в себя, по меньшей мере, ИД главного пользователя, открытый ключ и хост домена для главного пользователя публикующего узла. В операции 610 приема осуществляется прием документа идентифицирующей информации, после чего следует операция сохранения 712, на которой документ идентифицирующей информации сохраняется в базе данных распознанной идентифицирующей информации, подобной базе 156 данных, описанной и показанной в связи с фиг.1.

Спустя некоторое время после этого в операции 714 перехвата осуществляется перехват первоначального запроса для доступа к документам. Первоначальный запрос может исходить от главного пользователя или некоторого другого источника и имеет целью получение доступа к документам в местоположении, определяемом удобным для пользователя дескриптором/путем. Затем в операции 716 разрешения осуществляется разрешение удобного для пользователя дескриптора в первоначальном запросе с открытым ключом и хостом домена, указанными в документе идентифицирующей информации, с использованием ИД главного пользователя, который согласуется с удобным для пользователя дескриптором, с использованием процесса, детально описанного на фиг.5.

Затем в операции 718 преобразования выполняется вычисление на основе открытого ключа, чтобы преобразовать его в зашифрованное имя машины, и в операции 720 присоединения зашифрованное имя машины присоединяется к хосту домена. В одном варианте осуществления операция преобразования включает в себя выполнение некоторого алгоритма над открытым ключом, причем этот алгоритм является тем же самым, который использовался публикующим узлом в операции 702 регистрации. Этот алгоритм может представлять собой стандартный алгоритм, обычно используемый многими сетевыми узлами, или может быть конкретным алгоритмом, который был получен обращающимся за доступом узлом некоторым иным путем.

Поток 700 обработки затем переходит к операции 722 поиска, которая использует комбинацию зашифрованного имени машины/хоста домена для поиска местоположения зарегистрированной машины на DNS-сервере. После завершения операции 722 поиска операция 724 изменения изменяет первоначальный запрос для замены удобного для пользователя дескриптора местоположением зарегистрированной машины и посылает измененный запрос на публикуемые документы с использованием местоположения зарегистрированной машины вместо удобного для пользователя дескриптора. Если используется имя пути, то операция 614 дополнительно включает в себя запрос на доступ к документам, находящимся соответственно этому пути.

Преимущество использования способа, показанного потоком 700 обработки, состоит в том, что он позволяет публикующей машине использовать дополнительные меры защиты при использовании обычных DNS-серверов. Обычно DNS-адреса являются общедоступными, и потенциальные хакеры могут использовать DNS-серверы для нахождения имени машины публикующего узла и местоположения машины. Хакеры могут затем использовать эту информацию для получения

неавторизованного доступа к ресурсам публикующего узла. Регистрация зашифрованного имени машины в DNS-сервере препятствует отысканию хакерами имени машины публикующего узла, но затрудняет авторизованным пользователям получать доступ к ресурсам публикующего узла. Процесс 700 обработки обеспечивает возможность авторизованным обращающимся за доступом узлам получать доступ к ресурсам публикующего узла, зная только удобный для пользователя дескриптор. Обращающемуся за доступом узлу не требуется знать неудобное для пользователя зашифрованное имя машины или хост домена, чтобы получить доступ к ресурсам публикующего узла. Защищенность повышается, поскольку обращающийся за доступом узел должен принимать документ идентифицирующей информации публикующего узла, чтобы использовать способ разрешения имен.

Хотя изобретение описано применительно к компьютерным структурным признакам, методологическим действиям и машиночитаемым носителям, понятно, что изобретение, определенное в формуле изобретения, не должно ограничиваться описанными конкретными структурами, действиями или носителями. Например, различные форматы, иные, чем XML, могут использоваться для кодирования идентифицирующей информации. Поэтому конкретные структурные признаки, действия и носители раскрыты в качестве примеров вариантов осуществления, реализующих заявленное изобретение.

Используя вышеописанные методы разрешения имен, настоящее изобретение устанавливает, что удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующего узла, может быть ассоциирован с местоположением машины или обеспечивать его разрешение, так что главному пользователю обращающейся за доступом машины необходимо только знать удобный для пользователя дескриптор, чтобы получить доступ к запрашиваемым документам на публикующей машине. Последующий процесс ассоциирования прозрачен и реализуется независимо от главного пользователя и без его участия.

Приведенное выше описание, примеры и данные обеспечивают полное описание изготовления и использования состава изобретения. Поскольку множество вариантов осуществления изобретения могут быть реализованы без отклонения от его сущности и объема, настоящее изобретение определяется только формулой изобретения.

Формула изобретения

1. Способ доступа к документам, сохраненным на первой компьютерной системе, через вторую компьютерную систему, причем первая и вторая компьютерные системы соединены в сетевой среде, при этом упомянутый способ содержит:

сохранение на второй компьютерной системе документа идентифицирующей информации из первой компьютерной системы, причем документ идентифицирующей информации содержит удобный для пользователя дескриптор, идентифицирующий главного пользователя, и местоположение машины для первой компьютерной системы;

прием на пользовательском интерфейсе, реализованном на второй компьютерной системе, запроса на доступ к документам, сохраненным на первой компьютерной системе, причем запрос включает в себя удобный для пользователя дескриптор и направлен на первую компьютерную систему;

перехват на второй компьютерной системе запроса на доступ к документам от пользователя второй компьютерной системы, если запрос включает в себя удобный для пользователя дескриптор;

замену на второй компьютерной системе удобного для пользователя дескриптора запроса местоположением машины и передачу запроса на доступ к документам в местоположение машины, соответствующее первой компьютерной системе.

2. Способ по п.1, в котором удобный для пользователя дескриптор содержит адрес электронной почты.

3. Способ по п.1, в котором местоположение машины содержит IP-адрес.

4. Способ по п.1, в котором местоположение машины содержит открытый ключ.

5. Способ по п.1, в котором запрос на доступ к документам содержит запрос, инициированный главным пользователем.

6. Способ по п.1, дополнительно содержащий первоначальный этап приема на второй компьютерной системе документа идентифицирующей информации из первой компьютерной системы.

7. Способ публикации документов между множеством узлов, причем узлы соединены в сетевой среде, при этом способ содержит

передачу документа идентифицирующей информации из публикующего узла к обращающемуся за доступом узлу, причем документ идентифицирующей информации содержит удобный для пользователя дескриптор, идентифицирующий главного пользователя публикующего узла, и местоположение машины для публикующего узла;

сохранение документа идентифицирующей информации на обращающемся за доступом узле;

разрешение на обращающемся за доступом узле удобного для пользователя дескриптора с использованием местоположения машины в запросе на доступ к документам, причем запрос сделан к публикующему узлу от пользователя обращающегося за доступом узла через пользовательский интерфейс, реализованный на обращающемся за доступом узле, и

передачу запроса на доступ к документам из обращающегося за доступом узла к публикующему узлу.

8. Способ по п.7, в котором удобный для пользователя дескриптор содержит адрес электронной почты.

9. Способ по п.7, в котором удобный для пользователя дескриптор содержит номер телефона.

10. Способ по п.7, в котором местоположение машины содержит IP-адрес.

11. Способ по п.7, в котором местоположение машины содержит открытый ключ.

12. Способ по п.11, дополнительно содержащий использование открытого ключа для определения текущего местоположения машины для публикующего узла.

13. Способ по п.11, дополнительно содержащий регистрацию зашифрованного имени машины и зарегистрированного местоположения машины для публикующего узла в DNS-сервере, разрешение удобного для пользователя дескриптора с использованием открытого ключа,

преобразование открытого ключа в зашифрованное имя машины, использование зашифрованного имени машины для поиска зарегистрированного местоположения машины для публикующего узла на DNS-сервере,

передачу запроса на доступ к документам в зарегистрированное местоположение машины.

14. Способ по п.7, дополнительно содержащий проверку того, что обращающийся за доступом узел имеет авторизацию от публикующего узла на просмотр запрашиваемых документов перед публикацией запрашиваемых документов.

15. Способ по п.7, дополнительно содержащий доставку имени пути для

документов, сохраненных на публикующем узле, в обращающийся за доступом узел.

16. Способ по п.15, в котором имя пути доставляется в обращающийся за доступом узел посредством электронной почты.

5 17. Способ по п.7, дополнительно содержащий доставку имени пути для документов, сохраненных на публикующем узле, к главному пользователю обращающегося за доступом узла.

18. Способ по п.17, в котором имя пути доставляется к главному пользователю обращающегося за доступом узла посредством телефонного вызова.

10 19. Способ по п.7, в котором этап разрешения дополнительно содержит перехват запроса на доступ к документам, если запрос направлен на удобный для пользователя дескриптор;

15 отыскание согласующегося документа идентифицирующей информации, имеющего удобный для пользователя дескриптор, который совпадает с удобным для пользователя дескриптором в запросе;

определение местоположения машины из согласующегося документа идентифицирующей информации и

20 изменение запроса для замены удобного для пользователя дескриптора местоположением машины.

20. Способ по п.7, дополнительно содержащий

доставку имени пути в комбинации с удобным для пользователя дескриптором в обращающийся за доступом узел и

25 анализ имени пути из удобного для пользователя дескриптора перед разрешением удобного для пользователя дескриптора с использованием местоположения машины.

21. Способ по п.20, дополнительно содержащий добавление имени пути к запросу на доступ к документам перед передачей запроса к публикующему узлу.

30 22. Способ по п.7, в котором документ идентифицирующей информации дополнительно содержит более одного местоположения машины для главного пользователя, идентифицированного удобным для пользователя дескриптором.

23. Способ использования удобного для пользователя дескриптора для доступа к документам, сохраненным на первой компьютерной системе в сетевой среде, причем упомянутый способ содержит

35 сохранение на второй компьютерной системе документа идентифицирующей информации из первой компьютерной системы, причем документ

идентифицирующей информации содержит удобный для пользователя дескриптор, идентифицирующий главного пользователя первой компьютерной системы, и

40 местоположение машины для первой компьютерной системы, реализацию пользовательского интерфейса на второй компьютерной системе для обеспечения возможности второму пользователю второй компьютерной системы запрашивать доступ к документам, сохраненным на первой компьютерной системе;

45 прием на пользовательском интерфейсе, реализованном на второй компьютерной системе, запроса от второго пользователя второй компьютерной системы на доступ к первому документу из документов, сохраненных на первой компьютерной системе, причем запрос включает в себя удобный для пользователя дескриптор и направлен на первую компьютерную систему; перехват на второй компьютерной системе запроса из 50 пользовательского интерфейса на доступ к первому документу;

изменение на второй компьютерной системе запроса для замены удобного для пользователя дескриптора местоположением машины для первой компьютерной системы;

передачу измененного запроса от второй компьютерной системы в местоположение машины, соответствующее первой компьютерной системе, и доступ к первому документу на второй компьютерной системе.

5 24. Способ по п.23, в котором удобный для пользователя дескриптор представляет собой адрес электронной почты.

25. Способ по п.23, в котором местоположение машины содержит IP-адрес.

26. Способ по п.23, в котором местоположение машины содержит открытый ключ.

10 27. Способ по п.26, дополнительно содержащий использование открытого ключа для определения текущего местоположения машины для публикующего узла.

28. Способ по п.23, дополнительно содержащий первоначальный этап приема документа идентифицирующей информации из первой компьютерной системы.

29. Способ по п.23, дополнительно содержащий этап приема публикуемых документов из первой компьютерной системы.

15 30. Первая компьютерная система, содержащая

модуль хранения для хранения документа идентифицирующей информации, принимаемого из второй компьютерной системы, при этом документ идентифицирующей информации содержит удобный для пользователя дескриптор, идентифицирующий главного пользователя второй компьютерной системы, и местоположение машины для второй компьютерной системы; коммуникационный модуль, соединенный с возможностью коммуникации с модулем хранения для передачи от пользователя первой компьютерной системы запросов для доступа к документам, сохраненным на второй компьютерной системе;

25 модуль разрешения имени, соединенный с возможностью коммуникации с модулем хранения и коммуникационным модулем, для перехвата запросов на доступ к документам, сохраненным на второй компьютерной системе, и изменения каждого запроса для замены удобного для пользователя дескриптора местоположением машины, и

30 модуль пользовательского интерфейса, конфигурированный для обеспечения возможности пользователю первой компьютерной системы обращаться и управлять любым из модуля хранения, коммуникационного модуля и модуля разрешения имени.

35 31. Компьютерная система по п.30, в которой удобный для пользователя дескриптор является адресом электронной почты.

32. Компьютерная система по п.30, в которой местоположение машины содержит IP-адрес.

40 33. Компьютерная система по п.30, в которой местоположение машины содержит открытый ключ.

34. Компьютерная система по п.30, дополнительно содержащая коммуникационный модуль, соединенный с модулем разрешения имен, для передачи коммуникаций к второй компьютерной системе и приема коммуникаций от второй компьютерной системы.

45 35. Машиночитаемый носитель, содержащий сохраненную на нем компьютерную программу, содержащую инструкции для исполнения реализуемого компьютером способа для разрешения имен, причем упомянутый реализуемый компьютером способ содержит

50 сохранение на обращающейся за доступом компьютерной системе документа идентифицирующей информации из публикующей компьютерной системы, при этом документ идентифицирующей информации содержит удобный для пользователя дескриптор, идентифицирующий главного пользователя, и местоположение машины

для публикующей компьютерной системы; прием на пользовательском интерфейсе, реализованном на обращающейся за доступом компьютерной системе, инструкций от пользователя обращающейся за доступом компьютерной системы для генерации запроса на доступ к документам, сохраненным на публикующей компьютерной системе, причем запрос включает в себя удобный для пользователя дескриптор; перехват запроса на доступ к документам, сохраненным на публикующей компьютерной системе, при этом запрос содержит удобный для пользователя дескриптор, и

изменение на обращающейся за доступом компьютерной системе запроса для замены удобного для пользователя дескриптора местоположением машины.

36. Машиночитаемый носитель по п.35, в котором удобный для пользователя дескриптор содержит адрес электронной почты.

37. Машиночитаемый носитель по п.35, в котором местоположение машины содержит IP-адрес.

38. Машиночитаемый носитель по п.35, в котором местоположение машины содержит открытый ключ.

39. Машиночитаемый носитель по п.38, дополнительно содержащий использование открытого ключа для определения текущего местоположения машины для публикующего узла.

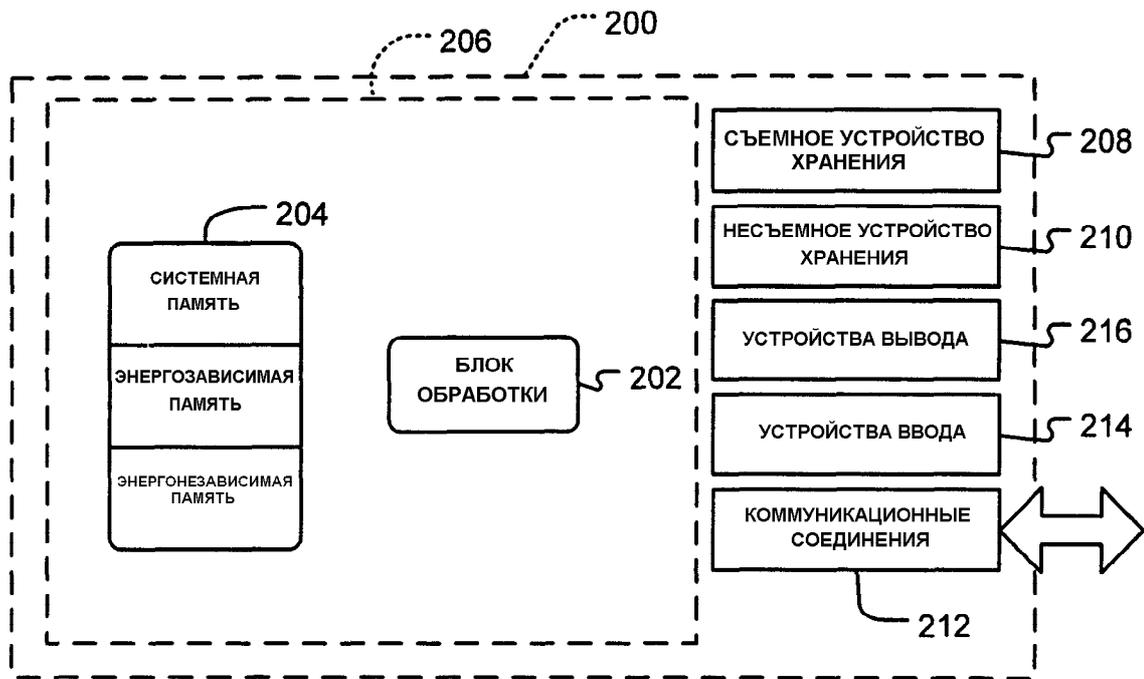
40. Машиночитаемый носитель по п.38, причем упомянутый реализуемый компьютером способ дополнительно содержит регистрацию зашифрованного имени машины и зарегистрированного местоположения машины для публикующего узла в DNS-сервере, разрешение удобного для пользователя дескриптора с использованием открытого ключа,

преобразование открытого ключа в зашифрованное имя машины, использование зашифрованного имени машины для поиска зарегистрированного местоположения машины для публикующего узла на DNS-сервере и

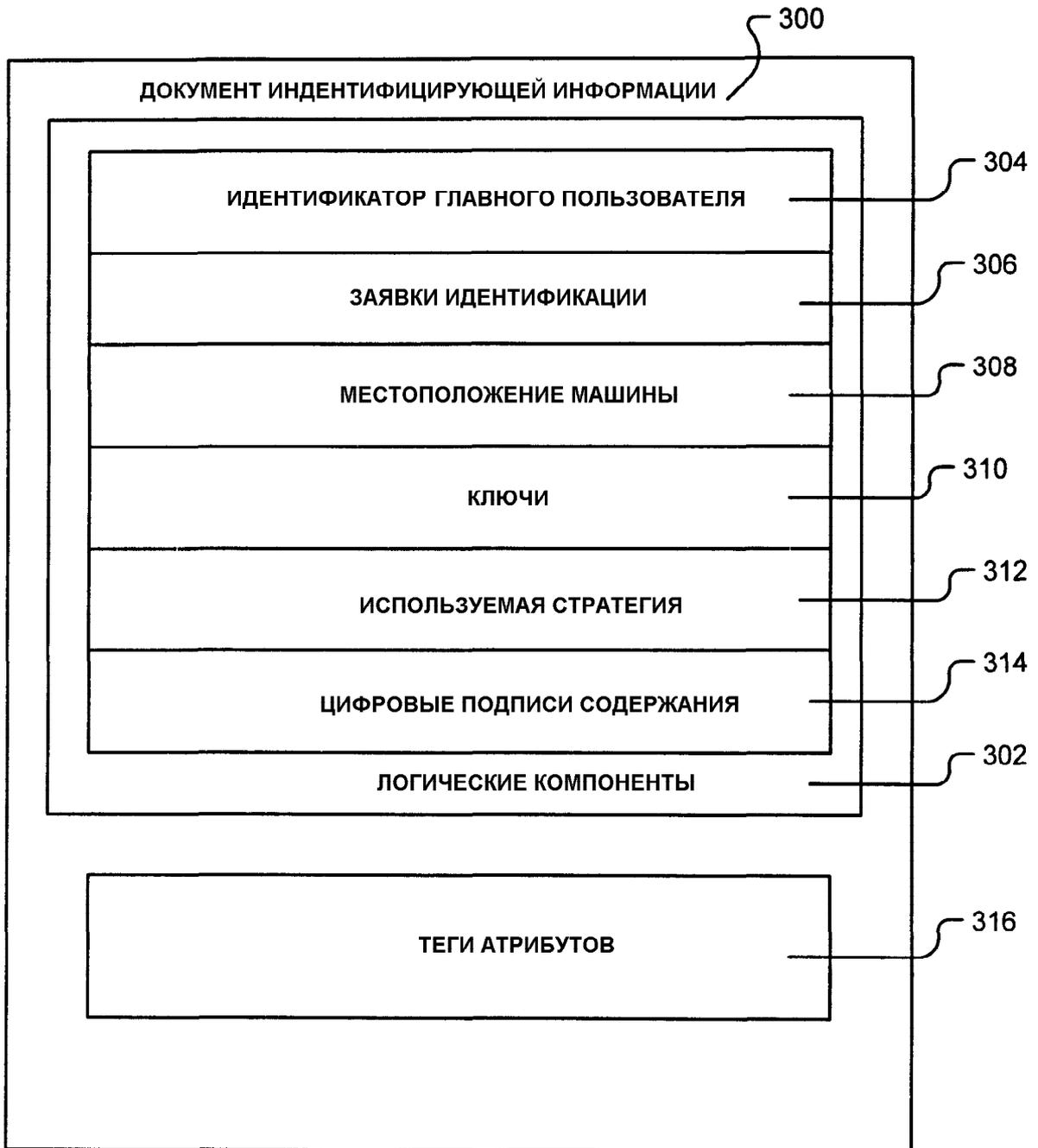
передачу запроса на доступ к документам в зарегистрированное местоположение машины.

41. Машиночитаемый носитель по п.40, в котором упомянутое преобразование содержит выполнение некоторого алгоритма над открытым ключом.

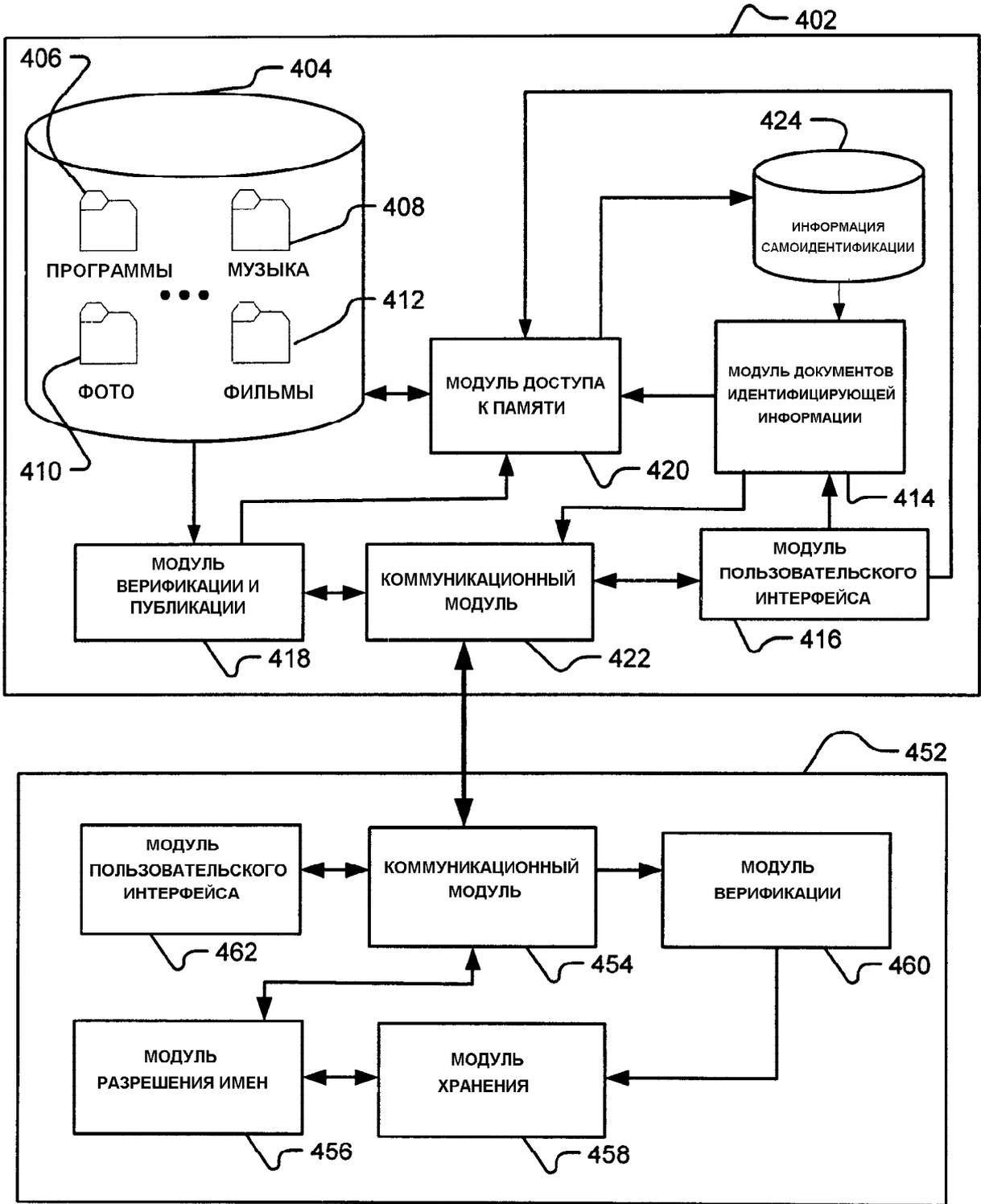
42. Машиночитаемый носитель по п.35, в котором документ идентифицирующей информации содержит более чем одно местоположение машины для главного пользователя, идентифицированного удобным для пользователя дескриптором.



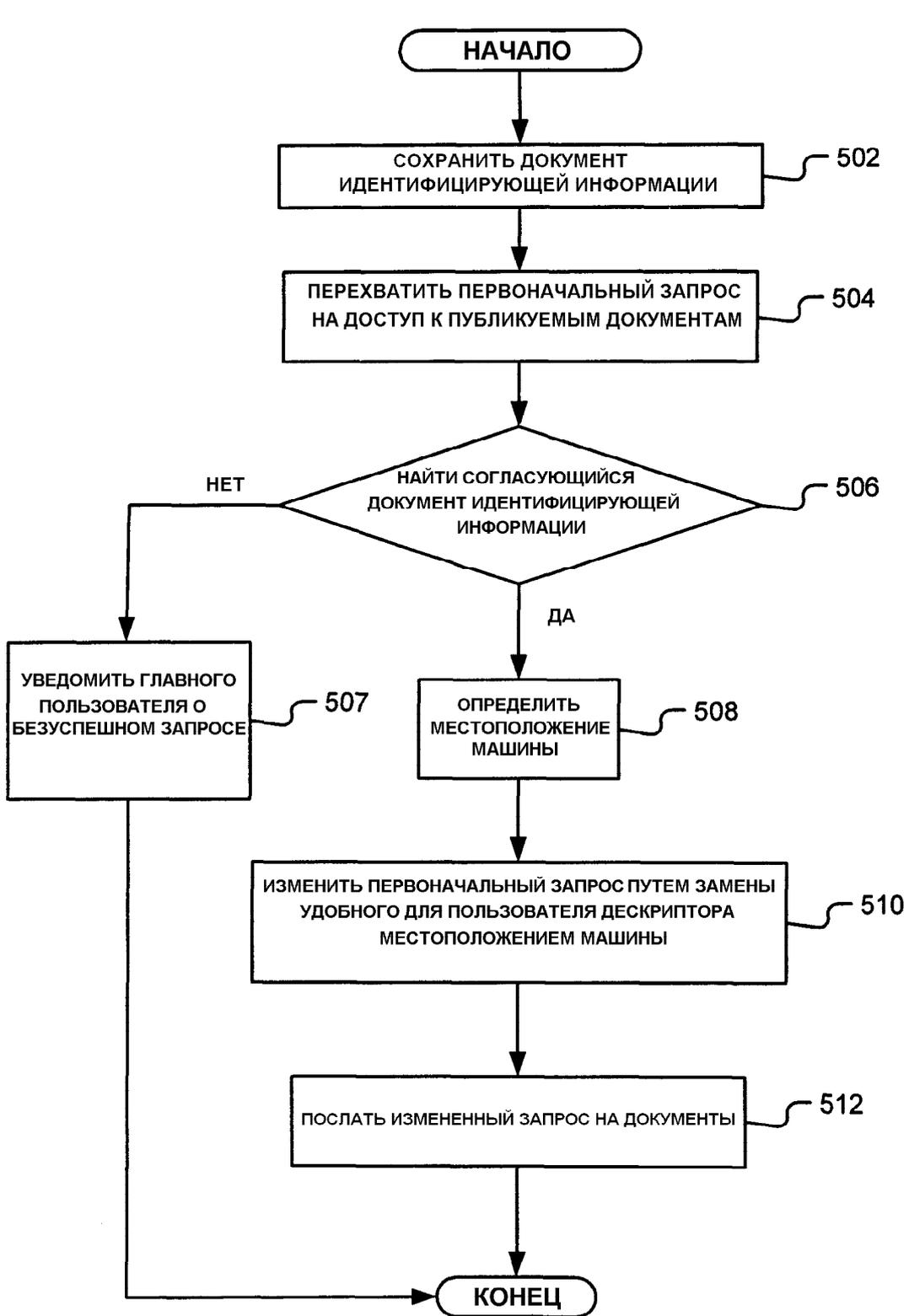
ФИГ.2



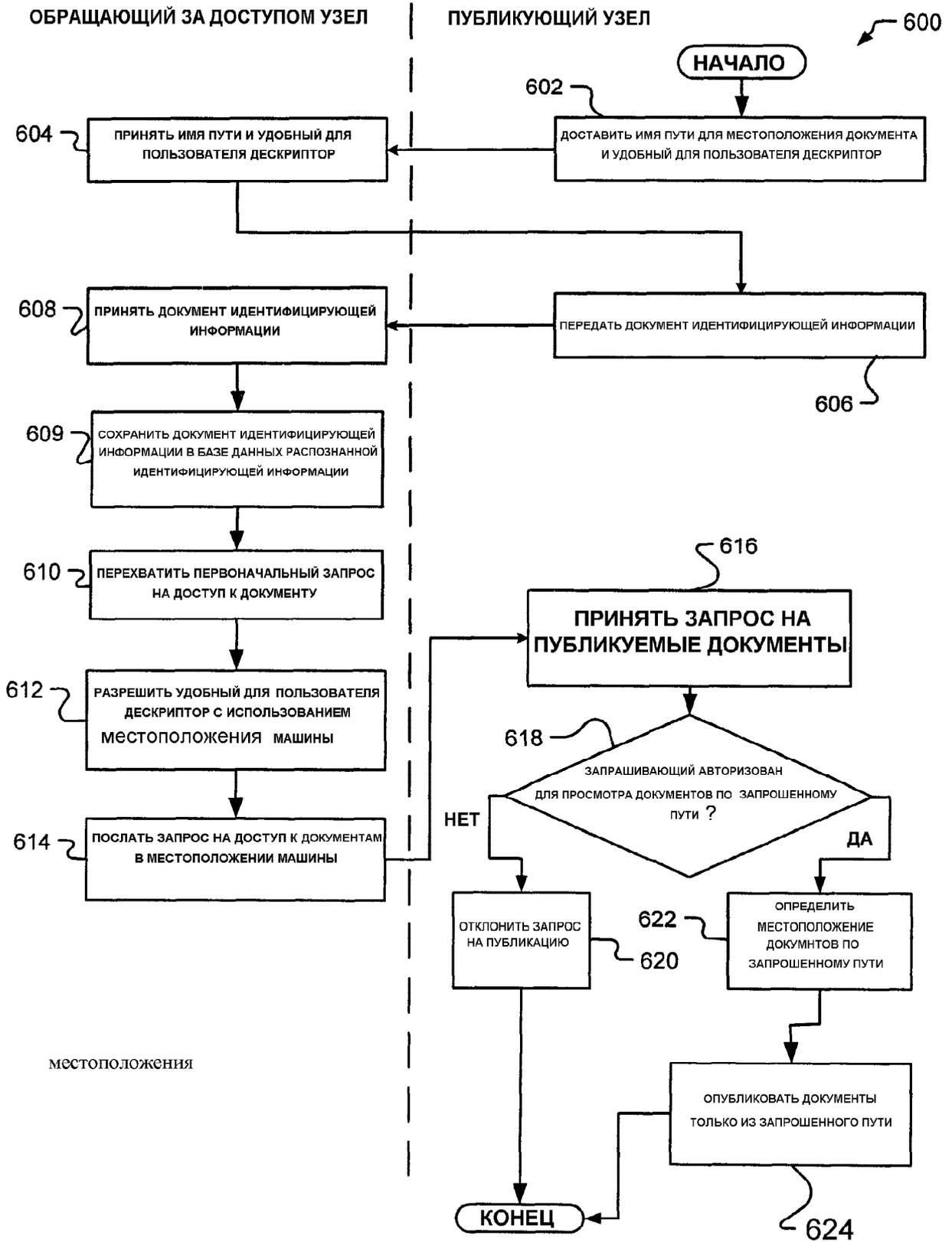
ФИГ.3



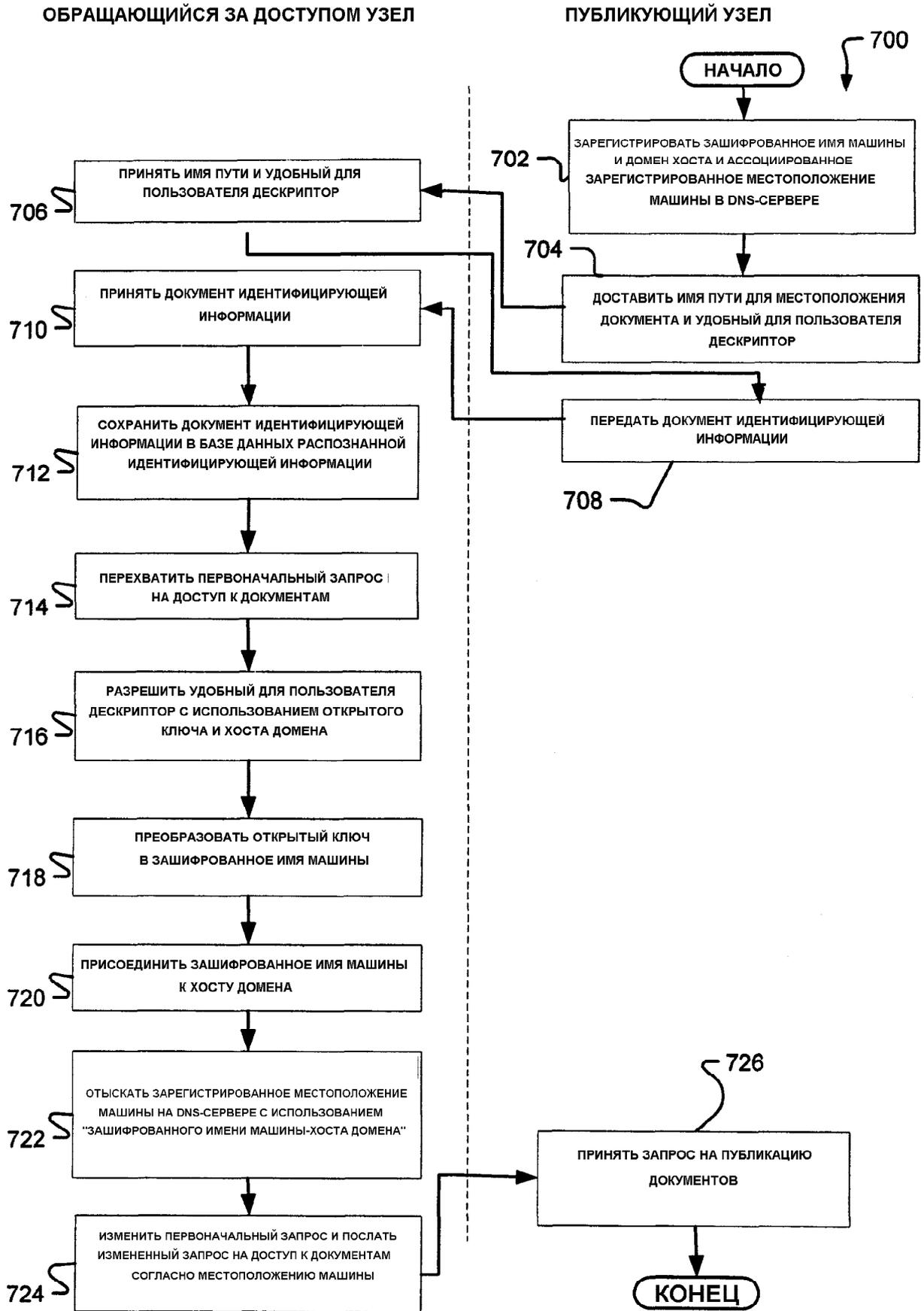
ФИГ.4



ФИГ.5



ФИГ.6



ФИГ.7