



ФЕДЕРАЛЬНАЯ СЛУЖБА  
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,  
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

## (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: 2007143965/09, 29.11.2007

(24) Дата начала отсчета срока действия патента:  
29.11.2007

(45) Опубликовано: 10.07.2009 Бюл. № 19

(56) Список документов, цитированных в отчете о  
поиске: RU 2289886 C1, 20.12.2006. JP 2006338213  
A, 14.12.2006. US 2007088958 A, 19.04.2007.  
WO 02052769 A1, 04.07.2002.

Адрес для переписки:  
129090, Москва, ул. Щепкина, 22, ЗАО ИВК,  
В.В. Андрееву

(73) Патентообладатель(и):

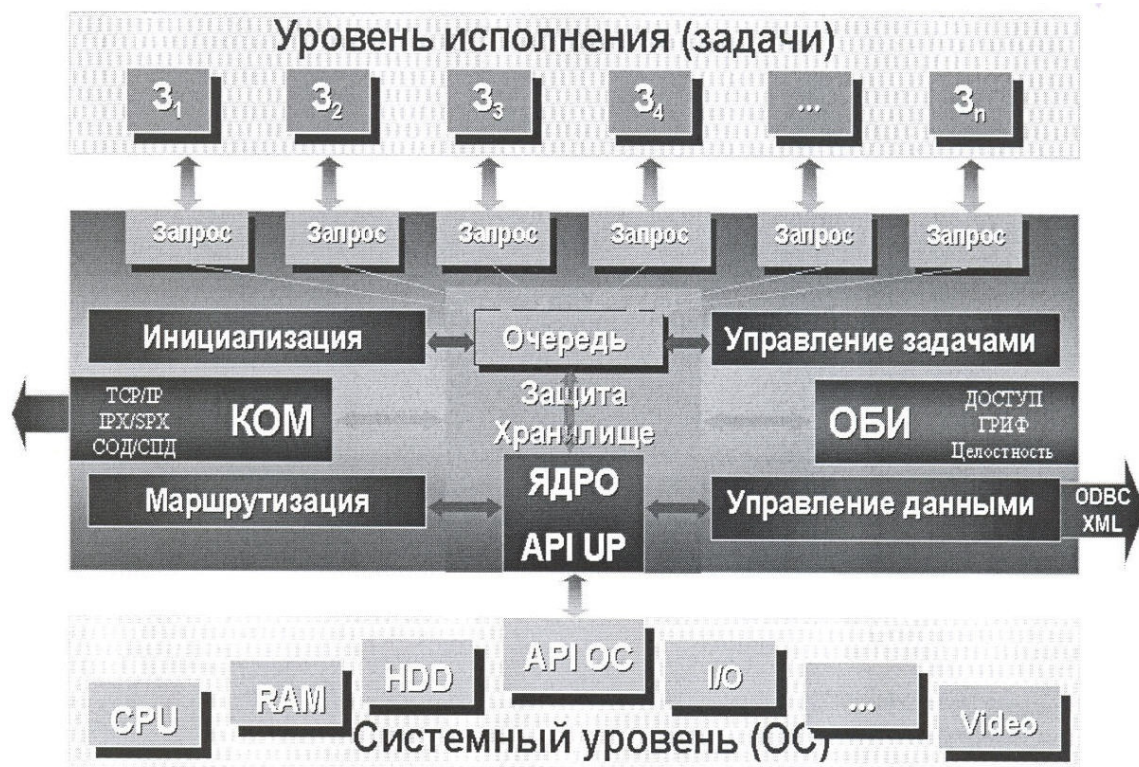
Закрытое акционерное общество  
"Информационная внедренческая  
компания" (ЗАО "ИВК") (RU)

## (54) СПОСОБ ГАРАНТИРОВАННОГО ДОВЕДЕНИЯ ИНФОРМАЦИИ В НЕОДНОРОДНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в обеспечении гарантированного доведения информации в неоднородной вычислительной сети до конкретных пользователей. Сущность изобретения заключается в том, что реализуют механизмы единообразного взаимодействия между вычислительными установками как в локальной, так и во всей вычислительной сети; обеспечивают взаимодействие между конечными приложениями посредством автоматического создания очередей; обеспечивают гарантированную доставку сообщений посредством возвращения на узел-отправитель квитанции о доставке;

создают на каждой вычислительной установке защищенное хранилище данных для хранения очередей, сообщений и таблиц маршрутизации; обеспечивают гарантированную обработку тела сообщения посредством указания номера конечного приложения-обработчика; систематически проверяют полномочия каждого должностного лица, допущенного к работе с информационными ресурсами; обеспечивают гарантированную идентификацию каждого сообщения за счет встроенного механизма идентификации должностных лиц на основе электронно-цифровой подписи, чем достигается юридическая значимость информационного обмена. 3 з. п. ф-лы, 3 ил.



Фиг. 1



FEDERAL SERVICE  
FOR INTELLECTUAL PROPERTY,  
PATENTS AND TRADEMARKS

## (12) ABSTRACT OF INVENTION

(21), (22) Application: **2007143965/09**, 29.11.2007

(24) Effective date for property rights:  
**29.11.2007**

(45) Date of publication: **10.07.2009 Bull. 19**

Mail address:

**129090, Moskva, ul. Shchepkina, 22, ZAO IVK,  
V.V. Andreevu**

(73) Proprietor(s):

**Zakrytoe aktsionernoe obshchestvo  
"Informatsionnaja vnedrencheskaja kompanija"  
(ZAO "IVK") (RU)**

## (54) METHOD OF GUARANTEED INFORMATION TRANSFER IN HETEROGENEOUS COMPUTER NETWORK

(57) Abstract:

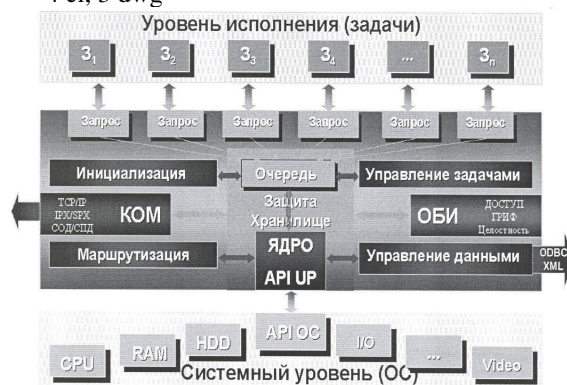
FIELD: information technologies.

SUBSTANCE: invention relates to computer engineering. According to the invention there are realised mechanisms of consistently interacting computing units in local network as well as in the entire computer network; interaction between finite applications is ensured through automatic queue formation; guaranteed messages delivery is secured by sending delivery receipt to node-sender; there is protected data storage for storing queues, messages and routing table set up on every computing unit; message body processing by indicating finite associated application number is guaranteed; authority of every official cleared for access to work with information resources is systematically checked; identification of every message is ensured using imbedded mechanism identifying officials over

electronic digital signature thereby achieving juridical relevance of data exchange.

EFFECT: ensuring information transmission to designated users in heterogeneous computer network.

4 cl, 3 dwg



Фиг. 1

Область техники, к которой относится изобретение

Настоящее изобретение относится к вычислительной технике, а конкретнее к способу гарантированного доведения информации в неоднородной вычислительной сети.

Уровень техники

Актуальной задачей систем электронного документооборота (СЭД) на современном этапе развития отрасли информационных технологий является задача объединения в единый процесс обработки электронных документов разрозненных удаленных информационных объектов заказчика и должностных лиц на этих объектах для обеспечения управляемости сквозным (возможно, даже оперативным) обменом документами. Еще более важным моментом в такого рода обмене является обеспечение гарантии информационного взаимодействия на комплексе разрозненных объектов автоматизации (и должностных лиц), связанных к тому же разнородными, а зачастую и недоверенными каналами связи, в случае реализации технических решений для юридически значимых СЭД.

В настоящее время известны различные способы доведения информации, в том числе и в неоднородной вычислительной сети.

Так, в патенте РФ № 2130643 (опубл. 20.05.1999) раскрыт способ обеспечения доступа к данным в системе управления базами данных «Линтер-ВС». В этом способе в процессе обработки запроса доступа производят несколько проверок для сравнения ранга допуска пользователя с рангом доступа запрашиваемых данных.

В патенте РФ № 2289886 (опубл. 20.12.2006); патенте США № 7177932 (опубл. 13.02.2007) раскрыты способ, шлюз и система для передачи данных между устройством в сети общего пользования и устройством во внутренней сети. Соединение внутренней сети с сетью общего пользования производится через шлюз, содержащий блок управления обменом, который распознает место назначения данных, адресованных в сеть общего пользования, на основе идентификатора, включенного в данные.

Заявка США № 2007-0088958 (опубл. 19.04.2007) раскрывает способ пользования электронными документами, в котором возможности по обработке документа зависят от прав пользователя.

Патенты США №№ 6237099 (опубл. 22.05.2001) и 6622162 (опубл. 16.09.2003) описывают способы доставки электронных документов в сети к разным пользователям.

В патентах США №№ 7263551 (опубл. 28.08.2007) и 7213066 (опубл. 01.05.2007) раскрыты способы сетевой доставки электронных документов к разным устройствам.

В заявках Японии №№ 2006-338213 (опубл. 14.12.2006), 2006-197150 (опубл. 27.07.2006), 2005-173656 (опубл. 30.06.2005), 2004-252506 (опубл. 09.09.2004), заявках США №№ 2005-262243 (опубл. 24.11.2005), 2004-212826 (опубл. 28.10.2004), заявке ЕПВ № 1102472 (опубл. 23.05.2001), международных заявках №№ WO 2007/085768 (опубл. 02.08.2007), WO 03/054767 (опубл. 03.07.2003) и WO 02/052769 (опубл. 04.07.2002) раскрыты различные способы обработки электронных документов в разнородной сети.

Все эти и многие другие документы решают частные задачи по доставке электронных документов в вычислительной сети. Но среди них нет такого источника, в котором предлагался бы или хотя бы подразумевался такой способ обработки информации в неоднородной вычислительной сети, который бы гарантировал, т.е. надежно (со 100%-ной вероятностью) обеспечивал доведение электронных

документов до конкретных пользователей.

#### Сущность изобретения

Под гарантированным доведением электронных документов понимается  
 5 непротиворечивое взаимодействие четырех ключевых гарантированных служб,  
 относящихся к операциям обмена данными в неоднородных  
 территориально-распределенных вычислительных сетях:

- доставку;
- хранение;
- 10 - обработку;
- идентификацию должностного лица.

Гарантированная доставка определяет прием-передачу произвольных электронных  
 документов (сообщений, файлов, документов) до любого конкретного должностного  
 лица вычислительной сети в избирательном и циркулярном режимах. Транспортные  
 15 возможности задают адресацию объектов автоматизации с расширенным  
 семантическим описанием имен и рангов должностных лиц (пользователей),  
 обеспечивают контроль за их действиями и выполнение принципов мандатного и  
 дискреционного доступа. Гарантией доставки является соответствующая квитанция.  
 20 Передача также снабжается маркером приоритета передачи, являющимся средством  
 определения его эффективной пропускной способности по каналу связи. Кроме того,  
 обеспечивается:

- практически 100%-ная вероятность передачи без искажений сообщения  
 произвольного объема (до ~1 Гбайт), в том числе и при перерывах в связи в период  
 25 передачи этого сообщения («докачка»);
- возможность адресации по статическим и динамическим IP-адресам;
- время установления соединения и передачи сообщений не нормируется и  
 определяется только реальной скоростью передачи в канале;
- 30 - автоматическое назначение альтернативных маршрутов передачи данных;
- программная коммутация каналов связи на узле-шлюзе при наличии аппаратной  
 возможности назначения альтернативного маршрута передачи.

Гарантированное хранение обеспечивает наличие защищенного  
 специализированного хранилища на каждом АРМ должностного (в том числе  
 35 уполномоченного) лица, в которое помещается не только вся очередь  
 входящих-исходящих сообщений, но и конфиденциальные (в том числе секретные)  
 документы. В случае разрыва канала связи неотправленные документы возвращаются  
 в очередь с автоматическим назначением альтернативных маршрутов передачи  
 40 данных. При отправке больших объемов данных обеспечивается "докачка"  
 недоставленной части сообщения в целях оптимизации загрузки канала.

Гарантированная обработка содержательной части сообщения по факту его  
 регламентной обработки обеспечивается направлением соответствующей квитанции  
 об обработке в адрес отправителя.

45 Информационный обмен между объектами вычислительной сети осуществляется по  
 схеме «каждый с каждым в дуплексном режиме по инициативе любого абонента».  
 Обеспечивается поддержка синхронного («клиент-сервер») и асинхронного (с  
 использованием очередей) режимов обмена данными между абонентами сети с  
 50 возможностью регистрации входящих и исходящих сообщений, в том числе на основе  
 поддержки механизма коммутации пакетов.

При этом обеспечивается взаимодействие произвольного количества объектов  
 территориально-распределенной вычислительной сети, основанной на применении

актуальных методов распределения ресурсов и доступа, современной системы защиты информации и кодирования, предоставлении пользователю максимального числа необходимых web-сервисов для организации управления как внешним, так и внутренним информационным пространством, с использованием различных механизмов и произвольных каналов связи (цифровых, аналоговых). Кроме того, обеспечивается взаимодействие произвольного количества пользователей системы (должностных лиц) на основе единого механизма разграничения доступа, а также произвольного количества прикладных процессов с обеспечением контроля целостности этих процессов.

Гарантированная идентификация должностного лица вычислительной сети осуществляется на основе стандартизированной PKI-технологии (Private Key Infrastructure) при помощи автоматического введения сертификата открытого ключа в тело любого исходящего сообщения, а также проверкой сертификатов всех входящих сообщений. Кроме того, может быть задействован механизм шифрования исходящего трафика должностного лица, предъявляющего свои полномочия посредством ключевой пары с последующей аутентификацией уже общесистемными средствами разграничения доступа.

Таким образом, существует необходимость в способе именно гарантированного доведения информации в неоднородной вычислительной сети до конкретных пользователей.

Эта задача решается заявляемым изобретением, в котором представлен способ гарантированного доведения информации в неоднородной вычислительной сети, образованной территориально-распределенными объектами автоматизации, связанными магистралью информационного обмена в единую глобальную вычислительную сеть, и включающей в себя, по меньшей мере, две соединенные сетью связи вычислительные установки, представляющие собой локальные и (или) глобальные объекты автоматизации, по меньшей мере, одна из которых снабжена отличной от других операционной системой, заключающийся в том, что: устанавливаются на каждую вычислительную установку общесистемное программное обеспечение для получения единой защищенной магистрали информационного обмена между всеми вычислительными установками неоднородной вычислительной сети; обеспечиваются на каждой вычислительной установке единые унифицированные средства межмашинного информационного обмена, реализующие физическую связность вычислительных установок в рамках единой защищенной магистрали информационного обмена; обеспечиваются, посредством средств межмашинного информационного обмена, единообразное взаимодействие как между вычислительными установками в локальной вычислительной сети объекта автоматизации, входящего в неоднородную вычислительную сеть, так и между глобальными объектами автоматизации в рамках неоднородной вычислительной сети; перенастраиваются в каждой операционной системе все системные интерфейсы по обмену данными на соответствующие механизмы обмена данными общесистемного программного обеспечения; обеспечиваются, с помощью средств межмашинного информационного обмена, взаимодействие между конечными приложениями вычислительных установок в рамках вычислительной неоднородной сети посредством автоматического создания очереди исходящих и входящих сообщений для каждого конечного приложения; рандомизируются в соответствии с заранее заданной процедурой тело каждого сообщения, подлежащего обмену по единой защищенной магистрали информационного обмена, для обеспечения защиты содержимого этого

сообщения от несанкционированного доступа; инкапсулируют в соответствии с  
 заранее заданной процедурой рандомизированное тело каждого исходящего  
 сообщения, подлежащего обмену по единой защищенной магистрали  
 информационного обмена, для обеспечения глобальной маршрутизации в рамках  
 5 неоднородной вычислительной сети и обработки указанного сообщения на  
 узле-получателе; обеспечивают гарантированную доставку сообщений в рамках  
 неоднородной вычислительной сети посредством возвращения на узел-отправитель  
 квитанции о доставке исходящего сообщения на узел-получатель; создают на каждой  
 10 вычислительной установке защищенное хранилище данных, которое  
 рандомизировано по тому же принципу, что и тело сообщения; сохраняют в  
 защищенном хранилище данных каждой вычислительной установки очереди  
 исходящих и входящих сообщений как в адрес вычислительной установки или  
 функционирующего на ней программного приложения, так и в адрес иной  
 15 вычислительной установки неоднородной вычислительной сети; обеспечивают  
 гарантированное хранение входящих и транзитных сообщений в защищенном  
 хранилище данных до завершения процесса гарантированной доставки; сохраняют в  
 защищенном хранилище данных каждой вычислительной установки таблицу  
 20 маршрутизации сообщений в рамках неоднородной вычислительной сети, а также  
 идентификатор каждого конечного программного приложения, функционирующего в  
 контексте общесистемного программного обеспечения; обеспечивают  
 гарантированную обработку тела сообщения посредством указания номера  
 конечного приложения-обработчика, при помощи которого тело сообщения следует  
 25 обработать, и отправляют по факту этой обработки на узел-отправитель  
 подтверждение об обработке; систематически проверяют полномочия каждого  
 должностного лица, допущенного к работе с информационными ресурсами  
 неоднородной вычислительной сети, и останавливают сеанс работы конкретного  
 30 должностного лица при несовпадении хотя бы одного параметра из  
 соответствующего профиля доступа, хранящегося в защищенном хранилище данных  
 вычислительной установки; обеспечивают гарантированную идентификацию  
 исходящего и (или) входящего либо транзитного сообщения за счет применения  
 встроенного механизма идентификации должностных лиц в вычислительной сети на  
 35 основе электронно-цифровой подписи, чем достигается юридическая значимость  
 информационного обмена.

Особенность данного способа состоит в том, что общесистемное программное  
 обеспечение формируют путем надстройки каждой из операционных систем базовым  
 40 набором транспортных протоколов, предназначенных для глобальной трехуровневой  
 адресации узлов и маршрутизации пакетов, а также набором форматов обмена  
 данными прикладного уровня; обеспечивают транзитное направление  
 информационных потоков в рамках неоднородной вычислительной сети за счет  
 механизмов гарантированного хранения сообщений в защищенных хранилищах  
 45 данных на узлах трассы конкретной передачи, а также автоматического назначения  
 альтернативного маршрута передачи в соответствии с таблицей маршрутизации  
 каждой вычислительной установки по трассе передачи; обеспечивают возможность  
 передачи служебных сообщений, в том числе и предписаний на исполнение,  
 50 позволяющих осуществлять удаленные воздействия в рамках глобальной  
 вычислительной сети; обеспечивают единообразную реализацию системы передачи  
 данных в рамках неоднородной вычислительной сети, в том числе в условиях  
 выраженной разнородности программно-аппаратных реализаций вычислительных

установок сети.

Еще одна особенность данного способа состоит в том, что перенастройку интерфейсов каждой операционной системы для обмена данными с другими вычислительными установками неоднородной вычислительной сети осуществляют 5 путем перенаправления информационных потоков между вычислительными установками и прикладными задачами через соответствующие прокси-соединения, имеющиеся в средствах общесистемного программного обеспечения, в том числе и прикладными задачами клиентов электронной почты; перенастройку интерфейсов 10 каждой операционной системы для обмена данными между конечными программными приложениями в данной операционной системе осуществляют путем перенаправления информационных потоков между этими программными приложениями через соответствующие механизмы межзадачного взаимодействия, имеющиеся в средствах общесистемного программного обеспечения; реализуют 15 механизм назначения приоритета отправки сообщения за счет автоматической установки «ширины» канала передачи с возможностью отправки сообщения с низшим приоритетом в «фоновом» режиме; реализуют механизм коммутации сообщений, при котором в зависимости от «ширины» канала передачи автоматически выбирают 20 величину минимальных пакетов отправки, на которые разделяют исходное сообщение перед отправкой, а также осуществляют механизм «досылки» неотправленной части сообщения при возникновении сбоя канала передачи.

Еще одна особенность данного способа состоит в том, что протоколируют все действия должностных лиц, осуществляющих локальные или глобальные 25 взаимодействия в рамках неоднородной вычислительной сети, в соответствующие тематические журналы, представляющие собой плоские таблицы, хранящиеся в защищенном хранилище данных общесистемного программного обеспечения на каждой вычислительной установке.

Краткое описание чертежей

Изобретение поясняется далее в подробном описании со ссылками на прилагаемые 30 чертежи.

Фиг.1 представляет общую каноническую схему обеспечения взаимодействия разнообразных информационных ресурсов каждого персонального компьютера, 35 сервера и т.п. с предоставлением унифицированного сервиса обмена с каналами связи (блок КОМ) в способе по настоящему изобретению.

Фиг.2 показывает виды информационного взаимодействия и обеспечивающие их методы и механизмы, осуществляемые в способе по настоящему изобретению.

Фиг.3 показывает возможные топологии вычислительных сетей с назначением 40 альтернативной маршрутизации, представленных в настоящем изобретении.

Подробное описание изобретения

Общие требования к современным АС, невыполнение которых может поставить точку в развитии любой информационной системы, относятся, прежде всего, к 45 обеспечению надежного (гарантированного) информационного обмена на созданной информационной инфраструктуре:

1) в части обмена данными (физическая связность):

- данные произвольного типа,
- произвольные каналы связи,
- произвольная вычислительная среда;

2) в части унификации данных (логическая связность):

- единое адресное пространство,

- единые/интегрированные классификаторы,

- согласованные форматы данных;

3) интеграция «унаследованных» и актуальных задач СПО посредством единой общесистемной среды исполнения;

4) реализация единой политики безопасности посредством единых механизмов защиты;

5) централизованное управление вычислительным процессом на объектах АС.

Общие вопросы функционирования современных автоматизированных систем (АС)

часто решаются кардинальным образом, затрагивающим саму основу АС - ее архитектуру. Реализуется трехуровневая модель организации вычислительного процесса в рамках АС с введением так называемой среды функционирования в виде общесистемного (системообразующего) программного обеспечения (ПО), основу которого составляет так называемое ПО «промежуточного слоя», часто относящееся к категории Message Oriented Middleware (ММ). Реализация общесистемного ПО может варьироваться от стандартизованного прикладного ПО, требующего серьезных доработок прикладных задач, до мета-приложения или сетевого провайдера, предоставляющего интерфейсы для СПО. Задачи общесистемной среды АС таковы:

- предоставление типовых гарантированных сервисов по обмену данными и оперативному управлению объектами и процессами в локальной и глобальной сетях объектов АС;

- обеспечение гарантированного взаимодействия функциональных подсистем и объектов АС, интеграция СПО на основе унифицированной асинхронной модели обмена данными;

- обеспечение управляемости единым вычислительным процессом на объектах АС на основе общесистемных соглашений в части адресации информационных объектов АС, форматов данных, системных событий и сценариев их обработки;

- обеспечение защиты информации в АС на основе единой непротиворечивой политики безопасности, построенной на общих механизмах разграничения доступа, контроля целостности, кодирования;

- наличие инструментария прикладного программирования для решения задач адаптации СПО в АС.

Здесь учтен тот небыстрый факт, что далеко не везде существуют устойчивые каналы связи, и не всегда есть возможность соединения с удаленным абонентом по цифровым выделенным каналам. Но, даже имея обычные возможности подключения, современная автоматизированная система обязана обеспечивать не только сбор и хранение информации в низовых звеньях, но возможность гарантированного доведения информации, возможность подключения к системе «мобильных» пользователей в рамках наделенных полномочий. Таким образом, основа безотказной работы АС в целом - встроенный механизм гарантированного доведения, включающий в себя гарантированные механизмы передачи, хранения и регламентной обработки информации с использованием службы «единого времени» и механизма гарантированной идентификации на основе технологии PKI (электронной цифровой подписи - ЭЦП).

Все здесь сказанное об общесистемной среде есть не что иное, как почти дословная трактовка известных принципов SOA - Service-Oriented Architecture (архитектура обслуживания запросов), одного из современных взглядов на принципы построения АС, реализующих такое общее понятие, как интеграционная платформа, в основе

функционирования которой лежит упомянутое общесистемное ПО.

К особенностям такого архитектурного подхода в деле создания АС произвольной природы можно сразу отнести тот факт, что любая технология, подразумевающая развитие хотя бы на 10 лет вперед, должна акцентировать внимание на том, что  
любые революционные идеи и методы в обязательном порядке должны позволять их интегрировать в уже имеющиеся информационные системы исключительно эволюционным путем. В противном случае они могут означать лишь очередной тупик в развитии. Обратим внимание, что общесистемные средства являются наиболее консервативным по своей природе объектом АС, который подвержен изменениям в меньшей степени, нежели чем ОС, функционирующая логически «ниже».

Общесистемное ПО класса MOM не является простым приложением, это мета-приложение (или служба), взаимодействующее с ОС на основе закрытых протоколов обмена, что создает новую сущность - композитный многоядерный продукт с высокой степенью защищенности, существенно выше, чем класс защищенности самой ОС.

Кроме того, имея в своем распоряжении многочисленные механизмы и способы адаптации возможностей конкретных прикладных задач до общесистемных требований, интеграционная платформа является средством вовлечения в АС любого актуального «унаследованного» ПО, необходимого заказчику. К основным преимуществам решения задач АС на основе интеграционной платформы являются следующие:

- унификация программно-аппаратной среды АС на системном уровне;
- унификация среды исполнения на уровне системных вызовов;
- интеграция разнородных программно-аппаратных платформ;
- единое адресное пространство наложенной сети;
- создание универсальной транспортной магистрали с динамической маршрутизацией и трансляцией протоколов;
- переносимость прикладного ПО, в том числе и «унаследованного» ПО;
- служба единого времени магистрали, фиксация системных событий;
- обеспечение разграничения доступа и контроля целостности на основе единых методов защиты;
- мониторинг состояния и контроль управления на аппаратном уровне и уровне исполнения.

На фиг.1 показана так называемая каноническая схема реализации вычислительного процесса на каждом рабочем месте (ПК, сервере и т.п.), когда весь информационный обмен на уровне данных идет по стандартизованным «стыкам» (ODBC, XML и пр.), а на уровне каналов связи реализуется общесистемными средствами (блок КОМ) с необходимым контролем доступа к каналу связи (блок ОБИ). Обозначения на фиг.1: КОМ - так называемый «транспортный коммутатор», т.е. набор процедур, отвечающих за функционирование того или иного канала связи на уровне протокола обмена; ОБИ - комплекс средств, фиксирующий обращения прикладных процессов к ресурсам системы и подтверждающий или отказывающий в доступе,  $Z_i$  -  $i$ -ая задача ( $i=1,2,\dots,n$ ), API UP - набор API-функций ядра общесистемных средств (Application Program Interface Universal Platform - интерфейс прикладного программирования универсальной платформы), API ОС - набор API-функций ядра системных средств (операционной системы - ОС), CPU - центральный процессор, RAM -

ОЗУ, HDD - накопитель на жестком диске, I/O - средства ввода-вывода, TCP/IP IPX/SPX СОД/СПД - протоколы транспортного уровня по модели OSI/ISO, ODBC

XML - стандартные интерфейсы взаимодействия в информационных системах (Open DataBase Connectivity - это открытый интерфейс доступа к базам данных и extensible Markup Language - расширяемый язык разметки).

К общесистемным задачам функционирования АС, возлагаемым на интеграционную платформу и общесистемные средства, относятся, прежде всего, задачи обмена данными между абонентами сети. К ним относятся:

- обмен документами, сообщениями, файлами между абонентами АС с возможностью перекодировки данных, если обработка осуществляется с использованием различных ОС, в том числе с автоматическим распознаванием форматов и запуском обрабатывающих программ на приемной стороне (удаленные управляющие воздействия);
- обмен данными в собственном представлении (для приложений, зарегистрированных в среде АС), а также в XML-представлении;
- режимы избирательной и циркулярной доставки информации до абонентов;
- гарантированное доведение информации до абонентов при отказе/восстановлении каналов связи, автоматическое назначение альтернативных маршрутов передачи данных;
- автоматическое квитирование факта доведения информации до обрабатывающей задачи на АРМ-получателе, возможность отправки уведомления источнику после завершения цикла обработки данных на приемной стороне;
- поддержка синхронного («клиент-сервер») и асинхронного (с использованием очередей) режимов обмена данными между абонентами;
- настройка адресации и ведение каталога адресов;
- ведение журнала входящих и исходящих сообщений;
- возможность изменения состава взаимодействующих абонентов при реконфигурации системы в случае включения (отключения) новых объектов в АС;
- возможность адресации по статическим и динамическим IP-адресам.

Общесистемные средства представляют собой модульную систему, состоящую из компактного надежного ядра и задач (утилит), функционирующих в его контексте. Они разделены на подсистемы по типу исполняемых ими задач для АС.

- Подсистема передачи данных. Средства асинхронного гарантированного доведения инкапсулированных сообщений в неоднородной территориально-распределенной АС. Динамическая маршрутизация. Трансляция протоколов.

- Подсистема интеграции. Средства обеспечения логической связности различных ПТС (программно-технических средств), в том числе: MS Windows NT/2000/XP/2003/CE, Linux, MacOS, OS/2, VM/ESA, Sun Solaris. Управление вычислительным процессом в разнородной среде АС.

- Подсистема хранения. Средства гарантированного хранения информации в защищенном хранилище на каждой вычислительной установке.

- Подсистема безопасности. Средства разграничения доступа к информационным ресурсам АС на основе идентификации и аутентификации пользователей (в том числе ЭЦП), а также контроля целостности вычислительного процесса АС. Интеграция со средствами защиты периметра.

- Подсистема представления данных. Web-ориентированное распределенное хранилище данных, средства поиска и доступа к разнородной информации АС. Семантический и статистический анализ. Управление ресурсами.

- Подсистема удаленного мониторинга и контроля функционирования клиентов АС

на основе обеспечения удаленных воздействий. ГИС-представление (ГИС - гео-информационная система, т.е. представление распределенных данных, спозиционированных на карт-фон).

- Универсальный API-набор. Средства быстрой разработки приложений.

Интеграционная платформа представляет собой развивающуюся систему, в перспективе подсистемы платформы могут меняться и расширять функциональность платформы в сторону задач, выдвигаемых заказчиком при построении АС.

Общесистемные средства, обеспечивающие возможности гарантированного доведения информации в территориально-распределенных неоднородных сетях, предоставляют широкие возможности в деле обеспечения взаимодействий разного рода внутри АС.

- Пользователь-Пользователь

при помощи встроенных средств межмашинного обмена на основе организационно-штатной структуры объекта АС (должностные лица) в рамках наделенных полномочий;

- Объект-Объект

при помощи средств межобъектового обмена на основе иерархической подчиненности (3 уровня) объектов АС и должностных лиц объектов в рамках наделенных полномочий;

- Данные-Данные

при помощи виртуальных «витрин данных» и средств промежуточного хранения на основе созданной инфраструктуры информационного обмена (пользователи, объекты) и общесистемных соглашений о представлении данных;

- Приложение-Приложение

при помощи очередей входящих/исходящих сообщений для каждого приложения, документов, регламентов информационного обмена, упорядоченных данных в XML-формате, а также возможности обеспечения удаленных воздействий на созданной инфраструктуре информационного обмена (пользователи, объекты, витрины).

Для обеспечения автоматизации на объектах АС разрабатывается процессный язык, на основании которого формализуются процессы прохождения документов и сообщений в АС. Определяются понятия системных событий, необходимых для построения цепочек процессов, сценарии обработки тех или иных событий в точках ветвления. Таким образом, вырабатываются общесистемные соглашения в части системных событий и регламентов, которые позволяют замкнуть круг обработки следующим типом взаимодействий.

- Процесс-Процесс

при помощи очередей ассоциированных процессов для каждого приложения, формализованных регламентов информационного обмена, упорядоченных данных, а также возможности отработки сценариев на созданной инфраструктуре информационного обмена (пользователи, объекты, витрины, приложения).

Эти взаимодействия, а также методы и механизмы, необходимые для реализации этих взаимодействий, показаны на фиг.2, где обозначено: П-П - пользователь-пользователь (действия 1-4), О-О - объект-объект (действия 5-8), Д-Д - данные-данные (действия 9-11), Пр-Пр - приложение-приложение (действия 12-15), Проц-Проц - процесс-процесс действия 16-18); Дл-Дл -... (действия 19-21).

Таким образом, появляется возможность осуществления крупномасштабных информационных проектов с использованием произвольных объектов автоматизации,

имеющихся в распоряжении заказчика. Причем, появляется возможность расширения функциональности таких АС за счет расширения топологии вычислительных сетей: от классических топологий типа «звезда», через актуальную топологию «двойная» или «иерархическая» звезда к сетеподобным решениям, использующим все возможности информационной инфраструктуры.

Это показано на фиг.3.

Настоящее изобретение реализует все вышесказанное в неоднородной вычислительной сети, которая образуется территориально-распределенными объектами автоматизации, связанными магистралью информационного обмена в единую глобальную вычислительную сеть. Неоднородная вычислительная сеть включает в себя по меньшей мере две соединенные сетью связи вычислительные установки, представляющие собой локальные и (или) глобальные объекты автоматизации, по меньшей мере одна из которых снабжена отличной от других операционной системой. В этой неоднородной вычислительной сети осуществляются следующие действия.

На каждую вычислительную установку устанавливают общесистемное программное обеспечение (ОПО) для получения единой защищенной магистрали информационного обмена между всеми вычислительными установками в неоднородной вычислительной сети. Примером такого ОПО может быть IBM Corp. (WebSphere (CICS, MQ Series etc.)), Microsoft Corp. (Windows (MSMQ), BizTalk Server etc.), Computer Associates (Unicenter), SAP AG (NetWeaver), TIBCO Software (Rendezvous), Oracle Corp.(OTC, OO4O, Fusion Middleware), BEA Systems (WebLogic Enterprise Platform), Sun Microsystems (Java Composite Application Platform Suite (CAPS)), ЗАО ИВК (ИВК Юпитер).

Это общесистемное программное обеспечение формируют, в частности, путем надстройки каждой операционной системы базовым набором транспортных протоколов, предназначенных для глобальной адресации узлов и маршрутизации пакетов, а также набором форматов обмена данными прикладного уровня.

На каждой вычислительной установке обеспечивают единые унифицированные средства межмашинного информационного обмена, реализующие физическую связность вычислительных установок в рамках единой защищенной магистрали информационного обмена. Посредством этих средств межмашинного информационного обмена обеспечивают единообразное взаимодействие как между вычислительными установками в локальной вычислительной сети объекта автоматизации, входящего в неоднородную вычислительную сеть, так и между глобальными объектами автоматизации в рамках неоднородной вычислительной сети. При этом в каждой операционной системе перенастраивают все системные интерфейсы по обмену данными на соответствующие механизмы обмена данными общесистемного программного обеспечения. Такую перенастройку интерфейсов каждой операционной системы для обмена данными с другими вычислительными установками в неоднородной вычислительной сети осуществляют, например, путем перенаправления информационных потоков между вычислительными установками и прикладными задачами через соответствующие прокси-соединения, имеющиеся в средствах общесистемного программного обеспечения, в том числе и такими прикладными задачами, как стандартные клиенты электронной почты. Перенастройку же интерфейсов каждой операционной системы для обмена данными между конечными программными приложениями в данной операционной системе осуществляют путем перенаправления информационных потоков между этими

программными приложениями через соответствующие механизмы межзадачного взаимодействия, имеющиеся в средствах общесистемного программного обеспечения.

С помощью средств межмашинного информационного обмена обеспечивают взаимодействие между конечными приложениями вычислительных установок в рамках вычислительной неоднородной сети посредством автоматического создания очереди исходящих и входящих сообщений для каждого конечного приложения. При этом тело каждого сообщения, подлежащего обмену по единой защищенной магистрали информационного обмена, рандомизируют в соответствии с заранее заданной процедурой для обеспечения защиты содержимого этого сообщения от несанкционированного доступа. В качестве такой процедуры можно указать, например, процедуру абонентского шифрования трафика на симметричных ключах.

В соответствии с этой заранее заданной процедурой инкапсулируют рандомизированное тело каждого исходящего сообщения, подлежащего обмену по единой защищенной магистрали информационного обмена, для обеспечения глобальной маршрутизации в рамках неоднородной вычислительной сети и обработки указанного сообщения на узле-получателе. Гарантированную доставку сообщений в рамках неоднородной вычислительной сети обеспечивают посредством возвращения на узел-отправитель квитанцию о доставке исходящего сообщения на узел-получатель.

При отправке сообщения реализуют механизм назначения приоритета за счет автоматической установки «ширины» канала передачи с возможностью отправки сообщения с низшим приоритетом в «фоновом» режиме. В этом случае реализуют механизм коммутации сообщений, при котором в зависимости от «ширины» канала передачи автоматически выбирают величину минимальных пакетов отправки, на которые разделяют исходное сообщение перед отправкой, а также осуществляют механизм «досылки» неотправленной части сообщения при возникновении сбоя канала передачи.

На каждой вычислительной установке создают защищенное хранилище данных, которое рандомизировано по тому же принципу, что и тело сообщения. В этом защищенном хранилище данных каждой вычислительной установки сохраняют очереди исходящих и входящих сообщений как в адрес вычислительной установки или функционирующего на ней программного приложения, так и в адрес иной вычислительной установки неоднородной вычислительной сети. В защищенном хранилище данных обеспечивают гарантированное хранение входящих и транзитных сообщений до завершения процесса гарантированной доставки. Кроме того, в защищенном хранилище данных каждой вычислительной установки сохраняют таблицу маршрутизации сообщений в рамках неоднородной вычислительной сети, а также идентификатор каждого конечного программного приложения, функционирующего в контексте общесистемного программного обеспечения.

При этом в неоднородной вычислительной сети обеспечивают транзитное направление информационных потоков за счет механизмов гарантированного хранения сообщений в защищенных хранилищах данных на узлах трассы конкретной передачи, а также автоматического назначения альтернативного маршрута передачи в соответствии с таблицей маршрутизации каждой вычислительной установки по трассе передачи. Кроме того, это позволяет обеспечить возможность передачи служебных сообщений, в том числе и предписаний на исполнение, позволяющих осуществлять удаленные воздействия в рамках глобальной вычислительной сети. Благодаря этому обеспечивается единообразная реализация системы передачи данных в рамках неоднородной вычислительной сети, в том числе в условиях выраженной

разнородности программно-аппаратных реализаций вычислительных установок сети.

Далее, гарантированную обработку тела сообщения обеспечивают посредством указания номера конечного приложения-обработчика, при помощи которого тело сообщения следует обработать, и отправляют по факту этой обработки на узел-отправитель подтверждение об обработке. Это является очередным механизмом в деле гарантированного доведения информации.

В сети систематически проверяют полномочия каждого должностного лица, допущенного к работе с информационными ресурсами неоднородной вычислительной сети, и останавливают сеанс работы конкретного должностного лица при несовпадении хотя бы одного параметра из соответствующего профиля доступа, хранящегося в защищенном хранилище данных вычислительной установки. При этом все действия должностных лиц, осуществляющих локальные или глобальные взаимодействия в рамках неоднородной вычислительной сети, протоколируют в соответствующие тематические журналы, представляющие собой плоские таблицы, хранящиеся в защищенном хранилище данных общесистемного программного обеспечения на каждой вычислительной установке.

Наконец, в сети обеспечивают гарантированную идентификацию исходящего и (или) входящего либо транзитного сообщения за счет применения встроенного механизма идентификации должностных лиц в вычислительной сети на основе электронно-цифровой подписи, чем достигается юридическая значимость информационного обмена.

Таким образом, благодаря предлагаемому способу обеспечивается гарантированное (со 100%-ной вероятностью) доведение электронных документов до конкретных пользователей. Одним из основных решений по созданию информационно-технологического обеспечения АС, в том числе исходя из перечисленных выше механизмов, является решение о ее архитектуре. Создание АС на трехуровневой архитектуре с применением продуктов «промежуточного слоя», реализующих общесистемные функции АС, позволяет решить все вопросы совместного функционирования разнородных информационных ресурсов на основе полноценной реализации гарантированного доведения информации в современных автоматизированных вычислительных сетях.

В данном описании настоящее изобретение раскрыто посредством примеров его возможного осуществления. Однако эти примеры являются лишь иллюстративными, а не ограничивающими, и объем данного изобретения определяется прилагаемой формулой изобретения с учетом любых возможных эквивалентов.

#### Формула изобретения

1. Способ гарантированного доведения информации в неоднородной вычислительной сети, образованной территориально-распределенными объектами автоматизации, связанными магистралью информационного обмена в единую глобальную вычислительную сеть, и включающей в себя по меньшей мере две соединенных сетью связи вычислительные установки, представляющие собой локальные и (или) глобальные объекты автоматизации, по меньшей мере одна из которых снабжена отличной от других операционной системой, заключающийся в том, что:

устанавливают на каждую вычислительную установку общесистемное программное обеспечение для получения единой защищенной магистрали информационного обмена между всеми вычислительными установками упомянутой

неоднородной вычислительной сети;

обеспечивают на каждой вычислительной установке единые унифицированные средства межмашинного информационного обмена, реализующие физическую связность упомянутых вычислительных установок в рамках упомянутой единой защищенной магистрали информационного обмена;

обеспечивают посредством упомянутых средств межмашинного информационного обмена единообразное взаимодействие как между вычислительными установками в локальной вычислительной сети объекта автоматизации, входящего в упомянутую неоднородную вычислительную сеть, так и между глобальными объектами автоматизации в рамках упомянутой неоднородной вычислительной сети;

перенастраивают в каждой операционной системе все системные интерфейсы по обмену данными на соответствующие механизмы обмена данными упомянутого общесистемного программного обеспечения;

обеспечивают с помощью упомянутых средств межмашинного информационного обмена взаимодействие между конечными приложениями вычислительных установок в рамках упомянутой вычислительной неоднородной сети посредством автоматического создания очереди исходящих и входящих сообщений для каждого упомянутого конечного приложения;

рандомизируют в соответствии с заранее заданной процедурой тело каждого сообщения, подлежащего обмену по упомянутой единой защищенной магистрали информационного обмена, для обеспечения защиты содержимого этого сообщения от несанкционированного доступа;

инкапсулируют в соответствии с заранее заданной процедурой рандомизированное тело каждого исходящего сообщения, подлежащего обмену по упомянутой единой защищенной магистрали информационного обмена, для обеспечения глобальной маршрутизации в рамках упомянутой неоднородной вычислительной сети и обработки указанного сообщения на узле-получателе;

обеспечивают гарантированную доставку сообщений в рамках упомянутой неоднородной вычислительной сети посредством возвращения на узел-отправитель квитанции о доставке исходящего сообщения на узел-получатель;

создают на каждой упомянутой вычислительной установке защищенное хранилище данных, которое рандомизировано по тому же принципу, что и тело сообщения;

сохраняют в упомянутом защищенном хранилище данных каждой упомянутой вычислительной установки очереди исходящих и входящих сообщений как в адрес упомянутой вычислительной установки или функционирующего на ней программного приложения, так и в адрес иной вычислительной установки упомянутой неоднородной вычислительной сети;

обеспечивают гарантированное хранение входящих и транзитных сообщений в упомянутом защищенном хранилище данных до завершения процесса гарантированной доставки;

сохраняют в упомянутом защищенном хранилище данных каждой упомянутой вычислительной установки таблицу маршрутизации сообщений в рамках упомянутой неоднородной вычислительной сети, а также идентификатор каждого конечного программного приложения, функционирующего в контексте упомянутого общесистемного программного обеспечения;

обеспечивают гарантированную обработку тела сообщения посредством указания номера конечного приложения-обработчика, при помощи которого тело сообщения следует обработать, и отправляют по факту этой обработки на узел-отправитель

подтверждение об обработке;

систематически проверяют полномочия каждого должностного лица, допущенного к работе с информационными ресурсами упомянутой неоднородной вычислительной сети, и останавливают сеанс работы конкретного должностного лица при  
5 несовпадении хотя бы одного параметра из соответствующего профиля доступа, хранящегося в защищенном хранилище данных упомянутой вычислительной установки;

обеспечивают гарантированную идентификацию исходящего, и(или) входящего,  
10 либо транзитного сообщения за счет применения встроенного механизма идентификации должностных лиц в вычислительной сети на основе электронно-цифровой подписи, чем достигается юридическая значимость информационного обмена.

2. Способ по п.1, в котором:

15 формируют упомянутое общесистемное программное обеспечение путем надстройки каждой из упомянутых операционных систем базовым набором транспортных протоколов, предназначенных для глобальной адресации узлов и маршрутизации пакетов, а также набором форматов обмена данными прикладного  
20 уровня;

обеспечивают транзитное направление информационных потоков в рамках упомянутой неоднородной вычислительной сети за счет механизмов  
гарантированного хранения сообщений в защищенных хранилищах данных на узлах  
25 трассы конкретной передачи, а также автоматического назначения альтернативного маршрута передачи в соответствии с таблицей маршрутизации каждой упомянутой вычислительной установки по упомянутой трассе передачи;

обеспечивают возможность передачи служебных сообщений, в том числе и предписаний на исполнение, позволяющих осуществлять удаленные воздействия в  
30 рамках упомянутой глобальной вычислительной сети;

обеспечивают единообразную реализацию системы передачи данных в рамках упомянутой неоднородной вычислительной сети, в том числе в условиях выраженной  
разнородности программно-аппаратных реализаций упомянутых вычислительных  
установок сети.

3. Способ по п.1, в котором:

упомянутую перенастройку интерфейсов каждой операционной системы для обмена данными с другими вычислительными установками упомянутой неоднородной  
вычислительной сети осуществляют путем перенаправления информационных  
40 потоков между вычислительными установками и прикладными задачами через соответствующие прокси-соединения, имеющиеся в средствах упомянутого общесистемного программного обеспечения, в том числе и такими прикладными задачами, как стандартные клиенты электронной почты;

упомянутую перенастройку интерфейсов каждой операционной системы для обмена  
45 данными между конечными программными приложениями в данной операционной системе осуществляют путем перенаправления информационных потоков между этими программными приложениями через соответствующие механизмы межзадачного взаимодействия, имеющиеся в средствах упомянутого общесистемного  
программного обеспечения;

реализуют механизм назначения приоритета отправки сообщения за счет автоматической установки «ширины» канала передачи с возможностью отправки  
50 сообщения с низшим приоритетом в «фоновом» режиме;

реализуют механизм коммутации сообщений, при котором в зависимости от «ширины» канала передачи автоматически выбирают величину минимальных пакетов отправки, на которые разделяют исходное сообщение перед отправкой, а также осуществляют механизм «досылки» неотправленной части сообщения при  
5 возникновении сбоя канала передачи.

4. Способ по п.1, в котором:

протоколируют все действия должностных лиц, осуществляющих локальные или глобальные взаимодействия в рамках упомянутой неоднородной вычислительной  
10 сети, в соответствующие тематические журналы, представляющие собой плоские таблицы, хранящиеся в упомянутом защищенном хранилище данных общесистемного программного обеспечения на каждой упомянутой вычислительной установке.

15

20

25

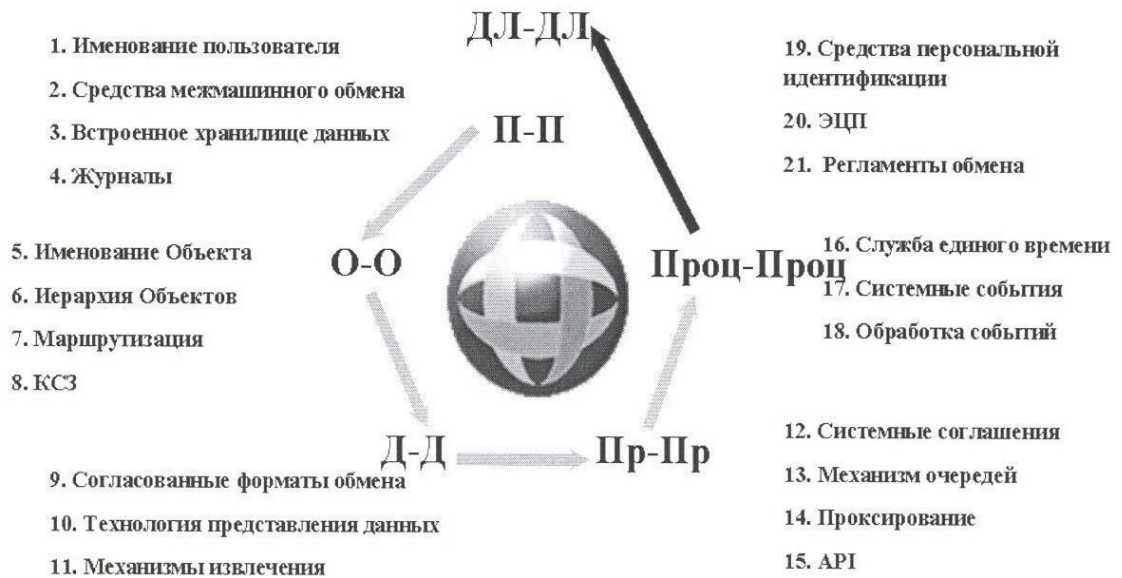
30

35

40

45

50



Фиг.2



Фиг. 3