РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 765 567**(13) **C2**

(51) МПК
H04L 29/12 (2006.01)
G06F 21/64 (2013.01)
G06F 21/62 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/62 (2021.08); G06F 21/64 (2021.08); H04L 61/2076 (2021.08); H04L 63/0876 (2021.08)

(21)(22) Заявка: **2019131257, 08.03.2018**

(24) Дата начала отсчета срока действия патента:
08.03.2018

Дата регистрации:
01.02.2022

Приоритет(ы):
(30) Конвенционный приоритет:
09.03.2017 EP 17160170.1

(43) Дата публикации заявки: **10.04.2021** Бюл. № **10**

(45) Опубликовано: **01.02.2022** Бюл. № **4**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **09.10.2019**

(86) Заявка PCT:
EP 2018/055846 (08.03.2018)

(87) Публикация заявки PCT:
WO 2018/162687 (13.09.2018)

Адрес для переписки:
115432, Москва, ул. Трофимова, 8А, кв. 12, Маркиной Е.Г.

(72) Автор(ы):
ГУЛБРАНДСЕН, Магнус, Скраастад (NO)

(73) Патентообладатель(и):
ГУЛБРАНДСЕН, Магнус, Скраастад (NO)

(56) Список документов, цитированных в отчете о поиске: **US 2016/0182519 A1, 23.06.2016. AAFAF OUADDAH et al., FairAccess: a new Blockchain-based access control framework for the Internet of Things: FairAccess: a new access control framework for IoT, SECURITY AND COMMUNICATION NETWORKS, vol. 9, no. 18, c. 5943-5964, 01.12.2016. BENSHOOF BRENDAN et al., Distributed Decentralized Domain Name Service",** (см. прод.)

(54) ПРОВАЙДЕР ДОСТУПА К БАЗОВОЙ СЕТИ

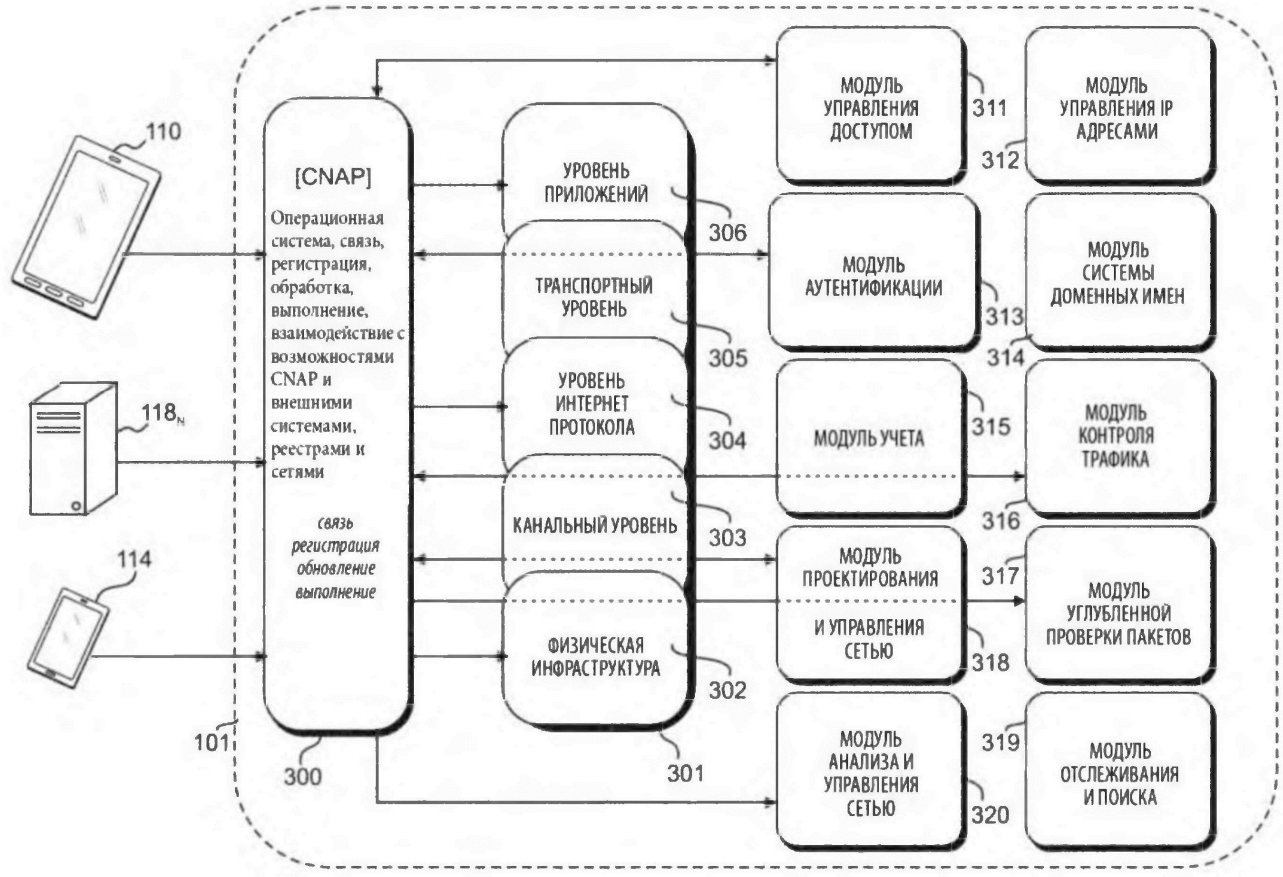
(57) Реферат:

Изобретение относится к способу предоставления доступа к сети узлам, таким как структуры и устройства данных, и соответствующая сетевая архитектура. Технический результат – повышение скорости доступа к сети доступа. По меньшей мере один провайдер доступа к базовой сети управляет доступом к сети в реальном масштабе времени посредством уровней стека протоколов для сети и последовательно присваивает сетевой коммуникационный адрес для одного или каждого запрашивающего доступ узла. Присвоенный сетевой адрес кодируется с уникальным параметром узла и уникальным параметром пользователя узла в реестре последовательных идентификаторов, который распределяется ко всем подключенным к сети узлам в реальном масштабе времени. Каждый узел обрабатывает реестр для проверки его последовательной целостности, и при определении потери последовательной целостности идентифицирует запись реестра, вызывающую потерю, и осуществляет широковещательную передачу оповещения, содержащего идентифицированную запись, к узлам в сети. Провайдер доступа к базовой сети отменяет

RU 2765567 C2

RU 2765567 C2

доступ к сети для узла, которому был присвоен сетевой коммуникационный адрес, соответствующий идентифицированной записи в реестре, либо после идентификации записи в реестре на этапе проверки, либо при получении оповещения. 2 н. и 12 з.п. ф-лы, 10 ил.



Фиг. 3

(56) (продолжение):
2016 IEEE INTERNATIONAL PARALLEL AND DISTRIBUTED PROCESSING SYMPOSIUM WORKSHOPS (IPDPSW), IEEE, с. 1279-1287, 23.05.2016. RU 2534950 C2, 10.12.2014.

RU 2765567 C2

RU 2765567 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 765 567**(13) **C2**

(51) Int. Cl.
H04L 29/12 (2006.01)
G06F 21/64 (2013.01)
G06F 21/62 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/62 (2021.08); G06F 21/64 (2021.08); H04L 61/2076 (2021.08); H04L 63/0876 (2021.08)

(21)(22) Application: **2019131257, 08.03.2018**

(24) Effective date for property rights:
08.03.2018

Registration date:
01.02.2022

Priority:
(30) Convention priority:
09.03.2017 EP 17160170.1

(43) Application published: **10.04.2021** Bull. № **10**

(45) Date of publication: **01.02.2022** Bull. № **4**

(85) Commencement of national phase: **09.10.2019**

(86) PCT application:
EP 2018/055846 (08.03.2018)

(87) PCT publication:
WO 2018/162687 (13.09.2018)

Mail address:
115432, Moskva, ul. Trofimova, 8A, kv. 12, Markinoj E.G.

(72) Inventor(s):
GULBRANDSEN, Magnus, Skraastad (NO)

(73) Proprietor(s):
GULBRANDSEN, Magnus, Skraastad (NO)

RU 2765567 C2

RU 2765567 C2

(54) PROVIDER OF ACCESS TO BASE NETWORK

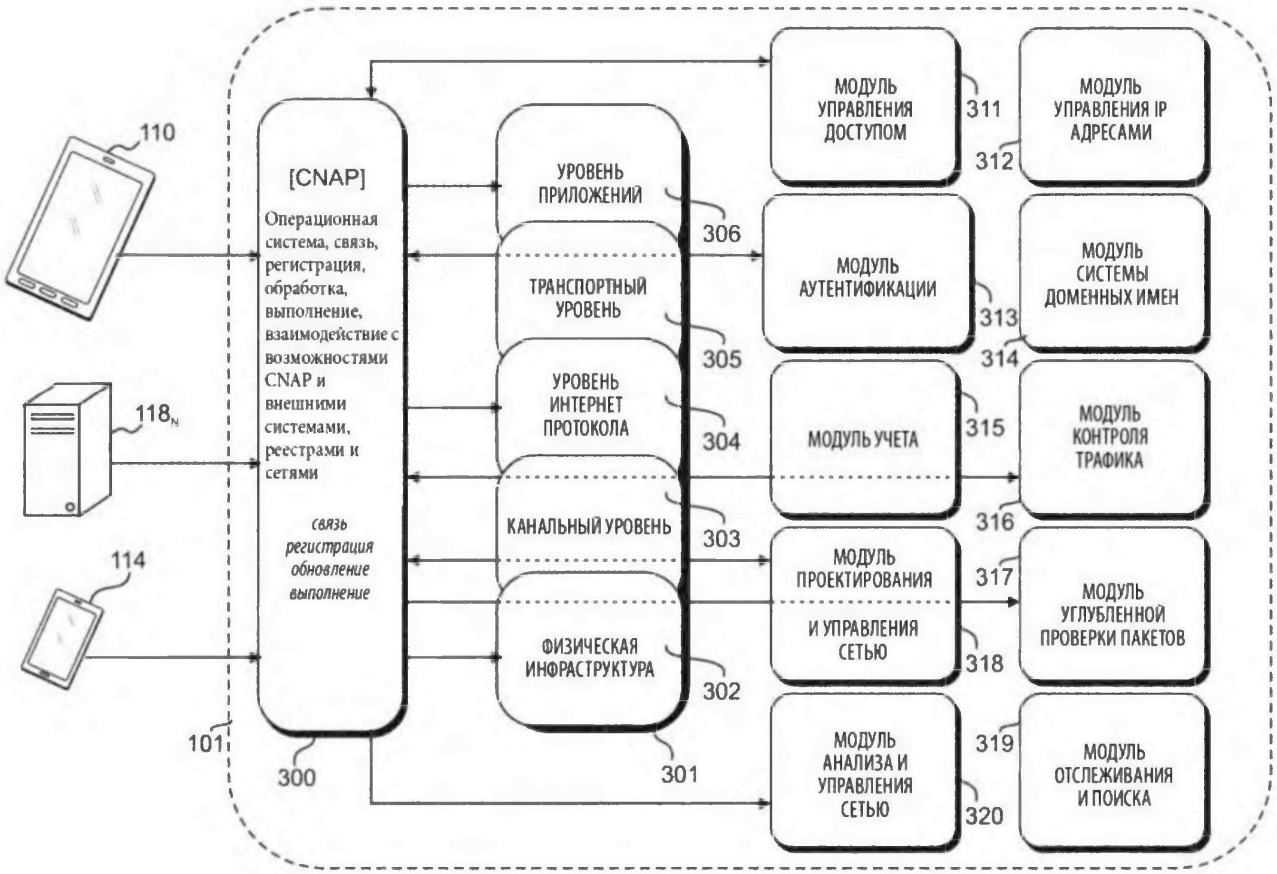
(57) Abstract:

FIELD: communication.

SUBSTANCE: invention relates to a method for providing network access to nodes, such as data structures and devices, and the corresponding network architecture. At least one provider of access to a base network manages access to the network in real time through levels of a protocol stack for the network and sequentially assigns a network communication address for one or each node requesting access. The assigned network address is encoded with a unique node parameter and a unique node user parameter in the registry of sequential identifiers, which is distributed to all nodes connected to the network in real time. Each node processes the registry to verify its sequential integrity, and, when determining the loss of sequential integrity, identifies a registry record causing the loss, and broadcasts an alert containing the identified record to nodes in the network. The provider of access to the base network cancels access to the network for the node that has been assigned with the network communication address corresponding to the record identified in the registry, either after identifying the record in the registry at the verification stage, or upon receiving the alert.

EFFECT: increase in the speed of access to the access network.

14 cl, 10 dwg



Фиг. 3

RU 2765567 C2

RU 2765567 C2

ОБЛАСТЬ ТЕХНИКИ

[001] Данное изобретение относится к системе и способу управления доступом устройств обработки данных к сетям. В частности, данное изобретение относится к системам и способам управления доступом устройств обработки данных к сетям посредством распределенного реестра, объединяющего адресный протокол и атрибуты идентификатора пользователей.

УРОВЕНЬ ТЕХНИКИ

[002] В современном мире вычислительные устройства, подключенные к сети посредством постоянных или полупостоянных соединений, выходят далеко за пределы обычных компьютеров и ноутбуков прошлых лет, и охватывают такие персональные терминалы связи, как смартфоны, промышленные и бытовые приборы, персональные транспортные средства и многие другие устройства, включая даже игрушки, все вместе обычно называемые как «вещи» в выражении «Интернет вещей», причем их суммарное количество увеличилось за сравнительно короткий промежуток времени, за двадцать-тридцать лет, от десятков-сотен тысяч по меньшей мере до нескольких десятков миллионов, параллельно с использованием почти повсеместной возможности сетевого подключения.

[003] Темп такого развития постоянно растет, в зависимости от общего числа вычислительных устройств, используемых в сети, в любой момент времени, в скором времени или уже сейчас, легко превышая численность людей, одновременно использующих их.

[004] В результате данной ситуации возникает две задачи, которые по своей природе связаны друг с другом. Во-первых, необходимо установить в соответствующий момент времени и поддерживать в течение определенного периода времени на любом конкретном узле сети уровень доверия относительно идентификатора пользователя, связанного с удаленным узлом, например, компьютером, подключенным к Интернету, холодильником, также подключенным к Интернету, смартфоном, подключенным к сотовой сети связи, или отдельным сеансом программного обеспечения как услуги на любой платформе. Во-вторых, необходимо учитывать постоянно растущее число сетевых узлов, связанных с каким-либо конкретным человеком, которое увеличивает этот уровень доверия во множестве сетей, работающих с использованием различных протоколов и имеющих изменяющиеся в широком диапазоне требования к аутентификации и пропускные способности.

[005] Недавние попытки найти выход из вышеуказанного затруднительного положения основывались на технологиях, основанных на цепочках блоков, для которых, как известно, требуются нетривиальные объемы вычислительной мощности компьютера для целей верификации и которые имеют ограниченную гибкость для адаптации к различным контекстам приложения. Кроме того, по существу анонимный дизайн Интернета приводит к беспристрастной нейтральности технологии в случае решений, ориентированных на узлы: в протоколе TCP/IP отправитель данных является потенциально анонимным, а интеллектуальные функции осуществляются в узлах, а не в сети, в целях устойчивости к ошибкам, удобства и эффективности. Такая конструктивная структура предотвращает аутентификацию в масштабе всей сети, вместо этого требуется аутентификация для конкретного сеанса, например, с использованием протокола безопасности транспортного уровня.

[006] Исследования для технологических решений вышеуказанных проблем обычно проводятся вне административного контекста контроля подлинности и соображений личной или национальной безопасности. Такое несоответствие между цифровой сферой

и административными структурами, такими как границы, национальности и другие юрисдикционные правила, приводит к появлению нетривиальных государственных ресурсов, предназначенных для аудита и наблюдения за сетевыми данными в целях безопасности, поскольку все еще крайне непрактично обеспечивать соблюдение отслеживаемости пользователей и границ в цифровых сетях.

[007] Аутентификация, отслеживаемость и контроль соблюдения установленных требований являются необходимыми условиями для создания стабильной, предсказуемой и безопасной среды. Ввиду вышеизложенного, таким образом, требуется масштабируемая сетевая архитектура, выполненная с возможностью аутентификации и контроля пользователя, устройства и/или идентичности структуры данных, а не отсрочки задачи дискретных сущностей специально для конкретной цели.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[008] Данное изобретение относится к архитектуре сети, включающей реестры и системы для информации, связи, целостности транзакций и безопасности, которая реализуется с помощью алгоритма, реализуемого одним или более провайдеров доступа к базовой сети (CNAP, core network access providers), взаимодействующих со всеми уровнями, включая нижние уровни инфраструктуры в сети связи для управления доступом пользователей к реестрам и системам и взаимодействию, при этом один из реестров интегрирует распределенный реестр идентификаторов узлов, систем и адресов связи с адресным протоколом и атрибутами идентификатора пользователя или узла. Данное изобретение относится к архитектуре и операционной системе, позволяющим проектировать системы, сети и реестры с правами и применением политик для обеспечения целостности информации, связи, транзакций, идентификатора и доступа, а также безопасности с использованием различных уровней инфраструктуры в сети связи и подключенных системах, сетях и реестрах для управления использованием систем, сетей и реестров. Данный способ осуществляется посредством систем провайдера доступа к базовой сети (CNAP), используемых для разрешенного доступа к доверенным системам, все из которых могут взаимодействовать с другими платформами, приложениями, реестрами и сетями.

[009] В соответствии с аспектом данного изобретения, с учетом вышесказанного предложен реализованный на компьютере способ предоставления каждому узлу сети доступа к сети (и сетевой системе или системам, которые работают или подключены к сети, и/или к любым другим узлам, подключенным к сети), причем сеть содержит по меньшей мере один стек протоколов, содержащий множество уровней, причем способ включает этапы: управление доступом в реальном масштабе времени и активностью в сети каждого уровня стека протоколов посредством по меньшей мере одного провайдера доступа к базовой сети, причем провайдер доступа к базовой сети содержит по меньшей мере один цифровой и/или физический объект; последовательное присвоение сетевого коммуникационного адреса одному или каждому запрашивающему доступ узлу у провайдера доступа к базовой сети; кодирование присвоенного сетевого коммуникационного адреса у провайдера доступа к базовой сети доступа с уникальным параметром узла и уникальным параметром пользователя узла в реестре идентификатора целостности; распределение реестра идентификатора целостности в реальном масштабе времени к каждому узлу, подключенному к сети; прием распределенного реестра идентификатора и его обработка в каждом узле, подключенном к сети, или в одном или более сертифицированных узлах для проверки его целостности, связанной со всеми соответствующими аспектами; идентификация записи в реестре, вызывающей потерю целостности, при определении потери целостности в реестре, и широковещательная

передача оповещения, содержащего идентифицированную запись реестра, к каждому узлу, подключенному к сети, или одному или более сертифицированным узлам; отмена или управление доступом к сети и подключенным к ней узлам и системам для узла, имеющего идентификатор, соответствующий идентифицированной записи в реестре или узлу, который получил коммуникационный адрес, либо при идентификации записи в реестре, вызывающей потерю целостности, либо при приеме оповещения у провайдера доступа к базовой сети. Целостность, относящаяся ко всем соответствующим аспектам, может включать ее последовательность, коэффициент идентичности и целостность процесса. В одном варианте реализации изобретения она может быть контролируемой или любой из других функциональных возможностей в CNAP или другими характерными системными возможностями. В одном варианте реализации изобретения провайдер доступа к базовой сети выполнен с возможностью приема компьютерных программ и информации, содержащей условия, управляющих доступом к различным системам, и интеллектуальные функции в зависимости от эксплуатационных требований и использования этих возможностей CNAP. В одном варианте реализации изобретения распределение реестра идентификатора целостности в реальном масштабе времени к каждому узлу, подключенному к сети, осуществляется с помощью CNAP с сертификацией, группы пользователей/узлов, предварительно настроенных посредством системной спецификации (например, группа банков), или каждым узлом, подключенным к сети. В одном варианте реализации изобретения проверка целостности дополнительно включает возможность немедленно выявлять изменения или нарушения в атрибутах идентификации пользователя (например, идентификатор/IP-адрес/машинный код) и реагировать в соответствии с предварительно настроенной системой узла (такой как блокировка CNAP скомпрометированного пользователя или блокировка доступа к базе данных или ограничение прав доступа пользователя). В одном варианте реализации изобретения могут быть оповещены один или более сертифицированных узлов, если узел идентифицирован как не имеющий целостности.

[0010] Способ по изобретению преимущественно сочетает и объединяет технологию прозрачного распределенного реестра, коммуникационный уровень и идентифицируемые атрибуты, присущие сети связи и подключенным к ней устройствам и системам, для безопасной идентификации и внесения любых изменений в статус, мгновенно обнаруживаемый узлами, являющимися составной частью реестра. Реестром управляют и осуществляют доступ в глобальном масштабе посредством одного или более провайдеров доступа к базовой сети и которым могут полностью или частично управлять с помощью общих платформ, управляемых множеством участников или одной организацией.

[0011] Используя алгоритм изобретения, провайдеры доступа к базовой сети имеют или могут получить полный контроль над узлами в пределах физической и виртуальной сети, а также над ее характеристиками и функциями. Системы и реестры, в которых доступом управляет провайдер доступа к базовой сети, могут быть указаны и применены во всех участвующих сетях по всей глобальной вычислительной сети, такой как Интернет, поскольку предоставляется система контроля доступа к реестру или системе, реализованная каждым провайдером доступа к базовой сети. Каждый провайдер доступа к базовой сети используется в качестве центральной точки аутентификации доступа, поскольку он выполнен с возможностью управления физическими и виртуальными функциями сети и ее использованием, посредством чего, даже несмотря на то, что провайдеры доступа к базовой сети не могут контролировать всю глобальную вычислительную сеть, такую как Интернет, они могут контролировать использование

своих систем. Они также могут контролировать своих пользователей и условия, на которых пользователю может быть предоставлен доступ к сети, системам и реестрам или их частям. Благодаря этому доступ пользователя ко всей глобальной вычислительной сети может контролироваться из CNAP пользователя. Поскольку все больше и больше CNAP согласуются с различными системами, параметрами сетей и реестров, интеграция и использование различных систем распространяются на все большее число пользователей и расширяющуюся географическую область.

[0012] Таким образом, способ по данному изобретению преимущественно устанавливает стандарт в сети в пределах более широкой сети, в которой аутентификация может быть принудительной, а уведомление о компрометировании зашифрованного криптографического ключа установленным для надлежащей отслеживаемости и целостности во всех коммуникационных линиях. Основополагающая сетевая архитектура и возможности основного провайдера доступа к сети, технология доступа к реестрам и системам, а также основные свойства реестра по данному изобретению обуславливают сетевую архитектуру, которая обеспечивает простоту масштабирования и реализации, повышенную гибкость и совместимость между различными системами и реестрами. Реестр и CNAP проверяют целостность последовательности и целостность всех зарегистрированных атрибутов идентификатора (криптологических, физических, цифровых или других атрибутов и т.д.). Это сделает невозможным изменение статуса реестра и идентификатора без того, чтобы это стало очевидным для узлов, имеющих доступ к реестру. Эта коммуникационная линия, связанная с распределением реестра и оповещением о компрометировании идентификатора, может использовать выделенные системы и/или сети с коммутацией каналов, в которых используется шифрование и в которых обеспечивается гарантированная доставка сообщений.

[0013] В варианте реализации способа этап последовательного присвоения сетевого коммуникационного адреса предпочтительно дополнительно включает сопоставление по меньшей мере одного уникального параметра структуры или устройства данных/аппаратного средства и/или по меньшей мере одного уникального параметра пользователя устройства обработки данных с одним или более заданными параметрами доступа. Один или каждый заданный параметр доступа может преимущественно выбираться из группы, включающей: координаты глобальной системы определения место положения (GPS, global positioning system), географические координаты точек сопряжения сети, IP-адреса или номера автономных систем, выданные региональными интернет-регистраторами (RIR, regional internet registries), сеансовые ключи или токены авторизации, предоставленные провайдерами прикладного программного обеспечения (ASP, application service providers).

[0014] Предпочтительно, базовые условия, например, MAC-адрес, IP-адрес и другие статические или полустатические технологические идентификаторы, криптографически выводятся, синтезируются, хэшируются и/или присоединяются к виртуальному идентификатору, так что возможное изменение в физическом сетевом протоколе, адресе сокета, номере порта или другой структуре данных, соответствующей такой релевантной информации, должно быть заметным в реестре. Соответственно, в варианте реализации способа этап кодирования предпочтительно дополнительно включает хэширование кодированного сетевого коммуникационного адреса, уникального параметра узла и уникального параметра пользователя узла, и в котором реестр идентификатора целостности является структурой данных цепочки блоков. В альтернативном варианте реализации способа этап кодирования может вместо этого, или также, включать дополнительный этап преобразования присвоенного сетевого коммуникационного

адреса в цифровую подпись или цифровой ключ. В альтернативном варианте реализации способа хэш-значение криптографически присоединяют к базовому физическому адресу коммуникационной линии и/или другим атрибутам идентификатора, при этом изменение в базовых условиях разрушит хэш-значение и реестр будет оповещен об этом.

[0015] Предпочтительно, провайдер доступа к базовой сети должен быть сертифицирован для работы, и, таким образом, предоставление или предотвращение доступа к сети или ее системам, если это соответствует конкретным технологическим и административным условиям для использования систем, подключенных к сети, применимо как для провайдера доступа к базовой сети, так и для узлов сети. Для разных систем могут потребоваться разные условия для принятия провайдером доступа к базовой сети. Такие условия могут относиться к одной или более отдельным функциям одной или всех возможностей провайдера доступа к базовой сети, доступным для управления его сетью и ее использования ее узлами. Некоторые системы могут потребовать от провайдера доступа к базовой сети использовать все его ресурсы для управления, улучшения или прекращения выполняемых функций и действий в сети.

[0016] Соответственно, вариант реализации способа может включать дополнительный этап сертификации по меньшей мере одного подключенного к сети узла в качестве второго провайдера доступа к базовой сети, в соответствии со списком заданных атрибутов провайдера доступа к базовой сети, выбранных из атрибутов аппаратных средств, атрибутов программного обеспечения, атрибутов связи и набора правил.

[0017] Некоторые системы могут также, или в качестве альтернативы, реализовывать или переносить задачу сертификации на множество уже сертифицированных провайдеров доступа к базовой сети в качестве критерия для голосования, при котором это множество должно проголосовать, чтобы одобрить, и тем самым сертифицировать, нового провайдера доступа к базовой сети. Использование целостности узлов и систем в сети и ее подразделениях эффективно повышается, так как увеличивается количество сертифицированных провайдеров доступа к базовой сети, соответствующих совокупным условиям различных сетевых систем.

[0018] Соответственно, в варианте реализации способа, включающем дополнительный этап сертификации, в сети, содержащей множество провайдеров доступа к базовой сети, этап сертификации подключенного к сети узла в качестве дополнительного провайдера доступа к базовой сети предпочтительно дополнительно включает этап голосования для сертификации узла в каждом из множества провайдеров доступа к базовой сети. В одном варианте реализации изобретения система голосования между несколькими узлами или CNAP включает голосование, при котором новый CNAP должен быть утвержден некоторым количеством или всеми существующими CNAP.

[0019] Вариант реализации способа, включающий дополнительный этап сертификации, может включать дополнительный этап определения географического местоположения каждого провайдера доступа к базовой сети.

[0020] Вариант реализации способа, включающий дополнительный этап сертификации, может включать дополнительный этап, на котором аннулируется сертификация провайдера доступа к базовой сети, когда он не в состоянии поддерживать один или более атрибутов списка заданных атрибутов систем, сетей и реестров провайдера доступа к базовой сети, которым должен соответствовать CNAP. В одном варианте реализации изобретения этот дополнительный этап может включать отмену доступа для CNAP и его узлов/пользователей с помощью автоматического технологического процесса, связанного с компьютерной программой, которая является составной частью реестра или системы и которая работает во всех CNAP, которые сертифицированы для

системы или реестра.

[0021] В соответствии с другим аспектом данного изобретения также предложена система, содержащая: по меньшей мере один стек протоколов, содержащий множество уровней; по меньшей мере одного провайдера доступа к базовой сети, функционально взаимодействующего с каждым уровнем стека протоколов и выполненного с возможностью приема информации в системах, подсетях и реестрах, подключенных к сети, и для управления в реальном масштабе времени доступом узлов к сети и их активностью в сети, причем провайдер доступа к базовой сети содержит по меньшей мере один цифровой и/или физический объект; один или более узлов, подключенных к сети, причем при запросе доступа к сети провайдером доступа к базовой сети одному или каждому из узлов последовательно присваивается сетевой коммуникационный адрес; и реестр идентификатора целостности, содержащий для каждого узла присвоенный сетевой коммуникационный адрес, закодированный в нем с уникальным параметром узла и уникальным параметром пользователя узла, причем реестр идентификатора целостности распределяется к каждому узлу, подключенному к сети, в реальном масштабе времени; причем один или каждый провайдер доступа к базовой сети и каждый узел дополнительно выполнены с возможностью обработки принятого реестра для проверки его целостности, идентификации записи в реестре, вызывающей потерю целостности, широковещательной передачи оповещения, содержащего идентифицированную запись реестра в пределах сети; и причем один или каждый провайдер доступа к базовой сети дополнительно выполнен с возможностью отмены или управления доступом к сети или конкретным системам или другим узлам для узла, потерявшего свою целостность, например, с помощью сетевого коммуникационного адреса, соответствующего идентифицированной записи реестра. В варианте реализации изобретения по меньшей мере один провайдер доступа к базовой сети, взаимодействующий с каждым уровнем стека протоколов, выполнен с возможностью управления в реальном масштабе времени доступом узлов в сеть и управления возможными действиями узлов в сети. В варианте реализации изобретения, если имеется несоответствие с идентификатором нижележащих узлов, в реестр отправляется оповещение. Изменение идентификатора может быть обнаружено с помощью CNAP или непосредственно в реестре.

[0022] В варианте реализации системы один или каждый провайдер доступа к базовой сети может быть дополнительно выполнен с возможностью проверки точности одного или более уникального(ых) параметра(ов) каждого пользователя узла, причем максимальное количество сетевых коммуникационных адресов, присваиваемое одним или каждым провайдером сетевого доступа, в сети равно количеству проверенных в ней идентификаторов.

[0023] В другом варианте реализации системы один или каждый провайдер доступа к базовой сети может быть дополнительно выполнен с возможностью преобразования каждого сетевого коммуникационного адреса, присвоенного узлу, в цифровую подпись или цифровой ключ.

[0024] В любом из вариантов реализации способа и системы, описанных в данной заявке, один или каждый уникальный параметр узла предпочтительно выбирают из группы, включающей: адрес управления доступом к среде (MAC, media access control), код международного идентификатора мобильного оборудования (IMEI, international mobile equipment identity), код идентификатора мобильного оборудования (MEID, mobile equipment identifier), электронный порядковый номер устройства (ESN, electronic serial number), идентификатор Android в виде шестнадцатеричной строки или идентификатор

другого типа, позволяющий аппаратным средствам связываться по сети.

[0025] В любом из вариантов реализации способа и системы, описанных в данной заявке, один или каждый уникальный параметр пользователя узла предпочтительно выбирают из группы, включающей: координаты глобальной системы определения местоположения (GPS), биометрические данные, персональный идентификационный номер (PIN, personal identification number), пароль, серийный номер паспорта, универсальный уникальный идентификатор (UUID, universally unique identifier) или идентификатор любого другого типа, который может идентифицировать пользователя.

[0026] В соответствии с другим аспектом данного изобретения также предложена структура данных, содержащая: по меньшей мере один сетевой коммуникационный адрес, по меньшей мере один уникальный параметр сетевого узла и по меньшей мере один уникальный параметр пользователя сетевого узла, для использования с алгоритмом, описанным в данной заявке, и в сетевой архитектуре, описанной в данной заявке (a) CNAP, (b) его база данных/сервер (300) связи, регистрации и обработки, (c) все возможности CNAP, (d) внешние системы, сети, базы данных, реестры и другие подключенные системы и узлы, (e) реестр идентификации пользователей. Это обеспечивает основу для проектирования систем, сетей и реестров, которые могут быть зарегистрированы и реализованы в CNAP для всех этих компонентов и подключенных систем для работы в соответствии с проектом системы. База данных приема и обработки в CNAP (300), выполненная с возможностью внешней связи, может регистрировать, хранить, обновлять и запускать компьютерные программы, которые взаимодействуют со всеми вышеупомянутыми возможностями и внешними системами и реестрами. Базы данных (300) содержат операционную систему, которая позволяет программам/системам данных использовать все внутренние и внешние возможности. Операционная система содержит конфигурацию связи, регистрацию программы/системы, реализацию и обновление программы/системы, блок обработки информации и интерфейс со всеми возможностями и системами для выполнения (например, состояний доступа и блокировки) зарегистрированной программы/системы. CNAP 300 содержит интеллектуальный концентратор, который может легко развертывать и обновлять системы, выполняющие функции в сетях, системах и реестрах и с помощью различных уровней технических средств. Проект системы/программы (требования и условия) реализуется посредством программы данных в CNAP (300) для использования возможностей CNAP для обеспечения поддержки системы, которая требуется и проектируется, владельцем системы (например, правительствами, компаниями, организациями, физическими лицами, консорциумами и т.д.). Для обеспечения унифицированных технических характеристик и совместимости с программами в сетях, связанных с системами, сетями и реестрами, выполненными с возможностью работы в операционной системе CNAP 300, операционная система и/или программы, работающие на ней, могут быть выполнены полностью или частично с открытым исходным кодом, чтобы все изменения распределялись на все сертифицированные узлы. Модуль CNAP 300 также можно сделать полностью или частично прозрачным, чтобы другие сертифицированные CNAP могли контролировать фактическую работу и связь между различными системами в реальном масштабе времени. Программа также может быть выполнена с возможностью функционирования только по назначению или самоуничтожения при ее взломе. Третья сторона, группа узлов или другая независимая система также могут управлять программой для CNAP. Сертифицированный CNAP и его пользователи должны быть постоянно совместимыми с программой/системой, чтобы иметь доступ. Программа может быть выполнена таким образом, чтобы заранее

спроектированная система применялась автоматически, чтобы ни CNAP, ни пользователи не могли нарушать условия системы без автоматической потери доступа. CNAP регистрирует и применяет системы/программы посредством своих возможностей и интерфейса с внешними блоками для совместимости с различными программами/системами и различными пользователями. Система идентификатора реестра может функционировать так, чтобы CNAP не мог присваивать адреса для связи без регистрации пользователя в реестре. Процесс и все атрибуты, связанные с реестром и его базовой информацией, можно сделать прозрачными для всех сертифицированных узлов. Любое нарушение распространяется на реестр по мере его появления. Узлы с доступом к информации о реестре могут быть регламентированы в системе/программе (например, только сертифицированные CNAP, группы узлов и баз данных, все подключенные узлы, включая всех пользователей). CNAP является контроллером шлюза, промежуточным по отношению к нескольким сетям, системам и реестрам с различным доступом и условиями эксплуатации, обеспечивающим интеллектуальные функции для функций и связи систем, сетей и реестров. Потенциальный проект программ/систем, которые могут быть реализованы в CNAP 300, увеличивается по мере расширения CNAP, его возможностей и подключенных систем. Эти системы взаимодействуют через реестр идентификации и операционную систему CNAP 300. CNAP обеспечивает целостность аутентификации и доступа между системами, сетями, пользователями с обеих сторон. Это позволяет расширить возможности проектирования системы и сети, в которых могут использоваться возможности CNAP. Сети, системы и реестры внутри сети (WAN, within the network) могут быть спроектированы для разных пользователей. Сети, системы и реестры могут взаимодействовать через CNAP, реестр идентификаторов и подключенные извне системы. Таким образом, реестр идентификатора и CNAP обеспечивают платформу для взаимодействия между системами, реестрами, приложениями и подсетями, подключенными к сети. Данное изобретение, таким образом, обеспечивает интерфейс для приема и хранения программ и систем с требованиями и параметрами для использования и доступа в сети и связанных с ней системах, подсетях и реестрах. В соответствии с аспектом данного изобретения, с учетом вышесказанного, предложен реализованный на компьютере способ предоставления каждому узлу сети доступа к сети (и сетевой системе или системам, которые работают в сети или подключены к ней), содержащий следующие этапы: управление доступом к сети на всех уровнях ее стека протоколов по меньшей мере с одним провайдером доступа к базовой сети в масштабе реального времени; последовательное присвоение сетевого коммуникационного адреса одному или каждому запрашивающему доступ узлу у провайдера доступа к базовой сети; кодирование присвоенного сетевого коммуникационного адреса у провайдера доступа к базовой сети с уникальным параметром узла и уникальным параметром пользователя узла в реестре последовательных идентификаторов; распределение реестра последовательных идентификаторов в реальном масштабе времени к каждому узлу, подключенному к сети; прием распределенного реестра идентификаторов и его обработка на каждом подключенном к сети узле для проверки его последовательной целостности; идентификация записи реестра, вызывающей потерю, при определении потери последовательной целостности, и широковещательная передача оповещения, содержащего идентифицированную запись реестра, к каждому узлу, подключенному к сети; и отмена доступа к сети для узла, имеющего сетевой коммуникационный адрес, соответствующий идентифицированной записи в реестре, или узла, которому присвоен IP-адрес, либо при идентификации записи в реестре, вызывающей потерю

последовательной целостности, либо при приеме оповещения у провайдера доступа к базовой сети. В соответствии с другим аспектом данного изобретения также предложена сетевая архитектура, содержащая: по меньшей мере один стек протоколов; по меньшей мере одного провайдера доступа к базовой сети, взаимодействующего с каждым уровнем стека протоколов и выполненного с возможностью управления в реальном масштабе времени доступом узлов к сети; один или более узлов, подключенных к сети, причем при запросе доступа к сети провайдером доступа к базовой сети одному или каждому из узлов последовательно присваивается сетевой коммуникационный адрес; и реестр последовательных идентификаторов, содержащий для каждого узла присвоенный сетевой коммуникационный адрес, закодированный в нем с уникальным параметром узла и уникальным параметром пользователя узла, причем реестр последовательных идентификаторов распределяется к каждому узлу, подключенному к сети, в реальном масштабе времени; причем один или каждый провайдер доступа к базовой сети и каждый узел дополнительно выполнены с возможностью обработки принятого реестра для проверки его последовательной целостности, идентификации записи в реестре, вызывающей потерю последовательной целостности, широковещательной передачи оповещения, содержащего идентифицированную запись реестра в пределах сети; и причем один или каждый провайдер доступа к базовой сети дополнительно выполнен с возможностью отмены доступа к сети для узла, имеющего сетевой коммуникационный адрес, соответствующий идентифицированной записи реестра.

[0027] Другие аспекты данного изобретения указаны в прилагаемой формуле изобретения.

КРАТКОЕ ОПИСАНИЕ ГРАФИЧЕСКИХ МАТЕРИАЛОВ

[0028] Изобретение будет легче понять из следующего описания его варианта реализации, приведенного исключительно в качестве примера, со ссылкой на прилагаемые чертежи, на которых.

[0029] На фиг. 1 проиллюстрировано логическое представление сетевой архитектуры в соответствии с вариантом реализации изобретения, содержащей множество узлов, подключенных к провайдеру доступа к базовой сети.

[0030] На фиг. 2 проиллюстрировано логическое представление сети, проиллюстрированной на фиг.1, развернутой в глобальной вычислительной сети.

[0031] На фиг. 3 проиллюстрировано общее представление приведенных в качестве примера возможностей провайдера доступа к базовой сети, реализованных в стеке протоколов сети, проиллюстрированной на фиг. 1 и 2, применительно к каждому запрашивающему доступ узлу.

[0032] На фиг. 4 проиллюстрирован пример реестра идентификатора целостности в соответствии с изобретением, поддерживаемого провайдером доступа к базовой сети и узлами, подключенными к сети, в сети, проиллюстрированной на фиг. 1-3.

[0033] На фиг. 5 проиллюстрировано масштабирование архитектуры сети и ее реестра идентификатора целостности для множества провайдеров доступа к базовой сети и его интерфейса с другими системами, сетями, реестрами и приложениями.

[0034] На фиг. 6 проиллюстрирована блок-схема варианта реализации алгоритма, реализующего сетевую архитектуру изобретения, выполненную у провайдера доступа к базовой сети.

[0035] На фиг. 7 проиллюстрирована блок-схема варианта реализации алгоритма, реализующего сетевую архитектуру изобретения, выполненную на каждом узле в сети.

[0036] На фиг. 8 проиллюстрирована блок-схема двух альтернативных вариантов реализации алгоритма, реализующего сетевую архитектуру изобретения, выполненную

в сети у множества провайдеров доступа к базовой сети.

[0037] На фиг. 9 проиллюстрирован первый алгоритм определения географического местоположения для каждого из множества провайдеров доступа к базовой сети.

[0038] На фиг. 10 проиллюстрирован второй алгоритм определения географического местоположения для каждого из множества провайдеров доступа к базовой сети.

ПОДРОБНОЕ ОПИСАНИЕ ГРАФИЧЕСКИХ МАТЕРИАЛОВ

[0039] В последующем описании в целях пояснения изложены конкретные подробности для облегчения понимания сущности изобретения. Для специалиста в данной области техники будет несложно понять, что принципы изобретения, описанные в данной заявке, могут быть применены на практике без включения этих конкретных подробностей, и что варианты реализации данного изобретения могут быть по-разному реализованы как процесс, установка, система, устройство или способ на материальном машиночитаемом носителе.

[0040] Компоненты и/или модули, показанные на схемах, иллюстрируют приведенные в качестве примера варианты реализации изобретения, а также показаны и описаны для облегчения понимания принципов изобретения, описанных в данной заявке. Для специалиста в данной области техники будет несложно понять, что такие компоненты и/или модули могут быть реализованы в виде отдельных компонентов или интегрированы в меньшей или большей степени, в том числе в пределах одной системы или компонента; такие компоненты и/или модули могут быть реализованы в виде программного обеспечения, аппаратного средства или их комбинации; и что функции или операции, описанные в данной заявке, могут быть реализованы в виде компонентов.

[0041] Ссылки в описании на соединения между компонентами, модулями, системами или устройствами на чертежах не предназначены для ограничения прямыми соединениями, но могут распространяться на непрямые соединения через одно или более промежуточных устройств, беспроводных соединений, при этом могут использоваться большее или меньшее количество соединений. Ссылки в описании на сообщения, блоки и данные относятся к группе битов, предназначенных для передачи по сети. Данные термины не должны интерпретироваться как ограничивающие варианты реализации данного изобретения какой-либо конкретной конфигурацией и могут взаимозаменяемо использоваться или заменяться такими терминами, как трафик данных, информация и любыми другими терминами, относящимися к группе битов. Ссылки в описании на вариант реализации изобретения означают, что конкретный признак, структура, характеристика или функция, описанные в связи с этим вариантом реализации изобретения, могут быть представлены более чем в одном варианте реализации изобретения.

[0042] Ссылки в описании на «пользователей» могут означать людей, организации, предприятия, группы, домашние хозяйства, системы, реестры, приложения, базы данных, серверы, сетевые устройства и другие идентифицируемые вещи или группы со средствами связи по сети связи. Ссылки в описании на «цепочку блоков» могут означать запись определенного количества цифровых активов, цифровых подписей, идентификаторов и передач между идентификаторами, которые зарегистрированы и хэшированы в непрерывную цепочку блоков, которая публикуется для всех участвующих идентификаторов, более того, в которой удвоение потребления вычислительных ресурсов предотвращаются путем проверки последовательности транзакций с помощью вычислительной мощности большинства компьютеров в сети, посредством которой проверяют самую длинную цепочку транзакций. Ссылки в описании на «распределенный реестр» могут означать реестр пользователей и цифровых активов, опубликованный

для всех участвующих узлов. Ссылки в описании на «воздушный зазор» могут означать физический, виртуальный, математический или криптографический или определяемый системой барьер, который не может быть преодолен путем подключения к сети связи для передачи электронных данных.

[0043] Ссылки в описании на «провайдера доступа к базовой сети» (в данной заявке «CNAP») могут означать по меньшей мере один цифровой и/или физический объект, обеспечивающий доступ к сети для новых узлов и их пользователей и контролирующий поддержание этого доступа к подключенным узлам посредством возможностей, способных повлиять на функциональные возможности сети для подключенного узла. Ссылки в описании на «возможности» CNAP распространяются по меньшей мере на доступ, учет, биллинг, аутентификацию, управление, контроль физической инфраструктуры и кабелей, канальный уровень, IP-уровень, сохранение и осуществление заранее заданных путей обмена данными посредством физических кабелей, схемы IP-маршрутизации, управление канальным уровнем, наблюдение, углубленная проверка пакетов, блокировка систем доменных имен, аналитические инструменты потоков данных и поведения, дешифрование и любые другие функциональные возможности, способные повлиять на возможности и функциональные возможности сети или ее частей.

[0044] Со ссылкой на графические материалы и первоначально на фиг. 1 и 2, проиллюстрировано логическое представление сетевой архитектуры в соответствии с вариантом реализации изобретения, содержащей множество узлов, подключенных к провайдеру 101 доступа к базовой сети (CNAP).

[0045] На фиг. 1 с точки зрения функциональности проиллюстрирована функция сетевого управления CNAP 101 для множества узлов, требующих доступа, которые по-разному представлены в виде планшетного компьютера 110, настольного компьютера 112, смартфона 114, сети 116, первого сервера 118_1 и первой базы 120_1 данных, хранящейся на дополнительном терминале 118_N с левой стороны, чтобы предоставить доступ к различным удаленным системам и реестрам, по-разному представленным с правой стороны как подключенное приложение 140, второй сервер 118_2, вторая база данных 120_2 хранящаяся на втором сервере 118_2 и включая реестр 150 идентификаторов.

[0046] На фиг. 2 проиллюстрирована та же сеть, что и на фиг. 1, развернутая как части более широкой глобальной вычислительной сети, например, Интернет 105, и, соответственно, подключенная к ней с помощью различных сетевых протоколов, в которой возможность сетевого соединения и совместимые сетевые протоколы каждого терминала позволяют терминалам соединяться друг с другом и передавать данные друг другу и принимать данные друг от друга в соответствии с алгоритмом, описанным в данной заявке.

[0047] В WAN 105 сетевая архитектура может содержать любое количество подсетей 132, функционально связанных с CNAP 101. В сетевой архитектуре CNAP 101 выполнен с возможностью аутентификации каждого запрашивающего доступ узла 110, 112, 114, 118_N, подключенного к базовой сети, причем каждый из CNAP 101 и каждый аутентифицированный узел 110, 112, 114, 118_N, которому предоставлен доступ, адаптируется для контроля постоянного аутентифицированного состояния каждого подключенного узла.

[0048] Тип терминала 110 обработки данных в сетевой архитектуре может быть терминалом мобильного персонального компьютера, которым управляет пользователь, которым в данном примере является планшетный компьютер 110. Планшетный

компьютер 110 передает и принимает данные, закодированные в виде цифрового сигнала, посредством беспроводной линии 133 передачи данных, соответствующей стандарту IEEE 802.11 («Wi-Fi™»), причем сигнал передается соответственно на планшетный компьютер или с него посредством устройства 131 локального маршрутизатора, которое обеспечивает взаимодействие планшетного компьютера 110 с сетью 105 связи WAN. Планшетный компьютер 110 дополнительно содержит сетевой интерфейс радиочастотной идентификации (RFID, Radio Frequency Identification), реализующий протоколы взаимодействия и обмена данными ближнего радиуса действия (NFC, Near Field Communication), для упрощения беспроводной передачи данных на короткое расстояние с соответствующими устройствами, такими как мобильный телефон 110 и/или устройство пользователя с поддержкой NFC, например, электронная платежная карта. Планшетным компьютером 110 может быть, например, iPad™, изготовленный Apple, Inc., Куппертино, Калифорния, США, или Surface™, производства Microsoft, Inc., Редмонд, Вашингтон, США.

[0049] Другим типом терминала 114 обработки данных в сетевой архитектуре может быть мобильное персональное устройство связи, которым управляет тот же пользователь мобильного персонального устройства 110 связи, или, в качестве альтернативного варианта, другим, которым управляет пользователь. Терминал 114 передает и принимает данные, включая голосовые и/или буквенно-цифровые данные, закодированные в виде цифрового сигнала, посредством беспроводной линии 137 передачи данных, причем сигнал ретранслируется соответственно на устройство 114 или от него с помощью ближайшего географически расположенного ретранслятора 138 линии радиосвязи из их множества. Множество ретрансляторов 138_N линии радиосвязи позволяют направлять цифровые сигналы между мобильными устройствами, такими как пользовательский терминал 114, и их предполагаемым получателем посредством удаленного шлюза 139. Шлюз 139 является, например, коммутатором сети связи, который связывает трафик цифрового сигнала между беспроводными телекоммуникационными сетями, такими как сеть, в которой присутствуют беспроводные линии 137 передачи данных, и WAN 105. Шлюз 139 дополнительно обеспечивает преобразование протокола, если требуется, например, если терминал 114 для передачи данных использует прикладной протокол беспроводной связи («WAP, Wireless Application Protocol») или защищенный протокол передачи гипертекста («HTTPS, Secure Hypertext Transfer Protocol»).

[0050] Другими видами терминалов обработки данных в сетевой архитектуре могут быть настольные персональные устройства 112 связи и серверы 118N, используемые соответствующими пользователями для личных или административных целей. Все такие терминалы передают и принимают данные, включая голосовые и/или буквенно-цифровые данные, закодированные в виде цифровых сигналов по проводным (132) или беспроводным (137) линиям передачи данных, причем сигналы ретранслируются соответственно на или из каждого терминала посредством устройства 131 локального маршрутизатора, которое обеспечивает взаимодействие компьютера 112, 118N с сетью 105 связи WAN.

[001] Еще одним типом терминалов обработки данных в сетевой архитектуре могут быть подключаемые к сети специализированные устройства, обычно называемые «вещами», включающие различные бытовые приборы и интерфейсы домашней автоматики, для применения в домашних условиях, камеры наблюдения и интерфейсы управления доступом к местоположению, интерфейсы промышленной автоматизации и многое другое. В зависимости как от их назначения, так и от конфигурации и

совместимости сетевых протоколов, такое устройство может быть подключено к сети посредством проводного или беспроводного соединения с глобальной вычислительной сетью 105 или с локальной вычислительной сетью 116N, взаимодействующей с глобальной вычислительной сетью 105, в любом случае с помощью CNAP 101.

[0051] Базовая сеть обслуживается посредством CNAP 101, который в данном примере реализован на компьютерном терминале, например, на сервере 118_N. CNAP передает и принимает данные, закодированные в виде цифрового сигнала, по проводной линии 130 передачи данных, причем указанный сигнал ретранслируется соответственно на сервер или с сервера посредством устройства 131 локального маршрутизатора, реализующего проводную локальную сеть, работающую в соответствии с протоколом передачи данных Gigabit Ethernet IEEE 802.3-2008. Маршрутизатор 131 сам подключен к WAN 105 посредством обычного оптоволоконного соединения по проводной телекоммуникационной сети 132.

[0052] На фиг. 3 проиллюстрирован обзор примерных возможностей провайдера 101 доступа к базовой сети, приемника и хранилища компьютерных программ для проектирования сетей и систем в сети или подключенных к ней, реализуемых в пределах стека 301 протоколов сети, показанной на фиг. 1 и 2, применительно к каждому запрашивающему доступ узлу 11ON, 114N, 116N, 118N, 140N. Основополагающим аспектом данного изобретения, который является неотъемлемой частью сетевой архитектуры, является протокол идентификации и распределенный реестр 150, а также CNAP, который выполнен с возможностью осуществления контроля и управления сетью. Таким образом, CNAP можно рассматривать как контроллер шлюза доступа к системе и реестру. Данное изобретение также относится к проектированию систем, в которых используются его возможности для воздействия на сеть и ее использование, и, таким образом, для обеспечения возможности проектирования систем и реестров, которые управляются CNAP. Это обеспечивается путем объединения определенного распределенного реестра 150, описанного в данной заявке, с сетевым протоколом 301 глобальной вычислительной сети на основе коммуникационных адресов/адресов сокетов, таких как, например, в контексте TCP/IP, и использованием CNAP 101, который обеспечивает доступ к сети связи посредством аппаратных средств и программного обеспечения в качестве опорного узла, который предоставляет и защищает доступ к реестрам и системам, развернутых на них, в соответствии с заранее заданным проектом различных систем.

[0053] CNAP 300 выполнен с возможностью внешней связи для приема и взаимодействия с программами и реестрами данных. Он выполнен с возможностью регистрации и реализации программ и операционных систем, которые взаимодействуют по меньшей мере с системой доступа и одной или более функциональными возможностями сети. CNAP 101 должен соответствующим образом функционально взаимодействовать с каждым уровнем стека 301 сетевых протоколов: базовым уровнем 302 физической «аппаратной» инфраструктуры, канальным уровнем 303 взаимодействия контента цифровой сигнализации с базовым слоем 302, уровнем 304 интернет протокола «IP», определяющим формат данных передаваемых через сеть (Интернет), транспортным уровнем 305 (протокол управления передачей (TCP, Transmission Control Protocol), обеспечивающим службы связи между хостами для приложений 140, и уровнем 306 приложений, обеспечивающим коммуникационные линии «процесс-процесс» служб связи для приложений 140. Данный стек сетевых протоколов и уровневая структура описаны в качестве примера, и в изобретении могут использоваться другие схемы сети.

[0054] Также CNAP 101 должен соответственно содержать один или более из

следующих атрибутов и их соответствующих функциональных возможностей, реализующих возможности управления сетью: модуль 311 управления доступом для обработки и предоставления или отклонения запросов доступа к сети удаленных узлов и управления их доступом после предоставления доступа; модуль 312 управления IP-адресами для управления пулом сетевых адресов и назначения сетевого адреса любому запрашивающему доступ узлу, прошедшему проверку подлинности, при опросе модулем 311 управления доступом; модуль 313 аутентификации для управления регистрацией уникальных параметров U_{PARAM} узлов и пользователей и для проверки параметров доступа любого запрашивающего доступ узла при опросе модулем 311 управления доступом; модуль 314 системы доменных имен, связанный с модулем 319 отслеживания и поиска для определения местоположения и идентификации узлов в базовой сети на основе присвоенных им сетевых адресов, и управляемый модулем 311 управления доступом для управления и, в зависимости от обстоятельств, блокировки связи с узлами; необязательный модуль 315 учета для управления подписками и обработки электронных платежей зарегистрированными пользователями; модуль 316 контроля трафика, связанный с модулем 317 углубленной проверки пакетов, для обнаружения контента сетевых соединений и, в частности, идентификации вредоносных программ, вирусов, спама или аналогичной вредоносной сетевой активности; модуль 318 проектирования и управления сетью для контроля и обновления или иного изменения подлежащих проверке атрибутов провайдера доступа к базовой сети, включающих заданный набор атрибутов аппаратных средств, атрибутов программного обеспечения, атрибутов связи и один или более наборов правил, ориентированных на условие обслуживания (CoS, Condition of Service), совместно реализующих условия для получения доступа к базовой сети и зарегистрированным системам в CNAP 300, таким как реестр идентификатора или специально спроектированная сеть или база данных доступа; и необязательный модуль 320 анализа и управления сетью для контроля и обновления или иного изменения атрибутов базовой сети, включающих заданный набор атрибутов аппаратных средств, атрибутов программного обеспечения, атрибутов связи и один или более ориентированных на качество обслуживания (QoS, Quality of Service) набор правил, совместно определяющих оптимальную полосу пропускания и ее использование в базовой сети.

[0055] Каждый доступ и использование систем в базовой сети должно всегда соответствовать заранее установленным критериям: CNAP 101 может использовать все свои возможные инструментальные программные средства 311-320, чтобы маркировать, отслеживать, блокировать и делать что-либо еще с пользовательским терминалом, сетевым соединением, подключенной базой данных или другой сетевой активностью. Базовая сеть и/или реестр 150 идентификаторов (или любая другая система, для которой CNAP сертифицирован для предоставления доступа) могут быть спроектированы с любыми подходящими условиями доступа для организаций и пользователей любого типа, которые разработчик системы сочтет подходящими. Например, работать вместе с CNAP 101 и предоставлять доступ пользователю через CNAP 101 может третья сторона, например, банк, предоставляющий клиенту доступ к реестру платежей.

[0056] CNAP 101 может препятствовать пользователю в получении доступа к открытой сети, требуя аутентификации и/или соответствия определенным заранее заданным сетевым, реестровым или системным политикам и условиям, реализованным модулями CNAP 311-320, в соответствии с условиями распределенной системы или реестра, условиями конкретной сетевой системы или реестра, который выполнен в виде

программы данных или операционной системы, связанной с и установленной в CNAP (300). Например, регулятивный орган или правительство может принять решение запретить пользователям доступ к неконтролируемым и анонимным финансовым реестрам цепочек блоков (криптографическая валюта на основе цепочки блоков), которые могут использоваться для финансирования терроризма, наркотиков, торговли людьми или другой незаконной деятельности, при этом модуль 318 проектирования и управления сетью определяет такие неконтролируемые и анонимные финансовые реестры цепочек данных в соответствующем наборе правил блокировки, выполняемом любым из них, или комбинацию возможностей изменения сети (таких как, например, аппаратное средство сети с коммутацией каналов, модуль мониторинга трафика совместно с DPI, блокировка конкретных систем, источников, каналов и коммуникационных линий, разрешение для связи только в соответствии с белым списком (положительно определенных)), при этом модуль 316 контроля трафика совместно с модулем 317 углубленной проверки пакетов проверяет активность узлов для выявления пакетов данных, соответствующих заблокированным реестрам цепочек данных.

[0057] На фиг. 4 проиллюстрирован пример реестра идентификатора целостности в соответствии с изобретением, обслуживаемого модулями 311-320 провайдера доступа к базовой сети совместно с подключенными к сети узлами 110_N, 114_N, 116_N, 118_N, 140_N в сети, проиллюстрированной на фиг. 1-3.

[0058] Реестр 150 идентификаторов целостности является распределенным реестром, используемым каждым подключенным к сети узлом 110_N, 114_N, 116_N, 118_N, 140_N в сети, как единым цифровым идентификатором, который может быть использован во всех средах обработки данных, доступных посредством базовой сети, где требуется идентификация для пользователя узла, примеры которых включают, например, права доступа к базе данных, процедуры электронных платежей, процедуры электронного голосования, электронное подписание контракта и защиту узлов.

[0059] В конкретном примере, проиллюстрированном на фиг. 4, узел 140 приложения, подключенного к сети, является, например, заявлением на получение туристической визы правительственного учреждения, требующей идентификации пользователя любого подключенного пользовательского устройства 110_N, 114_N, 116_N, 118_N, подающего заявление на визу в электронном виде. Идентификация может отображаться для тщательного рассмотрения заявлений пользователей, аутентификация которых осуществляется посредством реестра идентификатора целостности 150. Целостность компонентов, последовательности и обработки уникальных записей 401_N реестра должны быть проверены, чтобы быть подтвержденными, и каждая из них должна быть закодирована в виде открытого ключа на основе базового физического IP-адреса в CNAP 101 путем получения цифровой подписи или криптографического числа для каждого адреса базовой сети или другого идентификатора, присвоенного узлу.

[0060] В соответствии с алгоритмом, описанным в данной заявке, кодирование уникальных параметров U_{PARAM} каждого сетевого узла 110_N, 114_N, 116_N, 118_N, 140_N в качестве соответствующей узлу записи реестра, или записи 401_N в реестре 150 идентификаторов посредством CNAP 101, последовательно с записями, которые соответствуют непосредственно предыдущему узлу 110_{N-1}, 114_{N-1}, 116_{N-1}, 118_{N-1}, 140_{N-1} для получения доступа к базовой сети, зарегистрированными как собственная уникальная запись реестра или запись 401_{N-1} предыдущего узла, является неотъемлемой частью процедуры предоставления доступа к базовой сети, выполняемой CNAP 101.

Базовое условие, например, MAC, IP адреса и/или другой технологический идентификатор узла криптографически выводится, синтезируется, хэшируется и/или присоединяется к идентификатору, так что возможное изменение в физическом сетевом протоколе, адресе сокета, номере порта или другой базовой информации узла будет видимым в реестре 150 идентификаторов. В альтернативном варианте реализации изобретения возможности CNAP могут обнаруживать любые изменения в базовой физической среде, которые не соответствуют реестру, и оповещать реестр и связанные с ним CNAP, а также осуществлять соответствующие действия в собственных системах. Данный процесс и действия могут выполняться автоматически при обнаружении нарушения.

[0061] Идентификатор и его коммуникационный адрес не должны изменяться, поэтому существует ограниченное число транзакций для записи в реестре 150 идентификаторов и соответственно ограниченная возможность сигнализации в сети, связанная с распределением реестра 150 идентификаторов. Изменения происходят, когда новые идентификаторы регистрируются с новыми коммуникационными адресами, когда коммуникационный адрес меняет идентификатор, когда пользователь нарушает базовые физические характеристики, которые приводят к нарушению идентификатора (например, выход из системы или взлом другим объектом), когда узел пересекает границу сети что приводит к изменению CNAP, предоставляющего доступ, и сетевого адреса, или если пользователь меняет свой CNAP и получает новый IP, или если адреса изменяются (например, проксируются), чтобы скрыть идентификацию и/или местоположение отдельных лиц или организаций, или когда идентификация взломана, а IP-адрес получен неавторизованным пользователем.

[0062] Для вариантов реализации реестра 150 идентификаторов, основанного на технологии цепочки блоков, также проиллюстрированной на фиг.4, с добавлением хэш-значения 402_N закодированных уникальных параметров U_{PARAM} каждого узла, существует также ограниченное потребление ресурсов на обработку, связанное с доказательством выполнения работы проверки цепочки блоков из-за конечного числа адресов базовой сети, присваиваемых CNAP 101, которое в одном из высших значений равно точному количеству идентификаторов в реестре 150 (идентификатор может иметь множество IP-адресов). Кроме того, поскольку фактическое изменение идентификатора или IP-адреса относится к CNAP или другим узлам, присоединенным к реестру, доказательство выполнения работы не так уж важно для функции немедленного нарушения ключа, поскольку цель состоит в том, чтобы обнаружить «любые расходы», а не просто «удвоенные расходы».

[0063] Поскольку присвоенный сетевой адрес и идентификационные данные приводятся в соответствие с системой во время записи в реестр 150 идентификаторов посредством CNAP 101, целостность реестра является необратимой, из-за того, что является распределенной; данные, полученные из базовых физических факторов, хэшируются в цепочке и поэтому не могут быть скомпрометированы, без того, чтобы это не стало очевидным для всех узлов, присоединенных к реестру. Все узлы и блоки обработки в базовой сети могут обрабатывать доказательство выполнения работы независимо от других и не нуждаются в консенсусе, потому что любое изменение или изменение в кодированном идентификаторе пользователя или в кодированном физическом факторе узла (например, MAC, IMEI), неизменно уничтожает ключ записи реестра, например, если коммуникационный адрес смещается, если базовое физическое значение коммуникационного адреса, машинного адреса или другого идентификатора становится неточным по сравнению с хэшированным с информацией, заблокированной

посредством CNAP 101, в распределенном реестре 150. Теми, у кого есть доступ к реестру, могут быть только сертифицированные CNAP, или также все подключенные узлы, или подключенные базы данных доступа и другие системы, которые должны быть немедленно оповещены о потенциальном компрометировании ключа. Следует отметить, что нет необходимости рассчитывать на самую длинную цепочку доказательства выполнения работы. Прежде всего, CNAP или другие подключенные узлы должны иметь возможность получать информацию о любом нарушении и автоматически реагировать в соответствии с заранее установленными действиями, которые необходимо предпринять при нарушении ключа (например, запретить доступ для пользователя в базу данных доступа, разорвать сетевое соединение для идентификатора и IP-адреса в сети и т.д.).

[0064] Эти аспекты данного изобретения способствуют улучшению масштабируемости архитектуры базовой сети и обеспечивают оптимальный баланс между конфиденциальностью и отслеживаемостью.

[0065] В реестрах цепочек блоков транзакции имеют временную метку и хэшируются в блок, который проверен на точность информации. Требование к доказательству выполнения работы не может быть изменено, если оно не изменено во всех последующих блоках с меткой времени после и на всех подключенных узлах, которые имеют копию цепочки блоков. Для предотвращения двойных расходов и удовлетворения потребностей доверенных третьих сторон последовательность транзакций проверяется совокупной и наилучшей вычислительной мощностью компьютеров сети, способной создать наиболее длинную цепочку, что принимается в качестве доказательства выполнения работы, когда пользователь возвращается в сеть. Если недружелюбные субъекты управляют большей частью вычислительной мощности сети и способны как изменить доказательство выполнения работы, так и достичь и превзойти допустимую вычислительную мощность сети, в таком случае цепочка, ее последовательность и зарегистрированные значения могут оказаться некорректными.

[0066] С помощью реестра 150 идентификаторов в соответствии с данным изобретением подключенные сетевые узлы могут постоянно осуществлять наблюдение за всеми действиями по доступу и записи в реестр и, таким образом, нет никакой необходимости возвращаться к цепочке. Несомненно, вариант реализации изобретения учитывает альтернативу отсутствию блока, но только последовательность событий, которая содержит непрерывные метки времени и регистрируется в реестре. Более того, двойные расходы и точная последовательность транзакций коммуникационного адреса между пользователями также не являются критическими, поскольку первое изменение в записи 401 представляет наибольший интерес для подключенных узлов. В связи с этим следует понимать, что все изменения могут иметь отношение к контролю над пользователями и идентификаторами, но важнейшей частью защиты базы данных или сети является незамедлительная реакция на первое изменение.

[0067] Таким образом, данный подход реализует уникальную идентичность и повторяющуюся трассируемость и отслеживаемость для каждого подключенного к сети узла по всей базовой сети, причем любые изменения в такой уникальной записи реестра или записи 401_N с течением времени в процессе сетевого сеанса узла непосредственно противоречат целостности реестра при обновлении посредством CNAP, сразу же обнаруживаются с помощью встроенной проверки целостности реестра 150 и автоматически приводят к тому, что CNAP 101 завершает сетевой сеанс и/или блокирует трафик для узла, связанного с измененной записью 401 реестра, или даже другими действиями такими как, например, наблюдение за IP-адресом или

идентификацией в сети с помощью соответствующего CNAP, или другая активность от подключенного узла (например, аналогично прекращению доступа для пользователя к базе данных доступа).

[0068] На фиг. 5 проиллюстрировано, как сетевая архитектура и реестр 150 идентификаторов целостности соответственно масштабируется по множеству провайдеров доступа к базовой сети 101_{1-6}, причем приложения 140_{1-N}, распределенные реестры 500_{1-N}, распределенные системы 118_{1-N}, подсети 116_{1-N} могут все использовать реестр 150 идентификаторов и сеть соединенных CNAP 101_{1-6} в качестве посредника для взаимодействия множества систем и узлов.

[0069] В варианте реализации изобретения, проиллюстрированном на фиг. 5, множество CNAP 101_{1-6} функционирует как унифицированный контроллер шлюза для управления доступом от пользователей и вещей 110-112-114, систем 116-118, баз данных 120, приложений 140 и других подключенных реестров 500 в качестве узлов, для других аналогичных пользователей и вещей 110-112-114, систем 116-118, баз данных 120, приложений 140, а также других подключенных реестров 500.

[0070] Каждый CNAP индивидуально контролирует доступ к базовой сети для своих зарегистрированных пользователей и их соответствующих узлов и записывает свои соответствующие разрешения на доступ к сети в реестр 150 идентификаторов. Права доступа, присоединенные к пользователю с помощью CNAP 101_1, могут следовать за пользователем по отдельным областям и узлам базовой сети, будучи прозрачными для других CNAP 101_{2-6} посредством кодирования в общем реестре 150 идентификаторов, но при этом доступ к базовой сети для любого аналогично может быть прекращен любым CNAP 101_{1-6}.

[0071] Некоторые реестры на основе блоков цепочек или другие распределенные реестры 500, системы 118, приложения 140 и отдельные области 116 сети могут быть сделаны недоступными с помощью каждого или всех CNAP 101_{1-6} посредством соответствующих зарегистрированных наборов правил, реализованных и проверенных в CNAP 300 и обработанных их соответствующими модулями 301-320, в то же время, поддерживая их общую задачу принудительной идентификации и записи в реестре 150 идентификаторов целостности для предоставления и поддержки прав доступа к сети или прав для других систем, которые зарегистрированы и реализованы в CNAP 300.

[0072] На фиг. 6 проиллюстрирована блок-схема варианта реализации алгоритма, реализующего сетевую архитектуру изобретения, выполненную у провайдера доступа к базовой сети.

[0073] На этапе 601 CNAP 101 определяет, ожидается ли запрос доступа к сети от удаленного узла, например, 110, который кодирует множество данных узла, включая по меньшей мере один параметр U_{PARAM}, представляющий уникальный идентификатор устройства, например MAC-адрес или IMEI код. В случае утвердительного ответа на этапе 602 CNAP 101 обрабатывает запрос доступа к сети, чтобы декодировать его, и затем сравнивает уникальный параметр U_{PARAM} с сохраненными уникальными параметрами U_{PARAM} узлов, зарегистрированных в CNPA 101.

[0074] На этапе 603 CNAP 101 рассматривает, было ли получено совпадение в результате сравнения. В случае отрицательного ответа на этапе 604 CNAP 101 обрабатывает запрос доступа к сети как первый запрос незарегистрированного узла и переходит к регистрации запрашивающего узла для хранения как его уникального параметра U_{PARAM} так и уникального параметра пользователя U_{PARAM}, чтобы связать

его с ним. Этап 604 предпочтительно включает процедуру регистрации, требующую, чтобы пользователь запрашивающего узла 110 представил подтверждение идентификации, которое, или его часть, ссылка или аспект, может быть затем записано как уникальный параметр пользователя U_{PARAM}.

[0075] После этого, или в качестве альтернативы, когда совпадение было подтверждено на этапе 603, который идентифицирует запрашивающий узел 110 как зарегистрированный узел, CNPA 101 назначает следующий доступный сетевой адрес в конечном пуле присваиваемых адресов базовой сети запрашивающему узлу 110 на этапе 605. На этапе 606 CNAP 101 кодирует коммуникационный адрес, соответственно назначенный узлу 110, и его соответствующие параметры аутентификации, включая его зарегистрированный уникальный параметр U_{PARAM} и зарегистрированный уникальный параметр пользователя U_{PARAM} в реестре 150 идентификаторов, в качестве последовательной следующей записи в нем. Затем после регистрации CNAP 101 автоматически осуществляет широковещательную передачу реестра 150 идентификаторов, содержащего обновленную запись, ко всем узлам 110_N, 114_N, 116_N, 118_N, 140_N, подключенным к базовой сети, включая любые другие также подключенные к нему CNAP 101_N. После этого управление возвращается к вопросу на этапе 601, чтобы обработать следующий запрос доступа следующего узла 110_N, 114_N, 116_N, 118_N. Следует отметить, что реестр может распределяться ко всем пользователям, но необязательно. Он может распределяться только к сертифицированным CNAP. Он также может распределяться к другим подключенным системам и базам данных, которым необходимо иметь информацию о целостности идентификатора в реальном масштабе времени. Важно, чтобы различные реестры и системы могли проектировать разрешенный доступ к своим системам. Они могут задавать условия для пользователей, а также задавать условия для тех, кто получит доступ к информации из реестра (например, CNAP может иметь возможность предоставить разрешенный доступ своим пользователям на определенных условиях, установленных системой посредством реализованной в CNAP 300 программы данных, и система также может иметь разрешенный доступ к информации реестра).

[0076] Параллельно с функциональной возможностью управления доступом к сети и присущей ей аутентификацией узла, описанной со ссылкой на этапы 601-607, в качестве самого узла базовой сети, CNAP 101 также проверяет целостность реестра 150 идентификаторов, чтобы идентифицировать недопустимые записи реестра, соответствующие узлам с параметрами аутентификации, ставшими недействительными с момента кодирования на этапе 606, и, в качестве узла контроллера шлюза базовой сети, чтобы обеспечить целостность путем отмены доступа к сети для любого идентифицированного указанным образом узла.

[0077] Соответственно, второй поток обработки CNAP 101 работает одновременно с функциональными возможностями управления доступом к сети на этапах 601-607, причем на этапе 608 выполняется проверка, было ли получено оповещение от удаленного узла, содержащего недопустимую запись в реестре. Если ответ отрицательный, то на этапе 609 CNAP 101 осуществляет проверку целостности реестра идентификаторов, например, путем обработки кодированной записи реестра с помощью известного алгоритма доказательства выполнения работы. Преимущественно, из-за конечного числа присваиваемых адресов базовой сети потребление ресурсов для обработки, связанное с этапом 609, остается относительно небольшим по сравнению с реестрами целостности, независимо от типа цепочки блоков или иного, количество

записей для которых не ограничено или ограничено и, как известно, существенно нетривиально возрастает численно, например, в конкретной области валютных транзакций. Затем на этапе 610 выполняется проверка, появилась ли на этапе проверки недопустимая запись реестра. Если ответ отрицательный, тогда управление возвращается к этапу 608, причем поток проверки продолжает непрерывно проверять целостность реестра 150 идентификаторов до тех пор, пока не будет получено удаленное оповещение. Следует понимать, что отправляемое оповещение о любом изменении и CNAP имеет заранее заданные и автоматические действия в отношении информации, основанной на том, к какому пользователю она относится и какой системе соответствует этот пользователь (эти действия и процедуры зарегистрированы и реализованы в CNAP 300).

[0078] Если было принято удаленное оповещение и ответ на вопрос на этапе 608 является положительным или, альтернативно, если CNAP 101 локально идентифицировал недопустимую запись реестра на этапе 609 и ответ на вопрос на этапе 610 является положительным, то на этапе 611 CNAP 101 идентифицирует узел 110_N, 114_N, 116_N, 118_N, 140_N, соответствующий недопустимой записи реестра и сопоставляет ее с адресом базовой сети, который последний раз присваивался этому узлу. Если оповещение получено вследствие нарушения ключа и изменения в реестре (которое может быть вызвано физическим изменением базового состояния), CNAP может быть запрограммирован на немедленное принятие соответствующих действий, связанных с идентификаторами и адресами, связанными с изменением в реестре. CNAP 101 может, например, извлекать и декодировать кодированный адрес базовой сети, сопоставлять декодированный адрес базовой сети с зарегистрированным уникальным параметром U_{PARAM} узла и уникальным параметром пользователя U_{PARAM} и сравнивать зарегистрированные параметры аутентификации с закодированными в записи реестра, которая считаются недопустимой, чтобы проверить ее недопустимый символ. На этапе 612 CNAP 101 отменяет присвоение адреса базовой сети, начиная от узла 110, отделяя присвоенный ранее адрес базовой сети от зарегистрированного уникального параметра U_{PARAM} этого узла и уникального параметра пользователя U_{PARAM}, причем подключение этого узла к базовой сети автоматически разъединяется, при этом отмененный присвоенный адрес возвращается в пул присваиваемых сетевых адресов и становится доступным для следующего запрашивающего узла на этапе 601. Затем управление возвращается к вопросу на этапе 608.

[0079] На фиг. 7 проиллюстрирована блок-схема варианта реализации алгоритма, реализующего сетевую архитектуру изобретения, выполненную на каждом узле 110_N, 114_N, 116_N, 118_N в сети. Для каждого узла изначально требуется включение питания и, обычно на этапе 701, конфигурирование с помощью операционной системы, содержащей команды для управления обработкой базовых данных, взаимозависимостью и совместимостью ее аппаратных компонентов, в том числе подпрограммы передачи данных для конфигурирования узла для двусторонний связи по сети через один или более соответствующих интерфейсов, в конечном счете, соединенных с маршрутизатором 131_N или базовой станцией 138_N. На этапе 702, узел запрашивает доступ к базовой сети или доступ к системе в CNAP 101 и содержит в запросе по меньшей мере уникальный параметр U_{PARAM} его узла. Принимая во внимание этапы 601-607, описанные в данной заявке, на этапе 703 узел получает доступ к базовой сети после присвоения ему адреса базовой сети посредством CNAP 101, и получает копию реестра 150 идентификаторов от CNAP.

[0080] До тех пор, пока узел остается подключенным к базовой сети, следующая подпрограмма одновременно обновляет узел в отношении последующих удаленных узлов, подключающихся к базовой сети, и содействует совместному с CNPA 101 решению задачи поддержания целостности реестра 150 идентификаторов, посредством обработки реестра идентификаторов для проверки его целостности, например, путем обработки кодированного реестра с помощью аналогичного известного алгоритма доказательства выполнения работы как и в CNAP 101.

[0081] Соответственно, на этапе 704 выполняется определение, принял ли узел следующую версию реестра 150 идентификаторов аналогично версии, ранее принятой на этапе 703. Если ответ отрицательный, на этапе 705 выполняется следующее определение, было ли получено оповещение от удаленного узла, содержащего недопустимую запись реестра. В случае если ответ на вопрос этапа 705 отрицательный или, в качестве альтернативы, если на вопрос предыдущего этапа 704 дан положительный ответ и получена следующая версия реестра 150 идентификаторов, узел проверяет реестр идентификаторов на последовательную целостность на этапе 706, например, путем обработки кодированного реестра с помощью аналогичного известного алгоритма доказательства выполнения работы как и в CNAP на этапе 609. Затем на этапе 707 выполняется проверка, появилась ли на этапе проверки недопустимая запись реестра. Если ответ отрицательный, то управление возвращается к этапу 704 для проверки обновленного реестра 150 идентификаторов, причем поток проверки продолжает непрерывно проверять целостность реестра 150 идентификаторов до тех пор, пока не будет получено удаленное оповещение и не будет приняты последующие версии реестра 150 идентификаторов.

[0082] В случае если ответ на вопрос этапа 707 положительный или, в качестве альтернативы, если на вопрос предыдущего этапа 705 дан положительный ответ и получено оповещение, узел идентифицирует несоответствующую запись реестра из реестра идентификаторов на этапе 708, которая, принимая во внимание целостность символа, последовательности и процесса кодирования параметров узла в реестре, может в одном варианте реализации изобретения состоять из выбранной записи, имеющей несоответствующий присвоенный сетевой адрес (или цифровой ключ, представляющий его) относительно ее более ранней итерации или по сравнению с фактическим состоянием в базовой сети постоянно отслеживается и определяется CNAP в предыдущей итерации реестра. На этапе 709 узел осуществляет широкополосную передачу оповещения, содержащего несоответствующую запись реестра, в качестве недопустимой записи реестра, всем узлам, подключенным к базовой сети, включая, таким образом, CNAP 101, который должен обрабатывать его в соответствии с этапами 608-612.

[0083] Затем на этапе 710 выполняется определение, ввел ли пользователь узла команду прерывания, чтобы прервать работу узла, либо в режиме подключения к базовой сети или полностью. В случае отрицательного ответа на вопрос этапа 707 управление автоматически возвращается к вопросу этапа 704, осуществляя проверку следующей версии реестра 150 идентификаторов. В качестве альтернативы, в случае положительного ответа на вопрос этапа 707 пользователь может в конечном итоге отключить вычислительное устройство, реализующее узел.

С помощью данного способа, выполняемого на каждом подключенном узле, преимущественно узлы в базовой сети могут доверять своим собственным доказательствам выполнения работы, и для целей обнаружения нарушения идентификации каждый узел может доверять своей собственной оценке истории, последовательности и идентификаторам реестра 150 идентификаторов и не нуждается

в том, чтобы доверять тому, что проверено удаленным узлом с наилучшей вычислительной мощностью, а также тому, согласны ли другие узлы на изменение в реестре или нет, но просто передает проверку в CNAP 101, имея свой результат децентрализованного обнаружения изменений в узле.

[0084] На фиг. 8 проиллюстрирована блок-схема двух альтернативных вариантов реализации алгоритма, реализующего сетевую архитектуру изобретения, описанная со ссылкой на фиг. 6, выполненную в сети у множества провайдеров доступа к базовой сети, причем одинаковые ссылочные номера относятся к одинаковым этапам обработки данных. Оба варианта реализации изобретения представляют собой дополнительные потоки обработки, выполняющиеся одновременно с функциональной возможностью управления доступом к сети и присущей ей аутентификацией узла, описанной со ссылкой на этапы 601-607, причем отмена присвоения идентификатора и адреса базовой сети недопустимых записей реестра описаны со ссылкой на этапы 608-612.

[0085] В первом альтернативном варианте реализации изобретения на этапе 801 после каждой широкополосной передачи следующей версии реестра 150 идентификаторов этапа 607 выполняется определение, принял ли CNAP 101 запрос на сертификацию от удаленного узла 110_N, 114_N, 116_N, 118_N в сети. В случае отрицательного ответа на вопрос этапа 801 управление возвращается к определению запроса доступа узла на этапе 601. В качестве альтернативы, в случае положительного ответа на вопрос этапа 801, удаленный узел выбирается, чтобы быть сертифицированным как CNAP 101_{N+1} и является CNAP-кандидатом, запрашивающим сертификационное голосование посредством принимающего запрос голосующего CNAP 101.

[0086] На этапе 802 голосующий CNAP 101 осуществляет поиск подлежащих проверке параметров базовой сети в примерных характеристиках 301_{CN} стека протоколов базовой сети, с которыми, как ожидается, CNAP-кандидат будет полностью взаимодействовать.

[0087] На этапе 803 голосующий CNAP 101 осуществляет поиск подлежащих проверке атрибутов провайдера доступа к базовой сети $attr_1$, в примерном заданном наборе атрибутов аппаратных средств, атрибутов программного обеспечения, атрибутов связи и одного или более наборов правил, как описано со ссылкой на функциональные модули 311_{CN}-320_{CN} CNAP 101, и который, как ожидается, полностью реализует и дублирует CNAP-кандидат для выполнения роли CNAP в качестве контроллера шлюза в сети. Процедура проверки обеспечения соответствия CNAP условиям и функциональным возможностям системы/реестра, заданным программой данных, которая устанавливается в CNAP 300, может быть с открытым исходным кодом, чтобы обеспечить прозрачность для совместимости. Также может быть выполнено тестирование в реальном масштабе времени автоматизированных процедур для обеспечения доступа пользователей и реагирования на нарушения идентификации.

[0088] На этапе 804 голосующий CNAP 101 получает атрибуты узла $attr_2$ от CNAP-кандидата, в качестве примера, конкретные атрибуты аппаратных средств, атрибуты программного обеспечения, атрибуты связи и один или более наборов 311_2-320_2 правил CNAP-кандидата и, на следующем этапе 805 сравнивает их с перечисленными параметрами 301_{CN} базовой сети и перечисленными атрибутами CNAP $attr_1$ как для совместимости, так и для функциональной идентичности. В другом варианте реализации изобретения процесс проверки основан на производительности и осуществляется посредством тестирования нового CNAP и надлежащего функционирования его систем.

[0089] Голосующий CNAP 101 формирует свой голос на этапе 806 в виде функции

выходных данных этапа 805 сравнения, причем голос не выводится (посредством отрицательного голосования), когда один или более атрибутов $attr_2$ CNAP-кандидата не совпадают с подлежащими проверке параметрами 301_{CN} базовой сети и подлежащими проверке атрибутами аил провайдера доступа к базовой сети и, наоборот, выводится положительное голосование, когда атрибуты $attr_2$ CNAP-кандидата полностью соответствуют подлежащим проверке параметрам 301_{CN} соответствующей базовой сети и подлежащим проверке атрибутам провайдера доступа к базовой сети $attr_1$. Альтернативные варианты реализации изобретения могут предусматривать вывод положительного голоса на этапе 805, на котором выводится только частичное совпадение, например, на основе сопоставления только приоритетных или весомых атрибутов относительно необязательных или менее весомых атрибутов.

[0090] После положительного голосования голосующий CNAP, следовательно, сертифицирует CNAP-кандидат 101 как CNAP 101_{N+1} на этапе 807, причем сертифицированный CNAP 101_{N+1} может затем выполнять функцию контроллера шлюза, как описано в данной заявке, в частности, со ссылкой на фиг. 6 в данной заявке, параллельно и в тандеме с голосующим CNAP, эффективно разделяя потребление ресурсов для обработки, необходимых для управления доступом к сети. В альтернативном варианте без голосования CNAP-кандидат 101 остается несертифицированным.

[0091] Во втором альтернативном варианте реализации изобретения, показанном на фигуре пунктирными линиями в отличие от этапов 801-807 первого альтернативного варианта реализации изобретения, требование голосования в базовой сети по данному изобретению распределяется среди множества CNAP 101_{1-N}, причем CNAP-кандидат 101_{N+1} должен получить либо большинство голосов, либо единогласное голосование от всех голосующих CNAP 101_{1-N}, при этом каждый голосующий CNAP 101 должен провести сертификацию кандидата CNAP 101_{N+1}, по существу, как описано со ссылкой на этапы 801-807.

[0092] Этот второй альтернативный вариант реализации изобретения может быть эффективно объединен с вышеописанным первым альтернативным вариантом реализации изобретения после первого CNAP 101, сертифицирующего второй CNAP 101, как описано со ссылкой на этапы 801-807, причем базовая сеть, таким образом, содержит по меньшей мере два голосующих CNAP $101_{1,2}$, выполненных с возможностью осуществлять либо единогласное голосование, либо раздельное голосование по следующему третьему CNAP-кандидату 101_3.

[0093] В данном втором альтернативном варианте реализации изобретения в случае положительного ответа на вопрос этапа 801, при этом запрос сертификации CNAP был получен от удаленных узлов 110_N, 114_N, 116_N, 118_N в сети, также выполняется определение 902 того, получено ли требование для голосования независимое от сертификационных голосов от равноправных CNAP. В случае отрицательного ответа на вопрос этапа 902 управление возвращается к последовательности этапов 802-807.

[0094] В альтернативном варианте в случае положительного ответа на вопрос этапа 902 управление разделяется между последовательностью этапов 802-807, которая выполняется независимо для обработки собственного голоса CNAP применительно к запрашивающему узлу, и логикой удаленного сопоставления голосов, которая на этапе 903 начинается с поиска применимого порога голосования в соответствии с набором

правил базовой сети, например, заданное минимальное количество голосов или половина числа сертифицированных CNAP 101 в сети плюс один в случае большинства голосов, или общее количество сертифицированных CNAP 101 в сети в случае единогласного голосования. На этапе 904 голосующий CNAP опрашивает базовую сеть на предмет соответствующего решения по голосованию каждого удаленного равноправного CNAP, чтобы получить текущий подсчет голосов.

[0095] Когда на этапе 806 выводится независимое решение голосующего CNAP 101, то на этапе 905 текущее количество голосов этапа 904 либо увеличивается на собственный голос CNAP, если этот голос является сертификационным голосом, либо уменьшается на альтернативное решение CNAP о выводе без голосования. Затем на этапе 906 выполняется определение, соответствует ли увеличенное или уменьшенное количество голосов на этапе 905 пороговому значению базовой сети, полученному на этапе 903, или превышает его. В случае положительного ответа на вопрос этапа 906 управление переходит к этапу 807, и голосующий CNAP таким образом сертифицирует CNAP-кандидат 101 как CNAP 101_{N+1}, причем сертифицированный CNAP 101_{N+1} может затем осуществлять функции контроллера шлюза и сертификации CNPA, как описано в данной заявке, параллельно со всеми другими голосующими CNAP и в тандеме с ними, еще более эффективно разделяя потребление ресурсов для обработки, необходимой для управления доступом к сети. В альтернативном варианте в случае отрицательного ответа на вопрос этапа 906 голосующий CNAP 101 передает свое решение по голосованию своим равноправным CNAP по всей сети, каждый из которых может получить его при обработке своего собственного количества голосов в своем собственном экземпляре этапа 904.

[0096] Принимая во внимание описанные в данной заявке этапы обработки данных, CNAP 101 сертифицируется для работы и предоставления доступа или предотвращения доступа к сети и подключенным к ней системам, если он соответствует технологическим и административным условиям сети для использования, приемлемого одновременно для CNAP и его пользователей. Для разных систем могут потребоваться разные условия для сертификации CNAP, что может быть связано с функциональностью и возможностями одного или всех CNAP для управления доступом к сети и использования систем, подключенных к ней, и может потребоваться использование всех атрибутов CNAP для улучшения, управления и запрета параметров, функциональности и активности в сети. Система, которой должен соответствовать CNAP, может быть системой с открытым исходным кодом, необратимой, интегрированной в распределенный реестр, или контролируемой сторонней платформой или другим CNAP для целостности и прозрачности в процессе реализации. Закодированная программа также может быть разработана для уведомления других сертифицированных CNAP, если какой-либо код или условия будут изменены, добавлены, удалены или реорганизованы. Система может быть спроектирована для контроля и проверки, а также выявления изменений для других узлов или самой системы для оповещения об изменениях в системе перед окончательной сертификацией.

[0097] Технологическая совместимость процедуры сертификации преимущественно делает невозможным вмешательство одного узла или CNAP в архитектуру и функционирование сети. Все CNAP 101, которые сертифицированы и соответствуют атрибутам и политикам базовой сети, могут получать информацию из реестра идентификаторов и систем, подключенных к сети в соответствии со спецификацией сетевой архитектуры, и предоставлять доступ к узлам пользователей. Межсетевое применение преимущественно улучшает конкретную систему по мере того, как все

больше и больше CNAP сертифицируются и соответствуют условиям этой системы, соответственно масштабируясь по всей базовой сети.

[0098] Сертифицированный CNAP 101 может потерять свою сертификацию и, соответственно, способность предоставлять доступ к одному или более узлам, системам и реестрам, если он не остается совместимым с атрибутами и наборами правил базовой сети или если его узлы пользователей не соответствуют наборам правил использования базовой сети. Это аннулирование сертификата может быть автоматизированным, по умолчанию, если, например, атрибуты CNAP 311-320 не смогут отслеживать обновления для атрибутов и наборов правил базовой сети, и в результате сам CNAP теряет связь с базовой сетью; или если, например, информация об узле в реестре идентификаторов также связана с идентификатором CNAP и, когда присвоенный сетевой адрес или параметр пользователя U_{PARAM} узла становятся связанным с вредоносным программным обеспечением, компьютерным вирусом, спамом или подобной другой вредоносной сетевой деятельностью, CNAP становится связанным с ним с помощью его идентификатора.

[0099] На фиг. 9 и 10 проиллюстрированы соответствующие варианты реализации архитектуры базовой сети в соответствии с изобретением, в каждом случае управляемые с помощью множества CNAP $101_{1\text{-}N}$, причем для каждого CNAP определено его географическое положение, посредством проектирования с помощью его атрибутов географических координат и наборов правил базовой сети, применительно к государству-члену Европейского союза в варианте реализации изобретения на фиг. 9 и к географическому континенту в варианте реализации изобретения на фиг. 10.

[00100] В любом варианте реализации изобретения управление доступом запрашивающего узла к базовой сети в CNAP включает определение географического местоположения узла в CNAP для определения расстояния от узла относительно границы базовой сети. Эта процедура может быть реализована с помощью различных методов, таких как регистрация дополнительного узла или пользовательского уникального параметра $U_{PARAM}(x,y)$; определение географического местоположения; или определение географического местоположения географических координат узла в реальном масштабе времени, например, с помощью модуля 319 отслеживания и поиска; или оценка в реальном масштабе времени географических координат узла, полученных либо из IP-адреса запрашивающего узла, либо из ранее присвоенного адреса узла базовой сети; или любой комбинации данных методов. Данные о географическом местоположении соответствующих узлов также могут быть зарегистрированы на основе административной информации, такой как номер автономной системы для сети, регистрация в региональном интернет-реестре или другой организации, предоставляющей номерные ресурсы, или части лицензии от местного эмитента телекоммуникационных лицензий и т.д. Целью процедуры является определение присутствия узла в пределах или за пределами географического охвата CNAP, обрабатывающего запрос доступа этого узла, для предоставления или отклонения запроса доступа.

[00101] Соответственно, данное изобретение обеспечивает способы и системы для управления доступом к базовой сети через глобальную вычислительную сеть с помощью проверки подключенных к ней пользователей, чтобы предоставить доступ или заблокировать его к различным реестрам и системам, которые работают в инфраструктуре базовой сети или присоединены к ней. По меньшей мере один из реестров содержит систему, управляемую провайдерами доступа к базовой сети, которые

получают сертификацию в качестве контроллеров шлюза реестра, в соответствии с технологическими спецификациями и получая заданное количество голосов от текущих провайдеров доступа к базовой сети для подтверждения их сертификации. Как и в случае сертификации, провайдеры доступа к базовой сети могут предоставлять своим пользователям доступ к реестру идентификации, если такие пользователи соответствуют пользовательским спецификациям системы. Таким образом, изобретение использует инфраструктуру, протоколы информационных сетей, распределенные реестры и подключенные вычислительные системы для создания архитектуры, обеспечивающей эффективное построение сети для защиты идентификации, информации, прав и политик, включая механизм защиты от несанкционированного использования и других незаконных видов использования подключенных систем, в неконтролируемой среде.

[00102] Реестр объединяет идентифицируемые технологические атрибуты, такие как MAC-адрес, IMEI, IP-адрес и/или другой коммуникационный адрес сетевого протокола, с распределенным реестром адресных ресурсов своих пользователей, таких как открытые ключи, полученные из идентифицируемых технологических атрибутов (MAC-адрес, IMEI и т.д.), позволяя незамедлительно изменять прозрачность любых изменений в статусе идентификатора, закрепленного за коммуникационным адресом для всех узлов, имеющих доступ к реестру. Другие сети, системы, приложения, реестры могут взаимодействовать с помощью метода проверки базовой сети и реестра идентификаторов, а пользователи взаимодействуют с ними на основе одной цифровой идентификации, причем один или каждый CNAP 101 и идентификатор реализуют посредник для всех систем и реестров: архитектура основана на использовании одного или более CNAP, которые управляют инфраструктурой и доступом к ней (через «воздушные зазоры», блок канального уровня) в качестве точки предварительной квалификации и входа для различных распределенных систем и реестров, и в которые записывается каждая такая запись (устройства 110-118, базы данных 120, системы 116-118) в реестре 150 идентификаторов с частичным использованием технологии цепочки блоков, объединенной с системой коммуникационных адресов для реализации защищенной от несанкционированного доступа записи и публикации подключенных узлов ко всем узлам, в результате чего любые изменения идентификатора узла сразу становятся очевидными и сообщаются всем подключенным узлам. Данный реестр 150 идентификаторов и система 101 CNAP могут использоваться в качестве основы для других систем и могут обеспечивать взаимодействие между другими реестрами и системами.

[00103] Со ссылкой на вариант реализации изобретения, описанный со ссылкой на фиг. 10, примером такого реестра и платформы может быть глобальная система, выполненная с возможностью выдачи прав просмотра и копий на основе оригинальной работы в соответствии с алгоритмом, установленным владельцем прав с использованием распределенного реестра, например, типа цепочки блоков, в котором права реализуются посредством спецификации набора правил CNAP, а незаконный просмотр или копирование предотвращается только путем предоставления доступа разрешенным пользователям, которые являются допустимыми в записи реестра идентификаторов. Спецификация системы прав, установленная с помощью CNAP, которая использует возможности CNAP, может предотвратить незаконное использование и обеспечить права для пользователей сетей. Таким образом, варианты реализации данного изобретения могут использоваться для проектирования, использования и управления всеми типами административных и коммерческих политик, причем контроллер шлюза CNAP 101 обеспечивает доступ и совместимость с сетевыми системами, реализованными

на основе политик и других нормативных актов.

[00104] Например, реестр транзакций в национальной валюте может быть напрямую доступен через систему доступа CNAP. Такая валюта может быть выпущена с единицами количества или объема, которые зарегистрированы в реестре валют в соответствии с политикой, например, местного центрального банка, и количество может быть прозрачно зарегистрировано в распределенном реестре. Валюта может использовать программу данных, которая выполняет политику выпуска валюты на основе алгоритма и/или ввода из внешних источников, и она может быть реализована в или согласована с CNAP. Различные национальные, зарубежные или глобальные приложения и реестры, например, несколько распределенных реестров, управляющих разными валютами, могут взаимодействовать через реестр 150 идентификаторов, который обеспечивает надежную идентификацию по всем реестрам/валютам, и где значение от множества подключенных систем и реестров может быть связано с, и безвозвратно присоединено к различным идентификаторам, зарегистрированным в реестре 150 идентификаторов. Незаконные транзакции и/или валюты могут быть предотвращены с помощью спецификации регуляторной системы, в которой используются возможности CNAP для обеспечения политик и предотвращения транзакций между пользователями. Если пользователь имеет недействительную запись в реестре идентификаторов или он не авторизован и не идентифицирован, транзакции к таким пользователям и от них могут быть заблокированы. CNAP может предотвратить сигнализацию, связь, коммуникационные линии и использование приложений и систем, связанных с незаконными валютами. Платежные операторы, банки и другие финансовые организации могут получить доступ к реестру 150 идентификационных данных, который будет уведомлен в случае нарушения идентификационной информации пользователя.

[00105] Аналогично, со ссылкой на примерный вариант реализации изобретения, проиллюстрированный на фиг. 9, цифровыми паспортами можно управлять как на национальном, так и на региональном уровне посредством совместной сертификации взаимодействующими CNAP $_{1\text{-}N}$, чтобы поддерживать конфиденциальность и отслеживаемость пользователей посредством предоставления и блокирования доступа к различным системам и реестрам на основе заданных условий доступа и в которых недопустимая запись, возникающая в реестре 150 идентификаторов, приводит к уведомлению о нарушении идентификации. Географические границы также могут быть определены технически, и их пересечение может быть запрещено посредством системы доступа CNAP.

[00106] Такие варианты реализации изобретения могут обеспечить эффективные границы вокруг систем цифровой обработки данных, имеющих определенное географическое местоположение, таких как базы данных, системы и кибер-границы. Узлам 110_N, 114_N, 116_N, 118_N, имеющим доступ к реестру 150 идентификаторов, может быть предоставлен автоматический интерфейс с возможностями CNAP, включая средства управления сетью для ограничения связи с узлом, в котором выявлено нарушение идентификации. В таких вариантах реализации изобретения требование к личной информации пользователя U_{PARAM} может быть адаптировано к спецификации системы, в которой выбирается наименьший объем личной информации, достаточный для поддержания функции обеспечения конфиденциальности системы. Таким образом, посредством изобретения существует возможность создания системы, выполненной с возможностью обнаружения нарушение идентификации без необходимости доверять третьей стороне, что считается особенно актуальным в сфере кибербезопасности, а

также между правительствами.

[00107] Сетевая архитектура по данному изобретению преимущественно предотвращает вмешательство в базовую сеть и различные узлы, подключенные к ней, в контексте открытой WAN, например, через незаконные реестры, посредством процедуры доступа и управления, охватывающей физическое оборудование, сеть с коммутацией каналов и все сетевые возможности в CNAP, где все пользователи должны соответствовать спецификации системы, которая связана по меньшей мере с обработчиком 311 доступа и одной или более функциями 312-320 базовой сети, способными изменять функциональные возможности и возможное использование базовой сети в соответствии со спецификацией условий системы.

[00108] Варианты реализации данного изобретения могут быть закодированы на одном или более постоянных машиночитаемых носителях с командами для одного или более процессоров или блоков обработки, чтобы вызвать выполнение этапов. Следует отметить, что один или более постоянных машиночитаемых носителей должны содержать энергозависимую и энергонезависимую память. Следует отметить, что возможны альтернативные реализации, включая аппаратную реализацию, программную реализацию или программно-аппаратную реализацию. Аппаратно-реализованные функции могут быть реализованы с использованием ASIC, программируемых матриц, схем цифровой обработки сигналов или тому подобного. Соответственно, термин «средства» в любом пункте формулы изобретения предназначен для охвата как программных, так и аппаратных реализаций. Аналогично, термин «машиночитаемый носитель или носитель», используемый в данной заявке, включает программное обеспечение и/или аппаратное обеспечение, содержащее программу команд, реализованных на нем, или их комбинацию. Имея в виду эти альтернативные варианты реализации, следует понимать, что чертежи и сопровождающее описание предоставляют функциональную информацию, необходимую специалисту в данной области техники для написания программного кода (то есть программного обеспечения) и/или изготовления схем (то есть аппаратных средств) для выполнения требуемой обработки.

[00109] Следует отметить, что варианты реализации данного изобретения могут дополнительно относиться к компьютерным продуктам с постоянным материальным машиночитаемым носителем, на котором имеется компьютерный код для выполнения различных операций, реализуемых компьютером. Носитель и компьютерный код могут быть специально разработанными и сконструированными для целей данного изобретения, или они могут быть известными или доступными для специалистов в данной области техники. Примеры материальных машиночитаемых носителей включают, но не ограничиваются ими: магнитные носители, такие как жесткие диски, дискеты и магнитная лента; оптические носители, такие как CD-ROM и голографические устройства; магнитооптические носители; и аппаратные устройства, которые специально выполнены с возможностью хранения или хранения и выполнения программного кода, такие как специализированные интегральные схемы (ASIC), программируемые логические устройства (PLD), устройства флэш-памяти, а также устройства ПЗУ и ОЗУ. Примеры компьютерного кода включают машинный код, такой как созданный компилятором, и файлы, содержащие код более высокого уровня, которые выполняются компьютером с использованием интерпретатора. Варианты реализации данного изобретения могут быть реализованы полностью или частично как выполняемые компьютером команды, которые могут быть в виде программных модулей, которые выполняются устройством обработки. Примеры программных модулей включают библиотеки, программы, подпрограммы, объекты, компоненты и структуры данных.

В распределенных вычислительных средах программные модули могут быть физически расположены в локальном, удаленном или одновременно в локальном и удаленном оборудовании. Все аспекты изобретения могут быть реализованы виртуально и на прикладном уровне. В изобретении может использоваться любой тип методов обработки данных и связи, чтобы достичь цели осуществления инновационных принципов данного изобретения.

[00110] Для специалистов в данной области техники будет очевидным, что никакая вычислительная система или язык программирования не являются критическими для практического применения данного изобретения. Для специалистов в данной области техники также будет очевидным, что ряд вышеописанных элементов может быть физически и/или функционально разделен на подмодули или они могут быть объединены.

[00111] В описании термины «содержат, содержит, содержащийся и содержащий» или любая их вариация, а также термины «включают, включает, включенный и включающий» или любая их вариация считаются полностью взаимозаменяемыми, и им всем должна быть предоставлена наиболее широкая возможная интерпретация и взаимозаменяемость.

[00112] Изобретение не ограничивается вышеописанными вариантами реализации, но может варьироваться как конструктивно, так и на уровне элементов.

(57) Формула изобретения

1. Реализованный на компьютере способ управления доступом к сети и/или другим узлам и системам, подключенным к сети, включающий предоставление каждому узлу сети доступа к сети и/или другим узлам и системам, подключенным к сети, причем сеть содержит по меньшей мере один стек протоколов, содержащий множество уровней, при этом способ включает следующие этапы:

управление доступом к сети каждого уровня стека протоколов и ее работой в реальном масштабе времени посредством по меньшей мере одного провайдера доступа к базовой сети, причем провайдер доступа к базовой сети содержит по меньшей мере один цифровой и/или физический объект;

последовательное присвоение сетевого коммуникационного адреса для одного или каждого запрашивающего доступ узла у провайдера доступа к базовой сети;

кодирование присвоенного сетевого коммуникационного адреса у провайдера доступа к базовой сети с уникальным параметром узла и уникальным параметром пользователя узла в реестре идентификатора целостности;

распределение реестра идентификатора целостности в реальном масштабе времени к каждому узлу, подключенному к сети;

прием распределенного реестра идентификаторов и его обработка в каждом узле, подключенном к сети, или в одном или более сертифицированных узлах для проверки его последовательности, коэффициента идентичности и целостности процесса;

идентификация записи реестра, вызывающей потерю целостности, при определении потери целостности в реестре, и широковещательная передача оповещения, содержащего идентифицированную запись реестра, к каждому узлу, подключенному к сети, или одному или более сертифицированным узлам; и

отмена или управление доступом к сети, системе или реестру для узла, имеющего идентификаторы, соответствующие идентифицированной записи в реестре, либо при идентификации записи реестра, вызывающей потерю целостности, либо при приеме оповещения у провайдера доступа к базовой сети.

2. Способ по п. 1, отличающийся тем, что этап последовательного присвоения

сетевого коммуникационного адреса дополнительно включает сопоставление по меньшей мере одного уникального параметра структуры или устройства данных и/или по меньшей мере одного уникального параметра пользователя устройства обработки данных с одним или более заданных параметров доступа.

3. Способ по п. 2, отличающийся тем, что один или каждый заданный параметр доступа выбирают из группы, включающей: координаты глобальной системы определения местоположения (GPS), географические координаты точек сопряжения сети, IP-адреса или номера автономных систем, выданные региональными интернет-регистраторами (RIR), сеансовые ключи или токены авторизации, выпущенные провайдерами прикладного программного обеспечения (ASP).

4. Способ по п. 1 или 2, отличающийся тем, что этап кодирования дополнительно включает хэширование кодированного сетевого коммуникационного адреса, уникального параметра узла и уникального параметра пользователя узла, причем реестр идентификатора целостности является структурой данных цепочки блоков.

5. Способ по любому из пп. 1-4, отличающийся тем, что этап кодирования дополнительно включает преобразование присвоенного сетевого коммуникационного адреса в цифровую подпись или цифровой ключ.

6. Способ по любому из пп. 1-5, включающий дополнительный этап сертификации по меньшей мере одного подключенного к сети узла в качестве второго провайдера доступа к базовой сети в соответствии со списком заданных атрибутов провайдера доступа к базовой сети, выбранных из атрибутов аппаратных средств, атрибутов программного обеспечения, атрибутов связи и набора правил.

7. Способ по п. 6, отличающийся тем, что в сети, содержащей множество провайдеров доступа к базовой сети, этап сертификации подключенного к сети узла в качестве дополнительного провайдера доступа к базовой сети дополнительно включает этап голосования для сертификации узла у каждого из множества провайдеров доступа к базовой сети.

8. Способ по п. 6 или 7, включающий дополнительный этап определения географического местоположения каждого провайдера доступа к базовой сети.

9. Способ по любому из пп. 6-8, включающий дополнительный этап аннулирования сертификации провайдера доступа к базовой сети, когда он не в состоянии поддерживать один или более атрибутов из списка заданных атрибутов провайдера доступа к базовой сети.

10. Система управления доступом к сети и/или другим узлам и системам, подключенным к сети, с использованием способа управления доступа к сети и/или другим узлам и системам, подключенным к сети, как это определено в п. 1, содержащая:

по меньшей мере один стек протоколов, содержащий множество уровней;

по меньшей мере одного провайдера доступа к базовой сети, функционально взаимодействующего с каждым уровнем стека протоколов и выполненного с возможностью приема информации о системах, подсетях и реестрах, подключенных к сети, и управления доступом к сети узлов и их работой в сети в реальном масштабе времени, причем провайдер доступа к базовой сети содержит по меньшей мере один цифровой и/или физический объект;

один или более узлов, подключенных к сети, причем при запросе доступа к сети провайдером доступа к базовой сети одному или каждому узлу последовательно присваивается сетевой коммуникационный адрес; и

реестр идентификатора целостности, содержащий для каждого узла присвоенный сетевой коммуникационный адрес, закодированный в нем, с уникальным параметром

узла и уникальным параметром пользователя узла, причем реестр идентификатора целостности в реальном масштабе времени распределяется к каждому узлу, подключенному к сети;

причем один или каждый провайдер доступа к базовой сети или каждый узел дополнительно выполнены с возможностью:

обрабатывать полученный реестр для проверки его целостности;

идентифицировать запись в реестре, которая может привести к потере целостности;

передавать оповещение, содержащее идентифицированную запись реестра по сети;

причем один или каждый провайдер доступа к базовой сети дополнительно выполнен с возможностью отмены или управления доступом к сети для узла, имеющего сетевой коммуникационный адрес, соответствующий идентифицированной записи в реестре.

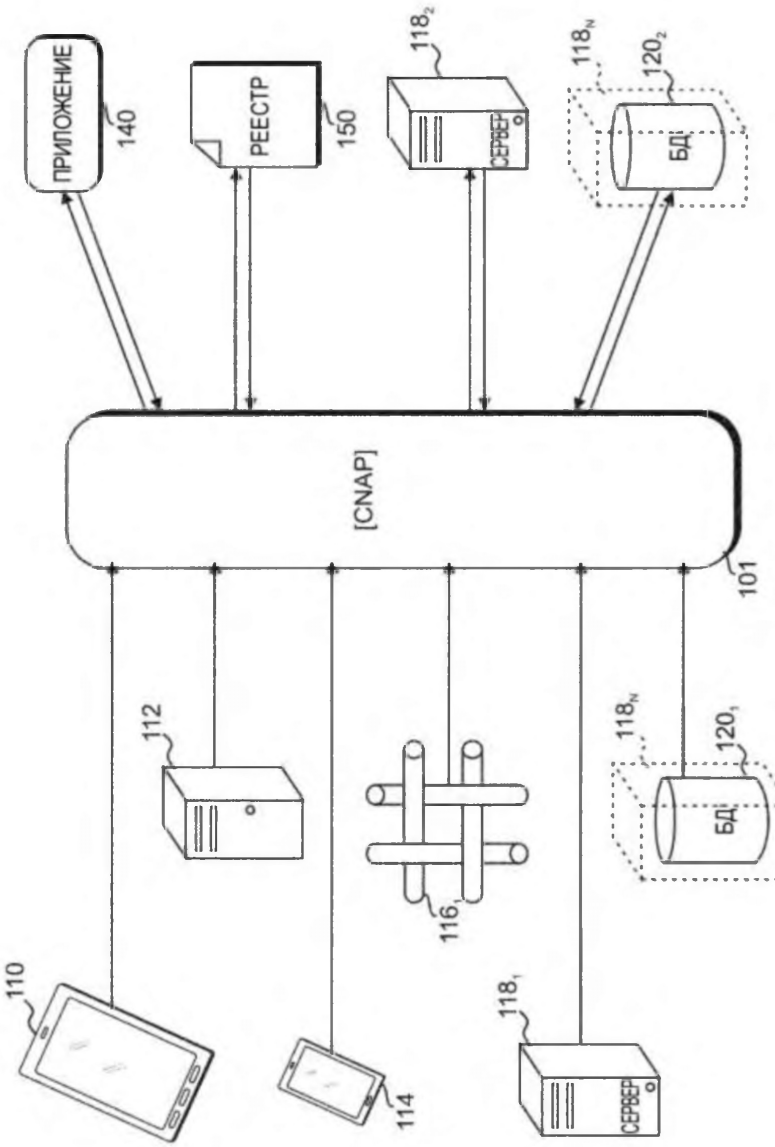
11. Система по п. 10, отличающаяся тем, что один или каждый провайдер доступа к базовой сети дополнительно выполнен с возможностью проверки достоверности одного или более уникального(ых) параметра(ов) каждого пользователя узла, причем максимальное количество сетевых коммуникационных адресов, присваиваемое одним или каждым провайдером сетевого доступа, в сети равно количеству проверенных в ней идентификаторов.

12. Система по п. 10 или 11, отличающаяся тем, что один или каждый провайдер доступа к базовой сети дополнительно выполнен с возможностью преобразования каждого сетевого коммуникационного адреса, присвоенного узлу, в цифровую подпись или цифровой ключ.

13. Система по любому из пп. 10-12, отличающаяся тем, что один или каждый уникальный параметр узла выбирают из группы, включающей: адрес управления доступом к среде (MAC), код международного идентификатора мобильного оборудования (IMEI), код идентификатора мобильного оборудования (MEID), электронный порядковый номер устройства (ESN), идентификатор Android в виде шестнадцатеричной строки.

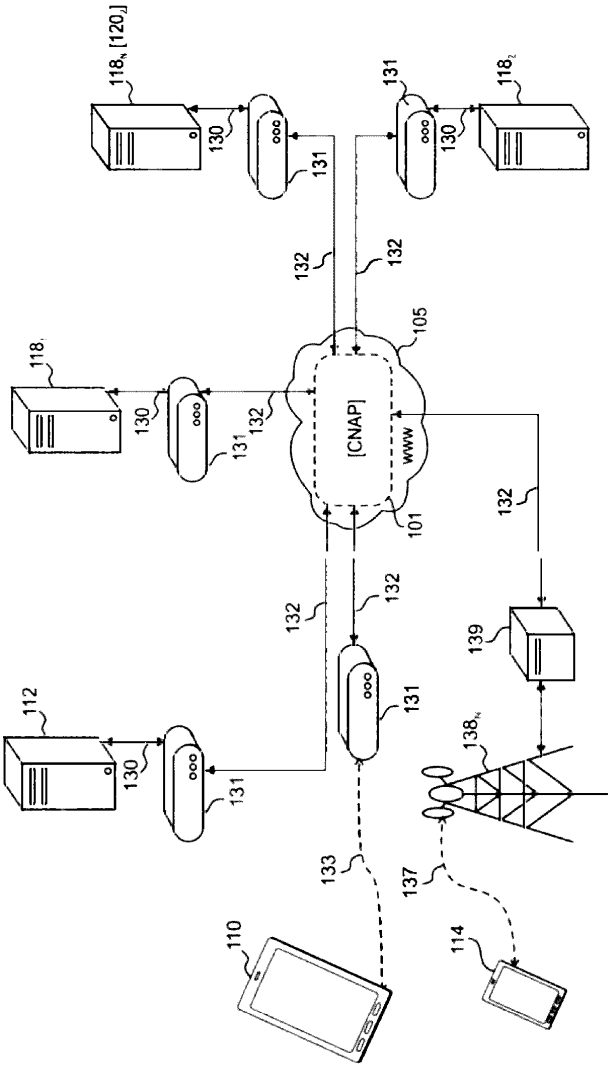
14. Система по любому из пп. 10-12, отличающаяся тем, что один или каждый уникальный параметр пользователя узла выбирают из группы, включающей: координаты глобальной системы определения местоположения (GPS), биометрические данные, персональный идентификационный номер (PIN), пароль, серийный номер паспорта, универсальный уникальный идентификатор (UUID).

1


ПРИЛОЖЕНИЕ
140
РЕЕСТР
150
118_2
СЕРВЕР
118_N
120_2
БД
[CNAP]
101
112
116
118_N
120_1
БД
110
114
118_1
СЕРВЕР

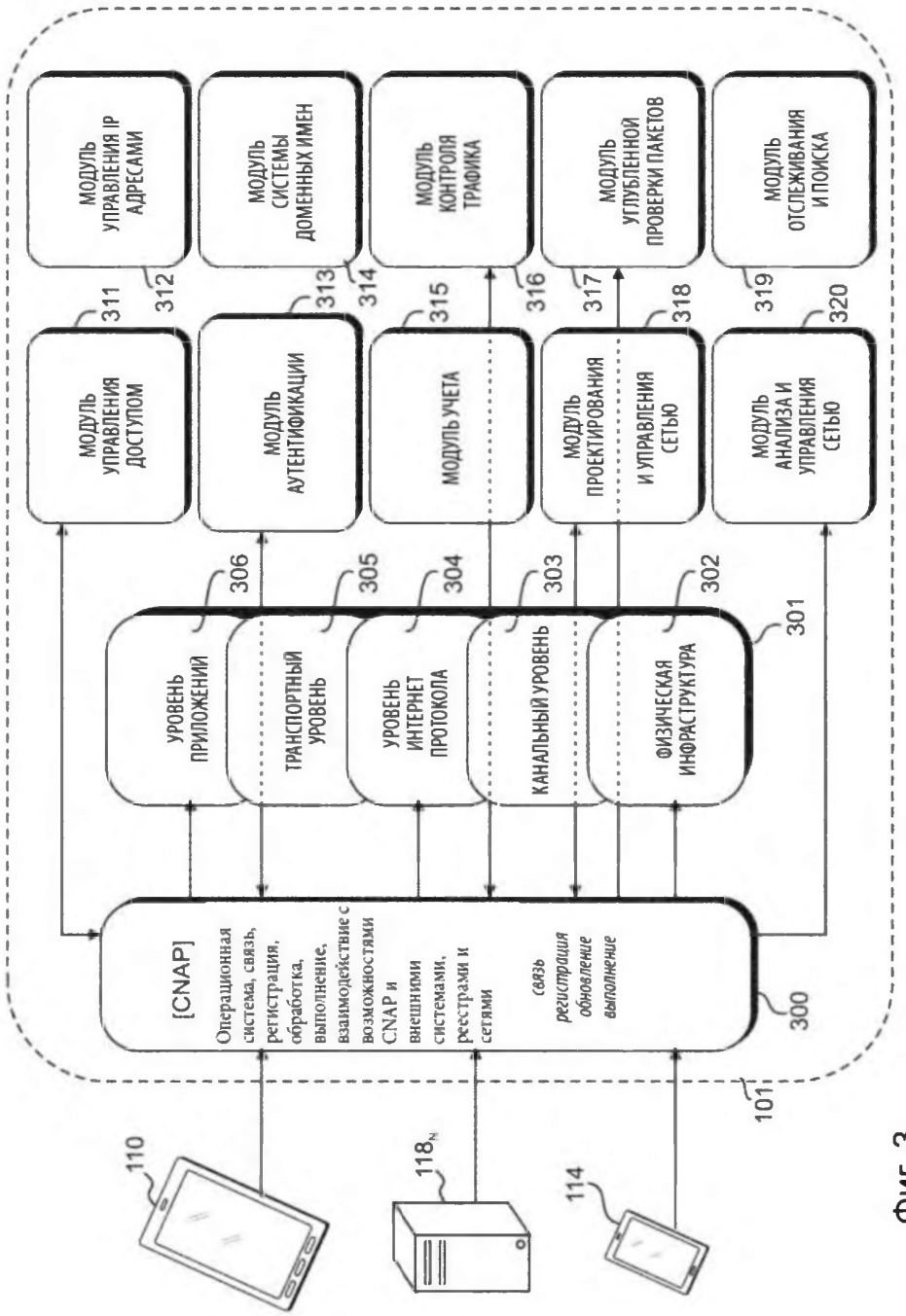
Фиг. 1

2


118k [120]
130
131
132
105
118
[CNAP]
www
101
139
112
138k
133
137
110
114

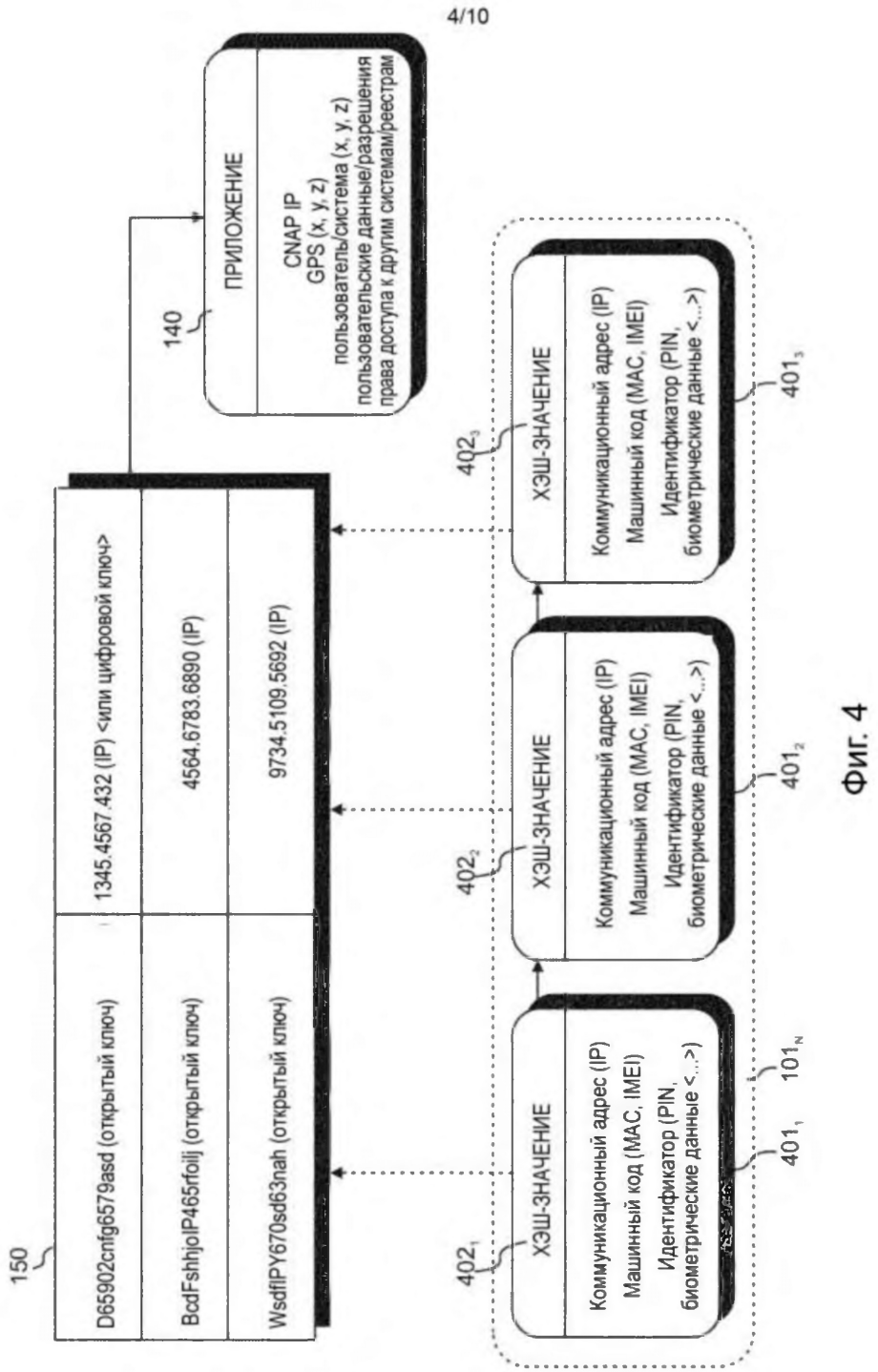
Фиг. 2

3

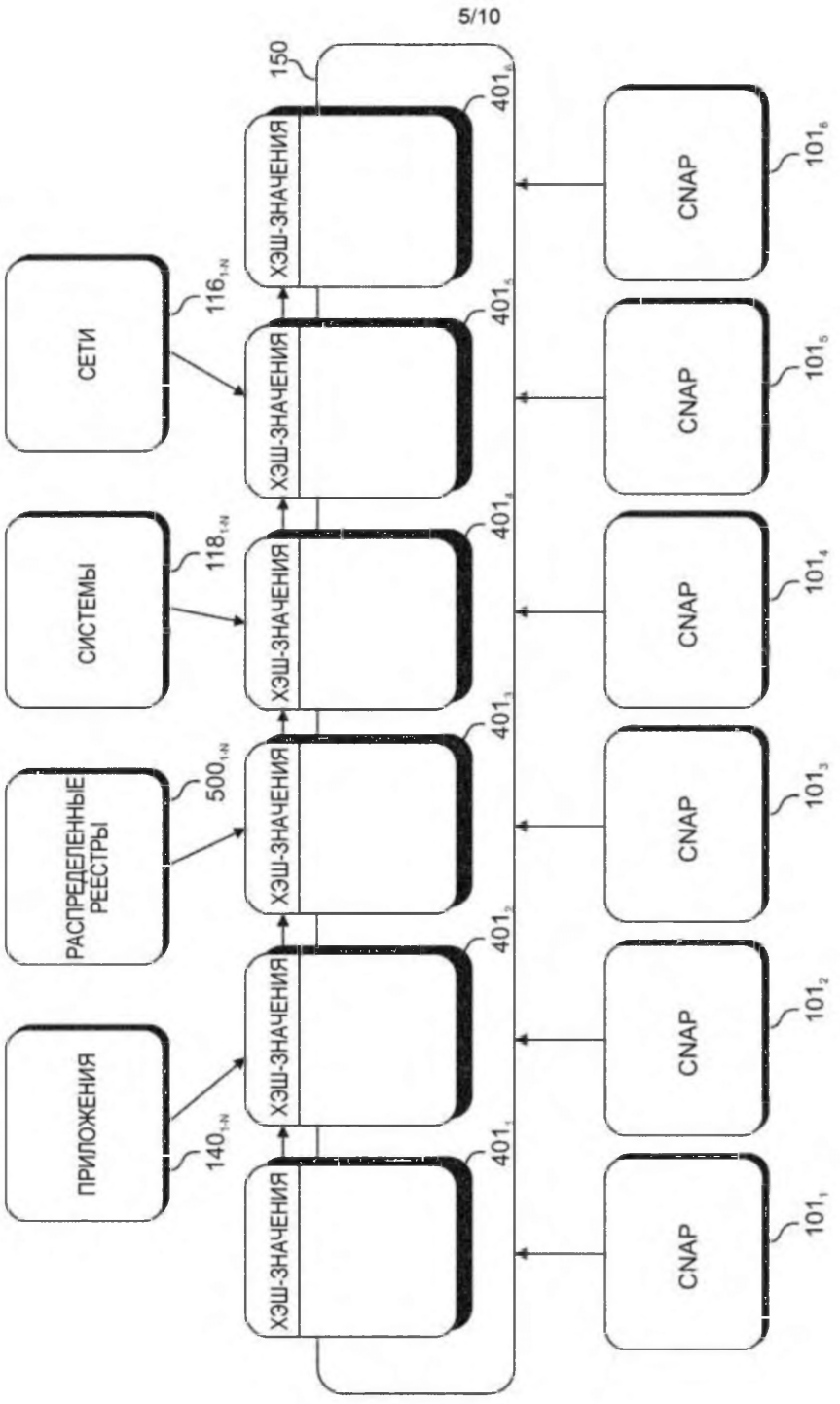

МОДУЛЬ УПРАВЛЕНИЯ IP АДРЕСАМИ
МОДУЛЬ СИСТЕМЫ ДОМЕННЫХ ИМЕН
МОДУЛЬ КОНТРОЛЯ ТРАФИКА
МОДУЛЬ УГЛУБЛЕННОЙ ПРОВЕРКИ ПАКЕТОВ
МОДУЛЬ ОТСЛЕЖИВАНИЯ И ПОИСКА
311
312
313
314
315
316
317
318
319
320
МОДУЛЬ УПРАВЛЕНИЯ ДОСТУПОМ
МОДУЛЬ АУТЕНТИФИКАЦИИ
МОДУЛЬ УЧЕТА
МОДУЛЬ ПРОЕКТИРОВАНИЯ И УПРАВЛЕНИЯ СЕТЬЮ
МОДУЛЬ АНАЛИЗА И УПРАВЛЕНИЯ СЕТЬЮ
306
305
304
303
302
301
УРОВЕНЬ ПРИЛОЖЕНИЙ
ТРАНСПОРТНЫЙ УРОВЕНЬ
УРОВЕНЬ ИНТЕРНЕТ ПРОТОКОЛА
КАНАЛЬНЫЙ УРОВЕНЬ
ФИЗИЧЕСКАЯ ИНФРАСТРУКТУРА
[CNAP]
Операционная система, связь, регистрация, обработка, выполнение, взаимодействие с возможностями CNAP и внешними системами, реестрами и сетями
связь
регистрация
обновление
выполнение
300
101
110
118N
114

Фиг. 3

4

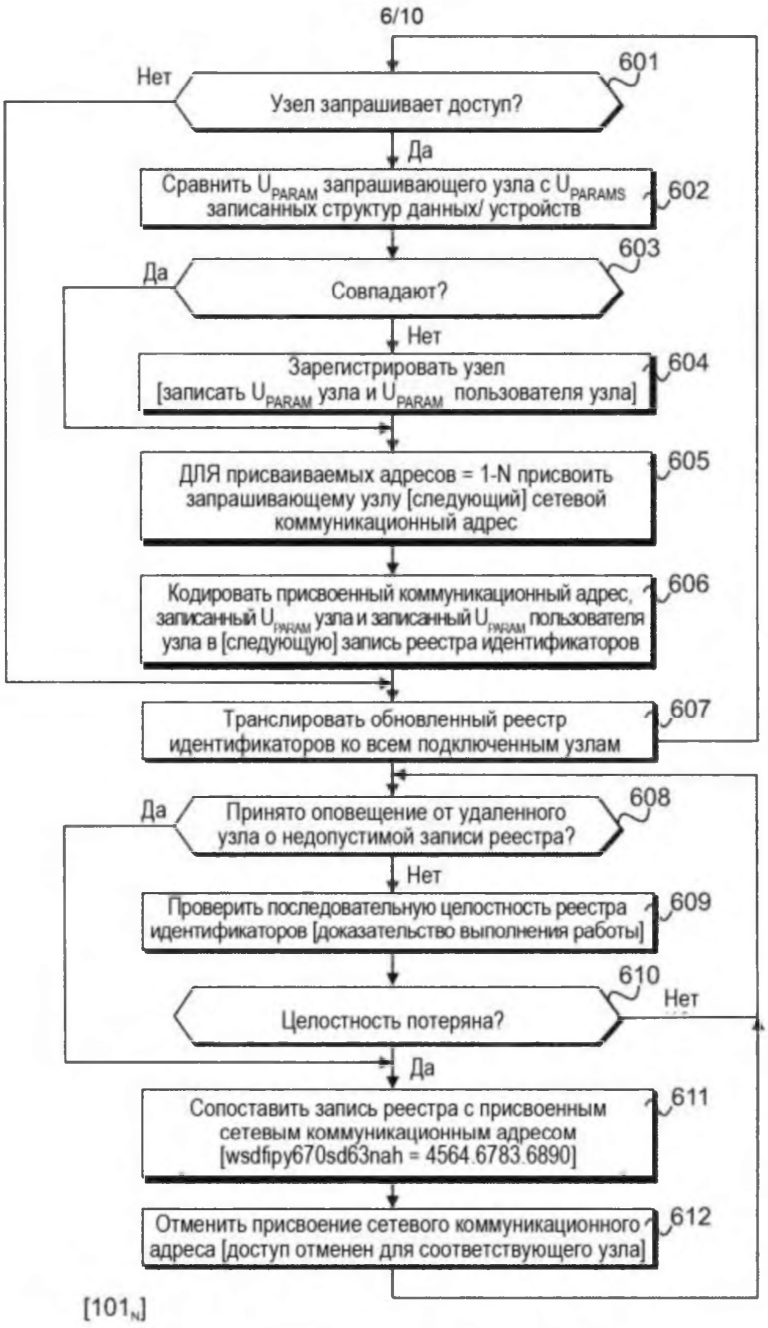

150
D65902cnfg6579asd (открытый ключ)
BcdFshhjoIP465rfoilj (открытый ключ)
WsdfIPY670sd63nah (открытый ключ)
1345.4567.432 (IP) <или цифровой ключ>
4564.6783.6890 (IP)
9734.5109.5692 (IP)
140
ПРИЛОЖЕНИЕ
CNAP IP
GPS (x, y, z)
пользователь/система (x, y, z)
пользовательские данные/разрешения
права доступа к другим системам/реестрам
402₁
ХЭШ-ЗНАЧЕНИЕ
Коммуникационный адрес (IP)
Машинный код (MAC, IMEI)
Идентификатор (PIN, биометрические данные <...>)
401₁
101_N
402₂
ХЭШ-ЗНАЧЕНИЕ
Коммуникационный адрес (IP)
Машинный код (MAC, IMEI)
Идентификатор (PIN, биометрические данные <...>)
401₂
402₃
ХЭШ-ЗНАЧЕНИЕ
Коммуникационный адрес (IP)
Машинный код (MAC, IMEI)
Идентификатор (PIN, биометрические данные <...>)
401₃

Фиг. 4


ПРИЛОЖЕНИЯ
$140_{1:N}$
РАСПРЕДЕЛЕННЫЕ РЕЕСТРЫ
$500_{1:N}$
СИСТЕМЫ
$118_{1:N}$
СЕТИ
$116_{1:N}$
150
ХЭШ-ЗНАЧЕНИЯ
401_1
401_2
401_3
401_4
401_5
401_6
CNAP
101_1
101_2
101_3
101_4
101_5
101_6

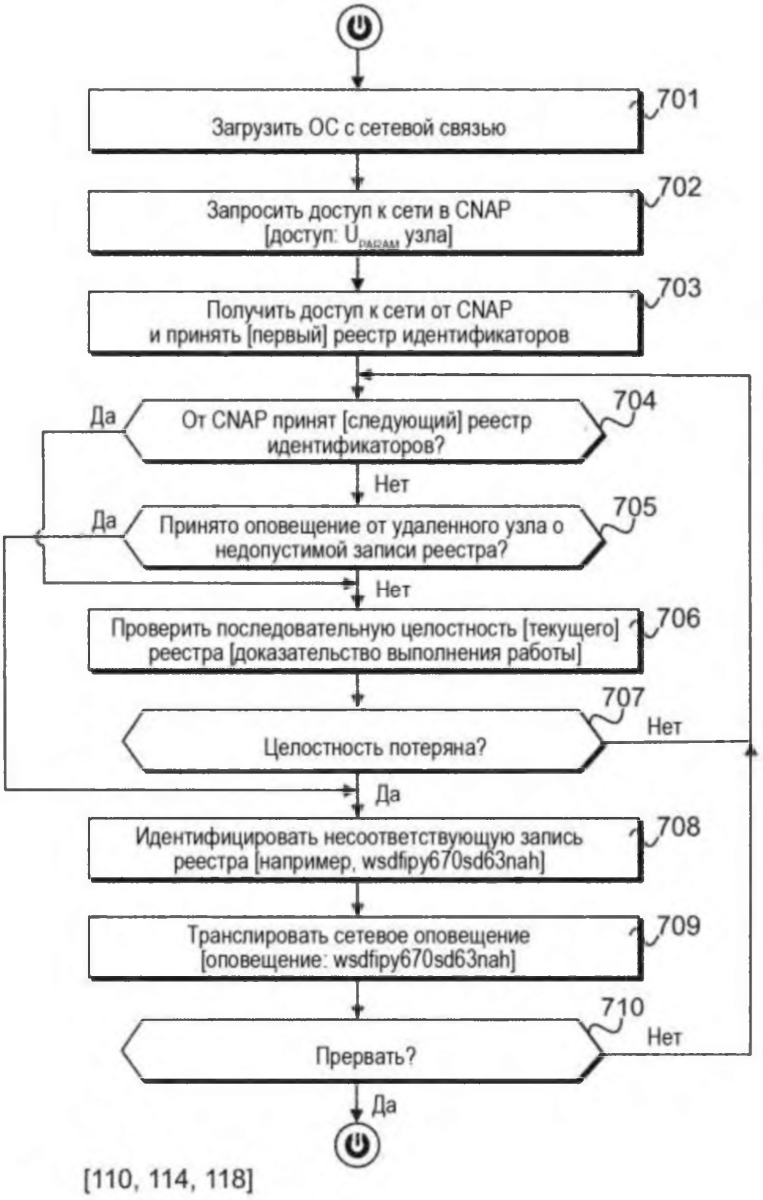
Фиг. 5

6


6/10
601
Нет
Узел запрашивает доступ?
Да
Сравнить U_{PARAM} запрашивающего узла с U_{PARAMS} записанных структур данных/ устройств
602
603
Да
Совпадают?
Нет
Зарегистрировать узел [записать U_{PARAM} узла и U_{PARAM} пользователя узла]
604
ДЛЯ присваиваемых адресов = 1-N присвоить запрашивающему узлу [следующий] сетевой коммуникационный адрес
605
Кодировать присвоенный коммуникационный адрес, записанный U_{PARAM} узла и записанный U_{PARAM} пользователя узла в [следующую] запись реестра идентификаторов
606
Транслировать обновленный реестр идентификаторов ко всем подключенным узлам
607
Да
Принято оповещение от удаленного узла о недопустимой записи реестра?
608
Нет
Проверить последовательную целостность реестра идентификаторов [доказательство выполнения работы]
609
610
Целостность потеряна?
Нет
Да
Сопоставить запись реестра с присвоенным сетевым коммуникационным адресом [wsdfipy670sd63nah = 4564.6783.6890]
611
Отменить присвоение сетевого коммуникационного адреса [доступ отменен для соответствующего узла]
612
$[101_N]$

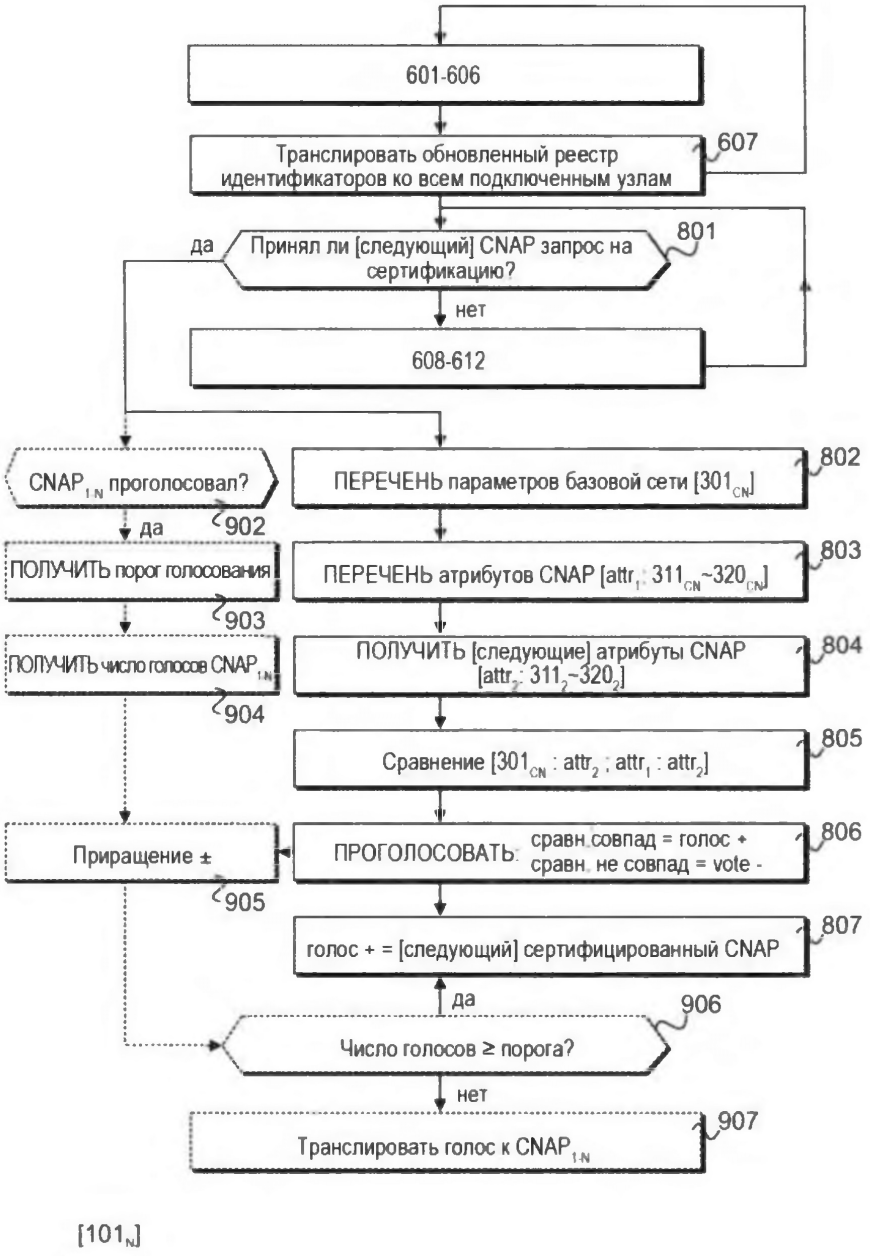
Фиг. 6

7


Загрузить ОС с сетевой связью
701
Запросить доступ к сети в CNAP
[доступ: U_{PARAM} узла]
702
Получить доступ к сети от CNAP
и принять [первый] реестр идентификаторов
703
Да
От CNAP принят [следующий] реестр идентификаторов?
704
Нет
Да
Принято оповещение от удаленного узла о недопустимой записи реестра?
705
Нет
Проверить последовательную целостность [текущего] реестра [доказательство выполнения работы]
706
Целостность потеряна?
707
Нет
Да
Идентифицировать несоответствующую запись реестра [например, wsdfipy670sd63nah]
708
Транслировать сетевое оповещение
[оповещение: wsdfipy670sd63nah]
709
Прервать?
710
Нет
Да
[110, 114, 118]

Фиг. 7

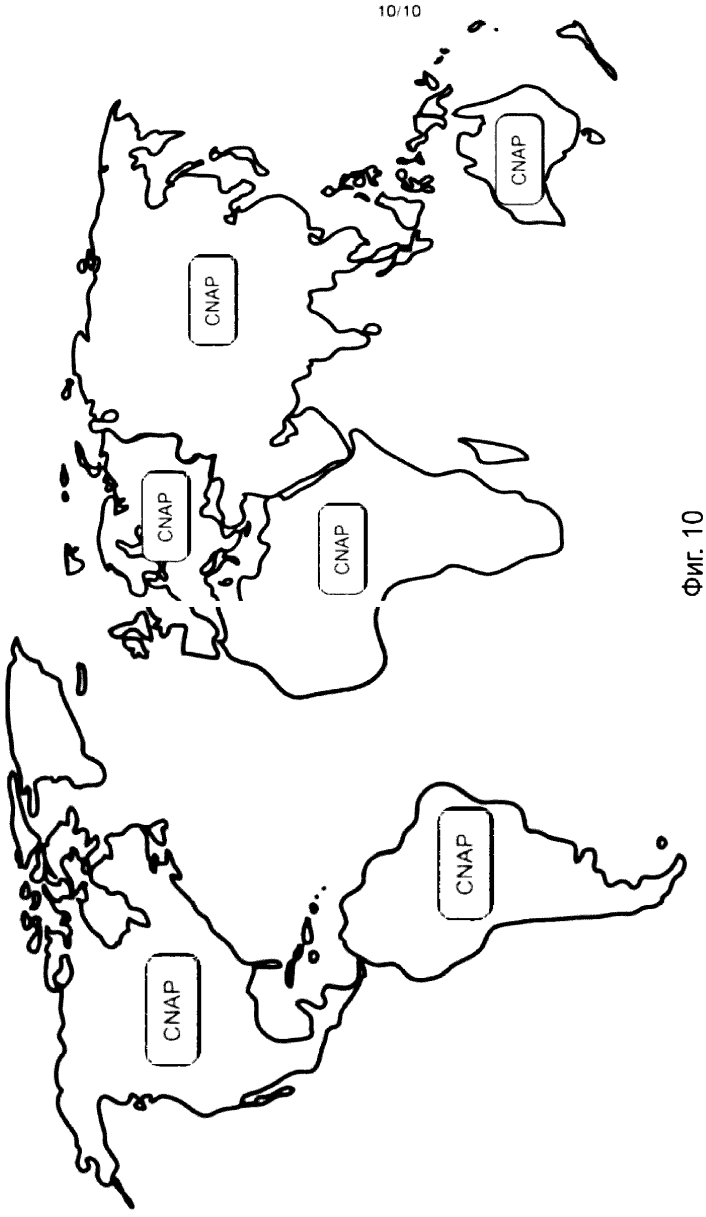
8


601-606
Транслировать обновленный реестр идентификаторов ко всем подключенным узлам
607
да
Принял ли [следующий] CNAP запрос на сертификацию?
801
нет
608-612
CNAP1-N проголосовал?
802
ПЕРЕЧЕНЬ параметров базовой сети [301CN]
да
902
ПОЛУЧИТЬ порог голосования
903
ПЕРЕЧЕНЬ атрибутов CNAP [attr1: 311CN~320CN]
803
ПОЛУЧИТЬ число голосов CNAP1-N
904
ПОЛУЧИТЬ [следующие] атрибуты CNAP [attr2: 3112~3202]
804
Сравнение [301CN : attr2 ; attr1 : attr2]
805
Приращение ±
905
ПРОГОЛОСОВАТЬ: сравн. совпад = голос + сравн. не совпад = vote -
806
голос + = [следующий] сертифицированный CNAP
807
да
906
Число голосов ≥ порога?
нет
907
Транслировать голос к CNAP1-N
[101N]

Фиг. 8

9

Фиг. 9



Фиг. 10