(19) Евразийское патентное ведомство

(11) 037189 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.02.17

(21) Номер заявки
201591358

(22) Дата подачи заявки
2015.06.08

(51) Int. Cl. ***G06F 17/00*** (2006.01)

(54) СОЗДАНИЕ ЗАЩИЩЕННЫХ ДАННЫХ В ЦЕПОЧКЕ ПОСТАВОК НЕФТИ И ГАЗА

(31) **PCT/US2014/041579**
(32) **2014.06.09**
(33) **US**
(43) **2016.04.29**
(86) **PCT/US2015/034662**
(87) **WO 2015/191443 2015.12.17**

(71)(73) Заявитель и патентовладелец:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Финкель Чарльз (US), Кемпбелл Марк, Ван Нгок Ти Кристоф, Касе Джорджио, Кёблер Фридрих, Нильсен Аксель (CH)

(74) Представитель:
Рыбина Н.А., Рыбин В.Н. (RU)

(56) US-B2-8676721
US-B2-7830273
US-A1-20130299591
US-B2-7424399
US-A1-20120158610
US-B2-8681000

(57) Настоящее изобретение в общем относится к системе и способу создания защищенных данных в цепочке поставок газа и нефти. Система создает защищенные данные, относящиеся к нефтегазовому ресурсу, во время перемещения по цепочке поставок. По меньшей мере одна система репозитория, собирающая защищенные данные, созданные путем сбора информации с помощью защищенного устройства наблюдения, отправляет защищенные данные в шлюз, являющийся частью системы глобального управления или системы управления целостностью, для создания кластеризованных событий. Изобретение также относится к системе и способу управления и контролирования данных между субъектами в цепочке поставок нефтегазового ресурса и, в частности, к системе и способу управления акцизным налогом для идентификации и согласования налоговых деклараций, объемов производства и оперативных отчетов.

037189 B1

037189 B1

Область техники

Настоящее изобретение в общем относится к системе и способу создания защищенных и надежных данных в цепочке поставок газа и нефти.

Уровень техники

Управление цепочками поставок является сложной задачей для организаций, регулярно занимающихся транспортировкой больших объемов продуктов в большом географическом регионе. Осуществление трассировки и слежения за товарами, изделиями или ресурсами в цепочке поставок само по себе является сложным, не говоря уже о дополнительных затруднениях в виде определения или подтверждения контрафакции, изменения маршрута транспортировки или замены состава определенного товара, изделий или ресурсов. В настоящее время существуют системы, в которых могут быть собраны и распределены товары, изделия или ресурсы, в которых информация о перемещении товара, изделий или ресурсов контролируется на протяжении цепочки поставок.

Нефтегазовая промышленность обычно разделена на три сектора: апстрим, мидстрим и даунстрим, как изображено на фиг. 2. Сектор апстрим известен как сектор разведки и добычи. Сектор апстрим включает в себя поиск и разведку потенциальных подземных или подводных залежей сырой нефти и природного газа (например, идентификацию потенциальных запасов углеводородов), бурение разведочных скважин и впоследствии бурение и заканчивание скважин, извлекающих и выводящих на поверхность (добывающих) сырую нефть и/или неочищенный природный газ. Сектор мидстрим включает в себя транспортировку (посредством трубопровода, железнодорожного транспорта, грузового транспорта и т.д.), хранение и оптовую торговлю сырыми или очищенными нефтепродуктами. Трубопроводы и другие многочисленные транспортные системы могут быть использованы для перемещения сырой нефти от мест добычи к перерабатывающим заводам и для подачи различных очищенных продуктов к дистрибьюторам в секторе даунстрим. Сектор даунстрим относится к очистке сырой нефти и к обработке и очистке неочищенного природного газа, а также к маркетингу и распределению продуктов, полученных из сырой нефти и природного газа. Сектор даунстрим предоставляет потребителям продукты, такие как бензин или моторное топливо, керосин, реактивное топливо, дизельное топливо, печное топливо, смазочные материалы, воски, асфальт, природный газ, и сжиженный нефтяной газ, а также сотни нефтехимических продуктов.

В последние годы наблюдается значительное увеличение незаконной деятельности, связанной с нефтегазовыми ресурсами. Например, число хищений нефти и газа в таких областях как Техас и Мексика выросло приблизительно в десять раз за последние десять лет. Коррупция, хищения, фальсификации, кражи и другая подобная незаконная деятельность происходит на всех фазах и секторах цепочки поставок, включая апстрим, мидстрим и даунстрим. Незаконные присоединения к трубопроводам, изменение маршрута транспортировки сырой нефти, угоны грузового транспорта, создание подземных туннелей и кража нефти на нефтеперерабатывающих заводах являются лишь некоторыми примерами незаконной деятельности, которые стали широко распространенными в данной промышленности. Из-за такого роста деятельности нефтегазовая промышленность столкнулась с несколькими проблемами. Например, происходящие события не всегда связаны друг с другом географически или другим образом и образуют цепочку разрозненных событий и происшествий. В настоящее время существует много разных решений и технологий для помощи в управлении, но они не являются однородными или совместимыми системами. Отсутствие координированной связи и прозрачности между областями, функциями и командами создает различные трудности, и отсутствие возможности фиксации и отслеживания событий препятствует учету. Таким образом, становится сложно или вообще невозможно своевременно реагировать на такие события и происшествия.

Таким образом, существует потребность в предоставлении интеллектуальной системы управления, способной контролировать и отправлять отчеты или предупреждения о незаконной деятельности, направленной на нефтегазовые ресурсы, одновременно повышая надежность, безопасность, соблюдение установленных норм и ответственность за состояние окружающей среды. Дополнительно, существует потребность в системе, удаленно отслеживающей и, согласно предписаниям и прогнозам, анализирующей события с ресурсами, происходящие в секторах апстрим, мидстрим и даунстрим, путем отслеживания, прогнозирования и предоставления данных в виде предупреждения для предоставления возможности принимать решения из любого местоположения. Дополнительно, существует потребность в защищенных данных, полученных в связи с товарами или изделиями, или в надежных и защищенных датчиках, которые будут эффективно использованы для защиты изделий или товаров в цепочке поставок нефти и газа. Дополнительно, существует потребность в системе, позволяющей редактировать защищенные, точные и надежные данные из секторов апстрим, мидстрим и даунстрим, что позволяет эффективно собирать налоги в цепочке поставок и позволяет на государственном уровне правильно взыскивать сумму налога, которая должна быть уплачена субъектами деятельности, участвующими в цепочке поставок нефти и газа. Термин "ресурсы", в контексте настоящей заявки, включает в себя все продукты переработки нефти и газа и инфраструктуру.

Краткое изложение изобретения

Настоящее изобретение посредством одного или нескольких из своих различных аспектов, вариан-

тов осуществления и/или специфических признаков или вспомогательных компонентов предоставляет различные системы, серверы, способы, носители и программы для установления связи с компилированными кодами, такими как, например, алгоритмы Java или добычи данных, или смесь аппаратных и программных элементов для создания данных с дополнительными атрибутами, применяемыми в системе глобального управления (GMS) или в системе управления целостностью (IMS), относящимися к управлению нефтегазовыми ресурсами.

В одном варианте осуществления предоставлена система для создания защищенных данных, относящихся к нефтегазовым ресурсам, во время прохождения по цепочке поставок, включающая по меньшей мере одну систему репозитория, собирающую защищенные данные, созданные путем сбора информации с помощью защищенного устройства наблюдения, и отправляющую защищенные данные в шлюз и/или модуль интеграции данных, являющийся частью системы глобального управления или системы управления целостностью, для создания кластеризованных событий.

В другом варианте осуществления предоставлен способ создания защищенных данных, относящихся к нефтегазовым ресурсам, во время прохождения по цепочке поставок, включающий в себя сбор защищенных данных, созданных путем сбора информации с помощью защищенного устройства наблюдения, по меньшей мере в одной системе репозитория, и отправку защищенных данных в шлюз и/или модуль интеграции данных, являющийся частью системы глобального управления или системы управления целостностью.

В еще одном варианте осуществления предоставлен постоянный машиночитаемый носитель, содержащий программу для создания защищенных данных, относящихся к нефтегазовым ресурсам, во время прохождения по цепочке поставок газа, при этом программа, при выполнении процессором, включает в себя сбор защищенных данных, созданных путем сбора информации с помощью защищенного устройства наблюдения, по меньшей мере в одной системе репозитория, и отправку защищенных данных в шлюз и/или модуль интеграции данных, являющийся частью системы глобального управления или системы управления целостностью, для создания кластеризованных событий или защищенного и надежного налогового отчета или KPI, используемого для взимания налогов, согласования налогов, исправления несоответствий данных, предоставленных из разных источников в цепочке поставок нефти и газа.

В одном аспекте платформа управления событиями получает обзор цепочки поставок, используя собранные защищенные данные для идентификации по меньшей мере одного из следующих видов деятельности: фальсификация, изменение маршрута транспортировки, замена состава, контрафакция, мошенничество и налоговое мошенничество, связанные с продуктом в цепочке поставок.

В другом аспекте система репозитория обменивается данными с платформой управления событиями посредством сети и включает в себя множество устройств хранения данных, доступных системе и распределенных в ней.

В еще одном аспекте стандартное устройство наблюдения выполнено с возможностью сбора стандартной информации о продукте из первого идентификатора продукта, при этом собранная информация образует стандартные данные, и защищенное устройство наблюдения выполнено с возможностью сбора стандартной информации о продукте из первого идентификатора продукта и защищенной информации из маркировки, при этом собранная информация образует защищенные данные.

В еще одном аспекте маркировка включает в себя состав, содержащий сложные соединения с люминесцентными свойствами по меньшей мере в одном из следующих диапазонов: УФ, ИК и ближний ИК и их сочетания, которые могут представлять химический ключ.

В другом аспекте первый идентификатор продукта соединен с аутентификатором.

В еще одном аспекте, когда защищенное устройство наблюдения собирает стандартную информацию и защищенную информацию, защищенные данные отправляются в систему репозитория и, когда стандартное устройство наблюдения собирает стандартную информацию, стандартные данные отправляются в систему репозитория.

В еще одном аспекте продукт представляет собой одно из следующего: бензин или моторное топливо, керосин, реактивное топливо, дизельное топливо, печное топливо, смазочные материалы, воски, асфальт, природный газ, сжиженный нефтяной газ и нефтехимические продукты.

В еще одном аспекте система репозитория сохраняет стандартные данные, связанные с продуктом, на протяжении жизненного цикла продукта в цепочке поставок, при этом стандартные данные имеют форму данных, характерных для первого идентификатора продукта.

В одном аспекте стандартное и защищенное устройство наблюдения представляет собой по меньшей мере один датчик, расположенный на протяжении цепочки поставок для сбора защищенной информации.

В другом аспекте датчик воспринимает данные, включающие в себя или относящиеся по меньшей мере к одному из следующего: температура, плотность, влажность, объем, сила тяжести, химический состав, давление, вес, изменение давления в трубопроводе, разница в весе транспортного средства или в объеме топлива, определение местонахождения по GPS, синхронизация местонахождения транспортного средства, географическая область, скорость потока, удельная проводимость, реология, мутность, формирование изображений, термическое формирование изображений, состояние датчика, показания тензо-

метрических датчиков, данные о погодных условиях, дорожные условия, состояние транспортного средства или дороги, скорость ветра, барометрические условия, количество атмосферных осадков, данные о техническом обслуживании или дата технического обслуживания, информация о персональном местоположении, радиочастотные данные, акустические данные, вязкость и местоположение по GPS.

В еще одном аспекте система репозитория сохраняет стандартные данные и защищенные данные, связанные с продуктом, на протяжении жизненного цикла объекта в цепочке поставок, при этом стандартные данные имеют форму данных, характерных для первого идентификатора продукта, и защищенные данные имеют форму данных, характерных для маркировки.

В другом аспекте стандартные данные и защищенные данные собираются одновременно защищенным устройством наблюдения.

В еще одном аспекте продукт отмечен первым идентификатором продукта и маркировкой.

В другом аспекте информация, собранная защищенным устройством наблюдения, получена от датчиков по меньшей мере в одном из трубопроводов на протяжении цепочки поставок нефти и газа, при этом маркировка продукта осуществлена химическим веществом, и трубопровод соединен с насосом заправочной станции, распространяющей продукт.

Краткое описание графических материалов

Настоящее изобретение далее описано в следующем подробном описании со ссылкой на упомянутое множество графических материалов, путем неограничивающих примеров предпочтительных вариантов осуществления настоящего изобретения, в которых подобные условные обозначения представляют подобные элементы на нескольких видах графических материалов.

На фиг. 1 показана примерная система для использования согласно вариантам осуществления, описанным здесь.

На фиг. 2 показана примерная цепочка поставок для использования в нефтегазовой промышленности.

На фиг. 3 показана еще одна примерная схема системы управления целостностью согласно описанному варианту осуществления.

На фиг. 4 показан пример сети цепочки поставок согласно описанному варианту осуществления.

На фиг. 5 показана примерная схема системы управления целостностью, взаимодействующей с платформой возмещения акцизного налога посредством интерфейса акцизной платформы согласно описанному варианту осуществления.

На фиг. 6A-6B показаны примерные схемы процесса кодировки и мечения объекта и отслеживания и аутентификации события согласно системе.

На фиг. 7 показана примерная блок-схема создания защищенного события согласно системе.

На фиг. 8 показан примерный глобальный репозиторий согласно системе.

На фиг. 9 показана примерная схема системы глобального управления согласно описанному варианту осуществления.

На фиг. 10 показана примерная схема интерфейса согласно одному варианту осуществления изобретения.

На фиг. 11A-11D показана примерная последовательность событий, в которых сбор данных происходит с течением времени для определения вероятности.

На фиг. 12 показана примерная схема интерфейса согласно одному варианту осуществления изобретения.

На фиг. 13 показан примерный вариант осуществления технологического маршрута интерфейса согласно одному варианту осуществления изобретения.

Подробное описание

Настоящее изобретение, благодаря одному или нескольким из своих различных аспектов, вариантов осуществления и/или специфических признаков или вспомогательных компонентов, таким образом, предназначено для предоставления одного или нескольких преимуществ, как отдельно указано ниже.

На фиг. 1 показана примерная система для использования согласно вариантам осуществления, описанным здесь. Система 100 изображена в общем виде и может включать в себя компьютерную систему 102, обозначенную в общем виде. Компьютерная система 102 может работать в качестве автономного устройства или может быть присоединена к другим системам или периферийным устройствам. Например, компьютерная система 102 может включать в себя одно или несколько из следующего: компьютеры, серверы, системы, сети связи или облачная среда или являться их частью.

Компьютерная система 102 может работать в качестве сервера в сетевой среде или в качестве пользовательского компьютера клиента в сетевой среде. Компьютерная система 102 или ее части, могут быть реализованы в виде различных устройств или встроены в различные устройства, такие как персональный компьютер, планшетный компьютер, телевизионная абонентская приставка, персональный цифровой помощник, мобильное устройство, карманный компьютер, портативный компьютер, настольный компьютер, устройство связи, беспроводной телефон, персональное доверенное устройство, веб-устройство или любая другая машина, способная выполнять набор команд (последовательных или других), определяющих действия, выполняемые этим устройством. Кроме того, хотя изображена одна компьютерная

система 102, дополнительные варианты осуществления могут включать в себя любую совокупность систем или вспомогательным систем, которые по отдельности или совместно выполняют команды или осуществляют функции.

Как изображено на фиг. 1, компьютерная система 102 может включать в себя по меньшей мере один процессор 104, такой как, например, центральный процессор, графический процессор или и то, и другое. Компьютерная система 102 также может включать в себя компьютерное запоминающее устройство 106. Компьютерное запоминающее устройство 106 может включать в себя статическое запоминающее устройство, динамическое запоминающее устройство или и то, и другое. Компьютерное запоминающее устройство 106 в качестве дополнения или альтернативы может включать в себя жесткий диск, оперативное запоминающее устройство, кэш или любую их комбинацию. Разумеется, специалистам в данной области будет очевидно, что компьютерное запоминающее устройство 106 может содержать любую комбинацию известных запоминающих устройств или одно устройство хранения данных.

Как показано на фиг. 1, компьютерная система 102 может включать в себя компьютерный дисплей 108, такой как жидкокристаллический дисплей, дисплей на основе органических светодиодов, индикаторная панель, твердотельный индикатор, электронно-лучевая трубка, плазменный дисплей или любой другой известный дисплей. Компьютерная система 102 может включать в себя по меньшей мере одно компьютерное устройство 110 ввода, такое как клавиатура, устройство дистанционного управления, содержащее беспроводную клавишную панель, микрофон, присоединенный к обработчику распознавания речи, камера, такая как видеокамера или фотоаппарат, устройство управления курсором или любую их комбинацию. Специалистам в данной области будет очевидно, что различные варианты осуществления компьютерной системы 102 могут включать в себя несколько устройств 110 ввода. Более того, специалистам в данной области также будет очевидно, что вышеуказанный перечень примерных устройств 110 ввода не является исчерпывающим и что компьютерная система 102 может включать в себя любые дополнительные или альтернативные устройства 110 ввода.

Компьютерная система 102 также может включать в себя устройство 112 считывания носителей данных и сетевой интерфейс 114. Кроме этого, компьютерная система 102 может включать в себя любые дополнительные устройства, компоненты, части, периферийные устройства, аппаратное обеспечение, программное обеспечение или любую их комбинацию, которые являются общеизвестными и расцениваются как относящиеся к компьютерную систему или включенные в нее, например, без ограничения, устройство 116 вывода. Устройство 116 вывода может представлять собой, без ограничения, динамик, аудиовыход, видеовыход, выход дистанционного управления или любую их комбинацию.

Каждый из компонентов компьютерной системы 102 может быть взаимосвязанным и осуществлять обмен данными посредством шины 118. Как изображено на фиг. 1, каждый из компонентов может быть взаимосвязан и осуществлять обмен данными посредством внутренней шины. Тем не менее, специалистам в данной области будет очевидно, что любые из компонентов также могут быть соединены посредством шины расширения. Более того, шина 118 может позволить осуществлять обмен данными посредством любого стандарта или другой спецификации, являющейся общеизвестной и изученной, такой как, без ограничения, шина PCI, шина PCI-express, интерфейс PATA, интерфейс SATA и т.д.

Компьютерная система 102 может сообщаться с одним или несколькими компьютерными устройствами 120 по сети 122. Сеть 122 может представлять собой, без ограничения, локальную сеть, глобальную сеть, Интернет, телефонную сеть или любую другую сеть, хорошо известную и изученную в данной области техники. Сеть 122, изображенная на фиг. 1, представляет собой беспроводную сеть. Тем не менее, специалистам в данной области будет очевидно, что сеть 122 также может представлять собой проводную сеть.

Дополнительное компьютерное устройство 120 изображено на фиг. 1 в виде персонального компьютера. Тем не менее, специалистам в данной области будет очевидно, что в альтернативных вариантах осуществления настоящей заявки устройство 120 может представлять собой портативный компьютер, планшетный ПК, персональный цифровой помощник, мобильное устройство, карманный компьютер, настольный компьютер, устройство связи, беспроводной телефон, персональное доверенное устройство, веб-устройство или любое другое устройство, способное выполнять набор команд, последовательных или других, определяющих действия, выполняемые этим устройством. Разумеется, специалистам в данной области будет очевидно, что вышеперечисленные устройства являются лишь примерными устройствами и что устройство 120 может представлять собой любое дополнительное устройство или приспособление, являющееся общеизвестным и изученным в данной области техники, в пределах объема настоящей заявки. Более того, специалистам в данной области подобным образом будет очевидно, что устройство может представлять собой любую комбинацию устройств и приспособлений.

Разумеется, специалистам в данной области будет очевидно, что вышеперечисленные компоненты компьютерной системы 102 являются лишь примерными и не должны расцениваться как исчерпывающие и/или всеобъемлющие. Более того, примеры компонентов, перечисленных выше, также являются примерными и не должны расцениваться как исчерпывающие и/или всеобъемлющие.

На фиг. 4 показана примерная сеть цепочки поставок. Система 500 включает в себя, например, сектор 508 апстрим, сектор 510 мидстрим, сектор 514 даунстрим, репозиторий и интерфейс 516 и службы

502, 504 и 506 обнаружения, с помощью которых разные компоненты системы 500 обмениваются данными по сети 520, такой как Интернет. Службы 502, 504 и 506 обнаружения включают в себя базу данных (и интерфейсы) для способствования обмену данными путем предоставления службы, создающей ссылку на информацию о продуктах и ресурсах (например, нефти и топливе) по мере их передвижения, например, по цепочке поставок от сектора 508 апстрим в сектор 510 мидстрим и в сектор 514 даунстрим. По мере прохождения продукта по цепочке поставок и его регистрации устройствами для сбора данных в каждом из секторов 508, 510 и 514 (как описано выше) собранные данные в форме стандартных или защищенных событий отправляются в соответствующую службу обнаружения. Это позволяет осуществлять контроль над продуктами по мере того, как они перемещаются по цепочке поставок и создают события (стандартные или защищенные) в режиме реального времени.

В частности, каждый продукт или ресурс или данные, отслеживаемые на протяжении цепочки поставок нефти и газа, включает в себя по меньшей мере один идентификатор и аутентификатор продукта. Следует понимать, что термин "продукт", в контексте настоящей заявки, может включать в себя любое сочетание терминов "ресурсы" и "данные" или может быть заменен ими. Другими словами, продукты, ресурсы и данные могут проходить по цепочке поставок. Любая ссылка на один термин в равной степени может включать в себя ссылку на другой термин, даже если это не указано в явном виде. Как было описано, устройство для сбора данных (например, датчик, камера и т.д.) может использоваться для идентификации идентификатора и аутентификатора продукта при возникновении одного из нескольких событий. Эти события могут включать в себя, без ограничения, поисковые и разведывательные работы, очистку, течение в трубопроводе, транспортировку грузовым автомобилем и т.д. Например, когда продукт отправляется от дистрибьютора к розничному торговцу, датчик или устройство сбора данных (например, ручное оповещение) у дистрибьютора указывает на отправку продукта и эта информация пересылается в соответствующую принимающую службу (например, розничную заправочную станцию, если продукт является топливом), и когда продукт поступает к розничному торговцу, другой датчик или устройство сбора данных указывает на прибытие продукта и эта информация сохраняется в соответствующей службе обнаружения. Следует понимать, что данные также могут быть "собраны" с помощью различных технологий. Например, может быть ручное оповещение о данных и поставках или некоторая группировка данных. В одном примере одно событие указывало бы на то, что продукт был загружен в Грузовой автомобиль №N. Другие данные указывали бы на местоположение по GPS Грузового автомобиля №N, демонстрируя, что он уезжает. Из этого можно было бы сделать логический вывод, что продукт уезжает. Дополнительный уровень защиты и безопасности предоставлен посредством репозитория и интерфейса 516, которые, как описано, сохраняют идентификатор и аутентификатор продукта, связанный или ассоциированный с соответствующим продуктом. Идентификатор и аутентификатор продукта предоставляют дополнительный уровень безопасности, поскольку лишь датчик (устройство для сбора данных), специально спроектированный для считывания идентификатора и аутентификатора продукта, может верифицировать соответствующий продукт, на который он помещен. Этот дополнительный уровень безопасности значительно уменьшает шанс попадания контрафактных и фальсифицированных товаров в цепочку поставок и позволяет системе получать как можно более защищенные и точные данные для последующего использования в системе интеграции данных или системе управления данными, являющихся частью систем GMS или IMS.

Предоставлено краткое описание процесса, относящегося к различным объектам на фиг. 4. Процесс начинается, например, с прохождения объекта по цепочке поставок, от сектора 508 апстрим через сектор 510 мидстрим в сектор 514 даунстрим. Ответственное хранение продукта регистрируется на протяжении цепочки поставок с помощью соответствующей службы обнаружения (которая может представлять собой одну и туже или разные службы). В некоторых вариантах осуществления регистрация происходит при фиксации события, относящегося к продукту. Другими словами, когда происходит установленное событие, событие, связанное с продуктом, учитывается службой обнаружения. Репозиторий и интерфейс 514 получают отчет об этой информации и сохраняют ее. Репозиторий и интерфейс 514 могут удостоверить подлинность продукта на основании информации идентификатора и аутентификатора продукта (например, маркировки), собранной ранее и сохраненной в них.

На фиг. 5 показана примерная схема системы управления целостностью согласно описанному варианту осуществления. Система управления целостностью IMS, сопряженная с платформой возмещения акцизного налога посредством интерфейса акцизной платформы (при этом указанная платформа является в основном программно реализованной платформой), включает в себя, без ограничения, систему управления данными DMS, модуль интеграции данных (или платформу обеспечения корпоративной связи), интерфейс шлюза и датчики или устройства сбора данных, применяемые для сбора данных из секторов апстрим, мидстрим и даунстрим, вместе с различными системами, хранящими и предоставляющими данные от будущих партнеров, франшизных предприятий и дочерних компаний юридического лица (не изображено). Система управления целостностью IMS также может включать в себя или охватывать внешние ресурсы, системы управления месторождением и ресурсами, прикладные системы, основанные на прогнозах и предписаниях, системы управления событиями, основанные на доказательном подходе, и существующие наследственные системы. Следует понимать, что система управления целостностью IMS

не ограничена описанными компонентами и не обязана включать в себя каждый из компонентов, изображенных в неограничивающем и примерном варианте осуществления. Например, система диспетчерского управления и сбора данных (ICS, такая как SCADA) может заниматься сбором данных вместо интерфейса шлюза. Как указано выше, данные могут храниться в одном репозитории или в нескольких репозиториях. Шлюз также может представлять собой беспилотные летательные аппараты, имеющие те же возможности, что и неподвижный шлюз, сопряженные с диспетчерским управлением и сбором данных и собирающие информацию непосредственно из датчиков или устройств сбора данных на уровнях апстрим, даунстрим и мидстрим.

Система управления целостностью IMS контролирует и управляет или сопрягается по меньшей мере с одним субъектом в цепочке поставок нефтегазовых ресурсов. Субъект может включать в себя, без ограничения, юридическое лицо, будущих партнеров, франшизные предприятия, дочерние компании и/или налоговое ведомство. Система и способ управления акцизным налогом для идентификации и согласования несоответствий между налоговыми документациями, объемами производства и оперативными отчетами от различных субъектов. Система управления целостностью IMS собирает неоднородные, неструктурированные и разрозненные данные из датчиков, устройств сбора данных и вспомогательных систем наблюдения в секторах апстрим, мидстрим и даунстрим нефтегазовой инфраструктуры (трубопроводов) для хранения и обработки собранных данных, используя сведения систем нефтегазовой инфраструктуры. Данные также собираются посредством дочерних компаний, франшизных предприятий и будущих партнеров, системы планирования корпоративных ресурсов или других систем финансового управления, таких как унаследованные пользовательские приложения. Данные, собранные у дочерних компаний, франшизных предприятий и будущих партнеров, могут включать в себя, например, данные о счетах-фактурах, платежах и управлении денежными средствами. Данные структурированы для дополнительной обработки и анализа, и целостность структурированных данных верифицируется и защищается для предотвращения фальсификации. Со временем, данные отправляются в систему управления данными DMS, в другом варианте осуществления - для фильтрации/преобразования, извлечения/аннотирования, выполнения корреляции, согласования, классификации и хранения.

В частности, собранные данные будут получены и обработаны в режиме реального времени и направлены в систему управления данными DMS. Система управления данными DMS в данном варианте осуществления включает в себя модуль фильтрации и преобразования, модуль извлечения/аннотирования, модуль выполнения корреляции и модуль классификации. Также в системе управления данными DMS находится хранилище данных и хранилище оперативных данных. Система управления данными DMS отвечает за фильтрацию и преобразование данных, собранных и зафиксированных датчиками, устройствами сбора данных, дочерней компанией, франшизным предприятием и/или будущими партнерами (которые могут быть защищенными и кластеризованными); извлечение и аннотирование отфильтрованных и преобразованных данных; выполнение корреляции извлеченных и аннотированных данных; и классифицирование коррелированных данных. Классифицированные данные затем отправляются в хранилище данных и хранилище оперативных данных на хранение.

Система управления данными DMS также отвечает за передачу (и хранение) данных, сохраненных в ее хранилище данных и хранилище оперативных данных, в интерфейс акцизной платформы. Интерфейс акцизной платформы включает в себя, например, модуль идентификации триггера налога, модуль представления оперативной отчетности, модуль соответствия ключевого показателя эффективности (KPI) требованиям налогового законодательства и модуль построения сводных данных. Интерфейс акцизной платформы является границей между системой управления данными DMS и платформой возмещения акцизного налога. Интерфейс акцизной платформы осуществляет вычисление и форматирование расчетных показателей акцизного налога на основании большого разнообразия данных, включая объемные оперативные и финансовые данные. Вычисленные и отформатированные данные идентифицируются как налогооблагаемая сделка для последующего согласования, и обратная связь по показателям KPI, относящимся к налогам, отправляются в информационную панель KPI (описана ниже) в платформе возмещения акцизного налога. В частности, интерфейс акцизной платформы идентифицирует налогооблагаемые сделки для согласования в модуле налоговой идентификации, осуществляет вычисление и форматирование данных в модуле представления оперативной отчетности, предоставляет обратную связь по форматированным данным в модуле соответствия требованиям налогового законодательства и создает сводные данные на выходе из модуля налоговой идентификации, модуля представления оперативной отчетности и модуля соответствия требованиям налогового законодательства в модуле построения данных. Дополнительно интерфейс акцизной платформы получает данные (которые могут быть защищенными и кластеризованными), созданные системой управления данными DMS, тем самым позволяя субъекту сравнивать и согласовывать по меньшей мере одно из следующего: акцизный налог, взимание налогов и показатель KPI, созданный другим субъектом/другими субъектами. Этот интерфейс позволяет системе управления целостностью IMS обеспечивать встроенный перекрестный контроль и согласование данных, относящихся к налогам, между независимыми источниками отчетов. В итоге это обеспечивает прозрачность уплаты налогов для того, чтобы можно было свести к минимуму мошенничество. В качестве примера, налоговые показатели KPI и соответствующие налоговые данные представляют собой слож-

ные данные и должны быть адаптированы в режиме почти реального времени, согласно особым правилам, предусмотренным государственными принципами налогообложения. Например, если объем проданной нефти составляет 5000 баррелей, величина налога может составлять 5%. Когда объем проданной нефти составляет 500000 баррелей, величина налога составляет всего 3%. Платформа возмещения налога соблюдает все правила обработки данных, предоставленных системой DMS и относящихся к налогам, для создания, на основании предоставленных правил, соответствующих налогов, которые должны быть уплачены. Другой пример происходит в секторе даунстрим, где заправочная станция может декларировать количество продаж в долларах, не соответствующее объему продукта, распределенному в данное место.

Платформа возмещения акцизного налога, сопряженная с IMS, включает в себя, без ограничения, обработчик корреляции финансовых сделок, модуль анализа данных (например, описательного, диагностического, упреждающего и предписывающего анализа), информационную панель KPI или отчетную информационную панель, модуль обнаружения, отправки отчетов и публикации специализированных данных, другой модуль системного интерфейса, веб-портал, мобильные приложения, обработчик рабочего процесса, архив сделок, обработку сделок и репозиторий сделок. Платформа возмещения акцизного налога получает сводные данные из интерфейса акцизной платформы (который получил защищенные и точные данные, относящиеся к налогам, от DMS, являющейся частью IMS) для идентификации и согласования несоответствий между сводными данными, автоматически созданными интерфейсом акцизной платформы, и соответствующей налоговой декларацией, созданной независимо или вручную (например, на уровне дочерних компаний или корпоративном уровне или любым субъектом, участвующим в цепочке поставок нефти и газа). Платформа возмещения акцизного налога также содержит репозиторий сделок, сохраняющий идентифицированные и согласованные данные от обработчика корреляций, процессор сделок для связывания идентифицированных и согласованных данных, архив сделок, сохраняющий архивированные идентифицированные и согласованные данные от обработчика корреляций; и модуль анализа данных, получающий обработанные и архивированные данные для описательного, диагностического, упреждающего и предписывающего анализа. Данные, отправленные в модуль анализа данных, могут быть введены в модуль упреждающего и предписывающего анализа (приложение для упреждающего и предписывающего анализа), использующий машинное обучение для идентификации последовательности измерений (фиг. 8A) или вычисленных данных, классифицированных как "события", требующие какого-либо действия и/или отчетности. Классификация события, ранее предоставленного системой управления данными, может быть подтверждена (человеком-оператором или машиной) и результаты отправлены в модуль упреждающего и предписывающего анализа для улучшения обучающего набора данных для алгоритма обучения, позволяя ему "обучаться" с течением времени. С помощью машинного обучения система управления целостностью IMS научится определять, какая последовательность измерений событий, взятых в совокупности, будет обозначать появление определенного события или кластера событий. С помощью "выученных" событий система способна применять исторические данные и улучшать точность с течением времени. Налоговые отчеты от платформы возмещения акцизного налога, предоставляемые дочерними нефтегазовыми компаниями, партнерами и франшизными предприятиями, могут включать в себя информацию о прошлых декларациях, их консолидациях и прогнозах на будущее. Соответственно, платформа возмещения акцизного налога позволяет осуществлять управление налогами с внешним интерфейсом для доступа налогоплательщика, объединенной налоговой документацией и репозиторием объема производства и согласования, встроенным модулем анализа данных и отчетной информационной панелью для налогового ведомства, интегрированной и централизованной системой для управления и взимания акцизного налога на нефть и газ, и для идентификации и согласования несоответствий между налоговыми документациями, объемами производства и оперативными отчетами, тем самым предоставляя эффективное взимание акцизного налога. В частности, в одном варианте осуществления, на стадии согласования налога, система автоматически выполняет проверку и перепроверку созданной вручную декларации, сравнивая ее с автоматически собранными данными (и преобразованными защищенным образом и используемыми для создания применимых кластеризованных данных, относящихся к налогам, способных создать защищенную и юридически действительную налоговую декларацию с целью верификации). Необходимо отметить, что одно определенное преимущество IMS согласно настоящему изобретению, при сопряжении с платформой возмещения налога посредством платформы акцизного налога, заключается в качестве данных, предоставленных указанной акцизной платформе. IMS не только собирает данные защищенным образом из различных источников, но также создает защищенные и точные данные, применимые для создания защищенных и надежных кластеризованных данных и отчета, применимых для эффективного повторного взимания налога и исправления несоответствий в цепочке поставок нефти и газа. IMS также обладает преимуществом, позволяющим на корпоративном уровне эффективно контролировать активность всех участников в цепочке поставок (дочерние компании, франшизные предприятия и т.д.) и эффективно управлять ими. Все защищенные собранные данные, предоставленные системой IMS корпоративному уровню, будут применяться для создания защищенного и надежного отчета и KPI для эффективного сравнения с отчетами и KPI, предоставленными на уровне дочерних компаний или на уровне франшизных предприятий. Благодаря сравнению надежного и защищенного отчета, пре-

доставленного системой IMS на корпоративном уровне, с отчетами от дочерних компаний и франшизных предприятий, эффективное управление внутри цепочки поставок нефти и газа позволит корпоративному уровню лучше увидеть неправильные или неэффективные элементы, а также увидеть способы исправления несоответствий в цепочке поставок нефти и газа.

На фиг. 6А показана примерная схема процесса маркировки продукта согласно системе. На этапе 700 создается идентификатор продукта с помощью вышеописанных технологий. Идентификатор продукта фиксируется в репозитории информации на этапе 702, и продукт маркируется идентификатором продукта на этапе 704. На этапе 706 информация о ресурсе (продукте) и соответствующий идентификатор продукта сохраняются вместе в репозитории и связываются друг с другом для последующего использования, например для последующей аутентификации продукта при его движении по цепочке поставок. На фиг. 6В показана примерная схема процесса отслеживания и аутентификации события согласно системе. На этапе 710 продукт движется по цепочке поставок, делая несколько остановок в разных сектора (например, апстрим, мидстрим и даунстрим). В каждом из секторов, когда происходит установленное событие (712), продукт идентифицируется с помощью устройства для сбора данных (например, датчика). Устройство для сбора данных, как описано, идентифицирует идентификатор продукта (маркировку) на этапе 714 и отчет о собранной информации подается для дальнейшей аутентификации на этапе 716. Доступные на рынке или незащищенные устройства для сбора данных (т.е. устройства, не способные считывать защищенное событие (как определено ниже)), считывают маркировку продукта, так что верификация события не включает в себя аутентификацию с помощью идентификатора или аутентификатора защищенного объекта. Устройство для сбора защищенных данных, с другой стороны, представляет прошедшее аутентификацию и выделенное устройство, считывающее маркировку продукта таким образом, чтобы идентификатор защищенного объекта или аутентификатор продукта могли быть идентифицированы и использованы для проверки и аутентификации продукта на протяжении цепочки поставок. В связи с этим идентификация и аутентификация продукта при появлении события обозначены термином "защищенное событие".

Другими словами, событие, в результате которого информация была отправлена в систему, является "защищенным" благодаря тому факту, что устройство для сбора данных способно идентифицировать и верифицировать надлежащее соответствие продукту идентификатора или аутентификатора продукта. Например, защищенный идентификатор или аутентификатор объекта могут представлять собой маркировку ресурса, идентифицированного и связанного с событием.

Далее описан пример процесса, описанного на фиг. 6А и 6В. Цепочка поставок включает в себя "партнеров" в трех различных секторах: апстрим-партнера, мидстрим-партнера и даунстрим-партнера. Апстрим-партнер отправляет событие в сервер обнаружения, указывающее на будущее выполнение поиска и разведки продукта в цепочке поставок. Когда апстрим-партнер закончил производство продукта, получив устойчивый продукт (например, нефть или топливо), продукт отмечается идентификатором и аутентификатором продукта. Идентификатор и аутентификатор продукта, соответствующие продукту/продуктам, сохраняются в репозитории, и другое событие создается и отправляется в сервер обнаружения, указывая на то, что продукт был произведен и направлен к мидстрим-партнеру. После получения мидстрим-партнером продукт сканируется защищенным устройством наблюдения (например, датчик) для верификации и аутентификации продукта с помощью идентификатора и аутентификатора продукта, и мидстрим-партнер передает продукт далее, к даунстрим-партнеру. Другое событие отправляется в сервер обнаружения, указывая на то, что мидстрим-партнер отгрузил продукт даунстрим-партнеру. После получения даунстрим-партнером следующее событие отправляется в сервер обнаружения, указывая на получение продукта, и продукт снова может быть верифицирован и аутентифицирован на протяжении цепочки поставок путем идентификации идентификатора и аутентификатора продукта с помощью защищенного устройства наблюдения (например, датчика).

События, отправленные и сохраненные в сервере обнаружения, который может представлять собой один и тот же или разные серверы обнаружения, могут быть рассмотрены партнерами в цепочке поставок с помощью известных технологий, таких как база данных событий, очереди и таблицы регистрации данных. События могут быть образованы в форме разнообразных классов, в зависимости от продукта, проходящего по цепочке поставок. Партнеры также могут получать уведомления и сообщения с помощью защищенных веб-отчетов, отправки предупреждений и отправки сообщений по электронной почте, SMS или с помощью любых других средств, известных специалисту в данной области. Когда партнер хочет выполнить аутентификацию и верификацию продукта, в систему может быть отправлен запрос посредством платформы 605 сериализации и интерфейса, описанных выше. Помимо типичной информации, такой как тип события, дата события, имя партнера и т.д., партнер также может запрашивать или автоматически получать информацию об аутентичности продукта (при условии использования защищенного устройства наблюдения для считывания идентификатора и аутентификатора продукта). В связи с этим продукт можно сравнить с информацией, сохраненной в платформе 605 сериализации и интерфейса. Если сравнение выявило соответствие, то продукт может быть верифицирован, как описано выше.

На фиг. 7 показана примерная блок-схема создания защищенного события согласно системе. Примерная система 800 защищенных событий включает в себя различные компоненты, например защищен-

ное устройство 802 наблюдения (например, датчик), продукт 810 с маркировкой 804 (например, нефть или топливо с маркировкой), защищенное событие 806 и репозиторий 808. Различные компоненты могут быть соединены друг с другом посредством проводной или беспроводной связи и могут составлять часть одной и той же сети или разных сетей (не изображены). По мере перемещения продукта по цепочке поставок защищенное устройство наблюдения собирает данные о продукте. Собранные данные включают в себя информацию о стандартном событии и информацию о защищенном событии. Собранные данные образуют защищенное событие 806, передаваемое в репозиторий 808 для хранения. Другой раскрытый вариант осуществления описывает хранение защищенного события 806 в репозитории 808, при этом изобретение не ограничено таким вариантом осуществления. Вместо этого защищенное событие 806 может храниться в защищенном устройстве 802 наблюдения или в любом другом месте, доступном по сети.

Маркировка 804 на продукте 810 включает в себя информацию о стандартном событии и информацию о защищенном событии. В одном варианте осуществления маркировка 804 включает в себя информацию о стандартном событии и о защищенном событии. Другими словами, маркировка может включать в себя различные химические составы или включать в себя вспомогательные идентификаторы, идентифицирующие информацию о стандартном и/или защищенном событии. В другом варианте осуществления информация о стандартном событии отделена от информации о защищенном событии. Защищенное событие 806 представляет собой любую комбинацию данных (маркировки), в которых присутствует информация о защищенном событии. Например, первый идентификатор продукта идентифицирует информацию о стандартном событии (первая маркировка или отсутствие маркировки), и аутентификатор или второй идентификатор продукта (в форме маркировки) идентифицирует информацию о защищенном событии (вторая маркировка). Тем не менее, следует понимать, что изобретение не ограничено описанным вариантом осуществления, который по своей сути является примерным. Защищенное устройство 802 наблюдения осуществляет аутентификацию маркировки 804 и может добавлять подпись или шифрование в собранные данные и сохраняет их в качестве защищенного события 806 в репозитории 808.

На фиг. 8 показана примерный глобальный репозиторий согласно системе. Глобальный репозиторий 900 включает в себя, например, репозиторий R1, репозиторий R2 и репозиторий Rn. Репозитории R1, R2 и Rn могут быть расположены в одной и той же сети или в разных сетях и могут быть связаны с одним и тем же ответственным хранителем или с разными ответственными хранителями (например, ответственными хранителями в секторах апстрим, мидстрим и даунстрим) на протяжении цепочки поставок S. В изображенном примере несколько событий происходят по мере движения объекта по цепочке поставок S. Событие в примерном варианте осуществления представлено буквенно-цифровым обозначением En, где n является целым числом, представляющим номер события. В данном случае всего изображено семь событий (E1-E7). События En со звездочкой ("*") представляют защищенное событие, а события без звездочки представляют стандартное или незащищенное событие. Как описано выше, стандартное событие создается, когда устройство для сбора стандартных данных (обычное устройство наблюдения NOD) считывает информацию о стандартном событии, идентифицированную на продукте в цепочке поставок S. С другой стороны, защищенное событие создается, когда устройство для сбора защищенных данных (защищенное устройство наблюдения SOD) считывает информацию о стандартном событии и информацию о защищенном событии на продукте в цепочке поставок S, при этом данная информация проходит аутентификацию защищенным устройством наблюдения SOD. Как описано, NOD и SOD могут представлять собой датчики или любое устройство, способное идентифицировать маркировку продукта (или любые другие параметры, собранные защищенным устройством наблюдения). В изображенном варианте осуществления репозиторий R1 получает защищенные события E1* и E3*, собранные из защищенного устройства наблюдения SOD, и стандартное событие E2, собранное из обычного устройства наблюдения NOD. Репозиторий R2 получает стандартное событие E4, собранное обычным устройством наблюдения NOD, и репозиторий Rn получает защищенное событие E6*, собранное защищенным устройством наблюдения SOD, и стандартные события E5 и E7, собранные обычным устройством наблюдения NOD.

В значительной степени, способность выполнять аутентификацию продукта с помощью устройства для сбора защищенных данных улучшает способность обнаружения контрафактных продуктов и/или продуктов с замененным составом или фальсифицированных продуктов в определенном местоположении в цепочке поставок S. Другими словами, в системе управления настоящего изобретения обнаружение аутентификации может происходить в определенном местоположении, поскольку защищенные события основаны на считывании идентификатора или аутентификатора продукта (например, маркировки) и поскольку разные защищенные устройства для сбора данных могут создавать разные защищенные события на основании идентификатора или аутентификатора продукта. В традиционных системах управления, использующих, например, EPCIS и традиционную (обычную) технологию датчиков, контрафакция и/или замена состава и/или изменение маршрута транспортировки и фальсификация продуктов, ресурсов или товаров не могут быть обнаружены в определенном местоположении в цепочке поставок S и даже не могут быть идентифицированы как происходящие в некотором местоположении между двумя точками (т.е. двумя точками устройств для сбора данных) в цепочке поставок S. Причина этого заключается в том, что событие, собранное в традиционной системе, как описано выше, является стандартным или незащищенным событием, в котором не отсутствует дополнительный уровень аутентификации. Ис-

пользуя систему глобального управления поставками согласно настоящему изобретению, возможно получить местоположение фальсификации и/или контрафакции более быстрым образом, чем в традиционных системах управления, благодаря дополнительному уровню аутентификации системы глобального управления поставками согласно настоящему изобретению. В действительности, поиск местоположения фальсификации и/или контрафакции может быть значительно ускорен, поскольку он может быть ограничен частью цепочки поставок, находящейся между устройством для сбора защищенных данных, где аутентификация отслеживаемого продукта (или данных, собранных из SOD) завершилась неудачей, и расположенным непосредственно перед ним устройством для сбора защищенных данных в цепочке поставок S (т.е. между двумя точками сбора данных SOD).

На фиг. 9 показана примерная схема системы глобального управления согласно описанному варианту осуществления. Система глобального управления GMS включает в себя, без ограничения, центр управления CCC, систему управления данными, модуль интеграции данных, пользовательский интерфейс, интерфейс шлюза, датчики, устройства сбора данных и систему глобального управления поставками (описанную здесь), используемые для сбора данных из секторов апстрим, мидстрим и даунстрим. Система глобального управления GMS также может включать в себя или охватывать внешние ресурсы, такие как ERP-системы, системы управления месторождением и ресурсами, упреждающие и предписывающие приложения, системы управления событиями, основанные на доказательном подходе, и существующие наследственные системы. Следует понимать, что система глобального управления GMS не ограничена описанными компонентами и не обязана включать в себя каждый из компонентов, изображенных в неограничивающем и примерном варианте осуществления. Например, система глобального управления поставками или система диспетчерского управления и сбора данных (ICS, такая как SCADA) может заниматься сбором данных вместо интерфейса шлюза. Как указано выше, данные могут храниться в одном репозитории или в нескольких репозиториях.

Система глобального управления управляет нефтегазовыми ресурсами защищенным образом (или незащищенным образом, при желании) путем контроля над нелегальной деятельностью в цепочке поставок, предупреждения органов власти и/или уполномоченного персонала и реагирования на незаконную деятельность соответствующим образом. Система глобального управления GMS собирает неоднородные, неструктурированные и разрозненные данные из датчиков, устройств сбора данных и вспомогательных систем наблюдения, а также предоставленные устройством SOD, включая систему глобального управления поставками, в секторах апстрим, мидстрим и даунстрим нефтегазовой инфраструктуры (трубопроводов), для хранения и обработки собранных данных, используя сведения систем нефтегазовой инфраструктуры. Данные структурированы для дополнительной обработки и анализа, и целостность структурированных данных верифицируется и защищается для предотвращения фальсификации. Со временем, как описано выше, данные отправляются в центр управления CCC для того, чтобы персонал отреагировал на кражу или подобные происшествия, связанные с эксплуатацией. Этот процесс позволяет быстрее реагировать по сравнению с современными системами, а также предоставлять доказательную базу, содержащую материальное доказательство, которое может быть принято в суде, действующем по нормам статутного и общего права, для поддержки обвинения преступников. Например, беспилотные летательные аппараты могут использоваться для предоставления доказательства, полученного на месте преступления, свидетельствующего о том, что событие имело место.

Система управления целостностью IMS собирает неоднородные, неструктурированные и разрозненные данные из датчиков, устройств сбора данных и вспомогательных систем наблюдения, включая данные из системы глобального управления поставками, а также предоставленные устройством SOD, включая систему глобального управления поставками, в секторах апстрим, мидстрим и даунстрим нефтегазовой инфраструктуры (трубопроводов), для хранения и обработки собранных данных, используя сведения систем нефтегазовой инфраструктуры. В отличие от GMS, собранные данные структурируют для дополнительной обработки и анализа и целостность структурированных данных верифицируют и защищают для предотвращения фальсификации, и данные кластеризуют таким образом, чтобы все данные, относящиеся к теме налогов или к теме KPI, или к управлению дочерними компаниями или франшизными предприятиями на корпоративном уровне, создавались и использовались для создания защищенной налоговой отчетности, защищенного отчета для того, чтобы корпоративный уровень эффективно управлял разными субъектами в цепочке поставок нефти и газа, позволяя осуществлять согласование данных, относящихся к налогам и KPI, и исправлять возможные существующие несоответствия в цепочке поставок нефти и газа.

Несмотря на свои разные цели, обе системы полагаются на общие признаки, такие как, например, шлюз или модули BRE, или кластеризованные защищенные события, для создания предупреждений или защищенного отчета или защищенных данных, относящихся к налогам. Тем не менее, эти системы GMS и IMS будут в значительной степени полагаться на защищенные и точные данные, предоставленные устройством SOD, для их эффективного использования для собственных целей и функций. Предупреждения и вмешательство для системы GMS, например, повторное взимание налога или согласование данных, относящихся к налогам, или исправление несоответствий для IMS. Чем больше защищенных данных и надежных данных будет в системе, тем лучше будут кластеризованные события и соответствующий за-

щищенный отчет (KPI, расчетный показатель налога и величина или согласование налога) в цепочке поставок нефти и газа.

В частности, собранные данные будут получены и обработаны в режиме реального времени и направлены в центр управления ССС (который может иметь форму физического командного центра управления и/или приложения, функционально независимого от персонала, или любой их комбинации) для соответствующего отображения персоналу командного центра. Структурированные данные будут анализироваться согласно вычислительным моделям и/или алгоритмам для идентификации событий, где события могут представлять собой происшествия, связанные с эксплуатацией, такие как незаконная деятельность, описанная выше, а также проблемы, связанные с эксплуатацией, которые могут быть идентифицированы и отображены операторам в режиме реального времени. Параллельно с этим (или в другое время) структурированные данные и события введены в модуль упреждающего и предписывающего анализа (приложение для упреждающего и предписывающего анализа), использующий машинное обучение, как описано выше, для идентификации последовательности измерений или вычисленных данных, классифицированных как "события", требующие какого-либо действия и/или отчетности. Классификация события, ранее предоставленного системой управления данными, может быть подтверждена (человеком-оператором или машиной) и результаты отправлены в модуль упреждающего и предписывающего анализа для улучшения обучающего набора данных для алгоритма обучения, позволяя ему "обучаться" с течением времени. С помощью машинного обучения система глобального управления или система управления целостностью научится определять, какая последовательность измерений событий, взятых в совокупности, будет обозначать появление определенного события или кластера событий. С помощью "выученных" событий система способна применять исторические данные и улучшать точность с течением времени. Точности также может способствовать осуществление человеком или беспилотным летательным аппаратом верификации на месте события и использование предупреждений, созданных системой.

Система управления данными, подобно центру управления ССС, также может обмениваться данными с модулем упреждающего и предписывающего анализа, который будет применять машинное обучение к структурированным данным и событиям в качестве обучающих наборов для классификации событий, которые могут быть расценены как последовательность измерений. Модуль упреждающего и предписывающего анализа предоставляет информацию для идентификации вероятных событий (с переменной степенью вероятности) в будущем, или происходящих событий, которые могут быть отправлены в качестве событий в центр управления ССС. Модуль упреждающего и предписывающего анализа также может предписывать ответную реакцию на событие, которая вероятнее всего приведет к положительному результату, на основании истории событий. Подобным образом распознанные (или известные) тенденции, возникающие с течением времени, могут быть использованы для улучшения кластеризованных событий для более точного создания предупреждений в центре управления ССС.

На фиг. 10 показана примерная схема интерфейса согласно одному варианту осуществления изобретения. Как изображено, интерфейс (шлюз) получает данные из одного или нескольких различных источников. Например, данные, собранные из датчиков в секторах апстрим, мидстрим и даунстрим и обработанные системами SCADA, передаются в интерфейс шлюза. В альтернативном варианте осуществления шлюз заменяет промышленную систему управления (такую как SCADA) и собирает данные непосредственно из датчиков в секторах апстрим, мидстрим и даунстрим или из других источников, например из системы глобального управления поставками (использующей вышеупомянутое защищенное устройство наблюдения). Интерфейс шлюза преобразовывает (например, сортирует, форматирует и модифицирует) собранные данные в защищенные и отформатированные данные, совместимые с системой и, в частности, с модулем интеграции данных, перед их отправкой в систему управления данными для анализа системой глобального управления или в системе управления целостностью.

На фиг. 11A-11D изображены примерные измерения датчиков и датчики, собирающие данные на протяжении цепочки поставок согласно описанному варианту осуществления. Собранные данные обрабатываются системой управления целостностью, и кластеризованные и структурированные данные создаются или непосредственно публикуются в качестве налогового отчета, финансового отчета, отчета о показателе KPI, защищенного бланка налоговой декларации или любого отчета, применимого для подготовки итоговой налоговой декларации. После того, как определенная последовательность измерений (или последовательность событий), связанная с описанием событий, стала известной (т.е. выучена приложением для упреждающего и предписывающего анализа), события могут помечаться в режиме реального времени баллом вероятности, обозначающим вероятность того, что последовательность разворачивающихся измерений создаст в результате идентифицируемое событие (событие налогообложения или последовательность, подлежащих налогообложению). На фигурах заштрихованные прямоугольники представляют величины, полученные от заданного датчика. На фиг. 11A показано примерное количество датчиков 1 ... m, выполненных с возможностью сбора последовательности событий. На фиг. 11B, 11C и 11D показана примерная последовательность событий, в которой данные, собранные с течением времени t, представляют низкую вероятность, среднюю вероятность и высокую вероятность, соответственно, возникновения события (обозначенной здесь термином "вероятность события"). Вероятность события от-

правляется в систему управления данными DMS, при этом интерфейс акцизной платформы и платформа возмещения акцизного налога идентифицируют событие, подлежащее налогообложению, такое как "500 баррелей топлива продано в месте X в заданную дату".

Для улучшения эффективности с помощью модуля упреждающего и предписывающего анализа, на основании прошлых событий, содержащихся в исторических данных измерений и событий, из исторических данных могут быть созданы модели и использованы для способствования прогнозированию будущих событий (т.е. событий, подлежащих налогообложению) перед тем, как датчики и устройства сбора данных начнут регистрировать данные. Используя эти упреждающие данные, платформа возмещения акцизного налога (сопряженная с системой DMS в системе IMS, как описано на фиг. 5) и персонал, работающий на платформе возмещения акцизного налога, могут быть предупреждены о прогнозируемых областях событий, подлежащих налогообложению, идентифицированных системой, использующей данные в системе, такие как время суток, день недели, месяц или определенные даты, предыдущие последовательности событий и т.п. Из вышеописанного становится понятно, что система управления целостностью IMS способна фиксировать развитие событий, относящихся к налогам, и соединять их вместе для предоставления истории для анализа и улучшения анализа данных в системе управления данными DMS. На основании предыдущих сведений о событиях, произошедших в прошлом, исторических данных и верификации того, что события на самом деле имели место, таких, как данные об объемной производительности насоса, количестве транспортированного топлива и количестве баррелей топлива, данные о платежах и управлении денежными средствами и создании счета-фактуры, будущие события могут быть более точно спрогнозированы и сами события могут быть лучше истолкованы при осуществлении контроля и анализа. Дополнительно, благодаря тому, что система управления целостностью IMS по своей сути основана на прогнозах и предписаниях, она способна снизить уровень коррупции, например, рабочий персонал в дочерней компании, сторонней компании, франшизном предприятии и т.д. с меньшей вероятностью предоставит фальсифицированные налоговые документы, учитывая осуществление контроля и управления платформой возмещения акцизного налога. Соответственно, людям, вовлеченным в незаконную деятельность, станет все сложнее избегать обнаружения путем удаления данных, изменения данных, подкупа персонала, контролирующего данные, и т.д.

В значительной степени, для предотвращения таких типов ситуаций, система управления целостностью предоставляет: защищенные и не поддающиеся подделке данные, которые не могут быть удалены, предупреждения, основанные на корреляции кластеризованных событий, уведомляющие о высокой вероятности фальсификации (например, фальсификации информации, относящейся к налогам), при этом указанная фальсификация будет отображена оператору и зафиксирована в виде предупреждений, которые также не поддаются подделке и не могут быть удалены. В качестве альтернативы или дополнения, сама система может вмешиваться вместо персонала для идентификации и отправки срочной информации внешним органам власти, таким как налоговое ведомство, юридическое лицо, управляющее корпорацией, и т.д. Соответственно, роль системы заключается в предоставлении альтернативы человеческим ошибкам и некомпетентности при обнаружении такой фальсифицированной информации.

Дальнейшие неограничивающие примеры системы управления целостностью IMS описаны ниже применительно к секторам мидстрим и даунстрим. В секторе мидстрим незаконная деятельность, связанная с налогами, обычно осуществляется путем модификации собранных данных и/или фальсификации записей и материалов, таких как налоговые отчеты и налоговые декларации. Например, при получении квитанции в ходе налогооблагаемой сделки, таком как получение квитанции об оплате для приобретения 500 баррелей нефти, квитанция может быть подделана таким образом, чтобы акцизный налог был сведен к минимуму. При этом в ходе подготовки налогового отчета информация, относящаяся к налогооблагаемой сделке, будет отражать подделанную квитанцию. В качестве мер противодействия и согласно целям системы управления целостностью IMS, на емкости с нефтью могут быть установлены несколько датчиков и/или устройств сбора данных, которые будут осуществлять контроль и сбор данных из них. Например, каждая емкость с нефтью может содержать датчик, обнаруживающий перемещение емкости с нефтью из распределительного центра в розничную торговую точку, обозначающее осуществление покупки емкости/емкостей с нефтью. Система управления целостностью IMS может быть использована для осуществления контроля и сбора данных, относящихся к сделке, по мере ее осуществления. Собранные данные из датчиков и устройств сбора данных будут отправлены в соответствующий шлюз (фиг. 8) или промышленную систему управления ICS и переданы в систему управления данными DMS и далее, в центр управления CCC, как описано выше в настоящей заявке. Дополнительно, собранные данные должны быть обновлены таким образом, чтобы они могли быть истолкованы для предоставления выводов и рекомендаций. Например, если датчик(и) или устройство/устройства сбора данных обнаруживают всего лишь покупку емкости/емкостей с нефтью один раз в неделю, датчик(и) и устройство/устройства сбора данных не могут фиксировать действие покупки на протяжении остальных шести дней в неделю. С другой стороны, если покупка емкости/емкостей с нефтью измеряется ежедневно, дважды в день, датчик(и) и устройство/устройства сбора данных смогут точнее обнаруживать и рассчитывать покупку емкости/емкостей с нефтью (или любой другой тип данных), обозначающую осуществление налогооблагаемой сделки или деятельности. Беспилотный летательный аппарат или персонал, связанные с определени-

ем местоположения датчика/датчиков и устройства/устройств сбора данных, могут попеременно или одновременно контролировать региональное местоположение, могут собираться изображения из локальной камеры, и система может быть уведомлена об осуществлении деятельности.

Другой неограничивающий пример данных в секторе мидстрим представляет собой автоцистерну, транспортирующую сырую нефть и нефтепродукт. В данном примере собранные данные представляют собой GPS-информацию, созданную пройденным маршрутом автоцистерны, и объем содержимого автоцистерны. Если данные, собранные с течением времени, указывают, например, на то, что автоцистерна стоит на месте дольше, чем ожидалось, или что объем содержимого автоцистерны изменился, это может указывать на осуществляемую или на осуществленную незаконную деятельность. Например, изменение объема содержимого автоцистерны может указывать на то, что некто пытается уклониться от отправки отчета о событии как о налогооблагаемой сделке. В другом примере автоцистерна может остановиться в зоне ночного отдыха. Поскольку известно, что в этих зонах осуществляется регулярная остановка в течение длительного периода, датчики объема на автоцистерне могут быть активированы для осуществления контроля над изменением содержимого автоцистерны. Любое изменение, обнаруженное датчиками, может быть направлено по системе управления данными DMS в центр управления CCC после выполнения анализа данных. Обработчики обучения системы получат сведения об области и ожидаемой деятельности в этой зоне, и применят эти сведения в дальнейшем анализе. Как и ранее, подобная деятельность может указывать на то, что некто пытается уклониться от определенного события, последствием которого является уплата налогов.

В секторе даунстрим предоставлен неограничивающий пример, в котором собранные данные включают в себя объем, произведенный на перерабатывающем заводе. Данные об объеме могут быть связаны, например, с количеством автоцистерн, необходимым для транспортировки содержимого автоцистерн (топлива) в розничные магазины. Подразумевается, что после прибытия топлива в розничные магазины оно загружается в цистерны магазинов для хранения. В данном случае, происходит передача объема и сбыт топлива. Датчики и устройства сбора данных в таком случае могут использоваться для измерения изменений соответствующих объемов и измерения наличных средств, образованных продажей топлива. Если объемы и продажи не совпадают, это может указывать на незаконную деятельность, такую как создание фальсифицированных документов для того, чтобы уклониться или избежать события, подлежащего налогообложению. Эта информация также может быть применима для повторного взимания или согласования налогов, для оценки количества топлива, требуемого в конкретной области, и т.д. Как следует понимать, данные не только собираются, но также сохраняются в репозитории и преобразуются в сумму кластеризованных событий, которые могут быть связаны, использованы или проанализированы для предписывающего или упреждающего действия.

На фиг. 12 показана примерная схема интерфейса согласно одному варианту осуществления изобретения. Интерфейс, который в данной заявке также обозначен терминами "шлюз" или "интерфейс шлюза", связывает датчики данных, расположенные на протяжении секторов апстрим, мидстрим и даунстрим, с внешними источниками, такими как сервисная шина предприятия ESB или система глобального управления данными, посредством модуля интеграции данных. Как изображено, шлюз разделен на три уровня, включающие в себя: (1) компьютер (например, для подписания и хранения), обменивающийся данными с промышленными системами управления (такими как SCADA, OPC, AS-i MODBUS и Ethercat). Драйверы могут представлять собой комбинацию физических интерфейсов и программного обеспечения, (2) обработчик бизнес-правил (BRE), осуществляющие корреляцию, защиту, аутентификацию, фильтрацию, согласование, обеспечивает невозможность подделывания и создает данные, содержащие ключевые значения. BRE, на основании собранных данных, будет создавать ассоциации с данными, собранными в объекты, создавать события, основанные на отсутствии целостности объектов, создавать предупреждения, основанные на событиях, или события, основанные на пороговых значениях или на бизнес-правилах или на тенденциях, и (3) интерфейсы, сопряженные с внешними системами с помощью, например, HTTPS, SSL или любого другого программного или аппаратного протокола.

Интерфейс шлюза предоставляет, помимо других признаков, механизм для преобразования собранных данных в формат, имеющий большую защиту и совместимый с внешней системой, в которую будут отправлены преобразованные данные или объекты или события или предупреждения, созданные в шлюзе. Например, интерфейс шлюза будет обеспечивать защиту данных, собранных из датчиков и/или устройств сбора данных, а также форматирование собранных данных для придания им совместимости с системой интеграции данных перед их использованием в системе глобального управления или в системе управления целостностью, особенно на уровне системы управления данными (DMS). Интерфейс шлюза сопрягается с внешними системами с помощью, например, протоколов, таких как HTTPS, SSL и т.д. Внешние интерфейсы включают в себя, без ограничения, сервисную шину предприятия ESB или промышленную систему управления ICS, такую как система управления шлюзом GMS, описанная здесь, системы осуществления сделок или системы осуществления финансовых сделок.

На уровне драйвера, драйверы, обменивающиеся данными с внешними системами, такими как система ICS, могут представлять собой аппаратное обеспечение, программное обеспечение или их комбинацию. Аппаратное обеспечение и программное обеспечение предпочтительно являются устойчивыми к

взлому и защищенными для того, чтобы предотвратить атаки на физическое аппаратное обеспечение, а также злонамеренные атаки на программное обеспечение, например осуществляемые хакерами, введением нежелательных данных и т.п. Данные, которые будут образованы и созданы в интерфейсе шлюза, будут более защищенными и будут обеспечивать улучшенные свойства в дополнение к данным, собранным из различных репозиториев данных, таких как SCADA или ICS. Защищенные и улучшенные данные затем будут предоставлены системе глобального управления или системе управления целостностью и будут способствовать созданию кластеризованных событий. Шлюз также будет верифицировать аутентичность данных, полученных из датчика/датчиков и устройства/устройств сбора данных, и отсутствия их искажения внешними источниками или другим образом. Другими словами, шлюз в первую очередь будет обладать способностью осуществлять аутентификацию получаемых данных перед защитой данных и добавлением дополнительных свойств. Это будет обеспечивать выполнение аутентификации данных, предназначенных для защиты и улучшения, перед их поступлением в систему глобального управления или в систему управления целостностью, и предотвратит отправку искаженных данных в систему глобального управления или в систему управления целостностью. Одна слабость существующих систем в цепочке поставок нефти и газа заключается в невероятно большом объеме данных. Если система становится загрязненной или зараженной поддельными, подложными, сфабрикованными или неточными данными, собранные данные не будут надежными и любые события или кластеризованные события, созданные в системе глобального управления или в системе управления целостностью, потенциально могут скомпрометировать предупреждения, созданные из кластеризованных событий. Соответственно, любые данные, предназначенные для доступа или использования в системе глобального управления или в системе управления целостностью (посредством модуля интеграции данных), с помощью шлюза, должны быть как можно более защищенными и точными. Пример выполнения аутентификации данных, которые будут введены в шлюз, заключается в том, чтобы собирать из датчиков, особенно SOD, или из нескольких временных интервалов информацию, которая должны быть собрана в короткий период времени, и верифицировать, чтобы собранные данные всегда имели одинаковую сущность (например, данные о температуре собираются десять раз в течение 30 секунд и величина практически не изменяется, в таком случае данные производят впечатление верных). Другой пример выполнения аутентификации или удостоверения точности данных заключается в добавлении к датчику электронной системы или механизма, защищающего данные от фальсификации или изменения маршрута транспортировки и защищающего датчик любыми способами, при этом данные, собранные из датчика и затем отправленные в шлюз, будут как можно более точными. Другой пример обеспечения точности данных заключается в: i) использовании датчика, защищенного от несанкционированных манипуляций; ii) сравнении данных с данными из других датчиков для того, чтобы убедиться, что они согласованы друг с другом (например, если температура повышается в одном датчике, повышается ли она в соседних датчиках? Как следствие, изменяется ли давление? и т.д., iii) обнаружении аномалий: применении машинного обучения к прошлым данным для обнаружения аномальных показаний датчиков.

Интерфейс шлюза собирает данные посредством физических интерфейсов, ведущих к промышленным датчикам, использующим промышленные протоколы связи, такие как OPC или Ethercat, или посредством виртуальных (т.е. программных) интерфейсов, ведущих к существующим системам контроля или управления, таким как SCADA. Интерфейсы приводятся в действие, например, с помощью программных драйверов, которые могут быть динамически загружены или выгружены в зависимости от физических или виртуальных требований. Например, при наличии физически соединенных трех устройств, приводимых в действие протоколом OPC, и одного устройства, приводимого в действие протоколом Ethercat, будут присутствовать три драйвера OPC и один драйвер Ethercat.

Когда данные достигают интерфейса шлюза, обработчик бизнес-правил BRE создает новые данные контроля путем корреляции собранных данных, фильтрации несущественных данных, например событий, не относящихся к безопасности, подтверждения правильности доступа для считывания/записи их в уровень драйвера в уровень интеграции (в обоих направлениях) и применения правил безопасности/доступа/аутентификации, при необходимости используя внешнюю систему. Тем не менее, следует понимать, что эти функции являются лишь примерными и BRE не ограничен такими функциями.

На уровне интерфейса, программное обеспечение в интерфейсе шлюза также может взаимодействовать с внешними системами на основании требований контроля. Например, интерфейс может включать в себя интерфейс электронной почты, web-интерфейс и т.д. Уровень интерфейса также может быть сопряженным с сервисной шиной предприятия ESB в качестве системы обмена сообщениями (например, использующей протокол, такой как REST по HTTPS) для интеграции данных из всех интерфейсов шлюза и внешних систем в компонент хранения данных системы глобального управления или в систему управления целостностью. Также следует понимать, что хотя на схеме изображен интерфейс, ведущий к интерфейсу шлюза, интерфейс шлюза также может быть непосредственно соединен или представлять собой часть системы глобального управления или часть системы управления целостностью.

Программное обеспечение сервисной шины предприятия ESB представляет собой систему обмена сообщениями, подобную продуктам MQueue Series и BMC Control компании IBM™. Программное обеспечение шины ESB, которое в настоящем варианте осуществления обозначено термином "модуль инте-

грации данных, составляющий часть системы глобального управления или системы управления целостностью" (хотя следует понимать, что ESB также может представлять собой отдельный объект), может представлять собой приложение, такое как Open ESB, разработанное компанией Sun Microsystems™, или WSO2 ESB.

Язык программирования, использующий технологию JAVA, может использоваться в качестве языка программирования для получения такого программного обеспечения.

Обработчик бизнес-правил BRE (второй уровень) действует в качестве преобразующей обработки собранных данных и применяет правила, которые могут быть выполнены таким образом, чтобы представлять определенный интересующий элемент, такой как потенциальное нарушение безопасности. BRE контролирует всю деятельность и точки измерения загруженных драйверов вместе с любыми физически или виртуально присоединенными устройствами. Благодаря доступу ко всем этим точкам в режиме реального времени BRE может создавать новые точки измерения или данные, применимые для создания кластеризованных событий в системе глобального управления или в системе управления целостностью. BRE, на основании собранных данных, также будет создавать ассоциации с данными, собранными в объекты, создавать события, основанные на отсутствии целостности объектов, создавать предупреждения, основанные на событиях, или события, основанные на пороговых значениях или на бизнес-правилах или на тенденциях. Например, точка измерения A на физически присоединенном устройстве (таком как датчик температуры) и точка измерения B (такая, как переменная из внешней программной системы SCADA) при определенных пороговых значениях могут создавать новые данные, основанные как на точке измерения A, так и на точке измерения B. Например, могут быть созданы новые данные C, где новые данные C представляют собой добавление к точкам измерения A и B и могут составлять событие. Это позволяет BRE коррелировать данные для лучшего понимания событий по мере их появления. События, созданные в шлюзе, основаны на данных, собранных из датчиков, устройств сбора данных или систем ICS. К этим данным, точность которых была проверена перед поступлением в шлюз, добавляются свойства для получения улучшенных данных.

В одном варианте осуществления, если датчики, устройства сбора данных или системы ICS не являются надежными или не способны проверить точность данных, проверка выполняется в шлюзе. События, созданные в шлюзе, будут применимы в системе управления данными DMS системы глобального управления или в системе управления целостностью для создания кластеризованных событий или надежного защищенного налогового отчета или защищенного KPI или для помощи в повторном взимании налога или возмещении налога или для исправления несоответствий (на основании того, через какую систему, GMS или IMS, они будут проходить). Кластеризованные события или надежный защищенный налоговый отчет или защищенный KPI или помощь в повторном взимании налога или возмещении налога или исправление несоответствий используются в системе глобального управления или в системе управления целостностью для создания и/или отображения предупреждений на уровне CCC и, в контексте настоящего изобретения, позволят эффективно мобилизовать соответствующую службу для устранения происшествий (например, полицию при краже, пожарную службу при взрыве и т.д.). С другой стороны, BRE также будет обладать способностью анализировать релевантность данных, собранных из датчиков, устройств сбора данных или систем ICS, если они хорошо структурированы в виде событий, собраны из датчиков SOD в цепочке поставок и если эти данные достаточно хорошо защищены, BRE отправит их непосредственно в модуль интеграции данных, для их последующей обработки в GMS или IMS для создания кластеризованных событий или надежного защищенного налогового отчета или защищенного KPI или для помощи в повторном взимании налога или возмещении налога или для исправления несоответствий.

BRE также может действовать автономно, если доступно достаточно физической и/или виртуальной информации для определения, на основании событий собранных данных, применимых для создания в системе глобального управления или в системе управления целостностью кластеризованных событий, не доверяя данным любой внешней системы, кластеризованные события будут применимы для определения действий, таких как оповещения, для идентификации или предупреждения о нарушениях безопасности и других действиях. Определение/определения кластеризованных событий управляется посредством модуля управления данными системы глобального управления или в системе управления целостностью как часть "обучающейся" сущности системы. BRE сохраняет эти данные и создает очередь из них, при необходимости, и шифрует или подписывает каждые данные для того, чтобы убедиться в том, что каждые данные являются полными, аутентичными, поддающимися учету, неопровержимыми и защищенными от внешнего доступа, модификации, нарушения и уничтожения. Следует понимать, что могут использоваться один или несколько признаков, ни одного или все эти признаки, в дополнение к другой форме функциональности. Зашифрованные данные потом могут быть доступны внешним системам на основании, например, профилей безопасности системы, запрашивающей информацию.

На фиг. 13 показан примерный вариант осуществления технологического маршрута интерфейса согласно одному варианту осуществления изобретения. Драйверы интерфейса шлюза собирают данные из разнообразных источников, включая, без ограничения, физические источники, программируемые логические контроллеры (PLC) и дистанционные терминалы (RTU) и любой другой тип источника. Обработ-

чик бизнес-правил BRE обрабатывает данные, коррелирует данные и создает из данных события или последовательность событий, как подробно описано выше. Данные и события необязательно могут быть подписаны аппаратным или программным модулем безопасности (HSM или SSM). События и улучшенные данные могут храниться в защищенном репозитории или хранилище данных. Шлюз затем осуществляет проверку для того, чтобы определить, куда будут отправлены данные (доступна ли система GMS), например, в систему глобального управления или в систему управления целостностью или в другую внешнюю систему. Если доступна система глобального управления или система управления целостностью, то данные или события форматируются и утверждаются для использования системой глобального управления или в системе управления целостностью. Данные, отправляемые во внешнюю систему, могут быть отформатированы и утверждены в зависимости от требований внешней системы. Данные или события, проходящие сквозь шлюз, отправляются в модуль интеграции данных, сохраняющий данные или события, получающий данные из хранилища, создающий, например, структуру данных, содержащих ключевые значения, из данных, сортирующий структурированные данные и анализирующий структурированные данные, используя вычислительные модели и алгоритмы для идентификации корреляции между данными, применимыми для создания кластеризованных событий или надежного защищенного налогового отчета или защищенного KPI или помогающих в повторном взимании налога или возмещении налога или исправляющих несоответствия в системе глобального управления или в системе управления целостностью. Данные также проверяются на целостность структурированных данных и безопасность структурированных данных для предотвращения фальсификации. Интерфейс данных может представлять собой независимый интерфейс или часть системы управления данными. Если интерфейс является отдельным, данные затем проходят в систему управления данными для обработки согласно вариантам осуществления, описанным выше.

Следующие примеры и описание относятся к системе глобального управления поставками или системе управления целостностью (системе слежения) в качестве источника для сбора данных в качестве альтернативы использованию датчиков или устройств сбора данных. Другими словами, защищенное устройство наблюдения (SOD), описанное выше применительно к системе глобального управления поставками (слежения и трассировки), может быть заменено датчиками и устройствами сбора данных, описанными применительно к системе глобального управления или в системе управления целостностью. Например, в секторе мидстрим цепочки поставок, защищенные данные D могут создаваться в трубопроводе с помощью датчиков для сбора данных, и защищенные данные D могут создаваться путем наблюдения и обнаружения маркированного топлива в автоцистерне. Например, маркировка будет находиться в топливе (или другом ресурсе) таким образом, чтобы регулярная проверка и верификация вдоль маршрута автоцистерны создавали защищенные данные D (которые могут быть переданы в систему глобального управления или в систему управления целостностью). Например, если концентрация продукта (например, топлива) изменяется на протяжении трубопровода, датчики (выполняющие функцию защищенного устройства наблюдения (SOD)) создадут защищенные данные D путем добавления защищенного алгоритма или другого атрибута. Защищенные данные D также могут быть созданы на основании анализа топливной маркировки сырой нефти в сравнении с данными, собранными на трубопроводе, и могут быть введены в ERP и переданы в интерфейс шлюза. Созданные данные будут использованы для создания защищенных кластеризованных событий внутри системы управления данными и применимых для создания предупреждений в центре управления CCC для систем GMS или IMS. В другом варианте осуществления, вместо осуществления маркировки продукта (например, топлива), датчики на трубопроводе будут выполнять функцию защищенного устройства наблюдения (SOD) вместе с классическим датчиком, измеряющим указанные значения и отправляющим их в репозиторий. Датчик будет отправлять данные с зашифрованным и защищенным атрибутом/атрибутами, и будет проверять и перепроверять данные перед их отправкой в качестве защищенных данных для того, чтобы удостовериться в аутентичности данных.

Другой неограничивающий пример создания защищенных данных D происходит в секторе даунстрим. В процессе переработки, применяемой для создания топлива или моторного топлива, разные партии топлива могут иметь разную маркировку. Лишь соответствующее топливо с защищенной маркировкой будет отправлено в определенную область страны. В одном варианте осуществления разные химические маркировки в разных местоположениях на протяжении разных каналов приводят к разным розничным торговцам. Химическая маркировка основана, например, на особых смесях органических или неорганических люминесцентных соединений (ИК, ближний ИК, УФ), при этом каждая особая смесь представляет особый химический ключ. В другом варианте осуществления разные сорта или типы топлива имеют разные маркировки. Благодаря сбору данных можно определить, была ли сообщенная сделка на определенный сорт топлива заключена на правильный физический продукт, для того, чтобы обнаружить, что некто задекларировал, например, сделки на продукт, облагаемый низким налогом, в то время как на самом деле заключил сделку на продукт, облагаемый высоким налогом.

Сбор данных с помощью защищенного устройства наблюдения SOD предоставит способность определения факта осуществления любой незаконной деятельности, такой как кража или изменение маршрута транспортировки продукта, в ходе транспортировки. Например, в области страны (например, Си-

налоа), произведенное топливо должно быть маркировано соединениями A, B и C. Маркированное топливо затем будет распределено в заправочную станцию в Синалоа. С другой стороны, в области Сакатекас топливо, маркированное соединениями D, E и F, будет транспортироваться по дороге, пока не прибудет к заправочной станции в Сакатекас. Если по какой-либо причине топливо, маркированное соединениями D, E и F, получают или обнаруживают на заправочной станции в Синалоа, система глобального управления GMS (после получения собранных данных, относящихся к маркированному топливу) определит, что в какой-то момент продукт подвергся незаконному вмешательству. Например, будет определено, что топливо, изначально предназначенное для транспортировки в Сакатекас, было направлено (незаконно) в область Синалоа. Подобным образом, трубопровод может быть изолирован согласно области, и защищенные данные D, созданные в областях трубопроводов, будут собраны защищенным устройством наблюдения SOD. В свою очередь, система глобального управления GMS будет предупреждена на основании кластеризованных событий, созданных особыми защищенными данными D (связанными с датчиками в особой области трубопровода). На основании этой информации система глобального управления GMS будет способна точно определить местоположение проблем в определенной области.

Используя систему глобального управления цепочками поставок для трассировки, отслеживания и хранения защищенных событий на протяжении цепочки поставок, сохраненная информация может использоваться совместно с системой глобального управления GMS и, в частности, с компонентом шлюза. В данном контексте, например, система глобального управления цепочками поставок выполняет функцию промышленной системы ICS для предоставления такой информации в шлюз или модуль интеграции данных, как изображено на фиг. 8. Как описано выше, данные, собранные из любой части цепочки поставок нефти и газа, используются для создания кластеризованных событий (защищенных), уведомлений и предупреждений в системе глобального управления в центре управления CCC и для предписывающего или предупреждающего воздействия на уровне вмешательства. Эти предупреждения, например, основаны и получены в результате кластеризованных событий, которые были разработаны с помощью процессов добычи данных, использования исторических данных и верификации, а также обработки данных на основании ранее собранных данных.

Сбор данных с помощью защищенного устройства наблюдения SOD предоставит способность определения дополнительного влияния незаконной деятельности на повторное взимание налогов и возможность ее обнаружения системой IMS. Например, сбор устройством SOD данных относительно объема топлива, доставленного в резервуаре или автоцистерне в заправочную станцию, позволит системе получить верную оценку объема, транспортированного от завода к заправочной станции, и соответствующий налог, который должен быть уплачен государству. Объем, коррелированный с маркировкой топлива, как было описано ранее, и также собранный устройством SOD, позволит узнать время получения заправочными станциями определенного маркированного топлива, и позволит рассчитать величину налога, которую соответствующая заправочная станция должна будет уплатить государству.

Дальнейшие примеры освещают сбор данных и информации из глобальной цепочки поставок, передаваемые в систему глобального управления или в систему управления целостностью. Следует понимать, что примеры не являются ограничивающими.

Маркировка топлива

Разные маркировки (например, разные химические составы) из разных областей и/или разные концентрации маркировки/маркировок используются для маркирования продукта, такого как топливо. Например, топливо с маркировкой/маркировками транспортируется по трубопроводу или в цистернах грузового автомобиля. Если в топливе обнаруживаются изменения концентрации маркировки топлива или присутствие другой жидкости (такой как вода), система (например, датчики или защищенное устройство наблюдения SOD) обнаружит изменение и заметит разницу по мере передвижения продукта из одной области в другую область. SOD или датчик могут использоваться для сбора данных о маркированном топливе и будут создавать соответствующее защищенное событие/события или данные для доставки в систему управления шлюзом (в шлюз или модуль интеграции данных). Эти данные затем могут использоваться для обнаружения контрафакции, изменения маршрута транспортировки, кражи материала, мошенничества, налогового мошенничества и т.д., как описано выше.

Осуществление контроля над трубопроводом

На уровне трубопровода продукт (например, топливо) может контролироваться с помощью датчиков или ручных датчиков (SOD). Эти датчики представляют собой защищенные датчики, которые могут использоваться в дополнение к традиционным датчикам или вместо них. Традиционный датчик не способен обнаруживать любые маркировки в продукте, в то время как защищенные датчики могу обнаруживать такие маркировки. Соответственно, любые данные, собранные защищенными датчиками, могут быть добавлены к данным традиционных датчиков и верифицированы или проверены аппаратным модулем безопасности HSM или модулем SSM, и верифицированные/проверенные данные защищенным образом отправляются в шлюз и/или модуль интеграции данных. Каждый датчик может быть уникальным и защищенным образом отправлять защищенные события и данные. С другой стороны, данные, собранные из SOD, избыточно проверяются или получаются несколько раз и усредняются и верифицируются для подтверждения точности информации в собранных данных перед их передачей в шлюз и/или модуль

интеграции данных. Дополнительно, данные могут включать в себя уникальную метку, отражающую их положение на протяжении трубопровода, и сохраняемую в соответствующем репозитории или в кластеризованных событиях, созданных на уровне системы управления данными в системе глобального управления или в системе управления целостностью. Получение информации на протяжении трубопровода, а также ее местоположения может осуществляться при появлении проблемы и/или выполнении технического обслуживания на уровне трубопровода.

Контроль над насосом заправочной станции

Создание защищенных событий также может происходить для осуществления контроля над потреблением и подачей нефтепродукта на уровне заправочной станции. Например, каждый насос в заправочной станции может быть оснащен защищенным устройством наблюдения SOD (например, датчиком), способным определять маркировку внутри топлива и передавать информацию защищенным образом. Это обеспечит уверенность в том, что для определенной маркировки заправочная станция авторизована распределять топливо (моторное топливо), тем самым обеспечивая надлежащую продукта с не измененным составом к заправочной станции. SOD также может использоваться для создания защищенных событий и данных, связанных с объемом потребленного моторного топлива или доставленного моторного топлива в сочетании с количеством моторного топлива, проданного на заправочной станции. Эти данные, созданные устройством SOD, могут применяться для различных целей, например, включая повторное взимание налога и для определения соответствия величины прибыли на заправочной станции и объема моторного топлива, доставленного транспортным средствам на заправочной станции. Как и в примере трубопровода, информация из SOD может быть защищена системами HSM или SSM и уникальным и защищенным образом обмениваться данными со шлюзом и модулем интеграции данных.

Хотя изобретение было описано со ссылкой на несколько примерных вариантов осуществления, следует понимать, что использованные слова являются описательными и иллюстративными, но не ограничивающими. Могут быть внесены изменения в пределах сферы действия прилагаемой формулы изобретения, в том виде, в котором она заявлена в настоящее время и в ее измененном виде, не отступая от объема и идеи изобретения в его аспектах. Хотя изобретение было описано со ссылкой на конкретные средства, материалы и варианты осуществления, изобретение не предназначено для ограничения описанными сведениями, вместо этого изобретение охватывает все функционально эквивалентные структуры, способы и применения, находящиеся в пределах объема прилагаемой формулы изобретения.

Хотя машиночитаемый носитель может быть описан как один носитель, термин "машиночитаемый носитель" включает в себя один носитель или несколько носителей, такие как централизованная или распределенная база данных, и/или соответствующие кэши и сервера, сохраняющие один или несколько наборов команд. Термин "машиночитаемый носитель" также должен включать в себя любой носитель, способный хранить, шифровать или содержать набор команд для выполнения процессором или вынуждающих компьютерную систему выполнять один или несколько любых вариантов осуществления, описанных здесь.

Машиночитаемый носитель может содержать постоянный машиночитаемый носитель или носители и/или содержать временный машиночитаемый носитель или носители. В определенном неограничивающем примерном варианте осуществления машиночитаемый носитель может включать в себя твердотельное запоминающее устройство, такое как карта памяти или другой модуль, вмещающий одно или несколько энергонезависимых постоянных запоминающих устройств. Кроме этого, машиночитаемый носитель может представлять собой оперативное запоминающее устройство или другое энергозависимое перезаписываемое запоминающее устройство. Дополнительно, машиночитаемый носитель может включать в себя магнитно-оптический или оптический носитель, такой как диск или магнитные ленты или другое устройство хранения данных для сбора сигналов несущей, таких как сигналы, отправленные по передающей среде. Соответственно, считается, что описание включает в себя любой машиночитаемый носитель или другие эквиваленты и носители последующих поколений, в которых могут храниться данные или команды.

Хотя в настоящей заявке описаны конкретные варианты осуществления, которые могут быть реализованы в виде сегментов кода в машиночитаемых носителях, следует понимать, что выделенные аппаратные реализации, такие как специализированные интегральные схемы, программируемые логические матрицы и другие аппаратные устройства, могут быть построены для реализации одного или нескольких вариантов осуществления, описанных здесь. Применения, которые могут включать в себя различные варианты осуществления, изложенные здесь, могут включать в себя большое разнообразие электронных и компьютерных систем. Соответственно, настоящая заявка может охватывать реализации программного обеспечения, программно-аппаратного обеспечения и аппаратного обеспечения или их комбинации.

Хотя в настоящем техническом описании описаны компоненты и функции, которые могут быть реализованы в определенных вариантах осуществления, со ссылкой на определенные стандарты и протоколы, изобретение не ограничено этими стандартами и протоколами. Такие стандарты периодически замещаются более быстрыми или более эффективными эквивалентами, обладающими по существу теми же функциями. Соответственно, заменяющие стандарты и протоколы, обладающие такими же или подобными функциями, считаются их эквивалентами.

Изображения вариантов осуществления, описанные здесь, предназначены для предоставления общего понимания различных вариантов осуществления. Предполагается, что изображения не будут служить полным описанием всех элементов и признаков приспособления и систем, использующих структуры или способы, описанные здесь. Множество других вариантов осуществления могут быть очевидны специалистам в данной области после рассмотрения изобретения. Другие варианты осуществления могут быть использованы и выведены из настоящего изобретения таким образом, чтобы структурные и логические замещения и изменения могли быть осуществлены в пределах объема изобретения. Дополнительно, изображения предназначены лишь для образования представления и могут быть изображены не в масштабе. Некоторые пропорции в изображениях могут быть преувеличены, в то время как другие пропорции могут быть сведены к минимуму. Соответственно, описание и фигуры нужно расценивать как пояснительные, но не ограничивающие.

Один или несколько вариантов осуществления изобретения могут быть обозначены здесь, по отдельности или вместе, термином "изобретение" лишь для удобства, и не предполагая добровольного ограничения объема данной заявки любым конкретным изобретением или новаторское идеей. Более того, хотя определенные варианты осуществления были изображены и описаны в настоящей заявке, следует понимать, что любая последующая конструкция, предназначенная для достижения той же или подобной цели, может быть замещена изображенными определенными вариантами осуществления. Предполагается, что данное изобретение охватывает любые и все последующие адаптации или вариации различных вариантов осуществления. Комбинации вышеописанных вариантов осуществления и другие варианты осуществления, не описанные здесь особым образом, будут очевидны специалистам в данной области после рассмотрения описания.

Реферат изобретения предоставлен для того, чтобы удовлетворить требованиям 37 C.F.R. §1.72(b) и подан с пониманием того, что он не будет использован для трактовки или ограничения объема или смысла формулы изобретения. Кроме этого, в вышеизложенном подробном описании различные признаки могут быть сгруппированы вместе или описаны в одном варианте осуществления для упрощения изобретения. Данное изобретение не должно быть истолковано как подразумевающее, что заявленные варианты осуществления требуют больше признаков, чем указано в явном виде в каждом пункте формулы изобретения. Вместо этого, как отражено в следующей формуле изобретения, патентоспособный объект изобретения может быть направлен на менее чем все признаки описанных вариантов осуществления. Таким образом, следующая формула изобретения включена в подробное описание, при этом каждый пункт формулы изобретения является самостоятельным, поскольку определяет отдельно заявляемый объект изобретения.

Вышеописанный объект изобретения следует расценивать как наглядный и не ограничивающий, и предполагается, что прилагаемая формула изобретения охватывает все подобные модификации, улучшения и другие варианты осуществления, находящиеся в пределах истинной идеи и объема настоящего изобретения. Таким образом, до максимальной степени, разрешенной законом, объем настоящего изобретения должен быть определен наиболее широким из допустимых толкований следующих пунктов формулы изобретения и их эквивалентов и не должен ограничиваться вышеизложенным подробным описанием.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система для идентификации или предупреждения незаконной деятельности в отношении нефтегазовых ресурсов путем создания защищенных данных, относящихся к нефтегазовым ресурсам, во время перемещения по цепочке поставок, содержащая

по меньшей мере один датчик, расположенный на протяжении цепочки поставок и выполненный с возможностью сбора данных, включающих незащищенную информацию из идентификатора продукта и защищенную информацию из маркировки, аутентификации маркировки и добавления шифрования к собранным данным, создавая тем самым зашифрованные данные, причем продукт маркирован при помощи идентификатора продукта и маркировки;

по меньшей мере одну систему репозитория, которая выполнена с возможностью сбора и хранения зашифрованных данных из по меньшей мере одного датчика и

отправляет их в интерфейс шлюза,

причем интерфейс шлюза обеспечивает механизм для преобразования зашифрованных данных, полученных из по меньшей мере одной системы репозитория, в формат, имеющий дополнительную защиту и который совместим с системой интеграции данных перед использованием в системе глобального управления или системе управления целостностью, относящейся к управлению нефтегазовыми ресурсами, для создания кластеризованных событий, используемых для идентификации или предупреждения незаконной деятельности в отношении нефтегазовых ресурсов, и, дополнительно, интерфейс шлюза выполнен с возможностью проверять, перед преобразованием зашифрованных данных, полученных из по меньшей мере одной системы репозитория, что зашифрованные данные, полученные из по меньшей мере одной системы репозитория, являются подлинными данными и не были искажены внешними источниками.

2. Система по п.1, дополнительно содержащая платформу управления событиями для получения обзора цепочки поставок с применением собранных защищенных данных для идентификации по меньшей мере одного из следующих видов деятельности: фальсификация, изменение маршрута транспортировки, замена состава, контрафакция, мошенничество и налоговое мошенничество, связанные с продуктом в цепочке поставок.

3. Система по п.2, в которой система репозитория обменивается данными с платформой управления событиями посредством сети и включает в себя множество устройств хранения данных, доступных системе и распределенных в ней.

4. Система по п.1, в которой маркировка включает в себя состав, содержащий соединения с люминесцентными свойствами по меньшей мере в одном из следующих диапазонов: УФ, ИК и ближний ИК и их сочетания, которые могут представлять химический ключ.

5. Система по п.4, в которой продукт представляет собой одно из нижеперечисленного: бензин или моторное топливо, керосин, реактивное топливо, дизельное топливо, печное топливо, смазочные материалы, воски, асфальт, природный газ, сжиженный нефтяной газ и нефтехимические продукты.

6. Система по п.1, в которой датчик дополнительно воспринимает данные, включающие в себя или относящиеся по меньшей мере к одному из следующего: температура, плотность, влажность, объем, сила тяжести, химический состав, давление, вес, изменение давления в трубопроводе, разница в весе транспортного средства или в объеме топлива, определение местонахождения по GPS, синхронизация местонахождения транспортного средства, географическая область, скорость потока, удельная проводимость, реология, мутность, формирование изображений, термическое формирование изображений, состояние датчика, показания тензометрических датчиков, данные о погодных условиях, дорожные условия, состояние транспортного средства или дороги, скорость ветра, барометрические условия, количество атмосферных осадков, данные о техническом обслуживании или дата технического обслуживания, информация о персональном местоположении, радиочастотные данные, акустические данные, вязкость и местоположение по GPS.

7. Система по п.4, в которой система репозитория сохраняет зашифрованные данные, связанные с продуктом, на протяжении жизненного цикла объекта в цепочке поставок.

8. Система по п.7, в которой незащищенная информация и защищенная информация собирается одновременно.

9. Система по п.1, в которой по меньшей мере один датчик расположен по меньшей мере в одном из трубопроводов на протяжении цепочки поставок нефти и газа и реагирует на химическое вещество, маркирующее продукт, а трубопровод соединен с насосом в заправочной станции, распространяющей продукт.

10. Способ для идентификации или предупреждения незаконной деятельности в отношении нефтегазовых ресурсов посредством системы по любому из пп.1-9, включающий:

с помощью по меньшей мере одного датчика, расположенного на протяжении цепочки поставок, сбор данных, включающих незащищенную информацию из идентификатора продукта и защищенную информацию из маркировки, аутентификацию маркировки и добавление шифрования к собранным данным, создавая тем самым зашифрованные данные, причем продукт маркирован при помощи идентификатора продукта и маркировки;

по меньшей мере в одной системе репозитория сбор и хранение зашифрованных данных из по меньшей мере одного датчика и

отправку их в интерфейс шлюза,

причем интерфейс шлюза преобразует зашифрованные данные, полученные из по меньшей мере одной системы репозитория в формат, имеющий дополнительную защиту и который совместим с системой интеграции данных перед использованием в системе глобального управления или системе управления целостностью, относящейся к управлению нефтегазовыми ресурсами, для создания кластеризованных событий, используемых для идентификации или предупреждения незаконной деятельности в отношении нефтегазовых ресурсов, и, дополнительно, интерфейс шлюза проверяет перед преобразованием зашифрованных данных, полученных из по меньшей мере одной системы репозитория, что зашифрованные данные, полученные из по меньшей мере одной системы репозитория, являются подлинными данными и не были искажены внешними источниками.

11. Способ по п.10, дополнительно включающий получение обзора цепочки поставок, в платформе управления событиями, с применением собранных защищенных данных для идентификации по меньшей мере одного из следующих видов деятельности: фальсификация, изменение маршрута транспортировки, замена состава, контрафакция, мошенничество и налоговое мошенничество, связанные с продуктом в цепочке поставок.

12. Способ создания защищенных данных по п.11, в котором система репозитория обменивается данными с платформой управления событиями посредством сети и включает в себя множество устройств хранения данных, доступных системе и распределенных в ней.

13. Способ по п.10, в котором маркировка включает в себя состав, содержащий соединения с люминесцентными свойствами по меньшей мере в одном из следующих диапазонов: УФ, ИК и ближний ИК и

их сочетания, которые могут представлять химический ключ.

14. Способ по п.13, в котором продукт представляет собой одно из нижеперечисленного: бензин или моторное топливо, керосин, реактивное топливо, дизельное топливо, печное топливо, смазочные материалы, воски, асфальт, природный газ, сжиженный нефтяной газ и нефтехимические продукты.

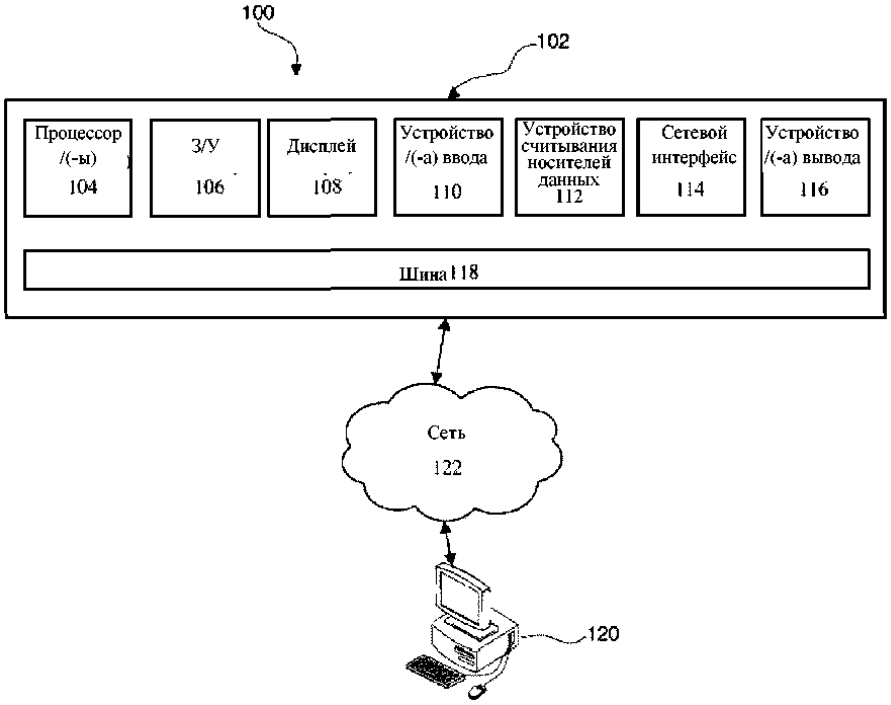
15. Способ по п.10, в котором датчик дополнительно воспринимает данные, включающие в себя или относящиеся по меньшей мере к одному из следующего: температура, плотность, влажность, объем, сила тяжести, химический состав, давление, вес, изменение давления в трубопроводе, разница в весе транспортного средства или в объеме топлива, определение местонахождения по GPS, синхронизация местонахождения транспортного средства, географическая область, скорость потока, удельная проводимость, реология, мутность, формирование изображений, термическое формирование изображений, состояние датчика, показания тензометрических датчиков, данные о погодных условиях, дорожные условия, состояние транспортного средства или дороги, скорость ветра, барометрические условия, количество атмосферных осадков, данные о техническом обслуживании или дата технического обслуживания, информация о персональном местоположении, радиочастотные данные, акустические данные, вязкость и местоположение по GPS.

16. Способ по п.13, в котором система репозитория сохраняет зашифрованные данные, связанные с продуктом, на протяжении жизненного цикла объекта в цепочке поставок.

17. Способ по п.16, в котором незащищенная информация и защищенная информация собирается одновременно.

18. Способ по п.10, в котором по меньшей мере один датчик расположен по меньшей мере в одном из трубопроводов на протяжении цепочки поставок нефти и газа и реагирует на химическое вещество, маркирующее продукт, а трубопровод соединен с насосом в заправочной станции, распространяющей продукт.

19. Постоянный машиночитаемый носитель, хранящий программу для создания защищенных данных, относящихся к нефтегазовому ресурсу, во время перемещения по цепочке поставок, при этом программа, при выполнении процессором, обеспечивает выполнение компьютером способа по любому из пп.10-18.



Фиг. 1

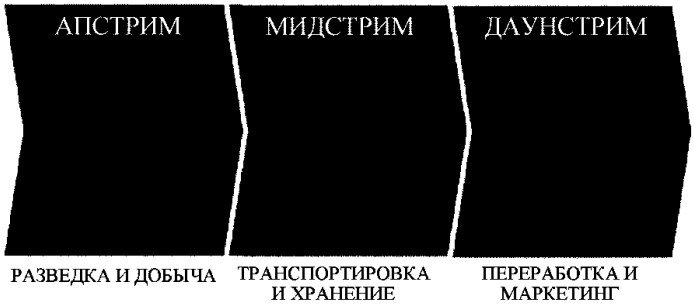
Фиг. 2

ЦЕЛЕВОЕ ВМЕШАТЕЛЬСТВО

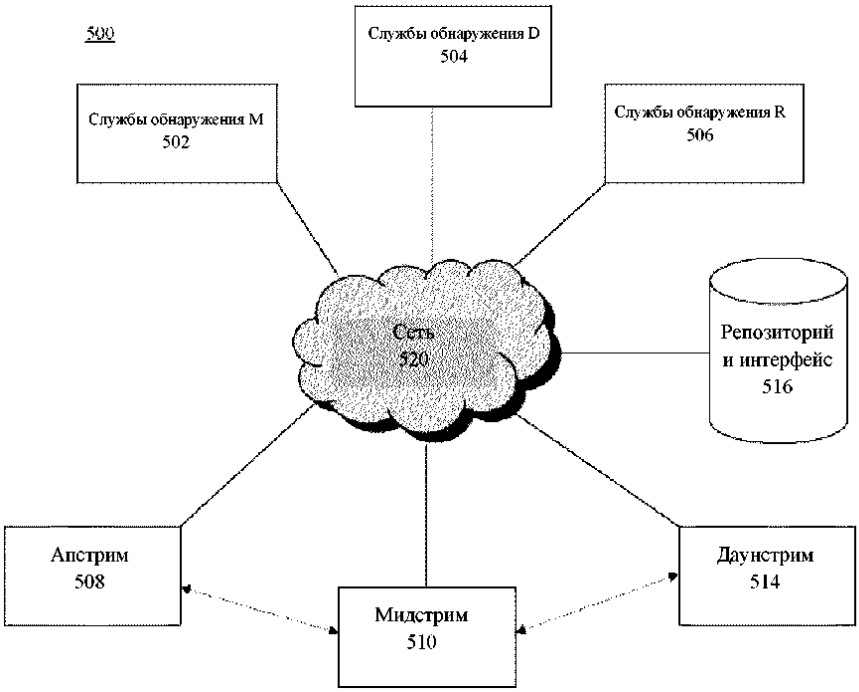
КОМАНДОВАНИЕ И УПРАВЛЕНИЕ

БОЛЬШИЕ ДАННЫЕ

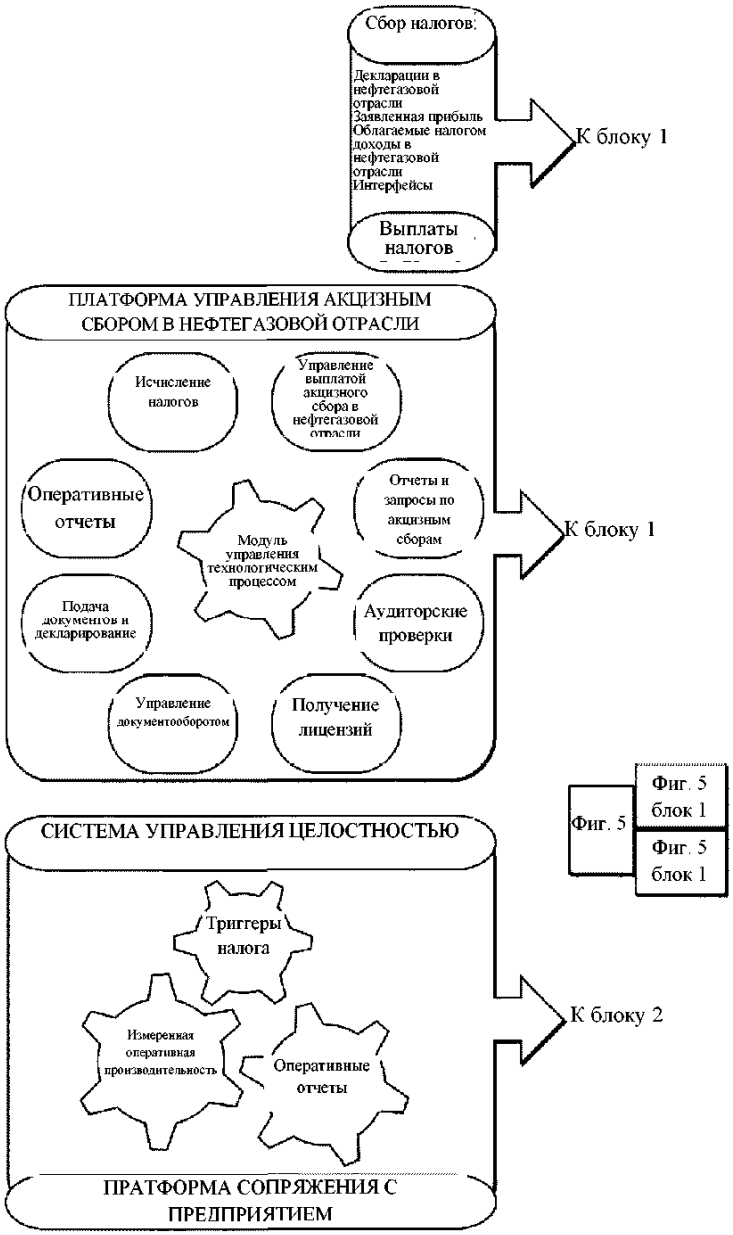
ИНТЕГРАЦИЯ



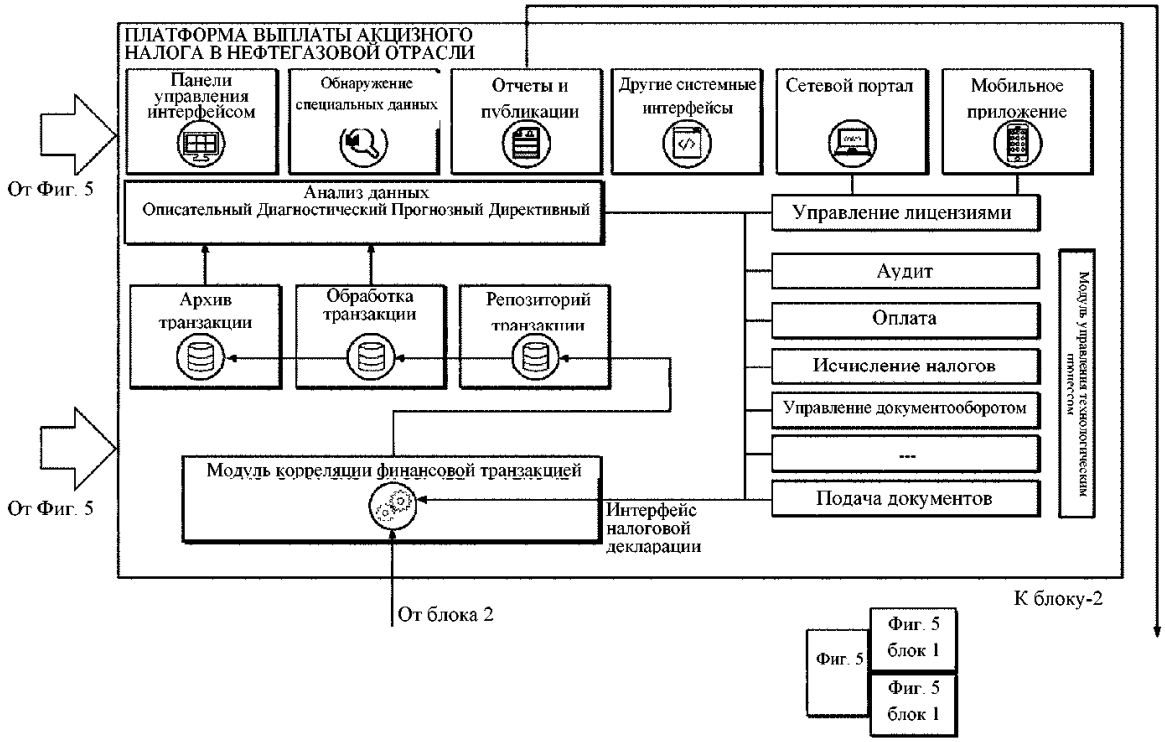
Фиг. 3


500
Службы обнаружения D
504
Службы обнаружения M
502
Службы обнаружения R
506
Сеть
520
Репозиторий
и интерфейс
516
Апстрим
508
Мидстрим
510
Даунстрим
514

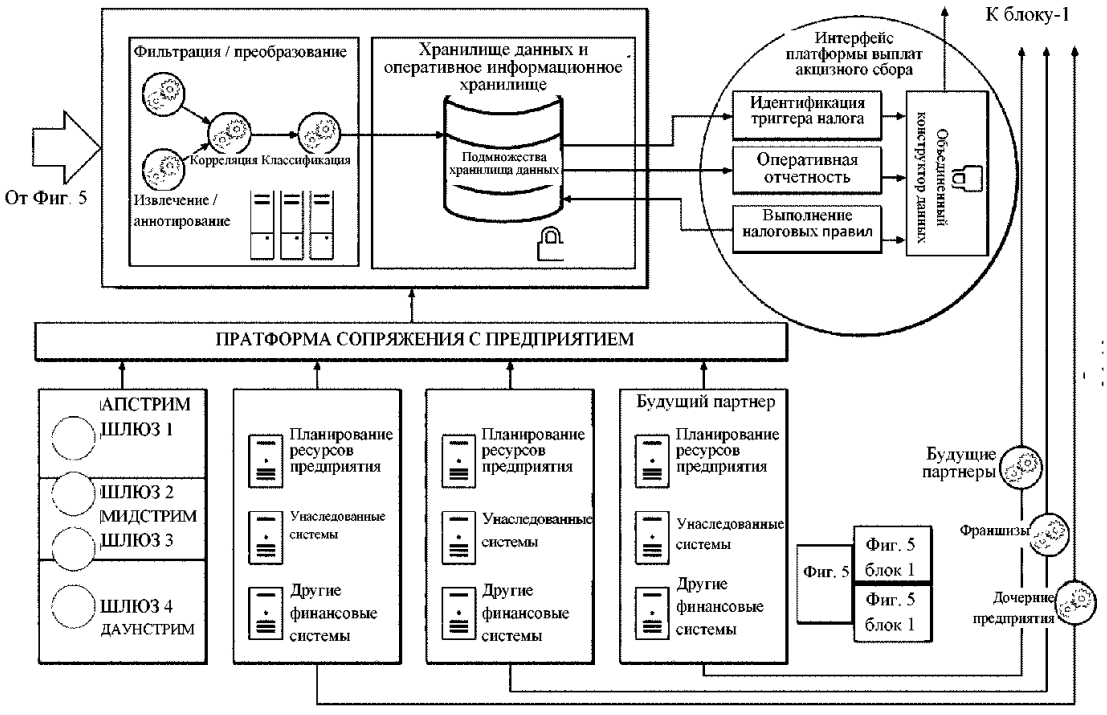
Фиг. 4


Сбор налогов
Декларации в нефтегазовой отрасли
Заявленная прибыль
Облагаемые налогом доходы в нефтегазовой отрасли
Интерфейсы
Выплаты налогов
К блоку 1
ПЛАТФОРМА УПРАВЛЕНИЯ АКЦИЗНЫМ СБОРОМ В НЕФТЕГАЗОВОЙ ОТРАСЛИ
Исчисление налогов
Управление выплатой акцизного сбора в нефтегазовой отрасли
Оперативные отчеты
Модуль управления технологическим процессом
Отчеты и запросы по акцизным сборам
Подача документов и декларирование
Аудиторские проверки
Управление документооборотом
Получение лицензий
К блоку 1
Фиг. 5
Фиг. 5 блок 1
Фиг. 5 блок 1
СИСТЕМА УПРАВЛЕНИЯ ЦЕЛОСТНОСТЬЮ
Триггеры налога
Измеренная оперативная производительность
Оперативные отчеты
К блоку 2
ПРАТФОРМА СОПРЯЖЕНИЯ С ПРЕДПРИЯТИЕМ

Фиг. 5



Фиг. 5 блок 1



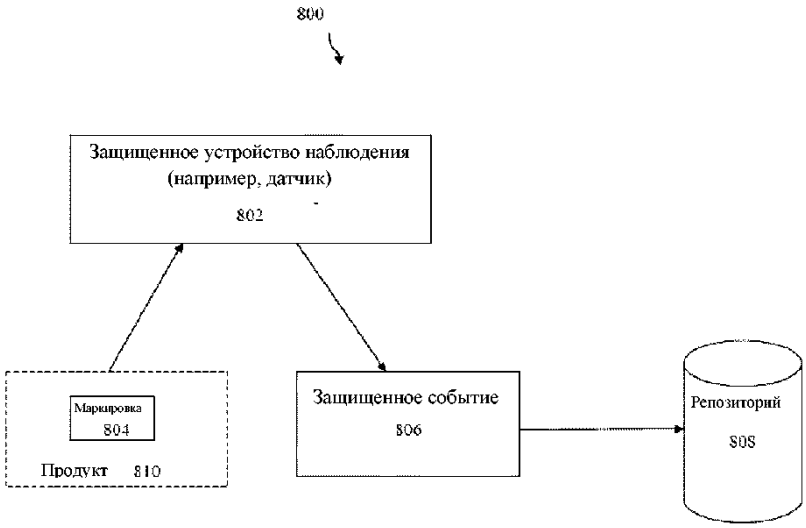
Фиг. 5 блок 2


Создание идентификатора продукта
700
Сбор данных
702
Маркировка продукта идентификатором продукта
704
Сохранение информации о продукте и соответствующего идентификатора продукта в репозитории
706

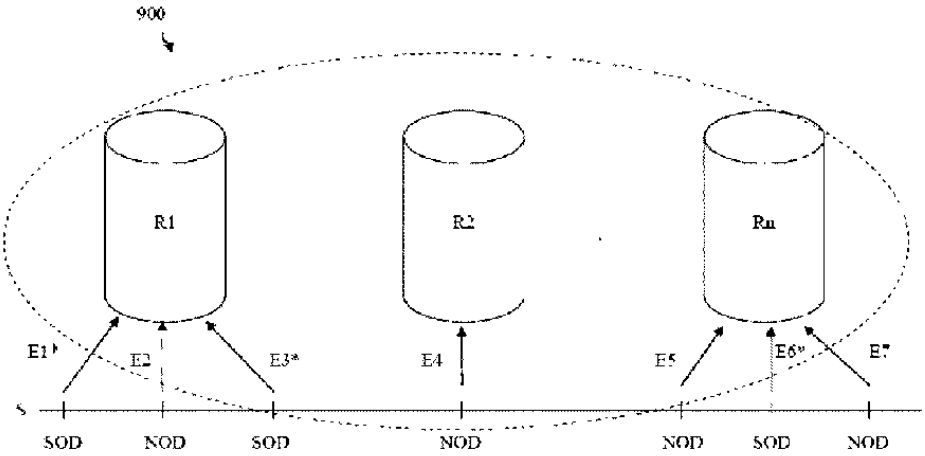
Фиг. 6А


Перемещение продукта по цепочке поставок
710
Возникновение события
712
Сканирование продукта с помощью датчика и верификация маркировки
714
Аутентификация и сообщение собранных (отсканированных) данных
716

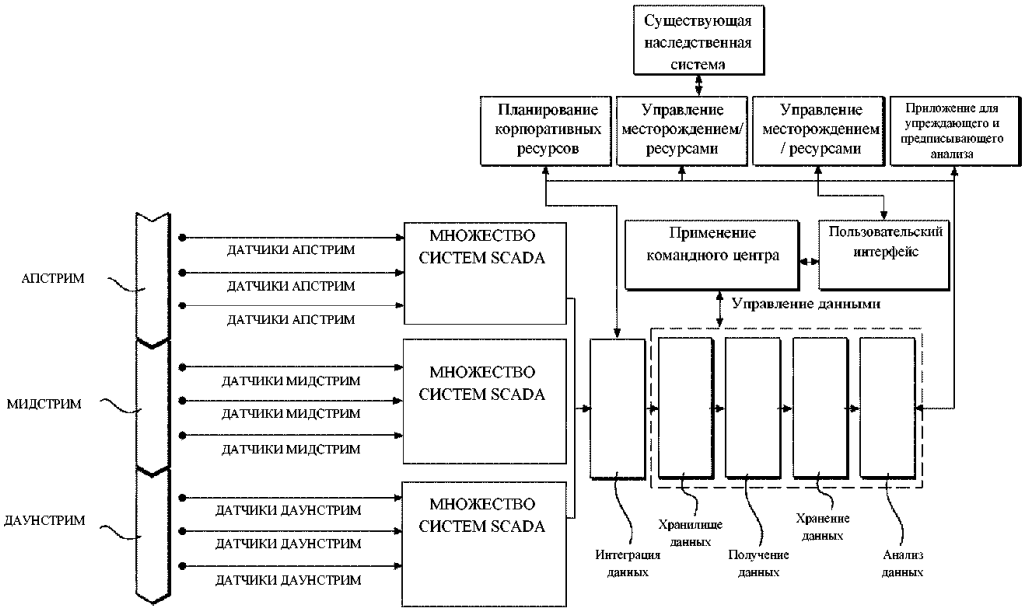
Фиг. 6В


800
Защищенное устройство наблюдения (например, датчик)
802
Маркировка
804
Продукт 810
Защищенное событие
806
Репозиторий
808

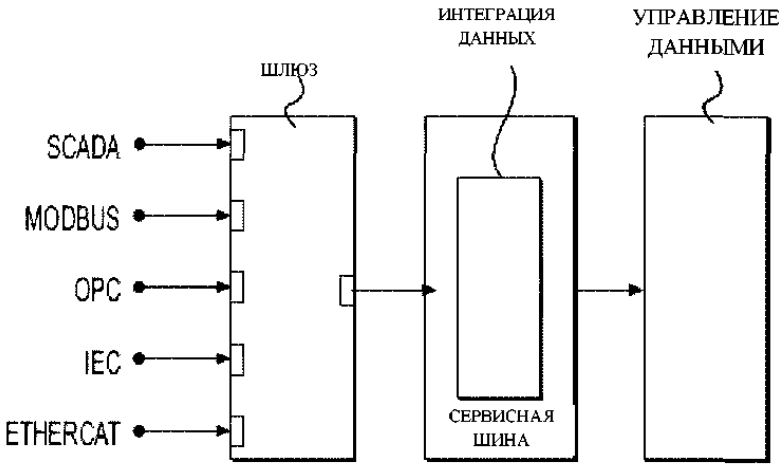
Фиг. 7



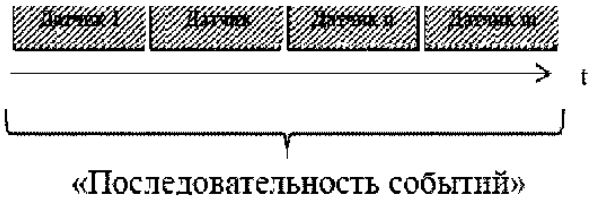
Фиг. 8



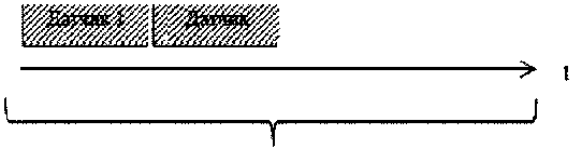
Фиг. 9



Фиг. 10



Фиг. 11A

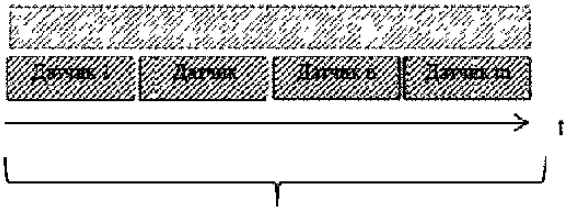


«Низкая вероятность»

Фиг. 11B

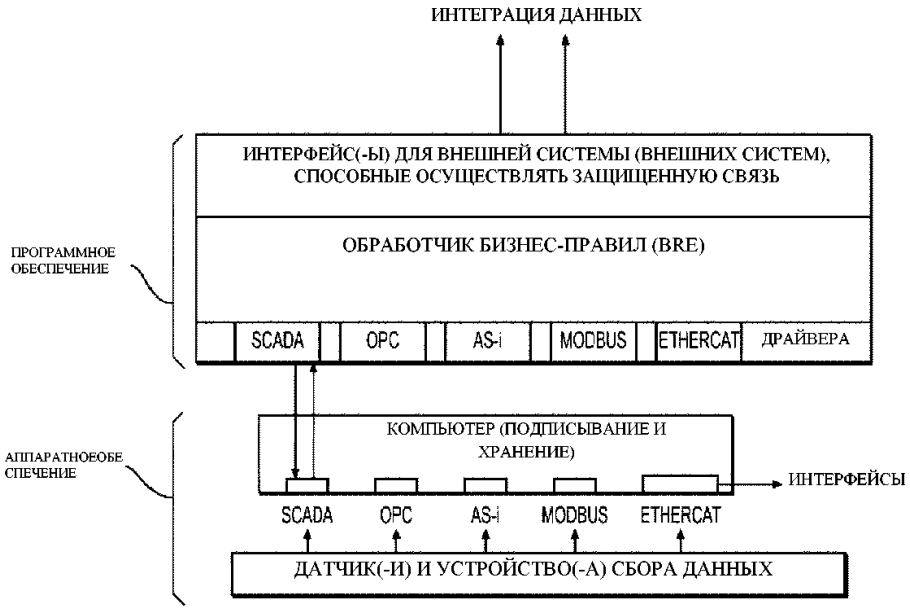
«Средняя вероятность»

Фиг. 11C

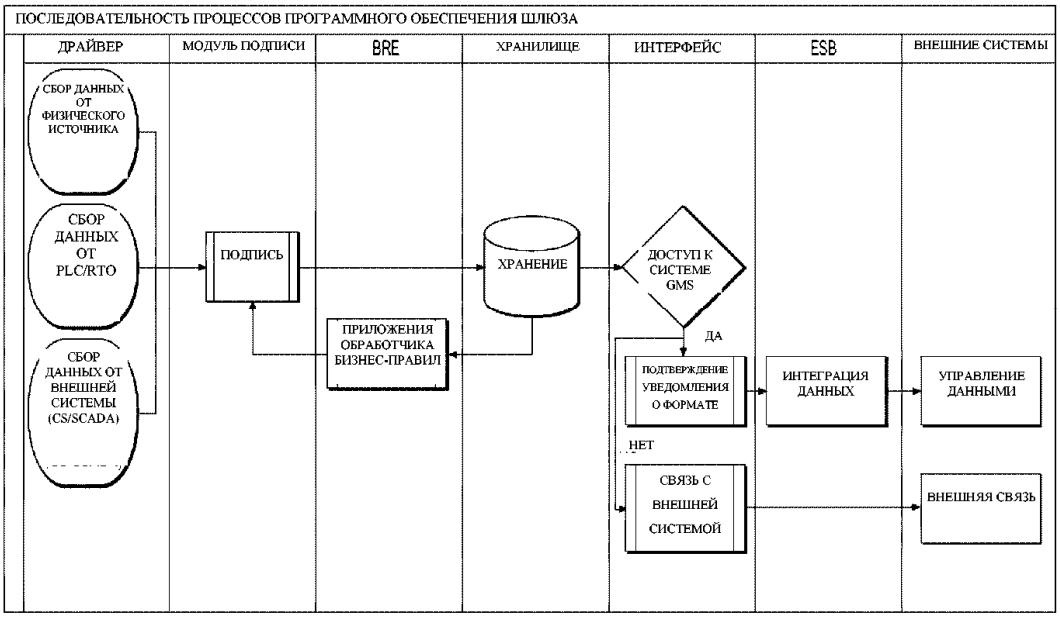


«Высокая вероятность»

Фиг. 11D



Фиг. 12



Фиг. 13

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2