РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 463 658** (13) **C2**

(51) МПК
G06Q 20/28 (2012.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2009136566/08, 01.04.2008**

(24) Дата начала отсчета срока действия патента:
01.04.2008

Приоритет(ы):
(30) Конвенционный приоритет:
04.04.2007 US 11/696,350

(43) Дата публикации заявки: **10.04.2011** Бюл. № 10

(45) Опубликовано: **10.10.2012** Бюл. № **28**

(56) Список документов, цитированных в отчете о поиске: **US 2003/0135380 A1, 17.06.2003. US 2003/0135474 A1, 17.06.2003. WO 2007/024822 A1, 01.03.2007. US 7046682 B2, 08.11.2001. RU 2002110094 A, 10.03.2004.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **02.10.2009**

(86) Заявка PCT:
US 2008/059030 (01.04.2008)

(87) Публикация заявки PCT:
WO 2008/124396 (16.10.2008)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ВЕСТЕРИНЕН Уилльям Дж. (US),
КАРПЕНТЕР Тодд (US),
ДРЭЙК Стефен Р. (US),
МАЙЕРС Марк (US)

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

(54) ПРЕДВАРИТЕЛЬНО ОПЛАЧЕННЫЙ ДОСТУП К ОБРАБОТКЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ПЕРЕНОСНЫХ УСТРОЙСТВ ХРАНЕНИЯ ДАННЫХ

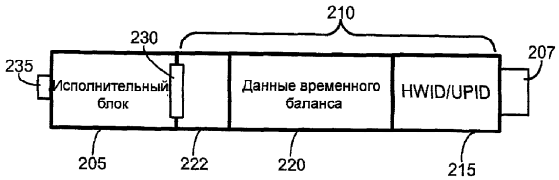
(57) Реферат:

Изобретение относится к средствам разблокировки подписного режима компьютера. Технический результат заключается в уменьшении времени, требующемся для пользователя, чтобы безопасным образом разблокировать подписной компьютер. Устанавливают соединение между съемным устройством учета обработки данных и модулем защиты компьютера через защищенную среду начальной загрузки, хранящуюся в компьютере, при этом съемное устройство учета обработки данных включает в себя некоторое количество единиц учета доступа, хранящееся в защищенной флэш-памяти съемного устройства учета обработки данных. Обеспечивают защиту соединения между устройством учета обработки данных и модулем защиты. Определяют, превышает ли упомянутое количество единиц учета доступа пороговое значение. Ограничивают функционирование компьютера, если упомянутое количество единиц учета доступа

RU 2463658 C2

RU 2463658 C2

ниже порогового значения. Исполняют по меньшей мере одно приложение на компьютере, если упомянутое количество единиц учета доступа выше порогового значения. Уменьшают упомянутое количество единиц учета доступа в процессе исполнения упомянутого по меньшей мере одного приложения и в ответ на потерю связи между съемным устройством учета обработки данных и модулем защиты принудительно реализуют перезагрузку компьютера в защищенную среду начальной загрузки. 3 н. и 15 з.п. ф-лы, 6 ил.



ФИГ. 2

RU 2463658 C2

RU 2463658 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 463 658** (13) **C2**

(51) Int. Cl.
G06Q 20/28 (2012.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009136566/08, 01.04.2008**

(24) Effective date for property rights:
01.04.2008

Priority:
(30) Convention priority:
04.04.2007 US 11/696,350

(43) Application published: **10.04.2011** Bull. 10

(45) Date of publication: **10.10.2012 Bull. 28**

(85) Commencement of national phase: **02.10.2009**

(86) PCT application:
US 2008/059030 (01.04.2008)

(87) PCT publication:
WO 2008/124396 (16.10.2008)

Mail address:
129090, Moskva, ul. B. Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery"

(72) Inventor(s):
VESTERINEN Uill'jam Dzh. (US),
KARPENTER Todd (US),
DREhJK Stefen R. (US),
MAJERS Mark (US)

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

RU 2463658 C2

(54) PREPAID ACCESS TO DATA PROCESSING USING PORTABLE DATA STORAGE DEVICES

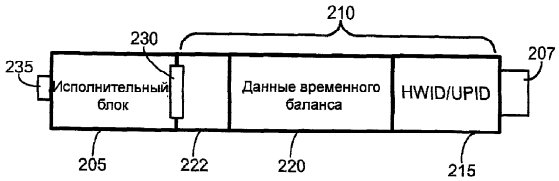
(57) Abstract:

FIELD: information technology.

SUBSTANCE: connection is established between a detachable data processing accounting device and a computer security module through a secure booting environment stored on the computer, wherein the detachable data processing accounting device includes a certain number of access accounting units stored in the secure flash memory of the data processing accounting device. The connection between the data processing accounting device and the security module is secured. It is determined whether said number of access accounting units exceeds a threshold value. Operation of the computer is restricted if said number of access accounting units is below the threshold value. At least one application on the computer is used if said number of access accounting units exceeds the threshold value. Said number of access accounting units is reduced during execution of said at least one application and in response to loss of connection between the detachable data processing accounting device and the security module, the computer is forcibly rebooted in the secure booting environment.

EFFECT: reducing time needed by a user to safely unblock a subscription computer.

18 cl, 6 dwg



ФИГ. 2

RU 2463658 C2

УРОВЕНЬ ТЕХНИКИ

Данный Раздел «Уровень Техники» предназначен для предоставления основного контекста данной заявки на изобретение и не предназначен для описания отдельной проблемы, которая будет решаться.

Модели деловой деятельности с обеспечением выплат из текущих поступлений или с оплатой за использование и с подписной платой использовались во многих областях коммерческой деятельности, от сотовых телефонов до коммерческих прачечных самообслуживания. При развертывании деловой деятельности с обеспечением выплат из текущих поступлений поставщик, например поставщик сотовых телефонов, предлагает использование аппаратных средств (сотового телефона) по цене ниже рыночной в обмен на обязательство оставаться подписчиком их сети. В данном конкретном примере потребитель получает сотовый телефон за небольшие деньги или бесплатно в обмен на подписание договора о подписке на заданный период времени. В течение срока действия договора поставщик услуг возвращает стоимость аппаратных средств, взимая с потребителя плату за использование сотового телефона.

Модель деловой деятельности с обеспечением выплат из текущих поступлений основывается на том принципе, что предоставляемые аппаратные средства имеют небольшую или никакую ценность, или пользу, отдельно от поставщика услуг. Для иллюстрации, в случае, если подписчик, упомянутый выше, перестает оплачивать его или ее счет, поставщик услуг дезактивирует их учетную запись, и, несмотря на то, что сотовый телефон может быть включен, звонки не могут совершаться, потому что поставщик услуг не позволит этого. Дезактивированный телефон не имеет никакой «ликвидационной» ценности, потому что телефон не будет работать где-нибудь в другом месте, а комплектующие детали нелегко вторично использовать, и они не имеют существенной цены на черном рынке. Когда лицевой счет пополняется, поставщик услуг восстанавливает подключение устройства к сети и разрешает подписчику совершать звонки.

Эта модель хорошо работает, когда поставщик услуг, или другая организация, принимающая на себя финансовый риск по предоставлению субсидируемых аппаратных средств, имеет жесткий контроль над использованием аппаратных средств и когда устройство имеет небольшую ликвидационную ценность. Эта модель деловой деятельности не работает хорошо, когда аппаратные средства имеют широкое применение вне зоны контроля поставщика услуг. Поэтому обычный персональный компьютер не удовлетворяет этим критериям, так как персональный компьютер может иметь широкое применение за пределами первоначального намерения, а компоненты персонального компьютера, например устройство отображения или дисковый накопитель, могут иметь значительную ликвидационную ценность.

В обычной вычислительной системе с обеспечением выплат из текущих поступлений пользователь приобретает код, который подлежит обмену на некоторое количество часов обработки данных на специально оборудованном электронном устройстве. Пользователь может добавлять время к существующему остатку на счете, приобретая дополнительные коды. Однако для того, чтобы гарантировать защищенность временного баланса пользователя и надежно отслеживать использованное время, система сохраняет данные, отражающие временной баланс, в защищенном модуле на самом устройстве. Сохранение временного баланса пользователя на одном устройстве не допускает получения пользователем вычислительных услуг на любой другой машине, кроме устройства, содержащего в

себе данные об остатке на счете.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Данный раздел «Сущность Изобретения» предусмотрен для представления в упрощенной форме набора концепций, которые дополнительно описываются ниже в разделе «Подробное описание». Данный раздел «Сущность Изобретения» не предназначен для установления ключевых признаков или существенных признаков заявляемого предмета изобретения, а также не предназначен для использования в качестве ограничения объема заявляемого предмета изобретения.

Форма съемного устройства хранения данных, такого как устройство с памятью с групповой перезаписью, подключаемое по универсальной последовательной шине (USB - universal serial bus) (UFD - USB flash device), может предоставить возможность надежного хранения и доступа к временному балансу вычислительной системы с оплатой за использование или с подписной платой. Вычислительное устройство может устанавливать защищенное соединение с переносным защищенным вычислительным устройством для доступа к сохраненному временному балансу или другим представленным на устройстве, исчерпываемым данным. В процессе работы устройство может сокращать этот баланс. При достижении порогового сокращения баланса пользователь может добавить больше данных, чтобы продолжить использование устройства. Устройство может включать в себя обрабатывающее устройство и устройство хранения данных, включающее в себя идентификационные и подписные данные. Дополнительно, устройство может хранить конфигурационные данные, которые могут использоваться компьютером для привязки устройства к конкретной подписной услуге или поставщику интернет-услуг.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Фиг.1 является иллюстрацией компьютера, который реализует способ или включает в себя устройство для использования USB-устройства с памятью с групповой перезаписью и другое переносное устройство хранения данных в качестве средства доступа к предварительно оплаченной обработке данных;

Фиг.2 является упрощенной и представительной структурной схемой устройства хранения данных для предоставления возможности предварительно оплаченной обработки данных;

Фиг.3 является упрощенной и иллюстративной структурной схемой системы, поддерживающей модель деловой деятельности с оплатой за использование и с подписной платой;

Фиг.4 является упрощенной и иллюстративной функциональной схемой способа для предоставления возможности защищенному компьютеру использовать переносное устройство хранения данных для контролирования и хранения количества приобретенного доступа или подписного времени в вычислительной системе с предоплатой;

Фиг.5 является другой упрощенной и иллюстративной функциональной схемой способа для предоставления возможности защищенному компьютеру использовать переносное устройство хранения данных для контролирования и хранения количества приобретенного доступа или подписного времени в вычислительной системе с предоплатой; и

Фиг.6 является еще одной упрощенной и иллюстративной функциональной схемой способа для предоставления возможности защищенному компьютеру использовать переносное устройство хранения данных для контролирования и хранения количества приобретенного доступа или подписного времени в вычислительной системе с

предоплатой.

ПОДРОБНОЕ ОПИСАНИЕ

Несмотря на то, что последующий текст излагает детальное описание многочисленных различных вариантов осуществления, нужно понимать, что правовой объем настоящего описания определяется формулировками формулы изобретения, изложенной в конце данного раскрытия. Это детальное описание должно рассматриваться только как иллюстративное и не описывает все возможные варианты осуществления, поскольку описание каждого возможного варианта осуществления было бы нецелесообразным, или даже невозможным. Могли бы быть реализованы многочисленные альтернативные варианты осуществления, с использованием или современной техники или техники, разработанной после даты подачи заявки на данный патент, которые будут по-прежнему находиться в пределах объема формулы изобретения.

Также нужно понимать, что если термин явно не определяется в данном патенте с использованием фразы «Как используется в данном документе, термин '_____' настоящим определяется, как означающий …» или подобной фразы, то не подразумевается ограничение значения этого термина, явное или косвенное, помимо его прямого или обычного значения, и такой термин не должен интерпретироваться как ограниченный в объеме на основании какого-либо утверждения, сделанного в каком-либо разделе данного патента (за исключением формулировок в формуле изобретения). В случае если какой-либо термин из пунктов формулы изобретения в конце данного патента упоминается в данном патенте таким образом, что он соответствует единственному значению, это делается только для ясности, чтобы не запутывать читателя. Это не подразумевает, что такой термин в пункте формулы изобретения ограничивается, косвенно или иначе, таким единственным значением. Наконец, если элемент пункта формулы изобретения не определяется словом «средство» и описанием функционирования, кроме подробного описания какой-либо структуры, это не подразумевает, что объем какого-либо элемента пункта формулы изобретения будет интерпретироваться на основании применения шестого пункта § 112 Раздела 35 Кодекса законов США.

Большая часть функциональных возможностей настоящего изобретения и многие принципы настоящего изобретения лучше всего реализуются в программах или инструкциях программного обеспечения и в интегральных схемах (ИС), таких как специализированные ИС, или с их использованием. Ожидается, что средний специалист в данной области техники, несмотря на возможно значительные усилия и многочисленные проектные решения, обусловленные, например, располагаемым временем, современной техникой и экономическими соображениями, руководствуясь идеями и принципами, раскрытыми в данном документе, будет способен без труда производить такие программы и инструкции программного обеспечения и ИС при проведении минимума исследований. Следовательно, для краткости и минимизации любого риска затруднения понимания принципов и идей настоящего изобретения дальнейшее обсуждение такого программного обеспечения и ИС, если таковые имеются, будет ограничено тем, без чего не обойтись в отношении предпочтительных вариантов осуществления.

Многие дорогостоящие компьютеры, персональные цифровые помощники, электронные записные книжки и т.п. предшествующего уровня техники не подходят для защищенного использования на основе подписки без модификации. Для возможности обеспечивать исполнение договора от поставщика услуг, т.е. «ПИУ» или

другой обеспечивающей исполнение обязательств организации, требуется способность влиять на работу устройства даже при том, что устройство может быть не подключено к поставщику услуг, например к сети Интернет. Первый этап мер по обеспечению исполнения обязательств может включать в себя простое предупреждение в виде всплывающего окна или с использованием другого графического интерфейса, указывающее приближение критической точки по условиям договора. Второй этап мер по обеспечению исполнения обязательств, например, после истечения оплаченных за использование минут или завершения периода подписки может состоять в представлении пользовательского интерфейса в системном режиме для увеличения суммы на счете и восстановления обслуживания. Последним рычагом поставщика для принуждения к исполнению условий соглашения о подписке или выплатах из текущих поступлений является блокирование устройства. Такой исключительный шаг может быть уместен, когда оказывается, что пользователь преднамеренно пытается нарушить ведение учета или работу других систем защиты, действующих в устройстве.

Применения возможности приведения электронного устройства в режим с ограниченной функциональностью могут выходить за рамки приложений с оплатой за использование и с подписной платой. Например, технологии для расхода мощностей могли бы использоваться для обеспечения соблюдения лицензий операционной системы или отдельных приложений.

Фиг.1 иллюстрирует логическое представление вычислительного устройства в форме компьютера 110, которое может использоваться в режиме с оплатой за использование или с подписной платой. В иллюстративных целях, компьютер 110 используется, чтобы продемонстрировать принципы настоящего раскрытия. Однако подобные принципы в равной степени применяются для других электронных устройств, включающих в себя, но не ограничивающихся этим, сотовые телефоны, персональные цифровые помощники, универсальные проигрыватели, бытовые приборы, игровые системы, развлекательные системы, телевизионные приставки и автомобильную электронику приборной панели, среди прочего. Обращаясь к Фиг.1, иллюстративная система для реализации заявляемых способа и устройства включает в себя вычислительное устройство общего назначения в форме компьютера 110. Компоненты, показанные обведенными пунктирной линией, формально не являются частью компьютера 110, но используются для демонстрации иллюстративного варианта осуществления на Фиг.1. Компоненты компьютера 110 могут включать в себя, но не ограничиваются этим, обрабатывающее устройство 112, системное запоминающее устройство 114, интерфейс 116 запоминающего устройства/графического взаимодействия, также известный как микросхема северного моста, и интерфейс 118 ввода/вывода, также известный как микросхема южного моста. Запоминающее устройство 114 и графическое обрабатывающее устройство 120 могут быть связаны с интерфейсом 116 запоминающего устройства/графического взаимодействия. Монитор 122 или другое устройство вывода графических данных может быть связано с графическим обрабатывающим устройством 120.

Набор системных шин может связывать различные системные компоненты, в том числе высокоскоростная системная шина 124 между обрабатывающим устройством 112, интерфейсом 116 запоминающего устройства/графического взаимодействия и интерфейсом 118 ввода/вывода, управляющая шина 126 между интерфейсом 116 запоминающего устройства/графического взаимодействия и системным запоминающим устройством 114, и шина 128 ускоренной обработки

графических данных (AGP - advanced graphics processing) между интерфейсом 116 запоминающего устройства/графического взаимодействия и графическим обрабатывающим устройством 120. Системная шина 124 может быть любого из нескольких типов шинных структур, включающих в себя, в качестве примера, но не ограничения, шину Архитектуры Промышленного Стандарта (ISA - Industry Standard Architecture), шину Микроканальной Архитектуры (MCA - Micro Channel Architecture) и Расширенную шину ISA (EISA - Enhanced ISA). Поскольку системные архитектуры развиваются, другие шинные архитектуры и наборы микросхем могут использоваться, но зачастую в целом являясь преемниками этой модели. Например, такие компании как Intel и AMD поддерживают хаб-архитектуру Intel (IHA - Intel Hub Architecture) и Гипертранспортную архитектуру соответственно.

Компьютер 110 обычно включает в себя множество машиночитаемых носителей. Машиночитаемые носители могут быть любыми имеющимися в распоряжении носителями, которые доступны посредством компьютера 110, и включают в себя как энергозависимые, так и энергонезависимые носители, как съемные, так и стационарные носители. В качестве примера, но не ограничения, машиночитаемые носители могут охватывать компьютерные носители данных и средства связи. Компьютерные носители данных включают в себя как энергозависимые, так и энергонезависимые носители, как съемные, так и стационарные носители, реализованные согласно любому способу или технологии для хранения такой информации, как машиночитаемые инструкции, структуры данных, программные модули или другие данные. Компьютерные носители данных включают в себя, но не ограничиваются этим, ОЗУ, ПЗУ, ЭСППЗУ, запоминающие устройства с групповой перезаписью или запоминающие устройства, созданные по другой технологии, компакт-диск, универсальный цифровой диск (DVD - digital versatile disks) или другое запоминающее устройство на оптическом диске, магнитные кассеты, магнитную ленту, запоминающее устройство на магнитном диске или другие магнитные запоминающие устройства, или любые другие носители, которые могут использоваться для хранения необходимой информации и которые могут быть доступны посредством компьютера 110. Средства связи обычно воплощают машиночитаемые инструкции, структуры данных, программные модули или другие данные в модулированном сигнале данных, таком как несущая волна или другой транспортный механизм, и включают в себя любые средства доставки информации. Термин «модулированный сигнал данных» означает сигнал, чья одна или более характеристики устанавливаются или изменяются таким образом, чтобы кодировать информацию в сигнале. В качестве примера, но не ограничения, средства связи включают в себя проводные средства, такие как проводная сеть или однопроводное соединение, и беспроводные средства, такие как акустическая волна, РЧ, инфракрасное излучение и другие беспроводные средства. Любые комбинации из вышеупомянутого также должны быть включены в сферу машиночитаемых носителей.

Системное запоминающее устройство 114 включает в себя компьютерные носители данных в форме энергозависимого и/или энергонезависимого запоминающего устройства, такого как постоянное запоминающее устройство (ПЗУ) 130 и оперативное запоминающее устройство (ОЗУ) 132. Системное ПЗУ 130 может содержать постоянные системные данные 134, такие как идентифицирующая и производственная информация. В некоторых вариантах осуществления базовая система ввода/вывода (БСВВ) также может храниться в системном ПЗУ 130. ОЗУ 132 обычно содержит данные и/или программные модули, которые непосредственно

доступны и/или в данный момент обслуживаются обрабатывающим устройством 112. В качестве примера, но не ограничения, Фиг.1 демонстрирует операционную систему 136, прикладные программы 138, другие программные модули 140 и программные данные 142.

Интерфейс 118 ввода/вывода может связывать системную шину 124 с рядом других шин 144, 146, и 148, которые соединяют множество внутренних и внешних устройств с компьютером 110. Шина 144 последовательного интерфейса периферийных устройств (SPI - Serial Peripheral Interface) может подключаться к запоминающему устройству 150 базовой системы ввода/вывода (БСВВ), содержащему в себе основные процедуры, способствующие передаче информации между элементами внутри компьютера 110. Например, БСВВ может исполняться в процессе начальной загрузки.

Микросхема 152 управляющего устройства ввода/вывода может использоваться для подключения ряда 'традиционных' периферийных устройств, таких как гибкий диск 154, клавиатура/мышь 156 и печатающее устройство 158. В одном варианте осуществления микросхема 152 управляющего устройства ввода/вывода подключается к интерфейсу 118 ввода/вывода с помощью шины 146 с малым числом выводов (LPC - low pin count). Микросхема управляющего устройства ввода/вывода широкодоступна на свободном рынке.

В одном варианте осуществления шина 148 может быть шиной Взаимодействия Периферийных Компонентов (PCI - Peripheral Component Interconnect), или ее разновидностью, и может использоваться для подключения высокоскоростных периферийных устройств к интерфейсу 118 ввода/вывода. Шина PCI также может именоваться как шина Расширения. Разновидности шины PCI включают в себя шины Скоростного Взаимодействия Периферийных Компонентов (PCI-E - Peripheral Component Interconnect-Express) и Расширенного Взаимодействия Периферийных Компонентов (PCI-X - Peripheral Component Interconnect - Extended), первая имеет последовательный интерфейс, а вторая обратно совместима с параллельным интерфейсом. В других вариантах осуществления шина 148 может быть шиной ATA (advanced technology attachment - присоединение по передовой технологии) для подключения накопителей, в форме последовательной шины ATA (SATA - Serial ATA) или параллельной шины ATA (PATA - Parallel ATA).

Компьютер 110 также может включать в себя другие съемные/стационарные, энергозависимые/энергонезависимые компьютерные носители данных. Только в качестве примера, Фиг.1 демонстрирует привод 160 жесткого диска, который считывает или осуществляет на них запись, стационарные энергонезависимые магнитные носители. Съемные носители, такие как запоминающее устройство 162, подключаемое с помощью универсальной последовательной шины (USB), или привод 164 CD/DVD, могут подключаться к шине PCI 148 напрямую или через интерфейс 166. Другие съемные/стационарные, энергозависимые/энергонезависимые компьютерные носители данных, которые могут использоваться в иллюстративной операционной среде, включают в себя, но не ограничиваются этим, кассеты с магнитной лентой, карты памяти с групповой перезаписью, универсальные цифровые диски, цифровую видеоленту, твердотельное ОЗУ, твердотельное ПЗУ и тому подобное.

Приводы и соотнесенные с ними компьютерные носители данных, обсуждавшиеся выше и продемонстрированные на Фиг.1, обеспечивают хранение машиночитаемых инструкций, структур данных, программных модулей и других данных для компьютера 110. На Фиг.1, например, привод 160 жесткого диска продемонстрирован

как хранящий операционную систему 168, прикладные программы 170, другие программные модули 172 и программные данные 174. Заметим, что эти компоненты могут как совпадать, так и отличаться от операционной системы 136, прикладных программ 138 других программных модулей 140 и программных данных 142. Операционной системе 168, прикладным программам 170, другим программным модулям 172 и программным данным 174 в данном документе назначены другие номера, чтобы продемонстрировать, что, по меньшей мере, они являются другими копиями. Пользователь может вводить команды и информацию в компьютер 110 через устройства ввода, такие, как мышь/клавиатура 156 или другая комбинация устройств ввода. Другие устройства ввода (не показаны) могут включать в себя микрофон, координатную ручку, игровой манипулятор, антенну спутниковой связи, сканирующее устройство или тому подобное. Эти и другие устройства ввода часто соединяются с обрабатывающим устройством 112 по одной из шин интерфейса ввода/вывода, такой как SPI 144, LPC 146 или PCI 148, но могут использоваться и другие шины. В некоторых вариантах осуществления другие устройства могут связываться с параллельными портами, инфракрасными интерфейсами, игровыми портами и тому подобным (не изображены) через посредство микросхемы 152 управляющего устройства ввода/вывода.

Компьютер 110 может функционировать в сетевой среде, используя логические соединения с одним или более удаленными компьютерами, такими как удаленный компьютер 178, через посредство сетевого интерфейсного управляющего устройства (NIC - network interface controller) 180. Удаленный компьютер 178 может быть персональным компьютером, обслуживающим узлом, устройством маршрутизации, сетевым ПК, равноправным устройством или другим публичным сетевым узлом, и обычно включает в себя многие или все элементы, описанные выше по отношению к компьютеру 110. Логическое соединение, изображенное на Фиг.1, может включать в себя локальную вычислительную сеть (ЛВС), глобальную вычислительную сеть (ГВС) или и то, и другое, но также может включать в себя другие сети. Такие сетевые среды являются обычным явлением в учрежденческих, корпоративных компьютерных сетях, внутрикорпоративных сетях на базе технологии Интернет и сети Интернет.

В некоторых вариантах осуществления сетевой интерфейс может использовать модем (не изображен), когда широкополосное соединение недоступно или не используется. Следует принять во внимание, что показанное сетевое соединение является иллюстративным и может использоваться другое средство для установления каналов связи между компьютерами.

Компьютер 110 также может включать в себя модуль защиты (МЗ) 182. МЗ 182 может быть способен осуществлять контроль защиты, управление использования с оплатой за использование или с подписной платой и обеспечение исполнения политики, связанной со сроками и условиями, соотнесенными с платным использованием. МЗ 182 может, в частности, быть пригодным для того, чтобы безопасно задействовать компьютер 110 в модели деловой деятельности с субсидированным приобретением. МЗ 182 может быть набором виртуализованных контейнеров, исполняющихся на обрабатывающем устройстве 112 или реальных контейнеров, таких как встроенное обрабатывающее устройство или управляющее устройство. В одном варианте осуществления МЗ 182 подключается к интерфейсу 118 ввода/вывода по шине SPI 144. В другом варианте осуществления МЗ 182 может быть воплощен в обрабатывающем устройстве 112, как автономный компонент, или в

гибридной схеме, такой как многокристальный модуль. Схема 184 синхронизации может быть частью МЗ 182, чтобы способствовать обеспечению защищенности от несанкционированного вмешательства. Чтобы предоставить возможность пользовательского управления настройками местного времени, включающими в себя переход на летнее время или перемещение между часовыми поясами, схема 184 синхронизации может поддерживать свое время в формате UTC (UTC - Universal Time, Coordinated - всемирное время по Гринвичу), а пользовательское время может рассчитываться, используя устанавливаемое пользователем смещение. МЗ 182 также может включать в себя криптографическую функцию или криптографическое ядро, которое может выполнять функцию устройства проверки подлинности для любого взаимодействия между МЗ 182 и другими устройствами. Например, криптографическое ядро МЗ 182 может обеспечивать подсистему обработки и шифрования модуля 182 защиты, которая достигает соответствующего Гарантированного Уровня Оценки Универсальных Критериев, чтобы гарантировать, что компьютер 110 и любое взаимодействие с МЗ 182 не могут быть дискредитированы.

Дополнительно, МЗ может включать в себя программно-аппаратное обеспечение и разновидность защищенного запоминающего устройства или устройства 186 хранения данных. Защищенное устройство 186 хранения данных может включать в себя подпрограммы или приложения, которые могут обеспечивать защищенную работу компьютера 110 при посредстве модуля 182 защиты. Дополнительно, защищенное устройство 186 хранения данных может включать в себя любые другие данные, к которым можно безопасно обращаться, сохранять или изменять их, без несанкционированного вмешательства. В одном варианте осуществления защищенное устройство 186 хранения данных включает в себя локальный модуль контроля использования, который управляет распределением времени использования. Локальный модуль контроля использования защищенного устройства 186 хранения данных может рассчитывать предварительно оплаченное время доступа пользователя или информацию о подписке и может описываться в Заявке на патент США Номер 10/988907, и Заявке на патент США Номер 11/612433, полное раскрытие которых настоящим включается в данный документ путем ссылки. Защищенное устройство 186 хранения данных также может хранить ключи шифрования или другую информацию для обеспечения защищенной связи с МЗ 182.

Устройство 186 хранения данных также может включать в себя устройство хранения данных для важных системных элементов, устройства, на котором работает МЗ 182. Защищенное устройство 186 хранения данных также может включать в себя запоминающее устройство, выделенное для непосредственной работы МЗ 182, такое, например, как устройство хранения данных для хранения тарифного кода для доступа к подписным данным и уменьшения их значения. Дополнительно, приложение для использования при обеспечении функциональных возможностей в период ограниченных режимов работы, таких как «режим аппаратного ограничения» (HLM - hardware limited mode), также может храниться в защищенном устройстве 186 хранения данных. Чтобы поддерживать ограниченный режим работы, вторая БСВВ, и дополнительно, альтернативная копия второй БСВВ, также может храниться в защищенном устройстве 186 хранения данных. Вторая БСВВ может использоваться для начальной загрузки компьютера или другого электронного устройства, в состав которого входит МЗ 182. Вторая БСВВ может задействоваться как защищенная среда начальной загрузки, чтобы заменить стандартную БСВВ 150, для обеспечения

соблюдения политики безопасности подписки или другой политики безопасности. Кроме того, МЗ 182 также может иметь возможность в любое время принудительно выполнить перезагрузку системы, что может гарантировать, что условия оплаты за использование или подписной платы выполняются, а также обеспечивает чистую среду для запуска БСВВ или для нормальной или для ограниченной работы.

Другое устройство 188 может хранить идентификацию пользователя и данные, связанные с подписным остатком на счете, для разблокирования компьютера 110, оснащенного МЗ 182. В одном варианте осуществления измерительное приложение, хранящееся в защищенном устройстве 186 хранения данных МЗ 182, может связываться с устройством 188 учета обработки данных для доступа к данным идентификации и подписного остатка на счете. Обращаясь к Фиг.2, устройство 188 учета обработки данных может быть съемным запоминающим устройством в любой форме. В одном варианте осуществления устройство 188 учета обработки данных представляет собой накопитель с памятью с групповой перезаписью, подключаемый по универсальной последовательной шине (UFD - USB flash drive). Устройство 188 учета обработки данных может включать в себя исполнительный блок 205, который может включать в себя обрабатывающее устройство для установления защищенного соединения с МЗ 182. В одном варианте осуществления при запуске или вставлении устройства 188 учета обработки данных МЗ 182 и устройство 188 учета обработки данных устанавливают защищенный канал связи, используя PKI (Public Key Infrastructure - инфраструктуру открытых ключей). Устройство 188 учета обработки данных может связываться с МЗ 182. В одном варианте осуществления устройство 188 связывается с МЗ 182 через интерфейс компьютера 110. Запоминающее устройство может связываться с компьютером 110 при посредстве любой комбинации 1394, USB, Интерфейса Малых Компьютерных Систем сети Интернет, последовательной связи, параллельной связи, инфракрасной связи, беспроводной связи ближнего радиуса действия, технологий BlueTooth, 802.x, или другого средства связи.

В дополнительном варианте осуществления устройство 188 связывается с модулем 182 защиты при посредстве БСВВ 150 или защищенной предзагрузочной среды, сохраненной в МЗ 182 защищенного устройства 186 хранения данных, что дополнительно объясняется ниже. Еще в одном дополнительном варианте осуществления устройство 188 учета обработки данных связывается с МЗ 182 при посредстве API, выполняющегося на компьютере 110. МЗ 182 может принудительно выполнить перезагрузку компьютера 110, если устройство 188 учета обработки данных, содержащее в себе данные подписки, удаляется.

Другие варианты осуществления могут включать в себя предохранитель 189 активации. Предохранитель 189 может быть любым устройством или аппаратно-программным обеспечением, которое может быть избирательно приведено в действие из неактивного состояния, чтобы допустить установление связи между интерфейсом 118 ввода/вывода и МЗ 182. При отключении, т.е. когда предохранитель 189 не поддерживает соединение между МЗ 182 и интерфейсом 118 ввода/вывода, компьютер 110 не может работать как подписное вычислительное устройство, а скорее, как обычный ПК. Однако при приведении в действие, т.е. когда предохранитель 189 поддерживает соединение между МЗ 182 и интерфейсом 118 ввода/вывода, компьютер может работать как подписное вычислительное устройство. В одном варианте осуществления предохранитель 189, однажды приведенный в действие, чтобы разрешить связь между МЗ 182 и другими компонентами и устройствами, не может быть отключен. Например, компьютер 110 может быть

изначально изготовлен для работы в качестве обычного, неподписного ПК, а позднее может быть активирован поручителем или подписчиком для работы в качестве подписного ПК. Следовательно, в то время как предохранитель активизирован и при начальной загрузке, подключении или отключении устройства 188, аппаратно-программное обеспечение МЗ 182 (т.е. вышеописанный локальный модуль контроля использования защищенного устройства 186 хранения данных) может произвести поиск суммы подписки или времени использования, сохраненных на устройстве 188 учета обработки данных.

Возвращаясь к Фиг.2, устройство 188, как проиллюстрировано, может быть представлено и выполнено в разных формах, чтобы включать в себя элементы, которые описываются ниже. Например, устройство 188 может включать в себя интерфейс 207, который может предоставить возможность связи между устройством 188 и МЗ 182. Как описано выше, устройство 188 может связываться с компьютером 110 через МЗ 182 при посредстве любой комбинации 1394, USB, Интерфейса Малых Компьютерных Систем сети Интернет, последовательной связи, параллельной связи, инфракрасной связи, беспроводной связи ближнего радиуса действия, технологий BlueTooth, 802.x, или другого средства связи. В одном варианте осуществления интерфейс 205 представляет собой штырьковый USB-разъем типа A, который обеспечивает интерфейс для главного компьютера 110.

Устройство 188 также может включать в себя область 210 памяти или данных. Областью 210 данных может быть отдельный кристалл памяти с групповой перезаписью, или множественные кристаллы памяти с групповой перезаписью, которые хранят уникальную идентификацию аппаратного оборудования (HWID - hardware identification), или Универсальный Идентификатор, или UPID могут однозначно идентифицировать устройство для любого другого подключенного устройства, например вычислительного устройства 110 или удаленного вычислительного устройства 178. В дополнительном варианте осуществления устройство 188 может хранить данные, отражающие данные 220 подписки или доступа пользователя, для разблокирования компьютера 110 или исполнения приложений учета обработки данных. Дополнительно, область 210 данных может включать в себя конфигурационные данные 222. В одном варианте осуществления конфигурационные данные могут предоставлять информацию, которая может осуществлять привязку компьютера 110, который задействует устройство 188, к конкретному поставщику интернет-услуг (ПИУ).

Кроме того, как обсуждалось выше, устройство 188 учета обработки данных может включать в себя исполнительный блок 205, который может предоставить возможность защищенного соединения между устройством 188 и любым другим устройством, например компьютером 110. В одном варианте осуществления исполнительный блок 205 включает в себя криптографическую функцию, как описано выше по отношению к защищенному устройству 186 хранения данных МЗ 182. Криптографическую функцию устройства 188, которая может выполнять функцию модуля проверки подлинности для любого взаимодействия между устройством 188 и компьютером 110. Например, криптографическая функция исполнительного блока 205 может обеспечивать подсистему обработки и шифрования устройства 188, которая достигает соответствующего Гарантированного Уровня Оценки Универсальных Критериев, чтобы гарантировать, что устройство 188 и любое взаимодействие между устройством 188 и компьютером 110 не могут быть дискредитированы. В одном варианте осуществления криптографическое ядро и исполнительный блок 205

выполняют функцию карт со встроенным микропроцессором серии SLE, которые производятся компанией Infineon Technologies AG, Мюнхен, Германия.

Другие варианты осуществления устройства 188 учета обработки данных включают в себя батарею 230 для сохранения некоторых данных из области 210 данных или возможности обеспечения источника энергии для индикатора 235, который может приводиться в действие, когда подписные данные 220 достигают порогового значения, или устройство 188 дискредитировано, или больше не может функционировать. Несколько светодиодов индикатора 235 могут сообщать пользователю различные уведомления, например уведомление о низком временном балансе 220 или другом балансе использования или уведомление о полном или достаточном балансе. Индикатор 235 также может включать в себя видеоэкран, который передает в численном выражении баланс времени доступа, оставшийся на устройстве 188, или любую другую информацию, связанную с любыми данными, хранящимися на устройстве 188.

Фиг.3 является упрощенной и иллюстративной структурной схемой системы 300, поддерживающей использование компьютера или другого электронного устройства с оплатой за использование и с подписной платой. Обслуживающий узел 302 контроля использования может служить высоконадежной конечной точкой для запросов на предоставление услуг от одного или более электронных устройств, участвующих в деловой экосистеме с оплатой за использование.

Одно электронное устройство 304 может быть подобным компьютеру 110, показанному на Фиг.1, с подключенным устройством 188 учета обработки данных. Другие электронные устройства 306 могут функционировать в основном так же, как иллюстративное устройство 304. Связь между обслуживающим узлом 302 контроля использования и электронным устройством 304 может осуществляться по сети 308, которая может включать в себя наземную линию связи, радиосвязь или широкополосные сети, или другие сети, известные в данной области техники.

Расчетный обслуживающий узел 310 может быть связан с обслуживающим узлом 302 контроля использования и может поддерживать данные учетной записи, соответствующие электронному устройству 304. Данные учетной записи также могут сохраняться на устройстве 188. Расчетный обслуживающий узел 310 также может служить расчетным центром для финансовых операций, связанных с электронным устройством 304, таких как пополнение или увеличение суммы на счете для учетной записи с оплатой за использование, поддерживаемой на расчетном обслуживающем узле 310 и записанной на устройстве 188. В одном варианте осуществления электронное устройство 304, использующее устройство 188 учета обработки данных, устанавливает соединение со средством 312 продаж, которое связывается с расчетным обслуживающим узлом 310. В другом варианте осуществления устройство 188 учета обработки данных устанавливает соединение непосредственно с расчетным обслуживающим узлом 310. Средство продаж может представлять собой торговый автомат или другой автономный киоск самообслуживания. Пользователь может подключить 312 продаж, выбрать количество подписного времени для ОС, приложения, или иного, для загрузки на устройство 188, произвести оплату и получить данные доступа. Данными доступа может быть какая-либо сумма на счете, время 220 доступа к какой-либо защищенной ОС или приложению электронного устройства 304, 306, или любые другие данные, которые могут быть записаны на расчетном обслуживающем узле 310 и сохранены на устройстве 188 для использования компьютером 110. В дополнительном варианте осуществления пользователь может

приобрести общее количество времени, которое может использоваться для любой ОС, приложения, или любой другой работы на защищенном электронном устройстве 304. Конечно, многие другие данные, время доступа и информация о подписке могут приобретаться и сохраняться на устройстве 188 учета обработки данных.

В одном сценарии пользователь, желающий добавить время на устройство 188, может подключить устройство 188 к средству 312 продаж в розничной торговой точке или через другой компьютер 110, переместиться через последовательность пользовательских интерфейсов для осуществления оплаты времени 220 доступа и загрузки времени 220 на устройство 188. После этого пользователь может использовать приобретенное время 220 на клиентском устройстве 110 с защищенной обработкой данных, подключив устройство 188 к компьютеру 110. После этого устройство 188 может установить защищенное соединение с компьютером 110, который может, в свою очередь, передать код на обслуживающий узел 302, который возвращает подписанный пакет на компьютер 110. Пакет может содержать в себе данные, отображающие количество времени 220, приобретенного пользователем. Компьютер 110 может использовать время 220 доступа из устройства 188, пересылая данные об этом на LPM (LPM - lower provisioning module - модуль контроля использования нижнего уровня) защищенного устройства 186 хранения данных, и временной баланс 220 может обновляться. Как объяснялось выше, LPM может исполняться в модуле 182 защиты или другом аппаратном или с аппаратной поддержкой "контейнере" в системе 110. В одном варианте осуществления LPM осуществляет доступ к приобретенным временным балансам, имеющимся на устройстве 188, и обновляет их. В другом варианте осуществления LPM синхронизирует временной баланс на устройстве 188 с балансом, локально сохраненным в защищенном устройстве 186 хранения данных. Когда приобретенное время 220 истекает или расходуется на компьютере 110, пользователю может быть выдано несколько предупреждений, которые могут сопровождаться сокращением функциональных возможностей компьютера 110. Если пользователь не осуществляет оплату большего количества времени 220 доступа, компьютер 110, в конечном счете, переходит в режим, в котором пользователю может быть представлен текстовый интерфейс, который может позволить ему только подключить пополненное устройство 188. В этом состоянии, которое может именоваться как Режим Аппаратной Блокировки (HLM - Hardware Locked Mode), компьютер 110 может быть непригоден ни для чего, кроме подключения действующего устройства 188. Компьютер 110 может ввести в действие HLM, только работая в Режиме Управления Системой (SMM - System Management Mode), который может не разрешить операционным системам или приложениям загружать что-либо, кроме ограниченной БСВВ для HLM и связанного кода.

В другом сценарии пользователь приобретает количество времени для использования такого оплачиваемого программного обеспечения на компьютере 110, как ОС, приложения или и то, и другое. Пользователь также может приобрести возможность использовать оплачиваемую обработку текстов или другие приложения, хранящиеся на компьютере 110, исходя из количества использований, количества полных страниц, или любого другого измеримого использования. Как только пользователь исчерпывает приобретенное использование 220 для приложения, пользователь не может обратиться к приложению с компьютера 110, пока не будет приобретено больше времени. В одном варианте осуществления, приложения в устройстве 304, 306 хранятся в защищенной области 186 данных таким образом, что

нет возможности установить или сохранить приложение на жестком диске 160 компьютера 110. Например, приложения в компьютере 110 могут быть в формате Softgrid®, разработанном Корпорацией Microsoft, Редмонд, Вашингтон.

Пользователь может перевести его или ее доступ к компьютеру 110 в системе с оплатой за использование на любой компьютер 110, выполненный с возможностью доступа к устройству 188 учета обработки данных. В одном варианте осуществления пользователь переносит его или ее время использования на компьютер 110 в кафе с предоставлением доступа в сеть Интернет, в котором есть машины с модулем 182 защиты. Компьютер 110 в кафе может функционировать, только если клиент подключает устройство 188 учета обработки данных, которое содержит действующие данные 220 времени доступа. Широко известны и другие системы платежей для учетной записи с предоплатой, например, применительно к предварительно оплаченным сотовым телефонам или другим подвижным вычислительным системам, равно пригодные в этой модели деловой деятельности.

Фиг.4 является упрощенной и иллюстративной функциональной схемой способа 400 для предоставления возможности защищенному компьютеру 110 использовать переносное запоминающее устройство 188 для контролирования и хранения количества приобретенного доступа или подписного времени 220 для операционных систем 136, 168, прикладных программ 138, 170, других программных модулей 140, 172 и других данных 142, 174. Способ 400 содержит ряд действий, графически представленных на Фиг.4 в виде блоков. Действия могут исполняться в любом подходящем порядке для выполнения описываемой задачи. На этапе 405 компьютер 110 может загружаться или перезагружаться. Например, если перед включением компьютера 110 пользователь подключает устройство 188, компьютер 110 может конфигурироваться своей БСВВ 150 для проверки соединения с устройством 188 в процессе начальной загрузки. Если пользователь подключает устройство 188 после начальной загрузки, компьютер 110 может перезагрузиться, чтобы начать работать с устройством 188.

Процесс загрузки может предполагать следование нормальной последовательности загрузки, известной в данной области техники, за исключением того, что запрос на код БСВВ от интерфейса 118 ввода/вывода не может привести к чтению загрузочного кода БСВВ непосредственно из запоминающего устройства, например запоминающего устройства 150, но может привести к запросу от интерфейса 118 ввода/вывода к МЗ 182 на загрузочный код БСВВ, хранящийся в защищенном устройстве 186 хранения данных, например БСВВ защищенной загрузочной среды. В одном варианте осуществления интерфейс ввода/вывода обращается к БСВВ в МЗ 182, только если предохранитель 189 активизирован, как описано выше.

На этапе 410 может устанавливаться связь между устройством 188 и компьютером 110. В одном варианте осуществления связь между устройством 188 и компьютером 110 может быть защищенной. Например, защищенный канал может быть установлен между устройством 188 и компьютером 110 при помощи, по меньшей мере, или описанного выше криптографического ядра защищенного устройства 186 хранения данных в МЗ 182, или криптографической функции исполнительного блока 205 устройства 188. HWID/UPID 215 устройства 188 также могут подтверждаться при помощи МЗ 182 для установления защищенной связи.

В дополнительном варианте осуществления или выделенный, или аппаратно коммутируемый порт связи может использоваться для установления защищенной связи между устройством 188 и компьютером. При начальной загрузке между

устройством 188 и МЗ 182 может создаваться выделенный тракт, который может быть USB-трактом связи, который напрямую соединяет устройство 188 с МЗ 182. В процессе работы устройство 188 остается подключенным к порту, напрямую соединяющим его с МЗ 182 в процессе работы. Сигнал периодического контрольного сообщения, обмен которым происходит между МЗ 182 и устройством 188, может контролироваться аппаратно-программным обеспечением МЗ 182, чтобы гарантировать поддержание защищенной связи.

В качестве альтернативы коммутационное аппаратное обеспечение может регулировать уплотнение тракта, дополнительным трактом с использованием ОС в качестве посредника, после того, как компьютер 110 завершает загрузку и устанавливает защищенный канал. Поскольку коммутируемый тракт также может использовать ОС и различные управляющие программы в качестве магистрали, переключение с тракта может происходить в процессе начальной загрузки, что может привести к риску нарушения защиты. Чтобы снизить вероятность риска нарушения защиты, в состав защищенного устройства 186 хранения данных МЗ 182 может быть включен контрольный счетчик времени. В одном варианте осуществления контрольный счетчик времени устанавливается на продолжительность, учитывающую загрузку управляющей программы и ОС. Если на этапе 412 контрольный счетчик времени завершает работу прежде, чем защищенный канал через ОС восстановится, компьютер 110 может быть перезагружен или переведен в ухудшенный режим, что описывается для этапа 420. В одном варианте осуществления контрольный счетчик времени распознает защищенный канал, принимая сигнал периодического контрольного сообщения, порожденный МЗ 182 и отправленный приложению-посреднику ОС через USB-стеки, и на устройство 188. Используя или выделенный, или коммутируемый тракт, МЗ 182 задерживает сигнал "power OK" (готовность источника питания к использованию) для обрабатывающего устройства 112 и загружает в МЗ 182 Модуль Предоставления Услуг Нижнего Уровня (LPM) защищенного устройства 186 хранения данных. После этого МЗ 182 может обменяться с устройством 188 регистрационными данными, например инфраструктурой открытых ключей, по установленному защищенному тракту.

На этапе 415 МЗ 182 может проверить баланс времени 220 на устройстве 188. В одном варианте осуществления LPM защищенного устройства 186 хранения данных может обратиться к устройству 188, чтобы проверить временной баланс 220. Если на устройстве не осталось времени или время ниже пороговой величины, на этапе 420 компьютер 110 может войти в ухудшенный режим работы. В одном варианте осуществления МЗ 182 вводит компьютер 110 в еще более ухудшенное рабочее состояние, в результате чего компьютер 110 входит в Режим Аппаратной Блокировки, как описано выше. Пользовательский интерфейс Режима Аппаратной Блокировки может запросить, чтобы пользователь подключил устройство 188 с действующим временным балансом. Компьютер 110 может войти в ухудшенный режим, обращаясь к БСВВ ограниченной работы, сохраненной на МЗ 182. Значение времени не может уменьшаться на устройстве 188, пока компьютер 110 находится в Режиме Аппаратной Блокировки.

Дополнительно, LPM может обращаться к конфигурационным данным 222 устройства. В одном варианте осуществления конфигурационные данные 222 могут позволить LPM осуществлять привязку устройства 188 к конкретному ПИУ. Например, конфигурационные данные 222 могут быть ключами подтверждения подлинности, реализующими PKI, которая может представлять установление

подлинности и полномочий между пользователем и ПИУ. Может производиться обмен этими ключами в процессе начального предоставления услуг от устройства 188, например, при подключении к компьютеру 110.

Если на этапе 415 остается время на устройстве 188, на этапе 425 компьютер 110 может работать. В одном варианте осуществления компьютер может работать согласно БСВВ нормальной работы, доступной компьютеру 110 из МЗ 182 защищенного устройства 186 хранения данных или из запоминающего устройства 150. Действия пользователя в процессе работы могут регулироваться согласно подписным или другим данным 220 доступа, сохраненным на устройстве 188. Например, пользователь может иметь приобретенный доступ 220 к операционной системе 136, 168, к отдельным или группам прикладных программ 138, 170, или к другим модулям 140, 172, сохраненным на компьютере 110. Дополнительно, время 220 доступа может позволить пользователю использовать приложения, сохраненные на защищенном устройстве 186 хранения данных в МЗ 182. Как описано ранее, операционная система(ы) и приложения могут быть представлены в формате Softgrid®, чтобы к ним можно было получать безопасный доступ с компьютера 110, без сохранения на нем. Работа компьютера 110 также может включать в себя уменьшение значения данных 220 доступа, связанных с исполняемыми программами. В одном варианте осуществления LPM в МЗ 182 может постоянно уменьшать значение и изменять данные 220 доступа устройства 188.

На этапе 430 компьютер 110 может проверить соединение, установленное с устройством 188 на этапе 410. Если устройство 188 больше не подключено к компьютеру 110, он может перейти в ухудшенный режим, как описано по отношению к этапу 420. Если устройство 188 остается подключенным к компьютеру 100, способ 400 может перейти к этапу 415 для повторной проверки баланса и продолжения.

Фиг.5 является другой упрощенной и иллюстративной функциональной схемой способа 500 для предоставления возможности защищенному компьютеру 110 использовать переносное запоминающее устройство 188 для контролирования и хранения количества приобретенного доступа или подписного времени 220 для операционных систем 136, 168, прикладных программ 138, 170, других программных модулей 140, 172 и других данных 142, 174. На этапе 505 компьютер 100 может загружаться или перезагружаться, как описано по отношению к Фиг.4. Как и ранее, МЗ 182 может задержать сигнал "power OK" для интерфейса 118 ввода/вывода, чтобы загрузить в МЗ 182 LPM защищенного устройства 186 хранения данных. Однако, поскольку еще не установлен защищенный канал, LPM не может получить доступ к каким-либо подписным или временным данным 220 на устройстве 188.

На этапе 510 МЗ 182 может установить защищенный канал с устройством 188. В одном варианте осуществления МЗ 182 может загрузить защищенную загрузочную среду, сохраненную в защищенном устройстве 186 хранения данных. Например, МЗ 182 может загрузить БСВВ для защищенной конфигурации из защищенного устройства 186 хранения данных. Эта БСВВ может содержать процедуры, чтобы регистрировать и подключать защищенный канал между МЗ 182 и устройством 188. В дополнительном варианте осуществления БСВВ для защищенной загрузочной среды может быть написана с минимальным кодом, чтобы снизить возможные риски нарушения защиты. Затем МЗ 182 может обменяться регистрационными данными с устройством 188, чтобы установить защищенный канал.

На этапе 515 МЗ 182 может проверить баланс времени 220 на устройстве 188, как

описано по отношению к этапу 415. Если на устройстве не осталось времени, на этапе 520 компьютер 110 может войти в ухудшенный режим работы. Если на этапе 515 остается время на устройстве 188, на этапе 525 компьютер 110 может работать. Как и ранее, работа компьютера 110 также может включать в себя уменьшение значения данных 220 доступа, связанных с исполняемыми программами. На этапе 530 компьютер 110 может проверить соединение, установленное с устройством 188 на этапе 510. Если устройство 188 больше не подключено к компьютеру 110, он может перейти в ухудшенный режим на этапе 520, как описано по отношению к этапу 420. Если устройство 188 остается подключенным к компьютеру 100, способ 500 может перейти к этапу 515 для повторной проверки баланса и продолжения.

Фиг.6 является другой упрощенной и иллюстративной функциональной схемой способа 600 для предоставления возможности защищенному компьютеру 110 использовать переносное запоминающее устройство 188 для контролирования и хранения количества приобретенного доступа или подписного времени 220 для операционных систем 136, 168, прикладных программ 138, 170, других программных модулей 140, 172 и других данных 142, 174. На этапе 605 компьютер 110 может загружаться в обычном режиме, как будто LPM устройства 188 уже обнаружил положительный баланс на устройстве 188. На этапе 610 МЗ 182 может запустить контрольный счетчик времени, который может контролировать сигнал периодического контрольного сообщения от устройства 188 во времени. В другом варианте осуществления контрольный счетчик времени может контролировать сигнал периодического контрольного сообщения по установленному защищенному каналу между МЗ 182 и устройством 188. В одном варианте осуществления контрольный счетчик времени хранится и исполняется в пределах защищенного устройства 186 хранения данных в МЗ 182. После того, как выполнена начальная загрузка, на этапе 615 программное обеспечение, исполняющееся в пределах загруженной ОС, может установить защищенный канал от МЗ 182 к устройству 188. В другом варианте осуществления, МЗ 182 обменивается регистрационными данными с устройством 188 и порождает сигнал периодического контрольного сообщения.

Если на этапе 620 контрольный счетчик времени завершает работу прежде, чем принимается сигнал периодического контрольного сообщения, указывающий, что установлен защищенный канал между МЗ 182 и устройством 188, то на этапе 625 МЗ 182 может ввести компьютер 110 в ухудшенный рабочий режим. В качестве альтернативы при завершении работы контрольного счетчика времени МЗ 182 может принудительно выполнить перезагрузку компьютера 110. Если, однако, контрольный счетчик времени не завершил работу, на этапе 630 способ 600 может работать, как описано по отношению к Фиг.4 и 5.

На этапе 630 МЗ 182 может проверить баланс времени 220 на устройстве 188, как описано по отношению к этапу 415. Если на устройстве не осталось времени, на этапе 625 компьютер 110 может войти в ухудшенный режим работы. Если на этапе 630 остается время на устройстве, на этапе 635 компьютер 110 может работать. Как и ранее, работа компьютера 110 также может включать в себя уменьшение значения данных 220 доступа, связанных с исполняемыми программами. На этапе 640 компьютер 110 может проверить соединение, установленное с устройством 188 на этапе 615. Если устройство 188 больше не подключено к компьютеру 110, он может перейти в ухудшенный режим, как описано по отношению к этапу 420. Если устройство 188 остается подключенным к компьютеру 100, способ 600 может перейти к этапу 630 для повторной проверки баланса и продолжения.

Таким образом, устройство 188 может разблокировать защищенный компьютер 110 благодаря сохранению количества приобретенного доступа или подписного времени 220 для операционных систем 136, 168, прикладных программ 138, 170, других программных модулей 140, 172 и других данных 142, 174. Благодаря обеспечению защищенного канала связи между модулем 182 защиты компьютера 110 и устройством 188 пользователи подписной или с оплатой за использование вычислительной системы могут разблокировать любой защищенный компьютер 110 с помощью информации о подписке и доступе, сохраненной на переносном запоминающем устройстве 188.

Многочисленные модификации и изменения могут быть сделаны в технологиях и структурах, описанных и продемонстрированных в данном документе, не отступая от сущности и объема настоящего изобретения. Соответственно необходимо понимать, что способы и устройство, описанные в данном документе, являются лишь иллюстративными и не ограничивают объем настоящего изобретения.

Формула изобретения

1. Система для разблокировки подписного режима компьютера, содержащая:

упомянутый компьютер;

модуль защиты, который размещен на компьютере и сконфигурирован для осуществления связи со съемным устройством учета обработки данных, содержащим криптографический блок, блок исполнения, идентификатор, который уникальным образом идентифицирует съемное устройство учета обработки данных, и защищенную флэш-память, хранящую некоторое количество единиц учета подписки, ассоциированное с пользователем, причем модуль защиты содержит:

защищенную среду начальной загрузки, сконфигурированную для регистрации устройства учета обработки данных на компьютере в ответ на присоединение пользователем устройства учета обработки данных к компьютеру с возможностью осуществления связи;

модуль связи, сконфигурированный для установления, в ответ на упомянутую регистрацию, защищенного канала связи между блоком исполнения съемного устройства учета обработки данных и модулем защиты через защищенную среду начальной загрузки;

модуль контроля использования, сконфигурированный для доступа к, уменьшения и сохранения, в ответ на упомянутое установление, количества единиц учета подписки, хранящегося в защищенной флэш-памяти съемного устройства учета обработки данных, в процессе эксплуатации компьютера пользователем;

модуль проверки подлинности, сконфигурированный для связи с криптографическим блоком и для проверки защищенного канала связи в ответ на упомянутое установление; и

модуль обработки, сконфигурированный для разрешения исполнения по меньшей мере одного приложения на компьютере в ответ на упомянутую проверку защищенного канала связи и для дополнительной проверки того, что упомянутое количество единиц учета подписки остается выше порогового значения,

при этом модуль защиты дополнительно сконфигурирован для принудительной реализации перезагрузки компьютера в защищенную среду начальной загрузки в ответ на потерю связи между съемным устройством учета обработки данных и модулем защиты.

2. Система по п.1, в которой защищенный канал связи содержит выделенный тракт

между съемным устройством учета обработки данных и модулем защиты.

3. Система по п.1, в которой защищенный канал связи содержит аппаратно-коммутируемый порт связи между съемным устройством учета обработки данных и модулем защиты.

4. Система по п.3, в которой аппаратно-коммутируемый порт связи включает в себя модуль мультиплексирования, сконфигурированный для обеспечения защищенной связи между съемным устройством учета обработки данных и модулем защиты через выбранное одно из выделенного тракта и операционной системы компьютера.

5. Система по п.1, дополнительно содержащая модуль контрольного счетчика времени, сконфигурированный для измерения количества времени для загрузки операционной системы и драйверов компьютера.

6. Система по п.5, дополнительно содержащая модуль блокировки, сконфигурированный для ограничения исполнения упомянутого по меньшей мере одного приложения в ответ на то, что количество времени, отмеренное модулем контрольного счетчика времени, превышает пороговое значение.

7. Система по п.1, дополнительно содержащая модуль привязки, сконфигурированный для ограничения компьютеру возможности доступа к по меньшей мере одному поставщику Интернет-услуг.

8. Система по п.1, в которой посредством защищенного канала связи съемное устройство учета обработки данных связывается только с модулем защиты.

9. Способ разблокировки подписного режима компьютера, включающего в себя модуль защиты, причем способ содержит этапы, на которых: устанавливают соединение между съемным устройством учета обработки данных и модулем защиты компьютера через защищенную среду начальной загрузки, хранящуюся в компьютере, при этом съемное устройство учета обработки данных включает в себя некоторое количество единиц учета доступа, хранящееся в защищенной флэш-памяти съемного устройства учета обработки данных;

обеспечивают защиту соединения между устройством учета обработки данных и модулем защиты;

определяют, превышает ли упомянутое количество единиц учета доступа пороговое значение;

ограничивают функционирование компьютера, если упомянутое количество единиц учета доступа ниже порогового значения; исполняют по меньшей мере одно приложение на компьютере, если упомянутое количество единиц учета доступа выше порогового значения; поддерживают защищенное соединение между устройством учета обработки данных и модулем защиты в процессе исполнения этого по меньшей мере одного приложения;

уменьшают упомянутое количество единиц учета доступа в процессе исполнения упомянутого по меньшей мере одного приложения; и в ответ на потерю связи между съемным устройством учета обработки данных и модулем защиты принудительно реализуют перезагрузку компьютера в защищенную среду начальной загрузки.

10. Способ по п.9, в котором соединение между устройством учета обработки данных и модулем защиты содержит выделенный тракт.

11. Способ по п.9, дополнительно содержащий этапы, на которых:

мультиплексируют соединение между одним из выделенного тракта и операционной системы компьютера;

измеряют количество времени для загрузки операционной системы и драйверов компьютера; и

ограничивают исполнение упомянутого по меньшей мере одного приложения в ответ на то, что измеренное количество времени выше порогового значения.

12. Способ по п.9, в котором съемное устройство учета обработки данных включает в себя конфигурационные данные поставщика услуг.

13. Способ по п.12, дополнительно содержащий этапы, на которых:

идентифицируют поставщика услуг и данные доступа поставщика, исходя из конфигурационных данных поставщика услуг; и

привязывают компьютер к идентифицированному поставщику услуг, используя данные доступа поставщика.

14. Система для разблокировки подписного режима компьютера, включающая в себя съемное устройство учета обработки данных, связанное с модулем защиты из состава компьютера, причем по меньшей мере одно из съемного устройства учета обработки данных и модуля защиты включает в себя защищенное запоминающее устройство и защищенный процессор, выполненный с возможностью исполнения машиноисполняемого кода для выполнения способа, содержащего этапы, на которых:

устанавливают защищенное соединение между съемным устройством учета обработки данных и модулем защиты компьютера через защищенную среду начальной загрузки, хранящуюся в компьютере; передают некоторое количество единиц учета доступа из защищенной флэш-памяти съемного устройства учета обработки данных в модуль защиты;

исполняют по меньшей мере одно приложение компьютера в ответ на то, что упомянутое количество единиц учета доступа выше порогового значения;

ограничивают функционирование компьютера в ответ на то, что упомянутое количество единиц учета доступа ниже порогового значения; и в ответ на потерю связи между съемным устройством учета обработки данных и модулем защиты принудительно реализуют перезагрузку компьютера в защищенную среду начальной загрузки.

15. Система по п.14, в которой соединение между устройством учета обработки данных и модулем защиты содержит выделенный тракт.

16. Система по п.14, в которой способ дополнительно содержит этапы, на которых:

мультиплексируют защищенное соединение между одним из выделенного тракта и операционной системы компьютера;

измеряют количество времени для загрузки операционной системы и драйверов компьютера; и

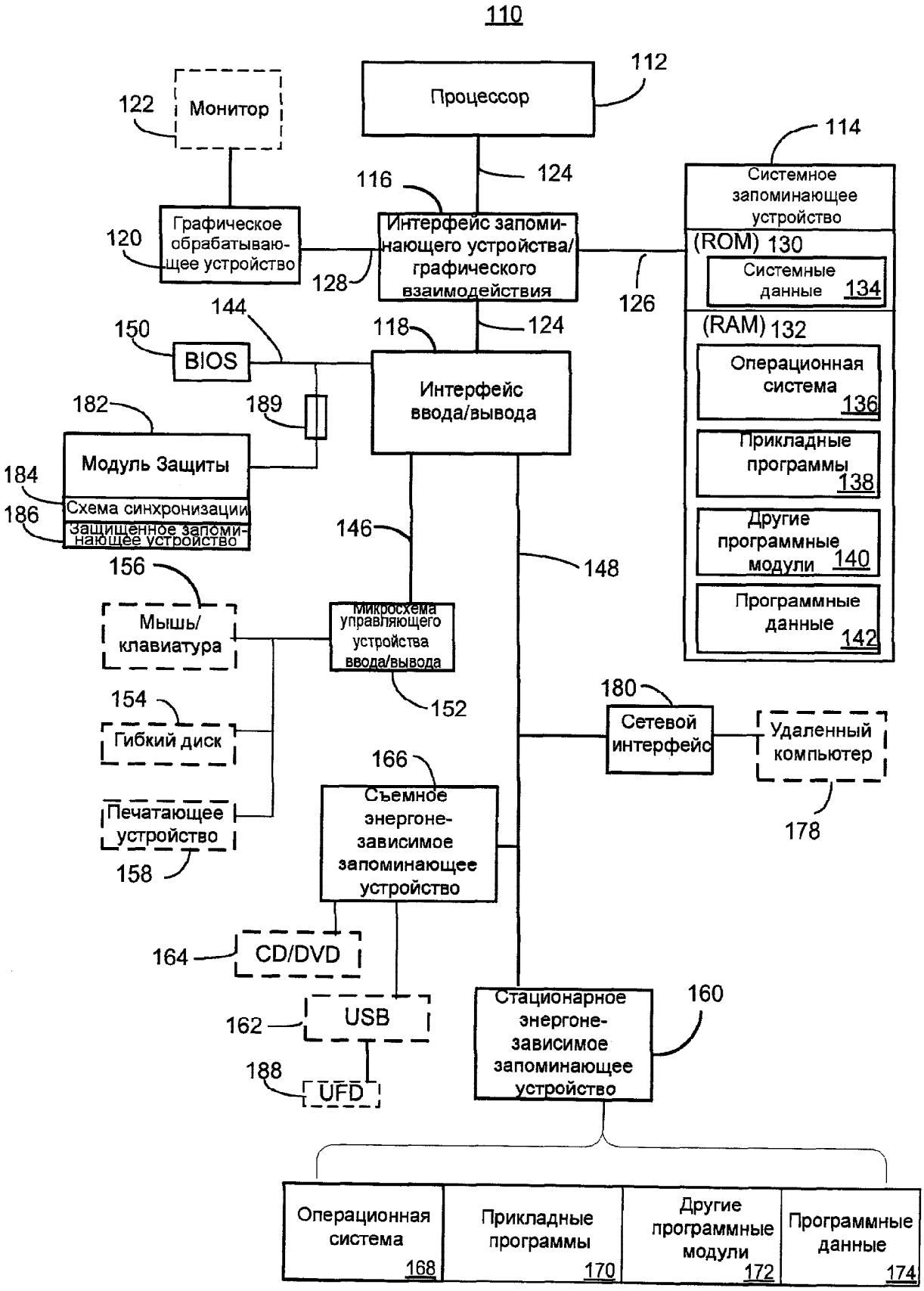
ограничивают исполнение упомянутого по меньшей мере одного приложения в ответ на то, что измеренное количество времени выше порогового значения.

17. Система по п.14, в которой съемное устройство учета обработки данных включает в себя конфигурационные данные поставщика услуг.

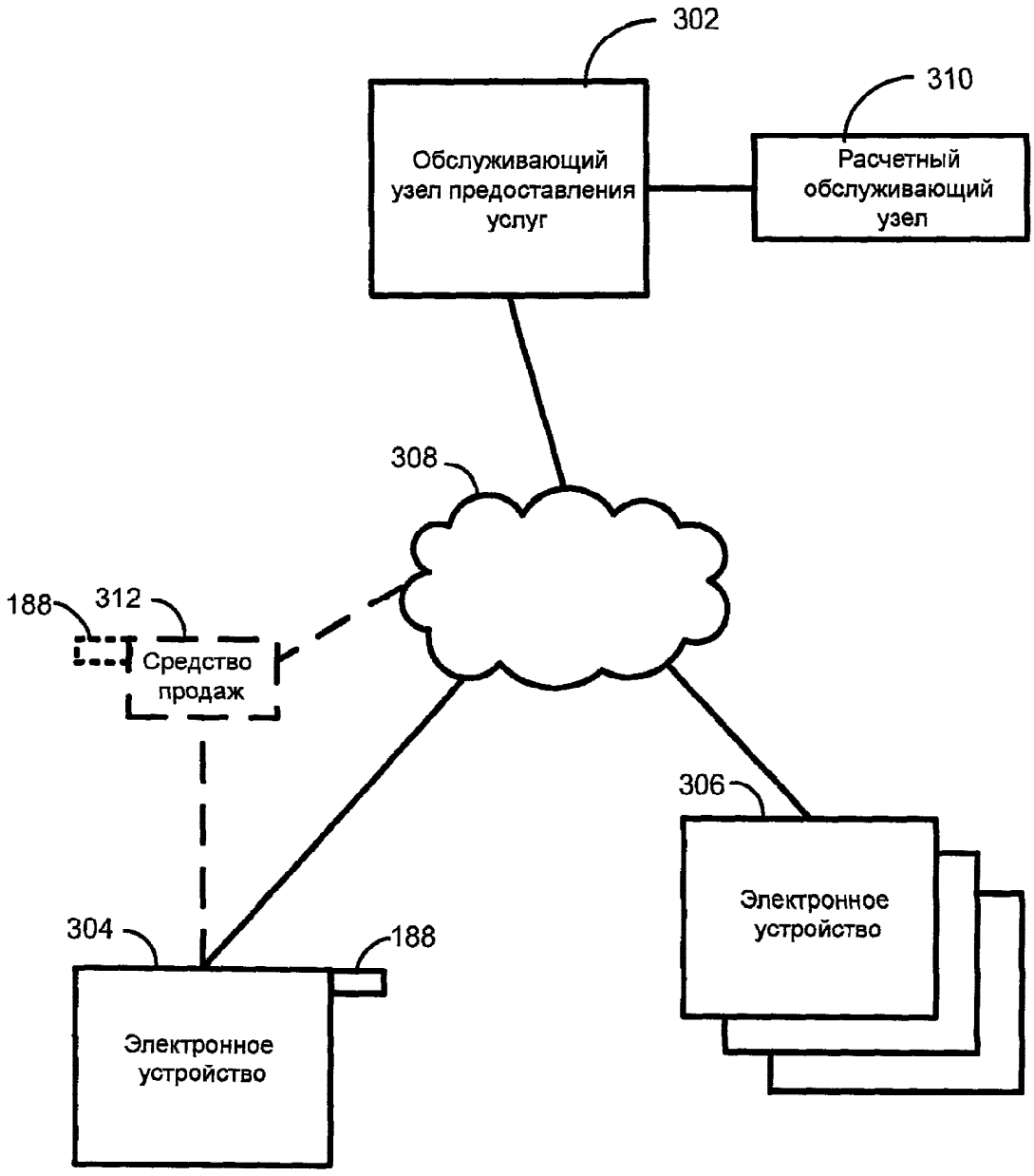
18. Система по п.17, в которой способ дополнительно содержит этапы, на которых:

идентифицируют поставщика услуг и данные доступа поставщика, исходя из конфигурационных данных поставщика услуг; и

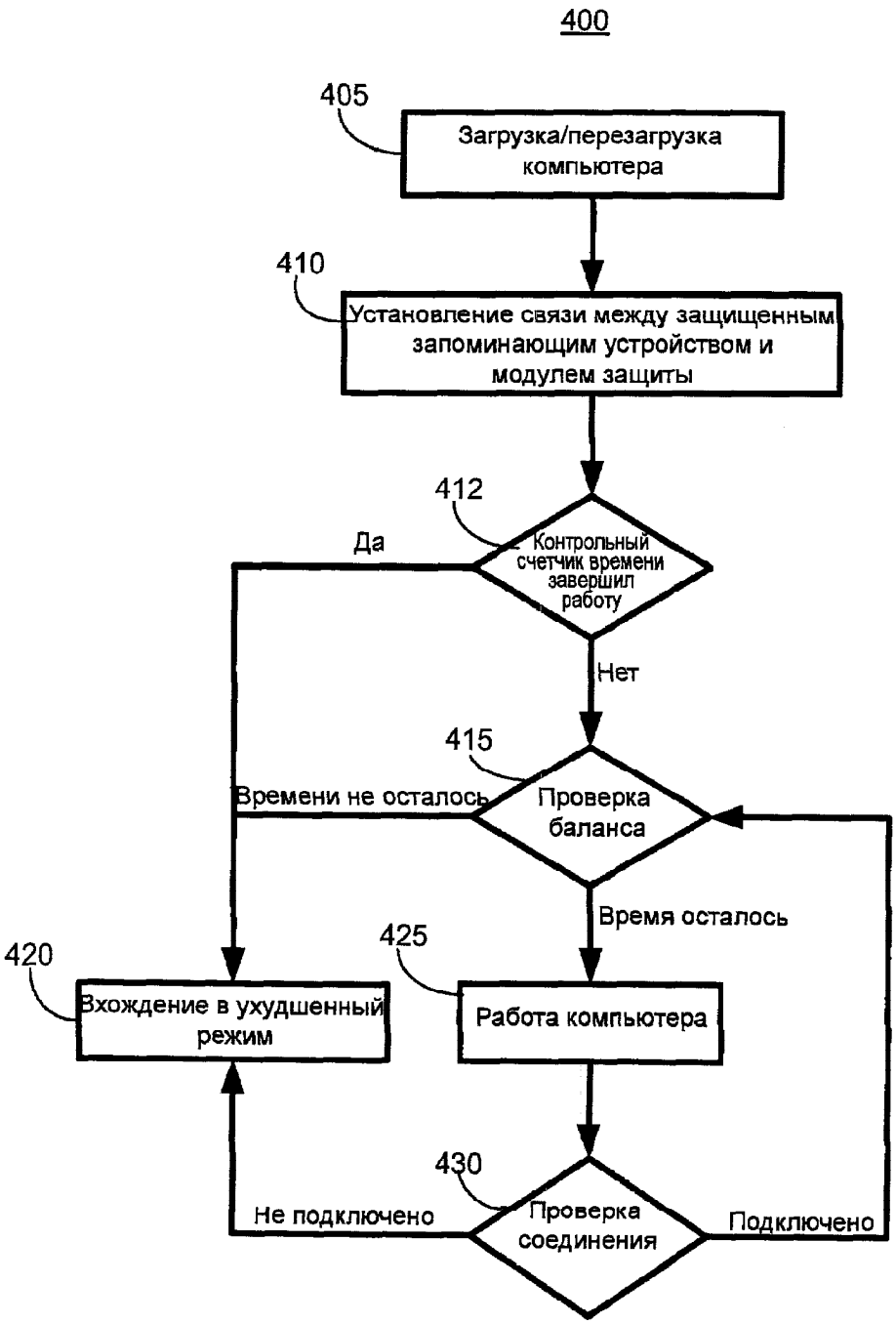
привязывают компьютер к идентифицированному поставщику услуг, используя данные доступа поставщика.


110
Процессор
112
Монитор
122
Системное запоминающее устройство
114
Графическое обрабатывающее устройство
120
Интерфейс запоминающего устройства/ графического взаимодействия
116
124
128
126
(ROM) 130
Системные данные 134
(RAM) 132
Операционная система 136
Прикладные программы 138
Другие программные модули 140
Программные данные 142
144
150
BIOS
118
Интерфейс ввода/вывода
182
189
Модуль Защиты
184
Схема синхронизации
186
Защищенное запоминающее устройство
146
148
156
Мышь/ клавиатура
Микросхема управляющего устройства ввода/вывода
152
180
Сетевой интерфейс
Удаленный компьютер
178
154
Гибкий диск
166
Съемное энергонезависимое запоминающее устройство
Печатающее устройство
158
164
CD/DVD
162
USB
188
UFD
Стационарное энергонезависимое запоминающее устройство
160
Операционная система 168
Прикладные программы 170
Другие программные модули 172
Программные данные 174

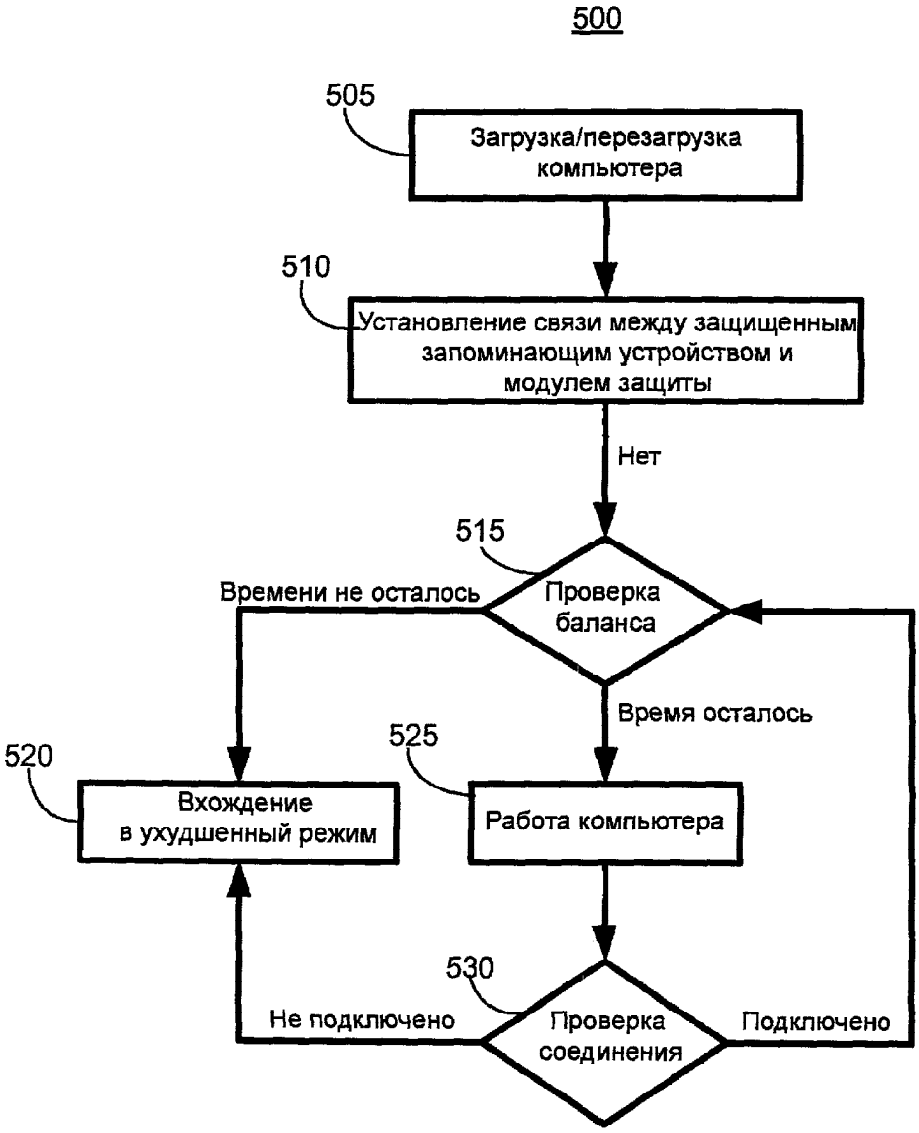
ФИГ. 1


300
302
Обслуживающий узел предоставления услуг
310
Расчетный обслуживающий узел
308
188
312
Средство продаж
306
Электронное устройство
304
188
Электронное устройство

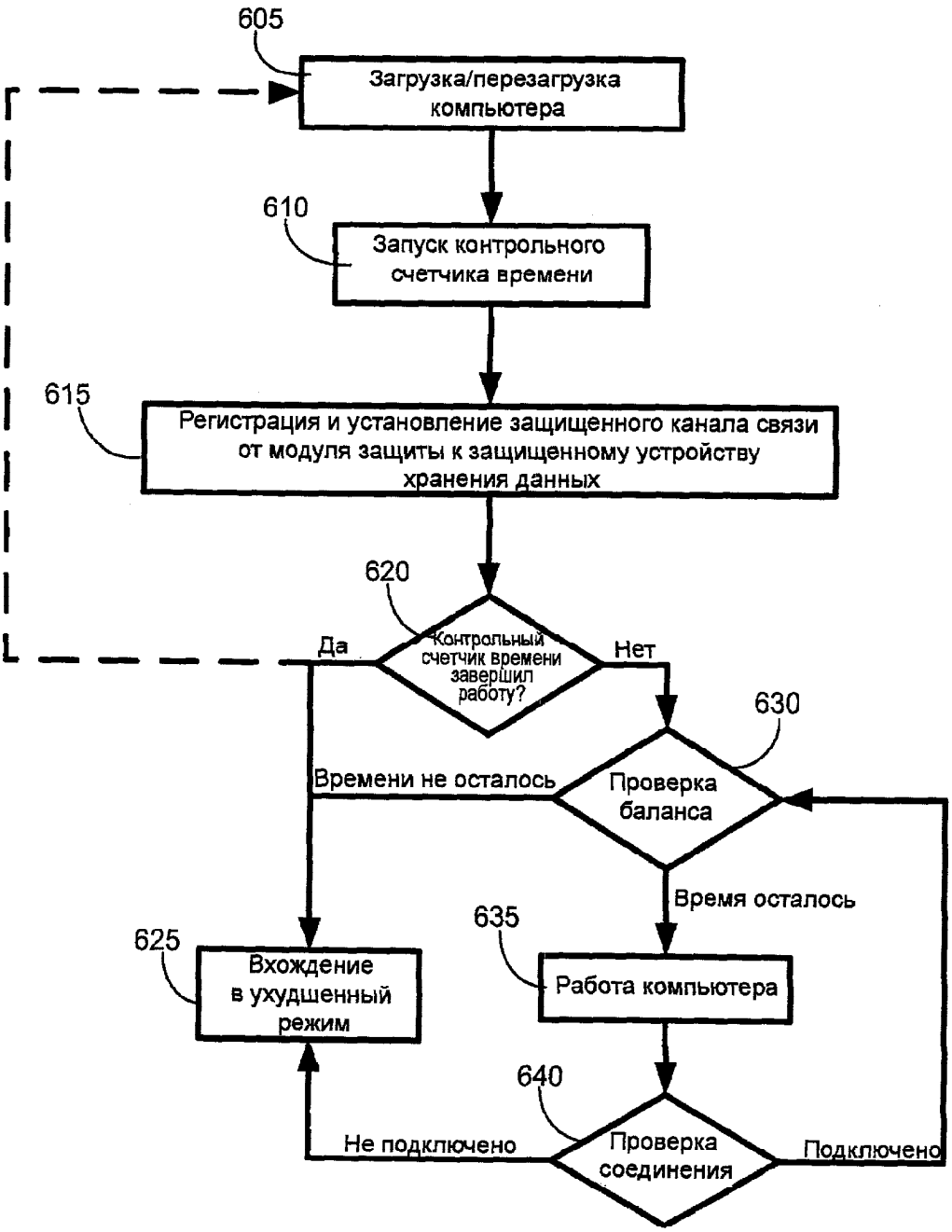
ФИГ. 3


400
405
Загрузка/перезагрузка компьютера
410
Установление связи между защищенным запоминающим устройством и модулем защиты
412
Контрольный счетчик времени завершил работу
Да
Нет
415
Проверка баланса
Времени не осталось
Время осталось
420
Вхождение в ухудшенный режим
425
Работа компьютера
430
Проверка соединения
Не подключено
Подключено

ФИГ. 4


500
505
Загрузка/перезагрузка компьютера
510
Установление связи между защищенным запоминающим устройством и модулем защиты
Нет
515
Проверка баланса
Времени не осталось
Время осталось
520
Вхождение в ухудшенный режим
525
Работа компьютера
530
Проверка соединения
Не подключено
Подключено

ФИГ. 5


600
605
Загрузка/перезагрузка компьютера
610
Запуск контрольного счетчика времени
615
Регистрация и установление защищенного канала связи от модуля защиты к защищенному устройству хранения данных
620
Контрольный счетчик времени завершил работу?
Да
Нет
630
Проверка баланса
Времени не осталось
Время осталось
625
Вхождение в ухудшенный режим
635
Работа компьютера
640
Проверка соединения
Не подключено
Подключено

ФИГ. 6