(19) Евразийское патентное ведомство

(11) 018277 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2013.06.28

(21) Номер заявки
201000310

(22) Дата подачи заявки
2007.09.04

(51) Int. Cl. *G06F 21/10* (2013.01)

(54) СПОСОБ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ ТОРГОВОЙ СДЕЛКИ В КОМПЬЮТЕРНОЙ СЕТИ

(31) **11/844,408**
(32) **2007.08.24**
(33) **US**
(43) **2010.10.29**
(86) **PCT/US2007/077503**
(87) **WO 2009/029116 2009.03.05**

(71)(73) Заявитель и патентовладелец:
БЕНЕДОР КОРПОРЕЙШН (US)

(72) Изобретатель:
Керротт Ричард Ф. (US)

(74) Представитель:
Шилан К.А. (RU)

(56) US-A-6078902
US-A1-2003161473
US-A1-2002069177
WO-A-9840809
EP-A-0773490

(57) Предлагаемые система и способ облегчают осуществление торговых сделок в компьютерной сети, включая приобретение сохраняемых в электронном виде продуктов. В соответствии с примерами осуществления настоящего изобретения "информация о покупателе" шифруется в потоке шифрованных данных и поток шифрованных данных передается при осуществлении торговой сделки от покупателя торговой организации. Проверяющая организация получает поток шифрованных данных, который посылается торговой организацией для проверки личных данных и авторизации платежей. Затем проверяющая организация проверяет идентификаторы, содержавшиеся в потоке шифрованных данных, и передает результаты проверки личных данных и авторизации платежей в торговую организацию. С целью создания персонифицированного электронного продукта торговая организация добавляет к приобретаемому электронному продукту поток шифрованных данных или уникальный идентификатор сделки.

018277 B1

018277 B1

Перекрестная ссылка к родственным заявкам

Данная заявка является частичным продолжением рассматриваемой в настоящее время заявки США № 10/970051 под названием "Способ и устройство для обеспечения безопасной торговой сделки в компьютерной сети", поданной 21 октября 2004 г., которая является продолжением заявки США № 09/726304, поданной 1 декабря 2000 г., которая издана в качестве патента США № 6839692, оба документа полностью включены в данную заявку.

Кроме того, в данной заявке заявлен приоритет на рассматриваемую в настоящее время предварительную заявку № 60/890230 под названием "Зашифрованные индивидуальные идентификаторы договоров к приобретенным средствам аудиовизуальной информации или к контенту средств аудиовизуальной информации", поданной 16 февраля 2007 г., которая полностью включена в настоящую заявку в виде ссылки.

Предпосылки создания изобретения и его краткое изложение

Область техники изобретения

Настоящий пример осуществления данного изобретения относится к обеспечению защиты электронной коммерции и подобных сделок, включая продажи товаров и услуг, между сторонами в компьютерных сетях типа интернета и к отслеживанию распространяемых электронных продуктов, типа электронных документов, электронных презентаций, электронных произведений, и к способам и системам хранения зашифрованных индивидуальных идентификаторов договоров в распространяемых электронных продуктах.

I. Предпосылки создания изобретения и краткое изложение первичной заявки.

Заявка № 10/970051 и патент США № 6839692, дата приоритета: 1 декабря 2000 г.

Настоящее изобретение относится к системе обеспечения защиты торговых сделок, осуществляемых в сети, и, в частности, к усовершенствованной системе защиты, которая только хранит и предоставляет зашифрованную информацию. Кроме того, изобретение относится к системе обеспечения регулируемых покупателем правил, включая временные пределы и пределы значений, для выполняемых в сети торговых сделок.

Рост популярности персональных компьютеров и сетей, соединяющих персональные компьютеры, вызвал в последние десятилетия драматический рост электронной торговли. Одним примером очень популярной сети является Всемирная паутина или Интернет (далее интернет). Однако электронной коммерции препятствует неспособность обеспечить удобную и безопасную систему платежей.

Для многих обычных систем платежей электронной коммерции требуются сложные пароли и алгоритмы шифрования, которые громоздки и не удобны для пользователей. В других традиционных системах платежей электронной коммерции требуется, чтобы все участвующие стороны договорились о формате защиты. К недостаткам таких систем относится то, что в них могут участвовать только те стороны, которые присоединились к этому "клубу" и согласились на специфический формат шифрования. Учитывая скорость, с которой торговые сайты поступают в текущие сети (например, интернет) и выходят из нее, нереально требовать от торговцев договориться об определенном формате.

В других системах платежей электронной коммерции требуется предоплата третьему лицу (стороннему продавцу), который, в свою очередь, выдает закодированный кредит в счет этого депозита. Помимо создания еще одного уровня к сетевым сделкам, эти программы под названием "бумажник" (wallet) и "наличные интернет-деньги", кроме того, создают другой уровень незащищенности информации о покупателе. Кроме того, в этих системах требуется, чтобы для участия в различных версиях этих систем регистрировались как покупатель, так и торговая организация.

В других системах платежей электронной коммерции требуется, чтобы пользователь приобрел определенные технические средства (например, устройство считывания кредитной карточки), которые являются объектом собственности по своей природе и неудобны в установке и использовании. Кроме того, если приобретения выполняются с использованием других компьютеров, то пользователь должен подвести к этим компьютерам данное техническое средство, что затрудняет оплату в этом типе системы платежей.

Независимо от системы платежей общим для традиционных систем является то, что покупатель для совершения сделки должен предоставить частную информацию торговой организации, третьему лицу (стороннему продавцу) и финансовому учреждению торговой организации. Из-за незащищенности покупателя это требование является самым большим препятствием для традиционных систем. Получает ли покупатель дополнительные технические средства или просто передает частную информацию третьим лицам (сторонним продавцам), информация о покупателе хранится в чьей-то базе данных. Уязвимость этих хранимых записей является вопросом глубокого беспокойства потенциальных покупателей и ответственных лиц.

Проблема состоит в том, сколько раз покупатель должен предоставлять в сеть, например в интернет, частную, уязвимую и/или конфиденциальную информацию для совершения сделки.

Поэтому в настоящем изобретении предлагается структура и способ защиты торговой сделки в компьютерной сети. В данном изобретении информация о покупателе шифруется в виде кода покупателя в запоминающем устройстве компьютера покупателя (компьютер покупателя подключается к компью-

терной сети). Затем, в соответствии с настоящим изобретением во время торговой сделки код покупателя передается по компьютерной сети торговой организации или торговой организации разрешается отправлять по компьютерной сети код покупателя финансовому учреждению. Финансовое учреждение расшифровывает код покупателя, проверяет информацию и возвращает торговой организации по компьютерной сети решение об авторизации сделки.

Важной особенностью настоящего изобретения является то, что кодируемая информация о покупателе, типа номера кредитной карточки ("код покупателя"), не доступна торговой организации и поэтому не уязвима. Код покупателя хранится только в запоминающем устройстве покупателя и в зашифрованном виде. Это позволяет покупателю совершать торговые сделки, не предоставляя зашифрованную информацию торговой организации, например номер кредитной карточки. Среди прочего, финансовое учреждение сравнивает данный адрес покупателя с исторической информацией по адресу покупателя, сохраняемой финансовым учреждением. У покупателя может быть больше одного авторизованного адреса доставки. Решение об авторизации сделки получает одобрение только в том случае, если адрес покупателя и исторический адрес совпадают. Если в результате предоставления неправильной информации об адресе авторизация не получена, то финансовое учреждение может поступать следующим образом: 1) одобрить сделку с исправленным адресом; 2) одобрить предмет сделки с покупателем с обновлением информации по адресу покупателя до выдачи кода авторизации и 3) отклонить авторизацию.

Защита информации о покупателе до ее поступления в сеть позволяет покупателю интерактивно сохранять управление источниками кредитования и расширять их использование. Это главное различие между предлагаемыми в настоящем изобретении и традиционными системами платежей электронной коммерции.

В системе по настоящему изобретению покупателю предоставляется доступ к его информации посредством персонального ключа, или кода доступа, однако только финансовое учреждение и его агенты владеют ключом для дешифровки, или кодом. Таким образом, в настоящем изобретении предлагается безопасное использование информации о покупателе, при этом не вводятся новые уровни и не появляются третьи лица, и эта информация не попадает в несметное число баз данных. В соответствии с предпочтительным примером осуществления настоящего изобретения код покупателя включает зашифрованную информацию о кредитной карточке.

Кроме того, в соответствии с предпочтительным примером осуществления настоящего изобретения в запоминающем устройстве можно хранить много зашифрованных кодов покупателя. Каждый из кодов покупателя может включать уникальный способ платежей. В соответствии с другим примером осуществления настоящего изобретения одна группа кодов покупателя может идентифицировать одну кредитную организацию, осуществляющую платеж, при этом каждый код покупателя в группе включает другое имя пользователя. При этом каждый код покупателя в группе включает уникальный кредитный лимит и позволяет покупателю авторизовать дополнительных пользователей для отдельной кредитной организации или отдельного кредитного учреждения. В соответствии с настоящим изобретением для разблокировки кода покупателя, кроме того, используется пароль в компьютере покупателя.

В соответствии с другим примером осуществления настоящего изобретения предлагается система, которая управляет компьютером покупателя. Система по настоящему изобретению включает шифратор для зашифровки информации о покупателе в виде кода покупателя в запоминающем устройстве компьютера покупателя и популятор (populator), который при совершении торговой сделки передает по компьютерной сети торговой организации код покупателя. Подключенный к сети компьютер покупателя передает по компьютерной сети финансовому учреждению код покупателя. Финансовое учреждение расшифровывает код покупателя и возвращает торговой организации по компьютерной сети решение об авторизации сделки.

В соответствии с предпочтительным примером осуществления настоящего изобретения код покупателя включает зашифрованную информацию об адресе покупателя, а в состав системы, кроме того, входит компаратор, расположенный в финансовом учреждении. Компаратор сравнивает адрес покупателя с историческим адресом покупателя, который хранится в финансовом учреждении. Решение о санкционировании сделки принимается, только если адрес покупателя и исторический адрес совпадают.

Кроме того, в состав системы может входить промежуточный сайт подтверждения кода, который является внешним по отношению к компьютеру покупателя и который подключен к компьютерной сети. Промежуточный сайт подтверждения кода принимает код покупателя до отправления кода покупателя по компьютерной сети в финансовое учреждение. Промежуточный сайт подтверждения подтверждает, имеет ли код покупателя надлежащий формат шифрования.

Шифратор может передать в устройство памяти множество зашифрованных кодов покупателя. Как упоминалось выше, каждый из кодов покупателя может включать уникальную систему платежей, или группа кодов покупателя может идентифицировать единственную кредитную организацию, осуществляющую платеж. Каждый код покупателя в группе может иметь другое имя пользователя и уникальные кредитные лимиты. Кроме того, система по настоящему изобретению включает графический интерфейс пользователя в компьютере покупателя для приема пароля с целью разблокировки кода покупателя.

II. Предпосылки создания изобретения и краткое изложение сущности частично продолжающейся

заявки.

Заявление о приоритете для предварительной заявки США 60/890230, дата приоритета: 16 февраля 2007 г.

Интернет изменил способ общения людей и способ, которым они занимаются бизнесом. При этом развивался и сам интернет. По мере того как компьютеры и технологии открывали новую эру, программное обеспечение упаковывалось на диски и продавалось. Вскоре появились скачиваемые или иначе передаваемые средства аудиовизуальной информации, типа цифровой музыки и кино. Такая активность заставляла отдельных лиц и целые группы искать способы получения прибыли от неправомерного копирования и продажи этих продуктов, что привело к появлению двух основных видов коммерческой деятельности: к получению прибыли, воруя работы других; и к получению прибыли, не используя пиратство. По мере того как интернет продолжает развиваться, все больше и больше этих средств аудиовизуальной информации скачивается из сети и распределяется, создавая другой уровень сложности и другую зону беспокойства.

Точно так же уязвимые к контенту сайты, типа сайтов, связанных с индустрией для взрослых и до недавнего времени с индустрией игр, выигрывали в популярности и стали несчастьем для регламентирования из-за природы интернета, отсутствия единой юрисдикции и имеющих исковую силу стандартов. Были предприняты дорогостоящие и сложные попытки вводить саморегулирование и отстаивание исковых требований в судебном порядке; однако защищая меньшинства и регулируя коммерцию в спорных вопросах, международная юрисдикция в лучшем случае доказала только наличие трудностей. Сложность состоит в том, как регулировать структуру, которая не имеет "места бизнеса" в традиционном смысле, не нарушая, при этом, права физических лиц и групп, которые в зависимости от юрисдикции, в который они постоянно пребывают, могут иметь различные степени частных прав и юридических защит, которые должны быть сбалансированы в ответ на попытки регулирования виртуальной юрисдикции и коммерции в сети интернет. Виртуальная коммерция в виртуальной среде создает необходимость договариваться о правах и юрисдикции для защиты и отстаивания этих прав в судебном порядке. Однако природа электронной коммерции создает дополнительную необходимость идентифицировать потребителя при обеспечении защиты личных данных потребителя от "воровства личных данных" и "мошенничества с личными данными" и при обеспечении защиты сделки как для потребителя, так и для торговой организации.

В настоящее время торговая организация сталкивается с множеством рисков при интернет-сделке. Если ребенок "заимствовал" кредитную карточку, дебетовую карточку или заранее оплаченную карточку родителя, если кто-то присвоил имя другого человека, если кто-то исказил свой возраст, чтобы попасть на сайт с ограничениями по возрасту, тогда требование продавца к оплате может быть отклонено. Все это представляет реальную проблему для продавца, занимающегося электронной коммерцией, который старается получить компенсацию за то, что он предлагает, потому что риск сделки принимает на себя торговая организация, а не банк-эмитент, где не остается никакой подписанной квитанции - "никакой подписи". В результате приходится сталкиваться с мошенничеством на миллионы долларов, отказом от уплаты долга и возвратом платежа по сделкам, что увеличивает издержки и риски для всех.

Учитывая вышесказанное, в настоящем изобретении предлагается способ, система и структура, которые создают, регистрируют, проверяют и обеспечивают сохранность версии зашифрованных индивидуальных идентификаторов договоров потребителя, которые могут, помимо всего прочего, вставляться вместе со средствами аудиовизуальной информации, купленными или иначе приобретенными по компьютерной сети, в авторизацию сделки, квитанцию и/или запись о продаже, создавая верификатор "наличия человека"/"наличия подписи".

Способ включает использование любого зашифрованного идентификатора договора пользователя или всех зашифрованных идентификаторов договоров пользователя, которые разработаны прежде или во время хранения на жестком диске пользователя или в любой другой подобной, предназначенной для этого компьютерной системе хранения. Способ и система включают разрешение на использование зашифрованных идентификаторов договоров, которые используются, не раскрывая продавцу, с которым осуществляется сделка, например, приобретение средства аудиовизуальной информации, конкретики зашифрованной информации, типа имени, адреса или номера кредитной/дебетовой/заранее оплаченной карточки. Другими словами благодаря настоящему изобретению отпадает необходимость в раскрытии и в последовательной регистрации у продавца и в его базе данных личных данных потребителя и другой информации.

Данный способ и система позволяют использовать зашифрованные идентификаторы договоров в качестве средства проверки одобрения пользователем уточняющих условий использования и приобретения, при этом это делается таким способом, который может, кроме того, встраиваться в загружаемые средства аудиовизуальной информации. Данные способ и система создают и контролируют вспомогательные учетные записи с уникальными идентификаторами пароля отчетности и корреспондирующего пароля пользователя. Данные способ и система возлагают ответственность за управление учетной записью и любыми вспомогательными учетными записями на первичного авторизованного/зарегистрированного пользователя. Зашифрованные идентификаторы дают возможность способу и системе обеспечивать безопасность и ограничивать доступ к средствам аудиовизуальной информации и

использование средств аудиовизуальной информации, приобретенных для такого использования, соблюдать условиям, и привилегированное право, для чего они приобретались, учитывая, таким образом, согласованное требование о соблюдении авторских прав и других защит.

В частности, в настоящем изобретении предлагается система и способ, позволяющие облегчить компьютеризированные торговые сделки с помощью сохраняемых в электронном виде продуктов (которые иногда упоминаются в данном документе как электронные продукты) типа литературных произведений, музыкальных произведений (записей) и видеопроизведений (кино, представления, видео и т.п.), при этом потребитель соглашается на соблюдение соответствующих прав, типа авторских прав.

В примерах осуществления настоящего изобретения "информация о покупателе" шифруется в поток шифрованных данных (который упоминается иногда как идентификатор покупателя (CID)). Такая информация об идентификаторе покупателя может включать идентификатор имени (который может соответствовать, а может и не соответствовать формальному имени покупателя), возможный идентификатор возраста покупателя (который может быть датой рождения, определенным возрастом, возрастным диапазоном, классификацией возраста), возможный идентификатор адреса (который может быть адресом покупателя или другим адресом) и идентификатор договора с покупателем, который содержит или идентифицирует основанное на договоре соглашение между покупателем и проверяющей организацией или финансовым учреждением (эмитентом кредита - credit issuer), что облегчает сделку по закупке.

Возможно, что, как только элементы потока шифрованных данных идентифицированы и согласованы, для расположения и идентификации этого специфического потока информации о покупателе (включая идентификатор компьютера) проверяющая организация может использовать единственный, уникальный идентификатор. Информация о покупателе хранится только в базе данных проверки, и только этот идентификатор и идентификатор компьютера могут передаваться в пункте продажи в виде потока шифрованных данных (вместе с незашифрованным BIN или номером маршрута эмитента кредита) продавцу.

Одно намерение программы и участников состоит в совершении "сделки с проверкой на наличие подписи", на которую могут полагаться все стороны сделки при обеспечении защиты личных данных покупателя.

В соответствии с примерами осуществления настоящего изобретения при осуществлении торговой сделки по покупке электронного продукта от покупателя торговой организации передается поток шифрованных данных. Проверяющая организация, которой может быть эмитент кредита или узел обработки эмитента кредита или его агент (например, проверяющая организация), получает поток шифрованных данных, который (в сочетании с покупной ценой) до обработки платежей посылает торговая организация для проверки личных данных и авторизации платежей. Затем, с целью проверки личных данных и санкционирования платежей проверяющая организация сравнивает с помощью перекрестных ссылок данные из потока шифрованных данных с данными из отдельной базы данных, содержащей информацию о покупателе. Затем, проверяющая организация передает результаты проверки личных данных и авторизации платежей торговой организации, которая завершает сделку с покупателем и обрабатывает сделку с целью платежей, как сделку с проверкой на "наличие подписи" в соответствии с предварительным договором всех сторон.

По результатам проверки личных данных и авторизации платежей торговая организация получает подтверждение фактического наличия покупателя при осуществлении торговой сделки и таким образом торговая организация получает гарантию, что она не проводит сделку ни с кем другим, кроме покупателя, и что покупатель выразил согласие быть связанным условиями сделки, проверенной в соответствии с договором между покупателем и эмитентом кредита. Договор между покупателем и эмитентом кредита предполагает использование договора в сделках с третьими лицами и уверенность в этом договоре, в частности, в обмен на защиту личных данных и удобства по примеру осуществления настоящего изобретения, представленному в настоящей заявке.

В соответствии с примерами осуществления настоящего изобретения поток шифрованных данных содержит идентификаторы (не обязательно персональную информацию о покупателе), по которым покупатель и эмитент кредита (например, банк) принимают договор, и проверка личных данных и авторизации платежей содержат, как и предполагалось, информацию, ограниченную уникальной сделкой, и по которой покупатель и эмитент кредита принимают договор. Такие идентификаторы были бы мало полезны, даже при расшифровке потока шифрованных данных.

Другая особенность примеров осуществления настоящего изобретения, представленных в данной заявке, состоит в том, что для разработки персонифицированного электронного продукта к приобретаемому электронному продукту, типа загружаемых цифровых средств аудиовизуальной информации, может добавляться поток шифрованных данных или результаты проверки сделки. Поток шифрованных данных или уникальные результаты проверки сделки (все вместе или по отдельности, иногда упоминаются в настоящей заявке как "идентификатор сделки") могут быть скрыты так, что покупатель не может удалить идентификатор сделки из персонифицированного электронного продукта. Кроме того, персонифицированный электронный продукт может быть нефункциональным (т.е. персонифицированный электронный продукт нельзя открыть или нельзя воспроизвести и т.п.), если удален поток шифрованных данных или идентификатор сделки, вместе или по отдельности. Таким образом, в персонифицированном

электронном продукте всегда сохраняется идентификатор сделки, который и позволяет идентифицировать покупателя, который приобретает электронный продукт (через проверяющую организацию). Кроме того, идентификатор сделки добавляется таким способом, что все копии купленного электронного продукта будут иметь данный идентификатор сделки. Таким образом, ввиду того, что все копии персонифицированного электронного продукта будут иметь данный идентификатор сделки, покупателя, который первоначально приобрел электронный продукт у торговой организации (источник копий), можно всегда идентифицировать путем обращения к базе данных по защите объектов проверки. "Идентификатор сделки" - это то, что возвращается проверяющей организацией, и потому, что это уникальный идентификатор, его можно, кроме того, использовать в виде вложенного идентификатора средства аудиовизуальной информации.

После добавления к приобретаемому электронному продукту идентификатора сделки, что делает электронный продукт персонифицированным, торговая организация поставляет персонифицированный электронный продукт покупателю. Каждый из персонифицированных электронных продуктов каждого из покупателей отличается уникальностью идентификатора сделки, что позволяет идентифицировать копии этого продукта для каждого покупателя, первоначально приобредшего электронный продукт. Кроме того, уникальность каждого идентификатора сделки позволяет идентифицировать источник неавторизированных копий купленного электронного продукта через безопасную базу данных, поддерживаемую проверяющей организацией.

Во время регистрации (когда покупатель заводит или изменяет у эмитента кредита свою учетную запись) и во время приобретения электронных продуктов покупатель может получить уведомление или предупреждение, что информация о нем будет всегда присутствовать в копиях любых персонифицированных электронных продуктов. Кроме того, во время приобретения электронного продукта подобное уведомление или предупреждение могут высвечиваться, сообщая покупателю, что он согласен связать себя условиями и штрафами, предусмотренными за несанкционированное использование или копирование электронного продукта; и каждый раз (или первые несколько раз) при открытии, воспроизведении и т.п. персонифицированного электронного продукта может высвечиваться такое же предупреждение. Такие постоянно повторяемые предупреждения могут применяться или не применяться к некоторым скачиваемым средства аудиовизуальной информации типа музыки. Такие предупреждения предназначены для того, чтобы препятствовать передаче покупателем копий персонифицированного электронного продукта другим лицам в нарушение прав торговой организации (например, незаконная передача или копирование), с помощью этих предупреждений покупатель оповещается о том, что незаконная передача или копирование могут быть прослежены через проверяющую организацию с использованием идентификатора сделки и/или потока шифрованных данных, и соглашается быть связанным условиями и сроками, сформулированными в этих предупреждениях. Подобное санкционированное использование и акцептное предупреждение могут, кроме того, использоваться для доступа на основе возрасте, для назначения цены продаж, основанной на возрасте или месте жительства и т.п. В примерах осуществления настоящего изобретения предлагается широкий диапазон идентификаторов покупателя, которые поощряют, продвигают электронную коммерцию и участвующие в ней стороны и обеспечивают им защиту.

Предупреждения, касающиеся авторского права и т.п., не могут быть применены к аудиосредствам аудиовизуальной информации после скачивания. Эти предупреждения важны до скачивания, однако, при том, что покупатель согласен связать себя содержавшимися в таких предупреждениях условиями, как условие сделки, согласно положению о присоединении, сформулированному в его договоре, он согласен связать себя с эмитентом кредита и согласен нести ответственность за нарушение условий. Стороны соглашаются нести ответственность за свои действия и намерения.

Шифрование информации о покупателе может выполняться, например, следующим образом. Сначала покупатель подключается к эмитенту кредита с помощью первого компьютеризованного устройства, и эмитент кредита скачивает программное обеспечение на первое компьютеризованное устройство. Продавцы (которые иногда упоминаются в настоящей заявке как "торговые организации"), могут, кроме того, действовать в качестве регистрирующего агента для эмитента кредита, переадресовывая покупателя на сайт эмитента кредита для регистрации проверяющей организацией. Преимущество этого состоит, например, в том, что, как только имеющийся в наличии пользователь кредитной карточки регистрирует свою карточку согласно программе, то согласно примерам осуществления настоящего изобретения этот пользователь/покупатель может выбирать ограниченное использование "карточки" в компьютерной сети типа интернета, обеспечивая, таким образом, защиту "карточке" от несанкционированного использования другими лицами. Покупатель передает имеющуюся уязвимую информацию, типа достоверных адресов доставки, дат рождения (для классификации возрастной группы), номеров банковских счетов, номера кредитной карточки и т.п., или соглашается доверить хранение этой информации. Некоторые элементы информации о покупателе (типа номеров банковских счетов и номера кредитной карточки) хранятся не в компьютеризованном устройстве покупателя, а только в базах данных эмитента кредита или проверяющей организации, хотя для обращения к такой информации могут использоваться кодированные или не кодированные идентификаторы. Другие элементы или идентификаторы (имя, адрес, ссылка на возраст и т.п.) информации о покупателе могут быть зашифрованы, чтобы создать поток шифрованных данных,

который хранится в компьютеризованном устройстве покупателя и который перед шифрованием может быть частично или полностью кодирован или не кодирован.

Используемый в настоящей заявке термин "эмитент кредита" является стенографическим термином, обозначающим организацию, которая предоставляет кредит покупателю. Это может быть торговая организация, продавец, банк, финансовое учреждение и т.п. Кроме того, такой эмитент кредита может включать в свой состав проверяющую организацию и может действовать через агента. Поэтому под термином "эмитент кредита" понимается любая из перечисленных выше организаций или все они. В соответствии с настоящим документом эмитент кредита может принадлежать к одному из нескольких типов эмитентов. Один тип эмитента выпускает кредитные карточки, дебетовые карточки и т.п. К другому типу эмитента относится организация, которая позволяет держателям механизма непогашенного кредита (card vehicle holders), типа держателей непогашенных кредитных карточек, регистрировать все "карточки", которые они хотят использовать в единственной организации, которая занималась бы обработкой кредитов. Другим типом эмитента может быть эмитент кредита, не выпускающий карточки и не являющийся банком, например Microsoft® или Yahoo!® или Google®; при этом данный эмитент от случая к случаю определяет линию кредитования физического лица и предоставляет ему сумму идентифицируемого кредита, который индивидуум может использовать в сети типа интернета. Специалистам понятно, что есть много других типов эмитентов кредита, которые не перечислены в настоящей заявке, но они могут быть среди примеров осуществления настоящего изобретения, представленных в настоящей заявке.

Кредиты обрабатываются эмитентом кредита или организацией, которая обрабатывает кредиты для него и иногда действует в качестве верификатора с участием продавцов, которые занимаются коммерцией в сети (эта альтернатива признает, что обычные кредитные карточки не обязательны в сети компьютерного типа, а вот то, что является необходимым, так это защита сторон в сделке с отслеживанием потока законной торговли). По выбору продавцов эта программа может продвигаться путем отсылки покупателей к их эмитенту кредита на регистрацию. Это обеспечивает защиту покупателя и его личных данных, повышает конкурентоспособность продавца, гарантирует продавцу оплату и снижает возврат платежей и мошенничество; все это служит для улучшения итоговых показателей продавца.

Банки и компании по разработке программного обеспечения могут считывать и проверять идентичность компьютеров, не загружая, при этом, программное обеспечение на компьютер "посетителя"; однако для выполнения других задач программное обеспечение может загружаться или устанавливаться другим способом. При авторизации покупателя эмитент кредита считывает и регистрирует уникальные идентификаторы технических устройств (типа серийных номеров материнских плат, жестких дисков, процессоров и т.п.) первого компьютеризованного устройства. Эти уникальные идентификаторы технических устройств, кроме того, входят в состав потока шифрованных данных. Затем эти же этапы повторяются для любых дополнительных компьютеризованных устройств, которые покупатель желает авторизовать и зарегистрировать для использования в будущих торговых сделках, если, например, у покупателя есть несколько компьютеров или он имеет доступ к нескольким компьютерам и компьютеризованным устройствам. Такие процессы могут выполняться, когда покупатель задает или изменяет учетную запись у эмитента кредита.

Проверяющая организация, финансовое учреждение и/или эмитент кредита (например, банк) определяет элементы потока шифрованных данных покупателя, включая начальный контракт/договор, на который будет полагаться торговая организация, поддерживающая эту программу. Это договор между эмитентом кредита и покупателем, на который полагается торговая организация в соответствии с договором между коммерческим банком и покупателем. Кроме того, в качестве эмитента кредита может выступать проверяющая организация или это может быть узел обработки эмитента кредита или агент, используемый эмитентом кредита, при этом узел обработки эмитента кредита или агент имеют доступ к базе данных, содержащей информацию о покупателе.

Некоторые типы покупателей: 1) новый покупатель (которому нужен кредит в компьютерной сети; новая кредитная карточка; новая дебетовая карточки или другая форма "загружаемой" карточки типа платежной дебетовой карточки); 2) непогашенная банковская операция (держатель механизма непогашенного кредита, например, по первому пункту, который можно использоваться для закупок по компьютерной сети типа интернета); или 3) новый покупатель с механизмом непогашенного кредита (человек с механизмом непогашенного кредита, или кредитной карточкой, например, по первому пункту может пожелать зарегистрировать некоторые или все эти "карточки" в единственной организации, которая позволит присоединить эту "программу" ко всем зарегистрированным "карточкам").

"Кредит" может быть в форме непогашенной кредитной карточки, дебетовой карточки и т.п. или может принимать форму недавно выпущенного "кредита" некоторого другого источника, желающего предоставить такой кредит идентифицируемому физическому лицу - своего рода "электронный аккредитив", или электронный кредит - подпадающий под различные правила и инструкции. В процессе регистрации эмитентом кредита идентификаторов покупателя и другой информации (банк, предположительно, будет располагать информацией о покупателе с непогашенным кредитом в своей базе данных), наряду с информацией о зарегистрированных технических устройствах, покупатель и эмитент кредита составляют договор о том, какие должны быть идентификаторы, подтверждающие наличие покупателя.

Вместо того чтобы сохранять в потоке шифрованных данных некоторые элементы информации о покупателе (например, идентификация возраста), их можно получить из базы данных, хотя дата рождения или уникальное слово могут составлять часть потока шифрованных данных.

В качестве одного из процессов проверки, которую торговая организация предпринимает по отношению к кому-то еще, но не к покупателю, примерно во время передачи потока шифрованных данных торговой организации, при этом перед фактической передачей потока шифрованных данных торговой организации (как часть процесса передачи потока шифрованных данных), в соответствии со способом по одному из примеров осуществления настоящего изобретения в поток шифрованных данных из компьютеризованного устройства, осуществляющего фактическую передачу потока шифрованных данных, может вводиться второй набор идентификаторов компьютеризованных устройств и метка времени и даты. Таким образом, если недобросовестный человек получил ненадлежащую копию потока шифрованных данных и использовал ненадлежащую копию потока шифрованных данных в компьютере (в компьютере покупателя, который не зарегистрирован проверяющей организацией), возможно, вместе с необходимым программным обеспечением по разработке и передаче потока шифрованных данных, поставляемых эмитентом кредита, и, при этом, вторые идентификаторы технических устройств, которые считываются только до передачи потока шифрованных данных, не согласуются с идентификаторами технических устройств в потоке шифрованных данных, то сделка не будет одобрена проверяющей организацией. Точно так же для разработки потока шифрованных данных, который отправляется торговой организации, может использоваться метка времени и даты, которая действует только ограниченный срок (например, минуты, часы, дни и т.п.). Кроме того, такие процессы увеличивают время проверки "наличия покупателя", выполняемой проверяющей организацией для обеспечения дополнительных гарантий продавцу в том, что он фактически имеет дело с покупателем, а не кем-то другим вместо реального покупателя. В дополнение к этой проверке наличия покупателя и договора на выполнение условий всегда, когда покупатель использует поток шифрованных данных или подпись, в соответствии с примерами осуществления настоящего изобретения эмитент кредита отказывает конкретному продавцу в доступе к программе, когда возникает подозрение на мошенничество продавца. Кроме того, это служит для защиты как покупателя, так и добросовестных продавцов.

Использование стандартной программы эмитента кредита для разработки потока шифрованных данных на компьютеризованном устройстве покупателя и передача потока шифрованных данных торговой организации на этап проверки гарантирует, что устройство, на котором установлено программное обеспечение, будет идентифицировано. Таким образом, если этот идентификатор не соответствует идентификатору в потоке шифрованных данных, под которые взят залог, сделка не будет одобрена.

В соответствии с примерами осуществления настоящего изобретения предлагается одна система или большее число систем, в которых используется шифратор, который устанавливается эмитентом кредита в компьютере покупателя. Шифратор шифрует информацию об идентификаторе покупателя в потоке шифрованных данных. Кроме того, эмитент кредита устанавливает агента пересылки в компьютере покупателя и торговца. Агент пересылки обеспечивает передачу потока шифрованных данных с компьютера покупателя на компьютер торговой организации при осуществлении торговой сделки по покупке электронного продукта.

У проверяющей организации имеется верификатор, который оперативно подключается как к компьютеру покупателя, так и к компьютеру торговой организации на этапе проверки сделки. В примерах осуществления настоящего изобретения для усиления степени защиты информации о покупателе верификатор устанавливается отдельно от компьютера покупателя и от компьютера торговой организации и обслуживается проверяющей организацией. База данных с информацией о платежах покупателя может находиться в проверяющей организации или отдельно от проверяющей организации. В любой ситуации база данных оперативно подключается только к верификатору, при этом ни покупатель, ни торговая организация не имеют доступа к базе данных.

Для выполнения этапов способа по настоящему изобретению агент пересылки с целью проверки платежей обеспечивает передачу потока шифрованных данных от компьютера торговой организации на верификатор. Кроме того, на основе информации из базы данных верификатор обеспечивает проверку личных данных и авторизацию платежей и передает результаты проверки личных данных и авторизации платежей торговой организации. Затем поток шифрованных данных или результаты проверки уникальных личных данных и авторизации платежей добавляются торговой организацией к приобретаемому электронному продукту с целью создания персонифицированного электронного продукта, который поставляется торговой организацией покупателю.

Эти и другие аспекты примеров осуществления настоящего изобретения будут более понятны после рассмотрения совместно со следующим описанием и прилагаемыми чертежами. Однако следует понимать, что указанные в описании предпочтительные примеры осуществления настоящего изобретения приводятся исключительно с целью иллюстрации, а не для наложения каких-либо ограничений. В примерах осуществления настоящего изобретения возможны различные изменения и модификации, что, однако, не является отступлением от сущности данного изобретения, и примеры осуществления данного изобретения содержат все такие модификации.

Краткое описание чертежей

Настоящие примеры осуществления данного изобретения будут более понятны из следующего детального описания со ссылкой на чертежи.

На фиг. 1 изображена блок-схема одного примера осуществления настоящего изобретения;

на фиг. 2 изображена блок-схема, иллюстрирующая пример осуществления настоящего изобретения;

на фиг. 3 изображена блок-схема, иллюстрирующая пример осуществления настоящего изобретения;

на фиг. 4 изображена схема системы по одному из примеров осуществления настоящего изобретения;

на фиг. 5 изображена схема системы по одному из примеров осуществления настоящего изобретения;

на фиг. 6 изображена схема потока шифрованных данных по одному из примеров осуществления настоящего изобретения;

на фиг. 7 изображена блок-схема, иллюстрирующая пример осуществления способа по настоящему изобретению;

на фиг. 8 изображена блок-схема, иллюстрирующая пример осуществления способа по настоящему изобретению;

на фиг. 9 изображена блок-схема, иллюстрирующая пример осуществления способа по настоящему изобретению; и

на фиг. 10 изображена схема системы по одному из примеров осуществления настоящего изобретения.

Детальное описание примеров осуществления настоящего изобретения

Настоящий пример осуществления данного изобретения, различные его признаки и выгодные детали объясняются более полно со ссылкой на примеры осуществления, которые, однако, не ограничивают пределы применимости данного изобретения и которые проиллюстрированы в прилагаемых чертежах и детально рассмотрены в приведенном ниже описании. Следует отметить, что признаки, проиллюстрированные в чертежах, не всегда показаны в масштабе. Чтобы не усложнять пример осуществления данного изобретения, не приводится описание известных компонентов и способов обработки. Примеры, используемые в настоящей заявке, служат для упрощения понимания способов осуществления настоящего изобретения. Соответственно данные примеры не должны рассматриваться как ограничение объема примеров осуществления настоящего изобретения.

I. Детальное описание оригинальной заявки № 10/970051 и патента США № 6839692, дата приоритета: 1 декабря 2000 г.

Теперь обратимся к чертежам и, в частности, к фиг. 1, на которой изображена блок-диаграмма примера осуществления настоящего изобретения. В частности, на фиг. 1 изображен персональный компьютер 100, подключенный к сети 170. Кроме того, к сети 170 подключен также сайт подтверждения кода 130, торговый сайт 140, финансовое учреждение 150 и кредитно-информационное бюро 160. Признаки, показанные на фиг. 1, размещены произвольно с целью иллюстрации настоящего изобретения. Специалистам понятно, что эти элементы можно размещать по-разному.

В качестве персонального компьютера 100 (который иногда упоминается в настоящей заявке как компьютер "покупателя") может применяться любое компьютеризованное устройство, которое может подключаться к сети 170. Поэтому под компьютером покупателя 100 можно понимать стандартный настольный персональный компьютер, мобильный компьютер, карманный персональный компьютер, сотовый телефон и т.п. В соответствии с предпочтительным примером осуществления настоящего изобретения компьютер покупателя 100 снабжается графическим интерфейсом пользователя (GUI) 110 и запоминающим устройством 112, типа магнитного жесткого диска или другого устройства хранения для чтения-записи. Кроме того, компьютер покупателя 100 снабжается шифратором 114, подключением к сети 116, популятором (populator) 118 и центральным процессором 120.

Финансовое учреждение 150 располагает базой данных исторических адресов 154, полученных от кредитно-информационного бюро 160, и компаратором 152, который используется для проверки адреса покупателя, что рассмотрено ниже.

На фиг. 2 в виде блок-схемы показана работа системы, изображенной на фиг. 1. В частности, система по настоящему изобретению добавляется к компьютеру покупателя 100. В соответствии с предпочтительным примером осуществления настоящего изобретения, используя графический интерфейс пользователя 110, покупатель вводит пароль, как показано в блоке 200, что обеспечивает дальнейший доступ к системе по настоящему изобретению. Затем через графический интерфейс пользователя 110 покупатель передает в систему по настоящему изобретению персональную информацию типа номера социального обеспечения, адреса, даты рождения, имен родственников, информации о кредитной карточке, банковской информации, информации о занятости и т.п. Шифратор 114 немедленно шифрует эту информацию и хранит зашифрованную информацию в виде кода покупателя в запоминающем устройстве 112, как показано в блоке 202.

Важной особенностью данного изобретения является то, что персональная информация покупателей хранится только в зашифрованном виде. Поэтому, если бы к запоминающему устройству пользователя 112 получил доступ неавторизованный пользователь, то персональная информация покупателя была бы обеспечена защитой, т.к. она зашифрована.

Процесс шифрования включает три элемента: 1) непосредственно код шифрования, который соответствует коду дешифрования, хранимому финансовым учреждением; 2) персональный ключ покупателя, пароль и/или персональный код доступа, который вводится и управляется покупателем, чтобы иметь доступ к зашифрованной информации; и 3) системный идентификатор компьютера покупателя, который обеспечивает доступ к зашифрованной информации только через компьютер покупателя. Как только вводится информация о покупателе, эти три элемента и необходимость повторно вводить любую информацию становятся прозрачными для всех сторон во время любой сделки электронной коммерции (например, двойной ключ или открытый ключ).

Если бы код шифрования попал к неавторизованному пользователю, то для обеспечения доступа к информации потребовался бы персональный ключа покупателя плюс доступ к информации от специальной системы хранения покупателя (например, системный идентификатор компьютера покупателя). Неавторизованный пользователь нуждался бы в коде дешифрования, чтобы получить доступ к информации, которая хранится только в финансовом учреждении (у эмитентов кредита) и у своих авторизованных агентов. В соответствии с предпочтительным примером осуществления настоящего изобретения этот элемент в формате "открытого ключа" или "двойного ключа" усиливает степень защищенности информации о покупателе.

Даже если неавторизованный пользователь преодолеет предшествующие элементы защиты, пользователь в системе по настоящему изобретению должен предоставить авторизованный адрес доставки; процедура, которая требует отдельной защищенной сделки с финансовым учреждением, с подтверждением по электронной почте покупателю. Это делает неавторизованный доступ непрактичным.

В другом примере осуществления настоящего изобретения пользователь может вводить несколько кодов покупателя, каждый из которых может включать другое кредитно-информационное бюро (например, другую кредитную карточку). Поэтому в настоящем изобретении пользователю предлагается вводить код покупателя для каждой из кредитных карточек пользователя.

Кроме того, для одной кредитной карточки можно вводить несколько кодов покупателя. Эти дополнительные коды покупателя могут включать разные лимиты расходования средств. Это позволяет пользователю устанавливать различные коды покупателя по бюджетным или другим подобным причинам. Например, в соответствии с настоящим изобретением пользователь может вводить разные коды покупателя на разные статьи личного или делового бюджета. По достижению лимита расходования средств дополнительные сделки (приобретения) исполняться не могут до тех пор, пока информация по бюджету не будет изменена или обновлена. План бюджета может обновляться автоматически, что позволяет автоматически исполнять бюджеты определенного периода. Примером этого может служить один код покупателя с использованием кредитной карточки для помесячных платежей провайдеру интернет-услуг за определенный период, например за один год. В данном случае код покупателя включает лимит месячного взноса за интернет-услуги и двенадцатимесячный лимит по всей сделке. Кроме того, в данном примере осуществления настоящего изобретения преимуществом для покупателя является возможность исправлять или отменять сделку в любое время, изменяя заявленные лимиты.

Точно так же родители могут вводить коды покупателя для каждого из своих детей, при этом каждый код покупателя потенциально включает различный лимит расходования средств. В одном из примеров осуществления настоящего изобретения лимиты расходования средств могут периодически обновляться для получения периодического разрешения на допуск. Этот аспект изобретения позволяет родителям устанавливать ежемесячное разрешение на допуск в интернет для своего ребенка. Родители устанавливают отдельно авторизованный код покупателя вместе с лимитами на определенный период (например, на месяц или на неделю). Эффект состоит в том, что родители контролируют выдачу и использование авторизованных вспомогательных учетных записей.

Эффект этих аспектов изобретения состоит в том, что финансовое учреждение продолжало бы контролировать оценку покупателя на кредитоспособность. Однако покупатель получал бы удовольствие от такого усиления контроля и использования этого кредита.

В соответствии с предпочтительным примером осуществления настоящего изобретения коды покупателя включают имя, адрес и номер кредитной карточки пользователя в зашифрованном виде. В соответствии с настоящим изобретением после установки кодов покупателя и их сохранения в зашифрованном виде в запоминающем устройстве 112 компьютер покупателя 100 работает в фоновом режиме, пока покупатель не пожелает сделать приобретение в сети 170. Во время закупки графический интерфейс пользователя 110 предоставляет пользователю различные варианты платежей (коды покупателя). После того как пользователь выберет соответствующий код покупателя, популятор (populator) 118 готовится отправить код покупателя на сайт торговой организации 140, выдавая команду на отправку кода покупателя по сети 170 на торговый сайт 140, как показано в блоке 204.

На фиг. 3 более детально показана функция, изображенная в блоке 204. В частности, в настоящем

изобретении код покупателя автоматически занимает соответствующую ячейку "проверки" на торговом сайте 140, используя популятор (populator) 118. Как показано на фиг. 3, когда покупатель переходит в окно проверки торгового сайта (300), то он помещает курсор в соответствующую ячейку (например, в поле номера кредитной карточки, в поля данных кода покупателя и т.п.) 302. На многих торговых сайтах 140 не предусмотрено поле даты кода покупателя. Поэтому в соответствии с настоящим изобретением на торговом сайте используется номер кредитной карточки (или другое подобное поле платежей). Длина зашифрованного поля данных кода покупателя больше длины номера кредитной карточки. Поэтому единственная модификация, необходимая торговому сайту 140, заключается в том, чтобы обеспечить ввод зашифрованных строк данных в более короткое поле номера кредитной карточки.

После того как пользователь поместит курсор в соответствующую ячейку, он нажимает предварительно заданную функциональную клавишу на клавиатуре (или выбирает кнопку на графическом интерфейсе пользователя) (304), это приводит к появлению всплывающего окна ввода ID пользователя и пароля (306). После ввода надлежащего ID пользователя и пароля весь код покупателя помещается (вписывается) в поле на торговом сайте. Пользователь не должен вводить свое имя, адрес и т.п. потому, что вся информация уже содержится в коде покупателя. Как показано ниже, после получения одобрения на предоставление кредита финансовое учреждение 150 возвращает имя, адрес доставки и номер авторизации кредита (не номер кредитной карточки) на торговый сайт 140, и пользователь не должен вводить эту информацию.

Если для разных кредитных карточек вводятся разные коды покупателя, то пользователь может выбирать код покупателя, который включает информацию о кредитной карточке с достаточным лимитом по кредиту, желательную процентную ставку и т.п., чтобы сделать покупку. Сам код покупателя является зашифрованным персональным потоком информационных данных и может быть несколько длиннее. Поэтому графический интерфейс пользователя предоставляет удобное меню выбора с аббревиатурой имен. Например, в одном из примеров осуществления настоящего изобретения предусмотрено ниспадающее меню с аббревиатурой кредитной карточки, что позволяет пользователю выбирать код покупателя, который используется. Если пользователь установил только один код покупателя, ниспадающее меню будет включать только эту единственную аббревиатуру кода покупателя. Таким образом, различные категории бюджета или детские имена могут также использоваться в виде аббревиатуры имен в ниспадающем меню, чтобы выбирать соответствующий код покупателя.

ID пользователей являются аббревиатурами кодов покупателей. Если ID пользователя/пароль неправилен (310), то генерируется сообщение об ошибке, и процедура возвращается к блоку 304, чтобы повторить ID пользователя/пароль. Как известно, разрешено ограниченное число повторений ID пользователя/пароля.

Если пароль/ID пользователя правилен (308), то покупателю предоставляется возможность установить правила платежей (312), типа автоматических ежемесячных платежей провайдеру интернет-услуг, что обсуждалось выше. Если никакие специальные правила за оплату услуг не задаются, то принимается единственная прямая схема платежей и процедура переходит к блоку 316. С другой стороны, если правила платежей заданы, то появляются другие всплывающие окна (314), чтобы провести покупателя с помощью мастера (wizard) и задать варианты платежей типа краткосрочного депозита, предельной суммы кредита и/или временных рамок и т.п.

Затем в соответствии с настоящим изобретением в блоке 316 берутся предварительно зашифрованные уязвимые данные покупателя, и к ним добавляется заданный номер сделки и правила (если имеются). В соответствии с настоящим изобретением перед прикреплением необходимой информации по маршрутизации также шифруются дополнительные данные (номер сделки по закупке, правила и т.п.), и в поле данных по коду покупателя или поле кредитной карточки 302 автоматически вводится полный код покупателя. Как упоминалось выше, код покупателя является зашифрованной строкой, состоящей из ряда кусков данных, включая номер кредитной карточки, правила, номер сделки, имя и адрес покупателя и т.п.

Обратимся снова к фиг. 2. Как показано в блоке 208, в соответствии с одним из примеров настоящего изобретения код покупателя отсылается непосредственно на торговый сайт 140. В другом примере осуществления настоящего изобретения используется сайт подтверждения кода 130 (позиция 206). В данном примере осуществления настоящего изобретения код покупателя вместо торгового сайта 140 направляется популятором (populator) 118 на сайт подтверждения кода 130. Сайт подтверждения кода 130, управляемый кредитно-информационным бюро, определяет, имеет ли код покупателя надлежащий формат, позволяя кредитно-информационному бюро периодически обновлять или изменять ключи общего пользования (например, коды шифрования и дешифрования). Если модуль подтверждения кода 130 определяет, что код покупателя неверен, то появляется сообщение об ошибке, в котором объясняется, что код покупателя неверен, как показано в блоке 212. Если код покупателя верен, то он модулем подтверждения кода 130 отсылается на торговый сайт 140, как показано в блоке 214.

После получения кода покупателя торговый сайт 140 направляет код покупателя в блок 150. Важная особенность изобретения состоит в том, что конфиденциальная информация в незашифрованном виде никогда не поступает в торговую организацию. Таким образом, торговая организация освобождает-

ся от ответственности за эту информацию.

Как показано, в блоке 218 расшифровывается код покупателя. Затем проверяется, приемлема ли кредитная сделка (например, есть ли у покупателя достаточный кредит), кроме того, с помощью компаратора 152 в исторической базе данных приемлемых адресов доставки 154, предоставляемых кредитно-информационным бюро 160, сравнивается адрес доставки, по которому должны отправляться товары. Этот аспект изобретения предотвращает отправку товаров по неверным адресам преступными элементами, минуя адрес покупателя.

В одном из примеров осуществления настоящего изобретения покупатель с помощью кредитно-информационным бюро может непосредственно задавать множество авторизованных адресов доставки. Эти адреса могут включать такие альтернативы, как офис или дом. Каждый адрес вводится в запоминающее устройство покупателя и хранится на нем в виде отдельной последовательности шифрованных данных как отдельный код покупателя. Если покупатель задает новые коды покупателя, то новые авторизованные адреса для покупателя отсылаются (через электронную почту или подобную электронную передачу) непосредственно от компьютера покупателя 100 в кредитно-информационное бюро 160 по сети 170 и пополняют список авторизованных адресов, связанных с покупателем, в базах данных кредитно-информационного бюро 160.

Как показано в блоке 220, если адрес доставки совпадает с адресом в базе данных 154 и у покупателя есть достаточный кредит, в торговую организацию 140 отсылается код подтверждения, имя, адрес и другая необходимая информация, как показано в блоке 224. В этом случае термин "совпадает" означает, что два адреса должны в значительной степени соответствовать друг другу. Таким образом, если небольшая часть номера улицы или почтового индекса неправильна или если орфография названия улицы не совсем совпадает, то сделка получает одобрение, и торговой организации предоставляется исправленный адрес. Однако, если адрес доставки не совпадает с авторизованным адресом покупателя (например, другой штат, другой город, другая улица и т.п.), то на торговый сайт 140 передается сообщение об ошибке и покупателю отсылается сообщение по электронной почте с объяснением причин отказа в заключении сделки.

Для определения авторизации кредитно-информационные бюро в настоящее время пользуются адресами. Однако их критерии определения соответствующего адреса меняются. В настоящем изобретении разработана система для устранения ошибок и мошенничества при этих авторизациях путем "исправления" такого адреса. Затем ответственность за то, что продукт отправляется только на авторизованный или исправленный адрес, ложится на торговую организацию. Этот аспект настоящего изобретения представляет дополнительный уровень защиты и разрешает покупателю "прерывать" и возвращать любые несанкционированные поставки.

В одном из примеров осуществления настоящего изобретения покупатель использует "мастера правил" (rule wizard) [314], чтобы временно ввести "непостоянный" адрес доставки, что позволяет покупателю отправлять подарки и т.п. другим людям. Для доступа к "мастеру" с целью внесения такого неповторяющегося изменения необходим системный идентификатор компьютера покупателя и пароль. Кроме того, по электронной почте покупателю отсылается подтверждение этой поставки в неавторизованный адрес, чтобы предупредить покупателя о возможности совершения мошеннической сделки.

Как упоминалось выше, в соответствии с предпочтительным примером осуществления настоящего изобретения торговый сайт 140 включает должным образом отформатированную область ввода (которая может быть текущим полем кредитной карточки), куда вводится код покупателя. Формат области ввода задается кредитно-информационным бюро 160 и требуется финансовым учреждением 150. Существует относительно небольшое количество национальных кредитно-информационных бюро 160 (Visa®, MasterCard®, American Express® и т.п.). Вообще, кредитно-информационное бюро 160 может диктовать формат информации, которая должна поставляться более многочисленными финансовыми учреждениями 150, которые имеют дело с кредитно-информационным бюро 160. В свою очередь, торговые сайты 140, которые хотят иметь дело с финансовыми учреждениями 150, должны выполнять требования формата данных финансового учреждения 150 (и, в свою очередь, кредитно-информационного бюро 160). Поэтому система по настоящему изобретению применима к сети, в которой непрерывно добавляется и удаляется большое количество торговых сайтов 140, типа сайтов интернета. В частности, при добавлении торговых сайтов 140 к сети каждый торговый сайт 140 выполняет требования финансового учреждения 150 и должен включать специализированный формат поля данных кода покупателя. Поэтому пользователь должен находить поле данных кода покупателя в огромном количестве веб-сайтов, которые позволяют покупателю делать покупки.

Другими словами, система по настоящему изобретению работает с относительно небольшим количеством национальных кредитно-информационных бюро 160, что позволяет задавать формат (который может измениться от агентства, продающего товары по кредитным карточкам к агентству, продающего товары по кредитным карточкам), который будет доступен торговым организациям 140. По мере того как ограниченное число кредитно-информационных бюро 160 контролирует большинство сетевых сделок по кредитам, формат области ввода кода покупателя будет распространен на большинство торговых сайтов

140. Таким образом, система по настоящему изобретению обеспечивает пользователя доступом фактически ко всем торговым сайтам 140, которые хотят иметь дело с финансовыми учреждениями (это фактически все торговые сайты, которые хотят совершить торговые сделки).

Кредитно-информационные бюро [160] заняты получением покупателей для использования кредитов (например, по своим кредитным карточкам). При этом в системе по настоящему изобретению разработана защита для покупателя помимо дополнительных особенностей по управлению своими кредитными средствами и их использованию кредитно-информационные бюро получают содействие в их продвижении. Кроме того, эти выгодные признаки не требуют дополнительных этапов. Выгода настоящего изобретения состоит в том, что оно устраняет этапы, которые включают повторный ввод информации о покупателе или отправку сообщения по почте с информацией о сторонних базах данных.

Важной характеристикой защиты является то, что торговый сайт 140 не имеет доступа к конфиденциальной информации о покупателе, например, такой как номер кредитной карточки. Напротив, торговый сайт 140 получает только зашифрованный код покупателя от покупателя 100 и код подтверждения сделки (и, возможно, исправленный адрес) от финансового учреждения 150. Поэтому, если любая из предшествующих сделок в сети 170 прервана или если торговый сайт испытывает несанкционированный доступ к записям, информация по кредитной карточке покупателя будет обеспечена защитой.

Кроме того, в системе по настоящему изобретению устранены многие проблемы, связанные с традиционными защищенными сетевыми сделками. В частности, все элементы настоящего изобретения должны быть на месте совершения сделки. В обычных системах один уровень защиты предусмотрен для всех сделок так, что, если база данных нарушена, то доступ получают все записи на этом "защищенном" сайте. В системе по настоящему изобретению создается дополнительный уровень защиты и поэтому защиту получают отдельные записи.

Как описано выше, выгоды, которые вытекают из настоящего изобретения, включают защиту интерактивного кредита индивидуального покупателя, управление, осуществляемое покупателем, и гибкое использование этого кредита.

II. Детальное описание частично продолжающихся примеров осуществления настоящего изобретения.

Заявление о приоритете для предварительной заявки США 60/890230, дата приоритета: 16 февраля 2007 г.

В настоящем изобретении предлагается реальное решение проблемы законодательного регулирования в области виртуальной мировой природы интернета, путем создания системы и использования способа для заключения индивидуальных договоров по индивидуальным сделкам - договоров, которые обеспечивают определенные права и безопасность для каждой стороны, участвующей в интернет-торговле. Путем разработки имеющих исковую силу условий договоров между сторонами, каждая из которых имеет законное основание полагаться на другую сторону (например, ожидать, что имеет дело с совершеннолетним, иначе говоря, с авторизованным участником, который разделяет или берет на себя ответственность за такую сделку), и путем разработки способов присоединения к таким договорам, включая договор быть связанными условиями всех приобретений, проверенных согласно таким договорам, в настоящем изобретении к каждой сделке между сторонами создаются законные и имеющие исковую силу права, основанные на имущественном праве каждой стороны, а не на виртуальной среде коммерческой деятельности.

Один из примеров осуществления настоящего изобретения сконцентрирован на контракте ("договоре с покупателем"), разработанном между эмитентом кредита и покупателем. Договор с покупателем позволяет эмитенту кредита действовать либо в качестве верификатора, либо действовать через авторизованный узел обработки эмитента кредита, либо агента, с целью авторизации и проверки сделки между покупателем и различными участвующими в ней продавцами. Согласно договору между покупателем и эмитентом кредита ожидаемы и допустимы различные соглашения к договорам между покупателем и продавцом, и согласно договору между покупателем и эмитентом кредита также ожидаемы и допустимы различные прямые или косвенные договора между эмитентом кредита и продавцом. Кроме того, существуют договора или контракты между проверяющей организацией, в качестве которой может выступать отдельная организация или организация, связанная с финансовым учреждением, которое выпускает кредитные, дебетовые и/или заранее оплаченные карточки, или другой финансовый провайдер, и индивидуальным покупателем/потребителем.

Договор с покупателем является центром всей деятельности в примерах осуществления настоящего изобретения. Он устанавливает правила и условия, которыми связан покупатель, то есть цена за защиту личных данных физического лица в компьютерной сети состоит в том, что договор с физическим лицом будет юридически подключен к его сделками всегда, когда согласованы все элементы, которые задают идентичность физических лиц в сети (например, его зарегистрированный компьютер с другими идентификаторами, которые отличают это физическое лицо от других, которые могут использовать этот компьютер или иметь доступ к нему). Этот договор охватывает приобретение (то есть договор об ответственности и оплате) и договор по условиям, типа удостаивания любого авторского права или торговых марок, приложенных к нему, и договор о юридической и персональной ответственности за криминал и

гражданские штрафы, охватывающие эти зарегистрированные права. Самым важным является то, что этот договор/контракт между эмитентом кредита и покупателем дает разрешение эмитенту кредита ссылаться на договор с покупателем и придерживаться его условий при любом договоре или любой сделке между покупателем и продавцом. Договор с покупателем, приложенный к любому договору между эмитентом кредита и покупателем, прямо или косвенно позволяет продавцу полагаться на договор между эмитентом кредита и покупателем при проверке договора между покупателем и продавцом. Другими словами, это средство платежа гарантирует оплату продавцу и не требует от физического лица, чтобы он раскрывал, регистрировал личные данные, находящиеся под защитой, или отказывался от них иным способом.

Договор с покупателем является центральным элементом для связанной с ним активности по сделкам, которые могут контролироваться системой по настоящему изобретению. Эта связанная с ним активность включает любую поддающуюся проверке сделку между покупателем и торговой организацией по компьютерной сети, которая может касаться как товаров, так и услуг; и сделку, обеспеченную прямо или косвенно контрактом между продавцом и финансовым учреждением ("договор с продавцом"), в соответствии с которым выплачиваемая продавцом компенсация по сделке между покупателем и продавцом может быть гарантирована или "обязательна". В соответствии с условиями договора с покупателем компенсация, выплачиваемая торговой организации, может быть в виде платежей, кредитоспособности, договора по условиям продажи или по предложениям торговой организации, или по любым другим условиям такого договора между покупателем и торговой организацией, которые может охватывать данный контракт и которые подтверждаются проверяющей организацией во время предварительного договора с торговой организацией.

Контракты, сформированные в соответствии с настоящим изобретением, обеспечивают, среди всего прочего, условия использования, доверие к третьим лицам и законодательную базу. Таким образом, в соответствии с примерами осуществления настоящего изобретения стороны могут придти к соглашению, что надлежащим отправлением правосудия для судебных споров является место проведения деловой активности торговой организации, местонахождение покупателя, имеющего дело с торговой организацией, или любое другое местоположение по выбору. Условия использования включают гарантию "наличия покупателя" (сродни "наличию подписи"), чтобы гарантировать, что торговая организация имеет дело только с идентифицированным покупателем и гарантировать, что торговая организация получит платежи, и не будет страдать от невозврата платежей. Эта гарантия наличия покупателя достигается, когда все зарегистрированные элементы идентификации покупателя присутствуют во время сделки, что подтверждается проверяющей организацией.

Проверяющая организация дает гарантию обеим сторонам сделки по договору между покупателем и эмитентом кредита и договору между эмитентом кредита и продавцом, обеспечивая выполнение всех условий, например, таких как подтверждение приобретения/"наличия подписи", договор о защите авторского права или проверка совершеннолетия. В сущности, на любую информация о покупателе, которую хранит эмитент кредита, могут полагаться третьи лица, фактически не выявляя, при этом, информацию о покупателе или идентичность покупателя. В этом отношении эмитент кредита действует как держатель кредита как от имени покупателя, так и от имени торговой организации, и проверяющая организация удостоверяет это при каждой индивидуальной сделке. Это может быть связанный элемент сделки или элемент типа условного депонирования у третьего лица, который защищает идентичность покупателя и права торговой организации, и элемент, на который торговая организация может отдельно полагаться.

Общие условия приобретения по сетям типа интернета включают использование банка, выпускающего кредитную карточку или дебетовую карточку, при этом независимо от того, базируется ли сделка на кредите или на заранее оплаченной карточке, банк-эмитент предоставляет кредит по карточке, пока оплата фактически не получена продавцом, если вообще будет получена. В обычной практике эту процедуру платежей выполняет банк, "носящий две шляпы": "банка-эмитента" и "банка-получателя". Как банк-эмитент, банк выдает кредит и карточку покупателю для использования при покупке товара, оплате услуг и т.п. Как банк-получатель, банк соглашается получить (и произвести оплату) долг, образовавшийся при использовании этих кредитных карточек. Согласно условиям обычной сделки по кредитной карточке по интернету банк, действующий как "банк-эмитент", использует свой договор для использования карточки согласно условиям, в соответствии с которыми требуется оплата и процентный доход по любому неоплаченному балансу. По отдельному типу договора банк, действующий как "банк-получатель", требует от торговых организаций, среди прочего, проверять идентичность пользователя кредитной карточки и заставить владельца кредитной карточки подписывать получение покупки. Это упрощенное объяснение сделок по кредитной карточке достаточно, чтобы обозначить проблему несанкционированного использования кредитной карточки и проверки личных данных для сделок по интернету или по любой подобной системе торговли через компьютер.

Договор между эмитентом кредита и продавцом играет дополнительную роль просеивания квалифицированных продавцов. Одним из элементов мошенничества в электронной коммерции является мошенничество продавца. Договора с продавцами, чьи истории с мошенничеством известны или которые подозреваются в мошенничестве, могут быть аннулированы, иными словами, они могут быть лишены

доступа к условиям платежей при наличии подписи, предусмотренным в настоящей заявке и к другим защитам, типа авторского права. Этот этап аттестации торговой организации необходим как для защиты покупателя, так и для ограничения мошенничества.

С учетом этих проблем в системе и процессе по примеру осуществления настоящего изобретения используется зашифрованный код ("поток шифрованных данных"), который позволяет третьей проверяющей стороне проверять наличие покупателя для торговой организации и проверять договор покупателя с эмитентом кредита, условия которого позволяют проверяющей организации подтверждать идентичность покупателя и договор, связанный условиями сделки с продавцом, включая оплату при наличии подписи. В соответствии с другим примером осуществления настоящего изобретения вместо того, чтобы только ссылаться на идентификатор договора с покупателем в потоке шифрованных данных, получение товара и условия сделки могут быть зашифрованы целиком и включены в поток шифрованных данных.

Согласно условиям договора между эмитентом кредита и покупателем проверяется договор между покупателем и продавцом и, при уверенности в нем, - договор между эмитентом кредита и покупателем, который обеспечивает условия договора между покупателем и продавцом через согласованное присоединение первых двух договоров. Договор между покупателем и продавцом является ожидаемым результатом, целью других двух договоров, в соответствии с которыми ожидается, что все стороны будут связаны своими частями отдельных договоров в таком пункте, который касается эмитента кредита, или его агента, например процессора, который проверяет наличие покупателя и договор по условиям сделки по запросу покупателя, что вызвано представлением поддающегося проверке потока шифрованных данных.

Таким образом, в соответствии с некоторыми примерами осуществления настоящего изобретения в отдельном договоре с покупателем (между проверяющей организацией или эмитентом кредита и покупателем) и в договоре с торгующей организацией (между торговой организацией и ее коммерческим банком) присутствует требование, по которому покупатель и торговая организация заключают договор с покупателем (между торговой организацией и покупателем), который разрабатывается во время торговой сделки между торговой организацией и покупателем. В соответствии с примерами осуществления настоящего изобретения требуется, чтобы эмитент кредита отсеивал продавцов в качестве дальнейшей защиты покупателя. В соответствии с примерами осуществления настоящего изобретения для каждой торговой сделки между торговой организацией и покупателем можно разрабатывать новый договор с покупателем, который, среди прочего, обязывает покупателя, если применимо к специальной сделке, соблюдать права интеллектуальной собственности торговой организации на средства аудиовизуальной информации и в котором присутствуют имеющие обязательную силу положения, если применимо к специальной сделке, относительно наличия, личных данных, возраста и т.п. покупателя.

Проверяющая организация связана по договору с эмитентом кредита с покупателем и через этот договор с другими сторонами и обеспечивает защиту личных данных и сделки покупателя, и проверку, авторизацию и защиту платежей и другие условия сделки (типа возраста, личных данных, места жительства, договора о соблюдении авторского права/обязательств по авторскому праву и т.п.) от имени торговой организации.

Перед созданием потока шифрованных данных (во время торговой сделки) необходимо наличие некоторых элементов, чтобы подтвердить личные данные индивидуального покупателя и проверить, что покупатель согласился быть связанным условиями безотлагательного договора с покупателем. Эта последовательность элементов может включать, среди прочего, имя (не обязательно имя владельца кредитной карточки), адрес для доставки или подтверждения статуса резидента (не обязательно адрес составления счетов владельца кредитной карточки), уникальный номер кредита покупателя или ID с финансовой организацией и идентичность зарегистрированных технических устройств компьютера, или компьютеров, которые покупатель намеревается авторизовать для таких сделок. Поток шифрованных данных создается от некоторых из этих элементов, типа имени, адреса, идентификатора договора с покупателем, идентификатора технических устройств компьютера и т.п., но не включает уязвимую информацию, типа номера кредитной карточки покупателя или номеров банковских счетов. Кроме того, к потоку шифрованных данных с целью обеспечения маршрутизации добавляется BIN (Bank Identification Number - идентификационный номер банка) или другой идентификатор маршрутизации, типа адреса IP, который не зашифрован.

В соответствии с условиями контракта между эмитентом кредита и покупателем, который разрабатывается во время регистрации, с целью подтверждения наличия покупателя во время сделки с торговой организацией проверяющая организация требует наличия всех необходимых элементов потока шифрованных данных. Торговой организации не известны личные данные покупателя, потому что эта информация зашифрована. Сделка подтверждается, как только проверка подтверждает наличие всех кодированных элементов, при этом торговая организация получает инструкцию о доставке, если эта информация требуется, и выполняется требование торговой организации о получении подписи и проверке личных данных покупателя (то есть торговая организация получит платеж и/или обратится за помощью по таким условиям сделки, как проверка возраста и/или авторское право).

В настоящем изобретении используются условия, разработанные покупателем при составлении договора с эмитентом кредита. Договор составлен таким образом, что покупатель несет ответственность по

всем сделкам, где присутствуют все требуемые элементы любого из потоков шифрованных данных покупателя. Кроме того, договор позволяет загружать поток шифрованных данных наряду с любыми цифровыми средствами аудиовизуальной информации, приобретаемыми покупателем в качестве записи по договору к условиям использования, типа защиты авторского права.

В одном аспекте настоящего изобретения предлагается система и способ для создания, проверки и вставки (при необходимости) согласованного в соответствии с контрактом "кода", который, при использовании со всеми элементами, действует как уникальная подпись индивидуального покупателя, подтверждающая наличие покупателя в сделке. Торговая организация имеет право полагаться на условия сделки по договору с покупателем, согласованные с покупателем (которые, кроме того, подтверждают личные данные и юрисдикцию). В настоящем изобретении предлагается защита личных данных в обмен на связывание по контракту всех сторон условиями таких сделок. Таким образом, в настоящем изобретении предлагается возможность защиты конфиденциальности и личных данных покупателя, начинающего сделку по приобретению в интернете, защищая, при этом, и права, и коммерческие выгоды торговой организации, предоставляющей продукт, услугу и т.п. В соответствии с примерами осуществления настоящего изобретения предлагается защита личных данных покупателя, которые остаются зашифрованными и/или защищенными иным способом, если условия договора не нарушены каким-либо образом.

Удаление "кода" делает носитель непригодным для использования, как описано в публикации патента США № 2007/0061580 (которая включена в настоящую заявку в качестве ссылки), при этом отсутствие водяных знаков или кода препятствует доступу к приобретаемому продукту со стороны электронных средств хранения аудиовизуальной информации. Согласно условиям договора и юрисдикции эмитента кредита наличие такого "кода" во множестве копий средств аудиовизуальной информации, в нарушение условий приобретения и защиты авторского права, дало бы торговой организации возможность считать покупателя ответственным за множественные копии. Таким образом, договор с покупателем является механизмом отстаивания в судебном порядке нарушений специально согласованного авторского права во время приобретения.

Короче говоря, в соответствии с настоящим изобретением предлагается способ, система, структура и устройство для продвижения, защиты и проверки коммерческих отношений в компьютерных сетях, типа интернета, путем защиты права покупателя, включая личные данные покупателя и финансовую информацию, и права торговой организации, включая платежи, причитающиеся торговой организации, и контроль, выполняемый торговой организацией, и защиты ее собственности на продукты и/или услуги, в частности, путем установления различных прав, согласованных по юрисдикции, для их защиты и отстаивания в судебном порядке. Таким образом, в соответствии с примерами осуществления настоящего изобретения разрабатывается обязательный контракт между сторонами сделки с наделением эмитента кредита и проверяющей организации обусловленной контрактом правоспособностью при согласии покупателя и торговой организации. В соответствии с примерами осуществления настоящего изобретения подтверждается, что предусмотрены элементы личных данных и надежности заемщика в сделке, и при этом обеспечивается защита личных данных покупателя и гарантии торговой организации по компенсации. Таким образом, настоящее изобретение может использоваться, чтобы установить элемент сделки с "проверенным наличием", установить элемент сделки с "проверенной подписью", установить возраст покупателя (например, в терминах "более 18", или "более 21", или "более 65"), установить элемент места жительства или доставки, установить связь покупателя/продавца с договором для покупателя и установить личные данные покупателя (без необходимости ее выявления или сохранения в режиме он-лайн), при этом, в частности, требуется, чтобы все компоненты потока шифрованных данных присутствовали и были проверены для совершения сделки.

Теперь обратимся к чертежам, в настоящем изобретении предлагается способ и система обеспечения прав при сделке по компьютерной сети 404. Как показано на фиг. 4, условия договоров 422, которые разработаны между покупателем 402, торговой организацией 450 и проверяющей организацией 420 и/или финансовым учреждением 440, хранятся в проверяющей организации 420. Проверяющая организация 420 может быть частью финансового учреждения (эмитента кредита) 440, как показано на фиг. 5, или быть независимой организацией, как показано на фиг. 4. В то время как на фиг. 4 показан единственный компьютер покупателя 410, единственная проверяющая организация 420, единственное финансовое учреждение 440 и единственная торговая организация 450, что иллюстрирует только один пример возможного осуществления настоящего изобретения, что понятно специалистам, то на фиг. 5 показан пример возможного (и наиболее вероятного) варианта с множеством компьютеров покупателей 410, множеством проверяющих организаций 420, множеством финансовых учреждений 440, множеством торговых организаций 450 и т.п. Поэтому в проверяющей организации 420 хранится множество договоров 422, по одному для каждой торговой сделки.

Способ включает регистрацию и хранение договора (договоров) 422 покупателя с эмитентом кредита/проверяющей организацией 440/420. Информация о покупателе хранится в базе данных 430, которая может находиться у эмитента кредита/проверяющей организации 440/420, как показано на фиг. 5 или как показано на фиг. 4, отдельно от эмитента кредита/проверяющей организации 440/420. Специалистам понятно, что, в то время как на фиг. 4 показана только одна база данных 430, может быть вариант и с

множеством баз данных 430, некоторые из которых могут быть у эмитента кредита/проверяющей организации. Кроме того, компьютер покупателя 410 подключен к торговой организации 450 и проверяющей организации 420 по одной или по большему количеству компьютерных сетей 404.

Чтобы получить доступ к шифратору 412 в компьютере покупателя 410 используется пароль. Шифратор 412 загружается в компьютер покупателя 410 проверяющей организацией 420 во время процесса регистрации покупателя. Шифратор 412 шифрует информацию о покупателе, чтобы сформировать поток шифрованных данных 414, который хранится в компьютере покупателя 410. Информация о покупателе не хранится в компьютере покупателя в незашифрованном виде. Кроме того, поток шифрованных данных не включает никакой персональной финансовой информации о покупателе, касающейся номера кредитной карточки, номеров банковских счетов и т.п., и такая информация хранится только в базе (базах) данных 430.

Кроме того, проверяющая организация загружает в компьютер покупателя 410 и торговой организации 450 агентов пересылки 416, 456. Агент пересылки 416 обеспечивает пересылку потока шифрованных данных 414 с компьютера покупателя на компьютер торговой организации 450 при осуществлении торговой сделки по приобретению электронного продукта 454.

У проверяющей организации 420 есть верификатор 424, который оперативно подключается как к компьютеру покупателя 410, так и к компьютеру торговой организации 450. В примерах осуществления настоящего изобретения для усиления степени защиты информации о покупателе верификатор 424 содержится отдельно от компьютера покупателя 410 и торговой организации и находится у эмитента кредита/проверяющей организации 440/420. База данных 430 с информацией о платежах покупателей может находиться у эмитента кредита/проверяющей организации 440/420 или вне проверяющей организации 420. В любом случае база данных 430 оперативно подключается только к верификатору 424 и ни покупатель, ни торговая организация не имеют доступа к этой базе данных.

В соответствии со способом по настоящему изобретению агент пересылки 416 пересылает поток шифрованных данных 414 (наряду с денежной суммой сделки) от компьютера торговой организации 450 к верификатору 424 для проверки платежей. Верификатор 424 генерирует проверку платежей по базе данных 430 и передает результаты проверки платежей торговой организации 450. Торговая организация добавляет поток шифрованных данных 414 и/или идентификатор сделки к приобретаемому электронному продукту с целью создания персонифицированного электронного продукта 454 (как показано на фиг. 6), который поставляется торговой организацией 450 в компьютер покупателя 410.

Поток шифрованных данных 414 может включать такую информацию, как имя покупателя, адрес доставки, дата рождения покупателя и идентификатор технических устройств компьютера покупателя. Адрес доставки может включать один из множества достоверных адресов доставки, что зависит от того, какой поток шифрованных данных 414 передается торговой организации 450. Таким образом, способ может позволить покупателю выбирать из множества сохраняемых потоков шифрованных данных 414, каждый из которых имеет другой надлежаще оформленный адрес доставки. В соответствии с предлагаемым способом выбранный поток шифрованных данных 414 вместе с идентификатором компьютера передается в сделке по компьютерной сети 404 торговой организации 450 как часть кода идентификатора (CID и идентификатор маршрутизации 416).

Посредством идентификатора маршрутизации 416 поток шифрованных данных 414 направляется по компьютерной сети 404 проверяющей организации 420. Проверяющая организация 420 расшифровывает поток шифрованных данных 414 и сравнивает идентификатор адреса доставки покупателя, идентификатор имени, идентификатор возраста или другие идентификаторы с авторизованными соответствующими идентификаторами покупателя, находящимися у проверяющей организацией 420, в виде "идентификаторов" имени, возраста, адреса и т.п., которые могут быть фактическими именами, адресами и т.п., или могут быть буквенно-цифровыми кодами, которые используются проверяющей организацией 420 для поиска имени, адреса, возраста и т.п., в базе данных 430. Если все в порядке, проверяющая организация 420 возвращает торговой организации 450 по компьютерной сети 404 решение об авторизации. Таким образом, проверяющая организация 420 может произвести (и возвратить торговой организации) проверку личных данных, авторизацию платежей и т.п. Проверяющая организация 420 проверяет, что условия проверенного наличия покупателя и электронной подписи были выполнены согласно договору 422 покупателя с проверяющей организацией 420, который подтверждает торговой организации 450, что покупатель принял на себя ответственность за сделку.

Кроме того, каждый из потоков шифрованных данных 414 может включать уникальный способ платежей, который отличается от способов платежей других потоков шифрованных данных 414. В соответствии с другим примером осуществления настоящего изобретения с помощью группы потоков шифрованных данных 414 можно идентифицировать отдельную кредитную организацию, осуществляющую платеж, при этом каждый поток шифрованных данных 414 в группе может включать другое имя пользователя, другое авторизованное и зарегистрированное устройство/компьютер, другой способ проверки возраста и/или другой адрес покупателя.

В соответствии с примерами осуществления настоящего изобретения проверки покупателей и авторизации платежей по сделкам по оказанию услуг или приобретению материальных товаров (типа стерео-

оборудования, фильтров, книг, бакалеи, одежды, мебели, компьютеров и т.п.) могут убывать. Однако в соответствии с примерами осуществления настоящего изобретения такие же сделки по электронным продуктам, которые имеют потенциал, непропорционально разделенный в компьютерных сетях, могут добавлять к электронным продуктам поток шифрованных данных или идентификаторов сделок. Таким образом, в части договора 422 покупатель соглашается встроить, впечатать и/или иначе прикрепить поток шифрованных данных 414 и идентификатор маршрутизации 416 к средствам аудиовизуальной информации или к контенту средств аудиовизуальной информации 454, приобретенных у торговой организации 450, как показано на фиг. 6. Перед передачей потока шифрованных данных 414 торговой организации 450 проверяющая организация может добавить поток шифрованных данных, который может содержать договор с покупателем или идентификатор договора с покупателем, или идентификатор сделки, к потоку шифрованных данных 414, чтобы обеспечить вступление в силу договора покупателя 422 между покупателем 402 и торговой организацией 450.

Этот процесс, кроме того, устанавливает юрисдикцию по осуществлению прав торговой организации 404, как установлено в договоре с покупателем 422. Решение об авторизации одобряется, только если поток шифрованных данных 414 и информация о покупателе в базе данных 430 согласуются. В соответствии со способом проверяющая организация 420 по электронной почте может отправить покупателю 414 подтверждение сделки. Поток шифрованных данных 414/CID хранится на запоминающем устройстве покупателя 408 только в зашифрованном виде.

Как показано в блок-схеме на фиг. 7, способ по настоящему изобретению облегчает торговые сделки с помощью компьютеров по сохраняемым в электронном виде продуктам (которые иногда упоминаются в данном документе как электронные продукты) типа литературных произведений, музыкальных работ (записей), видеоработ (кино, представления, видео и т.п.) и т.п.

Сначала в блоке 700 покупатель заключает договор покупателя с проверяющей организацией. Затем в блоке 702 в соответствии с примерами осуществления настоящего изобретения шифруется "информация о покупателе", чтобы получить поток шифрованных данных 704. Методики шифрования данных раскрыты, например, в патентах США №№ 7257225 и 7251326 (которые включены в настоящую заявку в качестве ссылок), и детали таких процессов не рассматриваются в настоящей заявке. Такая информация о покупателе может включать идентификатор имени (который может соответствовать, а может и не соответствовать формальному имени покупателя), идентификатор возраста покупателя (который может быть определенным возрастом, возрастным диапазоном, классификацией возраста), идентификатор адреса (который может быть адресом покупателя или другим адресом).

В соответствии с примерами осуществления настоящего изобретения в блоке 706 поток шифрованных данных передается от покупателя торговой организации при осуществлении торговой сделки по приобретению электронного продукта. В блоке 708 проверяющая организация получает поток шифрованных данных, который посылает торговая организация для проверки платежей. Затем, проверяющая организация пересылает поток шифрованных данных в отдельную базу данных, содержащую информацию о платежах покупателя (блок 710), чтобы создать уникальный идентификатор сделки, включающий проверку личных данных и/или авторизацию платежей в блоке.

В блоке 714 проверяющая организация передает уникальный идентификатор сделки от проверяющей организации в торговую организацию. Проверка личных данных и авторизация платежей подтверждают торговой организации фактическое наличие покупателя при осуществлении торговой сделки, при этом торговая организация получает гарантию, что она осуществляет сделку только с покупателем и больше ни с кем.

Как упоминалось выше, поток шифрованных данных 704 и проверка личных данных и авторизация платежей 710 лишены персональной информации о платежах покупателя, типа информации о кредитной карточке, информации о банковском счете и т.п., и могут принимать вид уникального идентификатора сделки. Таким образом, даже если поток шифрованных данных будет расшифрован, информация о платежах покупателя не будет раскрыта или использована. Таким образом, поток шифрованных данных, получаемый от покупателя, может быть изменен проверяющей организацией перед тем, как быть отправленным торговой организации, чтобы включать данные или информацию, которая является специфической для проводимой торговой сделке, или поток шифрованных данных может сопровождаться уникальным идентификатором сделки. В соответствии с примерами осуществления настоящего изобретения такой измененный поток шифрованных данных или уникальный идентификатор сделки могут использоваться вместо первоначального потока шифрованных данных. Таким образом, перед отправкой электронного продукта покупателю к нему может добавляться первоначальный поток шифрованных данных, измененный поток шифрованных данных и/или уникальный идентификатор сделки.

В примерах осуществления настоящего изобретения, в которых говорится об электронных продуктах, которые могут быть ненадлежащим образом скопированы и распространены по компьютерным сетям, как показано в блоке 716, торговая организация для создания персонифицированного электронного продукта 718 к приобретаемому электронному продукту добавляет поток шифрованных данных и/или уникальный идентификатор сделки. Чтобы покупатель не мог удалить поток шифрованных данных или идентификатор сделки из персонифицированного электронного продукта, поток шифрованных данных

или идентификатор сделки могут быть скрыты. Известны способы включения информации в цифровой продукт (см. патенты США №№ 6691229 и 5809160, которые включены в настоящую заявку в качестве ссылок). Кроме того, при удалении потока шифрованных данных или идентификатора сделки персонифицированный электронный продукт может потерять функциональность (т.е. персонифицированный электронный продукт нельзя открыть или воспроизвести и т.п.). Кроме того, известны способы управления доступом к цифровым продуктам через потоки шифрованных данных или водяные знаки (см. патент США № 7062069, который включен в настоящую заявку в качестве ссылки).

Таким образом, в персонифицированном электронном продукте всегда сохраняется поток шифрованных данных, что позволяет идентифицировать покупателя (через проверяющую организацию), который приобрел этот электронный продукт, и все копии купленного электронного продукта будут снабжены потоком шифрованных данных или идентификатором сделки. Таким образом, так как все копии персонифицированного электронного продукта будут снабжены потоком шифрованных данных, можно всегда идентифицировать покупателя, который первоначально приобрел этот электронный продукт у торговой организации (источник копий).

Как показано в блоке 720, после добавления к приобретаемому электронному продукту потока шифрованных данных или идентификатора сделки торговая организация поставляет персонифицированный электронный продукт покупателю. Каждый персонифицированный электронный продукт, распространяемый среди различных покупателей, отличается уникальностью потока шифрованных данных или идентификатора сделки, что позволяет по копиям электронного продукта идентифицировать покупателя, который первоначально приобрел этот электронный продукт. Кроме того, уникальность каждого потока шифрованных данных или идентификатора сделки позволяет проверяющей организации идентифицировать источник неавторизированных копий купленного электронного продукта. Таким образом, как показано в блоке 722, способ может включать этап идентификации покупателя по потоку шифрованных данных, который включен в персонифицированный электронный продукт.

Во время регистрации покупателя (когда покупатель заводит или изменяет свою учетную запись у эмитента кредита) и во время приобретения электронных продуктов покупатель получает уведомление или предупреждение о том, что информация о нем будет всегда присутствовать в копиях любых персонифицированных электронных продуктов. Кроме того, во время приобретения электронного продукта отображается подобное уведомление или предупреждение, сообщая покупателю, что он согласен связать себя условиями и штрафами за неавторизованное использование или копирование электронного продукта; и каждый раз (или первые несколько раз), когда персонифицированный электронный продукт открывается, воспроизводится и т.п. может высвечиваться такое же предупреждение. Такие предупреждения служат для предотвращения передачи покупателем копий персонифицированного электронного продукта другим лицам в нарушение прав торговой организации (например, при незаконной передаче или копировании), так как покупатель предупрежден о том, что незаконная передача или копирование могут быть отслежены проверяющей организацией и привести к нему с помощью потока шифрованных данных, то он соглашается быть связанным условиями, сформулированными в этих предупреждениях. Подобное авторизованное использование и предупреждения во время передачи продукта могут также применяться для доступа на основе возраста, для назначения цены на основе возраста или места жительства и т.п. В примерах осуществления настоящего изобретения учитывается широкий диапазон идентификаторов покупателя, которые поощряют, продвигают и защищают электронную коммерцию и участвующие в ней стороны.

На фиг. 8 показано шифрование информации о покупателе 702. Сначала с помощью первого компьютеризованного устройства 800 покупатель подключается к эмитенту кредита и проверяющая организация загружает некоторое программное обеспечение на первое компьютеризованное устройство 802. Покупатель предоставляет или соглашается предоставить проверяющей организации 804 доступ к существующей чувствительной информации, типа достоверных адресов доставки, своей даты рождения (или классификацию возрастной группы), своего номера банковского счета, номера кредитной карточки и т.п. Некоторые элементы информации о покупателе (типа номеров банковских счетов и номеров кредитных карточек) не хранятся в компьютеризованном устройстве покупателя, а вместо этого хранятся только в базах данных эмитента кредита и/или проверяющей организации, хотя для создания специфических ссылок на эту информацию могут использоваться кодированные или не кодированные идентификаторы. Другие элементы или идентификаторы (ссылки на имя, адрес, возраст и т.п.) информации о покупателе могут быть зашифрованы, чтобы создать поток шифрованных данных, который хранится на компьютеризованном устройстве покупателя и который перед шифрованием может быть частично или полностью кодирован или не кодирован.

Как показано в блоке 806 при авторизации покупателя эмитент кредита считывает с первого компьютеризованного устройства и регистрирует уникальные идентификаторы технических устройств (типа серийных номеров материнских плат, жестких дисков, процессора и т.п.). Кроме того, в блоке 808 эти уникальные идентификаторы технических устройств включаются в поток шифрованных данных. Затем эти же этапы повторяются для любых дополнительных компьютеризованных устройств, которые покупатель желает авторизовать и регистрировать для использования в будущих торговых сделках. Такие

процессы могут иметь место, когда покупатель вводит или изменяет свою учетную запись у эмитента кредита.

В данной заявке также учитывается использование "общего" или "незарегистрированного" компьютера. Можно "разрешить" аварийный доступ к физическому лицу, если доступ к его "учетной записи" осуществлялся с "незарегистрированного" компьютера и было дано распоряжение на "ограниченное" одобрение на использование данного компьютера по существующей учетной записи, при этом данное одобрение может быть ограничено по времени (например, 15 мин на одну покупку) или ограниченного по использованию (например, одноразовое использование на одну покупку).

В другом примере осуществления настоящего изобретения предусмотрен процессе проверки торговой организации, которая имеет дело не с одним покупателем: приблизительное время передачи потока шифрованных данных торговой организации, при этом перед фактической передачей потока шифрованных данных торговой организации (как часть процесса передачи потока шифрованных данных) в поток шифрованных данных вводится второй набор идентификаторов технических устройств и метка времени и даты с компьютеризованного устройства, осуществляющего фактическую передачу потока шифрованных данных. Поэтому, как показано на фиг. 9, после введения в поток шифрованных данных в блоке 900 идентификаторов технических устройств, в блоке 902 считывается второй набор идентификаторов технических устройств с фактического компьютера, который подключен к торговой организации. Затем в блоке 904 этот второй набор идентификаторов технических устройств (и, возможно, метка времени и даты) добавляется к потоку шифрованных данных и в блоке 906 измененный поток шифрованных данных (имеющий оба набора идентификаторов технических устройств) передается торговой организации.

Таким образом, если недобросовестный человек смог получить ненадлежащую копию потока шифрованных данных и использовал ненадлежащую копию потока шифрованных данных в компьютере (который не является одним из компьютеров покупателя, зарегистрированных в торговой организации) вместе с необходимым созданием потока шифрованных данных, поставляемым эмитентом кредита, и передачей программного обеспечения, то вторые идентификаторы технических устройств, которые считываются только до передачи потока шифрованных данных, не будут соответствовать первым идентификаторам технических устройств в потоке шифрованных данных, и сделка не будет одобрена проверяющей организацией. Точно так же можно использовать метку времени и даты, чтобы создавать поток шифрованных данных, который передается торговой организации, и действует только в течение ограниченного периода времени (например, минуты, часы, дни и т.п.). Такие процессы улучшают процесс проверки "наличия покупателя", выполняемый проверяющей организацией для обеспечения дополнительных гарантий торговой организации в том, что она фактически имеет дело с конкретным покупателем, а не с кем-то другим.

Примеры осуществления данного изобретения могут включать только технические устройства, только программное обеспечение или как элементы технических устройств, так и программного обеспечения. В соответствии с одним из примеров настоящее изобретение осуществлено в программном обеспечении, которое включает встроенное программное обеспечение, резидентное программное обеспечение, микрокоды и т.п., но не ограничено ими.

Кроме того, настоящий пример осуществления данного изобретения может относиться к компьютерному программному продукту с доступом к средствам аудиовизуальной информации, который используется в компьютере или считывается компьютером, и на котором записан программный код для использования на компьютере или при подключении к компьютеру либо в любой другой системе выполнения команд. В настоящем описании в качестве средства аудиовизуальной информации, которое используется в компьютере или считывается компьютером, может применяться аппарат, в состав которого может входить программа для использования в системе выполнения команд, в аппарате или устройстве или при подключении к ним, при этом данный аппарат может хранить такую программу, поддерживать с ней связь, распространять, или передавать.

В качестве средства аудиовизуальной информации может использоваться электронная, магнитная, оптическая, электромагнитная, инфракрасная или полупроводниковая система (или аппарат либо устройство) или среда распространения. Примеры читаемой компьютером среды включают полупроводниковое или твердотельное запоминающее устройство, магнитную ленту, сменную компьютерную дискету, оперативную память, постоянное запоминающее устройство, жесткий диск и оптический диск. Примеры оптических дисков включают компакт-диск как постоянное запоминающее устройство (CD-ROM), компакт-диск для чтения/записи (CD-R/W) и DVD.

Система обработки данных для хранения и/или выполнения программных кодов включает по крайней мере один процессор с непосредственной или косвенной связью с элементами памяти через системную шину. Элементы памяти могут включать местную память, используемую во время фактического выполнения программного кода, накопитель данных большой емкости и кэш-память, которые обеспечивают временное хранение, по крайней мере, некоторого программного кода, чтобы уменьшать количество обращений к коду в накопителе данных большой емкости во время выполнения программы.

Устройства ввода/вывода (которые включают клавиатуру, дисплеи, устройства управления позицией и т.п., но не ограничиваются ими) могут подключаться к системе либо непосредственно, либо через

промежуточные контроллеры ввода/вывода. Кроме того, к системе могут подключаться сетевые адаптеры, чтобы дать возможность системе обработки данных подключаться к другим системам обработки данных или отдаленным принтерам или запоминающим устройствам через промежуточные частные или общественные сети. Модемы, кабельный модем и карты Ethernet являются только некоторыми из доступных в настоящее время типов сетевых адаптеров.

На фиг. 10 изображена представительная аппаратная среда для осуществления настоящего изобретения. Эта схема иллюстрирует аппаратную конфигурацию компьютерной системы информационной обработки по настоящему изобретению. Система включает по крайней мере один процессор или центральный процессор 10. Центральные процессоры 10 подключены через системную шину 12 к различным устройствам, типа оперативной памяти (RAM) 14, постоянного запоминающего устройства (ROM) 16 и адаптера ввода/вывода 18. Адаптер ввода/вывода 18 может соединяться с периферийными устройствами, типа дисковых запоминающих устройств 11 и накопителей на магнитной ленте 13, или других запоминающих устройств для хранения программ, которые считываются системой. Система может считывать команды с запоминающих устройств для хранения программ и выполнять эти команды, чтобы исполнять методологию примеров осуществления настоящего изобретения. Кроме того, в состав системы входит адаптер интерфейса пользователя 19, который подключает клавиатуру 15, мышь 17, динамик 24, микрофон 22 и/или другие устройства интерфейса пользователя, типа сенсорного экранного устройства (не показано), к шине 12, чтобы объединить ввод пользователя. Кроме того, адаптер связи 20 подключает шину 12 к сети обработки данных 25, а адаптер дисплея 21 подключает шину 12 к устройству отображения 23, которое может быть устройством вывода типа монитора, принтера или передатчика, например.

Предшествующее описание конкретных примеров осуществления полностью отражает общий характер настоящего изобретения и поэтому, применяя данные знания, можно легко изменять и/или приспосабливать к различным приложениям конкретные воплощения, не отступая, при этом, от основной концепции, и поэтому такие адаптации и модификации предназначены для постижения в значении и диапазоне эквивалентов раскрытых примеров осуществления настоящего изобретения. Следует понимать, что фразеология или терминология, используемая в настоящей заявке, применяются только для описания, а не для ограничений. Поэтому, в то время как настоящие примеры осуществления данного изобретения были описаны в терминах предпочтительных примеров осуществления настоящего изобретения, специалисты понимают, что примеры осуществления настоящего изобретения могут применяться на практике с изменениями в рамках объема и сущности прилагаемых пунктов формулы.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ для обеспечения безопасной торговой сделки в компьютерной сети, который включает

шифрование информации о покупателе в потоке шифрованных данных, при этом упомянутая информация о покупателе включает идентификатор имени, идентификатор возраста покупателя, идентификатор адреса и идентификатор договора с покупателем;

передачу упомянутого потока шифрованных данных от покупателя торговой организации при осуществлении торговой сделки по приобретению электронного продукта;

маршрутизацию упомянутого потока шифрованных данных в проверяющую организацию;

создание упомянутой проверяющей организацией уникального идентификатора сделки, включающего по крайней мере один из результатов проверки личных данных и авторизации платежей на основе упомянутого потока шифрованных данных;

передачу упомянутой проверяющей организацией упомянутого уникального идентификатора сделки упомянутой торговой организации, при этом упомянутый поток шифрованных данных и упомянутый уникальный идентификатор сделки лишены персональной информации по платежам упомянутого покупателя;

добавление упомянутого потока шифрованных данных и упомянутого идентификатора сделки упомянутой торговой организацией к упомянутому приобретенному продукту с целью создания персонифицированного электронного продукта и

поставку упомянутой торговой организацией упомянутому покупателю упомянутого электронного продукта при условии, что каждый персонифицированный электронный продукт, поставляемый различным покупателям, отличается уникальностью своего потока шифрованных данных.

2. Способ по п.1, отличающийся тем, что упомянутое шифрование упомянутой информации о покупателе включает также следующие этапы:

a) подключение упомянутого покупателя к упомянутой проверяющей организации с помощью первого компьютеризованного устройства;

b) считывание идентификаторов технических устройств с упомянутого первого компьютеризованного устройства;

c) включение упомянутых идентификаторов технических устройств в упомянутый поток шифрованных данных и

d) повторение этапов a)-c) для дополнительных компьютеризованных устройств, которые упомяну-

тый покупатель желает использовать в какой-либо торговой сделке.

3. Способ по п.2, отличающийся тем, что передача упомянутого потока шифрованных данных от упомянутого покупателя упомянутой торговой организации включает также

приблизительное время передачи упомянутого потока шифрованных данных упомянутой торговой организации, при этом перед фактической передачей упомянутого потока шифрованных данных упомянутой торговой организации в упомянутый поток шифрованных данных включается второй набор идентификаторов технических устройств и метка времени и даты из компьютеризованного устройства, осуществляющего упомянутую фактическую передачу; и

прикрепление незашифрованного идентификатора маршрутизации к упомянутому потоку шифрованных данных.

4. Способ по п.1, отличающийся тем, что упомянутая проверка личных данных и упомянутая авторизация платежей подтверждает упомянутой торговой организации фактическое наличие упомянутого покупателя в упомянутой торговой сделке, при этом упомянутая торговая организация получает гарантию в том, что она осуществляет торговую сделку ни с кем иным, кроме упомянутого покупателя, и упомянутый идентификатор сделки позволяет упомянутой торговой организации передать сделку на обработку по определению наличия подписи.

5. Способ по п.1, отличающийся тем, что упомянутая уникальность каждого потока шифрованных данных позволяет идентифицировать источник неавторизованных копий упомянутого приобретенного электронного продукта с помощью упомянутой проверяющей организации.

6. Способ для обеспечения безопасной торговой сделки в компьютерной сети, который включает

шифрование информации о покупателе в потоке шифрованных данных, при этом упомянутая информация о покупателе включает идентификатор имени, идентификатор возраста покупателя, идентификатор адреса и идентификатор договора с покупателем;

передачу упомянутого потока шифрованных данных от покупателя торговой организации при осуществлении торговой сделки по приобретению электронного продукта;

маршрутизацию упомянутого потока шифрованных данных в проверяющую организацию;

создание упомянутой проверяющей организацией уникального идентификатора сделки, включающего по крайней мере один из результатов проверки личных данных и авторизации платежей на основе упомянутого потока шифрованных данных;

выполняемое проверяющей организацией сравнение с помощью перекрестных ссылок данных из потока шифрованных данных с данными из отдельной базы данных, содержащей информацию о покупателе, с целью создания упомянутого уникального идентификатора сделки;

передачу упомянутой проверяющей организацией упомянутой торговой организации по крайней мере одного результата упомянутой проверки личных данных и упомянутой авторизации платежей, при этом упомянутый поток шифрованных данных, упомянутые результаты проверки личных данных и упомянутая авторизация платежей лишены персональной информации по платежам упомянутого покупателя;

добавление по крайней мере одного упомянутого потока шифрованных данных, результатов проверки личных данных и авторизации платежей упомянутой торговой организацией к приобретенному продукту с целью создания персонифицированного электронного продукта;

поставку упомянутой торговой организацией упомянутому покупателю упомянутого электронного продукта при условии, что каждый персонифицированный электронный продукт, поставляемый различным покупателям, отличается уникальностью своего потока шифрованных данных.

7. Способ по п.6, отличающийся тем, что упомянутое шифрование упомянутой информации о покупателе включает также следующие этапы:

a) подключение упомянутого покупателя к упомянутой проверяющей организации с помощью первого компьютеризованного устройства;

b) считывание идентификаторов технических устройств с упомянутого первого компьютеризованного устройства;

c) включение упомянутых идентификаторов технических устройств в упомянутый поток шифрованных данных и

d) повторение этапов a)-c) для дополнительных компьютеризованных устройств, которые упомянутый покупатель желает использовать в какой-либо торговой сделке.

8. Способ по п.7, отличающийся тем, что передача упомянутого потока шифрованных данных от упомянутого покупателя упомянутой торговой организации включает также

приблизительное время передачи упомянутого потока шифрованных данных упомянутой торговой организации, при этом перед фактической передачей упомянутого потока шифрованных данных упомянутой торговой организации в упомянутый поток шифрованных данных включается второй набор идентификаторов технических устройств и метка времени и даты из компьютеризованного устройства, осуществляющего упомянутую фактическую передачу; и

прикрепление незашифрованного идентификатора маршрутизации к упомянутому потоку шифрованных данных.

9. Способ по п.6, отличающийся тем, что упомянутая проверка личных данных и упомянутая авторизация платежей подтверждает упомянутой торговой организации фактическое наличие упомянутого покупателя в упомянутой торговой сделке, при этом упомянутая торговая организация получает гарантию в том, что она осуществляет торговую сделку ни с кем иным, кроме упомянутого покупателя, и упомянутый идентификатор сделки позволяет упомянутой торговой организации передать сделку на обработку по определению наличия подписи.

10. Способ по п.6, отличающийся тем, что использование упомянутых перекрестных ссылок включает проверку содержания необходимых результатов проверки информации в упомянутом потоке шифрованных данных перед осуществлением упомянутой проверки личных данных и авторизации платежей.

11. Способ для обеспечения безопасной торговой сделки в компьютерной сети, который включает

шифрование информации о покупателе в потоке шифрованных данных, при этом упомянутая информация о покупателе включает по крайней мере один из следующих идентификаторов: идентификатор имени, идентификатор возраста покупателя, идентификатор адреса и идентификатор договора с покупателем;

передачу упомянутого потока шифрованных данных от покупателя торговой организации при осуществлении торговой сделки по приобретению электронного продукта;

маршрутизацию упомянутого потока шифрованных данных в проверяющую организацию;

создание упомянутой проверяющей организацией уникального идентификатора сделки на основе упомянутого потока шифрованных данных;

передачу упомянутой проверяющей организацией уникального идентификатора сделки упомянутой торговой организации, при этом упомянутый поток шифрованных данных и упомянутый уникальный идентификатор сделки лишены персональной информации по платежам упомянутого покупателя;

добавление упомянутого потока шифрованных данных упомянутой торговой организацией к упомянутому приобретенному продукту с целью создания персонифицированного электронного продукта;

поставку упомянутой торговой организацией упомянутому покупателю упомянутого электронного продукта при условии, что каждый персонифицированный электронный продукт, поставляемый различным покупателям, отличается уникальностью своего потока шифрованных данных.

12. Способ по п.11, отличающийся тем, что упомянутое шифрование упомянутой информации о покупателе включает также следующие этапы:

a) подключение упомянутого покупателя к упомянутой проверяющей организации с помощью первого компьютеризованного устройства;

b) считывание идентификаторов технических устройств с упомянутого первого компьютеризованного устройства;

c) включение упомянутых идентификаторов технических устройств в упомянутый поток шифрованных данных и

d) повторение этапов a)-c) для дополнительных компьютеризованных устройств, которые упомянутый покупатель желает использовать в какой-либо торговой сделке.

13. Способ по п.12, отличающийся тем, что передача упомянутого потока шифрованных данных от упомянутого покупателя упомянутой торговой организации включает также

приблизительное время передачи упомянутого потока шифрованных данных упомянутой торговой организации, при этом перед фактической передачей упомянутого потока шифрованных данных упомянутой торговой организации в упомянутый поток шифрованных данных включается второй набор идентификаторов технических устройств и метка времени и даты из компьютеризованного устройства, осуществляющего упомянутую фактическую передачу; и

прикрепление незашифрованного идентификатора маршрутизации к упомянутому потоку шифрованных данных.

14. Способ по п.11, отличающийся тем, что упомянутая проверка личных данных и упомянутая авторизация платежей подтверждает упомянутой торговой организации фактическое наличие упомянутого покупателя в упомянутой торговой сделке, при этом упомянутая торговая организация получает гарантию в том, что она осуществляет торговую сделку ни с кем иным, кроме упомянутого покупателя, и упомянутый идентификатор сделки позволяет упомянутой торговой организации передать сделку на обработку по определению наличия подписи.

15. Способ по п.11, отличающийся тем, что упомянутая уникальность каждого потока шифрованных данных позволяет идентифицировать источник неавторизованных копий упомянутого приобретенного электронного продукта с помощью упомянутой проверяющей организации.

16. Способ для обеспечения безопасной торговой сделки в компьютерной сети, который включает

шифрование информации о покупателе в потоке шифрованных данных, при этом упомянутая информация о покупателе включает идентификатор договора с покупателем;

передачу упомянутого потока шифрованных данных от покупателя торговой организации при осуществлении торговой сделки, при этом под торговой сделкой понимается как приобретение товаров, так и оказание услуг;

маршрутизацию упомянутого потока шифрованных данных в проверяющую организацию;

осуществление упомянутой проверяющей организацией проверки личных данных и авторизации платежей на основе упомянутого потока шифрованных данных и

передачу упомянутой проверяющей организацией упомянутой торговой организации по крайней мере одного результата упомянутой проверки личных данных и упомянутой авторизации платежей, при этом упомянутый поток шифрованных данных, упомянутые результаты проверки личных данных и упомянутая авторизация платежей лишены персональной информации по платежам упомянутого покупателя.

17. Способ по п.16, отличающийся тем, что упомянутое шифрование упомянутой информации о покупателе включает также следующие этапы:

a) подключение упомянутого покупателя к упомянутой проверяющей организации с помощью первого компьютеризованного устройства;

b) считывание идентификаторов технических устройств с упомянутого первого компьютеризованного устройства;

c) включение упомянутых идентификаторов технических устройств в упомянутый поток шифрованных данных и

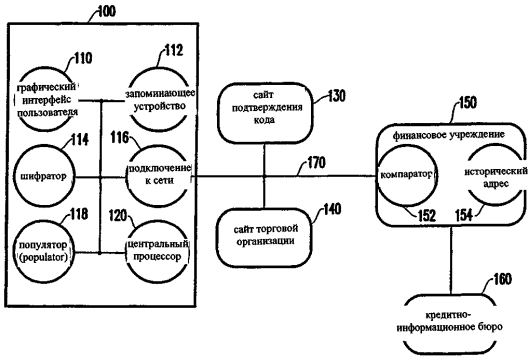
d) повторение этапов a)-c) для дополнительных компьютеризованных устройств, которые упомянутый покупатель желает использовать в какой-либо торговой сделке.

18. Способ по п.17, отличающийся тем, что передача упомянутого потока шифрованных данных от упомянутого покупателя упомянутой торговой организации включает также

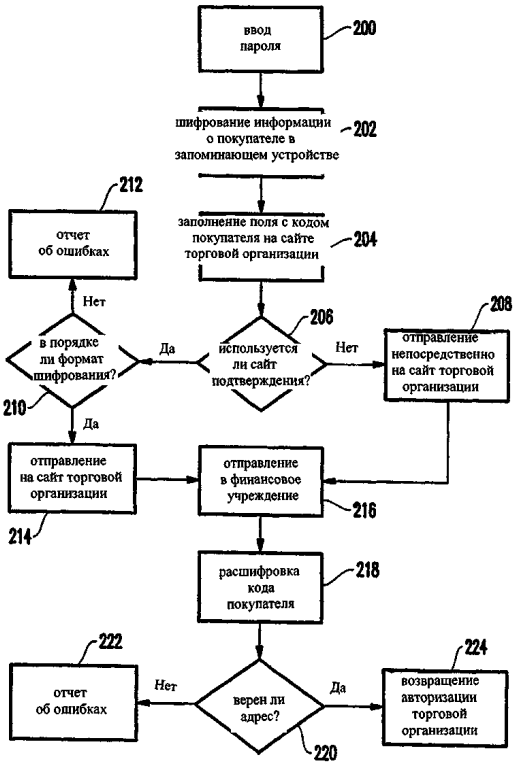
приблизительное время передачи упомянутого потока шифрованных данных упомянутой торговой организации, при этом перед фактической передачей упомянутого потока шифрованных данных упомянутой торговой организации в упомянутый поток шифрованных данных включается второй набор идентификаторов технических устройств и метка времени и даты из компьютеризованного устройства, осуществляющего упомянутую фактическую передачу; и

прикрепление незашифрованного идентификатора маршрутизации к упомянутому потоку шифрованных данных.

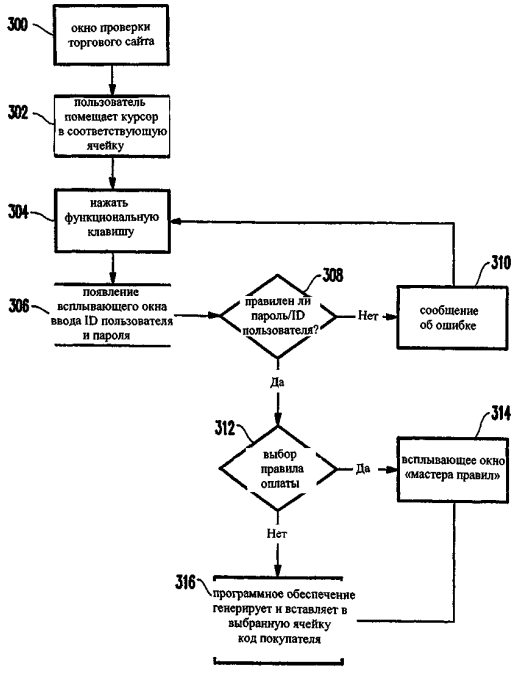
19. Способ по п.16, отличающийся тем, что упомянутая проверка личных данных и авторизации платежей подтверждает упомянутой торговой организации фактическое наличие упомянутого покупателя в упомянутой торговой сделке, при этом упомянутая торговая организация получает гарантию в том, что она осуществляет торговую сделку ни с кем иным, кроме упомянутого покупателя, и упомянутый идентификатор сделки позволяет упомянутой торговой организации передать сделку на обработку по определению наличия подписи.



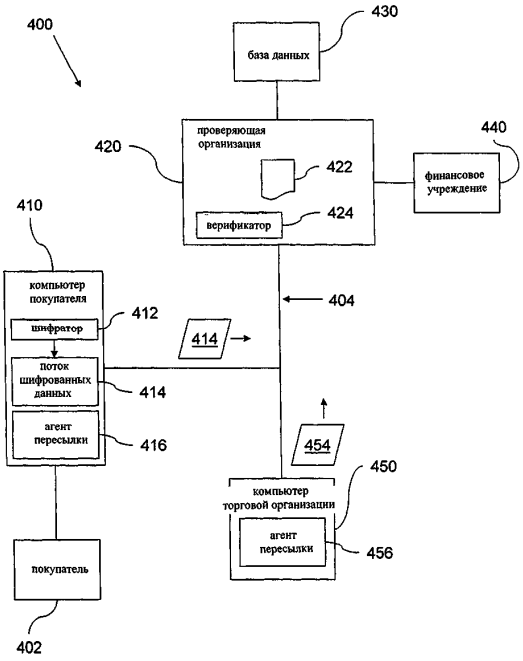
Фиг. 1


ввод пароля
200
шифрование информации о покупателе в запоминающем устройстве
202
заполнение поля с кодом покупателя на сайте торговой организации
204
используется ли сайт подтверждения?
206
Да
Нет
отправление непосредственно на сайт торговой организации
208
в порядке ли формат шифрования?
210
Нет
Да
отчет об ошибках
212
отправление на сайт торговой организации
214
отправление в финансовое учреждение
216
расшифровка кода покупателя
218
верен ли адрес?
220
Нет
Да
отчет об ошибках
222
возвращение авторизации торговой организации
224

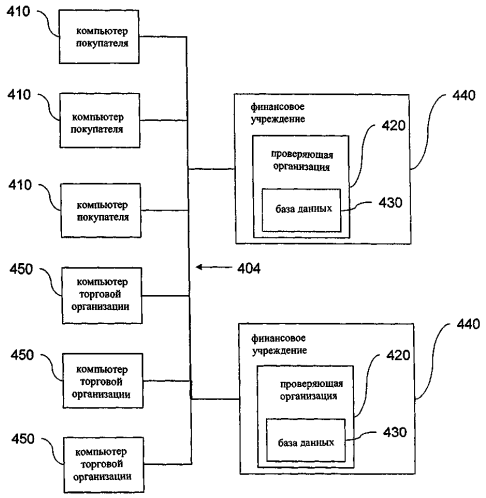
Фиг. 2


окно проверки торгового сайта
300
пользователь помещает курсор в соответствующую ячейку
302
нажать функциональную клавишу
304
появление всплывающего окна ввода ID пользователя и пароля
306
правилен ли пароль/ID пользователя?
308
Нет
сообщение об ошибке
310
Да
выбор правила оплаты
312
Да
всплывающее окно «мастера правил»
314
Нет
программное обеспечение генерирует и вставляет в выбранную ячейку код покупателя
316

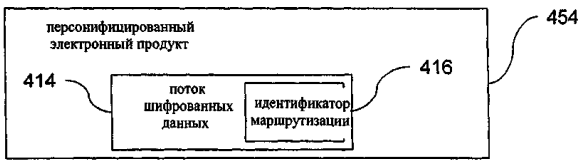
Фиг. 3



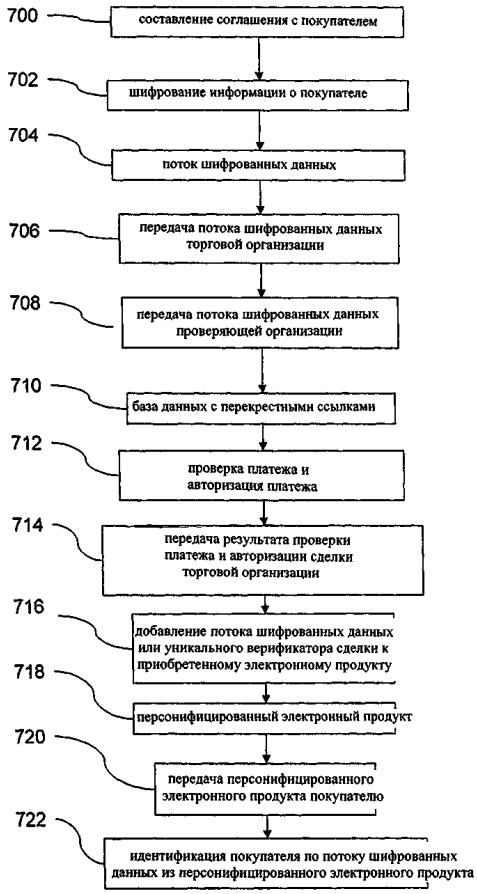
Фиг. 4



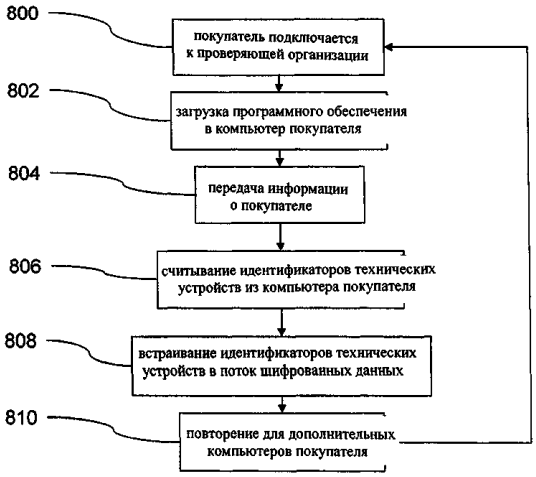
Фиг. 5



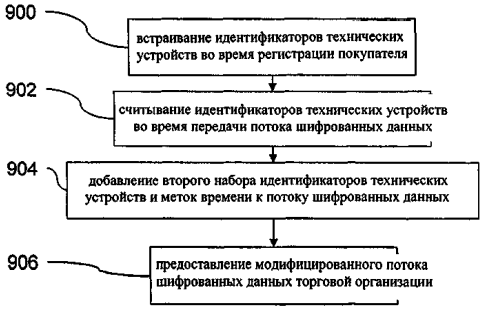
Фиг. 6



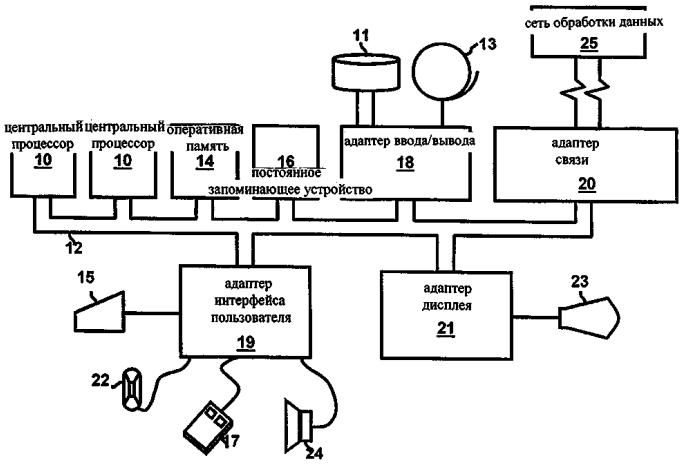
Фиг. 7



Фиг. 8



Фиг. 9


сеть обработки данных
25
11
13
центральный процессор
10
центральный процессор
10
оперативная память
14
16
постоянное запоминающее устройство
адаптер ввода/вывода
18
адаптер связи
20
12
15
адаптер интерфейса пользователя
19
адаптер дисплея
21
23
22
17
24

Фиг. 10