РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 252 451** (13) **C2**

(51) МПК[7] **G 06 F 17/60**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2002105505/09, 30.08.2000**

(24) Дата начала действия патента: **30.08.2000**

(30) Приоритет: **31.08.1999 (пп.1-4, 13-42)**
US 60/151,880
15.11.1999 (пп.5-12) US 60/165,577

(43) Дата публикации заявки: **10.09.2003**

(45) Опубликовано: **20.05.2005 Бюл. № 14**

(56) Список документов, цитированных в отчете о поиске: **EP 0917120 A, 19.05.1999. US 5534857 A, 09.07.1996. WO 99/21321 A, 29.04.1999. US 5832212 A, 03.11.1998. RU 2094846 C1, 27.10.1997.**

(85) Дата перевода заявки PCT на национальную фазу: **27.02.2002**

(86) Заявка PCT:
US 00/23817 (30.08.2000)

(87) Публикация PCT:
WO 01/16900 (08.03.2001)

Адрес для переписки:
127055, Москва, а/я 11, пат.пов. Н.К.Попеленскому

(72) Автор(ы):
БЕННЕТ Рассел (US),
БИШОП Фред (US),
ГЛЕЙЗЕР Эллиот (US),
ГОРГОЛ Зиг (US),
ДЖОНСОН Майкл (US),
ДЖОНСТОУН Дэвид (US),
ЛЕЙК Уолтер Д. (US),
РОЙЭР Коби (US),
СВИФТ Ник (GB),
СИМКИН Марвин (US),
УАЙТ Дерк (US),
ХОЛ Уильям Г. (US)

(73) Патентообладатель(ли):
Американ Экспресс Тревл Рилейтед Сервисиз Компани, Инк. (US)

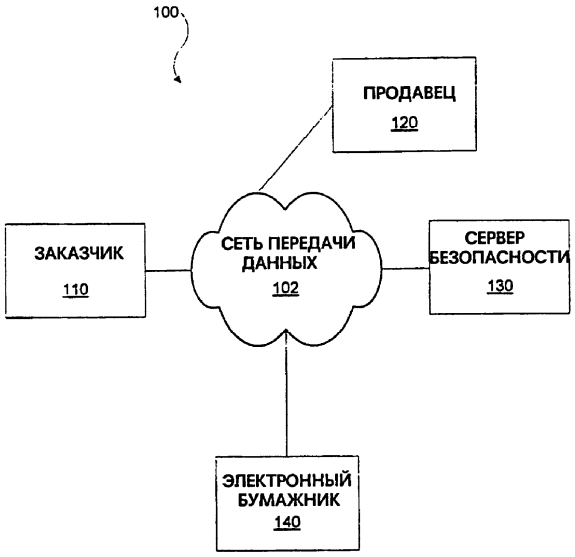
RU 2252451 C2

(54) СПОСОБ ПРОВЕДЕНИЯ ТРАНСАКЦИЙ, КОМПЬЮТЕРИЗОВАННЫЙ СПОСОБ ЗАЩИТЫ СЕТЕВОГО СЕРВЕРА, ТРАНСАКЦИОННАЯ СИСТЕМА, СЕРВЕР ЭЛЕКТРОННОГО БУМАЖНИКА, КОМПЬЮТЕРИЗОВАННЫЙ СПОСОБ ВЫПОЛНЕНИЯ ОНЛАЙНОВЫХ ПОКУПОК (ВАРИАНТЫ) И КОМПЬЮТЕРИЗОВАННЫЙ СПОСОБ КОНТРОЛЯ ДОСТУПА

(57) Реферат:

Изобретение относится в основном к способам и устройствам для проведения сетевых трансакций и может быть использовано в системах для авторизации и ведения бизнеса в сетях, таких как Интернет. Его использование позволяет получить технический результат в виде повышения надежности и достоверности при совершении сетевых электронных сделок. Технический результат достигается за счет того, что сначала осуществляют получение запроса на трансакцию от пользователя к серверу, выдают отклик пользователю, получают от пользователя ответ, основанный на упомянутом отклике, после чего осуществляют обработку упомянутого ответа и проверку пользователя. Затем составляют удостоверения на трансакцию, содержащие по крайней мере один ключ, и передают пользователю по крайней мере часть упомянутых удостоверений. Далее получают повторный запрос от пользователя, который содержит упомянутую часть удостоверений, и осуществляют проверку упомянутой части удостоверений упомянутым ключом для обеспечения доступа к трансакционной службе. 7 н. и 35 з.п. ф-лы, 16 ил.

RU 2252451 C2



Фиг.1

RU 2252451 C2

RU 2252451 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 252 451** (13) **C2**

(51) Int. Cl.[7] **G 06 F 17/60**

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2002105505/09, 30.08.2000**

(24) Effective date for property rights: **30.08.2000**

(30) Priority: **31.08.1999 (cl.1-4, 13-42) US 60/151,880**
15.11.1999 (cl.5-12) US 60/165,577

(43) Application published: **10.09.2003**

(45) Date of publication: **20.05.2005 Bull. 14**

(85) Commencement of national phase: **27.02.2002**

(86) PCT application:
US 00/23817 (30.08.2000)

(87) PCT publication:
WO 01/16900 (08.03.2001)

Mail address:
127055, Moskva, a/ja 11, pat.pov.
N.K.Popelenskomu

(72) Inventor(s):
BENNET Rassel (US),
BIShOP Fred (US),
GLEJZER Ehlliot (US),
GORGOL Zig (US),
DZhONSON Majkl (US),
DZhONSTOUN Dehvid (US),
LEJK Uolter D. (US),
ROJEhR Kobi (US),
SVIFT Nik (GB),
SIMKIN Marvin (US),
UAJT Derk (US),
KhOL Uil'jam G. (US)

(73) Proprietor(s):
Amerikan Ehkspress Trevl Rilejted Servisiz Kompani, Ink. (US)

RU 2252451 C2

(54) METHOD FOR PERFORMING TRANSACTIONS, COMPUTERIZED METHOD FOR NETWORK SERVER PROTECTION, TRANSACTION SYSTEM, ELECTRONIC WALLET SERVER, COMPUTERIZED ONLINE SHOPPING METHOD (VARIANTS) AND COMPUTERIZED ACCESS CONTROL METHOD

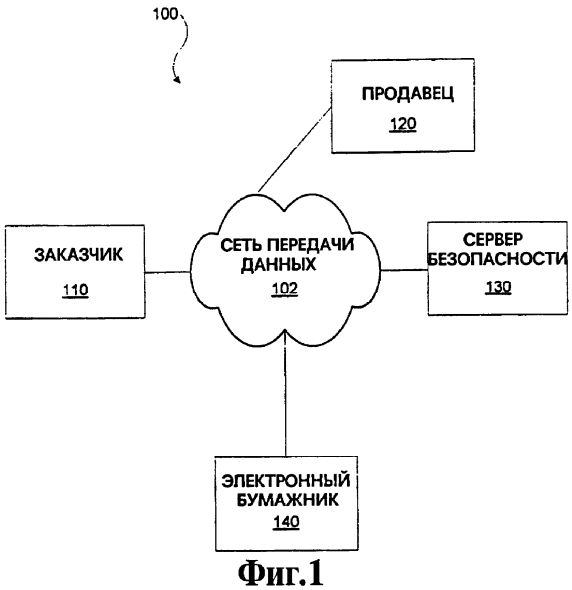
(57) Abstract:

FIELD: electronic financial transactions.

SUBSTANCE: method includes receiving request for transaction from user to server, generating response to user, receiving answer from user, based on response, after that said response is processed and user is checked. Then transaction authentications are performed, using at least one key, and at least portion of said authentication documents are sent to user. Then repeated query from user is received, which has portion of authentication documents mentioned above, and it is checked by said key to provide access to transaction service.

EFFECT: higher reliability and trustworthiness.

7 cl, 16 dwg



Фиг.1

RU 2252451 C2

Область техники, к которой относится изобретение

Данное изобретение в основном относится к способам и устройствам для проведения сетевых трансакций. В частности, данное изобретение относится к системам для авторизации и ведения бизнеса в сетях, таких как Интернет.

Уровень техники

За последние годы многие потребители осознали удобство и практичность приобретения товаров и услуг электронным способом. Доступно много способов осуществления электронной покупки (обычно называемых "е-коммерцией"), таких как телепрограммы "магазин на диване", звонок в ответ на телевизионную рекламу и им подобные. Но в последнее время прямые покупки по Интернет стали особенно популярны.

Начиная Интернет-трансакцию, покупатель обычно находит товары и/или услуги, просматривая онлайновые объявления, например такие как HTML-страницы, через браузер (средство навигации и просмотра) Всемирной Паутины (WWW). Платеж обычно осуществляется с помощью номера платежной карточки, который передается по безопасному каналу, такому как соединение с помощью слоя защищенных сокетов (SSL - Secure Sockets Layer), устанавливаемому между покупателем и продавцом. Номер платежной карточки - это обычно шестнадцатизначный номер кредитной карточки. Номера кредитных карточек обычно соответствуют стандартному формату, когда имеется четыре числа, разделяемые пробелами "0000 0000 0000 0000". Первые пять - семь цифр зарезервированы для целей обработки и идентифицируют банк-эмитент, тип карточки и т.д. Последняя, шестнадцатая, цифра используется как контрольная сумма этого шестнадцатиразрядного числа. Средние восемь - десять цифр используются для однозначной идентификации заказчика. Продавец затем обрабатывает номер платежной карточки, например, получая прямую авторизацию от эмитента карточки, после чего продавец совершает трансакцию (деловые операции, коммерческие сделки и т.п.). Стандарт SSL описан в документе "SSL протокол версии 3.0", от 18 ноября 1996 г., доступном в Интернет по адресу http://home.netscape.com/eng/ssl3/draft302.txt, ссылка на который приводится здесь для справок.

Хотя в Интернет ежедневно совершаются миллионы трансакций, обычная SSL трансакция часто обнаруживает некоторые уже выявленные недостатки. Несмотря на то что протокол SSL обычно обеспечивает безопасное соединение типа "от точки к точке" и оно не дает недобросовестным третьим лицам подслушивать и выманивать или добывать другими способами номера чужих карточек, этот протокол не дает полной уверенности в том, что номер платежной карточки сам по себе правильный или что личность, предоставившая данный номер, имеет на это законное право. Из-за большой вероятности подделки при проведении трансакций через сеть Интернет (Интернет-трансакции) большинство эмитентов платежных карточек взимают за Интернет-трансакции типа "(сама) карточка отсутствует" повышенные комиссионные. Иначе говоря, из-за повышенного риска трансакции типа "карточка отсутствует" облагаются почти всеми эмитентами карточек повышенными комиссионными для авторизации, чем если бы в руках продавца оказалась сама карточка.

Для того чтобы повысить безопасность, сниженную как следствие передачи номера платежной карточки по небезопасным сетям, многие предлагали использовать смарт-карточки (чип-карточки). Смарт-карточка обычно имеет встроенный микропроцессор и память для хранения данных прямо в карточке. Эти данные могут быть, например, криптографическим ключом или электронным бумажником (кошельком), в котором записано количество имеющейся валюты. Предлагалось множество очень искусных схем, но они обычно имели один бросающийся в глаза недостаток, тот, что они все нестандартные. Другими словами, продавцы для обслуживания смарт-карточек в своих web-магазинах обычно должны были бы приобретать дополнительное, заказное программное обеспечение. Более того, и по сей день стоимость администрирования смарт-карточек, включающая запись и поддержку криптографической информации, чрезмерна.

Предполагалось, что стандарт Безопасных Электронных Трансакций (SET - Secure

Electronic Transaction) улучшит ситуацию с безопасностью Интернет-трансакций посредством различных криптографических технологий. И хотя стандарт SET действительно улучшал безопасность по сравнению с трансакциями по стандарту SSL, сложность администрирования, включающая работу со множеством открытых и закрытых ключей, что требовалось для проведения трансакции, ограничила широкое применение SET. Стандарт SET также требовал приобретения продавцами, желающими работать по SET, специального программного обеспечения.

Существующая технология цифрового электронного бумажника, такая как цифровой электронный бумажник, предоставляемый, например, фирмой GlobeSet Inc. (1250 Capital of Texas Highway South, Building One, Suite 300, Austin, TX, 78746 (США)), дает возможность покупателям использовать разные изделия для карточных трансакций (такие как кредитные, платежные, дебитовые, смарт-карточки, номера расчетных счетов и им подобные) для того, чтобы платить за товары и онлайновые услуги (т.е. в режиме реального масштаба времени). В основном цифровой электронный бумажник - это инструмент, с помощью которого запоминается персональная информация (имя, адрес, номер платежной карточки, номер кредитной карточки и т.д.) для того, чтобы осуществлять электронную коммерцию или другое сетевое взаимодействие. Персональная информация может запоминаться на основном сервере или на стороне заказчика/пользователя (персональном компьютере или смарт-карточке) или сразу на и основном и пользовательском серверах. Основной сервер электронного бумажника состоит из web-сервера и сервера базы данных, который централизованно хранит персональную информацию о покупателе и информацию о кредитной карточке, его покупательских преференциях и профиле его онлайновых покупок (совершаемых в реальном масштабе времени).

Цифровой электронный бумажник главным образом осуществляет такие функции, как обслуживание однократного ввода логина и пароля, автозаполнения форм списка покупаемых товаров, одно- или двухкликовую покупку, персонализацию web-сайтов, отслеживание онлайнового заказа и доставки, подробный электронный чек, а также специальные предложения и акции, основанные на предыдущих покупках и выборе данного покупателя. Чаще всего используемая однокликовая покупка и активирует электронный бумажник, и подтверждает факт покупки сразу. Двухкликовая покупка сначала активирует электронный бумажник, затем вторым кликом подтверждается покупка.

Практически покупатель щелкает по ссылке на электронный бумажник и устанавливается SSL сессия с сервером электронного бумажника. Исполняется некий плагин браузера и покупатель таким образом дает свой логин-пароль или смарт-карточку для авторизации и получает доступ к содержимому электронного бумажника. При осуществлении покупки в онлайновом магазине соответствующая информация передается от сервера электронного бумажника web-серверу продавца.

Таким образом, понятно, что нужна новая система проведения электронных трансакций. Эта система должна улучшить ситуацию с безопасностью, одновременно не доставляя больших хлопот покупателям и продавцам. Кроме того, такая система должна хорошо интегрироваться с разными существующими системами электронных бумажников и другими услугами от различных поставщиков.

Сущность изобретения

В представленных примерах реализации данного изобретения пользователю предоставляют средство идентификации, такое как смарт-карточка, которое может быть использовано при проведении электронных трансакций. Это средство идентификации содержит цифровой сертификат и соответствующим образом авторизуется сетевым сервером, который осуществляет полностью или частично запрошенную пользователем трансакцию. Здесь пользователем является покупатель (заказчик), который инициирует трансакцию покупки, а сервер является сервером электронного бумажника, который в свою очередь взаимодействует с сервером безопасности для того, чтобы и придать новое качество надежности и приватности этой трансакции.

Электронные трансакции, такие как трансакции электронных покупок, осуществляются как получение на сервере запроса на трансакцию от пользователя, выдача отклика пользователю, получение от пользователя соответствующего ответа именно на этот отклик, обработка ответа для проверки инструмента трансакции, получение соответствующих удостоверений, включающих хотя бы один ключ для электронной трансакции, передача пользователю хотя бы части этих удостоверений, получение повторного запроса от пользователя, который включает в себя часть удостоверений, проверка действительности этих полученных частей удостоверений ключом для обеспечения доступа к трансакционной службе.

Кроме описанного способа проведения трансакций в данном изобретении предлагается компьютеризованный способ защиты сетевого сервера от его возможного использования в качестве базы для атак на сетевого клиента, в котором сначала осуществляют получение сетевым сервером запроса на соединение от сетевого клиента и сканирование части сетевого сервера на наличие спецсимволов, ассоциированных с протоколом, затем осуществляют проверку на отсутствие спецсимволов в любом ответе сетевого сервера сетевому клиенту и направляют ответ от сетевого сервера сетевому клиенту. Защита сетевого сервера от атак может осуществляться посредством ограничения доступа к сетевому серверу только доступом к той части сервера сети, которая по крайней мере обслуживает выбранный протокол, а также ограничивая возможность сканирования этой части сервера сети на спецсимволы выбранного протокола. Спецсимволы могут быть удалены или заменены обычными символами для целей уменьшения риска, связанного с особенностями выбранного протокола. Упомянутый протокол предпочтительно включает в себя элементы, написанные на языке JavaScript. Предпочтительно, чтобы сканируемые символы запоминались в системном журнале (лог файле) для целей создания журнала безопасности (лога безопасности). Лог безопасности может регулярно просматриваться для определения потенциально ненадежных спецсимволов. Некоторые запросы могут быть отклонены. Такая защита сетевого сервера может осуществляться во время трансакции электронной покупки, осуществляемой посредством электронного бумажника.

Данное изобретение также включает в себя инструмент проведения трансакции, такой как электронный бумажник, используемый для трансакций покупок и имеющий активатор и панель инструментов. Лучше, если такая панель инструментов будет иметь кнопку для загрузки пользователем небольшого активатора, и будет использовать элементы управления операционной системы, например системную панель. Такой инструмент проведения трансакции также включает в себя компоненту автозаполнения форм и компоненту автозапоминания для автозаполнения форм информацией, ранее введенной пользователем.

В изобретении также представлена трансакционная система для обеспечения проведения финансовых трансакций по запросу пользователя, работающего на пользовательском компьютере, подключенном к сети передачи данных. Система содержит авторизатор трансакции и сервер безопасности, сконфигурированный с возможностью проверки наличия средства идентификации в распоряжении пользователя и предоставления цифрового удостоверения упомянутому пользовательскому компьютеру в случае успешной проверки, причем авторизатор трансакции сконфигурирован с возможностью авторизации запроса пользователя на трансакцию на основе по крайней мере части упомянутых цифровых удостоверений, полученных пользовательским компьютером посредством сети передачи данных.

В предпочтительных вариантах выполнения система может содержать инструментальный сервер трансакции или сервер электронного бумажника, связанный с пользовательским компьютером посредством упомянутой сети передачи данных. Причем упомянутый сервер электронного бумажника может быть сконфигурирован с возможностью получения запроса на трансакцию от упомянутого пользовательского компьютера, связи с компьютерной системой продавца и передачи информации об упомянутом пользователе упомянутой компьютерной системе продавца. При этом компьютер пользователя содержит

инструмент проведения трансакции, являющийся клиентом электронного бумажника, и считывающее устройство, сконфигурированное с возможностью передачи информации между инструментом проведения трансакции и средством идентификации.

Средством идентификации может являться смарт-карточка. Предпочтительно, если сервер безопасности и авторизатор трансакции имеют между собой соединение передачи данных, изолированное от сети передачи данных, и инструмент проведения трансакции и сервер безопасности имеют между собой соединение передачи данных, изолированное от упомянутой сети передачи данных.

Средство идентификации может содержать цифровой сертификат однозначной идентификации пользователя данного средства идентификации. В частности, система содержит персональный идентификатор пользователя упомянутого средства идентификации для открытия ему доступа к цифровому сертификату.

Система также может включать в себя эмитент средства идентификации, а трансакция является трансакцией типа "карточка присутствует", установленной эмитентом средства идентификации.

В изобретении также предлагается сервер электронного бумажника для обеспечения проведения трансакций через цифровую сеть, который содержит интерфейс цифровой сети и приложение электронного бумажника, имеющее связь с базой данных, причем сервер электронного бумажника сконфигурирован с возможностью получения запроса на трансакцию от клиента электронного бумажника, обработки удостоверения от упомянутого клиента электронного бумажника для идентификации пользователя клиента электронного бумажника, выборки информации о пользователе из базы данных после идентификации упомянутого пользователя и совершения упомянутой трансакции от имени упомянутого пользователя с использованием упомянутой информации о пользователе.

В предпочтительных вариантах осуществления удостоверение содержит набор произвольных данных с цифровой подписью средства идентификации, находящегося в распоряжении упомянутого пользователя. При этом клиент электронного бумажника снабжен упомянутым набором произвольных данных посредством сервера безопасности.

Сервер может содержать формы продавца, заполненные информацией об упомянутом пользователе при совершении упомянутой трансакции от имени пользователя.

В изобретении далее предлагается компьютеризованный способ выполнения онлайновых покупок, в котором осуществляют авторизацию посредством сервера безопасности, получают удостоверения от упомянутого сервера безопасности, затем идентифицируют адрес продавца, откуда совершается покупка, передают упомянутые удостоверения на сервер электронного бумажника для авторизации упомянутого пользователя на сервере электронного бумажника, а после успешной авторизации на сервере электронного бумажника переадресовывают сообщения с упомянутым адресом продавца на упомянутый сервер электронного бумажника и направляют информацию об упомянутом пользователе от сервера электронного бумажника на адрес продавца, после чего получают информацию о результатах упомянутой покупки.

В другом варианте компьютеризованного способа выполнения онлайновых покупок осуществляют получение на сервер запроса от пользователя на трансакцию, который включает в себя адрес продавца и удостоверение, затем осуществляют проверку упомянутого удостоверения для идентификации пользователя, а по результатам упомянутой проверки осуществляют выборку пользовательской информации из базы данных, после чего заполняют онлайновые формы в соответствии с адресом продавца и выдают упомянутому пользователю информацию о результатах покупки.

В предпочтительных вариантах осуществления изобретения сервер безопасности объединяют с сервером. Цифровую подпись выполняют посредством смарт-карточки.

Кроме того, в изобретении предлагается компьютеризованный способ контроля доступа к службе, в котором сначала получают от пользователя запрос на вход, проверяют наличие у пользователя средства идентификации, после получения успешного результата проверки выдают удостоверение упомянутому пользователю, затем получают от

пользователя запрос на трансакцию, который включает в себя по крайней мере часть упомянутого удостоверения, и осуществляют обработку упомянутой части удостоверения для обеспечения доступа к упомянутой службе.

В предпочтительных вариантах осуществления изобретения упомянутую проверку осуществляют посредством запроса-ответа, которые содержат произвольные данные из средства идентификации, в частности цифровую подпись упомянутых произвольных данных. Упомянутая служба может быть представлена службой финансовой трансакции.

Перечень фигур чертежей и иных материалов

Вышеупомянутые и другие достоинства настоящего изобретения подробно раскрыты ниже в описании примеров его реализации с прилагаемыми чертежами, на которых одноименные элементы на соответствующих модулях имеют одинаковые цифровые обозначения.

Фиг.1-3 - схемы разных примеров реализации трансакционной системы.

Фиг.4 - блок-схема примера системы обслуживания покупателя.

Фиг.5 - блок-схема примера системы безопасности.

Фиг.6 - блок-схема примера электронного бумажника.

Фиг.7-10 - виды примеров экранных форм системы электронного бумажника, сформированные в соответствии с настоящим изобретением.

Фиг.11 - блок-схема алгоритма примера процесса обработки, выполняемого типовым приложением-активатором.

Фиг.12 - карта последовательности сообщений, применяемых во время процесса входа в систему.

Фиг.13 - карта последовательности сообщений, применяемых во время процесса покупки.

Фиг.14 - карта последовательности сообщений, иллюстрирующая потенциальную возможность возникновения проблем с безопасностью, присущую многим языкам написания скриптов.

Фиг.15 - карта последовательности сообщений нормального хода обмена данными без возникновения проблем с безопасностью, упомянутых в Фиг.14, и

Фиг.16 - блок-схема алгоритма примера процесса уменьшения объема ненужного исполняемого кода.

Сведения, подтверждающие возможность осуществления изобретения

Настоящее изобретение описано ниже как совокупность функциональных блоков и различных ступеней обработки. Благодаря этому такие функциональные блоки могут быть реализованы с помощью любого оборудования и/или программного обеспечения, сконфигурированного для выполнения указанных функций. Например, в настоящем изобретении могут быть задействованы различные компоненты на интегральных схемах (ИС), такие как логические элементы, хэш-таблицы, а также им подобные, и они могут выполнять различные функции под управлением одного или нескольких микропроцессоров или других устройств управления. Аналогично элементы программного обеспечения для целей настоящего изобретения могут быть реализованы на любом языке программирования или скриптов, таких как C, C++, JAVA, COBOL, Ассемблер, PERL и им подобным, с различными алгоритмами, реализуемыми на любых комбинациях структур данных, объектов, процессов, подпрограмм или других программных элементов.

Более того, необходимо отметить, что в настоящем изобретении могут быть задействованы любые технологии общего применения для передачи данных, запросов, обработки данных, управление взаимодействием и им подобных. И еще, данное изобретение может быть использовано для обнаружения и компенсации брешей в безопасности, возникающих при использовании языков написания скриптов, таких как JavaScript, VBScript и им подобных.

Необходимо отметить, что приведенная и описанная здесь конкретная форма реализации изобретения дана с целью наилучшего раскрытия данного изобретения и ни коим образом не ограничивает объем его притязаний. Действительно, для краткости мы не

можем дать в деталях сведения о традиционных способах обмена данными, разработке приложений и других функциональных аспектов составляющих его систем (и также составных частей используемых операционных компонентов). Более того, линии соединений, показанные на прилагаемых фигурах, представляют собой типичные функциональные взаимосвязи и/или физическую стыковку между различными элементами. Необходимо отметить, что в реальной системе электронных трансакций может присутствовать множество временных или дополнительных взаимосвязей или физических соединений.

Для целей упрощения описания примера реализации данное изобретение часто описывается как система электронной коммерции для применения в Интернет. Однако необходимо отметить, что можно дать множество применений настоящему изобретению. Например, эта система может быть использована для авторизации пользователей компьютерной системы, или для активации системы защиты паролем, или для любых других целей. Точно так же данное изобретение может использоваться совместно с любым типом персонального компьютера, сетевого компьютера, рабочей станции, ми ни компьютера, мэйнфрейма, и им подобным, под любой версией любой операционной системы, такой как Windows, Windows NT, Windows2000, Windows 98, Windows 95, MacOs, OS/2, BeOS, Linux, Unix и им подобным. Более того, хотя данное изобретение часто описывается здесь, как реализуемое на базе коммуникационного протокола TCP/IP, необходимо понимать, что данное изобретение так же могло бы быть реализовано и с использованием IPX, Appletalk, IP-6, NetBIOS, OSI или любого количества существующих или разработанных в будущем протоколов.

Далее, в качестве покупателя и продавца могут выступать конкретные люди, а также объекты, предприятия, в то время как под банком можно понимать любых эмитентов карточек, таких как компании-эмитенты карточек, компании-спонсоры карточек, или эмитенты, действующие по договору с финансовыми организациями. Платежная сеть может включать в себя уже существующие сети, которые на данный момент обслуживают трансакции по кредитным карточкам, дебетовым карточкам или финансовым/банковским карточкам других типов. Такая платежная сеть является закрытой сетью, что подразумевает, что она защищена от утечек информации, например, как в сети Американ Экспресс (American Express®), сети Визанет (VisaNet®) или Верифоун (Veriphone®).

Вдобавок, на некоторых фазах трансакции могут подключаться другие участники, такие как посреднические организации, однако эти участники на схемах не показываются. Для осуществления трансакции каждый ее участник оборудуется персональным компьютером. У покупателя есть персональный компьютер, у продавца есть компьютер или сервер, и банк имеет компьютер типа мэйнфрейма; однако любой из компьютеров может быть миниЭВМ, сервером на базе персонального компьютера, сетью компьютеров, лаптопов (дорожный компьютер), ноутбуков, карманных компьютеров, сеттопов или им подобных.

Теперь обратимся к фиг.1, трансакционная система 100 (для проведения трансакций) включает в себя по крайней мере один пользовательский компьютер 110, авторизатор трансакции, в частности компьютер (продавца) 120 авторизации трансакции, сервер 130 безопасности и дополнительный сервер 140 обслуживания трансакции. В некоторых реализациях изобретения, подробно здесь описанных, трансакционная система 100 используется для электронной коммерции, чтобы осуществлять трансакции покупки. Конкретнее, пользовательский компьютер 110 есть компьютер покупателя или заказчика (пользователя), компьютер 120 авторизации трансакции есть компьютер продавца, и сервер 140 обслуживания трансакции есть сервер электронного бумажника. Нужно отметить, что хотя трансакционная система, описанная здесь является системой электронной коммерции, настоящее изобретение равным образом может быть пригодно и для различных других трансакционных систем.

Некоторые компьютерные системы и серверы связаны между собой соответствующей цифровой сетью 102 передачи данных, которая может быть такой сетью, как Интернет, или другой общедоступной сетью. Эти сети могут включать АТС, интранет предприятий или

учебных заведений и им подобные. В некоторых реализациях изобретения, одна из которых показана на Фиг.2, компьютер продавца имеет электронную связь с сервером безопасности с

помощью отдельного соединения передачи данных, изолированного от сети 102. Точно так же в некоторых реализациях имеется канал 150, соединяющий сервер электронного бумажника 140 с сервером 130 безопасности, который идет отдельно от сети 102. В качестве каналов 150 и 152 могут использоваться такие каналы, как телефон, цифровая сеть связи с комплексными услугами (ISDN), выделенный канал по T1 или другие каналы передачи данных, такие как радиоканал и им подобные. Необходимо отметить, что канал 150 и канал 152 могут быть идентичными каналами, или в некоторых реализациях изобретения один может коренным образом отличаться от другого.

Некоторые варианты реализации изобретения, как показанные на Фиг.3, также включают сервер 160 приложений (прикладных программ). В некоторых реализациях база данных (не показана) и/или профиль-сервер (не показан) могут взаимодействовать с сервером 160 приложений и/или сервером электронного бумажника 140. Сервер 160 приложений может использоваться для равномерного распределения вычислительной нагрузки. Распределение нагрузки между электронным бумажником 140 и сервером 160 приложений может повысить эффективность и/или безопасность. Например, сервер 160 приложений может выполнять некоторые функции, выполняемые сервером электронного бумажника 140, такой как доступ к базе данных. Поскольку сервер 160 приложений не связан напрямую с сетью передачи данных 102, выполнение доступа к базе данных с сервера 160 приложений, а не с электронного бумажника 140 может повысить безопасность.

Необходимо отметить, что на хотя Фиг.1-3 проиллюстрированы некоторые примеры реализации изобретения, также возможно создание и других вариантов реализаций. Например, изобретение может включать канал 150 и не включать канал 152 и наоборот. Более того, компоненты (такие как покупатель (заказчик) 110, продавец 120, сервер 130 безопасности, сервер электронного бумажника 140 и сервер 160 приложений) могут быть и индивидуальными компьютерами, и рабочими группами сетей или компьютеров, целенаправленно взаимодействующими так, чтобы выполнить функции, описанные здесь. Функциональный вклад отдельной компоненты может быть распределен между одним или несколькими компьютерами так, чтобы реализовывалась описанная функциональность. Например, сервер электронного бумажника фактически может быть совокупностью web-серверов, серверов приложений и других типов серверов.

Для проведения трансакции покупатель 110 соответствующим образом устанавливает соединение посредством сети 102 с продавцом 120. Когда покупка уже должна быть совершена, покупатель обращается к серверу электронного бумажника 140. Покупатель затем перенаправляется серверу 130 безопасности для того, чтобы провести проверку того факта, что покупатель действительно является собственником смарт-карточки. Смарт-карточка может иметь цифровой сертификат, который однозначно идентифицирует карточку, например, создавая цифровое удостоверение в контексте текущей трансакции, как это описано ниже. В некоторых реализациях изобретения части цифрового удостоверения возвращаются покупателю 110, а другие части передаются на сервер электронного бумажника 140 посредством канала 150 безопасного соединения. Покупатель 110 может затем использовать цифровые удостоверения для того, чтобы авторизоваться на сервере электронного бумажника 140, который в свою очередь уже может совершить электронную трансакцию согласно полномочиям, полученным от покупателя 110. Сервер электронного бумажника 140 может включать функции для заполнения форм, заданных компьютером продавца 120. Когда продавец 120 получает идентификатор средства безопасной покупки от покупателя 110 или от сервера электронного бумажника 140, авторизация карточки может проводиться по каналу 152 так же, как и обычная авторизация платежной карточки. Согласно описанному выше передача данных может проводиться с использованием различных протоколов, например SSL или VPN и им подобных. Ввиду того что смарт-карточка содержит в себе идентификационную

информацию, которая однозначна для конкретной карточки и которую считывают и передают по сетям только электронным способом, трансакция покупки с использованием смарт-карточек является более безопасной, чем трансакция с использованием обычной платежной или кредитной карточки. Для трансакций с таким уровнем безопасности могут быть установлены более низкие комиссионные, и они могут обрабатываться как трансакции типа "карточка присутствует". Кроме того, если такая трансакция является трансакцией типа "карточка присутствует", то ответственность по риску подделки можно переложить с продавца на эмитента карточки.

Обратимся к Фиг.4, на которой типовой компьютер покупателя 110 (который также может называться компьютером заказчика или пользователя) представляет собой любую компьютерную систему, которая способна начать электронную трансакцию по сети 102. В некоторых реализациях изобретения компьютер покупателя 110 является персональным компьютером под управлением любой операционной системы 212, такой как любая версия операционной системы Windows от компании Microsoft, г. Редмонд Штат Вашингтон, США, или любой версии операционной системы MacOS от компании Apple, г. Купертино, штат Калифорния, США.

Компьютер покупателя 110 соответственно имеет программное и/или аппаратное обеспечение для обработки средства идентификации, в частности смарт-карточки 202, через интерфейс web-браузера 216 под управлением операционной системы 212. Web-браузер 216 - это программа, совместимая с компьютером 110, с помощью которой он общается по сети, как, например, программа Netscape Communicator от компании Netscape, г. Маунтин-Вью, Калифорния, США, или Internet Explorer от компании Microsoft, г. Редмонд Штат Вашингтон, США, или браузер AOL от компании America Online из г. Дьюллз, штат Вирджиния, США. В некоторых реализациях на компьютер покупателя 110 установлен инструмент проведения трансакции, например клиент 214 электронного бумажника, который является какой-либо компьютерной программой, способной взаимодействовать с сервером электронного бумажника. Типовым клиентом электронного бумажника является программа Microsoft Wallet или программа Globeset Wallet от компании Globeset, г. Остин, штат Техас, США, впрочем может использоваться любая программа.

Клиент 214 электронного бумажника и браузер 216 могут взаимодействовать с смарт-карточкой 202 посредством передачи данных считывающему устройству (терминалу) для обработки смарт-карточек под управлением операционной системы 212. Считывающим устройством 204 для обработки смарт-карточек является любое устройство считывания карточек, способное передавать информацию между клиентом 214 электронного бумажника и смарт-карточкой 202. В некоторых реализациях в качестве такого считывающего устройства использовался считыватель модели GCR410 от компании Gemplus, г. Редвуд-Сити, штат Калифорния, США, совместимый со стандартом ISO-7816, или любое другое подходящее считывающее устройство.

В качестве смарт-карточки 202 может использоваться любая, с помощью которой можно осуществлять электронные трансакции, например, любая смарт-карточка, выполненная в соответствии со следующими стандартами ISO, упомянутыми здесь как справочный материал:

ISO/IEC 7816-1:1998 Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 1: Физические характеристики.

ISO/IEC 7816-2:1999 Информационные технологии - Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 2: Размеры и расположение контактных площадок.

ISO/IEC 7816-3:1997 Информационные технологии - Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 3: Электронные сигналы и протоколы передачи данных.

ISO/IEC 7816-4:1995 Информационные технологии - Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 4: Система команд для межотраслевой передачи данных.

ISO/IEC 7816-5:1994 Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 5: Система присвоения номеров и процедура регистрации идентификаторов запросов.

ISO/IEC 7816-5:1996 Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 6: Элементы данных для межотраслевого обмена; и

ISO/IEC 7816-5:1994 Идентификационные карточки - Карточки на микросхемах с контактными площадками - Часть 7: Команды для межотраслевого обмена данными языка структурированных запросов данных из платежных карточек (SCQL).

Типовая смарт-карточка 202 - смарт-карточка, выполненная в соответствии со спецификацией ISO 7816, такой может быть и карточка на микросхеме SLE66, производимой компанией Infineon, г. Мюнхен, Германия. Микросхема SLE66 имеет встроенную память (такую, как память 16К, однако может использоваться и память большего или меньшего объема) и процессор под управлением операционной системы, например Multos (такой, как Multos v.4). Для некоторых реализаций изобретения под смарт-карточкой 202 также понимается и апплет (прикладные программы на языке "Джава" (JAVA)) для выполнения функций запоминания и обработки цифровых сертификатов и других криптографических функций. Для ознакомления с основами криптографии см. "Прикладная криптография: протоколы, алгоритмы и исходники на С", автор Брюс Шнайдер, издательство John Wiley & Sons (второе издание 1996 г.), ссылка на эту книгу дается здесь в качестве справочного материала. Например JAVA апплет X.509 может включаться в состав смарт-карточки для обработки сертификатов X.509, которые в нее будут записываться. И хотя в реализациях изобретения, описанных здесь, упоминаются смарт-карточки, необходимо отметить, что могут использоваться и другие средства идентификации, например, мобильный телефон системы глобальных телекоммуникаций GSM может заменять смарт-карточки в некоторых реализациях данного изобретения.

Теперь обратимся к Фиг.5. Сервер 130 безопасности соответствующим образом реализует взаимодействие с сетью 102, а модуль 304 безопасности и сервер 306 авторизации взаимодействуют с базой данных 310. Интерфейс 302 сети есть любая программа, которая может осуществлять взаимодействие с сетью 102, например, такая, как web-сервер. В некоторых реализациях интерфейс 302 сети может базироваться на программе Netscape Enterprise Server от корпорации Netscape, г. Маунтин-Вью, штат Калифорния, США. Интерфейс 302 сети получает электронные сообщения от сети 102 и направляет их соответствующим образом модулю 304 безопасности или серверу 306 авторизации.

Модуль 304 безопасности и сервер 306 авторизации могут быть разделены брандмауэром 308 (аппаратно-программные средства межсетевой защиты), который управляет данными, передаваемыми между сервером 130 безопасности и покупателем 110 или сервером электронного бумажника 140. Брандмауэр 308 может представлять собой любое устройство или программу управления (например, роутер управления доступом), способные ограничивать поток данных между внешней и внутренней сетью (не показаны). В некоторых реализациях изобретения модуль 304 безопасности соответствующим образом располагается вне брандмауэра для того, чтобы управлять передачей данных между сервером 130 безопасности и покупателем 110 или сервером электронного бумажника 140. Сервер 306 авторизации охраняет ценную конфиденциальную информацию, такую как база данных 310, которая может содержать перекрестные ссылки сертификатов X.509, хранимых в различных смарт-карточках 202, обслуживающих всю систему 100, позволяя поддерживать ее и в сети Интернет при хорошем уровне безопасности. Нужно понимать, что функции модуля 304 безопасности и сервера 306 авторизации могут быть соответствующим образом объединены или разделены в рамках настоящего изобретения.

Теперь обратимся к Фиг.6. Приведенный в качестве примера сервер 140 электронного бумажника включает в себя сетевой интерфейс 402, дополнительный сервер 404 апплетов и приложение 406 электронного бумажника. Сетевой интерфейс 402 является любой

программой, позволяющей осуществлять сетевое взаимодействие в сети 102, такой как web-сервер. В некоторых реализациях сетевой интерфейс 402 базируется на программе Netscape Enterprise Server от корпорации Netscape, г. Маунтин-Вью, штат Калифорния, США. Дополнительный сервер 404 апплетов реализует серверную часть функций программ распределенной обработки, таких как программы на JAVA или элементы управления ActiveX. Типовой сервер апплетов - это программа Java Applet Server от компании Sun Microsystems из г. Маунтин Вью, Калифорния. Сервер 404 апплетов и сетевой интерфейс 402 поддерживают функции приложения 406 электронного бумажника, который может включать обработку логина, получение данных из базы данных электронного бумажника 408 и/или управлять трансакциями, как это описано здесь. В некоторых реализациях настоящего изобретения сервер электронного бумажника 140 может включать в себя программу SERVERWALLET (другое наименование NETWALLET) от компании Globeset, г. Остин, штат Техас, США.

Некоторые реализации настоящего изобретения могут включать в себя приложение-активатор, которое соответствующим образом помогает покупателю совершить процесс покупки с помощью электронного бумажника. Приложение-активатор может представлять информацию в виде строки состояния, к примеру, или может само запускать программу-клиент 214 электронного бумажника (Фиг.4), когда это необходимо. К тому же активатор может поддерживать локальные кэш-сайты, обслуживаемые электронным бумажником.

Приложение-активатор может быть реализовано как обычное компьютерное приложение. В некоторых реализациях приложение-активатор выдает информацию на системную панель, как "плавающий битмэп", или другим подходящим способом. Графическое представление (т.е. иконки) может давать информацию о состоянии, такую как "зона поддерживаемого сайта", "зона поддерживаемой страницы авторизации", "зона поддерживаемой страницы оплаты", "нет открытых окон", "зона неподдерживаемой страницы" и/или подобную.

Плавающий битмэп может быть реализован как графический файл любого формата, например файл формата графического обмена (GIF). В различных вариантах реализации изобретения информация может отображаться в графическом, аудио, видео, аудио-видео, мультимедиа, анимационном и других форматах. Более того, файлы GIF могут быть заменены на файлы типа LZW, TIFF, анимированный GIF, JPEG, MPEG или любые другие типы графических, аудио или мультимедиа форматов или файлов.

В основном настоящее изобретение усовершенствовано путем оснащения средства проведения трансакции окном, в котором есть элементы управления, делающие это средство проведения трансакции проще в использовании. Средство проведения трансакции может быть использовано для различных электронных трансакций. Например, трансакций покупки, трансакций финансового консалтинга, трансакций оформления страховки, трансакций типа покупатель-покупатель в случаях с бартерными сделками, трансакций, относящихся к ответу на коммерческие предложения или с выдачей вознаграждений и других. Инструмент проведения трансакций, описанный здесь, является электронным бумажником, использующимся для трансакций покупки. Функционал электронного бумажника расширен путем включения в него функций окна с элементами управления для того, чтобы пользователю было проще пользоваться электронным бумажником. В основном настоящее изобретение включает в себя функции доступа к электронному бумажнику в виде реализации его на стороне заказчика, и серверную панель инструментов (тулбар), позволяющие пользователю при малых объемах загружаемого активатора использовать элементы управления интерфейса пользователя операционной системы, таких, например, как системная панель Microsoft Windows.

Активатор является объектным кодом, который выполняется на компьютере пользователя и имеет подпрограммы доступа к серверу электронного бумажника. Такой активатор может генерировать события и имеет процедурную логику, позволяющую общаться с электронным бумажником, реагируя на определенные пользовательские и системные действия или события. Обычно активатор представлен одним единственным

графическим элементом, например иконкой, которая в случае реализации под операционной системой Microsoft Windows будет находиться на системной панели и которая позволяет пользователю включать или выключать видимость тулбара электронного бумажника. В действительности в различных реализациях тулбар электронного бумажника является особым окном браузера, через которое имеется доступ к серверу электронного бумажника. Активатор взаимодействует с сервером электронного бумажника так, чтобы автоматизировать обновление объектного кода активатора путем загрузки его с сервера малыми порциями. Обычно перед началом загрузки у пользователя запрашивается подтверждение. В некоторых реализациях активатор взаимодействует не только с электронным бумажником, но и с другими приложениями типа коммерческих предложений или выдачи вознаграждений. Система поддерживает ряд важных опций для каждой своей web-страницы, скажем, динамическую и контекстную информацию, которая является специфичной для каждой страницы, просматриваемой пользователем. И активатор следит за просматриваемым унифицированным указателем информационного ресурса (URL), настраиваясь на просматриваемую страницу так, чтобы пользователь имел информацию о предоставляемых ему возможностях. Например, активатор может проверить, просматривает ли пользователь торговый сайт и предоставляемые ему в настоящий момент спецпредложения (скидки и т.п.). Активатор также может следить за версиями программного обеспечения на компьютере пользователя с тем, чтобы напоминать ему о возможном появлении более новых версий. Варианты реализации изобретения могут выполняться на любых сетях, таких как глобальные, локальные, Интернет, или на любых персональных компьютерах, устройствах радиосвязи и им подобных устройствах. Система может быть реализована под любой операционной системой, такой как Microsoft Windows, Mac OS, Linux, Windows CE, Palm OS и других.

Такой активатор, который предпочтительно реализуется на стороне заказчика, позволяет пользователю 110 быть в постоянном или прерываемом взаимодействии с компанией, хранящей электронный бумажник 140, например Американ Экспресс, без необходимости занимать место под лишние окна на экране пользовательского терминала. Как уже упоминалось, он позволяет компании, хранящей электронный бумажник, отслеживать и показывать пользователю потенциально интересные ему в текущий момент данные. Такие конфигурируемые средства управления позволяют покупателю быстро находить нужные web-сайты и немедленно запускать нужные функции, такие как авторизация цифровой платежной карточки. Клиентский тулбар предпочтительно может быть в основном реализован в виде отдельного окна, связанного с окном пользовательского браузера, и оно может поддерживать такую геометрию, чтобы создавалось впечатление, что оно является частью браузера пользователя. С одной лишь разницей, скажем, когда пользователь щелкает по его элементам управления, оно остается неизменным, в то время как в основное окно загружается нужный URL для выполнения указанного действия (такого как обращение к электронному бумажнику). Например, когда пользователь щелкнул по иконке электронного бумажника на системной панели, на экране в отдельном окне появляется тулбар 502 электронного бумажника 205, который связан с окном основного браузера 500, как это показано на Фиг.7. В другом варианте реализации тулбар заказчика расположен на рамке окна конкретного электронного бумажника, предоставляя в распоряжение пользователя дополнительные элементы управления, как это описано выше, в дополнительной области окна этого электронного бумажника, расширяющей основное окно. В третьем варианте реализации эта область разбросана по основному окну пользовательского браузера, для того чтобы использовать ее для электронного бумажника и других элементов управления, описанных выше.

Такая система дает удобный способ покупателям не только посещать избранные ими URL, но еще и запускать определенные функции, что может быть многоступенчатым и даже изменяющимся процессом, поскольку сайты продавцов постоянно обновляются. Такая система позволяет упростить жизнь пользователю, не только делая работу с электронным

бумажником и коммерческими сайтами проще, но и еще позволяя проще находить сам электронный бумажник и тулбар заказчика. Когда у пользователя много открытых окон, поиск окна электронного бумажника может стать затруднительным, особенно если учесть, что различные окна браузера могут захватывать фокус ввода в процессе навигации по сайтам и общения с ними. Таким образом, использование системной панели и серверного функционала есть самое лучшее сочетание для работы пользователя. В предпочтительном варианте реализации данная система может работать с любым известным браузером, например таким, как Netscape Navigator.

В то время как ранее созданные системы могли только представлять собой настраиваемый портал (например, My American Express. corm), который дает пользователю возможность посетить страницу и затем перейти по ссылке с этой страницы, предпочтительный вариант реализации настоящего изобретения дает возможность с удобством пользоваться окном с элементами управления, которое остается на экране пользователей, в то время как они путешествуют по web. К тому же тулбар заказчика позволяет автоматизировать действия пользователя, и это при том, что такие действия могут иметь место на коммерческом сайте третьей стороны. Более того, ранее созданные системы могли использовать отдельное окно браузера для отображения элементов управления электронным бумажником, в то время как настоящее изобретение использует обычное окно браузера, разделенное на части так, чтобы предоставить место, занимаемое самим электронным бумажником. Например, в предпочтительном варианте реализации изобретения имеется иконка электронного бумажника, доступная пользователю на системной панели (не показана). После щелчка по этой иконке на экране появляется тулбар 502 электронного бумажника, как это показано на Фиг.7. Присутствие этого тулбара не является навязчивым, одновременно позволяя пользователю работать с электронным бумажником. Тулбар 502 предпочтительно интегрирован в окно браузера 500.

Как показано на Фиг.8, когда пользователь нажмет кнопку торгового каталога на тулбаре 502, тулбар развернется и превратится в страницу торгового каталога 602. Пользователь может выбрать продавца в списке продавцов 604, расположенном здесь же на странице торгового каталога 602. После выбора продавца из списка продавцов 604 электронный бумажник переносит пользователя на сайт 702 продавца, выбранного пользователем, как это показано на Фиг.9. Обычно, когда электронный бумажник уже перенес пользователя на сайт 702 продавца, тулбар 502 принимает свои обычные размеры. Когда пользователь сделает покупку у продавца, например, поместив выбранное в корзину и начав оформление покупки, в настоящем изобретении само оформление покупки частично производится самим электронным бумажником. Как показано на Фиг.10, когда пользователь определится с нужной покупкой на сайте 702 продавца, на экран выдается интерфейс (окно) 802 оформления покупки. К примеру, интерфейс 802 оформления покупки выдается на одну сторону экрана браузера, а окно магазина продолжает оставаться на другой стороне экрана браузера. Большая часть информации, которую пользователь должен ввести для оформления покупки (например, имя, адрес, E-mail, информация о кредитной карточке и т.д.), уже была введена в электронный бумажник и сама появляется в окне 802 оформления покупки электронного бумажника. В предпочтительном варианте реализации изобретения пользователь может редактировать эту информацию.

В предпочтительном варианте настоящая система включает также способы и аппаратуру, наилучшим образом позволяющие надежно заполнять HTML-формы Web-сайтов. В конечном итоге пользователи могут сами определять содержание информации, которую они в основном хотят давать на сайты, независимо от их внешнего вида, маркировки и поведения. В предпочтительном варианте реализации настоящее изобретение включает в себя компоненту "автозапоминания", которая позволяет запоминать уже введенную информацию, и компоненту "автозаполнения", которая включает в себя совокупность мощных средств обработки, полученных путем анализа моделей поведения пользователей и сайтов.

Настоящее изобретение собирает информацию от пользователей, сохраняя ее надежно и безопасно на сервере, и затем распределяет ее по нужным полям форм под контролем пользователя. Система поддерживает привязку пользовательской информации к различным полям HTML-форм сайтов, представляющих интерес для пользователя. Такая информация затем используется для управления заполнением (или автозаполнением) HTML-форм теми пользователями, которые хотят взаимодействовать с этими сайтами.

Что касается функции "автозапоминания", и прежние варианты реализации электронного бумажника могли иметь функцию запоминания, но она должна была включаться пользователем. В настоящем варианте реализации "автозапоминания" пользователю не нужно ничего нажимать для запоминания формы, которую они только что заполнили, так как данная система сама запоминает поля, которые пользователи вводят в окне магазина. Когда форма отсылается (например, нажатием кнопки "Отправить" или "Купить"), электронный бумажник реагирует путем определения, является ли окно, запросившее отсылку формы, окном сайта нужного продавца. Если да, в таком случае электронный бумажник запоминает данные соответствующим образом, в противном случае он может запретить отсылку формы и продолжит нормальную работу. Среди элементов управления электронного бумажника может быть кнопка с надписью "Запомнить", или он может поддерживать опцию автоматического запоминания, которая может быть постоянно включена. Предпочтительно запоминаются все поля, кроме тех, которые используются для автозаполнения. В этом контексте ясно, что, когда пользователь вводит данные в определенное поле, это значение будет сохранено в системе. Компонента электронного бумажника определит значения поля, введенные таким способом, и безопасно передаст их на сервер через Интернет. Когда пользователь в следующий раз посетит эту страницу, электронный бумажник, в дополнении к автозаполнению полей формы, которые берутся из системы, будет также заполнять форму значениями, которые ранее запоминались. При обработке формы (автозаполнение) электронный бумажник безопасным образом считает значения с сервера.

В частности, что касается браузера Internet Explorer, то в данном изобретении соответствующим образом реализован элемент управления ActiveX, который сам подсоединяется в web-странице, такой, например как American Express Online Wallet. В предпочтительном варианте реализации этот элемент управления ActiveX имеет метод, который перехватывает события браузера во всех браузерах Internet Explorer, и поэтому American Express Online Wallet может по необходимости реагировать на эти события посредством функции JavaScript, загруженной в составе страницы American Express Online Wallet, позволяя таким образом получить полный документ в браузер Internet Explorer. Эта особенность позволяет системе перехватывать событие "Документ Завершен", инициируемое браузером Internet Explorer, которое означает окончание загрузки документа. Когда это событие перехвачено, элемент управления ActiveX уведомляет об этом страницу American Express Online Wallet путем вызова JavaScript функции, загруженной в составе страницы American Express Online Wallet. Эта функция отвечает на событие посредством соответствующего взаимодействия с элементом управления ActiveX для того, чтобы перехватить событие "Отправка Формы" для всех форм всех окон браузера Internet Explorer.

Когда пользователь заполнит форму на web-странице и щелкнет на кнопке "Отправить" (или любом элементе управления, таком как кнопка, отправляющая форму), страница American Express Online Wallet получает уведомление от элемента управления ActiveX путем вызова JavaScript функции, загруженной в составе страницы American Express Online Wallet.

Страница American Express Online Wallet затем соответствующим образом определяет, является ли документ, инициировавший событие "Отправить", нужным документом, посредством проверки URL - окна, которое инициировало это событие. Если событие нужно обрабатывать, тогда страница American Express Online Wallet должна вызвать функцию элемента управления ActiveX, которая в свою очередь считывает объектную модель

документа (DOM - document object model), который инициировал событие. Затем DOM просматривается и можно получить значения форм для последующей передачи их на сервер для запоминания. В предпочтительном варианте реализации элемент управления ActiveX обязан должным образом прекращать перехват событий браузера и событий "Отправка Формы" для того, чтобы уменьшить количество сбоев во время выполнения алгоритма.

Что же касается браузера Netscape, из-за особенностей реализации модели событий в Netscape система перехватывает события только из функций JavaScript. Если системе удастся получить привилегии уровня "Разрешить запись из браузера" (присваиваемые пользователем), тогда системе удастся выполнить функцию, которая позволяет внешнему окну перехватывать события другого окна. И далее система сможет считать объектную модель документа для всех фреймов данного окна. В процессе выполнения этого система оповещает каждую форму окна о том, что она желает перехватывать событие "Отправить". Таким образом, когда пользователь заполнит форму этого оповещенного системой окна и нажмет кнопку "Отправить" (или любой элемент управления, такой как кнопка, отправляющая форму) на этой странице, электронный бумажник оповещается и реагирует должным образом. Специалисты поймут, что настоящее изобретение может быть реализовано для каждой соответствующей трансакционной системы, включая, но не ограничиваясь любыми системами электронных бумажников.

Что же касается функции заполнения форм, то электронный бумажник, такой, например, как American Express Online Wallet, реализует функции заполнения для того, чтобы помочь пользователям в заполнении форм. Прежние системы, например такие, как поставляемая объединением GlobeSet, обычно использовали объект Помощник браузера (BHO - Browser Helper Object). Концепция с BHO часто имеет тот недостаток, что, например, браузер Internet Explorer 5.0 содержит баг (сбой), при котором загружается только первый BHO, указанный в реестре. Это же является проблемой и для любых приложений таким образом, что невозможно быть уверенным, загружены ли все BHO или нет. Более того, BHO загружаются для каждого экземпляра Internet Explorer, то есть много экземпляров BHO могут работать в какой-то момент времени, занимая память и замедляя просмотр всеми браузерами, а не только нужным.

Настоящее изобретение предпочтительно заменяет решение с BHO путем использования того же элемента управления ActiveX, который упоминался в описании функции "автозапоминания". Присоединяя элемент управления ActiveX к странице электронного бумажника, система соответствующим образом получает объектную модель любого документа, загруженного в любой браузер Internet Explorer, посредством использования, например, функций Shell Windows API. Когда пользователь нажимает кнопку "Заполнить Форму" на странице электронного бумажника, бумажник может реагировать, сначала получая объектную модель документа посредством использования элемента управления ActiveX. Далее, электронный бумажник может сохранять имена полей, составляющих форму, и отсылать их на сервер для эвристической обработки. Сервер ответит на этот запрос путем возврата значений, которые должны быть использованы при заполнении этих полей. Эти поля затем могут быть заполнены с использованием той же объектной модели документа, полученной ранее. Так, настоящее изобретение упрощает проблему ввода повторяющихся данных на формы web-сайтов. В дополнении к удобству заказчиков это увеличивает достоверность вводимых данных.

Если рассматривать более подробно, архитектура настоящего изобретения объединяет серверную модель каждого сайта (т.е. поля, страницы, ссылки и т.п.), серверную модель пользователя (т.е. его профиль), сгенерированную пользователем модель сайта (т.е. запоминание макросов, тэгов разметки, алгоритма перетаскивания), модель сайта, искусственно сгенерированную системой (т.е. наращивание и проверка моделей, сгенерированных пользователями), и эвристически сгенерированную модель сайта (т.е. предположения относительно семантической информации для полей, действий и т.п.). Настоящая система создает и хранит несколько особых типов моделей. Первая

характеризует сайт, например, как Вы оформляете покупку, как Вы добавляете что-то в корзину, как Вы ищете виды товаров, как Вы вводите Ваши преференции (например, в случаях с путешествиями) и т.п. Вторая модель характеризует пользователя, например, какие действия пользователю разрешены и какие имеются атрибуты профиля пользователя. Комбинируя эти две модели, настоящая система создает специальные возможности обработки, которые придают ей гибкость и мощь.

Эта система привязывает модель пользовательских возможностей к модели сайта там, где модели сайта генерируются известными способами. Модель сайта, как таковая, может быть создана пользователем, хостом, эмитентом кредитной карточки и даже провайдером сайта. В предпочтительном варианте реализации изобретения для представления модели сайта используются языки ECML/XML В некоторых вариантах реализации можно обмениваться моделями сайта с другими системами.

Например, пользователь может последовательно посещать сайты различных авиакомпаний и турагентств для того, чтобы купить авиабилеты. Каждый сайт имеет поля на различных экранах для того, чтобы собирать информацию, которая примерно одинакова для разных сайтов. Однако каждый сайт использует разные HTML-формы, которые размещены на различных URL и которые могут меняться время от времени. И хотя информация на разных сайтах по природе своей может быть очень похожей, на настоящее время нет общего механизма автоматизации процесса заполнения полей форм информацией о пользовательских предпочтениях (таких как пожелания о местах, меню обедов, скидках на родственников и т.п.). Каждый сайт может иметь свой профиль максимального запоминания пользовательских предпочтений. И при таком положении вещей один пользователь должен создавать свой профиль на каждом таком сайте отдельно.

В настоящее изобретение включена эвристическая модель распознавания полей. При таком подходе в идентификации нужных полей форм учитывается их пространственное расположение относительно надписей, относящихся к этим полям. Комбинации надписей к полю и HTML-атрибутов поля (особенно атрибут "name" HTML-элементов "input", "select" и "action") будут даны на вход эвристического функционала, который имеет словарь для облегчения идентификации нужных полей.

В другом варианте реализации настоящее изобретение включает в себя распознавание полей с помощью пользователя. При таком подходе пользователь по своей инициативе перехватывает ввод, нажимая кнопку "Запомнить" такого элемента управления, который позволит серверу забрать информацию о последовательности действий, которую выполняет пользователь. Когда пользователь выполняет это, он вполне может "отыграть назад" последовательность действий (похоже на запоминание макроса, применяемое в некоторых программах). Таким образом, появляется возможность подать последовательность действий пользователя в эвристический функционал и также запомнить ее прямо в таблицах разметки, которые используются этим функционалом.

В предпочтительном варианте реализации изобретения два вышеупомянутых подхода требуют некоторого вмешательства пользователя для того, чтобы полностью завершить процесс создания разметки заполнения и разметки расположения полей с целью наиболее полного отражения навигации по сайту и возможностей по заполнению полей, что и делает данное изобретение применимым. Когда это необходимо, живые люди действуют примерно таким же образом, как и алгоритм распознавания полей с помощью пользователя, хотя, конечно, они предоставят намного больше информации об их процессах навигации и заполнения форм, чем усредненный пользователь. Но в любых случаях, та информация, которая собирается, используется для создания карт процессов (или подробных карт сайтов), которые отражают последовательность действий (заполнение форм, HTTP ответ, HTTP запрос и т.п.), с помощью которых и осуществляется работа с сайтом. Также будет сгенерирована карта полей форм для каждой web-страницы карты процесса там, где карта полей определяет точные имена полей, которые могут использоваться для автоматизации отправки форм. Могут также потребоваться карты состояний для того,

чтобы отслеживать состояние пользователя во время взаимодействия с web-сайтом (например, такие состояния пользователя, как вошел в систему или не вошел в систему, будут влиять на результат определенных действий на сайте).

В предпочтительном варианте реализации изобретения процесс взаимодействия с пользователем может быть или полностью автоматизированным (пользователь сообщает о своем желании осуществить записанную в виде скрипта последовательность действий) или во взаимодействии может иметь место участие пользователя (здесь настоящее изобретение может автоматически заполнить поля форм, оставляя пользователю возможность корректировать, менять и заполнять любое поле, которое требует дополнительного ввода данных). В дополнении к известным товарам и услугам настраиваемая технология в виде карт процессов и полей может применяться и для новых товаров и услуг, позволяя предпринимателям облегчить автоматизацию ввода данных от посетителей сайта. Например, если предприниматель составил карты процессов и полей для своих заказчиков (любым способом, описанным выше), он может продавать эту информацию или услуги и товары заказчикам третьей стороны. Сайты, для которых существуют подобные карты, могут также выиграть от этого, поставляя аналогичный сервис и тем заказчикам, которые не имеют доступа к такой системе. Основополагающие процессы сами по себе основаны на системе, которая собирает информацию и преобразует ее, например, в XML или ECML. Эти стандартные представления могут формировать базу обмена информацией для упомянутых товаров и услуг.

Обратимся теперь к Фиг.11. Процесс 900, реализованный в программе-активаторе соответствующим образом, включает в себя инициализацию приложения (шаг 902), проверку универсального указателя ресурса (URL), в то время как пользователь просматривает сайт или делает онлайновой покупки (шаг 904), с определением просматривает ли пользователь поддерживаемый сайт (шаги 908 и 912) и с выдачей соответствующих ответов на шаге 908 и 912 (соответственно). Другие возможности (такие как бонусы, спецпредложения, отслеживание, безопасность и тому подобное) могут быть реализованы на шаге 916.

Шаг 902 инициализации соответствующим образом включает в себя запуск приложения активатора и инициализацию приложения. Приложение активатора может быть инициализировано как результат включения системы в работу, подсоединения к сети (такой как Интернет или локальная сеть) или инициализацией браузера (такого как Internet Explorer от компании Microsoft, г. Редмонд, штат Вашингтон, США или Netscape Navigator от компании Netscape, г. Маунтин-Вью, штат Калифорния, США). В некоторых вариантах реализации приложение-активатор может общаться с сервером 140 электронного бумажника (Фиг.1-3), приложением 406 электронного бумажника (Фиг.6) или с другим сервером сети 102 (сетевым сервером). Приложение-активатор соответствующим образом обращается к удаленному серверу для того, чтобы получить информацию, такую как список web-сайтов, доменных имен или URL, которые поддерживаются электронным бумажником.

Эта информация может получаться на регулярной основе (т.е. ежедневно, ежемесячно или при каждой инициализации программы-агента), или когда последует запрос от приложения-активатора или сервера. В различных вариантах реализации приложение-активатор хранит список поддерживаемых URL в кэше (быстродействующая буферная память), в файле на локальном диске или в памяти пользовательского компьютера.

По мере того как пользователь просматривает Интернет или другую сеть 102 передачи данных, приложение-активатор соответствующим образом отслеживает расположение пользователей в сети. Одним из способов отслеживания пользователя является способ отслеживания URL, используемых браузером пользователя. В таких реализациях приложение-активатор получает текущий URL от браузера пользователя (или от сетевого интерфейса системы соответственно) и сравнивает (шаг 906) текущий URL со списком поддерживаемых URL, полученных от удаленного сервера на шаге 902 инициализации. Такие сравнения показаны на логически выделенных шагах 906, 908, 912 и 916 на Фиг.11,

хотя эти шаги могут быть объединены или разбиты любым образом без потери смысла изобретения. Например, хотя на Фиг.11 показано выполнение многократного сравнения, для некоторых вариантов реализации изобретения достаточно однократного сравнения текущего URL со списком поддерживаемых URL.

Если текущий URL соответствует поддерживаемому URL, то приложение-активатор реагирует соответствующим образом. Например, если на текущем URL есть поддерживаемая страница оформления покупки (да, на шаге 908), тогда приложение-активатор выполняет процесс оформления покупки (шаг 910). Процесс оформления покупки может включать оповещение пользователя о том, что эта страница оформления покупки поддерживается путем выдачи окна сообщения или путем высвечивания определенной иконки на системной панели или в отдельном окне. Если приложение 214, обслуживающее электронный бумажник, еще не запущено, приложение-активатор может выдать окно диалога или другое оповещение пользователя, что эта страница поддерживается приложением 214, обслуживающим электронный бумажник. Такое окно может иметь кнопку или другой механизм, которым пользователь может запустить приложение 214, обслуживающее электронный бумажник.

Если текущий URL соответствует поддерживаемой странице оформления платежа (да, на шаге 912), приложение-активатор может предоставить приложению, обслуживающему электронный бумажник, инструкции по оформлению платежа или другие разрешающие инструкции в отношении приложения, обслуживающего электронный бумажник (шаг 914). Сообщения, циркулирующие между приложением-активатором, приложением, обслуживающим электронный бумажник, браузером и т.п., могут рассылаться с помощью технологий передачи сообщений Open Desktop, связывания и встраивания объектов (OLE - Object Linking and Embedding), вызовов объектных процедур и т.п.

В различных вариантах реализации изобретения функции, описанные выше, осуществляются с помощью cookies (пароль или фрагмент данных об обращении пользователя к серверу), как это описано ниже. Cookies используются для определения достоверного контекста пользователя. Если обнаружен достоверный контекст пользователя, тогда приложение-активатор либо запускает серверное приложение, либо запускает серверный тулбар, который позволит пользователю запустить другие приложения. Например, браузер пользователя может иметь некоторые cookies, которые могут указывать на возможность осуществления покупки или через обычный платеж, или по особой карточке. Активатор может выдать тулбар, который позволит пользователю выбрать нужный платежный инструмент (т.е. обычный платеж или по карточке электронного бумажника пользователя). Необходимо отметить, что доступные приложения не есть обязательно приложения, связанные с трансакциями покупки. В некоторых реализациях контекстная информация запоминается и на сервере и в cookies браузера. Например, cookies могут служить ключом, в соответствии с которым контекстная информация может быть загружена с сервера.

Другие функции (шаг 916) также могут быть включены в приложение-активатор. Например могут быть реализованы механизмы защиты (такие как те, что были описаны выше и еще будут описаны ниже), функции отслеживания заказчика, бонусы, спецпредложения и тому подобные. В случае с бонусами или спецпредложениями активатор может воспринимать текущий URL как относящийся к определенному товару или web-странице. Когда пользователь придет к определенному поддерживаемому URL, приложение-активатор отмечает совпадение и выдает пользователю (через окно диалога, браузер или как еще) спецпредложение, такое как возможность покупки определенного товара или возможность получение скидки при покупке. Необходимо отметить, что в приложение-активатор могут быть включены и другие функции в рамках настоящего изобретения.

В некоторых вариантах реализации настоящего изобретения клиент 214 электронного бумажника (Фиг.4) обеспечивает формы, предварительно заполненные специфичной информацией о покупателе. В соответствии с Фиг.1-3 пользователь может обращаться к

электронному бумажнику через обращение к web-серверу, такому как сервер электронного бумажника 140 сети 102. Для того чтобы воспользоваться электронным бумажником, пользователь заполняет регистрационную форму (которая может быть, например, сгенерирована CGI-скриптом). Сервер электронного бумажника 140 соответствующим образом получает демографическую, банковскую и другую информацию (т.е. адрес, адрес доставки, имя, номер кредитной карточки и т.п.) от сервера 306 авторизации (Фиг.5) или другого сервера частной сети. Эта информация может использоваться для конфигурирования клиента 214 электронного бумажника (Фиг.4), который однозначно закрепляется за каждым пользователем. Одним из способов конфигурирования клиента 214 электронного бумажника является создание конфигурационного файла, который ассоциируется с клиентом 214 и который считывается клиентом 214 для того, чтобы получить информацию для электронного бумажника, как это описано выше.

Регистрационная информация предпочтительно также включает в себя информацию о считывающем устройстве для обработки карточек, которая в свою очередь включает в себя указание на то, к какому порту, последовательному или USB, подключено считывающее устройство. Если пользователь согласен на установку приложения обслуживания электронного бумажника, пользователю устанавливается или поставляется считывающее устройство для обработки кредитных карточек, а также специальный код (такой как криптографический ключ, или пароль, или еще какой код в электронной или печатной форме). Затем пользователь регистрирует себя на сервере электронного бумажника 140 и авторизуется с помощью карточки или специального кода. После ввода специального кода пользователь получает особым образом сконфигурированное программное обеспечение для обслуживания электронного бумажника, которое может быть установлено на пользовательском компьютере 110 соответствующим образом. Процедура предварительного заполнения форм электронного бумажника может быть проведена с помощью любой кредитной или платежной карточки, путем простого ассоциирования версии программы обслуживания электронного бумажника со специальным кодом. Конфигурационная информация определенного пользователя ассоциируется с тем кодом, который был предоставлен этому пользователю, и пользователь впоследствии может использовать специальный код для авторизации себя на сервере электронного бумажника 140 для того получения копии программного обеспечения электронного бумажника, сконфигурированного данными специально для этого пользователя.

На Фиг.1-3 и 12 показано, как заказчик 110 соответствующим образом инициирует трансакцию путем входа на сервер электронного бумажника 140 посредством смарт-карточки 202. Для того чтобы зайти на сервер электронного бумажника 140, заказчик 110, может сначала подсоединиться к серверу 130 безопасности посредством браузера 216. Пользователь выбирает определенный URL для вызова входной страницы посредством обращения к закладке (букмарку), или щелкая по иконке или ссылке, или другим способом. Сервер безопасности может вернуть страницу авторизации посредством интерфейса 302 сети. В некоторых реализациях форма ввода и кнопка отправки пользовательского логина и пароля и гиперссылка авторизации смарт-карточки является частью страницы авторизации. Пользователь выбирает авторизацию смарт-карточки, и браузер 216 соответствующим образом реагирует, посылая сообщение на запрос авторизации 1002 (Фиг.12). Сервер 130 безопасности получает запрос на авторизацию 1002 и инициирует процесс авторизации смарт-карточки, как это необходимо. В некоторых реализациях сервер 130 безопасности формирует криптографический отклик (запрос) серверу 306 авторизации или модулю 304 безопасности в ответ на сообщение запроса на авторизацию 1002. Криптографический отклик 1004 есть сообщение любого рода, лишь бы он препятствовал атакам с повторами (т.е. таким атакам, при которых фальшивые сообщения формируются повторной посылкой ранее посланных пакетов авторизации), например отклик с посылкой произвольных данных, направленный на то, чтобы получить ответ от приложения X.509, хранимого в смарт-карточке 202. Отклик затем направляется в адрес заказчика 110 посредством сети 102 в качестве сообщения-отклика 1004.

По получении сообщения отклика (запроса) 1004, браузер 216 направляет сообщение 1004 клиенту 214 электронного бумажника для обработки смарт-карточкой 202. Если клиент 214 не запущен, то браузер 216 может автоматически запустить эту программу. Клиент 214 электронного бумажника затем соответствующим образом подготавливает ответ-подпись. Например, клиент 214 электронного бумажника может считывать информацию отклика сервера, формировать новый пользовательский запрос (т.е. второй криптографический отклик для смарт-карточки 202), скомбинировать оба отклика в двойной запрос и рассчитать хэш-код двойного запроса для последующего использования, например в криптографическом блоке криптографической системы типа 1 с открытым ключом (Public-Key Cryptography System 1 (PKCS1)). Хэш-код может быть рассчитан в соответствии с любым алгоритмом, таким, например, как MD3 или MD4, и использоваться для того, чтобы гарантировать полностью и точность данных в блоке двойного запроса. Под PKCS понимается криптографический стандарт с общим ключом, определяющий механизмы кодирования и подписи данных, и использованием открытого ключа криптосистемы RSA. Стандарт PKCS полностью определен в документе "PKCS #1: криптографические спецификации RSA версии 2.0" (PKCS #1: RSA Cryptography Specifications Version 2.0), датированном сентябрем 1998 г. (доступным на http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-1.html) и упомянутым здесь в качестве справочного материала.

Блок PKCS1 соответствующим образом доставляется на смарт-карточку 202 на обработку посредством считывающего устройства 204 для обработки карточек (шаг 1006 на Фиг.12). Для того чтобы получить доступ к карточке, в некоторых реализациях считывающее устройство 204 для обработки карточек взаимодействует с пользовательским компьютером, чтобы запросить от пользователя ввод персонального идентификатора, например персональный идентификационный номер (PIN) или другой однозначно определяющий идентификатор. В предпочтительном варианте реализации PIN хранится на самой карточке 202. В других случаях PIN или другой персональный идентификатор может храниться где-либо в системе, например в считывающее устройство 204 для обработки карточек или на компьютере покупателя 110. Пользователь соответствующим образом вводит персональный идентификатор для того, чтобы открыть доступ к смарт-карточке 202, которая получает блок двойного запроса от клиента 214 электронного бумажника и затем проставляет на блок цифровую подпись. В некоторых реализациях смарт-карточка 202 имеет личный ключ, используемый для расчета цифровой подписи для этого блока. Подписанный блок затем возвращается клиенту 214 электронного бумажника. В некоторых реализациях смарт-карточка 202 также обеспечивает сертификат (такой как сертификат X.509), который соответствует личному ключу, используемому для расчета цифровой подписи.

По получении подписи и сертификата от смарт-карточки 202 клиент 214 электронного бумажника соответствующим образом создает необходимое ответное сообщение 1008 для отсылки серверу 130 безопасности. И хотя ответное сообщение 1008 может быть в любом формате, в некоторых реализациях оно форматируется как сообщение PKCS7, как это определено в стандарте "PKCS#7 Стандарта синтаксиса криптографических сообщений. Техническая записка лаборатории RSA, версия 1.5", ("PKCS#7. Cryptographic Message Syntax Standard. An RSA Laboratories Technical Note") версии от 1 ноября 1993 г., доступное на ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-7.doc и полностью введенное в данное описание посредством ссылки.

По получении ответного сообщения 1008 сервер 130 безопасности обрабатывает это сообщение, как это необходимо (шаг 1010 на Фиг.12). В некоторых реализациях ответное сообщение 1008 направляется серверу 306 авторизации, который проверяет сертификат и подпись, полученные от смарт-карточки 202. При успешных верификации сертификата и проверки подписи в некоторых реализациях может быть сгенерировано средство безопасной идентификации, которое возвращается покупателю 110 или на смарт-карточку 202.

В дальнейшем, использование средства безопасной идентификации дает пользователю возможность устанавливать свою подлинность и безопасно работать с электронным бумажником. В некоторых реализациях сервер 306 авторизации может создавать дополнительное средство безопасной идентификации для того, чтобы идентифицировать пользователя. В других реализациях такое средство идентификации может состоять из многих частей, впоследствии привязываемых к соответствующему цифровому сертификату, смарт-карточке или другим данным, возможно, с использованием базы данных 310. В третьих вариантах реализации дополнительное средство идентификации и его части могут быть направлены покупателю (заказчику) 110 в сочетании с сообщением о перенаправлении 1012. В различных вариантах реализации дополнительное средство идентификации может быть направлено заказчику или поддерживаться на сервере 306.

По получении сообщения о перенаправлении 1012 покупатель 110 соответствующим образом соединяется с сервером электронного бумажника 140 и делает запрос на подключение. В некоторых реализациях сообщение 1014 "Запрос на подключение" соответствующим образом включает в себя средство идентификации и, возможно, дополнительное средство безопасной идентификации полностью или частично как составляющее сообщения о перенаправлении 1012. Сервер электронного бумажника 140 запрашивает сервер автоматизации, используя некую комбинацию средств безопасной идентификации полностью или частично так, чтобы осуществить идентификацию покупателя 110. Запрос 1016 и ответ 1018 соответствующим образом передаются через сеть передачи данных (канал) 150, которая в некоторых реализациях поддерживается отделенной от сети 102 для того, чтобы повысить безопасность системы 100. В альтернативных вариантах реализации может быть задействована сеть 102, которая в некоторых реализациях может предоставлять улучшенную безопасность посредством технологий виртуальной частной сети (Virtual Private Network), протокола SSL, использования общих секретных ключей и/или других криптографических средств. Если возвращаемые удостоверения 1018 в порядке, сервер электронного бумажника 140 считывает атрибуты соответствующего покупателя 110 из базы данных электронного бумажника и уведомляет покупателя об успешном входе в систему с помощью сообщения 1020. Необходимо отметить, что возможны и другие варианты реализации процедуры входа в систему. Необходимо также отметить, что для выполнения последовательности входа в систему 1000 могут использоваться любые шифровальные схемы, форматы сообщений и т.п.

Теперь обратимся к Фиг.13. Типовая процедура авторизации, пригодная для использования в торговых трансакциях, инициируется покупателем (пользователем) 110 путем посылки запроса 1102 на трансакцию на сервер электронного бумажника 140 для каждого события (такого как покупка), для которого авторизация необходима. Сервер электронного бумажника соответствующим образом опознает это событие и посылает сообщение-запрос 1104 серверу 130 безопасности, например, через коммуникационный канал 150 для формирования сообщения-запроса. Сервер 306 авторизации (или какой-нибудь другой компонент сервера 130 безопасности) затем формирует отклик 1106 (который может включать рандомизированные данные) и выдает отклик 1106 на сервер электронного бумажника 140 через, например, соединение (канал) 150. Сервер электронного бумажника получает отклик 1106 и направляет информацию отклика браузеру 216 в качестве сообщения-запроса на электронную подпись 1108. Браузер 216 запускает клиент 214 электронного бумажника, если это необходимо, и перенаправляет сообщение-запрос на электронную подпись 1108. В соответствии с описанным выше клиент 214 электронного бумажника формирует блок сообщения-запроса на электронную подпись как блок типа PKCS1 и включает в него запрос серверу, запрос заказчику и хэш-код. Результирующий блок сообщения-запроса на электронную подпись подается на смарт-карточку 202 посредством считывающего устройства 204 для обработки карточек. Смарт-карточка 202 соответствующим образом подписывает этот блок и прописывает копию встроенного в нее сертификата X.509.

Подписанный блок затем может быть возвращен клиенту 214 электронного бумажника, который формирует соответствующее сообщение-ответ на электронную подпись 1110 (такое как сообщение PKCS7) и посылает его серверу электронного бумажника 140. Сервер электронного бумажника 140 затем формирует сообщение о проверке подлинности 1112, которое включает в себя данные из сообщения-ответа на электронную подпись 1110 и средство безопасной идентификации, ассоциированное с покупателем 110 во время процесса входа в систему (такое как для примера процесса входа в систему, показанного на Фиг.10). В других реализациях применяемое средство безопасной идентификации получается от покупателя 110 как часть сообщения-ответа на электронную подпись 1110. Сообщение о проверке подлинности 1112 посылается серверу 130 безопасности через соединение 150. Сервер 130 безопасности может затем соответствующим образом перенаправить сообщение о проверке подлинности серверу 306 авторизации, который может проверить подпись и получить средство безопасной идентификации из базы данных 310 (шаг 1114 на Фиг.13). Это средство безопасной идентификации и/или дополнительный однозначный идентификационный код, полученные из базы данных, затем сравниваются со средством безопасной идентификации или идентификатором, полученным от сервера электронного бумажника 140. Если два этих объекта (т.е. средства безопасной идентификации или идентификаторы) идентичны, то можно заключить, что карточка, которая в настоящее время используется покупателем 110, есть та же карточка, которая использовалась покупателем 110 во время процедуры входа в систему. Затем соответствующее разрешающее или запрещающее сообщение 1116 посылается от сервера 130 безопасности серверу электронного бумажника 140 и трансакция может быть продолжена.

В некоторых вариантах реализации сервер 140 электронного бумажника играет во время трансакций роль прокси-сервера (представителя) покупателя 110. Например, сервер электронного бумажника 140 может заполнять формы заказа от имени покупателя, вводить адрес доставки, номер карточки и т.п. Продавец 120 может затем разрешить трансакцию покупки как трансакцию с обычной расходной карточкой с использованием обычной аппаратуры и программного обеспечения. Но необходимо понимать, однако, что предоставляемая раскрытыми здесь системами дополнительная безопасность позволит иметь большую степень доверия к личности покупателя, таким образом снижая дисконтные ставки на проведение трансакции.

Различные варианты реализации данного изобретения включают в себя дополнительную защиту брешей в системе безопасности. Из-за того что многие серверные функции, реализованные, к примеру, на сервере 130 безопасности или сервере электронного бумажника 140, могут включать в себя различные компоненты, написанные на языках скриптов, таких как JavaScript (в соответствии со спецификациями фирмы Sun Microsystems, г. Маунтин-Вью, штат Калифорния, США) или VBscript (в соответствии со спецификациями фирмы Microsoft, г. Редмонд, штат Вашингтон, США), серверы, подключенные к сети 102, могут предлагать различные функции, реализованные на таких серверных языках программирования, многим заказчикам 110 посредством доставки скриптов (кода) от сервера заказчику. Этот код интерпретируется, компилируется и как-то исполняется пользовательским компьютером 110. В реализациях, задействующих, например, JavaScript, скрипты интерпретируются и исполняются просмотровой программой (такой как Internet Explorer, Netscape Communicator и т.п.), выполняемых на пользовательском компьютере 110. В других вариантах реализации задействованы иные, не совместимые с PC браузеры, например телефоны, работающие по стандарту беспроводного протокола (Wireless Application Protocol, WAP), который поддерживает скрипты языка разметки WML. Многие языки написания скриптов могут иметь команды, объекты или другие механизмы управления данными, например для доступа к файлам на жестком диске пользователя или других манипуляций с данными на компьютере пользователя. Для того чтобы предотвратить получение исполняемого кода из несанкционированных источников, язык скрипта может включать в себя механизм, который

позволит пользователю разрешать скрипты, полученные только из доверенных источников. Например, пользователь, проводящий электронную трансакцию, как это описано выше, может разрешать исполнение скриптов, загруженных с сервера электронного бумажника, но может запрещать исполнение на своем компьютере скриптов, полученных из других источников.

Потенциальная проблема с безопасностью, обнаруживаемая во многих языках скриптов, показана на Фиг.14. Недобросовестный "хакер" может создать web-сайт 1204, который специально предназначен для проведения злонамеренных действий против пользователя законного web-сервера 1206. Хакерский сайт 1204 (обозначенный на фигуре как "преступный web-сервер") может, например, поставить пользователю фрагмент кода, такой как скрипт. Хакерский сайт 1204 может также заставить web-браузер пользователя 216 обратиться к определенному универсальному локатору ресурса (URL) на законном сервере 1206 (таком как сервер электронного бумажника 140 или любой другой сервер сети 102). Запрашиваемый URL может быть хитро переделан так, что законный сервер вернет, например, сообщение об ошибке или другой ответ браузеру 216 пользователя. В некоторых реализациях такой ответ законного сервера может включать в себя части запроса от браузера 216 пользователя или их вариации. Если такой ответ включает в себя JavaScript, VBscript или другой исполняемый код, сгенерированный как результат злонамеренных атак преступного сайта 1204, тогда ясно, что на компьютере пользователя можно исполнять такие коды. Этот пример иллюстрирует одну из многих технологий, благодаря которым "хакер" может заставить законный web-сервер вернуть спровоцированный ответ браузеру пользователя. Так как разные исполняемые системы и скриптовые языки содержат команды для получения доступа к файловой системе, реестру и т.п., понятно, что несанкционированное исполнение такого кода является крайне нежелательным. Тем не менее технология, показанная на Фиг.14, может позволить поставку на компьютер пользователя скрипта или другого кода от преступного сайта 1204. Так как компьютер пользователя считает, что скрипт пришел из надежного источника (т.е. от сервера электронного бумажника), то пользовательский компьютер может исполнять код с преступного сайта, создавая таким образом потенциальную угрозу повреждения или несанкционированного сброса данных, их разрушения и т.п. На Фиг.15 проиллюстрирован корректный порядок следования операций взаимодействия, который должен иметь место (вместо преступной атаки, как показано на Фиг.14).

Для того чтобы предотвратить образование таких потенциальных проблем с безопасностью, в различные варианты реализации настоящего изобретения включаются соответствующие технологии для уменьшения или устранения нежелательного исполняемого кода. Обратимся к Фиг.16. Процесс 1300, назначением которого является отражение скриптоподобных атак, соответствующим образом включает в себя шаги по уменьшению количества серверных частей, имеющих повышенные привилегии (шаг 1302), удалению опасных символов внутри этих частей сайта (шаг 1304), кодированию некоторых спецсимволов, где это необходимо (шаг 1306), и возможно записи в лог файл информации, которая идет пользователям от соответствующих частей web-сайта (шаг 1308).

Рассмотрим шаг 1302. Web-сайт обычно включает в себя различные страницы, каждая из которых имеет однозначно определяющий ее URL. Пользователи сайта могут оказывать повышенное доверие определенным серверам (таким как те, которые соответствуют зарекомендовавшим себя финансовым или торговым организациям). Ограничивая область высокого доверия только частью web-сайта (т.е. ограниченным подмножеством URL, соответствующим зарекомендовавшему себя web-сайту), можно понизить уровень доверия, оказываемого остальной части сайта, таким образом повышая безопасность. Доверие может быть ограничено определенной частью сайта путем конфигурирования web-браузера пользователя так, чтобы он, например, доверял только части сайта. Web-браузер может быть сконфигурирован вручную или с помощью скрипта, например поставляемого с сервера электронного бумажника. Когда только определенные страницы (т.е. часть) web-сайта получат повышенные привилегии, любой скрипт, полученный при

обращении к другим страницам, или вообще не будет выполняться, или по крайней мере не будет выполняться в режиме повышенных привилегий.

В дополнении к тому (или вместо того) чтобы конфигурировать клиента так, что он "доверяет" только определенной части сервера, сам сервер может быть сконфигурирован так, чтобы улучшить безопасность клиент-серверного взаимодействия. Например, для улучшения безопасности скрипты с повышенными привилегиями могут быть запрещены на большинстве серверов. Более того, данные, передаваемые на доверяемую часть web-сайта, могут быть отслежены и/или изменены перед отправкой их пользователю (шаг 1304 и 1306). Большинство языков написания скриптов используют специальные символы для формирования своих команд. Например, команды в языке JavaScript часто кодируются предложениями, помещенными между угловыми скобками (" <" и ">"). Следовательно угловые скобки могут быть удалены из любого контента, который должен быть возвращен с доверяемой части web-сайта. Если бы на web-странице, полученной с доверяемой части сайта, должна быть злонамеренная JavaScript программа, которая, например, пытается использовать угловые скобки, команды скрипта не будут исполняться на компьютере пользователя, так как эти команды не будут синтаксически правильно отформатированы после удаления угловых скобок. С другой стороны, некоторые "опасные" символы (такие как угловые скобки в JavaScript) могут быть возвращены в другом формате, например в формате "амперсанд" ("&"), или в значениях Американского кода обмена информацией (ASCII), или путем замены "опасных" символов безопасными, такими как символ "пробела" (шаг 1306). Необходимо отметить, что любые символы можно удалять или перекодировать только в зависимости от того, какой именно используется язык скрипта, исполнительная среда и т.п.

В некоторых вариантах реализации изобретения на дополнительном шаге 1308 соответствующим образом включается лог информации от различных частей web-сайта. Весь контент, в котором перекодируются или удаляются символы, может быть записан в лог файл так, чтобы этот лог может быть подвергнут анализу для определения, опасен ли данный web-сайт для того, чтобы подвергать опасности сетевого клиента. Например, весь контент (содержимое), полученный от web-страницы, весь контент, полученный из доверительной части, или контент от любой другой части web-сайта может быть записан в лог в один или несколько файлов данных. Эти файлы данных могут быть соответствующим образом просмотрены или еще как проанализированы для того, чтобы понять, были ли предприняты попытки предоставления незаконного контента пользователям сервера.

В некоторых случаях внутренние компьютеры могут быть подвергнуты атаке "преступного" сайта путем посылки контента, который содержит скрипт сетевому серверу, позволяющий записывать контент в файлы отслеживания (логи). Допустим, браузер был сконфигурирован давать повышенные привилегии файлам, хранящимся на сервере, как в реализациях, где пользователь просматривает файлы отслеживания через web и другие серверы электронной коммерции с использованием такого браузера, и при этом скрипт может быть запущен на сетевом клиенте под привилегиями сетевого сервера, доставившего эту запись отслеживания (т.е. под наивысшими привилегиями). Запуск такого скрипта может повлечь за собой удар, который может быть нанесен значительно позже после того, как скрипт был послан на сетевой сервер. Такая атака предотвратима путем использования таких же способов и процедур, какие были описаны выше для устранения передачи скриптов через сайты, как, например, вышеописанная "преступная" атака. Фильтр, такой как описанный на Фиг.16, запущенный на сетевом сервере, таком как web-сервер, или запущенный на сетевом клиенте, таком как браузер персонального компьютера, может отфильтровывать управляющие символы скриптов и перекодировать символы, отклонять символы или отклонять всю запись.

Соответствующие структуры, материалы, действия и эквиваленты всех элементов нижеприведенной формулы изобретения подразумевают включение в них любых структур, материалов и действий для обеспечения реализации упомянутых функций в совокупности с другими заявляемыми в частных вариантах элементами. Объем притязаний данного

изобретения следует определять в рамках заявляемых признаков формулы и их эквивалентов, не ограничивая его рассмотренными выше примерами.

Формула изобретения

1. Способ проведения трансакций, отличающийся тем, что сначала осуществляют получение запроса на трансакцию от пользователя к серверу, выдают отклик пользователю, получают от пользователя ответ, основанный на упомянутом отклике, после чего осуществляют обработку упомянутого ответа и проверку пользователя, затем составляют удостоверения на трансакцию, содержащие по крайней мере один ключ, и передают пользователю по крайней мере часть упомянутых удостоверений, далее получают повторный запрос от пользователя, который содержит упомянутую часть удостоверений, и осуществляют проверку упомянутой части удостоверений упомянутым ключом для обеспечения доступа к трансакционной службе.

2. Способ по п.1, отличающийся тем, что осуществляют трансакцию электронной покупки.

3. Способ по п.2, отличающийся тем, что осуществляют трансакцию электронной покупки посредством электронного бумажника.

4. Способ по п.1, отличающийся тем, что трансакцию осуществляют посредством смарт-карточки пользователя.

5. Компьютеризованный способ защиты сетевого сервера от его возможного использования в качестве базы для атак на сетевого клиента, отличающийся тем, что сначала осуществляют получение упомянутым сетевым сервером запроса на соединение от упомянутого сетевого клиента и сканирование части упомянутого сетевого сервера на наличие спецсимволов, ассоциированных с протоколом, затем осуществляют проверку на отсутствие спецсимволов в любом ответе сетевого сервера упомянутому сетевому клиенту и направляют ответ от сетевого сервера упомянутому сетевому клиенту.

6. Способ по п.5, отличающийся тем, что дополнительно осуществляют ограничение доступа к упомянутому сетевому серверу только определенной частью этого сетевого сервера для данного протокола.

7. Способ по п.5, отличающийся тем, что дополнительно осуществляют замену упомянутых спецсимволов на безопасные символы с уменьшением рисков, связанных с использованием избранного протокола.

8. Способ по п.5 или 6, отличающийся тем, что упомянутый протокол включает в себя элементы, написанные на языке JavaScript.

9. Способ по любому из пп.5-7, отличающийся тем, что дополнительно осуществляют запись упомянутых спецсимволов для создания журнала безопасности.

10. Способ по п.9, отличающийся тем, что дополнительно осуществляют проверку упомянутого журнала безопасности на установление принадлежности упомянутых спецсимволов к враждебным.

11. Способ по любому из пп.5-7, отличающийся тем, что упомянутую защиту сетевого сервера осуществляют во время трансакции электронной покупки.

12. Способ по п.11, отличающийся тем, что трансакцию электронной покупки осуществляют посредством электронного бумажника.

13. Трансакционная система для обеспечения проведения финансовых трансакций по запросу пользователя, работающего на пользовательском компьютере, подключенном к сети передачи данных, отличающаяся тем, что она содержит авторизатор трансакции и сервер безопасности, сконфигурированный с возможностью проверки наличия средства идентификации в распоряжении пользователя и предоставления цифрового удостоверения упомянутому пользовательскому компьютеру в случае успешной проверки, причем авторизатор трансакции сконфигурирован с возможностью авторизации запроса пользователя на трансакцию на основе по крайней мере части упомянутых цифровых удостоверений, полученных пользовательским компьютером посредством сети передачи данных.

14. Система по п.13, отличающаяся тем, что она дополнительно содержит инструментальный сервер трансакции.

15. Система по п.13, отличающаяся тем, что она дополнительно содержит сервер электронного бумажника, связанный с пользовательским компьютером посредством упомянутой сети передачи данных.

16. Система по п.15, отличающаяся тем, что упомянутый сервер электронного бумажника сконфигурирован с возможностью получения запроса на трансакцию от упомянутого пользовательского компьютера, связи с компьютерной системой продавца и передачи информации об упомянутом пользователе упомянутой компьютерной системе продавца.

17. Система по п.13 или 16, отличающаяся тем, что компьютер пользователя содержит инструмент проведения трансакции и считывающее устройство, сконфигурированное с возможностью передачи информации между инструментом проведения трансакции и средством идентификации.

18. Система по п.17, отличающаяся тем, что упомянутый инструмент проведения трансакции является клиентом электронного бумажника.

19. Система по п.13, отличающаяся тем, что средством идентификации является смарт-карточка.

20. Система по п.13, отличающаяся тем, что упомянутый сервер безопасности и упомянутый авторизатор трансакции имеют между собой соединение передачи данных, изолированное от сети передачи данных.

21. Система по п.17, отличающаяся тем, что упомянутый инструмент проведения трансакции и упомянутый сервер безопасности имеют между собой соединения передачи данных, изолированное от упомянутой сети передачи данных.

22. Система по п.13, отличающаяся тем, что средство идентификации содержит цифровой сертификат однозначной идентификации пользователя данного средства идентификации.

23. Система по п.22, отличающаяся тем, что она содержит персональный идентификатор пользователя упомянутого средства идентификации для открытия ему доступа к цифровому сертификату.

24. Система по п.13, отличающаяся тем, что она включает в себя эмитента средства идентификации, а трансакция является трансакцией типа ″карточка присутствует″, установленной эмитентом средства идентификации.

25. Сервер электронного бумажника для обеспечения проведения трансакций через цифровую сеть, отличающийся тем, что он содержит интерфейс цифровой сети и приложение электронного бумажника, имеющее связь с базой данных, причем сервер электронного бумажника сконфигурирован с возможностью получения запроса на трансакцию от клиента электронного бумажника, обработки удостоверения от упомянутого клиента электронного бумажника для идентификации пользователя клиента электронного бумажника, выборки информации о пользователе из базы данных после идентификации упомянутого пользователя и совершения упомянутой трансакции от имени упомянутого пользователя с использованием упомянутой информации о пользователе.

26. Сервер по п.25, отличающийся тем, что упомянутое удостоверение содержит цифровую подпись.

27. Сервер по п.26, отличающийся тем, что упомянутое удостоверение содержит набор произвольных данных с цифровой подписью средства идентификации, находящегося в распоряжении упомянутого пользователя.

28. Сервер по п.27, отличающийся тем, что упомянутый клиент электронного бумажника снабжен упомянутым набором произвольных данных посредством сервера безопасности.

29. Сервер по п.25 или 27, отличающийся тем, что он содержит формы продавца, заполненные информацией об упомянутом пользователе при совершении упомянутой трансакции от имени пользователя.

30. Компьютеризованный способ выполнения онлайновых покупок, отличающийся тем,

что осуществляют авторизацию посредством сервера безопасности, получают удостоверения от упомянутого сервера безопасности, затем идентифицируют адрес продавца, откуда совершается покупка, передают упомянутые удостоверения на сервер электронного бумажника для авторизации упомянутого пользователя на сервере электронного бумажника, а после успешной авторизации на сервере электронного бумажника переадресовывают сообщения с упомянутым адресом продавца на упомянутый сервер электронного бумажника и направляют информацию об упомянутом пользователе от сервера электронного бумажника на адрес продавца, после чего получают информацию о результатах упомянутой покупки.

31. Способ по п.30, отличающийся тем, что упомянутое удостоверение содержит цифровую подпись.

32. Способ по п.31, отличающийся тем, что упомянутое удостоверение содержит данные, полученные от сервера безопасности.

33. Компьютеризованный способ выполнения онлайновых покупок, отличающийся тем, что осуществляют получение на сервер запроса от пользователя на трансакцию, который включает в себя адрес продавца и удостоверение, затем осуществляют проверку упомянутого удостоверения для идентификации пользователя, а по результатам упомянутой проверки осуществляют выборку пользовательской информации из базы данных, после чего заполняют онлайновые формы в соответствии с адресом продавца и выдают упомянутому пользователю информацию о результатах покупки.

34. Способ по п.33, отличающийся тем, что упомянутое удостоверение содержит цифровую подпись.

35. Способ по п.34, отличающийся тем, что упомянутое удостоверение содержит данные, полученные от сервера безопасности.

36. Способ по п.35, отличающийся тем, что упомянутый сервер безопасности объединяют с упомянутым сервером.

37. Способ по любому из пп.34-36, отличающийся тем, что упомянутую цифровую подпись выполняют посредством смарт-карточки.

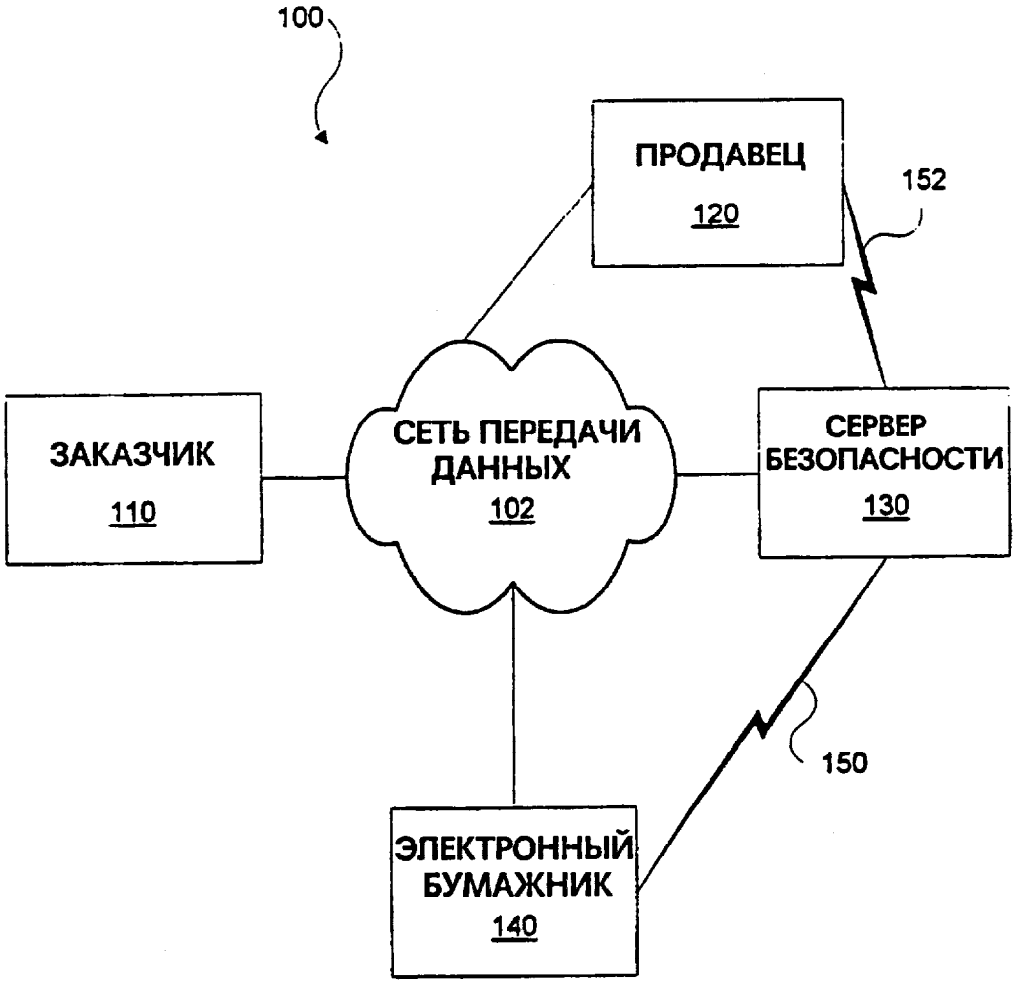
38. Компьютеризованный способ контроля доступа к службе, отличающийся тем, что сначала получают от пользователя запрос на вход, проверяют наличие у пользователя средства идентификации, после получения успешного результата проверки выдают удостоверение упомянутому пользователю, затем получают от пользователя запрос на трансакцию, который включает в себя, по крайней мере, часть упомянутого удостоверения, и осуществляют обработку упомянутой части удостоверения для обеспечения доступа к упомянутой службе.

39. Способ по п.38, отличающийся тем, что упомянутую проверку осуществляют посредством запроса-ответа.

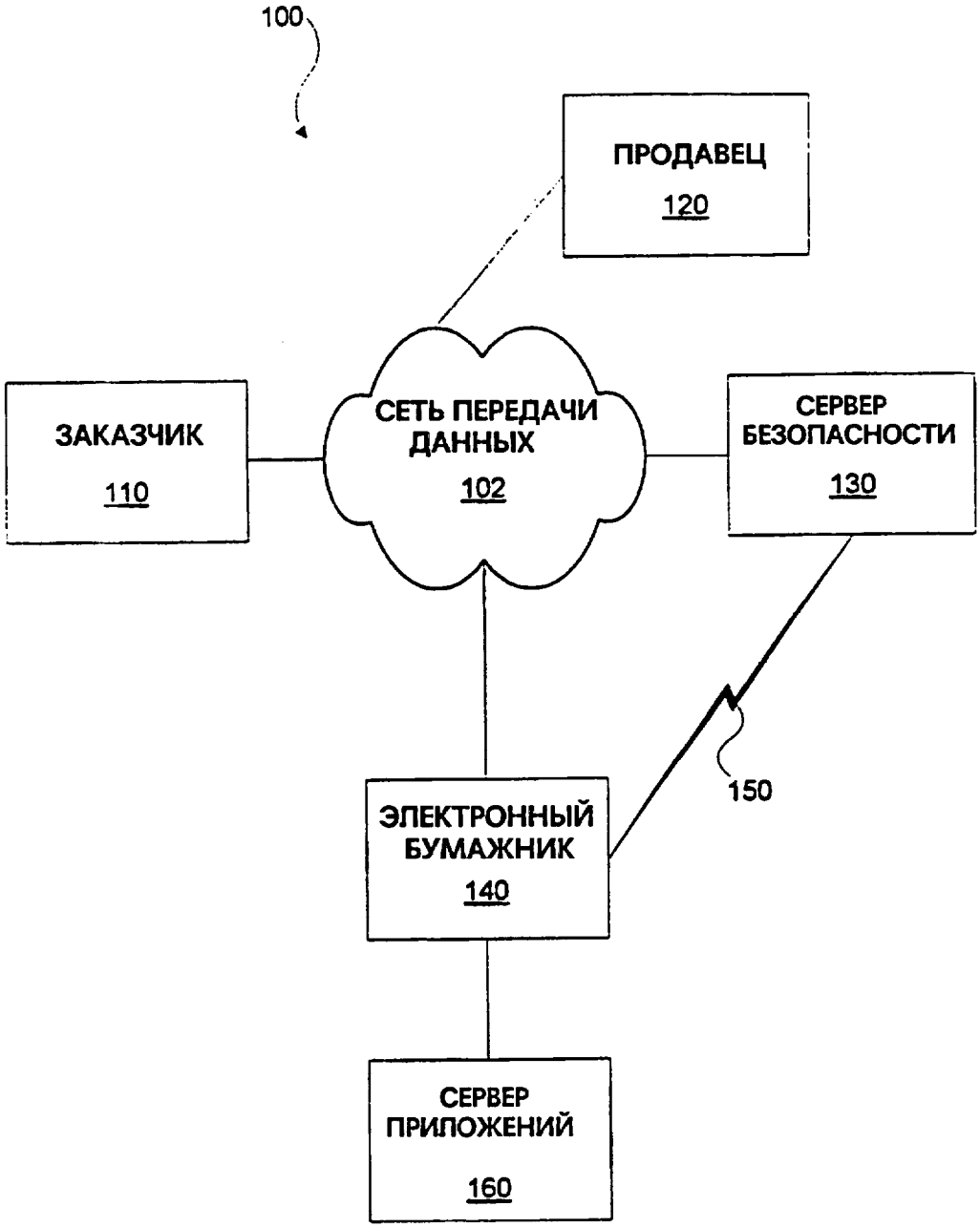
40. Способ по п.39, отличающийся тем, что упомянутые запрос-ответ содержат произвольные данные из средства идентификации.

41. Способ по п.40, отличающийся тем, что упомянутые запрос-ответ дополнительно содержат цифровую подпись упомянутых произвольных данных.

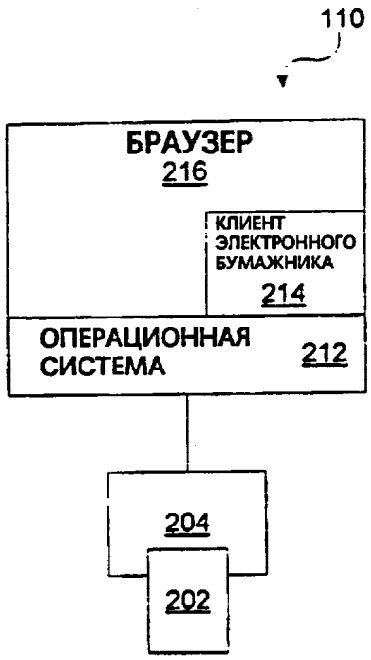
42. Способ по любому из пп.38-41, отличающийся тем, что упомянутая служба является службой финансовой трансакции.


100
ПРОДАВЕЦ
120
152
ЗАКАЗЧИК
110
СЕТЬ ПЕРЕДАЧИ ДАННЫХ
102
СЕРВЕР БЕЗОПАСНОСТИ
130
150
ЭЛЕКТРОННЫЙ БУМАЖНИК
140

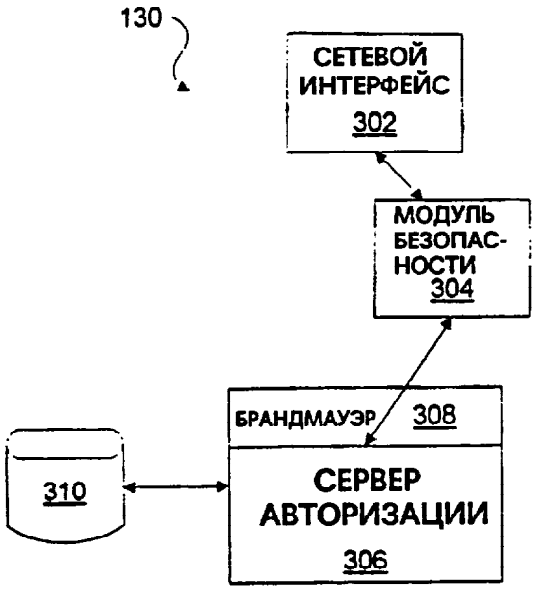
Фиг.2


100
ПРОДАВЕЦ
120
ЗАКАЗЧИК
110
СЕТЬ ПЕРЕДАЧИ ДАННЫХ
102
СЕРВЕР БЕЗОПАСНОСТИ
130
150
ЭЛЕКТРОННЫЙ БУМАЖНИК
140
СЕРВЕР ПРИЛОЖЕНИЙ
160

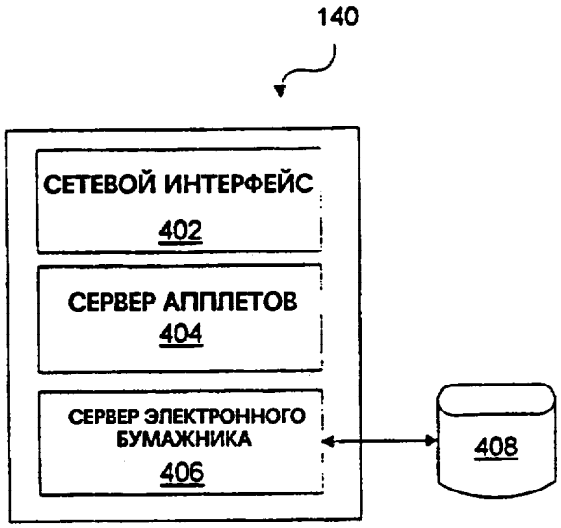
Фиг.3


110
БРАУЗЕР
216
КЛИЕНТ ЭЛЕКТРОННОГО БУМАЖНИКА
214
ОПЕРАЦИОННАЯ СИСТЕМА
212
204
202

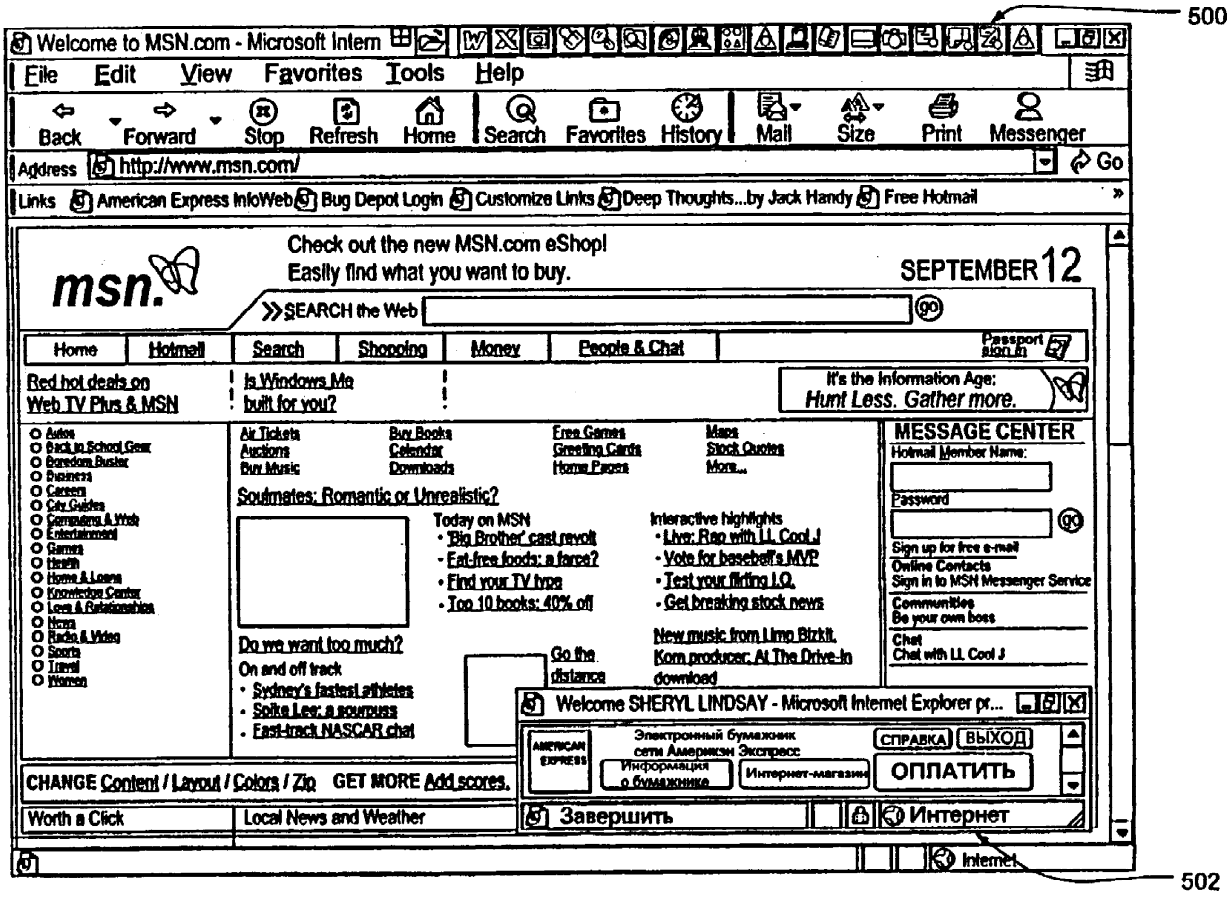
Фиг.4


130
СЕТЕВОЙ ИНТЕРФЕЙС
302
МОДУЛЬ БЕЗОПАС-НОСТИ
304
БРАНДМАУЭР
308
СЕРВЕР АВТОРИЗАЦИИ
306
310

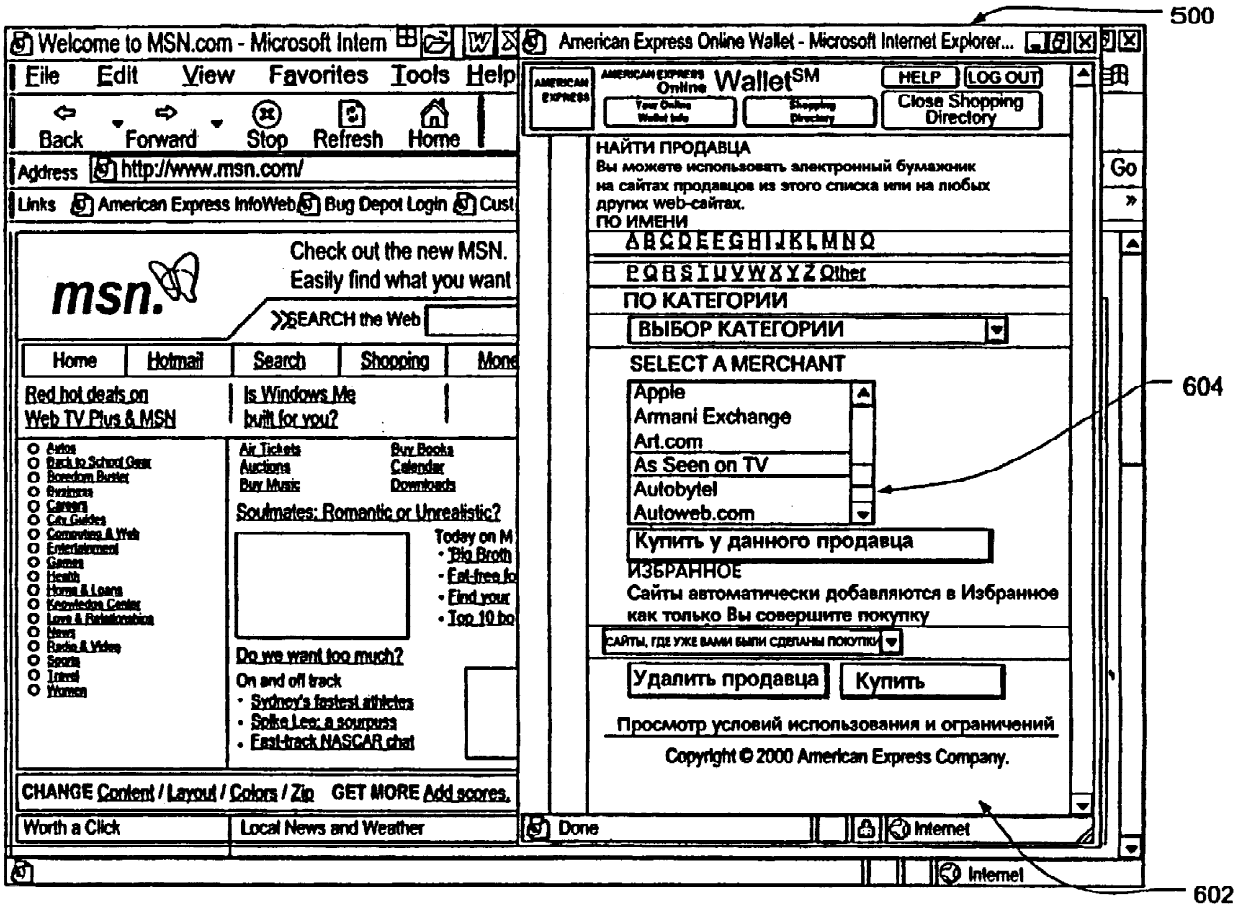
Фиг.5


140
СЕТЕВОЙ ИНТЕРФЕЙС
402
СЕРВЕР АППЛЕТОВ
404
СЕРВЕР ЭЛЕКТРОННОГО БУМАЖНИКА
406
408

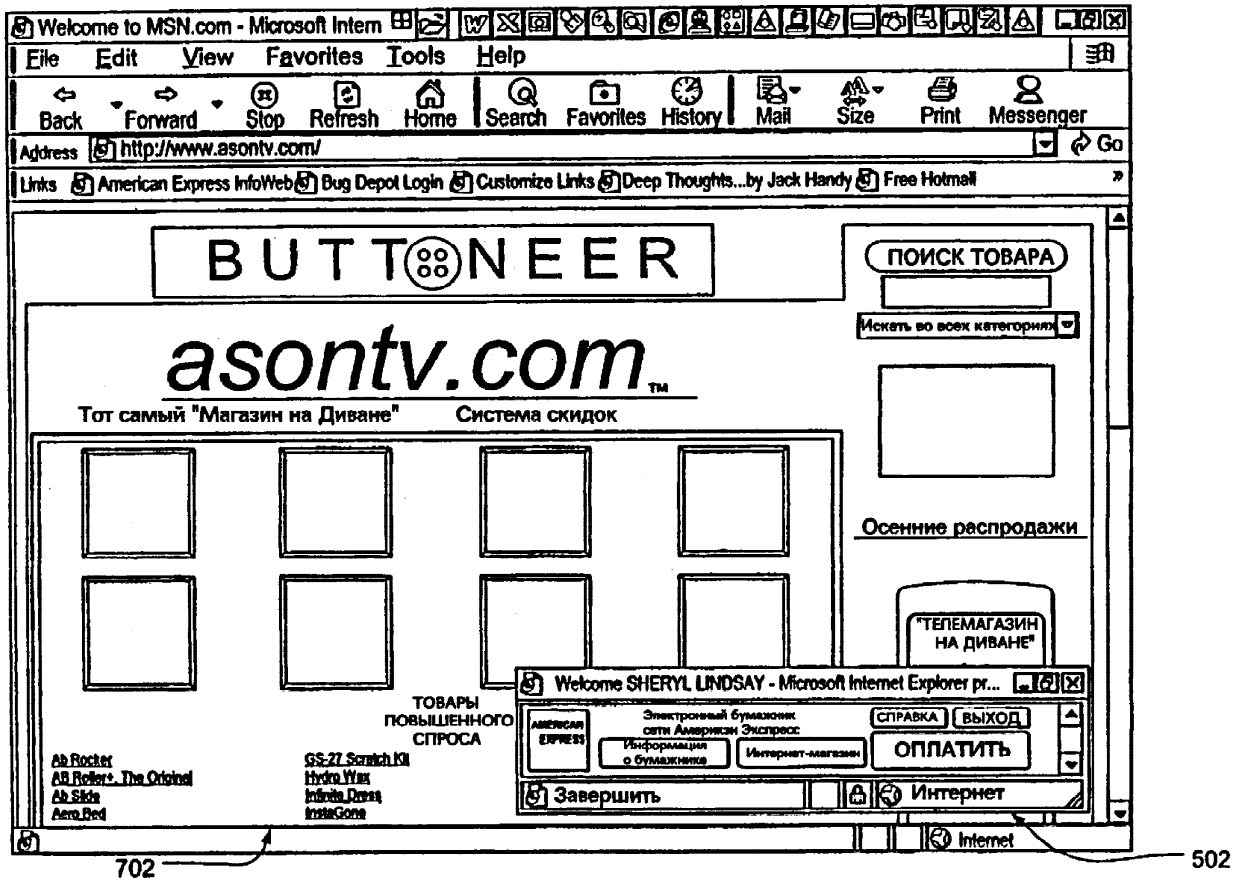
Фиг.6


500
Welcome to MSN.com - Microsoft Intern
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Size Print Messenger
Address http://www.msn.com/
Go
Links American Express InfoWeb Bug Depot Login Customize Links Deep Thoughts...by Jack Handy Free Hotmail
msn.
Check out the new MSN.com eShop!
Easily find what you want to buy.
SEPTEMBER 12
SEARCH the Web
Home Hotmail Search Shopping Money People & Chat
Passport sign in
Red hot deals on Web TV Plus & MSN
Is Windows Me built for you?
It's the Information Age: Hunt Less. Gather more.
Air Tickets Buy Books Free Games Maps
Auctions Calendar Greeting Cards Stock Quotes
Buy Music Downloads Home Pages More...
Soulmates: Romantic or Unrealistic?
Today on MSN
'Big Brother' cast revolt
Fat-free foods: a farce?
Find your TV type
Top 10 books: 40% off
Interactive highlights
Live: Rap with LL Cool J
Vote for baseball's MVP
Test your flirting I.Q.
Get breaking stock news
MESSAGE CENTER
Hotmail Member Name:
Password
Sign up for free e-mail
Online Contacts
Sign in to MSN Messenger Service
Communities
Be your own boss
Chat
Chat with LL Cool J
Do we want too much?
On and off track
Sydney's fastest athletes
Sofia Lee: a sourpuss
Fast-track NASCAR chat
Go the distance
New music from Limp Bizkit, Korn producer; At The Drive-In download
CHANGE Content / Layout / Colors / Zip GET MORE Add scores.
Worth a Click
Local News and Weather
Welcome SHERYL LINDSAY - Microsoft Internet Explorer pr...
Электронный бумажник сети Американ Экспресс
СПРАВКА ВЫХОД
Информация о бумажнике
Интернет-магазин
ОПЛАТИТЬ
Завершить
Интернет
Internet
502

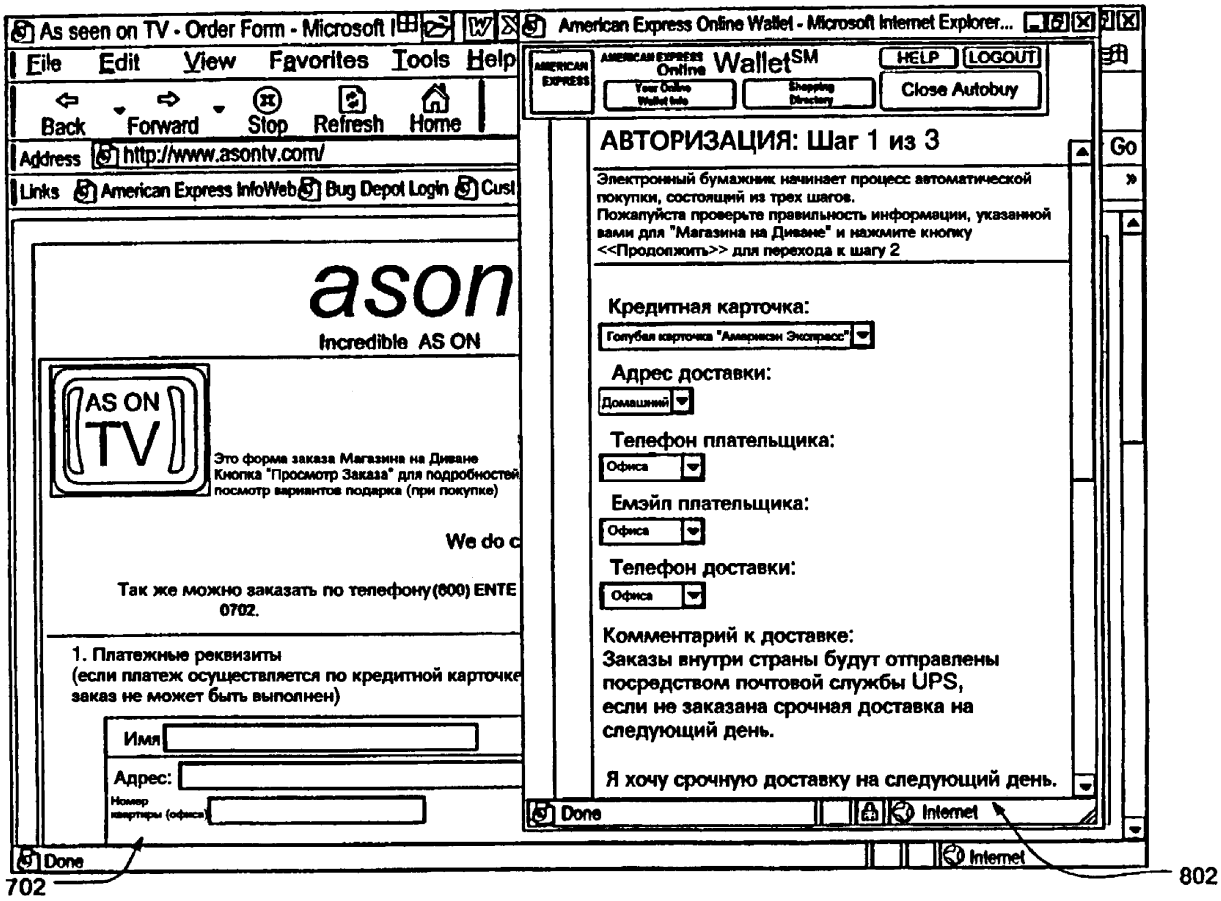
Фиг. 7


500
Welcome to MSN.com - Microsoft Intern
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home
Address http://www.msn.com/
Links American Express InfoWeb Bug Depot Login
msn.
Check out the new MSN.
Easily find what you want
SEARCH the Web
Home Hotmail Search Shopping
Red hot deals on Web TV Plus & MSN
Is Windows Me built for you?
Soulmates: Romantic or Unrealistic?
Do we want too much?
On and off track
CHANGE Content / Layout / Colors / Zip GET MORE Add scores.
Worth a Click
Local News and Weather
American Express Online Wallet - Microsoft Internet Explorer...
Wallet SM
HELP LOG OUT
Close Shopping Directory
НАЙТИ ПРОДАВЦА
Вы можете использовать электронный бумажник на сайтах продавцов из этого списка или на любых других web-сайтах.
ПО ИМЕНИ
A B C D E F G H I J K L M N O
P Q R S T U V W X Y Z Other
ПО КАТЕГОРИИ
ВЫБОР КАТЕГОРИИ
SELECT A MERCHANT
Apple
Armani Exchange
Art.com
As Seen on TV
Autobytel
Autoweb.com
604
Купить у данного продавца
ИЗБРАННОЕ
Сайты автоматически добавляются в Избранное как только Вы совершите покупку
САЙТЫ, ГДЕ УЖЕ ВАМИ БЫЛИ СДЕЛАНЫ ПОКУПКИ
Удалить продавца
Купить
Просмотр условий использования и ограничений
Copyright © 2000 American Express Company.
Done
Internet
602

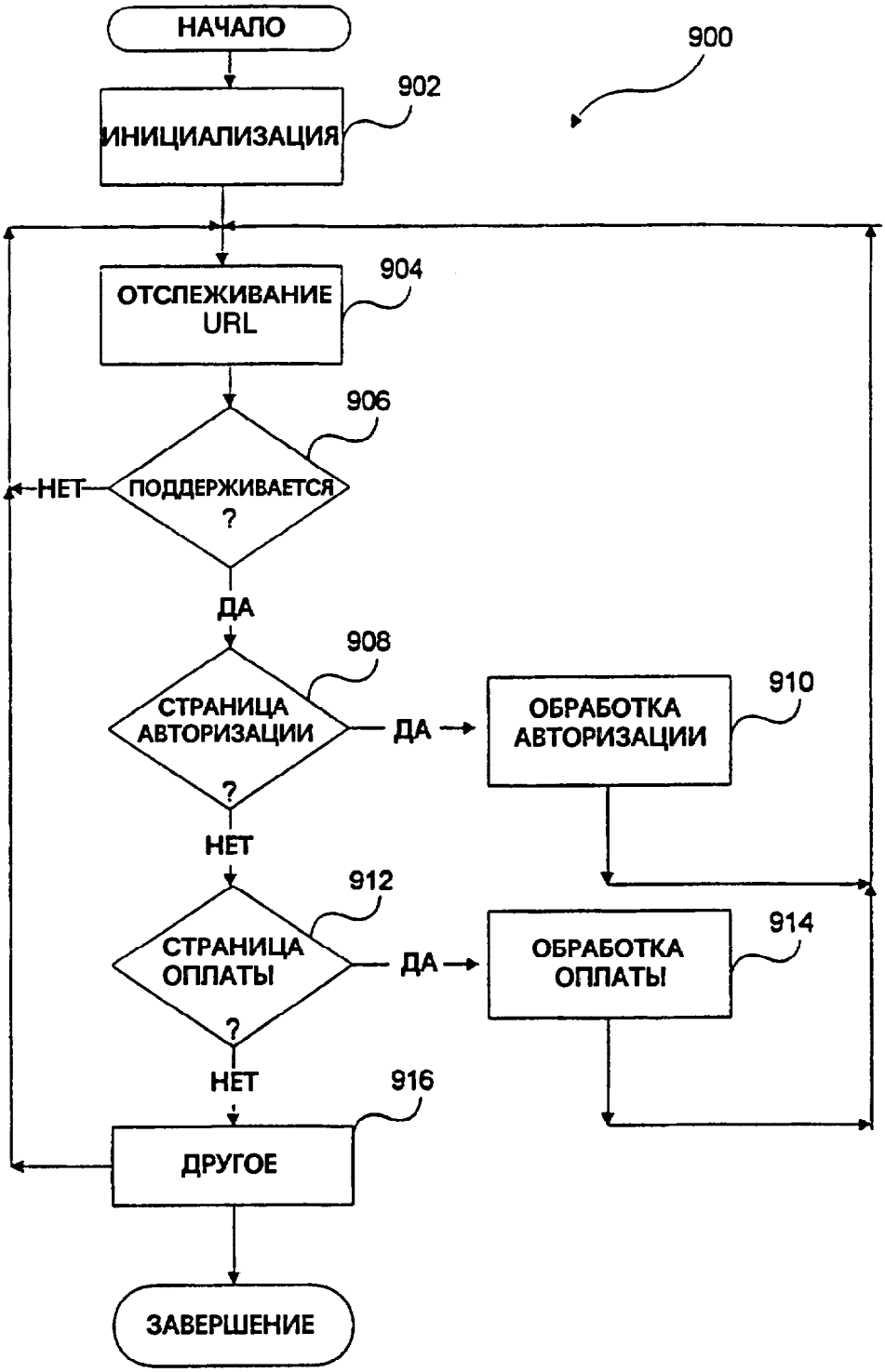
Фиг. 8


Welcome to MSN.com - Microsoft Intern
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Size Print Messenger
Address http://www.asontv.com/
Links American Express InfoWeb Bug Depot Login Customize Links Deep Thoughts...by Jack Handy Free Hotmail
BUTTONEER
asontv.com™
Тот самый "Магазин на Диване"
Система скидок
ПОИСК ТОВАРА
Искать во всех категориях
Осенние распродажи
"ТЕЛЕМАГАЗИН НА ДИВАНЕ"
ТОВАРЫ ПОВЫШЕННОГО СПРОСА
Ab Rocker
AB Roller+, The Original
Ab Slide
Aero Bed
GS-27 Scratch Kit
Hydro Wax
Infinite Dress
InstaGone
Welcome SHERYL LINDSAY - Microsoft Internet Explorer pr...
Электронный бумажник сети Американ Экспресс
СПРАВКА
ВЫХОД
Информация о бумажнике
Интернет-магазин
ОПЛАТИТЬ
Завершить
Интернет
Internet
702
502

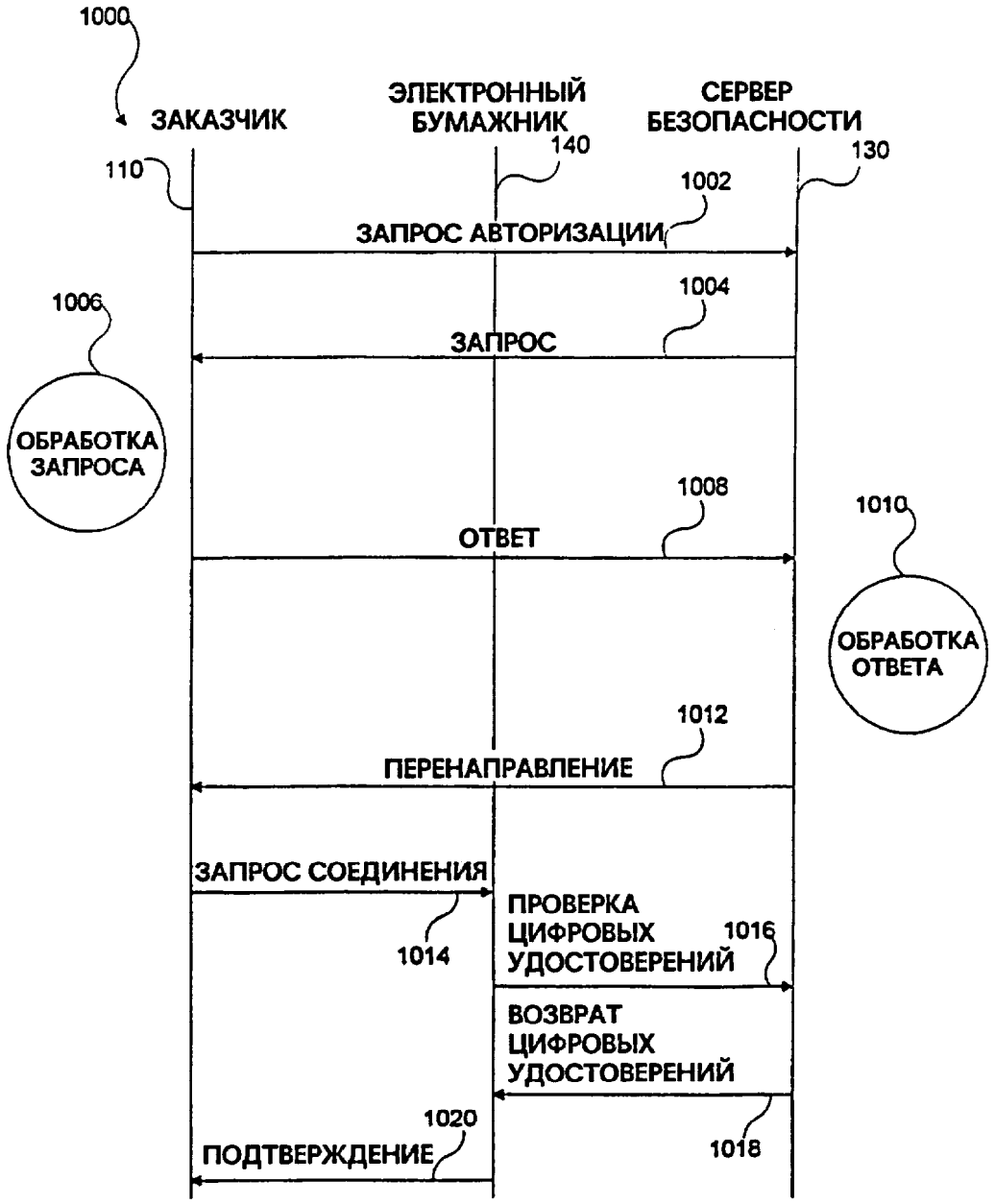
Фиг. 9


As seen on TV - Order Form - Microsoft I
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home
Address http://www.asontv.com/
Links American Express InfoWeb Bug Depot Login Cust
ason
Incredible AS ON
AS ON TV
Это форма заказа Магазина на Диване
Кнопка "Просмотр Заказа" для подробностей
посмотр вариантов подарка (при покупке)
We do c
Так же можно заказать по телефону (800) ENTE
0702.
1. Платежные реквизиты
(если платеж осуществляется по кредитной карточке
заказ не может быть выполнен)
Имя
Адрес:
Номер квартиры (офиса)
Done
Internet
702
American Express Online Wallet - Microsoft Internet Explorer...
AMERICAN EXPRESS
AMERICAN EXPRESS Online Wallet SM
HELP
LOGOUT
Your Online Wallet Info
Shopping Directory
Close Autobuy
Go
АВТОРИЗАЦИЯ: Шаг 1 из 3
Электронный бумажник начинает процесс автоматической покупки, состоящий из трех шагов.
Пожалуйста проверьте правильность информации, указанной вами для "Магазина на Диване" и нажмите кнопку <<Продолжить>> для перехода к шагу 2
Кредитная карточка:
Голубая карточка "Американ Экспресс"
Адрес доставки:
Домашний
Телефон плательщика:
Офиса
Емэйл плательщика:
Офиса
Телефон доставки:
Офиса
Комментарий к доставке:
Заказы внутри страны будут отправлены посредством почтовой службы UPS, если не заказана срочная доставка на следующий день.
Я хочу срочную доставку на следующий день.
Done
Internet
802

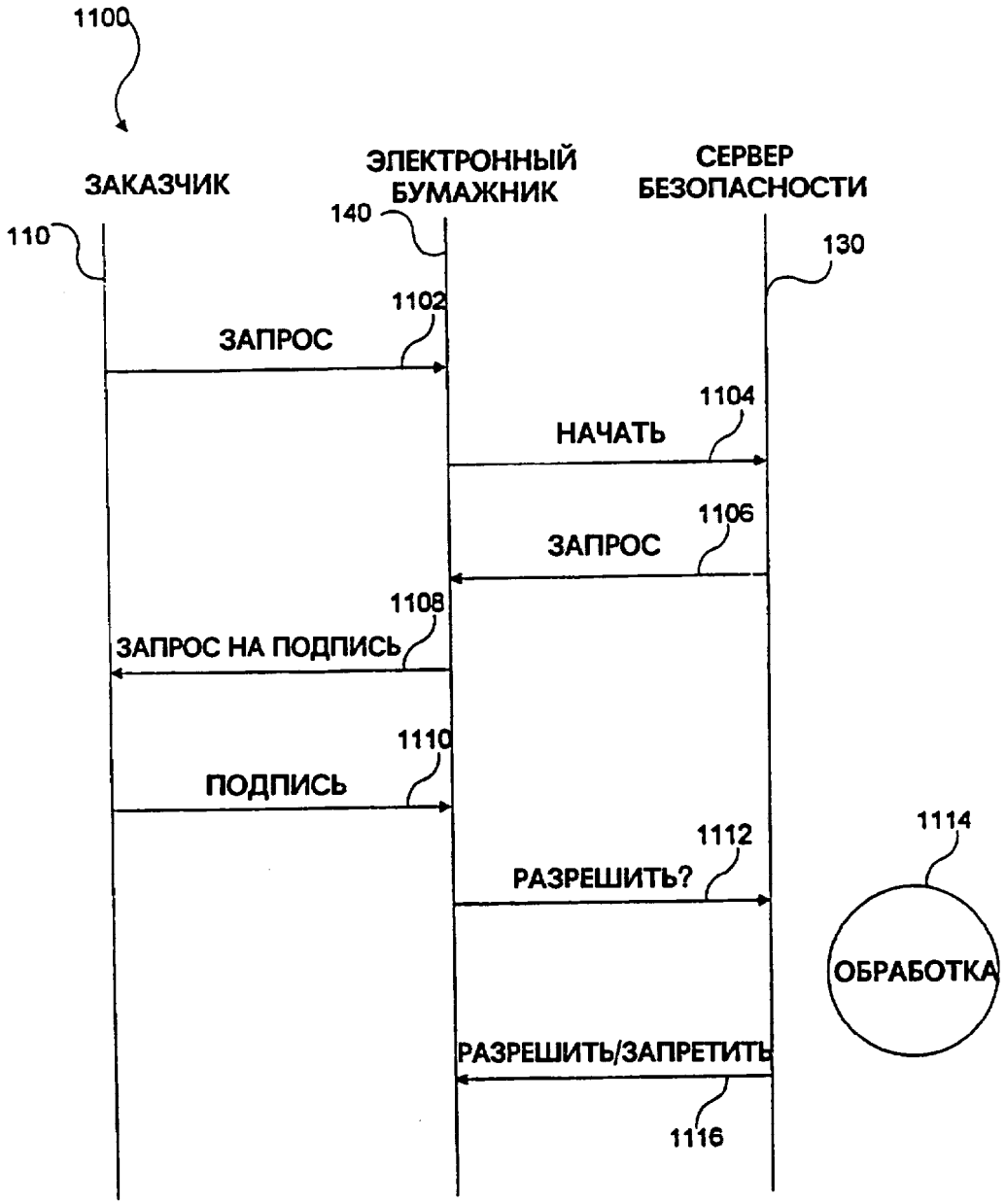
Фиг. 10


НАЧАЛО
900
902
ИНИЦИАЛИЗАЦИЯ
904
ОТСЛЕЖИВАНИЕ URL
906
НЕТ
ПОДДЕРЖИВАЕТСЯ ?
ДА
908
СТРАНИЦА АВТОРИЗАЦИИ ?
ДА
910
ОБРАБОТКА АВТОРИЗАЦИИ
НЕТ
912
СТРАНИЦА ОПЛАТЫ ?
ДА
914
ОБРАБОТКА ОПЛАТЫ
НЕТ
916
ДРУГОЕ
ЗАВЕРШЕНИЕ

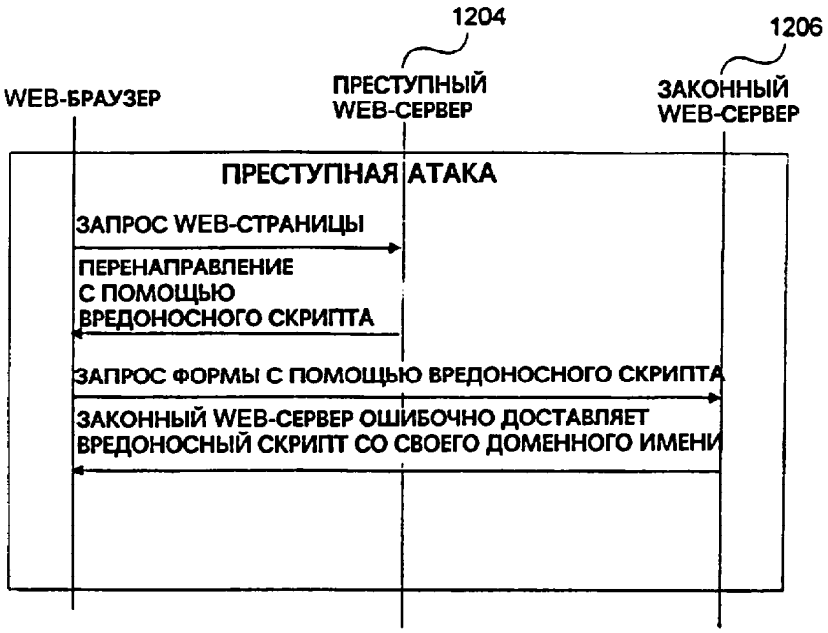
Фиг.11


1000
ЗАКАЗЧИК
ЭЛЕКТРОННЫЙ БУМАЖНИК
СЕРВЕР БЕЗОПАСНОСТИ
110
140
130
1002
ЗАПРОС АВТОРИЗАЦИИ
1004
1006
ЗАПРОС
ОБРАБОТКА ЗАПРОСА
1008
1010
ОТВЕТ
ОБРАБОТКА ОТВЕТА
1012
ПЕРЕНАПРАВЛЕНИЕ
ЗАПРОС СОЕДИНЕНИЯ
1014
ПРОВЕРКА ЦИФРОВЫХ УДОСТОВЕРЕНИЙ
1016
ВОЗВРАТ ЦИФРОВЫХ УДОСТОВЕРЕНИЙ
1018
1020
ПОДТВЕРЖДЕНИЕ

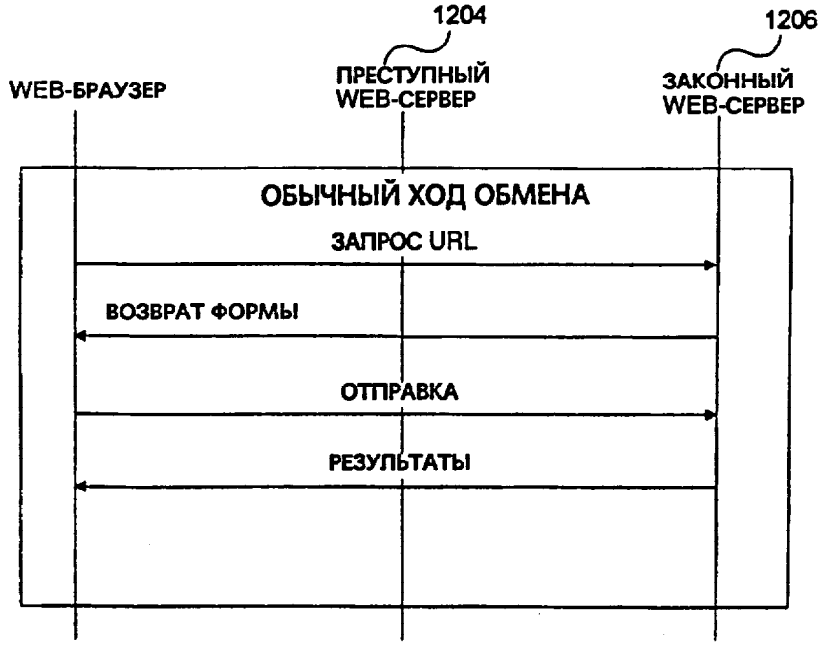
Фиг.12


1100
ЗАКАЗЧИК
ЭЛЕКТРОННЫЙ БУМАЖНИК
СЕРВЕР БЕЗОПАСНОСТИ
110
140
130
1102
ЗАПРОС
1104
НАЧАТЬ
1106
ЗАПРОС
1108
ЗАПРОС НА ПОДПИСЬ
1110
ПОДПИСЬ
1112
РАЗРЕШИТЬ?
1114
ОБРАБОТКА
РАЗРЕШИТЬ/ЗАПРЕТИТЬ
1116

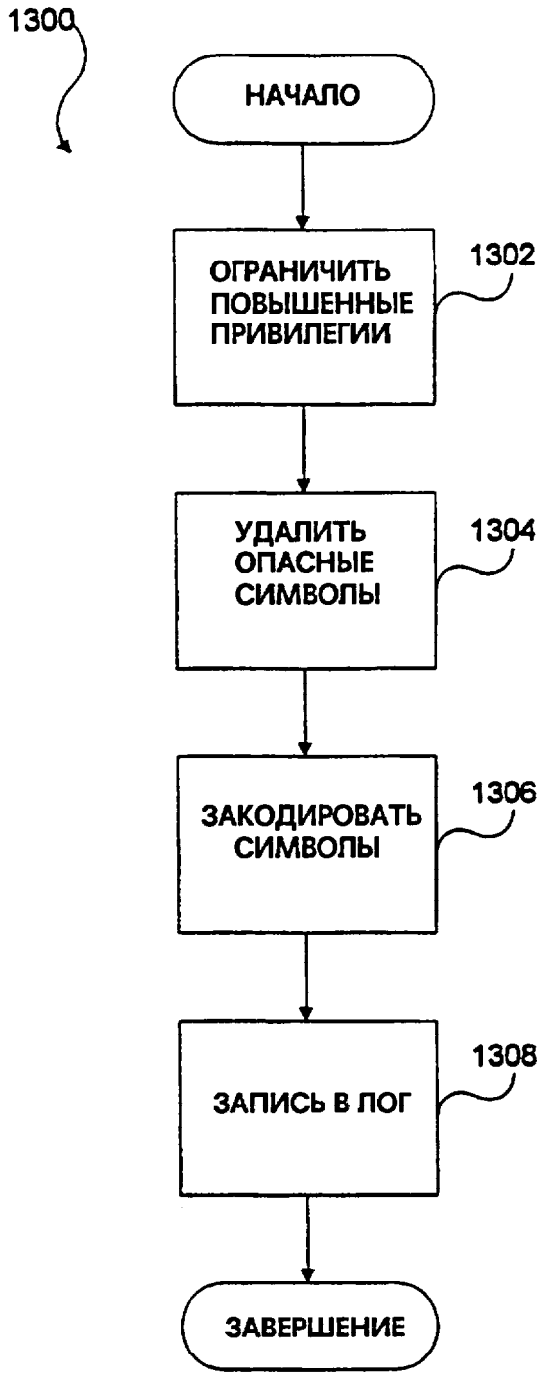
Фиг.13


1204
1206
WEB-БРАУЗЕР
ПРЕСТУПНЫЙ WEB-СЕРВЕР
ЗАКОННЫЙ WEB-СЕРВЕР
ПРЕСТУПНАЯ АТАКА
ЗАПРОС WEB-СТРАНИЦЫ
ПЕРЕНАПРАВЛЕНИЕ С ПОМОЩЬЮ ВРЕДОНОСНОГО СКРИПТА
ЗАПРОС ФОРМЫ С ПОМОЩЬЮ ВРЕДОНОСНОГО СКРИПТА
ЗАКОННЫЙ WEB-СЕРВЕР ОШИБОЧНО ДОСТАВЛЯЕТ ВРЕДОНОСНЫЙ СКРИПТ СО СВОЕГО ДОМЕННОГО ИМЕНИ

Фиг.14


1204
1206
WEB-БРАУЗЕР
ПРЕСТУПНЫЙ WEB-СЕРВЕР
ЗАКОННЫЙ WEB-СЕРВЕР
ОБЫЧНЫЙ ХОД ОБМЕНА
ЗАПРОС URL
ВОЗВРАТ ФОРМЫ
ОТПРАВКА
РЕЗУЛЬТАТЫ

Фиг.15


1300
НАЧАЛО
ОГРАНИЧИТЬ ПОВЫШЕННЫЕ ПРИВИЛЕГИИ
1302
УДАЛИТЬ ОПАСНЫЕ СИМВОЛЫ
1304
ЗАКОДИРОВАТЬ СИМВОЛЫ
1306
ЗАПИСЬ В ЛОГ
1308
ЗАВЕРШЕНИЕ

Фиг.16