РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 587 423** (13) **C2**

(51) МПК
G06F 21/00 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2013143484/08, 26.09.2013**

(24) Дата начала отсчета срока действия патента:
26.09.2013

Приоритет(ы):
(22) Дата подачи заявки: **26.09.2013**

(43) Дата публикации заявки: **10.04.2015** Бюл. № **10**

(45) Опубликовано: **20.06.2016** Бюл. № **17**

(56) Список документов, цитированных в отчете о поиске: **US 2013/0268357 A1,10.10.13. WO 2009/032187 A1,12.03.2009. EA 200900225A1, 30.12.2009. RU 2007138849A, 27.04.2009.**

Адрес для переписки:
125212, Москва, Ленинградское ш., 39а, стр. 3, АО Лаборатория Касперского, Управление по интеллектуальной собственности, Надежде Васильевне Кащенко

(72) Автор(ы):
Монастырский Алексей Владимирович (RU),
Голованов Сергей Юрьевич (RU),
Мартыненко Владислав Валерьевич (RU),
Русаков Вячеслав Евгеньевич (RU)

(73) Патентообладатель(и):
Закрытое акционерное общество "Лаборатория Касперского" (RU)

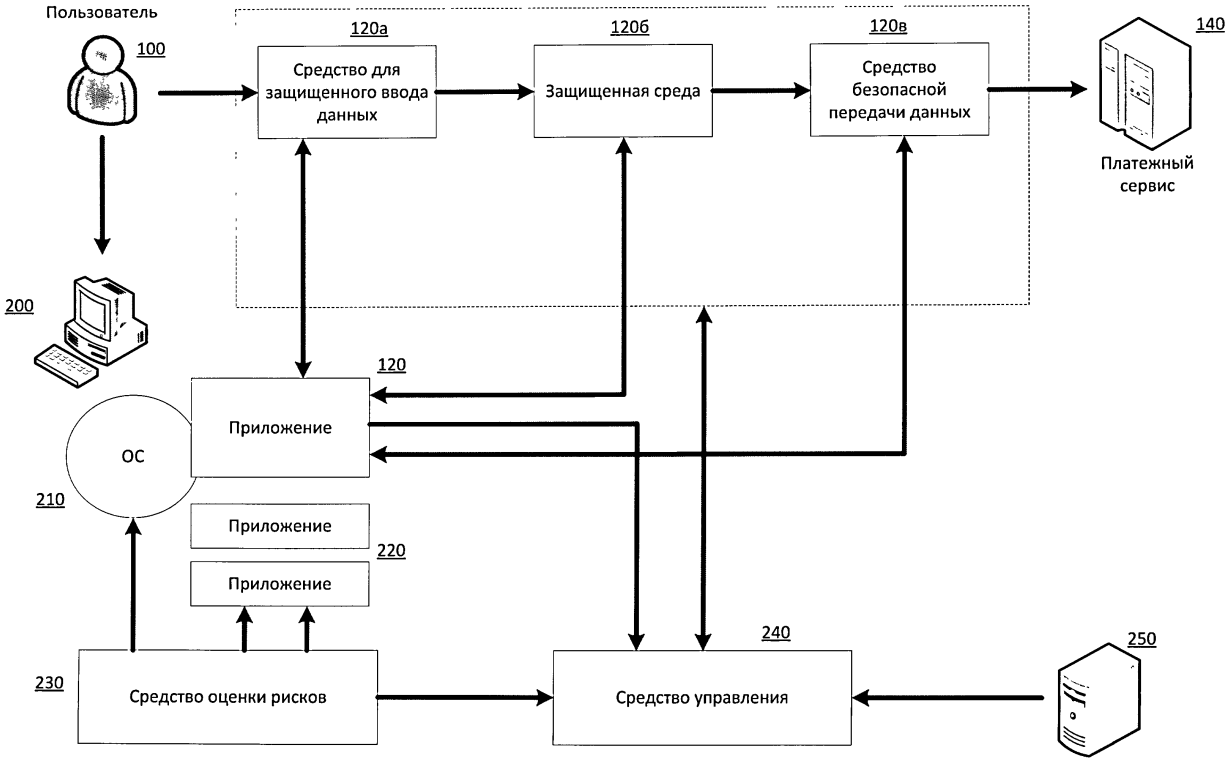
(54) СИСТЕМА И СПОСОБ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОНЛАЙН-ТРАНЗАКЦИЙ

(57) Реферат:

Изобретение относится к системам проведения онлайн-транзакций. Технический результат заключается в обеспечении безопасности проведения онлайн-транзакций. Реализуемая компьютером система содержит средство управления, предназначенное для определения начало проведения онлайн-транзакции, производимой с помощью приложения, используемого для проведения онлайн-транзакции, и связано со средством для защищенного ввода данных, с защищенной средой, со средством безопасной передачи данных и со средством оценки рисков, предназначенным для оценки рисков онлайн-транзакции и передачи информации об оценки рисков средству управления. 4 ил., 1 табл.

RU 2587423 C2

RU 2587423 C2



Фиг. 2

RU 2587423 C2

RU 2587423 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 587 423** (13) **C2**

(51) Int. Cl.
G06F 21/00 (2013.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2013143484/08, 26.09.2013**

(24) Effective date for property rights:
26.09.2013

Priority:
(22) Date of filing: **26.09.2013**

(43) Application published: **10.04.2015** Bull. № **10**

(45) Date of publication: **20.06.2016** Bull. № **17**

Mail address:
125212, Moskva, Leningradskoe sh., 39a, str. 3, AO Laboratorija Kasperskogo, Upravlenie po intellektualnoj sobstvennosti, Nadezhde Vasilevne Kashchenko

(72) Inventor(s):
Monastyrskij Aleksej Vladimirovich (RU),
Golovanov Sergej YUrevich (RU),
Martynenko Vladislav Valerevich (RU),
Rusakov Vyacheslav Evgenevich (RU)

(73) Proprietor(s):
Zakrytoe aktsionernoe obshshestvo "Laboratoriya Kasperskogo" (RU)

RU 2587423 C2

(54) SYSTEM AND METHOD OF PROVIDING SAFETY OF ONLINE TRANSACTIONS

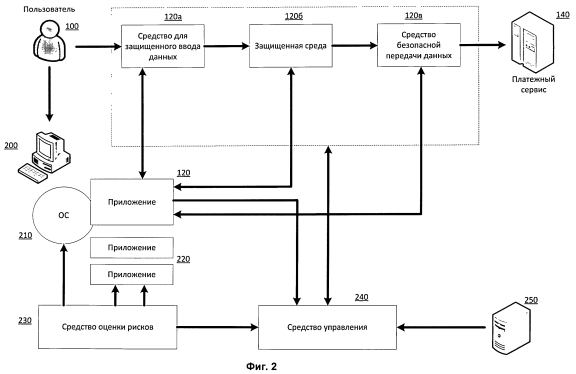
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to online transaction systems. System implemented by computer comprises control device designed to define beginning of online transaction performed by means of application used for performing online transaction, and is connected with device for ensuring protected data input, with protected medium, with device for secure data transmission and with device for assessing risks of online transactions and transmission of data on risk assessment onto control device.

EFFECT: providing safety of online transactions.

1 cl, 4 dwg, 1 tbl



Фиг. 2

RU 2587423 C2

Область техники

Изобретение относится к компьютерной безопасности, а более конкретно к системам и способам обеспечения безопасности онлайн-транзакций.

Уровень техники

В настоящее время существует большое количество программного обеспечения, с помощью которого можно проводить различные онлайн-транзакции. Многие транзакции совершаются с помощью онлайн-банкинга, используя стандартные браузеры, также используются отдельные банковские клиенты, которые особенно популярны на мобильных платформах. Среди других приложений, связанных с онлайн-транзакциями, можно отметить системы электронной валюты, как, например, BitCoin, или онлайн-игры, которые используют собственную систему микротранзакций, во время которых пользователь покупает внутриигровые предметы или внутриигровую валюту за счет реальных средств (например, используя свою банковскую карту).

Неудивительно, что с ростом онлайн-платежей этим сегментом услуг заинтересовались злоумышленники, которые активно исследуют возможные варианты перехвата данных транзакций с целью незаконного перевода средств. Как правило, кражу подобных данных осуществляют с помощью вредоносных программ, которые попадают на компьютеры пользователей (заражают их). Чаще всего подобные программы попадают на компьютеры через заражение популярных интернет-браузеров, выполняют перехват данных, вводимых с устройств ввода (таких как клавиатура или мышь), или перехватывают данные, отправляемые в сеть. Например, вредоносные программы, заражающие браузеры, получают доступ к файлам браузера, просматривают историю посещений и сохраненные пароли при посещении веб-страниц. Перехватчики ввода данных (англ. keyloggers) перехватывают ввод данных с клавиатуры или мыши, делают снимки экранов (англ. screenshots) и скрывают свое присутствие в системе с помощью целого ряда руткит-технологий (англ. rootkit). Подобные технологии также применяются при реализации перехватчиков сетевых пакетов (снифферов трафика, англ. traffic sniffers), которые перехватывают передаваемые сетевые пакеты, извлекая из них ценную информацию, такую как пароли и другие личные данные. Стоит отметить, что заражение чаще всего происходит с использованием уязвимостей в программном обеспечении, которые позволяют использовать различные эксплойты (англ. exploit) для проникновения в компьютерную систему.

Существующие антивирусные технологии, такие как использование сигнатурной или эвристической проверок, методы проактивной защиты или использование списков доверенных приложений (англ. whitelist), хотя и позволяют добиться обнаружения многих вредоносных программ на компьютерах пользователей, однако не всегда способны определить их новые модификации, частота появления которых растет день ото дня. Таким образом, требуются решения, которые могли бы обезопасить процедуру проведения онлайн-платежей у пользователей.

Существуют различные решения, которые направлены на обеспечение безопасности онлайн-транзакций. Возможным решением по противодействию вредоносным программам, которые перехватывают ввод данных с устройств ввода, является использование защищенных устройств ввода. Примером таких устройств является клавиатура с шифрованием вводимых данных или виртуальная клавиатура (http://support.kaspersky.com/kav2012/start?qid=208284630). Подобные решения обладают рядом недостатков: для клавиатуры с шифрованием вводимых данных также могут существовать перехватчики, которые осуществляют перехват данных до шифрования или уже после их расшифровки, а виртуальная клавиатура может быть

скомпрометирована с помощью использования вредоносных программ, которые делают снимки экрана через заданные промежутки времени.

Заявка US 20060136332 описывает использование связки "защищенное устройство поддержки транзакций плюс программный клиент на компьютере" для обеспечения безопасности транзакций. Программный клиент работает прозрачно для пользователя. Защищенное устройство содержит набор алгоритмов для обеспечения безопасности каждого известного типа транзакции. Однако заявка не затрагивает вопрос анализа безопасности компьютера в целом, т.е. при наличии неизвестных вредоносных программ ввод пользователем данных может быть скомпрометирован. В заявке WO 2005033943 описывается сервис для анализа веб-сервера платежной системы на предмет уязвимостей (например, наличия открытых портов). Посетителям веб-сервера (т.е. клиентам сервиса) будет отображаться информация о найденных уязвимостях, однако дальнейшие действия должны принимать сами пользователи. В патенте US 8024790 описан механизм определения того, что URL-адрес является важным с точки зрения ввода информации пользователем с целью принятия дальнейших мер по обеспечению безопасности, что может быть невозможно в том случае, если данный адрес был скомпрометирован (фишинговый сайт) или не был отмечен пользователем как важный.

Однако стоит отметить, что в приведенных публикациях не раскрывается комплексный подход для обеспечения безопасных онлайн-платежей, так как каждая публикация решает одну из проблем, связанных с безопасным проведением онлайн-транзакций, однако оставляет нерешенными другие, что не позволяет утверждать, что на стороне пользователя можно безопасно провести онлайн-транзакции.

Анализ предшествующего уровня техники и возможностей, которые появляются при комбинировании существующих решений в одной системе, позволяют получить новый результат, а именно систему и способ обеспечения безопасности онлайн-транзакций.

Раскрытие изобретения

Технический результат настоящего изобретения заключается в обеспечении безопасности онлайн-транзакций.

Согласно одному из вариантов реализации для достижения данного технического результата применяется способ проведения онлайн-транзакций, при этом способ содержит этапы, на которых определяют начало

проведения онлайн-транзакции, производимой с помощью приложения, используемого для проведения онлайн-транзакций; организовывают защищенную среду для исключения возможной компрометации приложения, используемого для проведения онлайн-транзакций; обеспечивают защищенный ввод данных для защиты от возможного перехвата данных при их вводе в приложение, используемое для проведения онлайн-транзакций; обеспечивают защищенную передачу данных от приложения, используемого для проведения онлайн-транзакций, на сторону платежного сервиса при проведении онлайн-транзакций.

Согласно одному из частных вариантов реализации начало проведения онлайн-транзакций определяется на основании запуска приложения, используемого для проведения онлайн-транзакций.

Согласно другому частному варианту реализации начало проведения онлайн-транзакций определяется на основании обучения.

Согласно еще одному частному варианту реализации обучение включает отслеживание по крайней мере одного из: запросов к сетевым ресурсам, которые могут принадлежать финансовым организациям, для корректного определения их как

платежных сервисов; наличия в активном окне приложения элементов с возможностью ввода данных.

Согласно одному из частных вариантов реализации в качестве защищенной среды может использоваться одно из: песочница; защита запущенного процесса приложения, используемого для проведения онлайн-транзакции, с помощью проверки изменений в адресном пространстве процесса; отслеживание подозрительных операций при выполнении потоков запущенного процесса приложения, используемого для проведения онлайн-транзакции; использование виртуальной машины, в которой будет запущено приложение, используемое для проведения онлайн-транзакции; запуск другого приложения для реализации возможностей приложения, используемого для проведения онлайн-транзакции.

Согласно другому частному варианту реализации защищенный ввод данных обеспечивается в виде одного из: виртуальной клавиатуры, аппаратного средства ввода данных, защиты буфера обмена.

Согласно еще одному частному варианту реализации после определения начала проведения онлайн-транзакции дополнительно проводят оценку рисков онлайн-транзакции.

Согласно одному из частных вариантов реализации оценка рисков онлайн-транзакции включает по меньшей мере один из следующих критериев: уязвимости приложений, включая уязвимости приложения, используемого для проведения онлайн-транзакции; инциденты на компьютере, на котором установлено приложение, используемое для проведения онлайн-транзакции; инциденты в сети, в которой находится компьютер, на котором установлено приложение, используемое для проведения онлайн-транзакции; статус антивирусного программного обеспечения; использование аппаратных средств аутентификации; частота проведения онлайн-транзакций; поведение пользователя.

Согласно одному из вариантов реализации для достижения данного технического результата применяется система проведения онлайн-транзакции, при этом система содержит следующие средства: средство управления, предназначенное для определения начала проведения онлайн-транзакции, производимой с помощью приложения, используемого для проведения онлайн-транзакции, при этом средство управления связано со средством для защищенного ввода данных, защищенной средой, средством безопасной передачи данных; средство для защищенного ввода данных, предназначенное для защиты от возможного перехвата данных при их вводе в приложение, используемое для проведения онлайн-транзакции, при этом средство для защищенного ввода данных связано с защищенной средой; защищенная среда, предназначенная для исключения возможной компрометации приложения, используемого для проведения онлайн-транзакции, при этом защищенная среда связана со средством безопасной передачи данных; средство безопасной передачи данных, предназначенное для предотвращения возможного перехвата и изменения данных, передаваемых на сторону платежного сервиса при проведении онлайн-транзакции.

Согласно одному из частных вариантов реализации начало проведения онлайн-транзакции определяется на основании запуска приложения, используемого для проведения онлайн-транзакции.

Согласно другому частному варианту реализации начало проведения онлайн-транзакции определяется на основании обучения.

Согласно еще одному частному варианту реализации обучение включает отслеживание по крайней мере одного из: запросов к сетевым ресурсам, которые могут принадлежать финансовым организациям, для корректного определения их как

платежных сервисов; наличия в активном окне приложения элементов с возможностью ввода данных.

Согласно одному из частных вариантов реализации в качестве защищенной среды может использоваться одно из: песочница; защита запущенного процесса приложения, используемого для проведения онлайн-транзакции, с помощью проверки изменений в адресном пространстве процесса; отслеживание подозрительных операций при выполнении потоков запущенного процесса приложения, используемого для проведения онлайн-транзакции; использование виртуальной машины, в которой будет запущено приложение, используемое для проведения онлайн-транзакции; запуск другого приложения для реализации возможностей приложения, используемого для проведения онлайн-транзакции.

Согласно другому частному варианту реализации средство для защищенного ввода данных реализовано в виде одного из: виртуальной клавиатуры, аппаратного средства ввода данных, защиты буфера обмена.

Согласно еще одному частному варианту реализации дополнительно содержится средство оценки рисков для проведения оценки рисков онлайн-транзакции, при этом средство оценки рисков связано со средством управления.

Согласно одному из частных вариантов реализации оценка рисков онлайн-транзакции включает по меньшей мере один из следующих критериев: уязвимости, включая уязвимости приложения, используемого для проведения онлайн-транзакции; инциденты на компьютере, на котором установлено приложение, используемое для проведения онлайн-транзакции; инциденты в сети, в которой находится компьютер, на котором установлено приложение, используемое для проведения онлайн-транзакции; статус антивирусного программного обеспечения; использование аппаратных средств аутентификации; частота проведения онлайн-транзакций; поведение пользователя.

Краткое описание чертежей

Дополнительные цели, признаки и преимущества настоящего изобретения будут очевидными из прочтения последующего описания осуществления изобретения со ссылкой на прилагаемые чертежи, на которых:

На Фиг.1а приведена типичная схема проведения онлайн-транзакций.

Фиг.1б иллюстрирует возможные угрозы для проведения онлайн-транзакций.

Фиг.1в иллюстрирует набор необходимых средств для защиты онлайн-транзакций в рамках реализации настоящего изобретения.

Фиг.2 показывает систему для защиты онлайн-транзакций в рамках реализации настоящего изобретения.

Фиг.3 иллюстрирует способ работы настоящего изобретения.

Фиг.4 представляет пример компьютерной системы общего назначения, в рамках которой может быть реализовано настоящее изобретение.

Описание вариантов осуществления изобретения

Объекты и признаки настоящего изобретения, способы для достижения этих объектов и признаков станут очевидными посредством отсылки к примерным вариантам осуществления. Однако настоящее изобретение не ограничивается примерными вариантами осуществления, раскрытыми ниже, оно может воплощаться в различных видах. Сущность, приведенная в описании, является ничем иным, как конкретными деталями, необходимыми для помощи специалисту в области техники в исчерпывающем понимании изобретения, и настоящее изобретение определяется в объеме приложенной формулы.

На Фиг.1а приведена типичная схема проведения онлайн-транзакций. Пользователь

100, используя средство ввода ПО, вводит всю необходимую информацию в приложение 120 для проведений онлайн-транзакций. В качестве средства ввода ПО можно рассматривать такие устройства, как клавиатура, мышь, сенсорный экран, которые подразумевают ввод данных самим пользователем. Приложение 120 для проведения онлайн-транзакций может быть как браузером, в котором с определенной веб-страницы можно произвести онлайн-транзакцию, так и специализированным банковским клиентом, а также любым другим приложением, в котором есть функционал онлайн-транзакций (например, игровое приложение World of Warcraft имеет собственный сервис для покупки виртуальных вещей за деньги). Для того чтобы онлайн-транзакция могла быть успешно произведена, требуется подключение к сети Интернет 130, через которую можно осуществить перевод денежных средств с помощью платежного сервиса 140. В данном случае под платежным сервисом подразумевается вся инфраструктура для денежных транзакций, включая, например, инфраструктуру банка-эмитента платежной карты, исполняющего банка и любых других посредников.

Фиг.1б иллюстрирует возможные угрозы для проведения онлайн-транзакций. Одной из возможных угроз 110а являются вредоносные (чаще всего троянские) программы, такие как перехватчики ввода данных (англ. keyloggers), которые перехватывают ввод данных с клавиатуры или мыши, делают снимки экранов (англ. screenshots). Перехват ввода данных может быть реализован с помощью библиотеки (англ. Dynamic Load Library, DLL), которая устанавливает перехватчики событий. Слежение за клавиатурным вводом может происходить лишь в окнах с определенными заголовками (т.е. происходит целенаправленное отслеживание приложений 120). Собранную информацию о вводе вредоносная программа 110а сохраняет в отдельный файл, чтобы затем передать на сторону злоумышленника с помощью, например, электронной почты. Стоит отметить, что вредоносные программы 110а используют целый ряд технологий для сокрытия присутствия в системе (например, rootkit-технологии) или затруднения обнаружения антивирусными приложениями (например, используя обфускацию кода). Также угрозы 110а могут использовать системные перехватчики (например, для операционной системы Windows это могут быть перехватчики на API-функции HttpSendRequestW(), HttpSendRequestAQ, HttpOpenRequestA()) для отслеживания сетевых запросов от приложения 120.

Другой пример угроз представляет собой компрометация приложения 120 с помощью вредоносного функционала 110б. Данный функционал 110б может иметь различную природу, например это может быть заражение исполняемого файла приложения 120 вирусом или же это может быть добавление DLL-модуля (англ. Browser Helper Object, BHO) в процесс браузера. Другие варианты реализации функционала 110б могут быть основаны на использовании уязвимостей в приложении 120, внедрении в адресное пространство работающего процесса приложения 120 и т.д.

Еще одним примером компьютерных угроз являются вредоносные приложения 110в, которые направлены на перехват и подмену сетевого трафика от приложений 120. Перехват и подмена могут быть реализованы с помощью добавления поддельных SSL-сертификатов для определенных сайтов, добавления DNS-записей для сетевых настроек (LAN, Wi-Fi), изменения файла hosts и др. Данные подходы направлены на переадресацию пользователя (а точнее, приложения 120) не к платежному сервису 140, а к вредоносному веб-ресурсу 110г (как правило, это фишинговые сайты), который может иметь схожий функционал для проведения онлайн-транзакций, однако в этом случае средства пользователя 100 будут переведены на счета злоумышленников. Вредоносный веб-ресурс 110г также может иметь созвучные названия доменов платежных сервисов 140,

иметь одинаковый интерфейс, что может ввести пользователя 100 в заблуждение. Еще один вариант работы вредоносных приложений 110в заключается в изменении ответа от платежного сервиса 140, например, путем подмены вебстраницы или добавлении вредоносного сценария.

Перечисленные выше угрозы 110а-110г очень часто не работают как отдельные приложения, а выступают в виде целого комплекса связанных между собой угроз для проведения незаконных онлайн-транзакций. Это связано с тем, что также постоянно совершенствуются и средства защиты от подобных транзакций - банки и владельцы платежных сервисов 140 улучшают качество работы, добавляя, например, новые методы аутентификации пользователей, антивирусные компании постоянно добавляют новые методы обнаружения угроз 110а-110г. Однако даже если получается предотвратить работу или использование почти всех угроз, даже одна угроза может привести к тому, что будет проведена непредусмотренная онлайн-транзакция или у пользователя будут украдены его важные данные. Таким образом, требуется комплексное решение для обнаружения, нейтрализации или обхода существующих угроз 110а-110г.

Фиг.1в иллюстрирует набор необходимых средств для защиты онлайн-транзакций в рамках реализации настоящего изобретения. С целью избежать возможного перехвата данных через средства ввода 110 пользователю 100 предоставляется средство для защищенного ввода данных 120а. Как правило, такое средство реализуется в виде виртуальной клавиатуры (http://www.techopedia.com/definition/716/virtual-kevboard), которая может содержать ряд улучшений для дополнительной защиты от кейлоггеров, например, в виде защиты от снимков экрана (используя перехват и блокирование процессов снятия скриншотов, выполняемых без использования клавиши PrtScr на клавиатуре, а также других стандартных комбинаций клавиш: Alt + PrtScr; Ctrl + PrtScr). Другие варианты реализации средства для защищенного ввода данных 120а могут быть также аппаратными средствами ввода данных с реализацией отдельного драйвера в операционной системе (ОС) для перевода введенных данных со средства 120а в набор символов для приложения 120. Также реализация средства 120а может использовать подходы для защиты буфера обмена, например, контролируя передачу данных между разными процессами и процессом приложения 120. Например, средство 120а может блокировать доступ к буферу обмена для всех приложений, кроме приложения 120 и ряда выделенных процессов (например, процесса приложения Notepad или процесса переднего плана, откуда пользователь может скопировать необходимые данные).

Для того чтобы исключить возможную компрометацию приложения 120, используется защищенная среда 120б, которая может быть реализована в виде ряда технологий:

- Использование технологий песочницы (http://www.techopedia.com/detinition/27682/sandbox-computer-securitv).;
- Защита запущенного процесса приложения 120 с помощью проверки (запрета) изменений в адресном пространстве процесса (т.е. предотвращения внедрения кода), анализа запуска новых потоков в рамках процесса приложения 120 и т.д.;
- Отслеживание подозрительных операций при выполнении потоков запущенного процесса приложения 120. Подобное отслеживание может быть реализовано с помощью технологий, описанных в патентной заявке US 20110083176. В рамках этого подхода можно запрещать следующие операции к процессу приложения 120 со стороны других процессов: внедрение кода, прямой доступ к памяти, снятие снимков экрана, попытки обращения к дочерним процессам процесса приложения 120;
- Использование виртуальной машины, в которой будет запущено приложение 120;
- Запуск другого приложения для реализации возможностей приложения 120.

Например, в случае браузера это может быть использование упрощенной версии браузера, которая реализует минимальный набор функционала для проведения онлайн-транзакций (отправка и прием веб-запросов, отображение веб-страниц, авторизация и работа с SSL-протоколом и т.д.).

С целью избежать возможного перехвата и/или изменения данных, которые будут пересылаться приложением 120 через Интернет 130 к платежному сервису 140, может использоваться средство безопасной передачи данных 120в, которое позволяет выполнять следующие функции:

- Отслеживание и проверка доменного имени платежного сервиса 140 с целью выделения вредоносных веб-ресурсов 110 г. Базы данных вредоносных веб-ресурсов ведут многие разработчики антивирусных продуктов (например, компании McAfee, Symantec, Kaspersky Lab);
- Проверка цифровых сертификатов платежных сервисов с помощью подходов, описанных, например, в патенте US 7739494;
- Проверка содержимого (контента) платежного сервиса, например, с помощью технологии, раскрытой в патенте US 8370939.

Фиг.2 показывает систему для защиты онлайн-транзакций в рамках реализации настоящего изобретения. Пользователь 100 использует компьютер 200, на котором установлена ОС 210 для работы с приложениями 220, из которых как минимум одно приложение 120 позволяет проводить онлайн-транзакции. Средство оценки рисков 230 анализирует ОС 210 и приложение 120 на наличие уязвимостей, файлы настроек, список установленных драйверов и запущенных служб и другие данные, имеющие отношение к компьютерной безопасности, с целью определения риска при возможном проведении онлайн-транзакции. Оценка рисков может быть произведена с помощью ряда метрик, например с помощью Common Vulnerability Scoring System (CVSS), которая может включать детальную информацию об уязвимостях (критичность, возможные последствия использования уязвимости, способы устранения уязвимости). Примеры критериев для работы средства оценки рисков:

- Уязвимости (критичность, возможные последствия использования уязвимости), в том числе уязвимости приложения 120 для проведения онлайн-транзакций;
- Инциденты на локальном компьютере 200 (обнаружение вредоносных программ, сетевых атак, спама и т.д.);
- Инциденты в сети, в которой находится компьютер 200 (сетевые атаки, отказ в обслуживании и т.д.);
- Статус антивирусного программного обеспечения (время последнего обновления антивирусных баз, доступность антивирусных серверов для запросов и т.д.);
- Использование аппаратных средств аутентификации. При использовании подобных средств возможность компрометации онлайн-транзакции падает, следовательно, риски уменьшаются;
- Частота проведения онлайн-транзакций. При повышении частоты онлайн-транзакций со стороны пользователя, как правило, возрастает риск проведения несанкционированных транзакций, которые пользователь может заметить не сразу ввиду большого количества транзакций;
- Поведение пользователя, которое может характеризовать его как пользователя с риском заражения неизвестными вредоносными программами. Один из подходов, описанный в патенте US 8312536, оценивает репутацию пользователя на основании репутации данных, которыми пользователь оперирует во время своей работы, например файлов или сайтов. Чем больше среди таких данных встречается вредоносных, тем

более худшей может оказаться репутация пользователя, что повышает риск при проведении онлайн-транзакции.

В одном из вариантов реализации средство оценки рисков может лишь закрывать найденные уязвимости путем скачивания и установки обновлений (патчей) для уязвимых приложений, изменять настройки работы приложения для уменьшения риска при проведении онлайн-транзакций.

Ниже приведены основные риски, связанные с проведением онлайн-транзакций:

- Потеря личных данных, таких как идентификационная информация пользователя;
- Некорректное проведение текущей онлайн-транзакции;
- Получение несанкционированного доступа третьих лиц к средствам хранения и проведения онлайн-транзакций, например, к приложениям 120, электронным кошелькам (англ. digital wallet).

Средство оценки рисков 230 может вычислять риск проведения онлайн-транзакций согласно определенным метрикам, при этом величина риска может быть выражено в виде числа или определенного значения. Пример рисков приведен ниже в таблице 1.

Таблица 1.

Условия	Риск (число)	Риск (значение)
Приложение 120 выполнено в виде отдельного приложения для проведения определенного вида онлайн-транзакций; Аппаратное подтверждение онлайн-транзакций; Антивирусное приложение имеет последнюю версию антивирусных баз.	1	Низкий
Приложение 120 выполнено в виде браузера; Подтверждение транзакций происходит через ввод данных с клавиатуры пользователем; Антивирусное приложение имеет последнюю версию антивирусных баз.	2	Средний
Приложение 120 выполнено в виде браузера; Подтверждение транзакций происходит через ввод данных с клавиатуры пользователем; Антивирусное приложение имеет устаревшую версию антивирусных баз; Определен ряд инцидентов, связанных с вредоносными программами.	3	Высокий

После того как средство оценки рисков 230 определило риски проведения онлайн-транзакций, оно передает эту информацию на сторону средства управления 240, которое регулирует работу средства для защищенного ввода данных 120а, защищенной среды 120б и средства безопасной передачи данных 120в. В зависимости от полученной информации, средство управления 240 может настроить вышеупомянутые средства следующим образом:

- средство для защищенного ввода данных 120а может быть как отключено (если не требуется использовать ввод данных от самого пользователя, например, при использовании аппаратных средств подтверждения онлайн-транзакций), так и включено, в зависимости от ряда условий, куда входит информация о приложении 120 (тип приложения, наличие уязвимостей, необходимость ввода данных и т.д.), ОС 210 и т.д.;
- защищенная среда 120б может использовать различные подходы для защиты приложения 120 (использование песочницы или виртуальной машины, контроль выполнения потоков процесса и др.), при этом чем выше уровень риска, тем более надежная используется защищенная среда 120б (например, при высоком уровне риска может использоваться отдельная виртуальная машина, сетевые соединения будут устанавливаться через отдельное VPN-соединение, в то время как при низком уровне риска защищенная среда может отсутствовать вовсе);
- средство безопасной передачи данных 120в может оперировать не только уровнем риска для проверки передаваемых данных, но и информацией об используемом приложении 120 (например, при использовании браузера будут проверены URL-адреса, по которым происходит обращение при проведении онлайн-транзакций, цифровые

сертификаты сайтов платежного сервиса 140 и т.д.).

Стоит отметить, что все настройки средства для защищенного ввода данных 120а, защищенной среды 120б и средства безопасной передачи данных 120в могут быть изменены самим пользователем или администратором для упрощения процедуры проведения онлайн-транзакций. С этой целью средство управления 240 может иметь собственный интерфейс (англ. Graphics User Interface, GUI). В предпочтительном варианте реализации средство управления 240, средство для защищенного ввода данных 120а, защищенная среда 120б, средство безопасной передачи данных 120в, средство оценки рисков 230 реализованы в виде отдельного приложения или же могут входить в состав антивирусного приложения. Средство управления 240 также предназначено для определения начала онлайн-транзакции для активации работы средства для защищенного ввода данных 120а, защищенной среды 120б, средства безопасной передачи данных 120в, средства оценки рисков 230 как по отдельности для каждого средства из перечисленных, так и всех вместе.

Для получения информации об уязвимостях, вредоносных приложениях и другой информации, касающейся безопасности онлайн-транзакций, средство управления 240 связывается с репутационным сервисом 250. Подобные сервисы могут быть реализованы в виде удаленного облачного сервиса или в виде локальной базы данных, которая содержит следующую информацию:

- информацию об уязвимостях;
- фишинговую базу сайтов;
- базу данных цифровых сертификатов;
- эвристические правила обнаружения фишинговых сайтов платежных сервисов, а также вредоносных сценариев, которые могут быть выполнены при обращении к подобным сайтам;
- правила настройки средств 120а-120в.

Фиг.3 иллюстрирует способ работы настоящего изобретения. На этапе 310 происходит определение начала онлайн-транзакции, которое может быть основано на:

- запуске приложения 120;
- определении момента начала онлайн-транзакции через приложение 120;
- выборе пользователя (пользователь может самостоятельно выбирать режим защиты онлайн-транзакции с помощью настоящей системы).

Примером момента начала онлайн-транзакции в случае веб-браузера могут служить следующие признаки: открытие известной веб-страницы платежного сервиса 140 (в случае онлайн-банкинга это будет сайт банка), установка https-соединения, наличие на странице характерных полей для ввода данных (логин-пароль).

Момент начала транзакции может задавать сам пользователь также в тех случаях, когда требуется обучение для определения в будущем аналогичных случаев. Для обучения могут использоваться следующие факторы:

- запросы к сетевым ресурсам, которые могут принадлежать финансовым организациям (например, к сайтам банков) для корректного определения их как платежных сервисов 140 в будущем. В случае браузера это может быть обращение к таким сайтам, как ebay.com, walmart.com, bestbuy.com, newegg.com и другим аналогичным;
- наличие в активном окне приложения 120 элементов с возможностью ввода данных, при этом элементы могут иметь характерные имена (идентификатор, логин, пароль, ID и т.д.) и содержать другие указывающие на возможность ввода данных свойства (например, для HTML-элемента ввод пароля в текстовое поле также содержит значение type="password");

- информация о приложении 120, которая определяет его как приложение для проведения онлайн-транзакций. Например, для отдельного банковского клиента по цифровой подписи можно удостовериться, что цифровая подпись принадлежит банку, что будет говорить о том, что данный клиент с большой долей вероятности будет использоваться для онлайн-транзакций.

После того как было определено начало онлайн-транзакции на этапе 310, следует опциональный шаг по определению рисков онлайн-транзакции на этапе 320. На этом этапе также может быть произведено снижение рисков онлайн-транзакции путем установки обновлений с целью закрытия уязвимостей или оповещение пользователя о риске. Далее на этапе 330 происходит организация защищенной среды для приложения 120. Данный этап может быть осуществлен заранее, еще до начала онлайн-транзакции. Затем на этапе 340 пользователь вводит данные для онлайн-транзакции, используя средство для защищенного ввода данных 120а. Для защищенной передачи данных по сети на этапе 350, помимо вышеперечисленных подходов (проверка доменных имен, цифровых сертификатов и т.д.), может также использоваться установление защищенного соединения (например, VPN-соединения), куда будет инкапсулировано текущее соединение к платежному сервису 140. После того как все данные были переданы и транзакция была завершена, на этапе 360 система прекращает свою работу. Стоит отметить, что этапы 330-350 необязательно должны следовать именно в такой последовательности, как отображено на Фиг.3, например, сначала может проверяться информация о платежном сервисе 140, к которому пытается обратиться приложение 120, и лишь затем будет происходить обеспечение защищенной среды и защищенный ввод данных.

В одном из вариантов реализации для защиты веб-банкинга с использованием браузера способ работы настоящего изобретения может выглядеть следующим образом:

- Открытие интернет-соединения;
- Проверка соответствия запрашиваемой веб-страницы сайту банка;
- Установление подлинности ресурса путем проверки цифрового сертификата;
- Анализ наличия уязвимостей в ОС 210;
- Блокирование использования веб-страницы банка в незащищенном режиме;
- Запуск защищенного браузера, в котором отображается только поле, требуемое для входа в веб-банкинг;
- Защита ввода данных пользователя во время сеанса работы с веб-банкингом;
- Завершение защищенной сессии при закрытии браузера.

Фиг.4 представляет пример компьютерной системы общего назначения, персональный компьютер или сервер 20, содержащий центральный процессор 21, системную память 22 и системную шину 23, которая содержит разные системные компоненты, в том числе память, связанную с центральным процессором 21. Системная шина 23 реализована, как любая известная из уровня техники шинная структура, содержащая в свою очередь память шины или контроллер памяти шины, периферийную шину и локальную шину, которая способна взаимодействовать с любой другой шинной архитектурой. Системная память содержит постоянное запоминающее устройство (ПЗУ) 24, память с произвольным доступом (ОЗУ) 25. Основная система ввода/вывода (BIOS) 26 содержит основные процедуры, которые обеспечивают передачу информации между элементами персонального компьютера 20, например, в момент загрузки операционной системы с использованием ПЗУ 24.

Персональный компьютер 20 в свою очередь содержит жесткий диск 27 для чтения и записи данных, привод магнитных дисков 28 для чтения и записи на сменные

магнитные диски 29 и оптический привод 30 для чтения и записи на сменные оптические диски 31, такие как CD-ROM, DVD-ROM и иные оптические носители информации. Жесткий диск 27, привод магнитных дисков 28, оптический привод 30 соединены с системной шиной 23 через интерфейс жесткого диска 32, интерфейс магнитных дисков 33 и интерфейс оптического привода 34 соответственно. Приводы и соответствующие компьютерные носители информации представляют собой энергонезависимые средства хранения компьютерных инструкций, структур данных, программных модулей и прочих данных персонального компьютера 20.

Настоящее описание раскрывает реализацию системы, которая использует жесткий диск 27, сменный магнитный диск 29 и сменный оптический диск 31, но следует понимать, что возможно применение иных типов компьютерных носителей информации 56, которые способны хранить данные в доступной для чтения компьютером форме (твердотельные накопители, флеш-карты памяти, цифровые диски, память с произвольным доступом (ОЗУ) и т.п.), которые подключены к системной шине 23 через контроллер 55.

Компьютер 20 имеет файловую систему 36, где хранится записанная операционная система 35, а также дополнительные программные приложения 37, другие программные модули 38 и данные программ 39. Пользователь имеет возможность вводить команды и информацию в персональный компьютер 20 посредством устройств ввода (клавиатуры 40, манипулятора «мышь» 42). Могут использоваться другие устройства ввода (не отображены): микрофон, джойстик, игровая консоль, сканнер и т.п. Подобные устройства ввода по своему обычаю подключают к компьютерной системе 20 через последовательный порт 46, который в свою очередь подсоединен к системной шине, но могут быть подключены иным способом, например, при помощи параллельного порта, игрового порта или универсальной последовательной шины (USB). Монитор 47 или иной тип устройства отображения также подсоединен к системной шине 23 через интерфейс, такой как видеоадаптер 48. В дополнение к монитору 47, персональный компьютер может быть оснащен другими периферийными устройствами вывода (не отображены), например, колонками, принтером и т.п.

Персональный компьютер 20 способен работать в сетевом окружении, при этом используется сетевое соединение с другим или несколькими удаленными компьютерами 49. Удаленный компьютер (или компьютеры) 49 являются такими же персональными компьютерами или серверами, которые имеют большинство или все упомянутые элементы, отмеченные ранее при описании существа персонального компьютера 20, представленного на Фиг.4. В вычислительной сети могут присутствовать также и другие устройства, например, маршрутизаторы, сетевые станции, пиринговые устройства или иные сетевые узлы.

Сетевые соединения могут образовывать локальную вычислительную сеть (LAN) 50 и глобальную вычислительную сеть (WAN). Такие сети применяются в корпоративных компьютерных сетях, внутренних сетях компаний и, как правило, имеют доступ к сети Интернет. В LAN- или WAN-сетях персональный компьютер 20 подключен к локальной сети 50 через сетевой адаптер или сетевой интерфейс 51. При использовании сетей персональный компьютер 20 может использовать модем 54 или иные средства обеспечения связи с глобальной вычислительной сетью, такой как Интернет. Модем 54, который является внутренним или внешним устройством, подключен к системной шине 23 посредством последовательного порта 46. Следует уточнить, что сетевые соединения являются лишь примерными и не обязаны отображать точную конфигурацию сети, т.е. в действительности существуют иные способы установления соединения

техническими средствами связи одного компьютера с другим.

В заключение следует отметить, что приведенные в описании сведения являются примерами, которые не ограничивают объем настоящего изобретения, определенного формулой.

Формула изобретения

Реализуемая компьютером система проведения онлайн-транзакции, при этом система содержит следующие средства:

а) средство управления, предназначенное для определения начала проведения онлайн-транзакции, производимой с помощью приложения, используемого для проведения онлайн-транзакции, настройки средства для защищенного ввода данных, защищенной среды и средства безопасной передачи данных, и при этом средство управления связано со средством для защищенного ввода данных, защищенной средой, средством безопасной передачи данных и средством оценки рисков, при этом начало проведения онлайн-транзакции определяется на основании обучения, которое включает отслеживание по крайней мере одного из: запросов к сетевым ресурсам, которые могут принадлежать финансовым организациям, для корректного определения их как платежных сервисов; наличия в активном окне приложения элементов с возможностью ввода данных;

б) средство оценки рисков для оценки рисков онлайн-транзакции и передачи указанной информации об упомянутой оценке рисков средству управления, при этом оценка рисков онлайн-транзакции включает по меньшей мере один из следующих критериев:

- уязвимости приложений, включая уязвимости приложения, используемого для проведения онлайн-транзакции;
- инциденты на компьютере, на котором установлено приложение, используемое для проведения онлайн-транзакции;
- инциденты в сети, в которой находится компьютер, на котором установлено приложение, используемое для проведения онлайн-транзакции;
- статус антивирусного программного обеспечения;
- использование аппаратных средств аутентификации;
- частота проведения онлайн-транзакций;
- поведение пользователя;

в) средство для защищенного ввода данных, предназначенное для защиты от возможного перехвата данных при их вводе в приложение, используемое для проведения онлайн-транзакции, при этом средство для защищенного ввода данных связано с защищенной средой, при этом средство для защищенного ввода данных обеспечивается в виде одного из: виртуальной клавиатуры, аппаратного средства ввода данных, защиты буфера обмена;

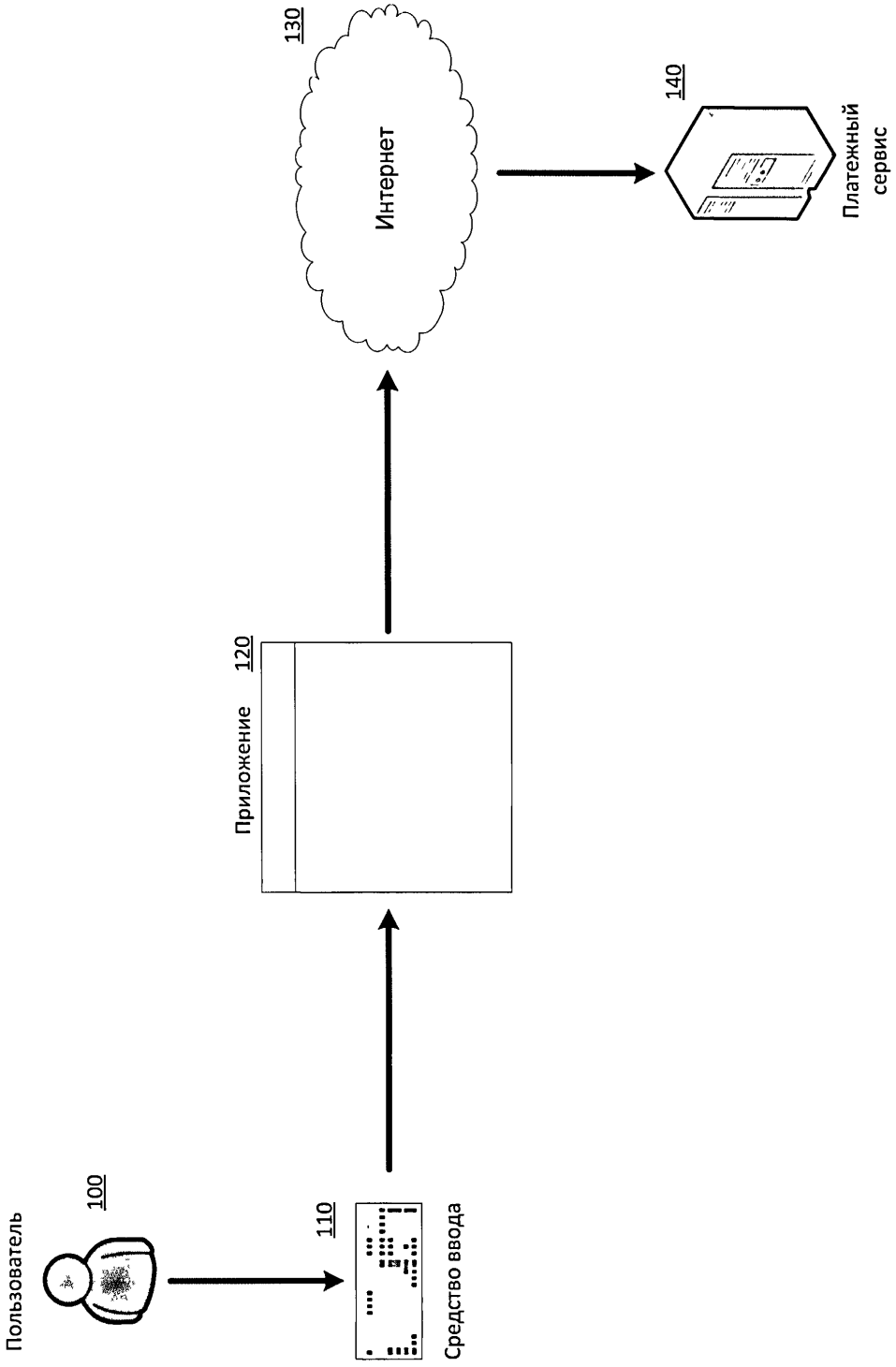
г) защищенная среда, предназначенная для исключения возможной компрометации приложения, используемого для проведения онлайн-транзакции, при этом защищенная среда связана со средством безопасной передачи данных, при этом в качестве защищенной среды может использоваться одно из:

- песочница;
- защита запущенного процесса приложения, используемого для проведения онлайн-транзакции, с помощью проверки изменений в адресном пространстве процесса;
- отслеживание подозрительных операций при выполнении потоков запущенного процесса приложения, используемого для проведения онлайн-транзакции;

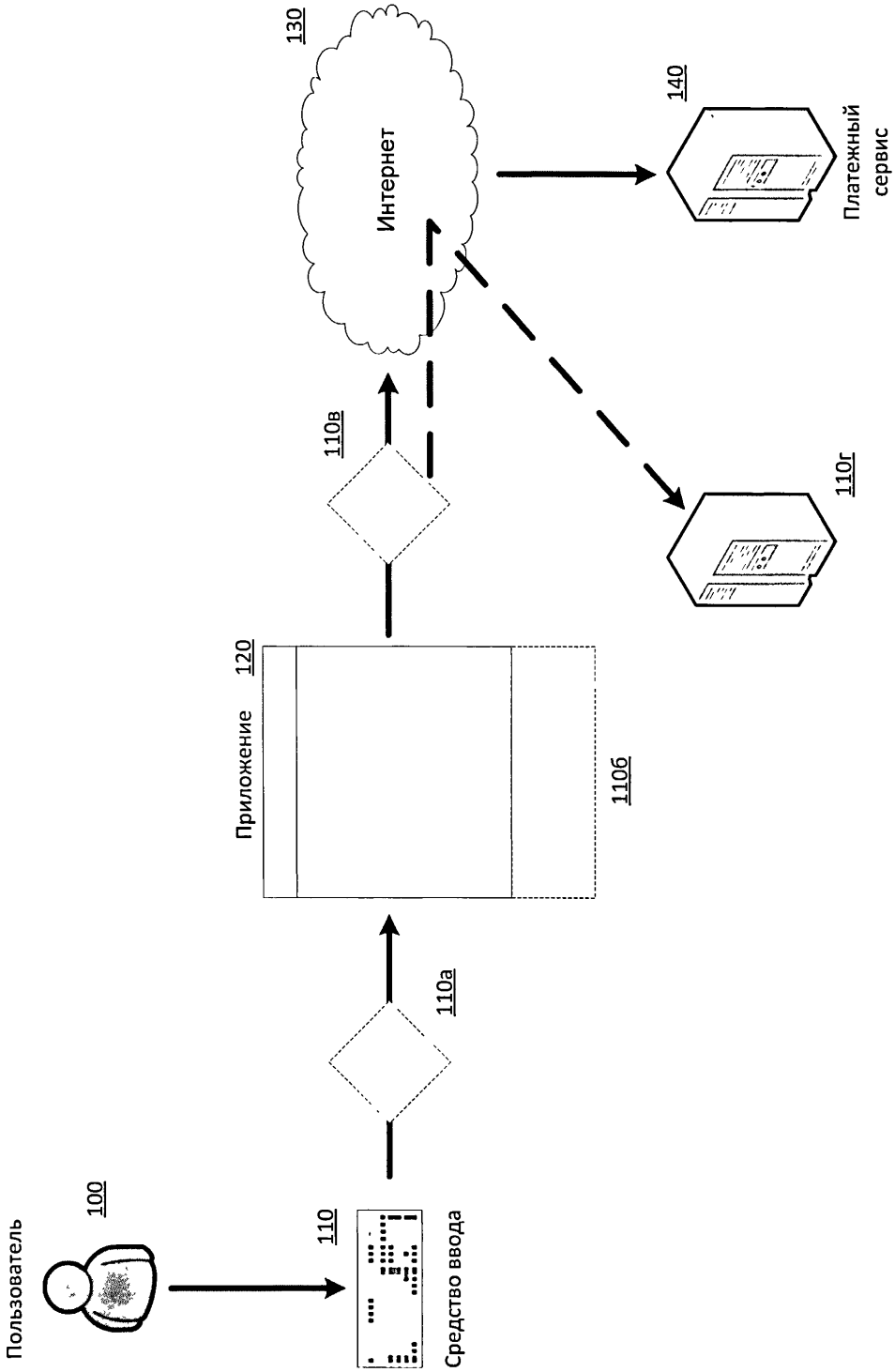
- использование виртуальной машины, в которой будет запущено приложение, используемое для проведения онлайн-транзакции;

- запуск другого приложения для реализации возможностей приложения, используемого для проведения онлайн-транзакции;

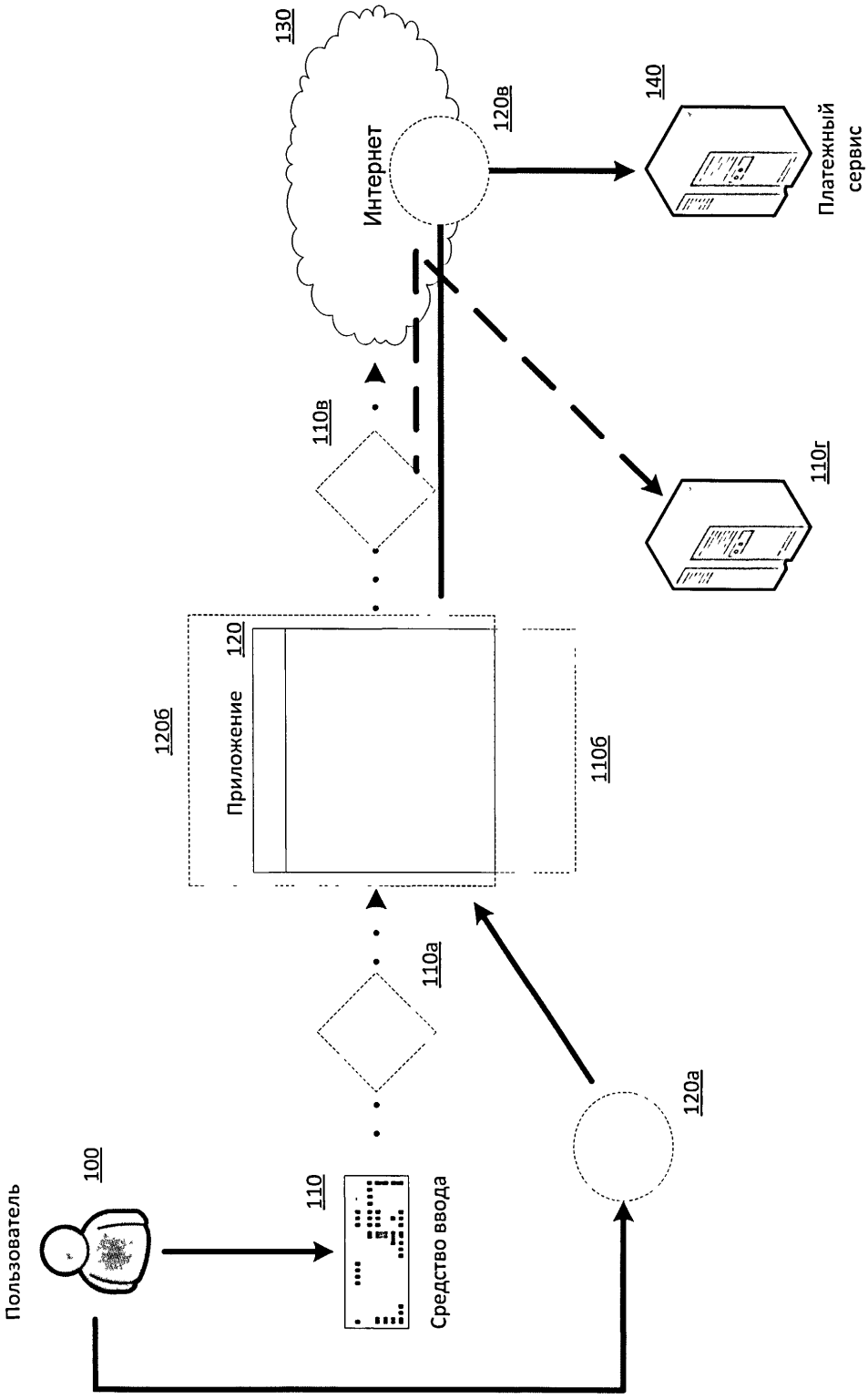
д) средство безопасной передачи данных, предназначенное для предотвращения возможного перехвата и изменения данных, передаваемых на сторону платежного сервиса при проведении онлайн-транзакции.


Пользователь
100
110
Средство ввода
Приложение
120
130
Интернет
140
Платежный сервис

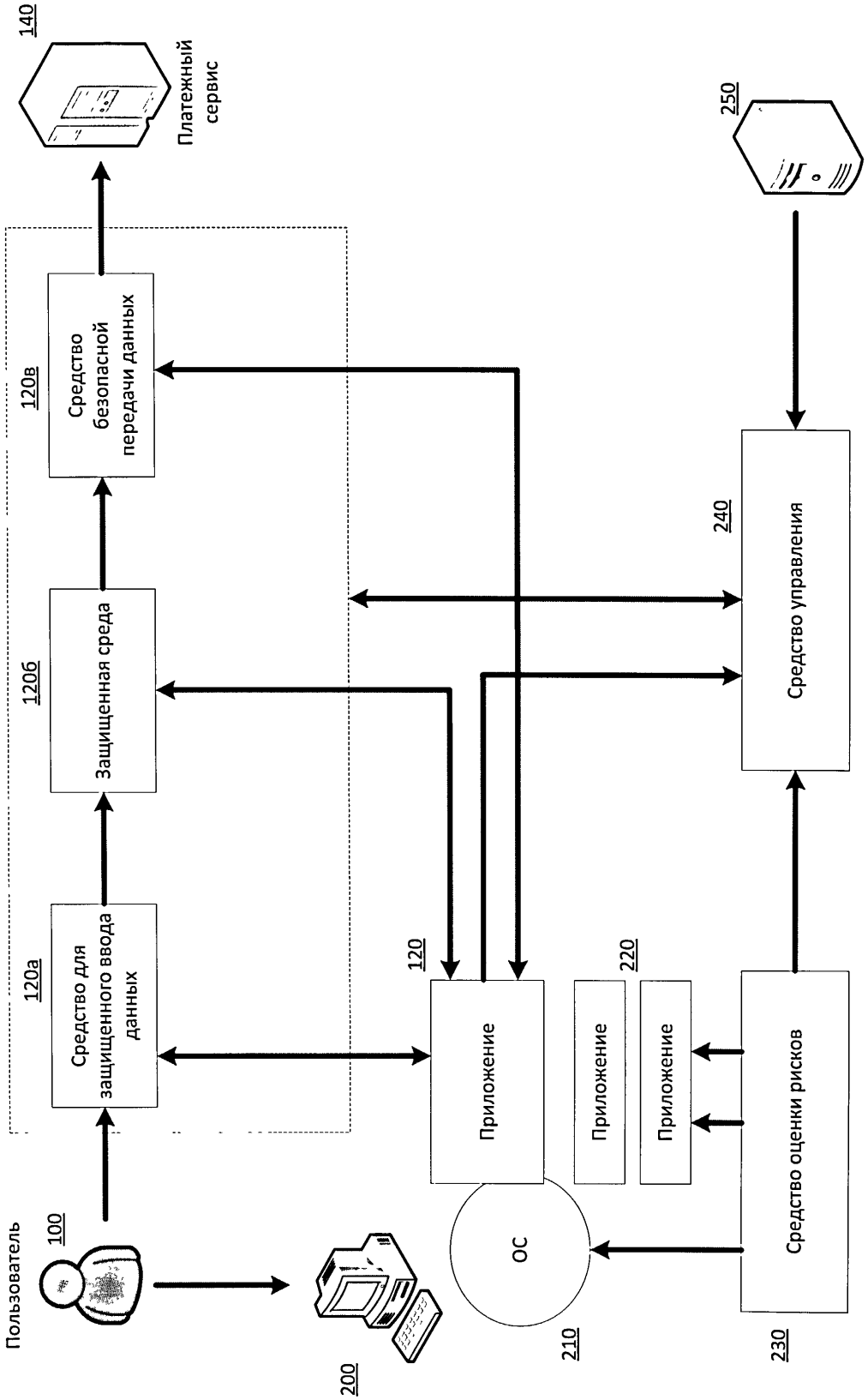
Фиг. 1а


Пользователь
100
110
Средство ввода
110а
Приложение
120
1106
110в
130
Интернет
140
Платежный сервис
110г

Фиг. 1б


130
Интернет
120в
140
Платежный сервис
110в
110г
120
Приложение
1206
1106
110а
120а
100
Пользователь
110
Средство ввода

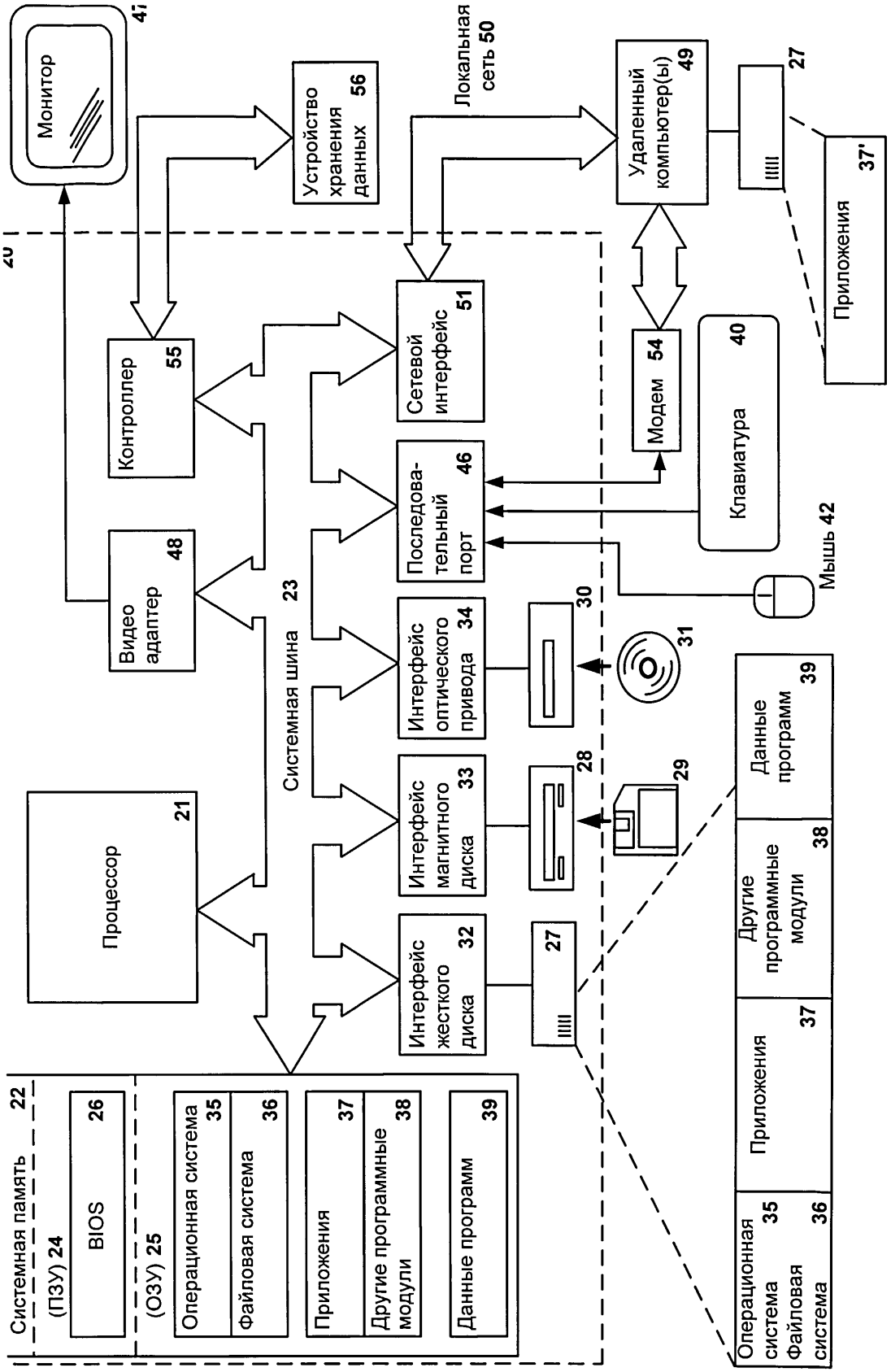
Фиг. 1в


140
Платежный сервис
250
120в
Средство безопасной передачи данных
240
Средство управления
1206
Защищенная среда
120а
Средство для защищенного ввода данных
120
Приложение
220
Приложение
Приложение
Пользователь
100
ОС
Средство оценки рисков
200
210
230

Фиг. 2


Определение начала проведения онлайн-транзакции
310
Определение рисков проведения транзакции
320
Организация защищенной среды для приложения
330
Обеспечение защищенного ввода данных
340
Обеспечение защищенной передачи данных
350
Завершение транзакции
360

Фиг. 3


Монитор
47
Устройство хранения данных 56
Локальная сеть 50
Удаленный компьютер(ы) 49
27
Приложения 37'
Сетевой интерфейс 51
Контроллер 55
Модем 54
Клавиатура 40
Последовательный порт 46
Видео адаптер 48
Мышь 42
Системная шина 23
Интерфейс оптического привода 34
30
31
Процессор 21
Интерфейс магнитного диска 33
28
29
Данные программ 39
Другие программные модули 38
Интерфейс жесткого диска 32
27
Приложения 37
Операционная система 35
Файловая система 36
Системная память 22
(ПЗУ) 24
BIOS 26
(ОЗУ) 25
Операционная система 35
Файловая система 36
Приложения 37
Другие программные модули 38
Данные программ 39

Фиг. 4