РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 635 276**(13) **C1**

(51) МПК
G06F 21/31 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2016125283, 24.06.2016**

(24) Дата начала отсчета срока действия патента:
24.06.2016

Дата регистрации:
09.11.2017

Приоритет(ы):
(22) Дата подачи заявки: **24.06.2016**

(45) Опубликовано: **09.11.2017** Бюл. № **31**

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

(72) Автор(ы):
Петровичев Дмитрий Леонидович (RU),
Баранов Артем Олегович (RU),
Гончаров Евгений Викторович (RU)

(73) Патентообладатель(и):
Акционерное общество "Лаборатория Касперского" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2386220 C2, 10.04.2010. EA 12094 B1, 28.08.2009. RU 2583710 C2, 10.05.2016. WO 2012/079170 A1, 21.06.2012. US 8528076 B2, 03.09.2013.**

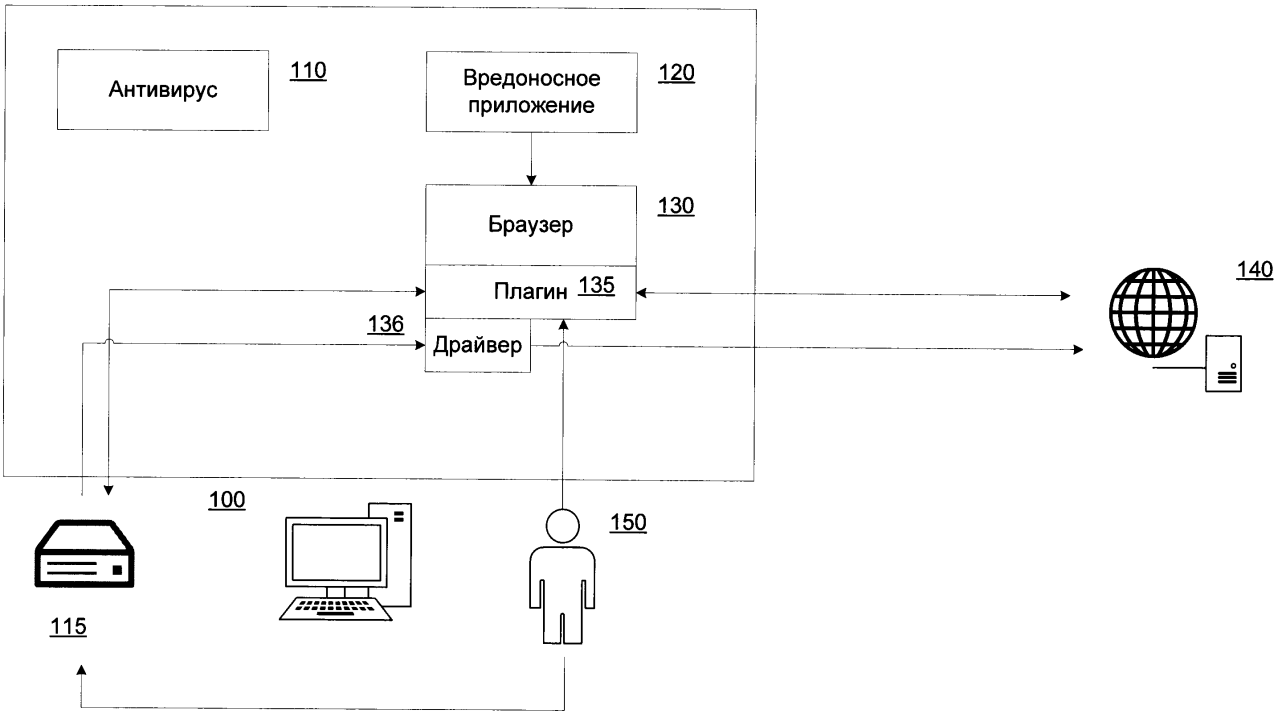
(54) Безопасная аутентификация по логину и паролю в сети Интернет с использованием дополнительной двухфакторной аутентификации

(57) Реферат:

Изобретение относится к области защиты данных от несанкционированного доступа, а более конкретно, к системам безопасной аутентификации. Техническим результатом является обеспечение защищенной передачи данных пользователя на сайт в сети Интернет. Система для защищенной передачи аутентификационных данных пользователя на сайт в сети Интернет содержит следующие средства: плагин в браузере, установленный на компьютере пользователя, при этом плагин предназначен для определения, что пользователь с помощью упомянутого браузера произвел соединение с сайтом, при взаимодействии с которым требуется защищать получаемые и передаваемые аутентификационные данные (далее - защищаемый сайт), и передачи информации о том, что произошло соединение с защищаемым сайтом, антивирусному приложению; антивирусное приложение, установленное на упомянутом компьютере, предназначенное для проверки операционной системы, установленной на упомянутом компьютере, на наличие уязвимостей и вредоносных приложений после получения упомянутой информации от плагина и передачи информации о проведенной проверке, а также информации, полученной от плагина, на устройство для безопасной передачи данных, и применения настроек безопасного канала передачи данных; устройство для безопасной передачи данных, предназначенное для: выбора настроек безопасного канала передачи данных между устройством для безопасной передачи данных и защищаемым сайтом на основании информации о проведенной антивирусным приложением проверке, передачи по безопасному каналу передачи данных между устройством для безопасной передачи данных и защищаемым сайтом аутентификационных данных пользователя на защищаемый сайт для аутентификации на данном сайте, при этом передача происходит на основании информации о том, что пользователь с помощью браузера произвел соединение с защищаемым сайтом, при этом аутентификационные данные хранятся на устройстве для безопасной передачи данных в зашифрованном виде. 2 н. и 6 з.п. ф-лы, 5 ил.

RU 2635276 C1

RU 2635276 C1



Фиг. 2

RU 2635276 C1

RU 2635276 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 635 276**(13) **C1**

(51) Int. Cl.
G06F 21/31 (2013.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2016125283, 24.06.2016**

(24) Effective date for property rights:
24.06.2016

Registration date:
09.11.2017

Priority:
(22) Date of filing: **24.06.2016**

(45) Date of publication: **09.11.2017** Bull. № **31**

Mail address:
125212, Moskva, Leningradskoe sh., 39a, str. 3, AO Laboratoriya Kasperskogo, Upravlenie po intellektualnoj sobstvennosti, Nadezhda Vasilevna Kashchenko

(72) Inventor(s):
Petrovichev Dmitrij Leonidovich (RU),
Baranov Artem Olegovich (RU),
Goncharov Evgenij Viktorovich (RU)

(73) Proprietor(s):
Aktsionernoe obshchestvo "Laboratoriya Kasperskogo" (RU)

RU 2635276 C1

(54) SAFE AUTHENTICATION WITH LOGIN AND PASSWORD IN INTERNET NETWORK USING ADDITIONAL TWO-FACTOR AUTHENTICATION

(57) Abstract:

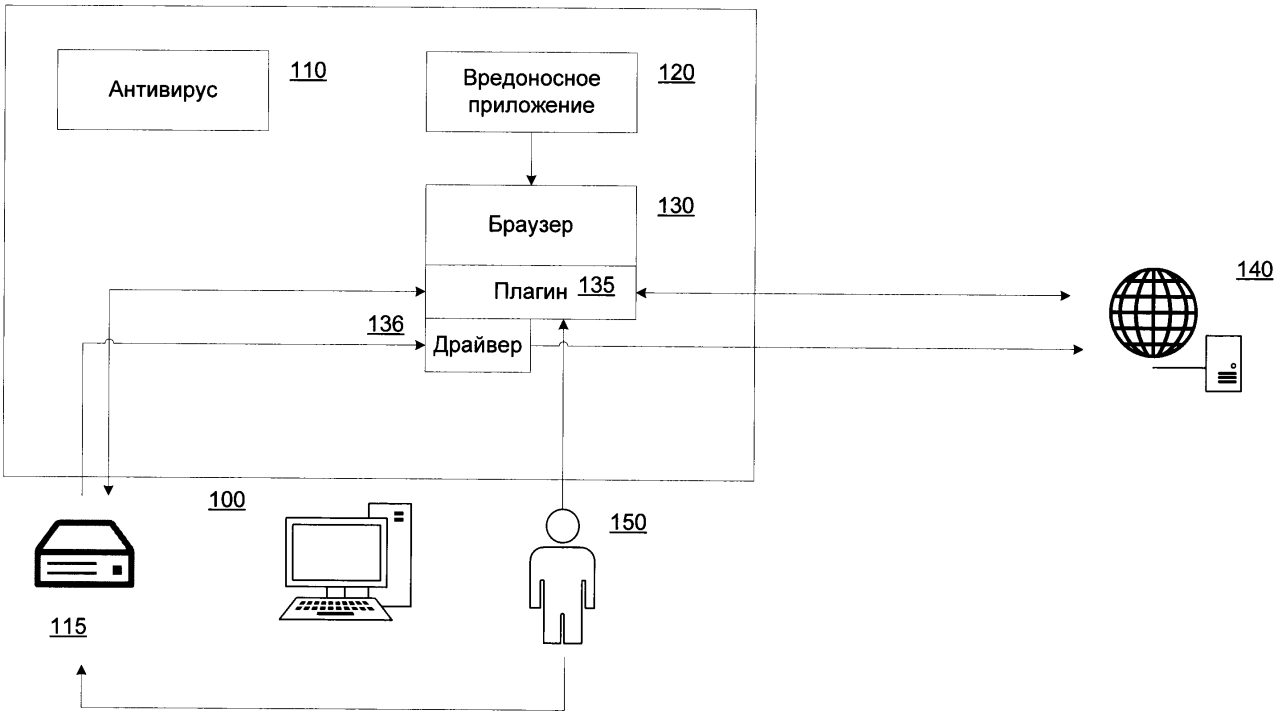
FIELD: information technology.

SUBSTANCE: system for secure transfer of user authentication data to an Internet site contains the following means: a plug-in in the browser installed on the user's computer, wherein the plugin is intended to determine that the user has made a connection to the site, which requires protection of the received and transmitted authentication data (hereinafter - the protected site) by means of the said browser, and transmission of information that a connection has occurred to the protected site to the anti-virus application; an anti-virus application installed on the computer to check the operating system installed on the computer for the presence of vulnerabilities and malicious applications after reception of the information from the plug-in and transmission of information about the check performed, as well as information received from the plug-in to the device for secure data transmission, and application of secure data channel settings; a device for secure data transmission, designed to: select the settings for the secure data channel between the device for secure data transmission and the protected site based on the information about the check performed by the anti-virus application, authentication data transmission via the secure data channel between the device for secure data transmission and the protected site for authentication on this site, with the transmission being based on information that the user has connected to the protected site using the browser, at that the authentication data is stored on the device for secure data transmission and encrypted.

EFFECT: provision of secure transmission of user data to an Internet site.

8 cl, 5 dwg

RU 2635276 C1



Фиг. 2

RU 2635276 C1

RU 2635276 C1

Область техники

Изобретение относится к технологиям защиты данных от несанкционированного доступа, а более конкретно, к системам безопасной аутентификации.

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 (приложения), которые особенно популярны на мобильных платформах. Среди других приложений, связанных с онлайн-транзакциями, можно отметить системы электронной валюты, как, например, WebMoney или PayPall, 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 (мошеннического) перевода средств. Как правило, кражу подобных данных осуществляют с помощью вредоносных программ (другой вариант - использование фишинга), 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 и последующей установки вредоносного программного обеспечения.

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 программно-аппаратные решения, которые вводят дополнительные факторы аутентификации, например отправка одноразового пароля (англ. One Time Password, OTP) на мобильный телефон пользователя или использование аппаратных устройств для аутентификации пользователя, однако они также могут быть уязвимы. Одним из примеров вредоносных программ, которые могут перехватывать OTP, является вредоносная программа Zeus. Таким образом, требуются технологии, которые могут

защитить данные пользователя во время транзакции от перехвата.

Например, в патенте US 9282094 упоминается отдельное устройство, которое работает при онлайн-транзакции. Оно может выполнять функции анализа безопасности при транзакции, а также служить для аутентификации. Однако даже такое решение не позволяет избежать кражи аутентификационных данных пользователя во время их ввода на компьютере.

Анализ предшествующего уровня техники позволяет сделать вывод о неэффективности и в некоторых случаях о невозможности применения предшествующих технологий, недостатки которых решаются настоящим изобретением, а именно системой безопасной аутентификации.

Раскрытие изобретения

Технический результат заключается в обеспечении защищенной передачи данных пользователя на сайт в сети Интернет.

Настоящий технический результат достигается с помощью системы аутентификации, которая содержит следующие средства: плагин в браузере, установленный на компьютере пользователя, при этом плагин предназначен для определения, что пользователь с помощью упомянутого браузера произвел соединение с сайтом, при взаимодействии с которым требуется защищать получаемые и передаваемые аутентификационные данные (далее - защищаемый сайт), и передачи информации о том, что произошло соединение с защищаемым сайтом, антивирусному приложению; антивирусное приложение, установленное на упомянутом компьютере, предназначенное для проверки операционной системы, установленной на упомянутом компьютере, на наличие уязвимостей и вредоносных приложений после получения упомянутой информации от плагина и передачи информации о проведенной проверке, а также информации, полученной от плагина, на устройство для безопасной передачи данных, и применения настроек безопасного канала передачи данных; устройство для безопасной передачи данных, предназначенное для: выбора настроек безопасного канала передачи данных на основании информации о проведенной антивирусным приложением проверке, передачи аутентификационных данных на защищаемый сайт для аутентификации на данном сайте, при этом передача происходит на основании информации о том, что пользователь с помощью браузера произвел соединение с защищаемым сайтом, при этом аутентификационные данные хранятся на устройстве для безопасной передачи данных в зашифрованном виде.

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:

Фиг. 1 иллюстрирует процесс доступа пользователя к сайту в Интернете в условиях недоверенной среды.

Фиг. 2 показывает пример работы настоящего изобретения для доступа пользователя к сайту в Интернете в условиях недоверенной среды.

Фиг. 3 показывает способ работы настоящего изобретения.

Фиг. 4 приводит пример работы способа настоящего изобретения.

Фиг. 5 представляет пример компьютерной системы общего назначения, с помощью 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 не чем 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. 1 отображен процесс доступа пользователя к сайту в Интернете в условиях недоверенной среды. Недоверенной средой считается компьютерная система 100, на которой даже в случае установки антивирусного приложения 110 сохраняется риск присутствия вредоносного приложения 120, которое может скомпрометировать работу пользователя 150 с защищаемым сайтом 140 (т.е. с сайтом, при взаимодействии с которым требуется защищать получаемые и передаваемые данные) через браузер 130. Антивирусное приложение 110 предназначено для проверки операционной системы, установленной на упомянутом компьютере, на наличие уязвимостей и вредоносных приложений. Результатом антивирусной проверки является следующий статус: какие и сколько было обнаружено вредоносных программ и уязвимостей. Как было отмечено в уровне техники, антивирусные технологии для поиска и обнаружения вредоносных приложений не могут гарантировать обнаружения и удаления всех вредоносных приложений по той причине, что создатели последних постоянно работают над методами обхода антивирусных проверок. Например, известны методы обфускации исполняемого кода для затруднения сигнатурного и эвристического анализов, а также методы антиэмуляции, которые позволяют избежать обнаружения вредоносного приложения во время его эмуляции с помощью антивирусного приложения. Таким образом, требуется решение, которое использует методы защиты получаемых и передаваемых данных с сайта 140.

Фиг. 2 показывает пример работы настоящего изобретения для доступа пользователя к сайту в Интернете в условиях недоверенной среды. По сравнению с Фиг. 1 добавляются устройство для безопасной передачи данных 115 и плагин в браузере 135. Разберем их основные функции.

Плагин в браузере 135 предназначен для определения того, что пользователь 150 с помощью упомянутого браузера 130 произвел соединение с защищаемым сайтом 140, и передачи информации о том, что произошло соединение с защищаемым сайтом 140, устройству для безопасной передачи данных 115. В одном из вариантов реализации плагин 135 поставляется как часть антивируса 110.

Определение установки соединения производится плагином 135 с помощью интерфейса программирования приложений (англ. Application Programming Interface, API), который предоставляется браузером 130, в рамках которого будет определен URL-адрес сайта 140 при анализе GET или POST-запроса. Это предпочтительный вариант реализации.

Еще один вариант реализации плагина 135 предусматривает установку отдельного драйвера 136 (он может входить в состав плагина 135, так и быть отдельным приложением) для перехвата сетевого трафика между браузером 130 и сайтом 140. На основании перехваченных данных можно определить URL-адрес сайта 140. Подобный драйвер также может использоваться для установки отдельного соединения между устройством 115 и сайтом 140. Данный драйвер также может получать информацию о сайте 140 - например, сертификат сайта 140.

Список защищаемых адресов хранится на устройстве безопасной передачи данных 115 вместе с зашифрованными данными, необходимыми для аутентификации. При

активации (подключении к компьютеру 100) устройства 115, список защищаемых адресов загружается в память плагина 135, который проверяет каждый посещаемый пользователем адрес на присутствие в этом списке. Плагин 135 может сохранять список адресов как в своей памяти, так и на жестком диске.

Таким образом, список адресов защищаемых сайтов может храниться как в плагине 135, так и на устройстве для безопасной передачи данных 115. Как правило, подобный список может быть создан как самим пользователем 150, так и предоставлен разработчиками устройства для безопасной передачи данных 115 или плагина 135 (как правило, разработчик один для обоих средств). Существует ряд подходов, которые обеспечивают безопасный доступ к сайтам для пользователя. Примером технологий, обеспечивающих безопасный доступ к сайтам, является технология "Безопасные платежи", разработанная Лабораторией Касперского.

Получив запрос на аутентификацию от защищаемого сайта 140, плагин 135 передает устройству 115 данный адрес и сам запрос, включающий информацию по сайту (например, форму аутентификации). Также можно передавать дополнительную информацию для проверки на устройстве 115, такую как: URL-адрес, информацию о сертификате(-ах) сайта, WHOIS информацию о домене, список полученных заголовков из ответа на запрос по URL-адресу, информацию о загруженных скриптах (сценариях) в виде сверток (хеш-сумм). Разберем более подробно данное устройство.

Под устройством для безопасной передачи данных 115 в настоящем изобретении понимается реальное устройство, система, компонент, группа компонентов, реализованных с использованием аппаратных средств, таких как интегральные микросхемы (англ. application-specific integrated circuit, ASIC) или программируемой вентильной матрицы (англ. field-programmable gate array, FPGA) или, например, в виде комбинации программных и аппаратных средств, таких как микропроцессорная система и набор программных инструкций, а также на нейроморфных чипах (англ. neurosynaptic chips). Предпочтительный вариант реализации устройства для безопасной передачи данных 115 включает процессор общего назначения, модуль памяти для хранения и использования временных данных, носитель информации с возможностью создания и шифрования разделов, а также как минимум один адаптер (как правило, USB) для соединения с компьютером 100, а также средства ввода/получения факторов аутентификации пользователя. Как уже говорилось выше, устройство 115 хранит список адресов защищаемых сайтов вместе с зашифрованными данными, связанными с этими сайтами (как правило, это связки логин/пароль и другие данные форм аутентификации, но также может включать другие конфиденциальные данные пользователя - например, платежные). Этот список может загружаться с устройства 115 в память плагина для сравнения с каждым следующим запросом.

Сразу после получения запроса на аутентификацию, переданного плагином 135, устройство 115 инициирует создание нового защищенного подключения к сайту 140, от которого получает сертификат. Новое защищенное соединение может быть создано с помощью драйвера 136. Для проверки (верификации) полученного сертификата устройство 115 запрашивает у драйвера 136, установленного на компьютере 100, полное дерево сертификатов для сайта 140 за исключением корневого сертификата. Используя собственный список корневых сертификатов, устройство 115 проверяет валидность (достоверность) всей цепочки сертификатов для сайта 140. Если проверка не была успешна, то защищенное соединение будет разорвано. Устройство 115 может также использовать и другую информацию от плагина 115 для проверки сайта 140 - например, полученные заголовки или список загруженных сценариев при установке соединения.

Например, устройство 115 сравнивает свертку (хеш-сумму) загруженных сценариев с сайта 140, полученную от плагина 135, с собственной хеш-суммой, которая хранится на устройстве 115, и если свертки не совпадают, то соединение с сайтом 140 будет разорвано.

Важным аспектом данного изобретения является информация (например, личные данные пользователя), которая хранится на носителе данных в устройстве 115, а также исполняемый код, который выполняется при получении данных от плагина 135. Отметим, что в одном из вариантов реализации, работа с устройством 115 может быть осуществлена только с помощью плагина 135. Например, для авторизации и обмена данными может быть использована архитектура PKI (англ. Public Key Infrastructure). Закрытый ключ для устройства 115 поставляется разработчиком данного устройства. Другой вариант реализации плагина 135 предполагает доступ к данным, которые хранятся в памяти плагина 135 через использование отдельного API, что позволит разработчикам сторонних устройств, подобных устройству 115, использовать данный плагин.

Также важен другой функционал устройства 115, а именно проведение второго фактора аутентификации пользователя. Использование второго фактора аутентификации известно из уровня техники и может быть реализовано с помощью OTP, подтверждения цифровой подписи пользователя, биометрических данных пользователя. Это позволяет защитить аутентификационные данные пользователя от снятия содержимого (дампа) памяти устройства 115 при его краже. Только после получения второго фактора аутентификации устройство 115 способно расшифровать аутентификационные данные пользователя и передать их на сторону сайта 140, как если бы эти данные были заполнены и отправлены с использованием браузера 130.

Устройство 115 проходит авторизацию и передает необходимые аутентификационные данные, которые относятся к сайту 140. Кроме аутентификационных данных устройство 115 может хранить и другую информацию - например, платежные данные по счетам/транзакциям пользователя. Подобная информация хранится в зашифрованном виде и расшифровывается только получения информации о проведении второго фактора аутентификации. После получения от сайта 140 ответа об успешной аутентификации, устройство 115 передает идентификатор новой сессии и прочую информацию, необходимую для идентификации авторизованного пользователя, плагину 135, который отправляет их в браузер 130 в ответ на отправку браузером первоначального запроса к сайту 140. Таким образом, браузер 130 сразу получает данные новой сессии пользователя, позволяя продолжить обычный веб-серфинг, но уже от лица авторизованного на сайте пользователя.

Рассмотрим, как информация пользователя может быть внесена на устройство 115. Один из вариантов реализации предусматривает продажу устройства 115 с уже внесенными данными пользователя со стороны банка, который также владеет сайтом 140. Еще один вариант реализации включает использование плагина 135, который запоминает информацию пользователя на сайте 140 (т.е. выполняет функцию менеджера паролей) и передает ее устройству 115.

Рассмотрим варианты, как аутентификационные данные пользователя 150 могут быть переданы на сторону сайта 140. Информация с устройства 115 может быть передана в ответ на сторону сайта 140 несколькими путями. Разберем некоторые из них:

- Вставка данных на веб-странице сайта 140. Определенные данные (например, логин и пароль) могут быть привязаны к URL-адресу вебстраницы и вставляются в определенные поля (как правило, поля для вставки логина и пароля имеют ряд

атрибутов, по которым их можно вычислить, например, атрибут «password» у тега «input»).

- Данные могут быть подготовлены заранее в виде GET/POST-запроса и отправлены на сервер в определенный момент времени или по наступлению какого-либо события. Самый простой пример - отправка POST-запроса с введенными в форму данными логина и пароля после получения ответа от сайта на GET-запрос вебстраницы, где данные логин и пароль нужно ввести.

Фиг. 3 показывает способ работы настоящего изобретения. На этапе 301 происходит определение входа пользователя на сайт (пользователь произвел соединение) во время его работы в браузере 130, после чего на этапе 302 определяется, что сайт является защищаемым сайтом 140. Более подробно про определение адреса сайта 140 приведено в описании Фиг. 2 в рамках описания работы плагина 135. На этапе 303 на устройство 115 приходит информация от плагина 135 о факте захода пользователя (т.е. пользователь произвел соединение) на сайт 140, после чего устройство 115 настраивает и использует защищенный канал передачи данных на этапе 304.

В предпочтительном варианте реализации в качестве защищенного канала данных выступает https-соединение. На этапе 305 устройство 115 извлекает всю связанную с сайтом 140 информацию и передает ее с помощью защищенного канала передачи данных. На этапе 306 пользователь продолжает работать в браузере 130 в обычном режиме.

Разберем пример работы способа настоящего изобретения более подробно на примере Фиг. 4. Во время обычного веб-серфинга пользователя с помощью браузера 130 (этап 1) с сайта 140 приходит форма для аутентификации (этап 2), которая перехватывается плагином 135 и передается в устройство 115 (этап 3). Устройство 115 использует плагин 135 для установки дополнительного, прямого https-соединения с сайтом 140 (этап 4) и получает сертификат этого сайта (этап 5). Для проверки валидности сертификата, устройство 115 запрашивает полное дерево сертификатов у плагина 135 с компьютера пользователя (этап 6). Используя список собственных (хранящихся на устройстве 115) корневых сертификатов, на устройстве 115 происходит проверка валидности полученного (этап 7) сертификата (этап 8), поиск аутентификационных данных на устройстве 115 для данного компьютера (этап 9), которые соответствуют сайту 140. Далее производят запрос к пользователю на получение второго фактора аутентификации (например, отпечатка пальца или пароля, напрямую вводимого в устройство 115) (этап 10) и расшифровку аутентификационных данных в памяти устройства 115 (этап 11). После успешного выполнения предыдущих шагов, устройство 115 (с помощью плагина 135, который лишь устанавливает TCP-соединение и передает данные устройству 115) завершает установку https-соединения с сайтом 140 (этап 12) и отправляет на сайт 140 заполненную форму аутентификации (этап 13). Для сервера (сайта 140) это выглядит как получение заполненной формы от браузера 130. Полученный ответ от сервера (этап 14) устройство 115 пересылает плагину 135, который передает их напрямую браузеру 130 (этап 15), таким образом браузер 130 сразу получает новую сессию (этап 16), полностью пропустив механизм авторизации.

Рассмотрим еще один важный аспект настоящего изобретения, который заключается в настройке безопасного канала передачи данных между устройством 115 и сайтом 140. Как уже говорилось ранее, компьютерная система 100 может быть заражена вредоносным приложением 120, которое не было обнаружено антивирусным приложением 110. Ввиду того, что устройство 115 не имеет доступа к ресурсам компьютерной системы 110 и не может провести дополнительную проверку данной

системы, устройство 115 периодически или же в момент запроса от антивирусного приложения 110 на передачу данных к сайту 140, запрашивает также у антивирусного приложения 110 следующие данные:

- время и статус последней антивирусной проверки;
- статус обновления антивирусных баз;
- тип соединения с сетью Интернет;
- информацию о последних известных компьютерных угрозах, которая поставляется всеми поставщиками антивирусного программного обеспечения (ПО), например, Лаборатория Касперского предоставляет ее в рамках участия в KSN (Kaspersky Security Network).

После получения данной информации на устройстве 115 проходит проверка этой информации с помощью ряда правил, которые определяют выбор настроек безопасного канала передачи данных между устройством 115 и сайтом 140.

Приведем несколько примеров для ясности.

Пример 1

Время и статус последней антивирусной проверки: минуту назад, вредоносное ПО не найдено.

Статус обновления антивирусных баз: загружена последняя версия антивирусных баз.

Тип соединения с сетью Интернет: VPN (Virtual Private Network).

Информация о последних известных компьютерных угрозах: не найдено.

Решение: данные можно предоставлять через плагин 135 в расшифрованном виде.

Пример 2

Время и статус последней антивирусной проверки: минуту назад, вредоносное ПО не найдено.

Статус обновления антивирусных баз: загружена последняя версия антивирусных баз.

Тип соединения с сетью Интернет: открытый доступ.

Информация о последних известных компьютерных угрозах: выявлено новое семейство вредоносного ПО Zeus.

Решение: данные можно предоставлять через плагин 135 в зашифрованном виде.

Пример 3

Время и статус последней антивирусной проверки: неделю назад, было найдено вредоносное ПО.

Статус обновления антивирусных баз: антивирусные базы обновлялись более недели назад.

Тип соединения с сетью Интернет: открытый доступ.

Информация о последних известных компьютерных угрозах: данных не получено.

Решение: данные следует предоставлять через отдельное защищенное соединение в зашифрованном виде.

Для применения подобных решений на компьютерной системе 100 занимается антивирусное приложение 110. В качестве одного из вариантов настроек можно предложить создание и использование VPN-соединения. Другой вариант предусматривает дополнительную защиту адресного пространства процессов браузера 130 и плагина 135 от возможных проверок со стороны вредоносного приложения 120, а также защиту буфера обмена и каналов межпроцессного взаимодействия (англ. inter-process communication, IPC).

Фиг. 5 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, сканер 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. 5. 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.

(57) Формула изобретения

1. Система для защищенной передачи аутентификационных данных пользователя на сайт в сети Интернет, которая содержит следующие средства:

- плагин в браузере, установленный на компьютере пользователя, при этом плагин предназначен для определения, что пользователь с помощью упомянутого браузера произвел соединение с сайтом, при взаимодействии с которым требуется защищать получаемые и передаваемые аутентификационные данные (далее - защищаемый сайт), и передачи информации о том, что произошло соединение с защищаемым сайтом, антивирусному приложению;
- антивирусное приложение, установленное на упомянутом компьютере, предназначенное для проверки операционной системы, установленной на упомянутом компьютере, на наличие уязвимостей и вредоносных приложений после получения упомянутой информации от плагина и передачи информации о проведенной проверке, а также информации, полученной от плагина, на устройство для безопасной передачи данных, и применения настроек безопасного канала передачи данных;
- устройство для безопасной передачи данных, предназначенное для:
  - выбора настроек безопасного канала передачи данных между устройством для безопасной передачи данных и защищаемым сайтом на основании информации о проведенной антивирусным приложением проверке,
  - передачи по безопасному каналу передачи данных между устройством для безопасной передачи данных и защищаемым сайтом аутентификационных данных пользователя на защищаемый сайт для аутентификации на данном сайте, при этом передача происходит на основании информации о том, что пользователь с помощью браузера произвел соединение с защищаемым сайтом, при этом аутентификационные данные хранятся на устройстве для безопасной передачи данных в зашифрованном виде.

2. Система по п. 1, в которой антивирусное приложение создает зашифрованное соединение с устройством для безопасной передачи данных.

3. Система по п. 1, в которой аутентификационные данные, которые хранятся на устройстве для безопасной передачи данных в зашифрованном виде, расшифровываются

только после получения от пользователя одного из факторов аутентификации, таких как: OTP (one time password), подтверждения цифровой подписи пользователя, биометрических данных пользователя.

4. Система по п. 3, в которой расшифрованные данные передаются антивирусному приложению.

5. Система по п. 4, в которой полученные антивирусным приложением расшифрованные данные передаются плагину в браузере, после чего упомянутые данные передаются на сторону защищаемого сайта.

6. Система по п. 4, в которой полученные антивирусным приложением расшифрованные данные передаются на сторону защищаемого сайта с помощью антивирусного приложения.

7. Система по п. 1, в которой настройка безопасного канала передачи данных включает использование VPN.

8. Способ для защищенной передачи аутентификационных данных пользователя на сайт в сети Интернет, реализованный средствами из системы по п. 1, содержащий этапы на которых:

а) определяют, что пользователь с помощью упомянутого браузера произвел соединение с сайтом, при взаимодействии с которым требуется защищать получаемые и передаваемые данные (далее - защищаемый сайт);

б) передают информацию о том, что произошло соединение с защищаемым сайтом, антивирусному приложению;

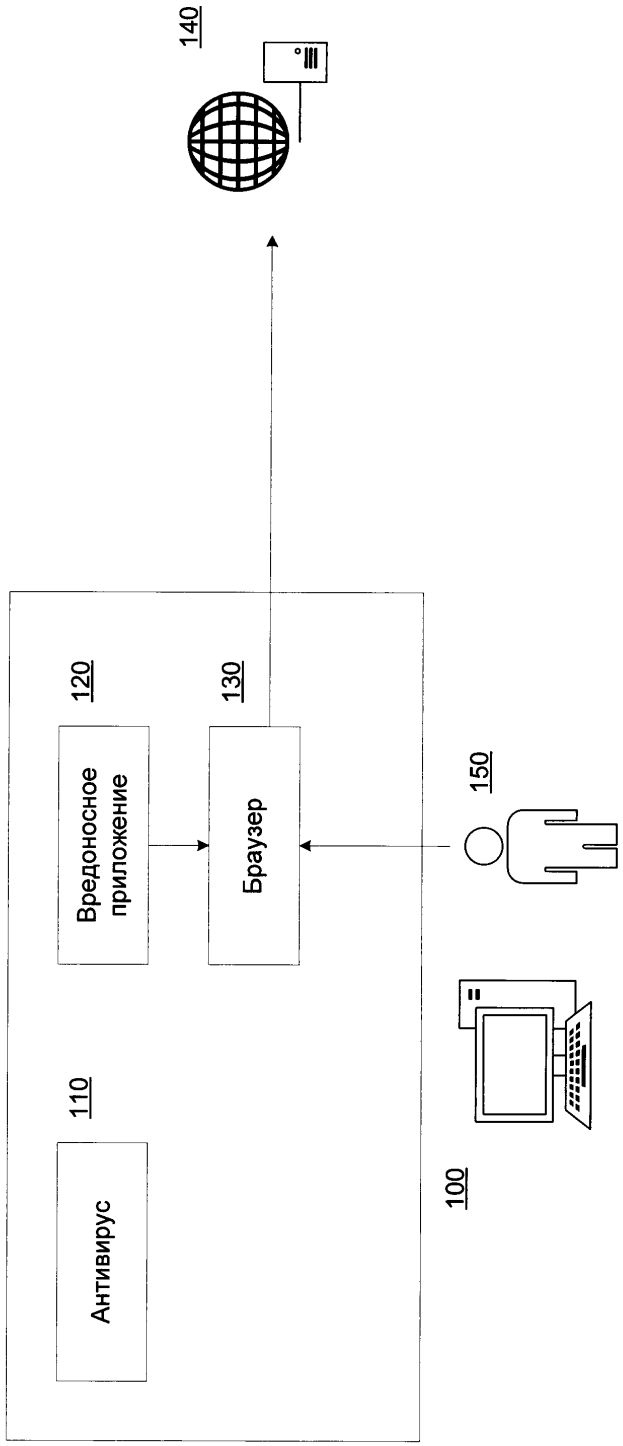
в) проверяют операционную систему, установленную на упомянутом компьютере, на наличие уязвимостей и вредоносных приложений после получения упомянутой информации от плагина и передачи информации о проведенной проверке, а также информации, полученной от плагина, на устройство для безопасной передачи данных;

г) выбирают настройки безопасного канала передачи данных на основании информации о проведенной антивирусным приложением проверке с помощью устройства для безопасной передачи данных;

д) применяют выбранные настройки безопасного канала передачи данных между устройством для безопасной передачи данных и защищаемым сайтом с помощью антивирусного приложения;

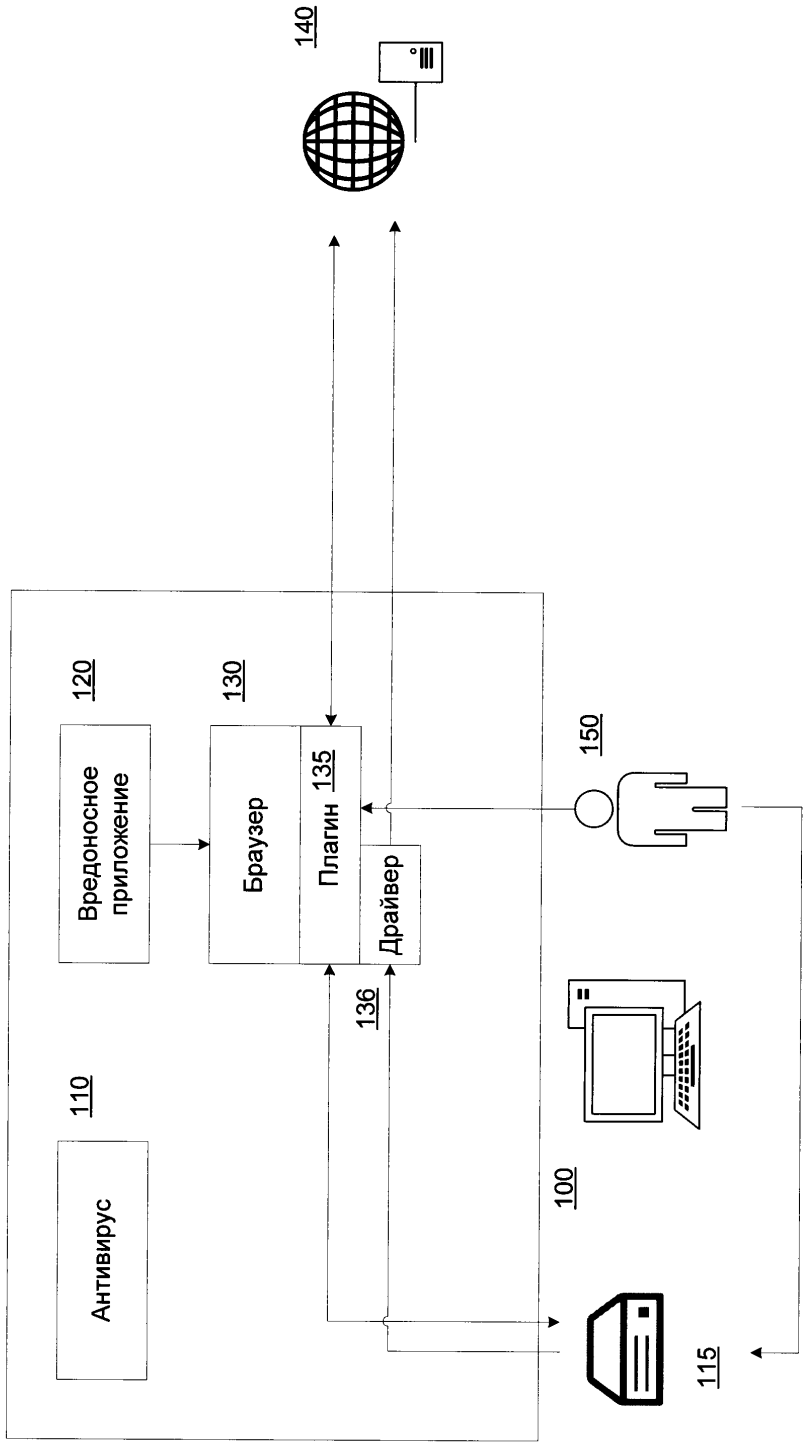
е) передают по безопасному каналу передачи данных между устройством для безопасной передачи данных и защищаемым сайтом аутентификационные данные пользователя на защищаемый сайт для аутентификации на данном сайте, при этом передача происходит на основании информации о том, что пользователь с помощью браузера произвел соединение с защищаемым сайтом, при этом аутентификационные данные хранятся на устройстве для безопасной передачи данных в зашифрованном виде.

1


140
120
130
Вредоносное приложение
Браузер
150
110
Антивирус
100

Фиг. 1

2


140
120
130
Вредоносное приложение
Браузер
Плагин 135
Драйвер
150
136
110
Антивирус
100
115

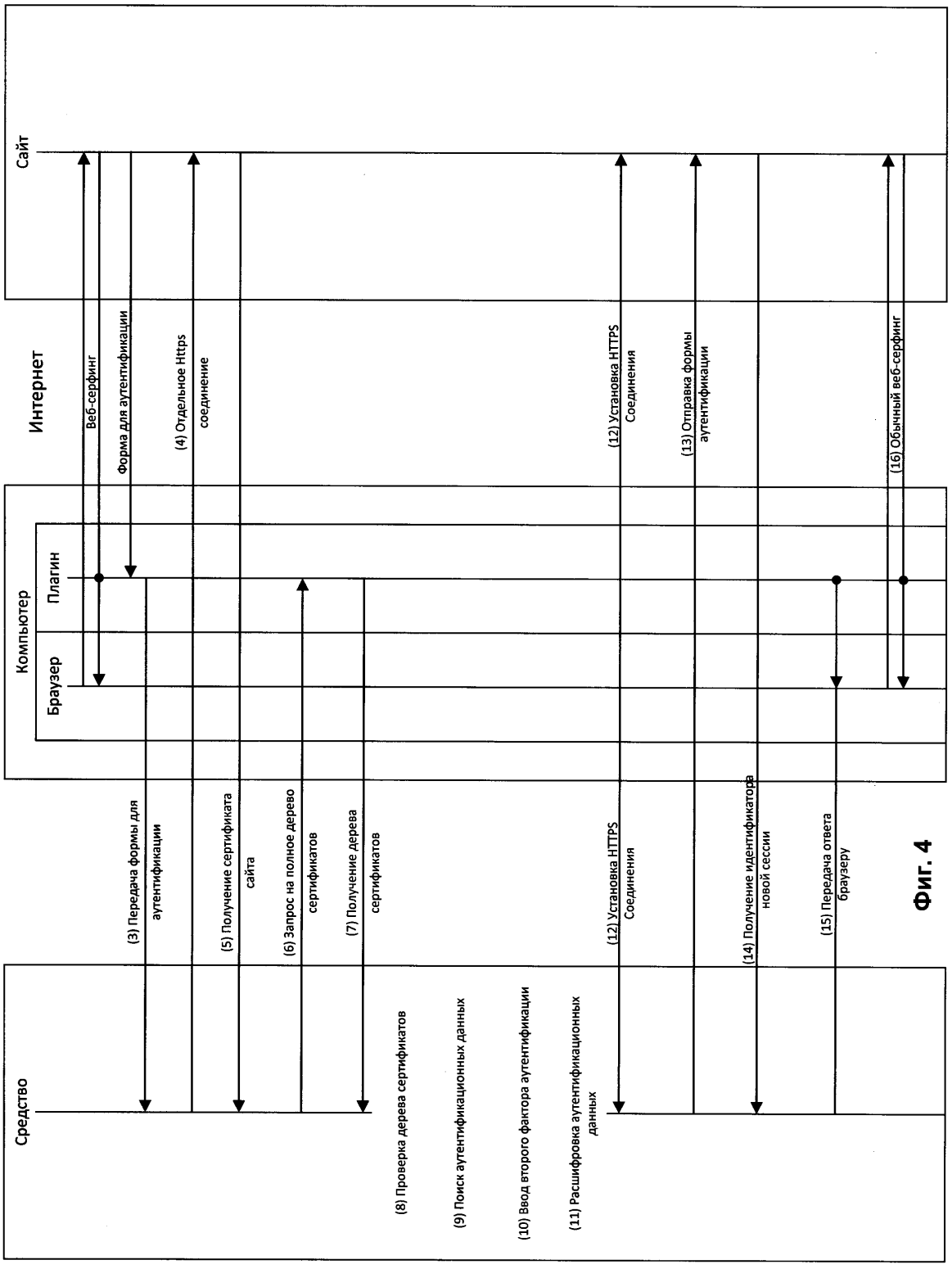
Фиг. 2

3

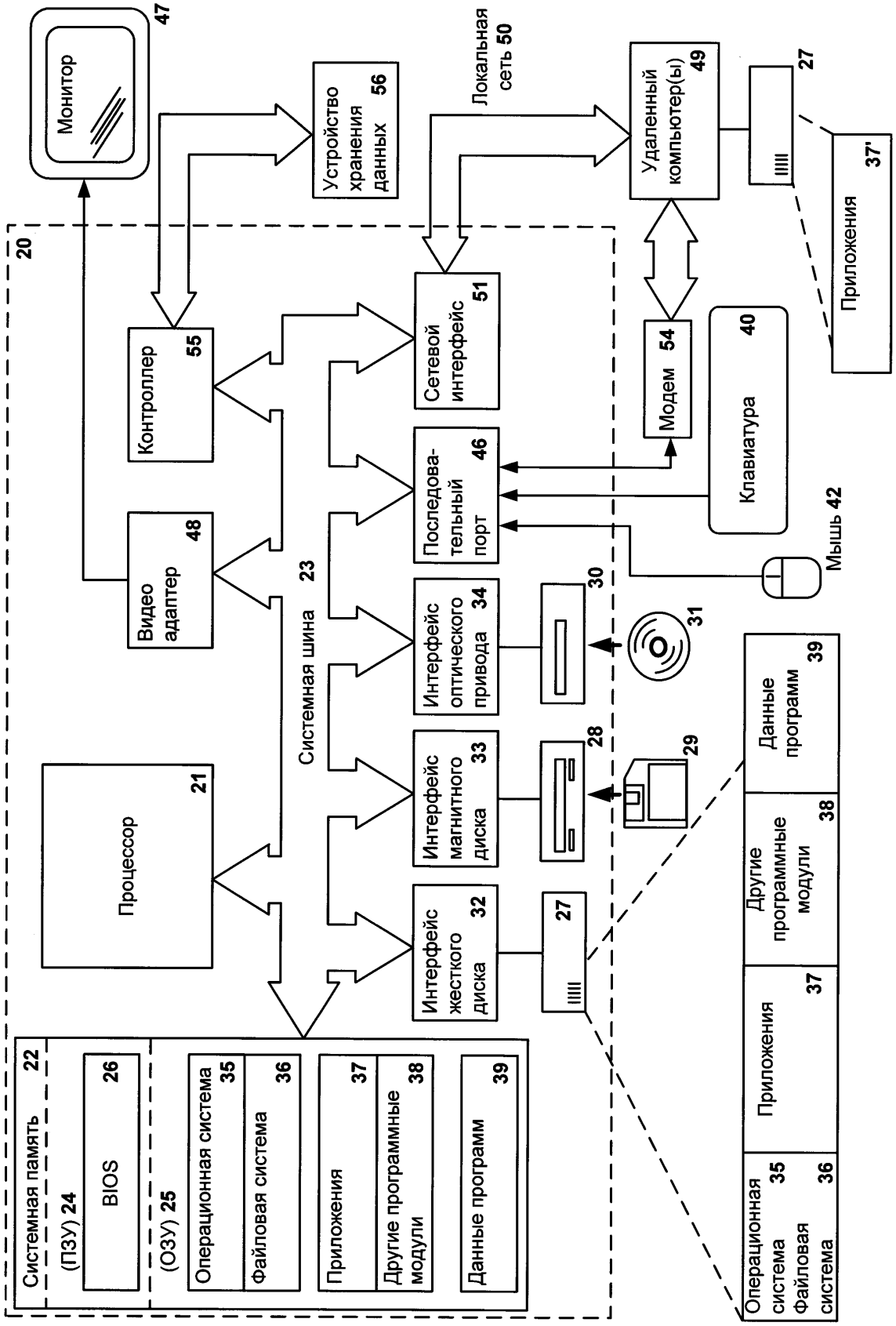

Определение входа на сайт
301
Подтверждение что сайт защищаемый
302
Передача информации о входе на сайт на устройство
303
Настройка канала передачи данных
304
Передача данных на сайт
305
Продолжение обычной работы браузера
306

Фиг. 3

4


Сайт
Интернет
Компьютер
Браузер
Плагин
Средство
Веб-серфинг
Форма для аутентификации
(4) Отдельное Https соединение
(12) Установка HTTPS Соединения
(13) Отправка формы аутентификации
(16) Обычный веб-серфинг
(3) Передача формы для аутентификации
(5) Получение сертификата сайта
(6) Запрос на полное дерево сертификатов
(7) Получение дерева сертификатов
(8) Проверка дерева сертификатов
(9) Поиск аутентификационных данных
(10) Ввод второго фактора аутентификации
(11) Расшифровка аутентификационных данных
(12) Установка HTTPS Соединения
(14) Получение идентификатора новой сессии
(15) Передача ответа браузеру

Фиг. 4


Монитор 47
Устройство хранения данных 56
Локальная сеть 50
Удаленный компьютер(ы) 49
27
Приложения 37'
20
Сетевой интерфейс 51
Контроллер 55
Модем 54
Клавиатура 40
Последова-тельный 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. 5