(19) Евразийское патентное ведомство

(11) 038161 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.07.16

(21) Номер заявки
202090168

(22) Дата подачи заявки
2020.01.28

(51) Int. Cl. ***G06F 21/31*** (2013.01)
G06F 21/44 (2013.01)
H04L 29/06 (2006.01)

(54) СПОСОБ И СИСТЕМА АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

(31) **2019135945**
(32) **2019.11.08**
(33) **RU**
(43) **2021.05.31**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Зарубинский Игорь Владимирович, Чубенко Алексей Геннадьевич, Жигалова Ирина Викторовна, Филичева Юлия Алексеевна, Нестерова Яна Олеговна, Глебов Иван Александрович, Лимина Наталия Юрьевна (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) YANG-WAI CHOW et al, "Authentication and Transaction Verification using QR Codes with a Mobile Device", Conference: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, November 2016, 14 л., размещено в Интернет: https://www.researchgate.net/publication /309816698_Authentication_and_Transaction_Verification_Using_QR_Codes_with_a_Mobile_Device раздел 4 , подразделы 4.1, 4.2

SHA LIU et al, "A Novel QR Code and mobile phone based Authentication protocol via Bluetooth", International Conference on Materials Engineering and Information Technology Applications (ME1TA 2015), August 2015, 9 л., размещено в Интернет: https://www.seman-ticscholar.org/paper/ A-Novel-QR-Code- and-mobile-phone-based-protocoi-via-Liu-Zhu/726ece0f02683ad6dd669bcl0eflac45eb5ef58c разделы "Preliminary phase", "Registration phase", "Login phase", "Authentication phase Security and Performance Analysis"

US-A1-20170223002

US-A1-2015089610

(57) Данное техническое решение в общем относится к области вычислительной техники, а в частности к способу и системе авторизации пользователя на веб-сайте при помощи QR-кода. Техническим результатом, достигаемым при решении вышеуказанной технической задачи, является обеспечение возможности отслеживания статуса QR-кода. Указанный технический результат достигается благодаря осуществлению способа аутентификации пользователя, выполняемого по меньшей мере одним вычислительным устройством, содержащего этапы, на которых: получают запрос на аутентификацию пользователя; получают данные о типе аутентификации, выбранном пользователем, и идентификатор (ID) единой учетной записи пользователя; регистрируют операцию аутентификации и формируют идентификатор операции; генерируют QR-код, в который включается информация об идентификаторе операции, и назначают ему соответствующий статус; отслеживают статус QR-кода; на основе данных о статусе QR-кода определяют, что операция подтверждена пользователем, причем в параметры операции сохраняют ID единой учетной записи пользователя; аутентифицируют пользователя по ID единой учетной записи пользователя.

038161 B1

038161 B1

Область техники

Данное техническое решение в общем относится к области вычислительной техники, а в частности к способу и системе авторизации пользователя на веб-сайте при помощи QR-кода.

Уровень техники

В настоящее время пользователи, вводящие свои учетные данные для авторизации на веб-сайте с помощью незащищенных устройств, сталкиваются с риском раскрытия своих учетных данных для посторонних лиц. В связи с этим требуется такой способ ввода данных пользователем для входа на веб-сайты, при котором не требуется вводить конфиденциальную информацию. Также в некоторых случаях пользователям может быть сложно вручную вводить учетные данные, например, на устройствах с ограниченными возможностями ввода. Наиболее близким техническим решением к заявленному решению является система и способ, раскрытые в заявке US 2015089610 (A1), опубл. 26.03.2015, позволяющие пользователю использовать доверенное устройство для предоставления конфиденциальной информации поставщику идентификационных данных с помощью QR-кода (Quick Response), чтобы поставщик идентификаторов мог получить доступ к веб-сайту или собрать информацию для веб-сайта. В известном решении пользователь может безопасно выполнить авторизацию на веб-сайте с незащищенного устройства, вводя конфиденциальную информацию в доверенное устройство. Поставщик идентификаторов может генерировать QR-код для отображения на веб-сайте на незащищенном устройстве. Пользователь с помощью приложения от поставщика идентификаторов, установленного на доверенном устройстве, может сканировать QR-код для передачи QR-кода поставщику идентификаторов. Поставщик идентификаторов может подтвердить QR-код и получить учетные данные для аутентификации пользователя или может собирать информацию для веб-сайта. Преимущественно, пользователь может выполнить безопасный вход на веб-сайт с ненадежных устройств, используя доверенное устройство. Недостатком известного решения является его ограниченный функционал, например в известном решении отсутствует функция отслеживания статуса QR-кода, в связи с чем снижается надежность системы.

Сущность технического решения

Технической проблемой или задачей, поставленной в данном техническом решении, является создание простого и надежного способа и системы авторизации пользователя в ресурсной системе посредством аутентификации с помощью QR-кода.

Техническим результатом, достигаемым при решении вышеуказанной технической задачи, является обеспечение возможности отслеживания статуса QR-кода для определения подтверждения пользователем операции аутентификации и его аутентификации. Дополнительным техническим результатом является обеспечение возможности отмены входа с ненадежного устройства после сканирования QR-кода.

Указанный технический результат достигается благодаря осуществлению способа аутентификации пользователя, выполняемого по меньшей мере одним вычислительным устройством, содержащего этапы, на которых: получают запрос на аутентификацию пользователя; получают данные о типе аутентификации, выбранном пользователем, и идентификатор (ID) единой учетной записи пользователя; регистрируют операцию аутентификации и формируют идентификатор операции; генерируют QR-код, в который включается информация об идентификаторе операции, и назначают ему соответствующий статус; отслеживают статус QR-кода; на основе данных о статусе QR-кода определяют, что операция подтверждена пользователем, причем в параметры операции сохраняют ID единой учетной записи пользователя; аутентифицируют пользователя по ID единой учетной записи пользователя.

В одном из частных примеров осуществления способа дополнительно выполняют этапы, на которых: на основе данных о статусе QR-кода определяют, что QR-код отсканирован пользователем; направляют пользователю запрос на подтверждение операции аутентификации.

В другом частном примере осуществления способа дополнительно выполняют этапы, на которых: получают от устройства партнера запрос кода авторизации, в параметры запроса которого включается ID учетной записи ресурсной системы; генерируют данные кода авторизации и направляют их ресурсной системе; получают от ресурсной системы запрос кода доступа, в параметрах которого включаются данные кода авторизации и ID учетной записи ресурсной системы; авторизуют ресурсную систему на основе результатов проверки данных кода авторизации, направленных ресурсной системе, и данных кода авторизации, полученных от ресурсной системы; отправляют в ресурсную систему код доступа, содержащий ID единой учетной записи пользователя. В другом частном примере осуществления способа дополнительно выполняют этапы, на которых: включают в параметры запроса кода авторизации параметр для предотвращения подделки межсайтовых запросов, сгенерированный устройством ресурсной системы, причем сгенерированные данные кода авторизации перенаправляют пользователю вместе с параметром для предотвращения подделки межсайтовых запросов; получают от пользователя посредством устройства ресурсной системы данные кода авторизации и параметр для предотвращения подделки межсайтовых запросов; на основе результатов сравнения параметра для предотвращения подделки межсайтовых запросов, сгенерированного устройством ресурсной системы, и упомянутого параметра, полученного от пользователя, формируют запрос на получение кода доступа, в который включаются данные кода авторизации.

В другом предпочтительном варианте осуществления заявленного решения представлена система

аутентификации пользователя, содержащая по меньшей мере одно вычислительное устройство и по меньшей мере одно устройство памяти, содержащее машиночитаемые инструкции, которые при их исполнении по меньшей мере одним вычислительным устройством выполняют указанный выше способ.

Краткое описание чертежей

Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей, на которых:

на фиг. 1 - представлен пример системы авторизации пользователя;

на фиг. 2 - представлен пример общего вида вычислительного устройства.

Подробное описание изобретения

Ниже будут описаны понятия и термины, необходимые для понимания данного технического решения.

В данном техническом решении под системой подразумевается, в том числе, компьютерная система, ЭВМ (электронно-вычислительная машина), ЧПУ (числовое программное управление), ПЛК (программируемый логический контроллер), компьютеризированные системы управления и любые другие устройства, способные выполнять заданную, четко определенную последовательность операций (действий, инструкций).

Под устройством обработки команд подразумевается электронный блок, вычислительное устройство, либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройств хранения данных. В роли устройства хранения данных могут выступать, но не ограничиваясь, жесткие диски (HDD), флеш-память, ПЗУ (постоянное запоминающее устройство), твердотельные накопители (SSD), оптические приводы.

Программа - последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

В соответствии со схемой, приведенной на фиг. 1, система 100 авторизации пользователя содержит: устройства 10 пользователя, ресурсную систему 20 (например, устройство партнера или другой автоматизированной системы (АС)), устройство 30 аутентификации пользователя и устройство 40 обработки запросов на аутентификацию пользователя.

Устройствами пользователя могут быть устройство 11 взаимодействия с сайтом и устройство 12 мобильного приложения. В частном варианте реализации решения устройство 11 взаимодействия с сайтом может представлять собой, например, портативный или стационарный компьютер, мобильный телефон или смартфон, планшет и пр., оснащённые прикладным программным обеспечением - браузером, обеспечивающим возможность просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач. Устройство 12 мобильного приложения представляет собой вычислительное устройство, которое сконфигурировано для работы с различными типами мобильных приложений, например с мобильным приложением Сбербанк-онлайн, и оснащено средствами, например фото и/или видео камерой, для фиксации изображений, в частности изображений QR-кода. Например, устройство 12 мобильного приложения может быть выполнено в виде мобильного телефона, смартфона или планшета. Для использования приложения на упомянутом устройстве 12 пользователю необходимо авторизоваться посредством идентификатора (ID) единой учетной записи пользователя. Упомянутый ID единой учетной записи пользователь может получить при регистрации через упомянутое приложение или другими известными из уровня техники возможностями у поставщика этого приложения, который генерирует ID единой учетной записи пользователя и направляет его в упомянутое устройство 12 для хранения.

Ресурсная система 20 интегрирует информационные, финансовые, материальные, трудовые ресурсы с необходимыми основными фондами, которые обеспечивают жизненный цикл продукции: материалы - продукция - товар. Целью ресурсной системы 20 является переработка материалов в товар, необходимый для пользователя. Задачей этой системы является обеспечение принятия решений относительно развития управляемого объекта - интегрированного ресурса на основе новых компьютерных технологий (см. О.С. Григоров и др., УПРАВЛЕНИЕ БИЗНЕС-ПОТЕНЦИАЛОМ ПРОИЗВОДСТВЕННЫХ СИСТЕМ, Новосибирск 2002, 56с, http://window.edu.ru/resource/799/37799/files/m bus1.pdf). Ресурсная система 20 может быть реализована на базе по меньшей мере одного сервера, сконфигурированного для предоставления пользователю устройства 11 через вебсайт различного вида услуги. Ресурсная система 20, в частном случае ее реализации, содержит модуль 21 обработки запросов пользователя и модуль 22 маршрутизации. Указанные модули могут быть реализованы на базе программно-аппаратных средств ресурсной системы 20, модифицированных в программной части таким образом, чтобы выполнять приписанные далее этим модулям функции. Устройство 30 аутентификации пользователя и устройство 40 обработки запросов на аутентификацию пользователя могут быть также реализованы на базе по меньшей мере одного сервера, при этом устройство 30 аутентификации пользователя может содержать модуль 31 связи с пользователем и модуль 32 аутентификации, а устройство 40 обработки запросов на аутентификацию пользователя может включать: базу 41 данных (БД) и модуль 42 обработки запросов на аутентификацию. Указанные модули также могут быть реализованы на базе программно-аппаратных средств

устройства 30 и устройства 40 соответственно, модифицированных в программной части таким образом, чтобы выполнять приписанные далее этим модулям функции.

Соответственно, пользователь посредством устройства 11 взаимодействия с веб-сайтом, в частности при помощи браузера, может перейти в ресурсную систему 20, например, посредством посещения веб-сайта ресурсной системы 20 или установки соответствующего приложения, для просмотра ее содержимого, информация о котором в устройство 11 направляется ресурсной системой 20. Например, пользователю может быть отображена информация о предоставляемых ресурсной системой 20 услугах (получение ипотеки, каталог товаров, предоставление информации о состоянии счетов и карт, осуществление платежей и т.д.), а пользователь может посредством устройства 11 направить запрос на получение по меньшей мере одной услуги, предоставляемой ресурсной системой 20.

В процессе формирования запроса на получение услуги либо в любой другой момент времени, например при входе в ресурсную систему 20 (т.е. авторизации), пользователь может направить запрос на авторизацию в ресурсную систему 20 для представления ему (пользователю) дополнительных функций, предусмотренных для авторизированных пользователей ресурсной системы 20. Для входа в ресурсную систему 20 пользователь может использовать единую учетную запись для аутентификации на множестве не связанных друг с другом Интернет-ресурсов, информация о которой содержится в БД 41 устройства 40 аутентификации пользователя, например, в виде UID. Для этого пользователь посредством устройства 11 взаимодействует с ресурсной системой 20, отправляя соответствующую команду/запрос на авторизацию, которая поступает в модуль 21 обработки запросов пользователя ресурсной системы 20.

Например, в случае входа на веб-сайт ресурсной системы 20 при помощи протокола OIDC (Open ID Connect) при получении запроса на авторизацию модуль 21 обработки запросов отправляет в модуль 22 маршрутизации запрос на получение параметра, защищающего от межсайтовых подделок (State), и параметра, защищающего от копирования запросов (Nonce). Модуль 22 маршрутизации известными из уровня техники методами формирует указанные параметры, создает операцию авторизации, сохраняет в параметрах операции значения State и Nonce, после чего возвращает указанные параметры и идентификатор операции авторизации в модуль 21. Модуль 21 сохраняет в памяти, которой он может быть дополнительно оснащен, идентификатор операции авторизации и направляет запрос кода авторизации (AUTHCODE) в модуль 31 связи с пользователем, отправляя в запросе State, Nonce, ссылку URI, на который нужно вернуть пользователя после успешной аутентификации (REDIRECTJJRI), и идентификатор (ID) ресурсной системы. Также ID ресурсной системы, пароль ресурсной системы и REDIRECTJJRI могут быть заранее занесены в БД 41 при регистрации ресурсной системы 20 в устройстве 40 обработки запросов на аутентификацию пользователя.

Модуль 31 аутентификации известными из уровня техники методами валидирует параметры запроса кода авторизации (AUTHCODE) и в случае успешной проверки направляет в устройство 11 взаимодействия с сайтом форму аутентификации, которая отображается пользователю. При выборе пользователем аутентификации с помощью QR-кода в модуль 31 аутентификации поступают от устройства 11 данные о типе аутентификации - аутентификация с помощью QR-кода (PAT_QR), после чего упомянутый модуль 31 формирует и направляет запрос аутентификации пользователя для получения QR-кода в модуль 42 обработки запросов. В запросе упомянутым модулем 31 отправляются данные о типе аутентификации (PAT QR), State, Nonce, ID ресурсной системы, REDIRECT_URI (далее - параметры OIDC), а также IP адрес, название браузера и операционной системы компьютера пользователя, собранные известными из уровня техники методами. Модуль 42 обработки запросов при получении запроса аутентификации пользователя регистрирует в БД 41 операцию аутентификации, формирует идентификатор операции (QRID), сохраняет полученные из модуля 31 данные вместе с идентификатором операции и присваивает операции статус "Новый", после чего модуль 42 генерирует QR-код, в который включается информация об идентификаторе операции.

Сгенерированный QR-код и идентификатор операции модуль 42 обработки запросов направляет в модуль 31 связи с пользователем для передачи и вывода его на устройстве 11 взаимодействия с веб-сайтом. Также модуль 31 в соответствии с заложенным в него пользователем устройства 30 программно-аппаратным алгоритмом периодически обращается посредством модуля 42 обработки запросов к БД 41 для получения текущего статуса операции аутентификации, отправляя в запросе проверки статуса идентификатор операции (QRID).

Далее для авторизации в ресурсной системе 20 пользователю необходимо запустить приложение на устройстве 12 мобильного приложения, известными из уровня техники методами авторизоваться в приложении посредством ID единой учетной записи пользователя, после чего с помощью мобильного приложения и устройства 12 мобильного приложения пользователю необходимо просканировать изображение, выведенное на устройстве 11 взаимодействия с веб-сайтом. При получении изображения QR-кода устройство 12 извлекает из него идентификатор операции (QRID) и направляет его в модуль 42 обработки запросов, который при получении идентификатора операции (QRID) меняет статус "Новый" для данного идентификатора операции (QRID) в БД 41 на статус "Отсканирован", после чего модуль 42 извлекает из БД 41 информацию об операции, в том числе ее идентификатор (QRID), и возвращает ее в модуль 12 мобильного приложения. Далее посредством устройства 12 мобильного приложения пользователь

подтверждает операцию, отправляя запрос на подтверждение аутентификации в модуль 42 обработки запросов с идентификатором операции (QRID) и статусом операции "Подтвержден". Дополнительно в запрос на подтверждение аутентификации упомянутое устройство 12 включает ID единой учетной записи пользователя. Также дополнительно пользователь известными из уровня техники средствами может подписать упомянутый запрос своей цифровой подписью, информация о которой сохранена в упомянутом устройстве 12.

Модуль 42 обработки запросов меняет статус для данного идентификатора операции (QRID) в БД 41 на статус "Подтвержден" и сохраняет в параметрах операции аутентификации ID единой учетной записи пользователя. Соответственно, когда модуль 31 связи с пользователем при обращении к БД 41 через модуль 42 обработки запросов определил, что идентификатор операции (QRID) имеет статус "Подтвержден", модуль 31 связи с пользователем отправляет идентификатор операции (QRID) в запросе к модулю 42 на получение кода авторизации AUTHCODE, REDIRECT URI и State, сохраненные для данного идентификатора операции (QRID) в БД 41.

При получении от модуля 31 связи с пользователем запроса кода авторизации модуль 42 аутентифицирует пользователя, от которого ранее был получен запрос на аутентификацию с аналогичным идентификатором операции (QRID), и возвращает посредством модуля 31 в устройство 11 взаимодействия с веб-сайтом AUTHCODE, REDIRECTJJRI и State. По REDIRECT URI устройство 11 взаимодействия с веб-сайтом перенаправляется в ресурсную систему 20 сайта партнера, после чего устройство 11 направляет в модуль 21 обработки запросов пользователя AUTHCODE и State.

Модуль 21 обработки запросов пользователя, получив AUTHCODE и State, передает их в модуль 22 маршрутизации в связке со значением текущей операции авторизации пользователя в ресурсной системе. Модуль 22 маршрутизации сверяет значение State, полученное от модуля 21, с тем значением State, которое сохранено в данных операции авторизации, сгенерированных ранее. Если значения совпадают, то модуль 22 обработки запросов пользователя направляет запрос в модуль 32 аутентификации на получение кода доступа, в который включается: полученное значение AuthCode, ID ресурсной системы, пароль ресурсной системы, REDIRECT URI (тот же самый URI, который был отправлен в запросе на код авторизации).

Модуль 32 аутентификации проверяет AuthCode посредством сравнения с AuthCode, который ранее был направлен модулем 31 в устройство 11 взаимодействия с веб-сайтом, идентификатор ресурсной системы и пароль ресурсной системы, после чего авторизует ресурсную систему на основе результатов проверки данных кода авторизации, направленных ресурсной системе, и данных кода авторизации, полученных от ресурсной системы, и выдает Access Token (код доступа) и ID__TOKEN (набор данных пользователя, который необходимы для идентификации пользователя в ресурсной системе, в том числе внешний iD пользователя АС банка (sub), передаваемый внешним потребителям, сформированный на основе ID единой учетной записи пользователя, извлеченного из параметров операции аутентификации, а также параметр Nonce). Модуль 22 маршрутизации, получив ID TOKEN, проверяет значение Nonce, которое сохранено в параметрах операции пользователя с тем, которое получено в ID_TOKEN. Если значения совпадают, то модуль 22 маршрутизации идентифицирует клиента по внешнему ID пользователя АС банка (sub), полученному в ID_TOKEN. Далее модуль 22 маршрутизации авторизует пользователя и возвращает в модуль 21 страницу для отображения пользователю, которая перенаправляется в устройство 11 взаимодействия с веб-сайтом. Таким образом, пользователь устройства 11 взаимодействия с веб-сайтом получает авторизированный доступ в ресурсную систему 20.

В общем виде (см. фиг. 2) вычислительное устройство содержит объединенные общей шиной информационного обмена один или несколько процессоров (201), средства памяти, такие как ОЗУ (202) и ПЗУ (203), интерфейсы ввода/вывода (204), устройства ввода/вывода (205), и устройство для сетевого взаимодействия (206).

Процессор (201) (или несколько процессоров, многоядерный процессор и т.п.) может выбираться из ассортимента устройств, широко применяемых в настоящее время, например, таких производителей, как: Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором или одним из используемых процессоров в системе (200) также необходимо учитывать графический процессор, например, GPU NVIDIA с программной моделью, совместимой с CUDA, или Graphcore, тип которых также является пригодным для полного или частичного выполнения способа, а также может применяться для обучения и применения моделей машинного обучения в различных информационных системах.

ОЗУ (202) представляет собой оперативную память и предназначено для хранения исполняемых процессором (201) машиночитаемых инструкций для выполнения необходимых операций по логической обработке данных. ОЗУ (202), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.). При этом, в качестве ОЗУ (202) может выступать доступный объем памяти графической карты или графического процессора.

ПЗУ (203) представляет собой одно или более устройств постоянного хранения данных, например жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.),

оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов системы (200) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов B/B (204). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п.

Для обеспечения взаимодействия пользователя с вычислительной системой (200) применяются различные средства (205) B/B информации, например клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (206) обеспечивает передачу данных посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (206) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации в составе системы (200), например, GPS, ГЛОНАСС, BeiDou, Galileo.

Конкретный выбор элементов устройства (200) для реализации различных программно-аппаратных архитектурных решений может варьироваться с сохранением обеспечиваемого требуемого функционала.

Модификации и улучшения вышеописанных вариантов осуществления настоящего технического решения будут ясны специалистам в данной области техники. Предшествующее описание представлено только в качестве примера и не несет никаких ограничений. Таким образом, объем настоящего технического решения ограничен только объемом прилагаемой формулы изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ аутентификации пользователя, выполняемый по меньшей мере одним вычислительным устройством, содержащий этапы, на которых:

получают запрос на аутентификацию пользователя;

получают данные о типе аутентификации, выбранном пользователем, и идентификатор (ID) единой учетной записи пользователя;

регистрируют операцию аутентификации пользователя и формируют идентификатор операции;

генерируют QR-код, в который включается информация об идентификаторе операции, и назначают ему соответствующий статус;

отслеживают статус QR-кода;

на основе данных о статусе QR-кода определяют, что операция аутентификации пользователя подтверждена пользователем, причем в параметры операции сохраняют ID единой учетной записи пользователя и аутентифицируют пользователя по ID единой учетной записи пользователя.

2. Способ по п.1, характеризующийся тем, что дополнительно выполняют этапы, на которых:

на основе данных о статусе QR-кода определяют, что QR-код отсканирован пользователем;

направляют пользователю запрос на подтверждение операции аутентификации.

3. Способ по п.1, характеризующийся тем, что дополнительно выполняют этапы, на которых:

получают от устройства партнера запрос кода авторизации, в параметры запроса которого включается ID учетной записи ресурсной системы;

генерируют данные кода авторизации и направляют их ресурсной системе;

получают от ресурсной системы запрос кода доступа, в параметрах которого включаются данные кода авторизации и ID учетной записи ресурсной системы;

авторизуют ресурсную систему на основе результатов проверки данных кода авторизации, направленных ресурсной системе, и данных кода авторизации, полученных от ресурсной системы;

отправляют в ресурсную систему код доступа, содержащий ID единой учетной записи пользователя.

4. Способ по п.3, характеризующийся тем, что дополнительно выполняют этапы, на которых:

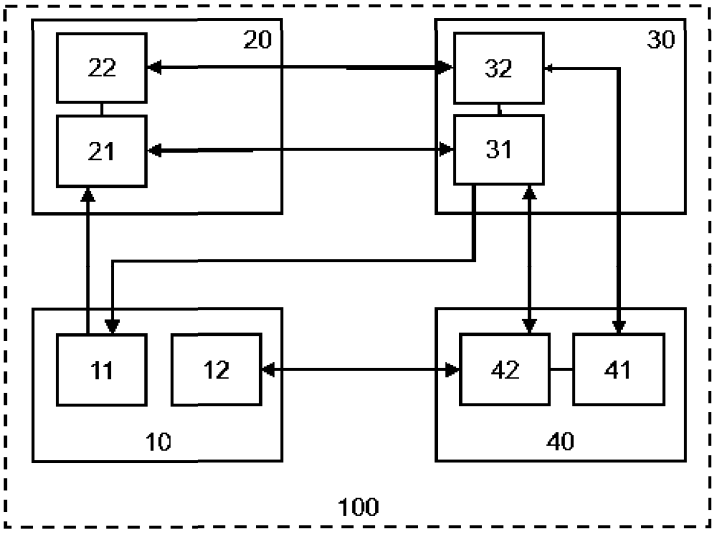
включают в параметры запроса кода авторизации параметр для предотвращения подделки межсайтовых запросов, сгенерированный устройством ресурсной системы, причем сгенерированные данные кода авторизации перенаправляют пользователю вместе с параметром для предотвращения подделки межсайтовых запросов;

получают от пользователя посредством устройства ресурсной системы данные кода авторизации и параметр для предотвращения подделки межсайтовых запросов;

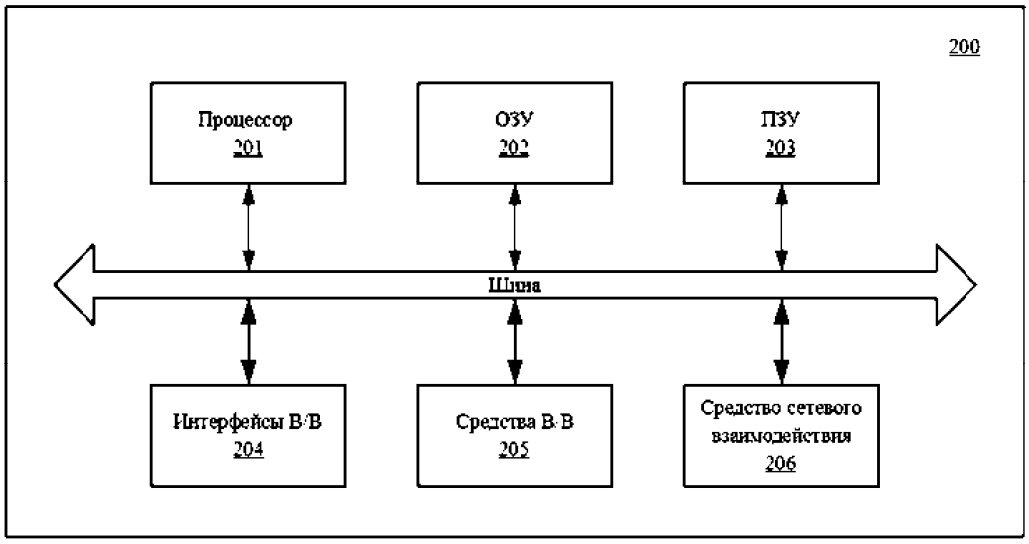
на основе результатов сравнения параметра для предотвращения подделки межсайтовых запросов, сгенерированного устройством ресурсной системы, и упомянутого параметра, полученного от пользова-

теля, формируют запрос на получение кода доступа, в который включаются данные кода авторизации.

5. Система аутентификации пользователя, содержащая по меньшей мере одно вычислительное устройство и по меньшей мере одно устройство памяти, содержащее машиночитаемые инструкции, которые при их исполнении по меньшей мере одним вычислительным устройством выполняют способ по любому из пп.1-4.



Фиг. 1



Фиг. 2