(19) Евразийское патентное ведомство

(11) 038055 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.06.29

(21) Номер заявки
201892088

(22) Дата подачи заявки
2018.10.16

(51) Int. Cl. ***G06F 21/62*** (2006.01)
G06F 21/32 (2006.01)

(54) СПОСОБ И СИСТЕМА ДЛЯ ДОВЕРЕННОГО БЕЗБУМАЖНОГО ПРЕДЪЯВЛЕНИЯ ДОКУМЕНТОВ

(31) **2018134907**
(32) **2018.10.03**
(33) **RU**
(43) **2020.04.30**

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

(74) Представитель:
Герасин Б.В. (RU)

(56) US-A1-20100088233
US-B1-8296477
US-A1-20160224773

(57) Изобретение относится, в общем, к сфере обработки цифровой информации, а в частности, к способу и системе для доверенного безбумажного предъявления документов. Техническим результатом, достигаемым при решении вышеуказанной проблемы, является обеспечение доверенного защищенного предъявления цифровых копий документов пользователя, с обеспечением подтверждения их неизменности и аутентичности. Заявленное решение реализуется с помощью системы для доверенного безбумажного предъявления документов, содержащей по меньшей мере один процессор, связанный с модулем регистрации и аутентификации, который выполнен с возможностью регистрации новых пользователей системы и последующей их аутентификации; модулем биометрической аутентификации и идентификации, который выполнен с возможностью получения биометрических данных пользователя и их последующего анализа в целях аутентификации для совершения операций с документами; модулем добавления документов, который предназначен для добавления в систему цифровых копий документов пользователя; модулем хранения документов, который предназначен для хранения и управления добавленными цифровыми копиями документов пользователей; модулем предъявления документов, который предназначен для предоставления добавленных цифровых копий документов получателю и настройки политик доступа предоставления упомянутых документов получателю; модулем электронной подписи документа, который предназначен для подписи добавляемых цифровых копий документов личной усиленной квалифицированной электронной подписью (УКЭП); модулем запроса документа, который предназначен для получения по меньшей мере одной подписанной копии цифрового документа пользователя, сохраненных в модуле хранения документов, от модуля предъявления документа.

038055 B1

038055 B1

Область техники

Настоящее решение относится, в общем, к сфере обработки цифровой информации, а в частности, к способу и системе для доверенного безбумажного предъявления документов.

Уровень техники

В качестве аналога заявленного решения можно рассматривать систему электронного документооборота Индии - DigiLocker (https://digilocker.gov.in). Данный программный продукт позволяет использовать цифровые копии государственных документов граждан, например, паспорт, водительское удостоверение, при их предъявлении уполномоченным лицам, организациям, и другом применении, в котором оригинал документа заменяется его цифровой копией, доступной посредством вычислительной сети Интернет.

Решение DigiLocker основано на цифровой платформе, которая позволяет хранить цифровые копии документов в профиле пользователя, который связан с уникальным идентификатором, в частности, с государственным номером гражданина Индии (Aadhaaar ID). При этом, основным недостатком данного решения является отсутствие применения дополнительных средств удостоверения аутентичности и неизменности документов, цифровые копии которых могут быть связаны с профилем пользователя, в частности, применении биометрической аутентификации предъявителя документов и использование электронной подписи копии документов. Также, известное решение ограничено в функционале по запросу и предоставлении копии документа, т.к. позволяет лишь формировать ссылку на облачное хранилище, содержащее копию документа, которое может быть передано соответствующему устройству посредством гиперссылки.

Раскрытие изобретения

Решаемой технической проблемой или технической задачей является обеспечение платформы доверенного предъявления цифровых копий документов пользователя с подтверждением их неизменности и аутентичности.

Техническим результатом, достигаемым при решении вышеуказанной проблемы, является обеспечение доверенного защищенного предъявления цифровых копий документов пользователя, с обеспечением подтверждения их неизменности и аутентичности.

Также, дополнительным эффектом от применения заявленного решения является повышение защищенности процесса предъявления документов пользователем, за счет использования биометрической идентификации предъявителя документов и использования средств криптографической защиты для копий документов, хранимых в облачной платформе.

Заявленное решение реализуется с помощью системы для доверенного безбумажного предъявления документов, содержащей по меньшей мере один процессор, связанный с модулем регистрации и аутентификации, который выполнен с возможностью регистрации новых пользователей системы и последующей их аутентификации;

модулем биометрической аутентификации и идентификации, который выполнен с возможностью получения биометрических данных пользователя и их последующего анализа в целях аутентификации для совершения операций с документами;

модулем добавления документов, который предназначен для добавления в систему цифровых копий документов пользователя;

модулем хранения документов, который предназначен для хранения и управления добавленными цифровыми копиями документов пользователей;

модулем предъявления документов, который предназначен для предоставления добавленных цифровых копий документов получателю и настройки политик доступа предоставления упомянутых документов получателю;

модулем электронной подписи документа, который предназначен для подписи добавляемых цифровых копий документов личной усиленной квалифицированной электронной подписью (УКЭП);

модулем запроса документа, который предназначен для получения по меньшей мере одной подписанной копии цифрового документа пользователя, сохраненных в модуле хранения документов, от модуля предъявления документа.

В одном из частных вариантов реализации системы регистрация пользователей осуществляется с помощью по меньшей мере одного идентификатора, выбираемого из группы: СНИЛС, номер телефона, адрес электронной почты, номер/серия паспорта, ИНН, номер медицинского полиса, уникальный идентификатор (УИД).

В другом частном варианте реализации системы после первичной регистрации пользователя выполняется его первичная аутентификация с помощью направления сообщения для последующего подтверждения на устройство пользователя с помощью сотовой и/или Интернет связи.

В другом частном варианте реализации системы сообщение содержит код подтверждения или гиперссылку на ресурс аутентификации.

В другом частном варианте реализации системы модуль аутентификации дополнительно назначает для каждого зарегистрированного пользователя предпочтительный способ аутентификации.

В другом частном варианте реализации системы модуль хранения документов представляет собой

облачное хранилище.

В другом частном варианте реализации системы биометрической аутентификации и идентификации регистрирует по меньшей мере один биометрический образец пользователя, выбираемый из группы: отпечаток пальца, изображение лица, аудиозапись голоса, изображение сетчатки глаза, изображение радужной оболочки, рисунок вен ладони, геометрия кисти руки.

В другом частном варианте реализации системы модуль добавления документов формирует цифровые копии документов на основании загружаемых пользователями в систему документов и/или с помощью запроса копий документов у соответствующих органов - издателей документов.

В другом частном варианте реализации системы модуль предъявления документа выполняет формирование QR-кода, содержащего ссылку на по меньшей мере один документ пользователя, содержащийся в модуле хранения.

В другом частном варианте реализации системы модуль электронной подписи документов дополнительно проверяет валидность электронной подписи (ЭП) для каждой копии документа.

В другом частном варианте реализации системы копия документа может содержать групповую ЭП.

В другом частном варианте реализации системы подписание копий документов УКЭП осуществляется с помощью облачной платформы.

Заявленное решение также реализуется с помощью способа предоставления заверенной цифровой копии документа пользователя, в ходе реализации которого

создают в облачной системе доверенного документооборота (ОСДД) профиль пользователя, который содержит, по меньшей мере, УИД пользователя и его биометрический образец, содержащий, по меньшей мере, изображение лица пользователя;

добавляют в упомянутую систему по меньшей мере одну цифровую копию документа пользователя;

осуществляют подписание упомянутой копии документа в ОСДД с помощью УЭКП пользователя;

устанавливают политики доступа для каждой копии добавленного документа в ОСДД;

связывают добавленные цифровые копии документов с соответствующим профилем пользователя;

с помощью устройства пользователя формируют информационный пакет, содержащий электронную ссылку на по меньшей мере одну копию документа и УИД пользователя, связанные с его профилем в ОСДД;

передают упомянутый пакет на устройство получателя;

на устройстве получателя осуществляют извлечение копии документа из полученной ссылки и проверяют ЭП пользователя;

получают с помощью устройства получателя биометрический образец пользователя, содержащий изображение лица пользователя;

передают с помощью устройства получателя полученный биометрический образец пользователя и полученный УИД пользователя в ОСДД и выполняют их сравнение с данными, связанными с профилем пользователя;

в случае успешного сравнения данных с профилем пользователя устройство получателя осуществляет обработку документов согласно установленной политике доступа.

В одном из частных вариантов реализации способа для копии документа содержит дополнительную ЭП.

В другом частном варианте реализации способа ОСДД предоставляет доступ к копии документа в случае проверки дополнительной ЭП.

В другом частном варианте реализации способа информационный пакет представляет собой QR-код.

В другом частном варианте реализации способа биометрический образец пользователя дополнительно включает по меньшей мере одно из: отпечаток пальца,

изображение сетчатки глаза, изображение радужной оболочки, изображение вен ладони, изображение геометрии кисти или образец голоса.

Заявленное решение также реализуется с помощью способа предоставления заверенной цифровой копии документа пользователя, при реализации которого

создают в облачной системе доверенного документооборота (ОСДД) профиль пользователя, который содержит, по меньшей мере, УИД пользователя, первый биометрический образец, который является изображением лица пользователя, и второй дополнительный биометрический образец;

добавляют в упомянутую систему по меньшей мере одну цифровую копию документа пользователя;

осуществляют подписание упомянутой копии документа в ОСДД с помощью УЭКП пользователя;

устанавливают политики доступа для каждой копии добавленного документа в ОСДД;

связывают добавленные цифровые копии документов с соответствующим профилем пользователя;

формируют с помощью устройства получателя первый запрос на предоставлении копии документа пользователя, причем запрос содержит получение изображения лица пользователя и дополнительного биометрического образца, соответствующего второму биометрическому образцу, сохраненному в про-

филе пользователя в ОСДД;

направляют упомянутый запрос в ОСДД;

с помощью ОСДД проверяют полученный запрос с профилем пользователя и передают на устройство получателя УИД пользователя;

формируют с помощью устройства получателя второй запрос, содержащий УИД пользователя, для получения цифровой копии документа;

получают с помощью устройства получателя доступ к по меньшей мере одной копии документа пользователя с соответствующей политикой доступа.

В частном варианте реализации способа дополнительный биометрический образец пользователя включает по меньшей мере одно из: отпечаток пальца, изображение сетчатки глаза, изображение радужной оболочки, изображение вен ладони, изображение геометрии кисти или образец голоса.

Краткое описание чертежей

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

фиг. 1 иллюстрирует архитектуру системы доверенного документооборота;

фиг. 2 иллюстрирует пример взаимодействия пользователя с системой документооборота;

фиг. 3 иллюстрирует пример схемы взаимодействия при предоставлении цифровой копии документа с помощью устройства пользователя;

фиг. 4, 5 иллюстрируют процесс предоставления цифровой копии документа с помощью устройства пользователя;

фиг. 6 иллюстрирует пример схемы взаимодействия при запросе цифровой копии документа с помощью устройства получателя;

фиг. 7, 8 иллюстрируют процесс запроса цифровой копии документа с помощью устройства получателя;

фиг. 9 иллюстрирует пример вычислительного устройства.

Осуществление изобретения

Заявленное решение позволяет с помощью облачной системы доверенного электронного документооборота (ОСДД) хранить и использовать для дальнейшего предоставления в необходимые органы и/или должностным лицам цифровые копии документов пользователя. К таким документам, в частности, могут относиться: паспорт, водительское удостоверение, страховой полис, медицинский полис, СНИЛС, свидетельство транспортного средства, паспорт технического средства и т.п.

На фиг. 1 представлена общая структура ОСДД (100). Пользователь (20) с помощью модуля аутентификации и регистрации (101) осуществляет создание своего профиля в системе (100). Пользователь (20) предоставляет данные для регистрации в системе, например уникальный идентификатор гражданина, которым может быть единый идентификатор гражданина (ЕИГ), ФИО, дата рождения, документ удостоверяющий личность, номер мобильного телефона, биометрические образцы, номер СНИЛС, адрес электронной почты, номер/серия паспорта, ИНН, номер медицинского полиса и т.п. Модуль (101) предназначен для регистрации нового пользователя системы и последующей аутентификации пользователя. Обычная аутентификация необходима для получения возможности использования функций модуля биометрической аутентификации и идентификации (102), модуля предъявления документа (104), модуля хранения документа (105). Модуль (101) направляет документы, предоставляемые для регистрации пользователем (20), для проверки во внешних системах, например, модуль (101) может взаимодействовать с "единым реестром уникальных идентификаторов граждан РФ" для проверки корректности введенного идентификатора, с реестром соответствия номеров мобильных телефонов и уникального идентификатора пользователя, с системой отправки смс-сообщений, с внутренней базой данных системы и т.д.

Пользователь (20) также предоставляет биометрические образцы для последующей аутентификации при предъявлении цифровых копий документов. Обязательным требованием является предоставление изображения лица пользователя (20), которое будет выступать основным критерием для его аутентификации. Дополнительно с профилем пользователя (20) могут связываться такие биометрические образцы, как: отпечаток пальца, аудиозапись голоса, изображение сетчатки глаза, изображение радужной оболочки, рисунок вен ладони, геометрия кисти руки и т.п.

Регистрация нового пользователя осуществляется следующим образом. Система (100) запрашивает у пользователя (20) уникальный идентификатор, пример которого был указан выше. В случае использования СНИЛС в качестве уникального идентификатора пользователя (20), система (100) дополнительно запрашивает номер мобильного телефона пользователя (20). В случае использования уникального идентификатора пользователя система (100) может запросить дополнительно номер мобильного телефона пользователя (20) или автоматически загрузить номер мобильного телефона пользователя, в случае, если этот номер (сим-карта) привязан к уникальному идентификатору пользователя в доступной смежной системе;

В случае обнаружения нескольких мобильных номеров система (100) предлагает выбрать один конкретный, который будет привязан в системе (100) к профилю пользователя. Получив уникальный идентификатор и/или номер мобильного телефона пользователя (дополнительно может использоваться адрес

электронной почты), система (100) с помощью модуля (101) отправляет на указанный номер мобильного телефона смс-сообщение с кодом подтверждения, который должен быть введен пользователем (20) в системе (100). Получив корректный код подтверждения, система (100) регистрирует нового пользователя (20), добавляя запись вида "уникальный идентификатор пользователя и/или номер мобильного телефона пользователя" в собственную базу данных, в которой хранится информация о профилях пользователей (20). Также профиль пользователя может содержать иную дополнительную информацию, например один или несколько адресов электронной почты, идентифицирующая информация, биометрические данные и т.п.

Система (100) предоставляет пользователю (20) возможность выбрать варианты последующей аутентификации, например, с помощью биометрического ввода (сканер отпечатка пальца, сканер сетчатки глаза/радужной оболочки и т.п.), с помощью мобильного устройства (смартфон, планшет), аутентификации по PIN-коду, двухфакторной аутентификации по связке логин/пароль и подтверждения кодом из СМС-сообщения или приложения для генерирования одноразовых кодов доступа и т.п.

В случае использования метода двухфакторной аутентификации система (100) в качестве логина использует уникальный идентификатор пользователя, полученный ранее, и секретную фразу, которую предлагается придумать и запомнить пользователю на этом этапе. Дополнительно может применяться биометрический образец голоса пользователя с произношением секретной фразы. После этого система (100) добавляет соль к хэшу парольной фразы и формирует новый хэш от полученной строки, который добавляет к записи о пользователе (20) в собственной базе данных.

Аутентификация зарегистрированного пользователя (20) в системе (100) осуществляется следующим образом. При входе зарегистрированного пользователя (20) в систему (100) ему предлагается использовать один из методов аутентификации: по отпечатку пальца, по PIN-коду, по связке логин + пароль и коду подтверждения из смс-сообщения или другой тип аутентификации, выбранный пользователем в процессе регистрации. В случае использования аутентификации по связке логин + пароль и коду подтверждения из смс-сообщения пользователь вводит секретную фразу, придуманную ранее и свой УИД. Система (100) с помощью модуля (101) сверяет введенные данные с теми, что хранит в собственной базе данных, и в случае полного совпадения отправляет на номер мобильного телефона пользователя (20), который получает из записи о пользователе в собственной базе данных, смс-сообщение с кодом подтверждения. Далее пользователь (20) вводит код подтверждения из смс-сообщения, и в случае совпадения данных аутентификация считается успешной.

После успешной аутентификации система (100) наделяет пользователя (20) правами использования функций следующих модулей: биометрической аутентификации и идентификации (102), предъявления документа (104), хранения документа (105). Модуль биометрической аутентификации и регистрации (102) предназначен для дополнительной аутентификации пользователя (20) и предоставления пользователю (20) на основе этой аутентификации специализированных прав. Также модуль (102) предназначен для идентификации личности пользователя (20) в процессе предъявления цифровой копии документа с помощью системы (100).

Входными данными модуля (102) являются пользовательский ввод и контекстная информация, полученная из смежных систем. Модуль (102) взаимодействует с центром биометрической аутентификации (108) для реализации алгоритмов биометрической проверки, с внутренней базой данных системы, с модулем запроса документов (107) для сбора биометрического образца, модулем электронной подписи документов (106), модулем добавления документов (103).

Для осуществления успешной аутентификации пользователь (20) должен единожды зарегистрироваться в центре биометрической аутентификации (108). Центром биометрической аутентификации (108) может быть отдельный специальный орган, который позволяет всем пользователям (20) очно предоставить биометрические образцы и производит удостоверение личности заявителя (20). При этом создается соответствие между биометрическими образцами пользователя и идентифицирующей его информацией, в частности, номером паспорта или уникальным идентификатором пользователя, номером мобильного телефона, ФИО, дата рождения и любая другая информация, позволяющая упростить идентификацию пользователя (20).

Центром биометрической аутентификации (108) также может выступать любая смежная система, предоставляющая открытый интерфейс для биометрической аутентификации и идентификации, имеющая профиль пользователя (20), содержащий идентифицирующую информацию и соответствующая законодательству РФ. Модуль биометрической аутентификации (102) проверяет права пользователя (20) в системе (100). Такими правами могут быть, например, обычный пользователь, получатель копии документа (в приложении доступны функции получения и проверки подлинности документов), издатель (может добавлять в хранилище пользователя документ, который выпускает, например, электронный полис ОСАГО может автоматически быть добавлен страховой компанией как издателем в хранилище пользователя), доверенный пользователь (доступен функционал биометрической регистрации новых пользователей). При этом получатели в общем случае получают доступ к модулю запроса документов (107) и дополнительно им назначается роль, в соответствии с которой они могут запрашивать документы (например, роль - ДПС, может запрашивать только водительское удостоверение, СТС, ПТС и полис ОСАГО;

ФНС - копии ИНН, паспорта и т.п.). Аутентификация зарегистрированного пользователя (20) с помощью модуля (102) осуществляется следующим образом. Система (100) запрашивает пользователя (20) предоставить биометрический образец - изображение лица, которое пользователь (20) получает с помощью камеры мобильного устройства, либо записывает видеоролик, передаваемый в систему (100). Система (100) получает изображение от устройства пользователя или выбирает кадр из полученного видеоролика.

Система (100) получает от модуля регистрации и аутентификации (101) контекстную информацию о пользователе (20), который в данный момент аутентифицирован в приложении, в частности, уникальный идентификатор и номер мобильного телефона. Полученная информация отправляется в смежный центр биометрической аутентификации (108), где производится сверка полученного биометрического образца пользователя (20) с образцом, хранящимся в центре (108). Для облегчения поиска может дополнительно осуществляется поиск по УИД пользователя и номеру мобильного телефона. В случае корректного совпадения биометрических образцов, УИД пользователя (20) и номера мобильного телефона, система (100) отправляет на номер мобильного телефона смс-сообщение с кодом подтверждения, который должен быть введен пользователем (20) в системе (100). В случае успешного ввода кода подтверждения пользователь (20) считается аутентифицированным.

При первой биометрической аутентификации система (100) получает от смежного центра биометрической аутентификации (108) контекстные данные пользователя: ФИО, дата рождения и другую информация, позволяющая упростить идентификацию пользователя (20) в дальнейшем. Данная информация сохраняется в системе (100) и не может быть изменена пользователем (20).

При успешной аутентификации система (100) получает от центра (108) роль пользователя и на ее основании предоставляет пользователю (20) доступ к функционалу системы (100). Биометрическая идентификация доступна пользователям (20) с правами "получатель" и необходима для удостоверения личности лица, предъявляющего документ. Идентификация осуществляется следующим образом. Получатель цифровой копии документа делает фотографию пользователя (20) с помощью собственного мобильного устройства. Система (100) отправляет фотографию в центр биометрической аутентификации (108), где происходит анализ фотографии на предмет схожести с изображением пользователя (20). По завершению поиска система (100) предоставляет отчет о степени схожести изображения пользователя (20) с данными, хранящимися в центре (108) для зарегистрированных пользователей (20).

В ряде случаев помимо фотографии система (100) может отправлять некоторые контекстные данные в центр биометрической аутентификации (108) для ускорения поиска соответствия, например, различного вида метаданные. Такие данные могут быть предварительно переданы пользователем получателю с помощью технологии кодирования информации в QR-код или NFC. В случае превышения необходимого порога "похожести" пользователь (20) считается идентифицированным, и получатель может сравнить документы, предъявленные пользователем с зарегистрированными доверенными пользователями.

Система (100) вместе с результатом получает из центра биометрической аутентификации (108) следующую информацию о предъявителе: УИД, сертификат электронной подписи. В дальнейшем эта информация используется для загрузки и проверки документа пользователя (20). Также система (100) получает данные о роли получателя. В дальнейшем эта информация используется для проверки прав получателя на запрашиваемый один или несколько документов пользователя (20).

Модуль добавления документов (103) предназначен для добавления в систему (100) цифровых копий документов пользователя (20), которые хранятся в системе (100). Предусмотрено несколько возможностей по добавлению документа: самостоятельное добавление документа пользователем (20), запрос на создание документа, или запрос на выпуск документа. Самостоятельное добавление документа в хранилище может быть, как доверенным, так и нет. Доверенное добавление цифровой копии документа подразумевает возможность предъявлять документ получателю по аналогии с обычным бумажным документом. Документы, добавляемые самостоятельно проходят процедуру классификации для автоматического добавления в правильную ячейку в хранилище модуля хранения документов (105).

Любое доверенное добавление документа возможно только после биометрической аутентификации пользователя (20). Каждая доверенная цифровая копия документа подписывается УЭКП пользователя (20).

Самостоятельное добавление копии документа пользователем осуществляется следующим образом. Пользователь (20) выполняет биометрическую аутентификацию посредством модуля (102). Далее пользователь (20) загружает в систему (100) фотографию или скан-копию документа, который он хочет добавить, при этом пользователь (20) самостоятельно указывает тип документа, например, паспорт, полис ОСАГО и т.п. Система (100) осуществляет проверку файла на наличие личной ЭЦП пользователя. Если документ содержит личную ЭЦП пользователя, то ее характеристики сверяются с сертификатом пользователя, который заранее загружается из центра биометрической аутентификации (108). Если сертификаты совпадают, то производится проверка на наличие дополнительных подписей в файле. Если сертификаты не совпадают, то система (100) отказывает пользователю в добавлении документа.

В случае обнаружения дополнительных ЭЦП система (100) разделяет их на следующие категории: чужая личная ЭЦП, системная ЭЦП, доверенная ЭЦП Издателя. В случае обнаружения чужой личной

ЭЦП система (100) проверяет тип добавленного документа с помощью автоматического классификатора документов. Если тип документа не совпадает с указанным ранее, то система (100) отказывает в добавлении документа. Если тип документа совпадает с указанным ранее, то система (100) проверяет по внутреннему справочнику необходимость и возможность наличия нескольких личных ЭЦП для данного документа. Если документ подразумевает групповую ЭЦП, то производится проверка на наличие дополнительных подписей в файле. Если документ не подразумевает групповую ЭЦП, то система (100) отказывает в добавлении документа.

В случае обнаружения доверенной ЭЦП Издателя система (100) проверяет подлинность ЭЦП. В случае отрицательного результата система (100) отказывает в добавлении документа. В случае положительного результата проверки система (100) проверяет наличие системной ЭЦП. Если системная ЭЦП присутствует, то документ добавляется в модуль хранения (105), связанный с профилем пользователя (20). Если системная ЭЦП отсутствует, то система (100) уточняет у пользователя (20) о необходимости добавления чужих личных ЭЦП на копию документа. Если ответ положительный, то система (100) производит автоматическую классификацию документа и сверяет по внутреннему справочнику возможность и необходимость нескольких личных ЭЦП на документе.

Если документ подразумевает групповую подпись, то система (100) предоставляет пользователю (20) возможность предоставить доступ к документу другим пользователям. После подписания документа всеми заинтересованными пользователями система (100) автоматически проставляет системную ЭЦП, которая изменяет технические характеристики документа на "не редактируемый" и добавляет документ в хранилище, связанное с профилем пользователя.

В случае обнаружения доверенной ЭЦП Издателя без личной ЭЦП система (100) отказывает в добавлении документа. В случае обнаружения системной ЭЦП без личной ЭЦП система (100) также отказывает в добавлении документа. В случае отсутствия ЭЦП на документе система (100) предлагает пользователю добавить личную ЭЦП. В случае положительного ответа пользователя (20) система (100) передает документ внешней системе облачной ЭЦП (модуль 106), где проставляется личная ЭЦП пользователя (20). Далее система (100) уточняет у пользователя (20) о необходимости добавления чужих личных ЭЦП на копию документа.

Если ответ положительный, то система (100) производит автоматическую классификацию документа и сверяет по внутреннему справочнику возможность и необходимость нескольких личных ЭЦП на документе. Если документ подразумевает групповую подпись, то система (100) предоставляет пользователю (20) возможность предоставления доступа другим пользователем, в противном случае система (100) не позволяет этого сделать.

После подписания документа всеми заинтересованными пользователями система (100) автоматически проставляет системную ЭЦП, которая изменяет технические характеристики документа на "не редактируемый" и добавляет документ в хранилище пользователя, связанное с его профилем. Если ответ о личной ЭЦП отрицательный, то система (100) добавляет документ в хранилище пользователя, но при этом данный документ не признается доверенным.

Модуль хранения документов (105) предназначен для хранения и управления добавленными цифровыми копиями документов пользователей (20). Модуль (105) предоставляет функционал для манипуляций с этими документами, в частности, удаление, переименование, создание ячеек для хранения классифицированных документов и т.д. Модуль (105) может представлять собой облачное хранилище.

Добавление копии документа с помощью запроса на создание документа осуществляется следующим образом. Пользователь (20) выполняет биометрическую аутентификацию с помощью предоставления своего биометрического образца. Пользователь (20) выбирает документ, цифровую копию которого необходимо создать. Система (100) формирует необходимый пакет документов из добавленных пользователем ранее и запрос на создание цифровой копии документа. Система (100) передает запрос на создание документа, пакет необходимых документов, УИД пользователя и другие данные о пользователе в зависимости от запрашиваемого документа на сторону издателя. После успешной передачи запроса система (100) "резервирует" в модуле хранения (105) ячейку для конкретного типа копии документа, изготовление которой запрашивает пользователь (20).

В случае отсутствия необходимых документов в хранилище пользователя система предлагает добавить нужные документы. На стороне издателя полученный запрос может быть обработан тем способом, который наиболее удобен издателю: ручная обработка запроса, автоматическая обработка запроса. Автоматическая обработка осуществляется с помощью собственного программного обеспечения издателя, который взаимодействует с системой (100) с помощью программного интерфейса, предоставляемого системой (100). Ручная обработка осуществляется в соответствии с внутренними регламентами оператора. Добавление документа в хранилище пользователя осуществляется с помощью указания УИД пользователя. При получении созданного документа и уникального идентификатора система проверяет наличие "зарезервированной" ячейки в модуле хранения (105) для указанного идентификатора. В случае наличия данной ячейки документ добавляется в хранилище пользователя для его профиля. В случае отсутствия в доступе к хранилищу пользователя отказывается.

Добавление документа с помощью запроса на выпуск документа осуществляется следующим обра-

зом. Пользователь (20) выполняет биометрическую аутентификацию. В зависимости от подключенных к системе (100) партнеров (ведомств, коммерческих организаций и т.д., каждый партнер - уникальное подключение) пользователь запрашивает выпуск цифровой версии документа, который пользователь уже имеет на "бумажном" носителе.

Система (100) формирует запрос, который содержит УИД и пользовательские данные, и отправляет этот запрос на собственный модуль ("агент"), который интегрирован в среду партнера. После формирования запроса система (100) "резервирует" ячейку в модуле хранения (105) под конкретный тип документа для выбранного пользователя (20). Полученный запрос агент конвертирует в формат для автоматического запроса информации по наличию выпускаемого документа для пользователя (20) и отправляет в собственную базу данных партнера. В случае обнаружения документа пользователя (20) в базе данных партнера, например, паспортный стол или ФНС, агент формирует pdf-файл (или иной тип файла), в который добавляет информацию о документе из базы данных партнера.

После формирования pdf-файла агент обращается к системе ЭЦП партнера и подписывает pdf-файл ЭЦП партнера, что добавляет свойство доверия к файлу. Подписанный pdf-файл агент возвращает системе (100), используя УИД пользователя и наличие "зарезервированной" ячейки в модуле (105) для его профиля. Система (100) предлагает пользователю (20) подписать документ личной ЭЦП. В случае отрицательного ответа добавление документа отменяется. В случае положительного ответа система (100) отправляет документ в модуль электронной подписи документа (106), где к документу добавляется личная ЭЦП пользователя (20), таким образом, документу присваивается свойство неотказуемости.

После получения личной ЭЦП пользователя система (100) добавляет собственную ЭЦП к pdf-файлу и запрещает внесение изменений в указанный файл с копией документа. После получения всех ЭЦП система (100) добавляет документ в зарезервированную ячейку модуля хранения (105) для профиля пользователя (20). Модуль электронной подписи документов (106) предназначен для подписи добавляемых в систему (100) цифровых копий документов личной усиленной квалифицированной электронно-цифровой подписью (УКЭП). Данный модуль (106) может выполняться в виде смежного сервиса, выполняющего подписание документов облачной ЭЦП. Интеграция осуществляется после биометрической регистрации пользователя (20). Существует два вида возможной интеграции: интеграция с существующим аккаунтом облачной ЭЦП, создание нового аккаунта в сервисе облачной ЭЦП. В рамках интеграции модуль передает системе облачной ЭЦП копии документов (файлы) для подписи личной ЭЦП пользователя.

Модуль предъявления документов (104) предназначен для предоставления добавленных цифровых копий документов получателю и настройки политик доступа предоставления упомянутых документов получателю. Модуль (104) обеспечивает удаленное и личное предъявления заранее добавленных копий документов получателю. Модуль запроса документов (107) предназначен для получения копии цифрового документа пользователя (20), сохраненных в модуле хранения документов (105), по запросу модуля предъявления документа (104).

Система (100) представляет собой программно-аппаратное решение, например, облачную платформу на базе одного или нескольких серверов. Основной процесс программной обработки данных для осуществления работы системы (100) выполняет один или несколько процессоров (вычислительный модуль). Указанные модули системы (100) связаны с одним или несколькими процессорами для осуществления необходимых операций информационной обработки для реализации их функционала. Специалисту также должно быть очевидно, что могут применяться различные решения в области параллельной обработки информационных потоков при выполнении необходимых алгоритмических вычислений при работе компьютерного устройства (или нескольких устройств). На фиг. 2 представлен пример взаимодействия пользователя (20) с ОСДД (100). Как было указано выше, пользователь (20) передает данные (201) для регистрации в ОСДД (100). Пользователь (20) предоставляет изображение своего лица как основной биометрический образец (202) в центр биометрической аутентификации (108). После регистрации пользователя (20) в ОСДД (100) для него создается профиль (250), который будет использоваться для доверенного обмена цифровыми копиями документов. В профиле (250) пользователь (20) осуществляется установки политики доступа для каждой копии цифрового документа. Под политикой доступа также подразумевается обеспечение доступа соответствующего лица/органа к цифровым копиям документов, что обусловлено перечнем документов, которые такое лицо или орган могут использовать в части идентификации и/или наличия разрешений у пользователя (20).

Как представлено на фиг. 3, предоставление цифровых копий документов пользователя (20) может осуществляться удаленно на устройство получателя документов (22) с помощью электронного устройства пользователя (21). Под термином "удаленно" понимается передача цифровых копий документов посредством информационных пакетов с помощью каналов передачи данных, например, TCP/IP, GSM/3G/4G, Wi-Fi, радиосвязь (Bluetooth, BLE, NFC) и т.п.

Согласно фиг. 4 способ удаленного предоставления документов (300) заключается в следующем.

Пользователь (20) формирует личный профиль (250) в ОСДД (100) с помощью вышеописанного процесса регистрации (этап 301). Далее выполняется загрузка в профиль (250) одной или несколько копий документов (этап 302), по меньшей мере одна из которых будет представлена устройству получателя (22). Добавленные копии документов в профиль пользователя (250) подписываются ЭП (УЭКП) пользо-

вателя (этап 303) для выполнения требования по их аутентичности и неотказуемости.

Для каждой подписанной копии документа в профиле (250) устанавливается соответствующая политика доступа, обеспечивающая предоставление для обработки данной копии уполномоченному (доверенному) устройству получателя (22) (этап 304). Далее пользователь (20) с помощью своего устройства (21), например, смартфона или планшета, выбирает одну или несколько копий документов из своего профиля (250) для передачи на устройство получателя (22). Из выбранных документов формируется информационный пакет для передачи на устройство (22) каналу передачи данных (этап 305).

На фиг. 5 представлен процесс обработки (400) информационного пакета, получаемого от устройства пользователя (21), с помощью устройства получателя (22). Информационный пакет может представляться в виде гиперссылки на цифровую копию документа с дополнительной информацией, например, УИД пользователя (20) в ОСДД (100), дополнительные метаданные, связанные с профилем пользователя (250). Пакет может быть зашифрован в QR-код или иной вид, пригодный для передачи с помощью радиоканала (Bluetooth, NFC и т.п.). Гиперссылка в пакете данных ведет к соответствующей копии документа, связанной с профилем пользователя (250). После получения информационного пакета устройством получателя (22), выполняется его последующая обработка (этап 401).

На этапе (402) выполняется переход по ссылке, полученной в информационном пакете от устройства пользователя (21). Устройство получателя (22) выполняет запрос на получение копии документа согласно полученной гиперссылке в ОСДД (100). Далее устройство получателя (22) проверяет наличие ЭП копии запрашиваемого документа (этап 403). Проверка ЭП выполняется с помощью запроса в модуль ЭП документов (106) в ОСДД (100). Если все ЭП валидны, то затем выполняется идентификация личности пользователя (20) с помощью устройства получателя (22).

Идентификация пользователя (20), предъявляющего копии документов посредством информационного пакета, выполняется с помощью получения биометрического образца пользователя, в частности, изображения его лица в момент проверки (этап 404). Получение изображение лица может осуществляться с помощью камеры, встроенной в устройство получателя (22), либо получаться с помощью связанного с устройством (22) средством фотовидеофиксации (например, камеры наблюдения, WEB-камеры, PTZ-камеры и т.п.).

После получения изображения лица пользователя (20) устройство получателя (22) формирует информационный пакет, содержащий фотоизображение пользователя (20) и УИД, полученный из переданного информационного пакета от устройства (21) (этап 405). Сформированный устройством (22) пакет передается в ОСДД (100) для проверки биометрического образца пользователя (202) и связанного с ним УИД. Полученные данные на этапе (406) ОСДД (100) проверяет с помощью передачи соответствующего запроса в центр биометрической аутентификации (108), который выполняет анализ схожести полученного изображения пользователя с информацией, хранящейся в его профиле (250). Анализ может выполняться с помощью различных фотограмметрических и/или аналитических алгоритмов. Дополнительно центр биометрической аутентификации (108) может направлять сертификат ЭП пользователя (20), который сравнивается с сертификатом, полученным с документом ранее при его загрузке в профиль пользователя (250).

В случае успешной проверки личности пользователя (20) на этапе (407) устройство получателя (22) принимает полученную по гиперссылке копию документа от устройства пользователя (21), ассоциирует представленную копию с надлежащим пользователем (20) и осуществляет дальнейшее использование копии документа согласно внутренним регламентам работы.

В качестве примера, пользователь (20) добавил в систему СТС, ПТС, ОСАГО и водительское удостоверение. И разрешил получателю (22) загружать автоматически только водительское удостоверение. Сотрудник ДПС с ролью инспектор может загружать только документы вида: водительское удостоверение, СТС, ОСАГО при выполнении биометрической аутентификации пользователя (20), например, с помощью служебного смартфона или планшета (22).

В случае ошибки идентификации предъявителя копии документа (этап 408), ОСДД (100) передает соответствующее сообщение на устройство получателя (22), которое отказывает в использовании полученной копии документа.

Как было указано выше в описании, копия документа пользователя (20) может содержать дополнительную ЭП, например, органа - издателя. В этом случае подтверждение аутентичности и неотказуемости копии документа предъявителя выполняется при условии проверки всех ЭП копии документа.

На фиг. 6 представлен вариант осуществления заявленного решения, при котором запрос копии документа устройством получателя (22) выполняется без использования электронного устройства пользователя (21). В данном случае используется помимо основного биометрического образца - изображения лица пользователя (20), один или несколько дополнительных образцов, которые позволяют идентифицировать предъявителя цифровых копий документов.

На фиг. 7 представлена последовательность этапов способа для выполнения указанной процедуры использования копий документов (500). На первом этапе (501) пользователь (20) выполняет процесс регистрации в ОСДД (100) с помощью предоставления биометрического образца - изображения лица, идентифицирующую его информацию и дополнительный биометрический образец для дальнейшего

формирования профиля пользователя (250) в ОСДД (100). В качестве дополнительного биометрического образца может использоваться, не ограничиваясь: отпечаток пальца, изображение сетчатки глаза, изображение радужной оболочки, изображение вен ладони, изображение геометрии кисти, образец голоса и т.п.

После процесса регистрации пользователь (20) загружает в профиль (250) одну или несколько копий документов (этап 502) и подписывает их личной УЭКП (этап 503).

Для каждого подписанного УЭКП цифрового документа устанавливается соответствующая политика доступа (этап 504).

На фиг. 8 представлен процесс (600) запроса и получения копий документов пользователя (20) с помощью устройства получателя (22) без формирования информационного пакета устройством пользователя (21).

При необходимости использования цифровой копии документа согласно способу (600) устройство получателя (22) фиксирует изображение лица пользователя (20), например, с помощью встроенной камеры или связанных с устройством (22) средств фотовидеофиксации (этап 601). Пользователь также предоставляет второй, дополнительный биометрический образец, который связан с его профилем (250) в ОСДД (100) (этап 602). Дополнительный биометрический образец получается с помощью средств, установленных или связанных с устройством получателя (22).

После получения двух биометрических образцов устройство (22) формирует первичный запрос (этап 603) и направляет его в ОСДД (100) (этап 604) для идентификации пользователя (20) (этап 605). В случае успешного сравнения биометрических образцов (этапа 606) с одним из зарегистрированных профилей (250) в ОСДД (100) последняя возвращает устройству получателя (22) УИД соответствующего пользователя (20), сертификат ЭП пользователя (этап 607). Дополнительно может также предоставляться информация о степени схожести основного биометрического образца пользователя (202). Далее устройство получателя (22) формирует второй запрос на получение доступа к одной или нескольким копиям документов профиля пользователя (250) (этап 608). Второй запрос содержит полученный ранее УИД пользователя, по которому предоставляется доступ к документам на основании политики доступа получателя (22) к одной или нескольким копиям документов.

Если для получателя (22) доступна по меньшей мере одна копия документа, то ОСДД (100) предоставляет доступ к ним в профиле пользователя (250). Копия документа (этап 609) может загружаться на устройство получателя (22). Далее проверяется наличие соответствующих ЭП копии документа и их валидность. Осуществляется сравнение полученного от ОСДД (100) сертификата ЭП пользователя, которой подписывается документ при его загрузке в ОСДД (100), и сертификат загруженного документа из второго запроса. Если проверка сертификатов успешна, то получатель (22) принимает копию документа как доверенный аутентичный документ должного предъявителя (20). Если на этапе (606) пользователь (20) не идентифицируется в ОСДД (100) (этап 610), то ОСДД (100) оповещает об этом устройство получателя (22), и пользователю (20) отказывается в предоставлении цифровых копий документов.

Как было указано выше, копия документа также может содержать несколько ЭП, например ЭП издателя или иного доверенного органа. В этом случае успешная проверка аутентичности копии документа будет только в случае успешной проверки всех ЭП такого документа.

На фиг. 9 представлен пример вычислительного устройства (700), которое применяется для реализации заявленного решения. Устройство (700) может выбираться из широкого спектра известных устройств, обеспечивающих необходимый функционал, например, компьютер, ноутбук, сервер, планшет, смартфон, портативная игровая приставка, мейнфрейм, суперкомпьютер и т.п. Как было указано выше, устройство пользователя (21), устройство получателя (22), ОСДД (100), могут быть частично организованы на базе или представлять собой один из примеров устройства (700). В общем случае, вычислительное устройство (700) содержит объединенные общей шиной один или несколько процессоров (701), средства памяти, такие как ОЗУ (702) и ПЗУ (703), интерфейсы ввода/вывода (704), устройства ввода/вывода (705) и устройство для сетевого взаимодействия (706).

Процессор (701) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п.

ОЗУ (702) представляет собой оперативную память и предназначено для хранения исполняемых процессором (701) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (702), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (703) 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 устройства (700) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (704). 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 вычислительным устройством (700) применяются различные средства (705) В/В 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 (706) обеспечивает передачу данных устройством (700) посредством внутренней или внешней вычислительной сети, например Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (706) 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, например, GPS, ГЛОНАСС, BeiDou, Galileo.

Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система для обеспечения доступа к цифровой копии документа пользователя, содержащая по меньшей мере один процессор, связанный посредством шины с модулем регистрации и аутентификации, который выполнен с возможностью регистрации новых пользователей системы и последующей их аутентификации;

модулем биометрической аутентификации и идентификации, который выполнен с возможностью получения биометрических данных пользователя и их последующего анализа в целях аутентификации для совершения операций с документами;

модулем добавления документов, который предназначен для добавления в систему цифровых копий изображений документов пользователя;

модулем хранения документов, который предназначен для хранения и управления добавленными цифровыми копиями документов пользователей;

модулем предъявления документов, который предназначен для предоставления добавленных упомянутых цифровых копий изображений документов получателю и настройки политик доступа предоставления упомянутых цифровых копий документов получателю, которая устанавливает перечень доступных цифровых копий документов для передачи модулю запроса документа, причем предоставление цифровых копий документов осуществляется путем формирования пакета данных, содержащего, по меньшей мере, гиперссылку на по меньшей мере одну цифровую копию документа пользователя, содержащуюся в модуле хранения документов;

модулем электронной подписи документов, который предназначен для подписи добавляемых цифровых копий изображений документов личной усиленной квалифицированной электронной подписью (УКЭП) и проверки валидности электронной подписи для каждой цифровой копии документа по запросу модуля запроса документов;

модулем запроса документов, который предназначен для получения по меньшей мере одной подписанной цифровой копии изображения документа пользователя, сохраненных в модуле хранения документов, от модуля предъявления документов.

2. Система по п.1, характеризующаяся тем, что регистрация пользователей осуществляется с помощью по меньшей мере одного идентификатора, выбираемого из группы: СНИЛС, номер телефона, адрес электронной почты, номер/серия паспорта, ИНН, номер медицинского полиса, уникальный идентификатор (УИД).

3. Система по п.2, характеризующаяся тем, что после первичной регистрации пользователя выполняется его первичная аутентификация с помощью направления сообщения для последующего подтверждения на устройство пользователя с помощью сотовой и/или Интернет связи.

4. Система по п.3, характеризующаяся тем, что сообщение содержит код подтверждения или гиперссылку на ресурс аутентификации.

5. Система по п.1, характеризующаяся тем, что модуль аутентификации дополнительно назначает для каждого зарегистрированного пользователя предпочтительный способ аутентификации.

6. Система по п.1, характеризующаяся тем, что модуль хранения документов представляет собой облачное хранилище.

7. Система по п.1, характеризующаяся тем, что модуль биометрической аутентификации выполнен с возможностью получения по меньшей мере одного биометрического образца пользователя, выбираемого из группы: отпечаток пальца, изображение лица, аудиозапись голоса, изображение сетчатки глаза,

изображение радужной оболочки, рисунок вен ладони, геометрия кисти руки.

8. Система по п.1, характеризующаяся тем, что модуль добавления документов формирует цифровые копии документов на основании загружаемых пользователями в систему документов и/или с помощью запроса копий документов у соответствующих органов - издателей документов.

9. Система по п.1, характеризующаяся тем, что копия документа может содержать групповую ЭП.

10. Система по п.10, характеризующаяся тем, что подписание копий документов УКЭП осуществляется с помощью облачной платформы.

11. Способ предоставления доступа к цифровой копии документов пользователя, содержащий этапы, на которых

создают в облачной системе доверенного документооборота (ОСДД) профиль пользователя, который содержит, по меньшей мере, УИД пользователя и его биометрический образец, содержащий, по меньшей мере, изображение лица пользователя;

добавляют в упомянутую систему по меньшей мере одну цифровую копию изображения документа пользователя;

осуществляют подписание упомянутой цифровой копии изображения документа в ОСДД с помощью УКЭП пользователя;

устанавливают политики доступа для каждой цифровой копии добавленного документа в ОСДД, причем политика доступа устанавливает перечень доступных цифровых копий документов для передачи устройству получателя;

связывают добавленные цифровые копии документов с соответствующим профилем пользователя;

с помощью устройства пользователя формируют информационный пакет, содержащий электронную ссылку на по меньшей мере одну цифровую копию изображения документа и УИД пользователя, связанные с его профилем в ОСДД;

передают упомянутый информационный пакет на устройство получателя;

на устройстве получателя осуществляют извлечение цифровой копии изображения документа из полученной электронной ссылки и проверяют УКЭП пользователя;

получают с помощью устройства получателя биометрический образец пользователя, содержащий изображение лица пользователя;

передают с помощью устройства получателя полученный биометрический образец пользователя и полученный УИД пользователя в ОСДД и выполняют их сравнение с данными, связанными с профилем пользователя;

в случае успешного сравнения данных с профилем пользователя устройство получателя осуществляет обработку согласно установленной политике доступа полученной по меньшей мере одной копии цифрового изображения документа по упомянутой электронной ссылке.

12. Способ по п.13, характеризующийся тем, что копия документа содержит дополнительную ЭП.

13. Способ по п.14, характеризующийся тем, что ОСДД предоставляет доступ к копии документа в случае проверки дополнительной ЭП.

14. Способ по п.13, характеризующийся тем, что информационный пакет представляет собой QR-код.

15. Способ по п.13, характеризующийся тем, что биометрический образец пользователя дополнительно включает по меньшей мере одно из: отпечаток пальца, изображение сетчатки глаза, изображение радужной оболочки, изображение вен ладони, изображение геометрии кисти или образец голоса.

16. Способ предоставления доступа к цифровой копии документов пользователя, содержащий этапы, на которых

создают в облачной системе доверенного документооборота (ОСДД) профиль пользователя, который содержит, по меньшей мере, УИД пользователя, первый биометрический образец, который является изображением лица пользователя, и второй дополнительный биометрический образец;

добавляют в упомянутую систему по меньшей мере одну цифровую копию изображения документа пользователя;

осуществляют подписание упомянутой цифровой копии изображения документа в ОСДД с помощью УКЭП пользователя;

устанавливают политики доступа для каждой упомянутой цифровой копии изображения добавленного документа в ОСДД, причем политика доступа устанавливает перечень доступных цифровых копий документов для передачи устройству получателя;

связывают добавленные цифровые копии изображений документов с соответствующим профилем пользователя;

формируют с помощью устройства получателя первый запрос на предоставление цифровой копии изображения документа пользователя, причем запрос содержит получение изображения лица пользователя и дополнительного биометрического образца, соответствующего второму биометрическому образцу, сохраненному в профиле пользователя в ОСДД;

направляют упомянутый запрос в ОСДД;

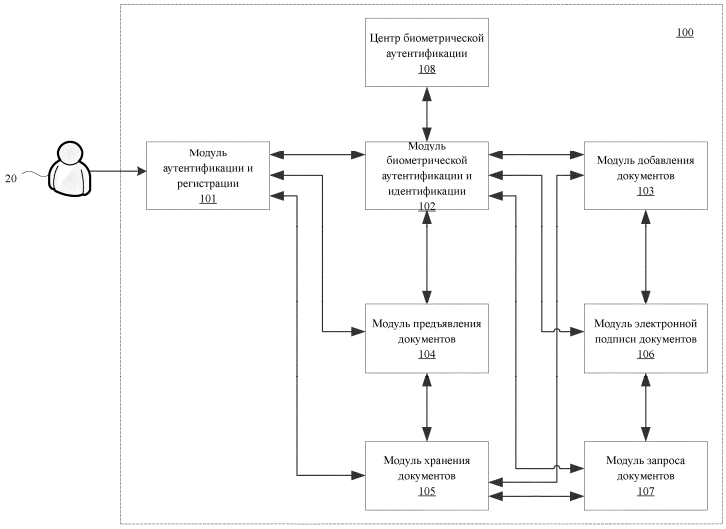
с помощью ОСДД проверяют полученный запрос с профилем пользователя и передают на устрой-

ство получателя УИД пользователя;

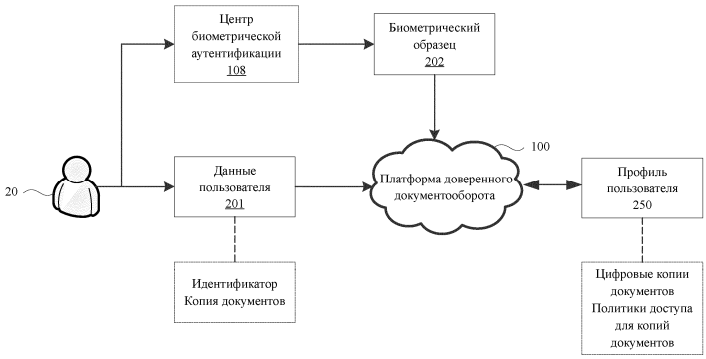
формируют с помощью устройства получателя второй запрос, содержащий УИД пользователя, для получения цифровой копии изображения документа пользователя;

проверяют с помощью устройства получателя УКЭП пользователя и в случае успешной проверки получают доступ к по меньшей мере одной цифровой копии изображения документа пользователя в соответствии с заданной политикой доступа.

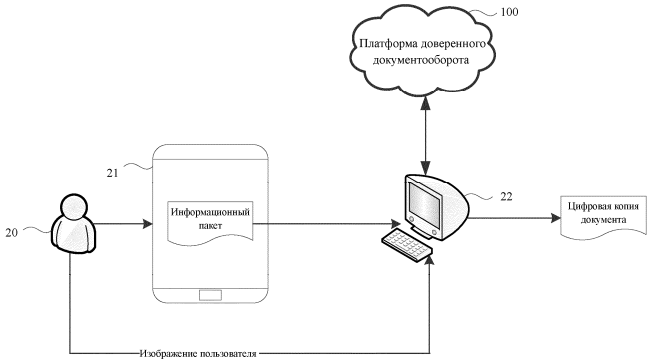
17. Способ по п.16, характеризующийся тем, что дополнительный биометрический образец пользователя включает по меньшей мере одно из: отпечаток пальца, изображение сетчатки глаза, изображение радужной оболочки, изображение вен ладони, изображение геометрии кисти или образец голоса.



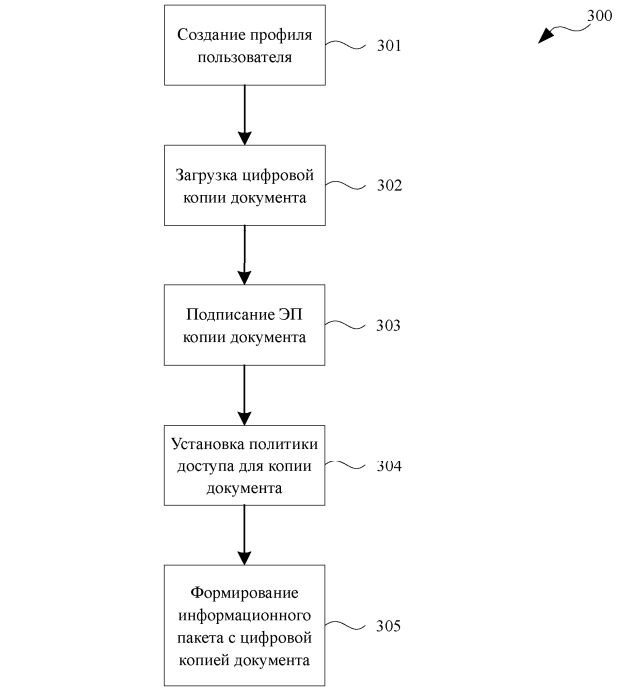
Фиг. 1



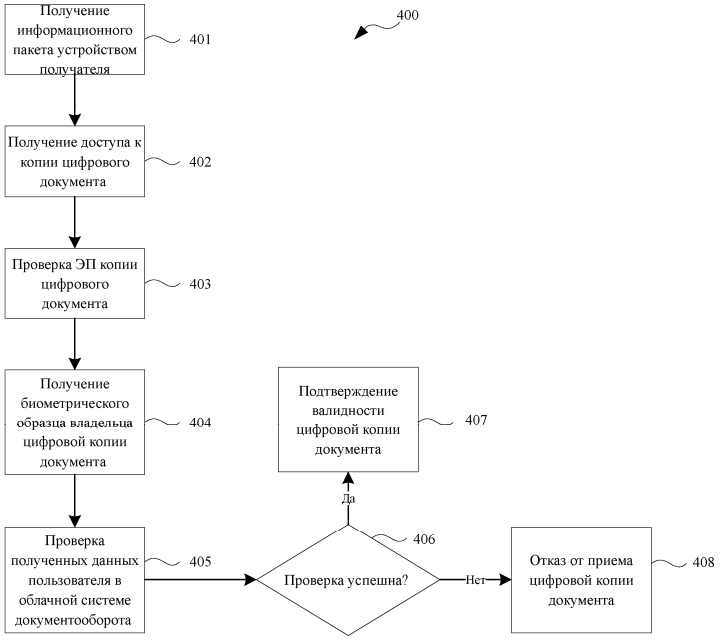
Фиг. 2



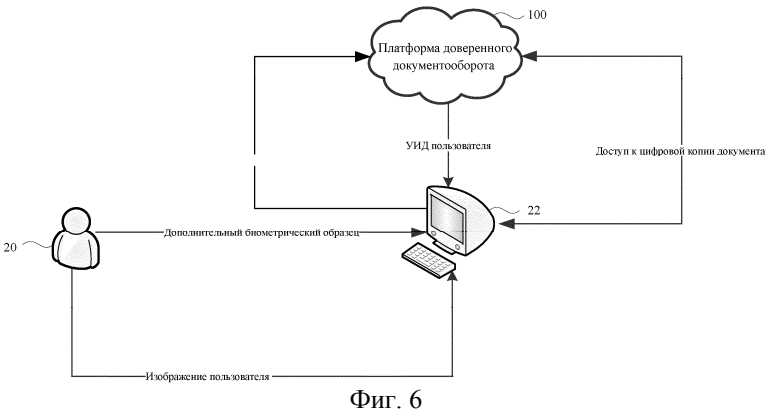
Фиг. 3



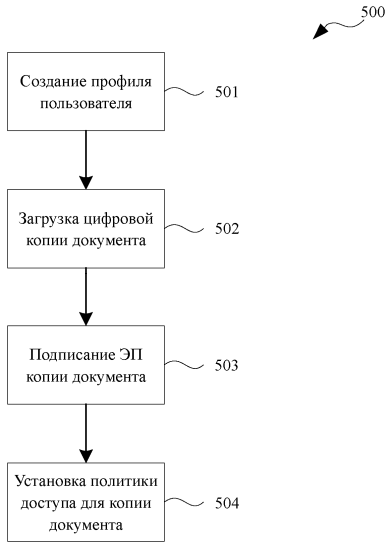
Фиг. 4



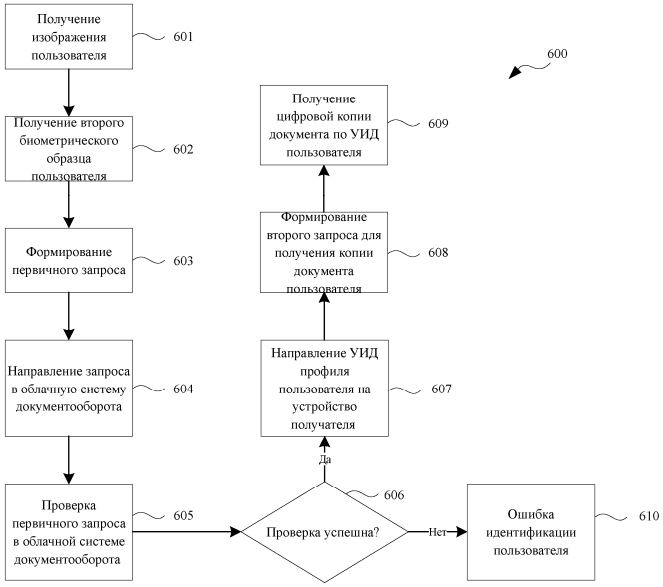
Фиг. 5



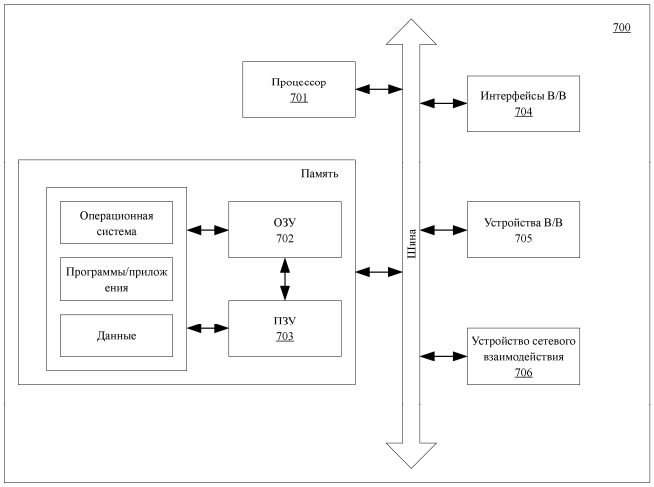
Фиг. 6



Фиг. 7



Фиг. 8



Фиг. 9