(19) Евразийское патентное ведомство

(11) 044528 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.08.31

(21) Номер заявки
201992482

(22) Дата подачи заявки
2019.11.18

(51) Int. Cl. ***G06F 17/00*** (2019.01)
G06K 9/00 (2006.01)
H04L 9/00 (2006.01)

(54) УНИВЕРСАЛЬНАЯ СИСТЕМА РАСПРЕДЕЛЕННОГО ЗАЩИЩЕННОГО ДИСТАНЦИОННОГО ГОЛОСОВАНИЯ

(31) **2019135322**
(32) **2019.11.05**
(33) **RU**
(43) **2021.05.31**

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

(72) Изобретатель:
Тамойкин Андрей Юрьевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) Электронное голосование. Итоги сезона годовых собраний 2017 г [онлайн]. ГлобалМск.ру 13 февраля 2018 [найдено 29.09.2020]. Найдено в <https://globalmsk.ru/news/id/16178>

Где голосуют и принимают решения? Современное корпоративное управление. Презентация [онлайн]. Национальный Расчетный Депозитарий 17 октября 2019 [найдено 29.09.2020]. Найдено в <https:/www.nsd.ru/upload/docs/conf/2019-10-17/vtb.pdf>

Как проводить онлайн-голосования в приложении "Моя Квартира" [онлайн]. РосКвартал 05 октября 2018 [найдено 29.09.2020]. Найдено в <https://roskvartal.ru/provedenie-oss/9564-kak-provodit-onlavn-golosovaniva-v-prilozhenii-mova-kvartira?utm_source=press_release&utm_medium=moya-kvartira&utm_campaign=news>

Как выбрать информационную систему для голосования на ОСС [онлайн]. РосКвартал 1 августа 2018 [найдено 29.09.2020]. Найдено в <https://roskvartal.ru/provedenie-oss/9285-kak-vybrat-informacionnuyu-sistemu-dlya-golosovaniva-na-oss?utm_source=press_release&utm_medium=mova-kvartira&utm_campaign=news>

ТБ Регистратор принял участие в ФИНОПОЛИС-2019 и выпустил первое небанковское мобильное приложение на iOS с применением ЕБС [онлайн]. ВТБ Регистратор 14 октября 2019 [найдено 29.09.2020]. Найдено в <https://www.vtbreg.com/company/news_of_legislation/events/1726250/>

RU-C1-2444063

US-A1-20040024635

(57) Изобретение относится к области вычислительной обработки данных, а в частности к системам удаленного голосования. Автоматизированная система дистанционного голосования, содержащая модуль регистрации и первичной аутентификации, осуществляющий регистрацию и первичную аутентификацию пользователя в системе для получения доступа к модулю биометрической аутентификации; модуль биометрической аутентификации, осуществляющий биометрическую аутентификацию пользователя, доступ к голосованию, формирование профиля и прав пользователя в системе с помощью алгоритмов биометрической проверки; модуль электронной подписи, осуществляющий возможность использования электронной подписи пользователем в системе и обеспечивающий идентификацию пользователя при сетевом подключении к системе; модуль управления активностью, осуществляющий возможность инициации и администрирования активности пользователем в системе; модуль проведения активности, осуществляющий возможность обработки и реализации, инициированной пользователем, активности; модуль интеграции с внешними системами, осуществляющий взаимодействие с внешними системами; модуль обработки внутренних запросов, осуществляющий интерпретацию внутренних запросов от модулей системы в запросы к модулю интеграции с внешними системами; модуль аудита, выполняющий мониторинг действий пользователя системы и ведения на основании фиксируемой информации системного журнала.

044528 B1

044528 B1

Область техники

Настоящее техническое решение, в общем, относится к области вычислительной обработки данных, а в частности, к системам распределенного защищенного дистанционного голосования.

Уровень техники

В настоящее время активности, связанные с голосованием (выборы, собрания собственников, референдумы и т.д.) накладывают дополнительные сложности на людей, принимающих в них участие: личное присутствие, выполнение дополнительных инструкций (например, отправка почтового сообщения определенного формата на определенный адрес, откреплениe/прикрепление к избирательному участку) и т.д., а также дополнительную ручную работу по организации, проведению и обработки полученных данных, что обусловлено законодательными нормативами, требованиями безопасности и другими нормами. Все это зачастую требует от Гражданина РФ дополнительных знаний, чтобы воспользоваться своим правом (например, организация общего собрания собственников многоквартирного дома), дополнительной активности (прийти на избирательный участок) и открывает возможности для мошенничества (заполнение бюллетеней за людей, не участвовавших в активности). Современные технологии позволяют реализовать систему, способную смягчить требования к участнику активности. Такие системы широко известны из уровня техники, например, из следующих патентных документов: US 7237717 Bl (IP HOLDINGS INC, 03.07.2007), US 8892456 B2 (BROADRIDGE INVESTOR COMMUNICATION SOLUTIONS INC, 18.11.2014). Общим недостатком существующих решений в данной области является недостаточная защищенность данных при реализации удаленного голосования.

Сущность технического решения

Заявленное техническое решение предлагает новый подход в области распределенного защищенного дистанционного голосования с помощью мобильных устройств.

Решаемой технической проблемой или технической задачей является создание новой платформы дистанционного голосования, обладающей высокой степенью надежности и точностью подсчета голосов.

Основным техническим результатом, достигающимся при решении вышеуказанной технической проблемы, является обеспечение возможности защищенного дистанционного голосования с помощью мобильных устройств.

Заявленный результат достигаются за счет автоматизированной системы дистанционного голосования, содержащей

модуль регистрации и первичной аутентификации, осуществляющий регистрацию и первичную аутентификацию пользователя в системе для получения доступа к модулю биометрической аутентификации;

модуль биометрической аутентификации, осуществляющий биометрическую аутентификацию пользователя, доступ к голосованию, формирование профиля и прав пользователя в системе с помощью алгоритмов биометрической проверки;

модуль электронной подписи, осуществляющий возможность использования электронной подписи пользователем в системе и обеспечивающий идентификацию пользователя при сетевом подключении к системе;

модуль управления активностью, осуществляющий возможность инициации и администрирования активности пользователем в системе;

модуль проведения активности, осуществляющий возможность обработки и реализации, инициированной пользователем, активности;

модуль интеграции с внешними системами, осуществляющий взаимодействие с внешними системами;

модуль обработки внутренних запросов, осуществляющий интерпретацию внутренних запросов от модулей системы в запросы к модулю интеграции с внешними системами;

модуль аудита, выполняющий мониторинг действий пользователя системы и ведения на основании фиксируемой информации системного журнала.

В одном из частных вариантов осуществления модули располагаются в едином вычислительном устройстве и объединены единой шиной.

В другом частном варианте осуществления по меньшей мере два модуля располагаются на различных вычислительных устройствах и объединены между собой каналами передачи данных.

В другом частном варианте осуществления вычислительное устройство представляет собой персональный компьютер, сервер или мейнфрейм.

Описание чертежей

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

фиг. 1 иллюстрирует общую схему заявленной автоматизированной системы дистанционного голосования;

фиг. 2 иллюстрирует общий вид вычислительного устройства для реализации системы.

Осуществление изобретения

В данном техническом решении могут использоваться для ясности понимания работы такие термины как "инициатор", "администратор", которые в общем виде следует понимать, как "пользователь" системы.

Автоматизированная система дистанционного голосования - система, позволяющая организовывать и проводить голосования (в том числе выборы, решения по определенным вопросам, соцопросы, референдумы, и т.д. далее активности). Система реализует необходимые условия проведения указанных активностей, такие как идентификация, анонимность, обработка результатов, формирование решений, аудит процесса, хранение данных и т.д. - в зависимости от необходимости для каждого конкретного типа активности. При этом система реализует данный функционал с использованием мобильных устройств пользователей системы и серверной части системы, что позволяет пользователям системы участвовать в голосовании или референдуме без личного присутствия на избирательном участке.

В системе реализованы следующие профили пользователей платформы:

Инициатор - лицо или группа лиц, инициирующее активность, в рамках которой требуется проведение голосования или референдума. Инициатор предоставляет в систему вопрос/вопросы, по которым требуется активность, необходимые свойства активности, формат активности, исходные данные (списки пользователей с правом доступа к активности, списки кандидатов, в случае выборов, перечень вопросов и т.д.) и дополнительные материалы для привязки к активности (пояснительная записка по законопроекту, информационные материалы для повестки собрания собственников, биографии кандидатов и т.д.).

Администратор - лицо или группа лиц, отвечающая за техническую организацию созданной активности. Администратор осуществляет действия, необходимые для реализации заявленных свойств активности, поддержку пользователей в момент проведения активности, обеспечивает общую безопасность и работоспособность системы, отвечает за производительность системы в момент активности.

Пользователь - гражданин, который имеет право участвовать в созданной активности. Для регистрации в системе пользователю необходимо однократно удаленно предоставить следующие данные: номер мобильного устройства, ФИО, дата рождения. После чего пройти биометрическую идентификацию для создания личного кабинета и обогащения профиля пользователя из доверенного источника. Биометрическая идентификация требует наличия заранее созданного биометрического профиля. Для этих целей система подключается к внешней биометрической системе и по полученному от пользователя биометрическому образцу запрашивает в биометрической системе данные из профиля пользователя, которые используются для создания личного кабинета пользователя.

После идентификации пользователя система отправляет OTP (one-time password) токен на номер мобильного устройства пользователя, указанный в биометрическом профиле для подтверждения регистрации вторым фактором. В случае успешного ввода пользователем второго фактора система создает личный кабинет и профиль пользователя, а также предлагает пользователю установить способ аутентификации для последующего использования: пин-код; биометрической аутентификации, поддерживаемой устройством. В процессе формирования профиля пользователя система сохраняет у себя ряд параметров, полученных из биометрического профиля, а также параметры, которые пользователь может дополнительно ввести самостоятельно в личном кабинете после регистрации. Данные параметры по выбору пользователя могут быть отображены в личном кабинете, или скрыты от пользователя и храниться исключительно во внутренних базах данных системы. По данным, введённым пользователем, система, при наличии возможности, проводит проверку их достоверности, для этого осуществляются запросы к внешним электронным реестрам, содержащим эти данные.

После формирования профиля пользователя система автоматически производит сверку этого профиля с профилем активности, который формируется при создании новой активности в системе. Если пользователь может принять участие в активности, то система автоматически предоставляет пользователю доступ для участия в активности. Для участия в ряде активностей (в которых требуется авторизация) пользователь должен использовать электронную цифровую подпись (ЭЦП), в том числе интегрированную с системой сервиса облачной ЭЦП. Помимо функционала участия в голосовании пользователю может быть назначена роль инициатора активности (включая грануляцию до конкретных видов активности и свойств, которые может назначить инициатор). Также роль инициатора может быть присвоена не конкретному пользователю, а отдельной учетной записи, которая соответствует, например, определенному ведомству.

В зависимости от своих прав в системе инициатор может создать активность: голосование или референдум - а также выбрать для созданной активности свойства. Перед созданием активности инициатор должен пройти биометрическую авторизацию в системе, для этого он предоставляет свой биометрический образец (лицо, отпечаток пальца или иное). Система осуществляет запрос во внешнюю биометрическую систему и отправляет инициатору OTP в виде пароля в SMS-сообщении. После того, как инициатор вводит SMS-сообщение, он считается авторизованным и получает доступ к функционалу создания активности согласно своим правам в системе.

Для создания активности инициатор должен указать следующие атрибуты: тип активности, название активности, временной диапазон доступности для голосования по создаваемой активности, перечень

вопросов, поставленных на голосование, дополнительные материалы для ознакомления, а также условия доступа пользователей к данной активности и свойства необходимые для проведения данной активности. После этого система проверяет достаточность входных данных и по возможности запрашивает дополнительные данные из третьих систем, с которыми существует интеграция. Пример: заочное голосование собственников многоквартирного дома. Инициатор указывает адрес дома, а система автоматически формирует реестр собственников жилых помещений этого дома из интегрированной государственной системы. В случае невозможности автоматического обогащения активности система запрашивает дополнительные данные у инициатора.

После формирования процесса проведения активности, система определяет круг пользователей, которые могут принять участие в активности путем сравнения профиля активности и профиля пользователя, а также получает (при возможности) дополнительную информацию из сторонних систем, при этом система должна быть в состоянии однозначно сопоставить профиль пользователя и дополнительные данные по этому пользователю из внешней системы (например, по уникальному идентификатору пользователя). После определения круга пользователей, которые могут принять участие в активности система с помощью push-уведомления (или SMS-сообщение, или email или иным способом) оповещает пользователя о доступности новой активности. Пользователь, который хочет принять участие в активности должен аутентифицироваться в приложении на своем устройстве, выбрать нужную активность и нажать "Принять участие". В этот момент приложение формирует запрос к системе о начале процесса активности. Система обрабатывает запрос и отправляет приложению директивы и данные согласно процессу активности.

Пользователь принимает участие в активности согласно процессу и отдает свой голос по тому или иному вопросу. Система обрабатывает голос пользователя согласно процессу активности и формирует конечный результат, который также, согласно процессу, может быть передан сторонней системе и/или возвращен инициатору активности. На фиг. 1 представлена общая схема заявленной системы (100). Система (100) принимает потоки информации, которые генерируются пользователями. Информация, поступающая в систему (100), распределяется по соответствующим модулям, ответственным за ее обработку в автоматизированном режиме. Система (100) содержит набор из взаимосвязанных модулей обработки данных.

Модуль регистрации и первичной аутентификации (101) предназначен для регистрации нового пользователя системы и последующей первичной аутентификации пользователя. Обычная аутентификация необходима для получения возможности использования функций модуля биометрической аутентификации (102) и модуля проведения активности (105). При обращении пользователя к системе (100), модуль регистрации и первичной аутентификации (101) запрашивает у пользователя номер мобильного устройства, ФИО и дату рождения. Получив указанные данные, модуль (101) отправляет на указанный номер мобильного устройства сообщение с кодом подтверждения, который должен быть введен пользователем. Получив корректный код подтверждения, модуль (101) регистрирует нового пользователя. Далее модуль (101) предоставляет пользователю возможность выбирать варианты последующей аутентификации, например, аутентификация по отпечатку пальца на мобильном устройстве, аутентификация по pin-коду на мобильном устройстве, аутентификация по связке логин/пароль и т.д. При входе в систему (100) зарегистрированного пользователя, модуль (101) предлагает использовать один из методов аутентификации, например, по отпечатку пальца, по pin-коду, по связке логин + пароль или любой другой метод аутентификации, поддерживаемый мобильным устройством пользователя. После успешной аутентификации модуль (101) передает право доступа пользователю к модулю биометрической аутентификации (102) и модулю проведения активности (105).

Модуль биометрической аутентификации (102) предназначен для биометрической аутентификации пользователя, обеспечения доступа к голосованию, формирования профиля и прав пользователя в системе. Модуль (102) взаимодействует со смежной системой биометрической аутентификации и идентификации для реализации алгоритмов биометрической проверки, с внутренней базой данных системы (100), а также с другими модулями, которым необходимо повысить уровень доверия к пользователю для предоставления доступа к дополнительным функциям или реализации различных свойств активности. Для успешной аутентификации пользователь должен однократно зарегистрироваться в "центре биометрической аутентификации". Центром биометрической аутентификации может быть отдельный специальный орган или любая другая система, в которых есть возможность пользователям очно предоставлять биометрические образцы и производится удостоверение личности заявителей. При обращении пользователя в центр биометрической аутентификации, создается соответствие между биометрическими образцами пользователя и его идентифицирующей информацией (номер паспорта или уникальный идентификатор пользователя, номер мобильного устройства, ФИО, дата рождения и т.д.). Далее модуль (102) запрашивает у пользователя биометрический образец (фото лица) и сравнивает полученную информацию с образцом хранящими в центре биометрической аутентификации.

Формирование профиля пользователя осуществляется последовательно. После регистрации модуль (102) запрашивает у пользователя биометрический образец - лицо; при этом модуль (102) не принимает фотографии, а самостоятельно выбирает кадр из видеоряда с камеры мобильного устройства. Далее сис-

тема (100) получает от модуля (102) контекстную информацию о пользователе, который в данный момент аутентифицирован в приложении (ФИО, дату рождения и номер мобильного устройства). Полученная информация сравнивается с образцами, хранящимися в центре биометрической аутентификации, для проверки подлинности. В случае корректного совпадения биометрических образцов, ФИО, даты рождения и номера мобильного устройства система (100) отправляет на номер мобильного устройства SMS-сообщение с кодом подтверждения, который должен быть введен пользователем в системе (100). После введения пользователем кода подтверждения система (100) формирует профиль пользователя во внутренней базе данных.

Формирование прав пользователя в системе (100) осуществляется последовательно. Для каждой активности в системе (100) заранее формируется перечень условий, которым должен соответствовать пользователь для получения прав как на саму активность, так и на то или иное действие в рамках активности. При формировании или изменении профиля пользователя он оценивается на соответствие условиям, необходимым для получения этих прав. Система (100) выдает права пользователю в момент их запроса, каждый раз анализируя запрос и его контекст, в соответствии с уровнем доверия данному пользователю.

Пример: пользователь имеет право инициировать собрание собственников, но никогда этого не делал - значит система (100) позволит это сделать только после дополнительной идентификации пользователя.

Для этих целей в систему (100) передаются статические данные о пользователе (например, геолокация мобильного устройства, метка времени и т.д.), а также динамические данные, которые система (100) рассчитывает самостоятельно (статистика по частоте запросов пользователя, уникальность запросов, поведение пользователя в системе (100) и т.д.), на основании которых формируется уровень доверия к конкретному запросу. В случае подозрения или низкого уровня доверия система (100) может выбирать способ аутентификации пользователя и предложит ему дополнительные проверки для повышения уровня доверия. А также система (100) может облегчать доступ пользователя, в случае высокого уровня доверия.

Определение правомерности участия пользователя в той или иной активности осуществляется последовательно. В рамках создания каждой активности формируется перечень критериев, по которым определяется круг лиц, допущенных к участию в активности. Далее каждый профиль пользователя сверяется с заданными критериями. В случае если активность доступна пользователю, система (100) формирует уведомление о возможности участия и отправляет его пользователю в виде push-уведомления, SMS-сообщения, email, и т.д.

Модуль электронной подписи (103) предназначен для использования электронной подписи пользователем в системе (100) и обеспечивающий идентификацию пользователя при сетевом подключении к системе (100). Модуль (103) взаимодействует с внешней системой облачной ЭЦП. Интеграция осуществляется после биометрической регистрации пользователя. Существует два вида возможной интеграции. Первый -интеграция с существующим аккаунтом облачной ЭЦП. Второй - создание нового аккаунта в сервисе облачной ЭЦП. В рамках интеграции модуль (103) передает системе облачной ЭЦП объекты, созданные в рамках активности для подписи личной ЭЦП пользователя. Также модуль (103) предоставляет пользователю сертификат для установления взаимной идентификации в рамках защищенной сессии (mutual TLS протокол).

Модуль управления активностью (104) предназначен для инициации и администрирования активности пользователем в системе (100). Доступ пользователя к модулю (104) определяется профилем пользователя с помощью модуля (102). Данный модуль (104) также содержит заранее подготовленные описания некоторых типов активностей, включая перечень условий для инициализации активности динамические переменные для организации активности и способы их получения (перечень вопросов/кандидатов, перечень пользователей, допущенных к активности и т.д.), а также набор свойств, которыми обладает активность. В модуле (104) формируется перечень условий, которым должен соответствовать профиль пользователя, чтобы получить права на создание того или иного типа активности. Далее в модуле (104) формируется базовый профиль активности, куда добавляется перечень переменных, значения для которых необходимо предоставить для инициализации активности. Для некоторых переменных может быть указана директива по получению значений из внешнего источника (если такой источник интегрирован), при этом данные директивы выполняются только после инициализации активности инициатором.

Инициация активности осуществляется последовательно. Профиль пользователя после создания или изменения сравнивается с перечнем условий по каждой активности и в случае совпадения, пользователю становится доступна функция инициализации новой активности. Пользователь, который хочет инициализировать новую активность, должен пройти авторизацию, при этом условия "сложности" авторизации прописаны в перечне условий для каждой активности. После прохождения авторизации инициатор должен указать значения переменных активности (включая, но не ограничиваясь: название активности, временной диапазон доступности для голосования по создаваемой активности, перечень вопросов, поставленных на голосование, дополнительные материалы для ознакомления и т.д.). В случае, если система (100) не может заполнить значения переменных автоматически, инициатор должен указать в активности перечень лиц, допущенных к участию, и перечень вопросов на обсуждение (или перечень кандидатов и т.д.). Перечень лиц, допущенных к участию, может представлять собой таблицу с конкретными

пользователями системы (100) или условия, по которым система (100) определит участников самостоятельно. После этого система (100) формирует окончательный профиль активности в соответствии с полученной информацией от инициатора, а также базовым профилем для инициируемой активности, добавляя свойства активности.

Помимо базовых профилей активности в системе (100) предусмотрено создание активности с нуля практически любым пользователем (минимальные условия для получения прав), в этом случае пользователь самостоятельно выбирает свойства активности и переменные, которые будут использоваться в активности. Лица, допущенные к такой активности, выбираются путем определения условий выбора профилей пользователя. Данный тип активности предназначен в основном для проведения опросов или социальных исследований. Каждый пользователь системы (100) в своем профиле может выбрать тип активности, которая будет ему предлагаться системой (100).

Окончательный профиль активности передается на исполнение в модуль проведения активности (105).

Модуль проведения активности (105) предназначен для обработки и реализации, инициированной пользователем, активности. Модуль (105) получает от модуля (104) профиль активности. Далее модуль (105) производит последовательно несколько этапов обработки профиля активности.

На первом этапе производится первичная обработка и создание технической базы активности. Из профиля активности создается новый объект активности, который содержит все информационные данные: название, повестка/вопросы/кандидаты, даты проведения активности, условия проведения активности, дополнительные материалы, перечень допущенных пользователей, если такой есть и т.д. Далее создается политика доступа к объекту активности, которая определяет порядок и правила доступа к данной активности и содержит следующие параметры: дата и время доступности активности, свойства доступа к активности, критерии авторизации для доступа к активности - данные условия формируются из переменных в профиле активности, свойств, которые указаны в профиле активности, а также из любой другой информации, указанной в профиле активности. Политика доступа привязывается к объекту активности по уникальному идентификатору и является его неотъемлемой частью. Далее осуществляется техническая реализация свойств активности ("наличие права у пользователя на принятие участия в голосовании" или у активности указано свойство "возможность голосования без авторизации" и т.д.).

После создания объекта активности и политики доступа к объекту активности модуль (105) формирует "жизненный цикл активности", который определяет очередность фаз активности (подготовка, сбор голосов, обработка голосов, подсчет голосов, оформление результатов, хранение результатов) и дату начала и продолжительность этих фаз по данным, указанным в профиле активности и предустановленным параметрам. Каждая фаза соответствует части автоматизированного процесса и содержит информацию по дополнительным директивам, которые должны быть выполнены для реализации тех или иных свойств активности (помимо свойств, которые отображаются в политике доступа к активности). Свойства активности могут соответствовать только одной из фаз жизненного цикла или распределяться по нескольким фазам, в зависимости от конкретного свойства. Фаза активности привязана к объекту активности и изменяется в соответствии с жизненным циклом фазы активности. После создания всех сущностей система (100) начинает работу с активностью согласно ее жизненному циклу, в порядке фаз.

На втором этапе производится обработка запросов пользователя, осуществленных в рамках активности. После создания профиля активности производится сверка профиля пользователя и условия допуска пользователя к активности. Если профиль пользователя проходит условия допуска к активности, то система (100) уведомляет пользователя об обнаружении новой активности. Пользователь, для которого были обнаружены активности, может принять в них участие - для этого он с помощью приложения со своего мобильного устройства отправляет в систему (100) запрос о получении дополнительной информации по активности. Система (100), получая запрос об активности от пользователя, проверяет текущую фазу активности и, если фаза позволяет добавить еще одного пользователя (подготовка, сбор голосов), то система (100) проверяет политику доступа, привязанную к объекту активности для предоставления доступа пользователю. Далее поочередно осуществляется проверка наличия свойств активности в политике доступа и производится по ним проверка пользователя. В случае успешной проверки система (100) отправляет на устройство пользователя данные об активности (название, даты и формат проведения, дополнительные материалы и т.д.). Помимо этого на этапе подготовки модуль (105) реализует следующее свойство (если оно активно "Конфиденциальность голоса в технических средствах обработки данных"). В случае наличия данного свойства система (100) после перехода на этап подготовки (сразу после создания сущностей активности: объект активности, политика доступа и жизненный цикл) осуществляет выпуск ключей ассиметричного шифрования. Также на этапе подготовки пользователь может просматривать дополнительную информацию по активности, а также редактировать документы по активности, если активность предполагает такую возможность (например, предлагать правки к документу). Этап подготовки длится от момента инициации активности до момента начала голосования по активности, указанном в профиле активности. Дальнейшие запросы пользователя к объекту активности проверяются в соответствии с политикой доступа к активности и маршрутизируются в соответствии с директивами, указанными для текущей фазы активности в соответствии с жизненным циклом активности.

На этапе сбора голосов пользователь формирует запрос к объекту активности об осуществлении голосования. Если активно свойство "Конфиденциальность голоса в технических средствах обработки данных" система (100) в ответ на запрос пользователя предоставляет публичный ключ. Далее пользователь осуществляет выбор по вопросам активности. Процесс добавления решения пользователя во внутреннюю базу данных системы (100) сопровождается регистрацией, в рамках которой каждому голосу добавляется отметка времени, в которую регистрация осуществилась. Все метки времени, в которые были зарегистрированы решения пользователей, дополнительно сохраняются отдельно от решений пользователей. После этого во внутренней базе данных решение пользователя записывается в формате: "Уникальный идентификатор", "Временная метка", "Пользователь", "Хэш-сумма, подписанная сертификатом открытого ключа пользователя", "Решение пользователя (в полученном виде: зашифрованное или открытое)". Из указанных значений обязательными являются только уникальный идентификатор, метка времени и решение. В конце этапа сбора голосов полученные решения пользователей подписываются с помощью ЭЦП системы (100) и передаются далее на обработку. Этап сбора голосов продолжается согласно данным, указанным в объекте активности.

На этапе обработки голосов система (100) автоматически подготавливает голоса для подсчета. Первичная обработка полученных голосов начинается с проверки целостности данных во внутренней базе данных системы (100). Для этого формируется хэш-сумма всех собранных данных и сверяется с подписанной хэш-суммой этого же набора данных. Если различий нет, то данные принимаются в обработку, если различия есть, то система (100) оповещает об этом инициатора и администратора. Далее модуль (105) запрашивает перечень меток времени, сформированный ранее при регистрации голосов. И для каждого голоса сверяет добавленную метку времени с перечнем меток времени - учитываются только те голоса, для которых найдены совпадения. Таким образом осуществляется проверка на возможное добавление голосов заинтересованными лицами. После прохождения проверок производится обработка директив свойств активности, добавленных в фазу обработки голосов. Если указано свойство "Защищенность от "принуждения" во время электронного голосования или нет", то анализируется набор данных, сформированный после первичных проверок по пользователям. Если выявлено несколько голосов, принятых от одного пользователя, то в рамках данного свойства модуль (105) удаляет из перечня голосов все голоса пользователя, кроме последнего. Если указано свойство "Возможность параллельного голосования или нет", то данное свойство подразумевает возможность активности по другим каналам (в том числе традиционное с личным присутствием на избирательном участке) параллельно с проведением активности в системе (100).

После выполнения директив указанных в фазе свойств модуль (105) подготавливает перечень данных для передачи на этап подсчета голосов. Если используется алгоритм случайных перестановок, то система (100) в качестве входных данных на следующий этап может передавать как перемешанные данные, так и первоначальный обезличенный перечень для проведения дополнительной проверки на двух наборах данных. На этапе подсчета голосов система (100) осуществляет директивы, описанные в свойствах, указанных в данной фазе или директивы по умолчанию. В завершение этапа подсчета голосов сформированные результаты подписываются ЭЦП системы (100) и сохраняются во внутренней базе данных.

Далее система (100) переходит на этап оформления результатов. Во время данного этапа результаты оформляются в заранее заданном виде (отчет, таблица, машинный вид и т.д.) и передаются инициатору активности. После чего модуль (105) формирует итоговый перечень данных для активности и подписывает его ЭЦП. К перечню дополнительно могут быть привязаны списки пользователей, принявших участие в этой активности, объект активности или данные из него. На этапе хранения результаты и дополнительные данные сохраняются в специализированную защищенную базу данных. После сохранения результатов модуль (105) закрывает любой доступ к проведенной активности.

Модуль интеграции с внешними системами (106) предназначен для взаимодействия с внешними системами. Модуль (106) передает во внешние системы результаты тех или иных этапов работы, взаимодействуя с модулем (105). Также предоставляет другим системам интерфейсы доступа, которые реализуют функционал обработки внешних запросов и предоставляют запрашиваемые данные по запросам от внешних систем. Модуль (106) также реализует функционал нормализации внешних данных, полученных из внешних систем для приведения этих данных в соответствие со схемами собственных баз данных системы (100). В качестве входных данных модуль (106) ожидает запрос от другого модуля системы (100) или запрос к программному интерфейсу от внешней системы. При получении запроса от другого модуля системы (100) модуль (106) формирует необходимую информацию для обработки внешней системой. После формирования необходимой информации модуль (106) устанавливает соединение с внешней системой согласно правилам внешней системы. Для этого модуль (106) использует алгоритмы, которые разработаны заранее для конкретной интеграции. Модуль обработки внутренних запросов (107) предназначен для интерпретации внутренних запросов от модулей системы (100) в запросы к модулю интеграции с внешними системами (106). В качестве входных данных модуль (107) ожидает запрос от другого модуля системы (100) (например, от модуля биометрической аутентификации и идентификации (102)). В запросе обязательно должен содержаться указатель на тип данных (например, "уникальный идентификатор пользователя"), который необходимо запросить во внешней системе. В случае отсутствия

данного идентификатора запрос отклоняется. Если идентификатор присутствует, модуль (107) анализирует таблицу связи между внутренним типом данных системы (100) и внешними системами, в которых можно получить данный тип данных. Таблица формируется и обновляется при каждом подключении внешнего источника данных. Если системы отсутствуют, то запрос отклоняется. Если внешние системы, в которых можно получить указанный тип данных, подключены к системе (100), то модуль (107) анализирует оставшуюся часть запроса на наличие мета-данных, которые необходимы внешней системе для предоставления данных необходимого типа. Если в запросе есть все мета-данные, то модуль (107) перенаправляет запрос в модуль интеграции с внешними системами (106). Если мета-данные отсутствуют, то модуль (107) формирует ответ с необходимостью предоставить дополнительные мета-данные к модулю, запросившему данные. Далее модуль (107) ожидает ответ от модуля интеграции с внешними системами (106). При получении ответа модуль (107) перенаправляет ответ в модуль, который осуществил запрос.

Модуль аудита (108) предназначен для реализации алгоритмов проверки действий пользователя системы (100) и ведения на основании фиксируемой информации системного журнала. При заполнении итогового бюллетеня активности на стороне клиента (мобильное устройство или персональный компьютер) формируется пакет данных вида: "Уникальный идентификатор", "Временная метка", "Пользователь", "Хэш-сумма, подписанная сертификатом открытого ключа пользователя", "Решение пользователя (в полученном виде: зашифрованное или открытое)" с учетом всех дополнительных свойств активности. Далее этот пакет разбивается модулем (108) на две составляющие: часть, описывающая пользователя (например, "Пользователь", "Хэш-сумма, подписанная сертификатом открытого ключа пользователя") и волеизъявление пользователя (например, "Уникальный идентификатор", "Временная метка" "Решение пользователя"). В итоге получается три самостоятельных пакета данных: полный набор отправляется по защищенному каналу связи с взаимной идентификацией на сторону серверной части системы (100) для дальнейшей обработки. Данные, описывающие пользователя отправляются в публичную не анонимную блокчейн-систему. Данные, описывающие волеизъявление пользователя, отправляются в публичную анонимную блокчейн-систему. После проведения активности модуль (108) публикует технические данные: в случае отсутствия шифрования бюллетеней - открытая обезличенная таблица с голосами пользователей (без привязки пользователей к этим голосам). В случае наличия шифрования обезличенная таблица, содержащая шифр тексты всех голосов. По завершению активности модуль (108) собирает информацию, полученную в блокчейн-системах и осуществляет сравнение этих данных.

На фиг. 2 представлен пример общего вида вычислительного устройства (300) для реализации системы (100).

В общем случае вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (1105) и устройство для сетевого взаимодействия (306). Процессор (301) (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 устройстве (300) также необходимо учитывать графический процессор, например, GPU NVIDIA или Graphcore, тип которых также является пригодным для полного или частичного выполнения исполнения системы (100), а также может применяться для обучения и применения моделей машинного обучения в различных информационных системах.

ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.). При этом в качестве ОЗУ (302) может выступать доступный объем памяти графической карты или графического процессора.

ПЗУ (303) 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 вычислительного устройства (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). 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 (300) применяются различные средства (305) 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 (306) обеспечивает передачу данных посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) 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. 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. Автоматизированная система дистанционного голосования с помощью мобильных устройств, содержащая взаимосвязанные между собой модули:

модуль регистрации и первичной аутентификации, выполненный с возможностью регистрации и первичной аутентификации пользователя в системе для получения доступа к модулю биометрической аутентификации;

модуль биометрической аутентификации, выполненный с возможностью биометрической аутентификации пользователя, доступа к голосованию, формированию профиля и прав пользователя в системе с помощью алгоритмов биометрической проверки;

модуль электронной подписи, выполненный с возможностью использования электронной подписи пользователем в системе и идентификации пользователя при сетевом подключении к системе;

модуль управления активностью, выполненный с возможностью инициации и администрирования активности пользователем в системе, а также формирования перечня условий, которым должен соответствовать профиль пользователя для права на создание активности;

модуль проведения активности, выполненный с возможностью обработки и реализации, инициированной пользователем, активности, создания политики доступа к объекту активности пользователем с привязкой к уникальному идентификатору и сверки меток времени, присвоенных каждому голосу пользователей с перечнем меток времени, сформированным при регистрации голосов;

модуль интеграции с внешними системами, выполненный с возможностью взаимодействия с внешними системами;

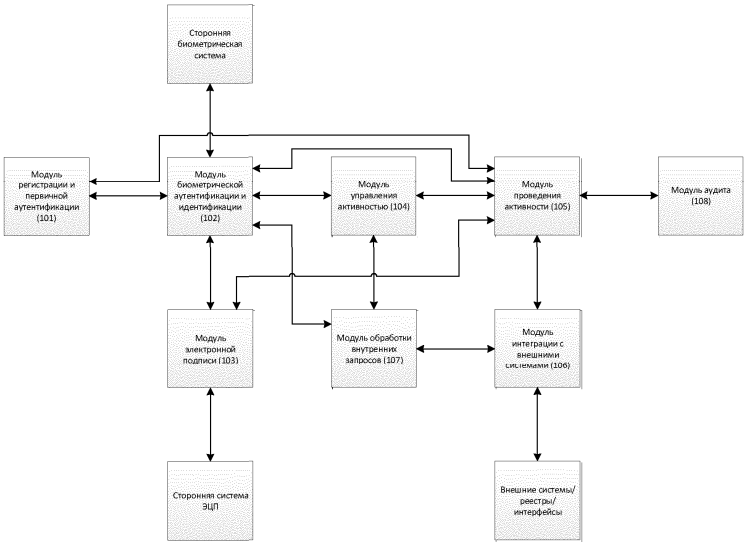
модуль обработки внутренних запросов, выполненный с возможностью интерпретации внутренних запросов от модулей системы в запросы к модулю интеграции с внешними системами;

модуль аудита, выполненный с возможностью проверки действий пользователя системы и ведения на основании фиксируемой информации системного журнала, а также формирования и отправки трех пакетов данных: пакета данных с полным набором данных о пользователе, включающем данные: "Уникальный идентификатор", "Временная метка", "Пользователь", "Хэш-сумма, подписанная сертификатом открытого ключа пользователя", "Решение пользователя", с отправкой по защищенному каналу связи с взаимной идентификацией на сторону серверной части системы, пакета с данными, описывающими пользователя, включающим данные: "Пользователь", "Хэш-сумма, подписанная сертификатом открытого ключа пользователя", с отправкой по каналу связи в публичную не анонимную блокчейн-систему, и пакета данных, описывающего волеизъявление пользователя, включающем данные: "Уникальный идентификатор", "Временная метка", "Решение пользователя", с отправкой по каналу связи в публичную анонимную блокчейн-систему.

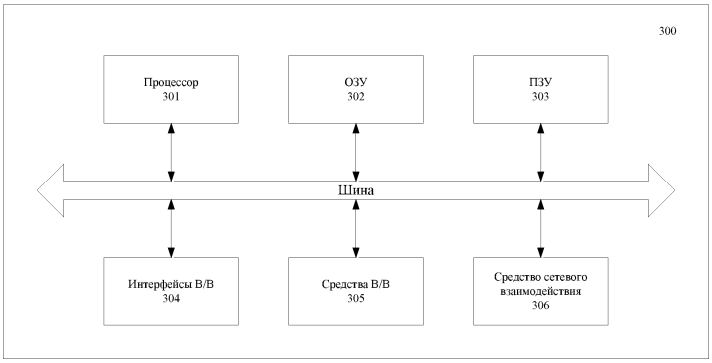
2. Система по п.1, характеризующаяся тем, что модули располагаются в едином вычислительном устройстве и объединены единой шиной.

3. Система по п.1, характеризующаяся тем, что по меньшей мере два модуля располагаются на различных вычислительных устройствах и объединены между собой каналами передачи данных.

4. Система по любому из пп.2, 3, характеризующаяся тем, что вычислительное устройство представляет собой персональный компьютер, сервер или мейнфрейм.


Сторонняя биометрическая система
Модуль регистрации и первичной аутентификации (101)
Модуль биометрической аутентификации и идентификации (102)
Модуль управления активностью (104)
Модуль проведения активности (105)
Модуль аудита (108)
Модуль электронной подписи (103)
Модуль обработки внутренних запросов (107)
Модуль интеграции с внешними системами (106)
Сторонняя система ЭЦП
Внешние системы/ реестры/ интерфейсы

Фиг. 1


300
Процессор 301
ОЗУ 302
ПЗУ 303
Шина
Интерфейсы В/В 304
Средства В/В 305
Средство сетевого взаимодействия 306

Фиг. 2