



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК

G06F 17/30964 (2018.08); H04M 3/42382 (2018.08); H04W 12/12 (2018.08)

(21)(22) Заявка: 2018109579, 18.08.2016

(24) Дата начала отсчета срока действия патента:
18.08.2016

Дата регистрации:
28.05.2019

Приоритет(ы):

(30) Конвенционный приоритет:
17.11.2015 US 62/256,204;
20.08.2015 US 62/207,444

(45) Опубликовано: 28.05.2019 Бюл. № 16

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 20.03.2018

(86) Заявка РСТ:
IL 2016/050912 (18.08.2016)

(87) Публикация заявки РСТ:
WO 2017/029677 (23.02.2017)

Адрес для переписки:
143026, Москва, ул. территория
инновационного центра "Сколково", 4, ООО
"ЦИС "Сколково"

(72) Автор(ы):

ДЖЕК, Игал (GB),
ЛАВИ, Офер (IL)

(73) Патентообладатель(и):

Общество с ограниченной ответственностью
"Визиллект" (RU)

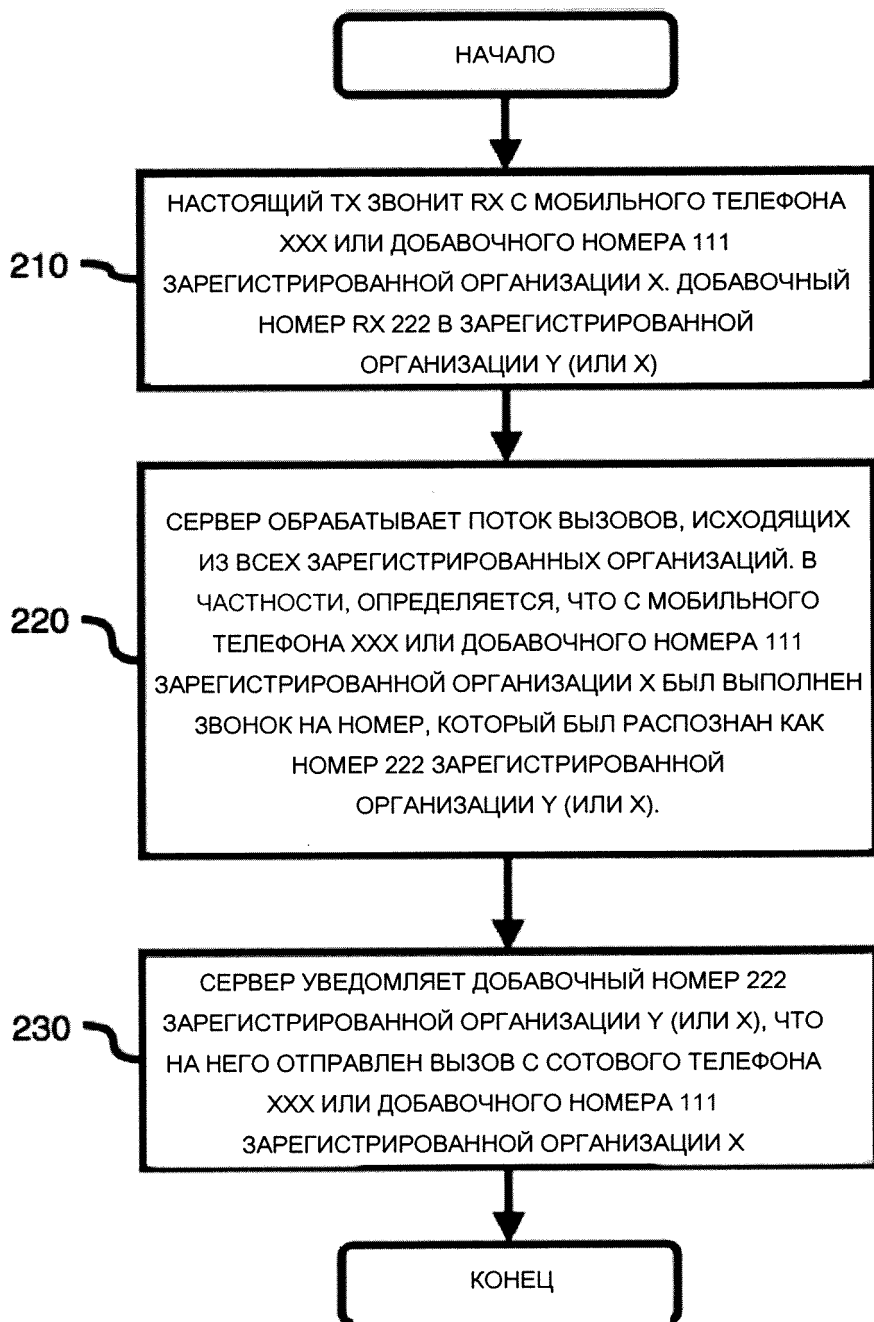
(56) Список документов, цитированных в отчете
о поиске: US 2014/233855 A1, 21.08.2014. RU
2405277 C2, 10.01.2010. US 2004/120478,
24.06.2004. KR 101399498, 30.05.2014.

(54) СИСТЕМА И СПОСОБ МОНИТОРИНГА СВЯЗИ, И/ИЛИ ВЫЯВЛЕНИЯ МОШЕННИКОВ, И/ИЛИ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ЗАЯВЛЕНИЙ/УТВЕРЖДЕНИЙ О ПРИНАДЛЕЖНОСТИ К КАКОЙ-ЛИБО ОРГАНИЗАЦИИ

(57) Реферат:

Система и способ, предназначенные для осуществления мониторинга связи и выявления мошенников tx, притворяющихся, что связываются с конечным пользователем gx по телефонной линии, связанной с организацией, к которой мошенник tx не имеет отношения. Технический результат заключается в предоставлении системы и способа мониторинга связи, и/или выявлении мошенников, и/или выяснении того, являются ли утверждения о принадлежности легитимному лицу и

определенной организации сделанными на законных основаниях или нет. Кроме того, система и способ подтверждения подлинности утверждения о принадлежности к организации содержат предоставление базы данных организаций, использование сервера/процессора для доступа к базе данных и через канал связи с конечными пользователями, предоставление конечным пользователям возможности получать от процессора аутентификацию заявленной принадлежности к организации. 6 н. и 23 з.п. ф-



ФИГ. 1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) **ABSTRACT OF INVENTION**

(52) CPC

G06F 17/30964 (2018.08); *H04M 3/42382* (2018.08); *H04W 12/12* (2018.08)(21)(22) Application: **2018109579**, 18.08.2016(24) Effective date for property rights:
18.08.2016Registration date:
28.05.2019

Priority:

(30) Convention priority:
17.11.2015 US 62/256,204;
20.08.2015 US 62/207,444(45) Date of publication: **28.05.2019** Bull. № 16(85) Commencement of national phase: **20.03.2018**(86) PCT application:
IL 2016/050912 (18.08.2016)(87) PCT publication:
WO 2017/029677 (23.02.2017)

Mail address:

143026, Moskva, ul. territoriya innovatsionnogo
tsentra "Skolkovo", 4, OOO "TSIS "Skolkovo"

(72) Inventor(s):

DZHEK, Igal (GB),
LAVI, Ofer (IL)

(73) Proprietor(s):

Obshchestvo s ogranichennoj otvetstvennostyu
"Vizillekt" (RU)(54) **SYSTEM AND METHOD OF MONITORING COMMUNICATION, AND/OR DETECTING SCAMMERS, AND/OR AUTHENTICATING STATEMENTS/ALLEGATIONS OF BELONGING TO ANY ORGANIZATION**

(57) Abstract:

FIELD: monitoring systems.

SUBSTANCE: system and a method for monitoring communication and detecting scammers tx, which pretend to communicate with an end user rx over a telephone line associated with an organization, to which the fraudster tx is not related. System and method of authenticating an organization membership claim include providing an organization database, using the server/processor to access the database and through a

communication channel with end users, enabling end users to obtain authenticated membership of the organization from the processor.

EFFECT: providing a system and method of monitoring communication, and/or detecting scammers, and/or clarifying whether statements of ownership of a legitimate person and a certain organization are legally established or not.

29 cl, 14 dwg

НАЧАЛО

210

НАСТОЯЩИЙ ТХ ЗВОНИТ RX С МОБИЛЬНОГО ТЕЛЕФОНА
XXX ИЛИ ДОБАВОЧНОГО НОМЕРА 111
ЗАРЕГИСТРИРОВАННОЙ ОРГАНИЗАЦИИ X. ДОБАВОЧНЫЙ
НОМЕР RX 222 В ЗАРЕГИСТРИРОВАННОЙ
ОРГАНИЗАЦИИ Y (ИЛИ X)

220

СЕРВЕР ОБРАБАТЫВАЕТ ПОТОК ВЫЗОВОВ, ИСХОДЯЩИХ
ИЗ ВСЕХ ЗАРЕГИСТРИРОВАННЫХ ОРГАНИЗАЦИЙ. В
ЧАСТНОСТИ, ОПРЕДЕЛЯЕТСЯ, ЧТО С МОБИЛЬНОГО
ТЕЛЕФОНА XXX ИЛИ ДОБАВОЧНОГО НОМЕРА 111
ЗАРЕГИСТРИРОВАННОЙ ОРГАНИЗАЦИИ X БЫЛ ВЫПОЛНЕН
ЗВОНОК НА НОМЕР, КОТОРЫЙ БЫЛ РАСПОЗНАН КАК
НОМЕР 222 ЗАРЕГИСТРИРОВАННОЙ
ОРГАНИЗАЦИИ Y (ИЛИ X).

230

СЕРВЕР УВЕДОМЛЯЕТ ДОБАВОЧНЫЙ НОМЕР 222
ЗАРЕГИСТРИРОВАННОЙ ОРГАНИЗАЦИИ Y (ИЛИ X), ЧТО
НА НЕГО ОТПРАВЛЕН ВЫЗОВ С СОТОВОГО ТЕЛЕФОНА
XXX ИЛИ ДОБАВОЧНОГО НОМЕРА 111
ЗАРЕГИСТРИРОВАННОЙ ОРГАНИЗАЦИИ X

КОНЕЦ

ФИГ. 1

РОДСТВЕННЫЕ ЗАЯВКИ

Приоритет заявлен, исходя из предварительной заявки на патент США №62/207444 под названием «Система и способ для подтверждения подлинности утверждений о принадлежности к какой-либо организации», поданной 20.08.2015, и из предварительной заявки на патент США №62/256204 под названием «Системы и способы мониторинга связи, в том числе для выявления мошенников», поданной 17.11.2015. Обе заявки включены в настоящее описание в полном объеме посредством ссылки.

ОБЛАСТЬ ТЕХНИКИ

Настоящее изобретение относится к области удостоверения подлинности, в частности, подлинности абонентов систем связи.

УРОВЕНЬ ТЕХНИКИ

Вишинг или голосовой фишинг заключается в использовании телефона для осуществления мошеннических действий в адрес пользователей под видом существующей организации.

Сервис Pindrop.com предлагает запатентованную, как заявлено, услугу, которая анализирует телефонные звонки для выявления злонамеренных действий и проверки легитимности вызывающих абонентов. В основе решений Центра по борьбе с высокотехнологическим мошенничеством (Call Center Anti-Fraud) компании Pindrop, используемых рядом крупнейших банков, страховых компаний, брокерских компаний и предприятий розничной торговли в США для выявления мошенничества и проверки клиентов, лежит технология Phoneprinting. С помощью данной технологии аудиовызов разбивается на 147 уникальных признаков для создания уникального идентификатора для каждого вызывающего абонента. С помощью технологии Phoneprinting компании Pindrop выявляются следующие характеристики: **ТИП ВЫЗОВА:** Что используется вызывающим абонентом: мобильный телефон, стационарный телефон или звонок по протоколу VoIP? Исследование, проведенное компанией Pindrop, показало, что 53% мошеннических звонков осуществляется по протоколу VoIP при 7,2% в случае законных звонков. **ГЕОЛОКАЦИЯ:** Где в действительности находится источник вызова? Вызов международный или внутренний? Совпадает ли местоположение, указанное аудиовыводом, с номером телефона, определенным по идентификатору вызывающего абонента? **УНИКАЛЬНЫЙ ТЕЛЕФОН:** Был ли данный вызывающий абонент замечен ранее? Мошенники часто меняют номера телефонов, но гораздо сложнее изменить аудиохарактеристики, которые используются компанией Pindrop для создания уникального идентификатора аудиохарактеристик вызова.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

В некоторых вариантах осуществления изобретения предлагается предоставлять систему и способ мониторинга связи и/или выявления мошенников и/или выяснения того, являются ли утверждения о принадлежности легитимному лицу и определенной организации сделанными на законных основаниях или нет. Например, автоинформатор или оператор связи, осуществляющий звонок на домашний телефон, может представиться как представитель клиентской службы компании X.

Таким образом, в соответствии, по меньшей мере, с одним из вариантов осуществления настоящего изобретения, предоставляются система, способ или программное обеспечение, предназначенные для осуществления мониторинга связи и выявления мошенников tx, притворяющихся, что связываются с конечным пользователем gx по телефонной линии, связанной с организацией, к которой мошенник tx не имеет отношения.

В соответствии, по меньшей мере, с одним из вариантов осуществления настоящего

изобретения также предоставляются система, способ или программное обеспечение, предназначенные для подтверждения подлинности утверждения принадлежности к какой-либо организации (заявленная принадлежность к организации), и содержащие следующие функции: Предоставление базы данных организаций; Использование сервера/процессора для доступа к базе данных; и - через канал связи с конечными пользователями - предоставление конечным пользователям возможности получать от процессора аутентификацию заявленной принадлежности к организации.

Также за исключением сигналов, изобретение представляет собой компьютерную программу, содержащую средства компьютерного программного кода для применения любого из способов, упомянутых и описанных в данном документе, при запуске упомянутой программы, по меньшей мере, на одном компьютере; и компьютерное программное обеспечение, содержащее обычно непереходный компьютерный или машиночитаемый носитель данных, например носитель данных, обычно материальный, содержащий машиночитаемый программный код, который при этом выполнен с возможностью применения для реализации каких-либо или всех способов, приведенных и описанных в данном документе. В соответствии с рекомендациями данного документа операции могут выполняться, по меньшей мере, одним компьютером, специально созданным для определенного функционального назначения, или компьютером общего назначения, специально настроенном на выполнение определенного функционального назначения, по меньшей мере, одной компьютерной программой, хранящейся, как правило, на непереходном машиночитаемом носителе данных. Термин «непереходный» используется в данном документе для исключения переходных, распространяющихся сигналов или волн, но в при этом включает в себя любую технологию энергозависимой или энергонезависимой компьютерной памяти, подходящую для приложения.

Для обработки, отображения, например, на экране компьютера или другом устройстве вывода информации, хранения и приема информации, которая используется или генерируется любым из способов и устройств, упомянутых и описанных в данном документе, могут использоваться любые подходящие процессоры, средства отображения и ввода; вышеупомянутые процессоры, средства отображения и ввода, включая компьютерные программы, должны соответствовать некоторым или всем вариантам осуществления настоящего изобретения. Некоторые или все функциональные возможности изобретения, упомянутые и описанные в данном документе, включающие в себя без ограничений операции в блок-схемах, могут выполняться любым одним или несколькими из следующих устройств: по меньшей мере одного обычного процессора персонального компьютера, рабочей станции, или другого программируемого устройства, или компьютера, или электронного вычислительного устройства, или процессора, как общего назначения, так и специально сконструированных, используемых для обработки; экрана дисплея компьютера и/или принтера и/или динамика для отображения; машиночитаемых накопителей, например, оптических дисков, CD-ROM, DVD, BluRays, магнитооптических дисков или других дисков; ОЗУ, ПЗУ, EPROM, EEPROM, магнитных, оптических или других карт для хранения; клавиатуры или мыши для приема. Модули, упомянутые и описанные в данном документе, могут включать в себя любую одну или комбинацию нескольких или множество следующих устройств: сервер, процессор данных, накопитель/запоминающее устройство, интерфейс связи, компьютерную программу, хранящуюся на накопителе/ЗУ.

Термин «процесс», используемый выше, предназначен для описания любого типа вычислений, манипуляций или преобразования данных, представленных как физические, например, электронные явления, которые могут возникать или происходить, например,

в регистраторах и/или накопителях, по меньшей мере, одного компьютера или процессора. Термин «процессор» включает в себя один блок обработки данных или несколько таких распределенных или удаленных блоков.

Упомянутые устройства могут взаимодействовать посредством любых обычных проводных или беспроводных цифровых средств связи, например, через проводную или сотовую телефонную сеть или компьютерную сеть, такую как Интернет.

Устройство настоящего изобретения может включать в себя, в соответствии с некоторыми вариантами осуществления изобретения, машиночитаемый накопитель, содержащий или иным образом сохраняющий программу инструкций, которая при ее исполнении машиной вводит в действие некоторые или все устройства, способы, функции и функциональные возможности изобретения, упомянутые и описанные в данном документе. В качестве альтернативы или в дополнение, устройство настоящего изобретения может включать в себя, в соответствии с некоторыми вариантами осуществления изобретения, программу, описанную выше, которая может быть записана на любом традиционном языке программирования, и, в некоторых случаях, аппарат для выполнения программы, например, компьютер общего назначения, который может быть, при желании, настроен или активирован в соответствии с рекомендациями настоящего изобретения. Любая из рекомендаций данного документа может в некоторых случаях подходящим образом работать в отношении сигналов, представляющих физические объекты или вещества.

Описанные выше и другие варианты осуществления подробно описаны в следующем разделе.

Любой товарный знак, встречающийся в тексте или чертежах, является собственностью его владельца и в данном документе используется только для объяснения или иллюстрации примера того, как может быть реализован вариант осуществления изобретения.

Если не указано иное, то, как видно из следующих описаний, следует понимать, что во всех описаниях спецификации, такие используемые термины, как «обработка», «вычисление», «оценка», «выбор», «ранжирование», «градуировка», «расчеты», «определение», «генерация», «переоценка», «классификация», «производство», «согласование изображений», «регистрация», «обнаружение», «привязка», «наложение», «получение» и т.п., относятся к действию и/или процессам, по меньшей мере, одного компьютера, вычислительной системы, процессора или аналогичных электронных вычислительных устройств, которые оперируют данными и/или преобразуют данные, представленные в физическом виде, например как электронные величины, в регистраторах и/или накопителях вычислительной системы, в другие данные, аналогично представляемые в виде физических величин в накопителях, регистраторах или других подобных устройствах для хранения, передачи или отображения информации. Термин «компьютер» следует понимать в широком смысле, охватывающем любое электронное устройство с возможностями обработки данных, в том числе, в качестве неограничивающего примера, персональные компьютеры, серверы, встроенные ядра, вычислительные системы, устройства связи, процессоры (например, цифровой сигнальный процессор (ЦСП), микроконтроллеры, программируемые пользователем вентильные матрицы (ППВМ), специализированные интегральные микросхемы (СИМС) и т.д.) и другие электронные вычислительные устройства.

Настоящее изобретение может быть описано, исключительно для упрощения, с точки зрения терминологии, характерной для конкретных языков программирования, операционных систем, браузеров, версий систем, отдельных продуктов и т.п. Следует

понимать, что такая терминология призвана четко и кратко изложить общие принципы работы и используется в качестве примера, а не для ограничения объема изобретения каким-либо конкретным языком программирования, операционной системой, браузером, версией системы или отдельным продуктом.

5 Элементы, отдельно перечисленные здесь, не обязательно должны быть отдельными блоками и, в качестве альтернативного варианта, могут образовывать один конструктивный элемент. Утверждение о возможности наличия какого-либо элемента или признака предназначено для включения (а) вариантов осуществления изобретения, в которых присутствует данный элемент или признак; (b) вариантов осуществления изобретения, в которых не присутствует данный элемент или признак; и (с) вариантов осуществления изобретения, в которых данный элемент или признак существуют выборочно, например, в зависимости от настройки или выбора пользователя.

Для генерации или иного предоставления информации, полученной оборудованием и способами, упомянутыми и описанными в данном документе, может использоваться 15 любое подходящее устройство ввода, например, датчик. Для отображения или вывода информации, генерируемой оборудованием и способами, упомянутыми и описанными в данном документе, может использоваться любое подходящее устройство вывода или дисплей. Любой подходящий процессор может использоваться для обработки или генерации информации в соответствии с приведенным в данном документе описанием, 20 и/или для выполнения функций, описанных в данном документе, и/или для ввода в работу какого-либо двигателя, интерфейса или другой системы, описанной в данном документе. Для хранения информации, полученной или генерируемой системами, упомянутыми и описанными в данном документе, может использоваться любое подходящее компьютеризированное хранилище данных, например, память компьютера. 25 Функциональные возможности, упомянутые и описанные в данном документе, могут быть разделены между сервером и множеством клиентских компьютеров. Эти или любые другие компьютеризированные компоненты, упомянутые и описанные в данном документе, могут связываться между собой через подходящую компьютерную сеть.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

30 На фиг. 1 показан пример последовательности для ситуации, в которой подлинный tx вызывает gx с добавочного номера телефона зарегистрированной организации.

На фиг. 2 показан пример последовательности для ситуации, в которой мошенник tx вызывает gx с мобильного телефона, номера VoIP-клиента или добавочного номера телефона зарегистрированной организации.

35 На фиг. 3-10 представлены диаграммы, иллюстрирующие аспекты вариантов осуществления настоящего изобретения, элементы которых могут быть предоставлены отдельно или в любой подходящей комбинации.

На фиг. 11-14 представлены блок-схемы последовательности операций, включающие в себя общую блок-схему последовательности операций и пример ее конкретного 40 варианта осуществления, как для мошеннического, так и для подлинного вызова, в соответствии с некоторыми вариантами осуществления настоящего изобретения.

Способы и системы, входящие в объем настоящего изобретения, могут включать в себя некоторые (любой подходящий комплект) или все функциональные блоки, показанные в специально изображенных вариантах осуществления в качестве примера, 45 в любом подходящем порядке, например, приведенном в данном документе.

Вычислительные, функциональные или логические компоненты, описанные и проиллюстрированные в данном документе, могут быть реализованы в различных формах, например, в виде аппаратных схем, включающих в себя без ограничений

специализированные сверхбольшие интегральные схемы, матрицы логических элементов или программируемые аппаратные устройства, включающие в себя без ограничений ППВМ или код программного обеспечения, хранящийся, по меньшей мере, на одном материальном или нематериальном машиночитаемом носителе, и исполняемый, по меньшей мере, на одном процессоре или любом подходящем сочетании устройств. Конкретный функциональный компонент может быть сформирован одной конкретной последовательностью программного кода или множеством последовательностей, которые действуют совместно или в соответствии с приведенным в данном документе описанием в отношении соответствующего функционального компонента. Например, компонент может быть распределен по нескольким кодовым последовательностям, включающим в себя без ограничений объекты, процедуры, функции, алгоритмы и программы, и может поступать из нескольких компьютерных файлов, обычно работающих синергетически.

Каждая функциональная возможность или способ, упомянутые в данном документе, могут быть реализованы в виде программного обеспечения, прошивки, оборудования или любого их сочетания. Функциональные возможности или операции, предусмотренные как реализуемые в виде программного обеспечения, могут альтернативно быть полностью реализованы в рамках соответствующего оборудования или программно-аппаратного модуля и наоборот. Любая логическая функциональная возможность, описанная в данном документе, может быть реализована, если и когда это необходимо, в виде приложения реального времени, которое может использовать любой подходящий архитектурный вариант, включающий в себя без ограничений ППВМ, специализированные интегральные микросхемы, процессор ЦОС или любое подходящее их сочетание.

Любой упомянутый в данном документе аппаратный компонент может в действительности включать в себя одно или несколько аппаратных устройств, например, чипы, которые могут быть размещены рядом или удалены друг от друга.

Любой способ, описанный в данном документе, должен включать в себя в рамках объема вариантов осуществления настоящего изобретения также любое программное обеспечение или компьютерную программу, выполняющую некоторые или все операции этого способа, включая мобильное приложение, платформу или операционную систему, например, хранящиеся на накопителе, а также объединяющую компьютерную программу с аппаратным устройством для выполнения некоторых или всех операций этого способа.

Данные могут храниться на одном или нескольких материальных или нематериальных машиночитаемых носителях, хранящихся в одном месте или в нескольких разных местах, разных сетевых узлах или разных устройствах хранения в одном узле или месте.

Следует понимать, что для хранения различных данных, предоставленных и используемых в данном документе, может использоваться любая технология хранения компьютерных данных, включая любой тип хранилища или накопителя, а также любые компьютерные компоненты и носители, которые сохраняют цифровые данные, используемые для производства вычислений в течение определенного промежутка времени, и любой тип технологий хранения информации. Подходящим устройством хранения данных или запоминания информации может быть устройство, являющееся первичным, вторичным, третичным или автономным; которое имеет любой тип, уровень, величину или категорию волатильности, дифференциации, изменчивости, доступности, адресности, мощности, производительности и использования энергии; и в основе которого используются любые подходящие технологии, например, полупроводниковые,

магнитные, оптические, бумажные и др.

ПОДРОБНОЕ ОПИСАНИЕ

В соответствии с некоторыми вариантами осуществления изобретения применяются следующие способы (каждая последовательность при этом может включать в себя некоторые или все указанные операции, соответственным образом упорядоченные, например, как показано):

Пример процедуры интеграции, которая может выполняться интегратором, когда он/она интегрирует или регистрирует организацию x, например, при подготовке к использованию способов блок-схем 1, 2, описанной далее; блок-схемы 1, 2, приведенные ниже, предполагают, что сервер уже зарегистрировал организацию x, которая имеет 1000 добавочных номеров в системе (к примеру).

На фиг. 1 показан пример последовательности для ситуации, в которой подлинный tx вызывает gx с добавочного номера телефона зарегистрированной организации. Способ, продемонстрированный на фиг. 1, обычно включает в себя некоторые или все из следующих операций, соответственным образом упорядоченных, например, как показано:

210: настоящий tx звонит gx с мобильного телефона xxx или добавочного номера 111 зарегистрированной организации x. Добавочный номер gx в зарегистрированной организации у (или x) - 222.

220: сервер обрабатывает поток вызовов, исходящих из всех зарегистрированных организаций. В частности, определяется, что с мобильного телефона xxx или добавочного номера 111 зарегистрированной организации x был выполнен звонок на номер, который был распознан как номер 222 зарегистрированной организации у (или x).

230: Сервер уведомляет добавочный номер 222 зарегистрированной организации у (или x), что на него отправлен вызов с сотового телефона xxx или добавочного номера 111 зарегистрированной организации x

На фиг. 2 показан пример последовательности для ситуации, в которой мошенник tx вызывает gx с мобильного телефона, номера VoIP-клиента или добавочного номера телефона зарегистрированной организации. Способ, продемонстрированный на фиг. 2, обычно включает в себя некоторые или все из следующих операций, соответственным образом упорядоченных, например, как показано:

310: мошенник tx звонит gx якобы с мобильного телефона xxx или добавочного номера 111 зарегистрированной организации x. Добавочный номер gx в зарегистрированной организации у (или x) - 222.

320: сервер обрабатывает поток входящих вызовов на все добавочные номера зарегистрированных организаций. В частности, определяется, что кто-то под видом сотового телефона xxx или добавочного номера 111 зарегистрированной организации x отправил вызов на добавочный номер 222 зарегистрированной организации у (или x). Сервер проверяет поток исходящих вызовов от всех зарегистрированных организаций и не находит в указанное время вызов с сотового телефона xxx или добавочного номера 111 зарегистрированной организации x на добавочный номер 222 зарегистрированной организации у (или x)

330: сервер разъединяет вызов между мошенником и добавочным номером gx 222 и/или предупреждает абонента добавочного номера gx 222 зарегистрированной организации у (или x), например следующим сообщением: предупреждение!! Лицо, которое звонит вам якобы с мобильного телефона xxx/добавочного номера 111 зарегистрированной организации x, на самом деле является мошенником! (уведомление

обычно отправляется через несколько каналов (например, в чат-приложение на рабочем столе пользователя или на мобильный телефон пользователя, если звонок направлен на его стационарный телефон и т.д.), которые не блокируются входящим вызовом; в качестве альтернативы или в дополнение, вызов может быть разъединен, если это

5 поддерживается платформой).

Применимость приведенных выше блок-схем никоим образом не ограничивается вызовами с фактического добавочного номера, т.е. телефона, подключенного к телефонной станции организации. Как показывают блок-схемы, вызовы могут также поступать с мобильного телефона или номера VOIP-клиента (т.н. «программного

10 телефона»), например, в соответствии с подробным описанием, приведенным ниже.

Решение определенных вариантов осуществления позволяет пользователям подтвердить подлинность любого представителя клиентской службы или «заявителя», претендующего на принадлежность к определенной организации или корпорации.

Всякий раз, когда представитель клиентской службы высказывает подобное утверждение (по телефону, при личном посещении, через текстовое сообщение, электронную почту

15 и т.д.), пользователь просто просит данного представителя воспользоваться

определенным решением вариантов осуществления изобретения, чтобы подтвердить, что он действительно представляет организацию, о принадлежности к которой он заявляет. Затем представитель отправляет номер мобильного телефона пользователя

20 в Сервис подтверждения подлинности (СПП) определенного варианта осуществления изобретения, или сам конечный пользователь предоставляет свои контактные данные, например, электронную почту, телефон, facebook и т.д., непосредственно в СПП или каким-либо другим образом не через заявителя. Это можно сделать через следующие сервисы:

25 А. Сервисный портал определенных вариантов осуществления изобретения

В. Портал организации/корпорации, который связывается с СПП через интерфейс API

С. Служебное приложение для смартфонов определенных вариантов осуществления изобретения

30 Затем СПП отправляет пользователю с помощью любой подходящей технологии, протокола или канала связи защищенное сообщение с подтверждением, что представитель действительно работает в заявленной организации/корпорации.

Решение одного из вариантов осуществления изобретения дополнительно позволяет корпоративным сотрудникам подтвердить подлинность любого звонка, сделанного с корпоративного номера (отделы по ИТ, HR, безопасности и т.д.), или сотрудника, претендующего на принадлежность к какой-либо организации или корпорации. Решение

35 определенных вариантов осуществления обрабатывает как внутрикорпоративные, так и межкорпоративные вызовы.

Внутрикорпоративным решением определенных вариантов осуществления предоставляются средства для автоматического подтверждения личности при осуществлении вызова между корпоративными пользователями. Это возможно в

40 следующих случаях:

А. Корпоративный пользователь звонит другому корпоративному пользователю

В. Корпоративный пользователь звонит в конференц-зал // на голосовой мост

45 Эти вызовы могут быть выполнены через:

А. мобильный телефон с поддержкой сервиса подтверждения подлинности

В. корпоративная мини АТС с поддержкой сервиса подтверждения подлинности

С. VOIP-клиент с поддержкой сервиса подтверждения подлинности

В некоторых вариантах осуществления Сервис подтверждения подлинности (СПП) затем отправляет вызываемым сторонам защищенное или персонализированное сообщение с подтверждением, что вызывающий абонент действительно работает в заявленной организации/корпорации. Сообщение может быть отправлено с помощью
 5 любой технологии, протокола или канала связи, подходящих для корпоративных пользователей (например, через компьютеры-клиенты, корпоративные чат-сервисы, персонализированные текстовые сообщения, уведомления на основе токенов безопасности (синхронизированный по времени одноразовый пароль), уведомления с голосовыми подписями, пейджеры), которые могут также учитывать информацию о
 10 присутствии и местоположении пользователя (например, на рабочем месте или вдали от него, на собрании, вне офиса).

Внутрикорпоративное решение определенных вариантов осуществления изобретения дополнительно предоставляет средства для подтверждения достоверности входящих вызовов при их выполнении между двумя корпоративными пользователями,
 15 принадлежащими к отдельным организациям. Это может быть осуществлено, когда корпоративный пользователь получает вызов через:

- А. мобильный телефон с поддержкой сервиса подтверждения подлинности
- В. корпоративная мини АТС с поддержкой сервиса подтверждения подлинности
- С. VOIP-клиент с поддержкой сервиса подтверждения подлинности

20 Когда это происходит, клиентская система (или мини АТС) отправляет идентификационную информацию по вызываемому абоненту в Сервис подтверждения подлинности (СПП) определенного варианта осуществления изобретения, которая определяет, является ли вызов законным, поддельным или неизвестным.

Последовательности могут включать в себя последовательности регистрации и/или
 25 подтверждения подлинности.

Конечному пользователю могут предоставляться последовательности регистрации, которые могут включать в себя некоторые или все из следующих последовательностей. Также могут быть предусмотрены соответствующие последовательности регистрации для организаций, принадлежность к которым должна быть подтверждена.

30 Последовательность регистрации конечного пользователя может быть идентична для всех сотрудников корпорации, как осуществляющих вызов, так и принимающих его.

Последовательность «Смартфон» - автономное приложение может выполнять некоторые или все из следующих операций, соответственным образом упорядоченных, например, как показано:

- 35 1. Пользователь устанавливает наше приложение на свой телефон
2. Пользователь запускает наше приложение на своем телефоне
3. Приложение просит пользователя ввести свой номер телефона
4. Пользователь вводит номер телефона
5. Приложение отправляет запрос на сервер для проверки номера телефона (при
 40 необходимости, через защищенное соединение). Происходит оперативная проверка, например, в соответствии с некоторыми или всеми операциями 6-9, приведенными ниже.
6. Сервер отправляет текстовое сообщение с кодом подтверждения на указанный номер телефона
7. Пользователь вводит код из текстового сообщения в наше приложение.
- 45 8. Приложение отправляет код обратно на сервер (при необходимости, через защищенное соединение), который определяет, действителен ли он и отправляет в приложение соответствующий ответ.

9. Затем сервер сохраняет некоторые или все из следующих данных пользователя в

базу данных, связанную с сервером:

- a. Номер телефона
- b. Идентификатор устройства
- c. Push-токен
- 5 d. Тип мобильной платформы
- e. Версия мобильной платформы
- f. (и некоторые другие данные, таких как язык пользователя, версия клиентской системы и т.д.)

В дополнение могут осуществляться некоторые или все из следующих операций:

10 10. Затем сервер дополнительно проверяет, привязан ли номер пользователя в системе к какой-либо корпорации. Если это так, сервер регистрирует принадлежность к этой корпорации в информации о пользователе.

11. Сервер отправляет клиенту ответ с подтверждением правильности или
15 неправильности кода и указанием любых дополнительных операций, которые могут быть выполнены клиентом. Дополнительные операции индивидуально настраиваются для каждого корпоративного пользователя и могут включать в себя, по меньшей мере, любое сочетание следующих операций:

a. Персонализированная голосовая подпись:

i. В этом случае клиентская система предлагает пользователю записать
20 персонализированную голосовую подпись.

ii. Эта голосовая подпись затем сохраняется в клиентской системе, а также может быть защищенным образом отправлена на сервер.

iii. Эта голосовая подпись может использоваться впоследствии при получении пользователем подтверждения подлинности с сервера.

25 Это позволяет гарантировать, что подтверждение подлинности действительно получено через наше приложение, а не из другого приложения, установленного на телефоне, маскирующегося под наше приложение (с помощью той же иконки, названия и т.д.),

b. Персонализированная текстовая кодовая фраза:

30 iv. В этом случае клиентская система предлагает пользователю ввести персонализированную кодовую фразу.

v. Затем эта кодовая фраза защищенным образом отправляется на сервер.

vi. Эта кодовая фраза может использоваться впоследствии при получении пользователем подтверждения подлинности с сервера. Это позволяет гарантировать,
35 что подтверждения подлинности, полученные по незащищенным соединениям (например, SMS, Flash SMS, MMS), действительно отправлены с нашего сервиса.

c. Персонализированная фотография:

vii. В этом случае клиентская система предлагает пользователю предоставить персонализированную фотографию (либо из галереи телефона, либо с помощью камеры
40 телефона).

viii. Эта персонализированная фотография затем сохраняется в клиентской системе, а также может быть защищенным образом отправлена на сервер.

ix. Эта персонализированная фотография может использоваться впоследствии при получении пользователем подтверждения подлинности с сервера. Это позволяет
45 гарантировать, что подтверждения подлинности, полученные по незащищенным соединениям (например, MMS), действительно отправлены с нашего сервиса.

Последовательность «Смартфон» - комплект разработки ПО может включать в себя некоторые или все из следующих операций, соответственным образом упорядоченных,

например, как показано:

1. Пользователь устанавливает приложение корпорации, включающее в себя наш комплект разработки ПО, на свой телефон

2. Пользователь запускает приложение на своем телефоне

5 3. Приложение просит пользователя ввести свой номер телефона

4. Пользователь вводит номер телефона

5. Приложение отправляет запрос на сервер с помощью комплекта разработки ПО для проверки номера телефона (при необходимости, через защищенное соединение). Происходит оперативная проверка, например, в соответствии с некоторыми или всеми операциями 6-9, приведенными ниже.

10 6. Сервер отправляет текстовое сообщение с кодом подтверждения на указанный номер телефона

7. Пользователь вводит код из текстового сообщения в приложение.

8. Приложение отправляет код обратно на сервер с помощью комплекта разработки ПО (при необходимости, через защищенное соединение), который определяет, действителен ли он и отправляет в приложение соответствующий ответ.

9. Затем сервер регистрирует, например, в базе данных, связанной с сервером, подходящие данные пользователя, включающие в себя без ограничений некоторые или все из следующих:

20 a. Номер телефона

b. Идентификатор устройства

c. Push-токен

d. Тип мобильной платформы

e. Версия мобильной платформы

25 f. Язык пользователя

g. Версия клиентской системы

В дополнение могут осуществляться некоторые или все из следующих операций:

10. Сервер отправляет клиенту ответ с подтверждением правильности или неправильности кода и указанием любых дополнительных операций, которые могут быть выполнены клиентом. Дополнительные операции индивидуально настраиваются для каждого корпоративного пользователя и могут включать в себя, по меньшей мере, любое сочетание следующих операций:

a. Персонализированная голосовая подпись:

35 i. В этом случае клиентская система предлагает пользователю записать персонализированную голосовую подпись.

ii. Эта голосовая подпись затем сохраняется в клиентской системе, а также может быть отправлена на сервер.

iii. Эта голосовая подпись может использоваться впоследствии при получении пользователем подтверждения подлинности с сервера. Это позволяет гарантировать, что подтверждение подлинности действительно получено через наше приложение, а не из другого приложения, установленного на телефоне, маскирующегося под наше приложение (с помощью той же иконки, названия и т.д.),

b. Персонализированная текстовая кодовая фраза:

45 i. В этом случае клиентская система предлагает пользователю ввести персонализированную кодовую фразу.

ii. Затем эта кодовая фраза отправляется на сервер.

iii. Эта кодовая фраза может использоваться впоследствии при получении пользователем подтверждения подлинности с сервера. Это позволяет гарантировать,

что подтверждения подлинности, полученные по незащищенным соединениям (например, SMS, Flash SMS, MMS), действительно отправлены с нашего сервиса.

с. Персонализированная фотография:

5 i. В этом случае клиентская система предлагает пользователю предоставить персонализированную фотографию (либо из галереи телефона, либо с помощью камеры телефона),

ii. Эта персонализированная фотография затем сохраняется в клиентской системе, а также может быть отправлена на сервер. Эта персонализированная фотография может использоваться впоследствии при получении пользователем подтверждения
10 подлинности с сервера. Это позволяет гарантировать, что подтверждения подлинности, полученные по незащищенным соединениям (например, MMS), действительно отправлены с нашего сервиса.

Последовательность «Веб-браузер» - приложение Facebook может выполнять некоторые или все из следующих операций:

15 1. Пользователь добавляет специальное приложение Facebook к своей учетной записи Facebook

2. Пользователь запускает приложение Facebook

3. Приложение просит пользователя ввести свой номер телефона

4. Пользователь вводит номер телефона

20 5. Приложение отправляет запрос на сервер для проверки номера телефона (при необходимости, через защищенное соединение). Происходит оперативная проверка, например, в соответствии с некоторыми или всеми операциями 6-9, приведенными ниже.

6. Сервер отправляет текстовое сообщение с кодом подтверждения на указанный номер телефона

25 7. Пользователь вводит код из текстового сообщения в приложение Facebook

8. Приложение отправляет код обратно на сервер (при необходимости, через защищенное соединение), который определяет, действителен ли он и отправляет в приложение соответствующий ответ.

9. Затем сервер регистрирует, например, в базе данных, связанной с сервером,
30 подходящие данные пользователя, включающие в себя без ограничений некоторые или все из следующих:

a. Номер телефона

b. Идентификатор пользователя в Facebook

c. Язык пользователя

35 d. Версия приложения

Последовательности подтверждения подлинности может включать в себя некоторые или все из следующих последовательностей:

Последовательность «Телефонный звонок» может включать в себя некоторые или все из следующих операций, соответственным образом упорядоченных, например, как
40 показано:

1. Пользователь получает входящий вызов

2. Вызывающий абонент заявляет, что является представителем корпорации N

3. Пользователь просит вызывающего абонента/заявителя подтвердить подлинность, используя наш сервис

45 4. Вызывающий абонент/заявитель регистрируется в нашем приложении виджет/портал/сервис (используя имя пользователя и пароль, предоставленные во время пост-верификационной стадии регистрации представителя), чтобы ввести номер телефона пользователя и (необязательно) текстовое сообщение (например, «Это Дэн из

корпорации N - Я хотел бы совершить звонок технического специалиста для обслуживания нашего оборудования») - затем эта информация:

- a. Ретранслируется в СПП через один из наших интерфейсов API, и
- b. Сохраняется в базе данных, связанной с СПП

5 Наш портал производит поиск номера телефона пользователя в базе данных и находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.). Эта информация основана на данных, полученных от пользователя (номер телефона, идентификатор устройства, push-токен, тип мобильной платформы, версия мобильной платформы, язык пользователя, версия клиентской системы и т.д.) в рамках последовательности регистрации.

10 6. Дополнительно (по желанию): представитель получает код подтверждения от нашего приложения виджет/портал/сервис

7. Наш портал (как правило, только в том случае, если вызывающий абонент/заявитель определен системой как представитель корпорации N) отправляет защищенное уведомление (т.е. уведомления не могут быть подделаны или отправлены какой-либо третьей стороной), например, с помощью push-токена пользователя, на устройство пользователя, содержащее некоторые или все из следующих данных:

- a. Наименование корпорации
- b. Код подтверждения из пункта №6 выше (по желанию)
- 20 c. Имя представителя (по желанию)
- d. Текстовое сообщение, введенное представителем (по желанию)
- e. Страна, в которой зарегистрирована корпорация N (по желанию)
- 8. Дополнительно (по желанию): пользователь может запросить у представителя код подтверждения.

25 На фиг. 3 изображены различные компоненты и соединения, используемые в последовательности подтверждения подлинности посредством телефонного звонка согласно варианту осуществления данного решения.

Последовательность «SMS-сообщение» может включать в себя некоторые или все из следующих операций, соответственным образом упорядоченных, например, как

30 показано:

1. Пользователь получает текстовое сообщение якобы от представителя корпорации N

2. Пользователь просит представителя подтвердить подлинность, используя наш сервис

35 3. Представитель использует наше приложение виджет/портал/сервис, чтобы ввести номер телефона пользователя и (необязательно) текстовое сообщение (например, «Это Дэн из корпорации N - Я хотел бы совершить звонок технического специалиста для обслуживания нашего оборудования») - затем эта информация:

- a. Ретранслируется в СПП через один из наших интерфейсов API, и
- 40 b. Сохраняется в базе данных, связанной с СПП

4. Наш портал производит поиск номера телефона пользователя в базе данных и находит соответствующую информацию для связи с пользователем (например, тип и версия платформы, идентификатор и т.д.). Эта информация основана на данных, полученных от пользователя (номер телефона, идентификатор устройства, push-токен, тип мобильной платформы, версия мобильной платформы, язык пользователя, версия клиентской системы и т.д.) в рамках последовательности регистрации.

45 5. Дополнительно (по желанию): представитель получает код подтверждения от нашего приложения виджет/портал/сервис

6. Наш портал отправляет защищенное уведомление (т.е. уведомления не могут быть подделаны или отправлены какой-либо третьей стороной), например, с помощью push-токена пользователя, на устройство пользователя, содержащее по меньшей мере один из следующих видов данных:

- 5 а. Наименование корпорации
- б. Код подтверждения из пункта №5 выше (по желанию)
- с. Имя представителя (по желанию)
- д. Текстовое сообщение, введенное представителем (по желанию)
- е. Страна, в которой зарегистрирована корпорация N (по желанию)
- 10 7. Дополнительно (по желанию): пользователь может запросить у представителя код подтверждения

На фиг. 4 изображены различные компоненты и соединения, используемые в последовательности подтверждения подлинности посредством SMS-сообщения согласно варианту осуществления данного решения:

- 15 Последовательность «Обслуживание на дому» (физическое присутствие заявителя и конечного пользователя в одном и том же помещении) может включать в себя некоторые или все из следующих операций, соответствующим образом упорядоченных, например, как показано:

1. Человек, заявляющий, что является представителем корпорации N, стучит в дверь
- 20 пользователя

2. Пользователь просит представителя подтвердить подлинность, используя наш сервис

3. Представитель использует:

- а. наше приложение виджет/портал/сервис, чтобы ввести номер телефона
- 25 пользователя и (необязательно) текстовое сообщение (например, «Это Дэн из корпорации N - Я хотел бы совершить звонок технического специалиста для обслуживания нашего оборудования») - затем эта информация:

- i. Ретранслируется в СПП через один из наших интерфейсов API, и

- ii. Сохраняется в базе данных, связанной с СПП

- 30 б. наш биометрический сканер, установленный на объекте пользователя, для сканирования сетчатки/отпечатка пальца и т.д. Биометрический сканер отправляет эту информацию на наши серверы вместе с номером телефона пользователя или другим идентификатором установки - эта информация хранится в базе данных, связанной с СПП.

- 35 4. Наш портал производит поиск номера телефона пользователя в базе данных и находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.). Эта информация основана на данных, полученных от пользователя (номер телефона, идентификатор устройства, push-токен, тип мобильной платформы, версия мобильной платформы, язык пользователя, версия клиентской
- 40 системы и т.д.) в рамках последовательности регистрации.

5. Дополнительно (по желанию): представитель получает код подтверждения от нашего приложения виджет/портал/сервис

6. Наш портал отправляет защищенное уведомление (т.е. уведомления не могут быть подделаны или отправлены какой-либо третьей стороной), например, с помощью push-токена пользователя, на устройство пользователя, содержащее:
- 45

- а. Наименование корпорации
- б. Код подтверждения из пункта №5 выше (по желанию)
- с. Имя представителя (по желанию)

- d. Текстовое сообщение, введенное представителем (по желанию)
- e. Страна, в которой зарегистрирована корпорация N (по желанию)

7. Дополнительно (по желанию): пользователь может запросить у представителя код подтверждения

5 На фиг. 5 изображены различные компоненты и соединения, используемые в последовательности подтверждения подлинности при обслуживании на дому согласно варианту осуществления данного решения:

Последовательность «Веб-сайт» может включать в себя некоторые или все из следующих операций, соответственным образом упорядоченных, например, как

10 показано:

1. Пользователь получает входящий вызов
2. Вызывающий абонент заявляет, что является представителем корпорации N
3. Пользователь просит представителя подтвердить подлинность, используя наш сервис

15 4. Представитель использует наше приложение виджет/портал/сервис, чтобы ввести номер телефона пользователя и (необязательно) текстовое сообщение (например, «Это Дэн из корпорации N - Я хотел бы совершить звонок технического специалиста для обслуживания нашего оборудования») - эта информация:

a. Ретранслируется в СПП через один из наших интерфейсов API, и

20 b. Сохраняется в базе данных, связанной с СПП

5. Пользователь переходит на сайт корпорации N, и с помощью нашего виджета на сайте вводит свой номер телефона. Эта информация ретранслируется в СПП через один из наших интерфейсов API.

6. Наш портал производит поиск номера телефона пользователя в базе данных и

25 находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.). Эта информация основана на данных, полученных от пользователя (номер телефона, идентификатор устройства, push-токен, тип мобильной платформы, версия мобильной платформы, язык пользователя, версия клиентской системы и т.д.) в рамках последовательности регистрации.

30 7. Наш портал отправляет защищенное уведомление (т.е. уведомления не могут быть подделаны или отправлены какой-либо третьей стороной), например, с помощью push-токена пользователя, на устройство пользователя, содержащее:

- a. Наименование корпорации
- b. Имя представителя (по желанию)

35 c. Текстовое сообщение, введенное представителем (по желанию)

d. Страна, в которой зарегистрирована корпорация N (по желанию)

На фиг. 6 изображены различные компоненты и соединения, используемые в последовательности подтверждения подлинности через веб-сайт согласно варианту осуществления данного решения:

40 Последовательность для автоматической отправки подтверждения подлинности (инициируется звонком корпоративного пользователя), например, в соответствии с фиг. 7:

1. Корпоративный пользователь звонит с одного из следующих номеров:

a. его мобильный телефон с поддержкой сервиса подтверждения подлинности

45 (например, мобильный телефон с одним из следующих вариантов программ, имеющих функциональную возможность подтверждения подлинности: приложение для смартфонов, комплект разработки ПО для смартфонов, компонент аппаратных средств, приложение STK, исходное приложение и т.д.).

б. добавочный номер корпоративной мини АТС с поддержкой сервиса подтверждения подлинности (АТС должна быть выполнена с возможностью работы с сервером системы подтверждения подлинности, например, с помощью запроса на предварительно настроенный URL-адрес в случае, если исходящий вызов совершается с любого из его добавочных номеров, путем установки программного плагина сервиса подтверждения подлинности и т.д.).

с. VOIP-клиент с поддержкой сервиса подтверждения подлинности (клиентская система должна быть выполнена с возможностью работы с сервером подтверждения подлинности, например, с помощью запроса на предварительно настроенный URL-адрес в случае совершения исходящего вызова).

2. Компонент сервиса подтверждения подлинности / мини АТС / VOIP-клиент отправляет на сервер системы подтверждения подлинности информацию о набранном номере телефона.

3. Затем сервер создает список реальных телефонов назначения (ADL):

а. В начальном состоянии список реального назначения (ADL) имеет вид пустого списка.

б. Если обнаруживается, что исходный номер назначения принадлежит к группе номеров корпоративной конференц-связи (например, через интеграцию с провайдером/сервером конференц-связи), то список участников этой конференции извлекается (из провайдера/сервера конференц-связи) и добавляется в ADL.

с. В ином случае исходный номер назначения добавляется в ADL без изменений.

4. После этого каждый номер в ADL проверяется сервером:

а. Сервер производит поиск номера в базе данных и находит соответствующую информацию для связи с вызываемым пользователем (тип и версия платформы, идентификатор, предпочтительный канал уведомления, поддерживаемые каналы уведомлений и т.д.).

б. Если обнаруживается, что номер телефона принадлежит корпоративному пользователю, наш портал отправляет защищенное уведомление на устройство этого пользователя со следующим содержанием:

i. Наименование корпорации

ii. Имя вызывающего абонента

iii. Для получения любой дополнительной информации, требуемой для выбранного канала уведомлений, см. раздел «Последовательность определения канала уведомлений для отправки подтверждения подлинности», описанная в данном документе.

Последовательность для проверки внутрикорпоративного входящего вызова, например, в соответствии с фиг. 8:

1. Корпоративный пользователь получает вызов на один из следующих номеров:

а. его мобильный телефон с поддержкой сервиса подтверждения подлинности (мобильный телефон с одним из следующих вариантов программ, имеющих функциональную возможность подтверждения подлинности: приложение для смартфонов, комплект разработки ПО для смартфонов, компонент аппаратных средств, приложение STK, исходное приложение и т.д.).

б. добавочный номер корпоративной мини АТС с поддержкой сервиса подтверждения подлинности (АТС должна быть выполнена с возможностью работы с сервером системы подтверждения подлинности, например, с помощью запроса на предварительно настроенный URL-адрес в случае, если входящий вызов совершается на любой из его добавочных номеров, путем установки программного плагина сервиса подтверждения подлинности и т.д.).

с. VOIP-клиент с поддержкой сервиса подтверждения подлинности (клиентская система должна быть выполнена с возможностью работы с сервером подтверждения подлинности, например, с помощью запроса на предварительно настроенный URL-адрес в случае получения входящего вызова).

5 2. Компонент сервиса подтверждения подлинности / мини АТС / VOIP-клиент отправляет на сервер системы подтверждения подлинности информацию по идентификации вызывающего абонента.

3. Затем сервер определяет достоверность заявленного идентификатора вызывающего абонента, проверяя, действительно ли вызов был выполнен с заявленного номера
10 телефона:

а. Если номер телефона закреплен за одним из пользователей сервиса подтверждения подлинности, и вызов был сделан не с него (информация, доступная через Последовательность для автоматической отправки подтверждения подлинности (инициированной описанным в данном документе вызовом, совершенным
15 корпоративным пользователем), сервер определит статус вызова как «поддельный».

б. Если номер телефона закреплен за одним из пользователей сервиса подтверждения подлинности, и вызов был сделан с него (информация, доступная через Последовательность для автоматической отправки подтверждения подлинности (инициированной описанным в данном документе вызовом, совершенным
20 корпоративным пользователем), сервер определит статус вызова как «законный».

с. Если номер телефона не закреплен ни за одним из пользователей сервиса подтверждения подлинности, то сервер определит статус вызова как «неизвестный».

4. После этого сервер сообщит статус вызова вызываемому пользователю:

а. Сервер производит поиск пользователя в базе данных и находит соответствующую
25 информацию для связи с вызываемым пользователем (тип и версия платформы, идентификатор, предпочтительный канал уведомления, поддерживаемые каналы уведомлений и т.д.).

б. Затем сервер отправляет защищенное уведомление на устройство этого пользователя со следующим содержанием:

30 i. Статус вызова (поддельный, законный или неизвестный)

ii. Если вызов является законным: Имя вызывающего абонента и принадлежность к корпорации.

iii. Для получения любой дополнительной информации, требуемой для выбранного канала уведомлений, см. раздел «Последовательность определения канала уведомлений
35 для отправки подтверждения подлинности», описанная в данном документе.

Последовательность для определения канала уведомления для использования при отправки подтверждения подлинности, например, в соответствии с фиг. 9

40 Когда от системы СПП требуется определить, какой канал уведомлений использовать для отправки подтверждения подлинности на устройство пользователя, она выполняет некоторые или все из следующих операций:

1. Если в систему интегрирована система физического контроля доступа: запускается проверка, находится ли пользователь в здании.

а. Если пользователя нет в здании: предпочтительными считаются мобильные каналы отправки уведомлений.

45 2. Если в систему интегрирован корпоративный чат-сервис: используется информация о доступности абонента этой системы

а. Если пользователь имеет статус «Недоступен» (или аналогичный статус): предпочтительными считаются мобильные каналы отправки уведомлений.

б. Если пользователь имеет статус «Не беспокоить» (или аналогичный статус): каналы отправки уведомлений на рабочий стол отклоняются.

3. Если в систему интегрирована корпоративная система календарного планирования: используется информация календаря пользователя, чтобы определить, находится ли

пользователь в настоящее время на совещании.

а. Если пользователь находится на совещании: предпочтительными считаются мобильные каналы отправки уведомлений.

4. Проверяются настройки пользователя по предпочтительному каналу уведомлений.

а. Если пользователь установил один или несколько предпочтительных каналов уведомлений, то для каждого из этих каналов:

i. Если канал отправки уведомлений еще не был отклонен предыдущими операциями - он считается предпочтительным.

ii. Если пользователь установил обязательный канал отправки уведомления, он считается предпочтительным, даже если был отклонен предыдущими операциями.

5. Выбирается канал отправки уведомлений для использования - создается список всех известных каналов уведомлений, упорядоченный в соответствии с конфигурацией конкретной организации, а затем:

а. Из списка удаляются все каналы отправки уведомлений, которые были отклонены предыдущими операциями.

б. Из списка удаляются все каналы отправки уведомлений, которые не поддерживаются для этого пользователя в соответствии с его регистрационной информацией.

с. Если во время предыдущих операций был выбран предпочтительный канал отправки уведомления, и он все еще в списке - выбирается он.

д. Если во время предыдущих операций были выбраны несколько предпочтительных каналов отправки уведомлений, и все из них все еще в списке - выбирается первый предпочтительный канал в списке.

е. В иных случаях выбирается первый канал отправки уведомлений в списке.

6. Используйте дополнительную информацию в соответствии с выбранным каналом отправки уведомлений (эта последовательность также может быть применена в отношении других описанных в данном документе последовательностей).

а. Если выбранный канал отправки уведомлений подразумевает использование персонализированной кодовой фразы (предоставляемой пользователем через клиентскую систему или ИТ-персонал корпорации):

i. Сервер использует ранее полученные пользовательские настройки и включает кодовую фразу пользователя в подтверждение подлинности.

б. Если выбранный канал отправки уведомлений подразумевает использование персонализированной фотографии (предоставляемой пользователем через клиентскую систему или ИТ-персонал корпорации):

i. Сервер использует ранее полученные пользовательские настройки и включает персонализированную фотографию пользователя в подтверждение подлинности.

с. Если для выбранного канала уведомлений требуется синхронизированный по времени одноразовый пароль:

i. Сервер извлекает одноразовый пароль с корпоративного ОТП-сервера, который, в свою очередь, включен в подтверждение подлинности.

д. Если выбранный канал отправки уведомлений подразумевает использование сформированной сервером персонализированной голосовой подписи (предоставляемой пользователем через клиентскую систему или ИТ-персонал корпорации):

i. Сервер использует ранее полученные пользовательские настройки и включает голосовую подпись пользователя в подтверждение подлинности.

e. Если выбранный канал отправки уведомлений подразумевает использование сформированной клиентской системой персонализированной голосовой подписи (предоставляемой пользователем через клиентскую систему):

i. Клиентская система сервиса подтверждения подлинности воспроизводит голосовую подпись при получении уведомления.

Возможно много технологических вариаций, например, среди прочих, различные технологии для запуска отправки подтверждения подлинности.

Например, представители могут использовать любую из следующих возможностей для отправки подтверждений подлинности пользователям:

- o наш веб-портал
- o наш виджет (с помощью технологии единого входа) на своем внутреннем сервисном портале
- o внутренний сервисный портал (через интерфейс API)
- o специальное сервисное приложение на смартфоне

Система может использовать любое из следующих запускающих событий для автоматической отправки подтверждений подлинности пользователям:

- телефонный звонок, совершенный с мобильного телефона, на котором установлено наше приложение для смартфонов, в операционных системах, поддерживающих мониторинг исходящих вызовов.

- телефонный звонок, совершенный с мобильного телефона, на котором установлено приложение с интегрированным нашим комплектом разработки ПО для смартфонов, в операционных системах, поддерживающих мониторинг исходящих вызовов.

- телефонный звонок, сделанный с мобильного телефона с SIM-картой, на которой установлено наше приложение STK, при включенном сервисе Call Control («Управление звонками»).

- телефонный звонок, сделанный с мобильного телефона, на котором установлен наш компонент аппаратных средств.

- телефонный звонок, сделанный с мобильного телефона, на котором установлено наше исходное приложение.

- телефонный звонок, сделанный с VOIP-клиента, интегрированного с нашим сервером (например, с помощью запроса на предварительно настроенный URL-адрес в случае совершения исходящего вызова).

- телефонный звонок, сделанный с добавочного номера корпоративной мини АТС, выполненной с возможностью работы с нашим сервером (например, с помощью запроса на предварительно настроенный URL-адрес в случае, если исходящий вызов совершается с добавочных номеров, путем установки программного плагина сервиса подтверждения подлинности и т.д.).

Система может использовать любое из следующих запускающих событий для проверки входящих вызовов в сторону ее пользователей:

- телефонный звонок, совершенный на мобильный телефон, на котором установлено приложение НМ для смартфонов, в операционных системах, поддерживающих мониторинг входящих вызовов.

- телефонный звонок, совершенный на мобильный телефон, на котором установлено приложение с интегрированным комплектом разработки ПО НМ для смартфонов, в операционных системах, поддерживающих мониторинг входящих вызовов,

- телефонный звонок, совершенный на мобильный телефон с SIM-картой, на которой установлено наше приложение STK, при включенном сервисе Call Control («Управление звонками»).

- телефонный звонок, совершенный на мобильный телефон, на котором установлен наш компонент аппаратных средств НМ.

- телефонный звонок, совершенный на мобильный телефон, на котором установлено наше исходное приложение.

- телефонный звонок, совершенный на VOIP-клиент, интегрированного с сервером ML (например, с помощью запроса на предварительно настроенный URL-адрес в случае совершения исходящего вызова).

- телефонный звонок, совершенный на добавочный номер корпоративной мини АТС, выполненной с возможностью работы с сервером НМ (например, с помощью запроса на предварительно настроенный URL-адрес в случае, если входящий вызов совершается на добавочные номера, путем установки программного плагина сервиса подтверждения подлинности и т.д.).

Конечные пользователи могут использовать любой из следующих сервисов для запроса подтверждения подлинности:

- наш виджет на веб-сайте корпорации
- расширение браузера
- приложение для смартфона
- приложение для смартфона с комплектом разработки ПО
- приложение STK, установленное на SIM-карте
- исходное приложение на его мобильном телефоне
- биометрический сканер, установленный на объекте пользователя

Пользователь может, например, использовать любой из следующих способов для защищенного получения подтверждения подлинности от нашего сервиса:

- приложение для смартфонов, через которое могут быть получены защищенные push-уведомления от нашего сервиса
- приложение для смартфонов с комплектом разработки ПО, через которое могут быть получены защищенные push-уведомления от нашего сервиса
- приложение STK, установленное на SIM-карте, для получения зашифрованных уведомлений от нашего сервиса
- компонент аппаратных средств на его мобильном телефоне для получения зашифрованных уведомлений от нашего сервиса
- мобильный телефон, получающий защищенную идентификацию вызывающего абонента через базовые протоколы мобильной сети (например, CNAM GSM)
- приложение для обмена мгновенными сообщениями на рабочем столе, используемое корпорацией

- SMS-сообщение с любым сочетанием следующих данных (или пустое):

- персонализированная текстовая кодовая фраза

- синхронизированный по времени одноразовый пароль

- срочное SMS-сообщение с любым сочетанием следующих данных (или пустое):

- персонализированная текстовая кодовая фраза

- синхронизированный по времени одноразовый пароль

- MMS-сообщение с любым сочетанием следующих данных (или пустое):

- персонализированная текстовая кодовая фраза

- синхронизированный по времени одноразовый пароль

- персонализированная фотография
- сообщение на пейджер с любым сочетанием следующих данных (или пустое):
- синхронизированный по времени одноразовый пароль
- персонализированная текстовая кодовая фраза
- 5 ○ приложение для смартфонов, через которое могут быть получены защищенные push-уведомления от нашего сервиса вместе с любым сочетанием следующих данных (или без них):
 - персонализированная голосовая подпись (сформированная клиентской системой или сервером)
- 10 ■ персонализированная текстовая кодовая фраза
- синхронизированный по времени одноразовый пароль
- персонализированная фотография
- приложение для смартфонов с комплектом разработки ПО, через которое могут быть получены защищенные push-уведомления от нашего сервиса вместе с любым
- 15 сочетанием следующих данных (или без них):
 - персонализированная голосовая подпись (сформированная клиентской системой или сервером)
 - персонализированная текстовая кодовая фраза
 - синхронизированный по времени одноразовый пароль
- 20 ■ персонализированная фотография
- компонент аппаратных средств на его мобильном телефоне для получения зашифрованных уведомлений от нашего сервиса вместе с любым сочетанием следующих данных (или без них):
 - персонализированная голосовая подпись (сформированная клиентской системой
 - 25 или сервером)
 - персонализированная текстовая кодовая фраза
 - синхронизированный по времени одноразовый пароль
 - персонализированная фотография
 - веб-браузер, подключенный к веб-сервису (например, Facebook), через который
 - 30 могут быть получены защищенные уведомления
 - стороннее приложение для смартфонов (например, приложение Facebook для смартфонов), через которое могут быть получены защищенные push-уведомления
- Система СПП может полагаться на несколько механизмов, чтобы определить, какой канал отправки уведомлений необходимо использовать для отправки подтверждения
- 35 подлинности пользователю, некоторыми из которых являются:
 - Корпоративный чат-сервис / Система, предоставляющая информацию о присутствии - система СПП может использовать информацию о присутствии и/или отправлять подтверждение подлинности в приложение чат-сервиса, установленное на рабочем столе пользователя, с помощью таких протоколов, как XMPP, IRC, PSYC,
 - 40 SIMPLE, другие общедоступные или проприетарные протоколы.
 - Система управления доступом (PACS/PIAM) - система СПП может использовать информацию управления доступом с помощью таких протоколов, как oBIX, Active Directory®/LDAP, другие общедоступные или проприетарные протоколы.
 - Корпоративная система календарного планирования - система СПП может
 - 45 использовать информацию календаря с помощью таких протоколов, как протокол доступа к календарю (CAP), протокол доступа к веб-календарю (WCAP), CalDAV, GroupDAV, протокол OSID для календарного планирования, другие общедоступные или проприетарные протоколы.

о Каталог предприятия - система СПП может собирать информацию о настройках пользователя с помощью таких протоколов, как Active Directory®/LDAP, другие общедоступные или проприетарные протоколы.

Последовательности на рис. 7-9 могут включать в себя все или любой подходящий комплект описанных выше операций, соответственным образом упорядоченных, например, как указано выше.

На фиг. 10 изображены компоненты и соединения, некоторые или все из которых могут использоваться в последовательностях подтверждения подлинности согласно варианту осуществления данного решения.

Выдача подтверждения подлинности

Система может выдать подтверждение подлинности организациям (частным и государственным), которые удовлетворяют требованиям, например, некоторым или всем из приведенных ниже. Как правило, в процессе верификации проверяются правосубъектность и статус заявителя. Процесс является обширным и строгим, чтобы гарантировать, что наше подтверждение подлинности будет выдаваться только заслуживающим доверия и немошенническим организациям.

Процесс подачи заявки

Организации, желающей зарегистрироваться в нашем сервисе, чтобы стать сертифицированным юридическим лицом, может быть предложено подать заявку через наш веб-сайт. Форма может потребовать внести соответствующие данные, например, некоторые или все из следующих:

1. Наименование организации
2. Организационно-правовая форма (частная организация, государственное учреждение)
3. Юрисдикция государственной регистрации
4. Регистрационный номер
5. Фактический адрес местонахождения предприятия
6. Телефон
7. Имя домена (необязательно)
8. Контактная информация
 - a. Факс
 - b. Электронная почта
 - c. Контактное лицо
9. Копия свидетельства о государственной регистрации

Заявителю может быть автоматически отправлено письмо с подтверждением и указанием, что запрос был получен и обрабатывается.

Процесс верификации

В процессе проверки система обычно не полагается на какие-либо самостоятельно введенные данные (такие как адрес и номера телефонов). Все данные, предоставленные заявителем для получения нашего подтверждения подлинности, обычно проверяются на надежность сторонних источников, например, с помощью некоторых или всех из описанных далее процессов.

Правосубъектность и статус заявителя

Необходимо убедиться, что заявитель юридически зарегистрирован, и официальное название соответствует официальным государственным записям. В тех случаях, когда используется торговое название, необходимо проверять любые альтернативные имена, отличающиеся от юридического названия заявителя в сертифицированных базах данных.

- В отношении частных организаций данная проверка осуществляется

непосредственно через регистрирующий орган в юрисдикции регистрации заявителя. Мы также проверим записи об организации в регистрирующем органе на наличие таких пометок, как «неактивная», «недействительная» и т.п.;

- В отношении государственных организаций данная проверка осуществляется непосредственно через один из следующих источников:
 - о сертифицированный правительственный источник информации политического подразделения, к которому относится эта государственная организация;
 - о высшее руководящее правительственное учреждение того же политического подразделения, к которому относится заявитель, или
 - о судья, являющийся действующим членом федеральной, государственной или местной судебной системы в пределах этого политического подразделения, или
 - о адвокат, представляющий государственную организацию.

Физическое наличие

- Необходимо перепроверить в разных источниках адрес, указанный в заявке, относительно сертифицированной государственной базы данных. Если указанный адрес не удастся проверить при обращении в правительственную базу данных, может потребоваться выезд на место для выяснения причин расхождения. От лиц, проводящих проверку, возможно, потребуется сфотографировать объект и работу предприятия или поговорить с персоналом компании.

Наличие операционной деятельности

Чтобы проверить наличие операционной деятельности заявителя необходимо:

1. Убедиться, что у заявителя есть активный текущий депозитный счет в регулируемом финансовом учреждении. При проверке, что у заявителя есть активный текущий депозитный счет в регулируемом финансовом учреждении, мы принимаем только заверенную документацию непосредственно из учреждения, проверяя; и/или
2. Также подтверждение может быть получено заверенным правовым заключением или заверенным письмом от бухгалтера о том, что у заявителя есть активный текущий депозитный счет в регулируемом финансовом учреждении.

Номер телефона

- Необходимо убедиться, что номер телефона, указанный в приложении, является основным номером телефона для запрашивающей организации. Это осуществляется посредством прямого звонка на номер и проверки списков телефонных каталогов.

Имя домена (необязательно)

- Заявитель, желающий получить подтверждение подлинности для использования с нашим виджетом на своем веб-сайте или через расширение нашего браузера, должен владеть соответствующим доменным именем или управлять им. Мы проверим записи по регистрации сайта (базу данных Whois), или мы попросим заявителя внести изменения в веб-сайт под этим доменным именем.

Авторизация физического лица

- Необходимо убедиться, что физическое лицо, подающее заявку на получение подтверждения, является законным официальным представителем заявителя. Требуется проверить личность подписывающего договор лица (в большинстве случаев это руководитель уровня C). Обычно это подтверждается документацией в письменном виде. Один из способов, с помощью которого мы можем проверить эти данные, - связаться с отделом кадров заявителя. Мы можем дополнительно потребовать личной проверки, во время которой физическое лицо должно предоставить следующую документацию:

- Личное заявление, содержащее некоторые или все из следующих сведений:

о ФИО, под которым человек известен или был известен (включая все другие используемые имена);

о Адрес фактического места жительства;

о Дата рождения; и

5 о Подтверждение, что вся информация, содержащаяся в заявке, верна.

● Действительный подписанный удостоверяющий личность документ государственного образца с фотографией лица и подписью.

10 ● По меньшей мере два дополнительных удостоверяющих личность документа с указанием имени физического лица, один из которых должен быть выдан финансовым учреждением.

После завершения проверки организации может быть предложено зарегистрировать каждого из своих представителей в системе через наш веб-портал. Для каждого представителя регистрируются, по меньшей мере, следующие данные:

15 1. ФИО - используется для отображения имени представителя для пользователя при отправке подтверждения подлинности системой СПП

2. Имя пользователя - используется представителем для входа на наш веб-портал

3. Пароль - используется представителем для входа на наш веб-портал

Интерфейс API для проверки кода

20 Ниже приведен пример интерфейса API, способного обеспечить процесс проверки кода, необходимой для последовательности регистрации.

Запросы и ответы интерфейса API передаются с помощью протокола HTTP (при необходимости, через несколько протоколов) с использованием HTTP-запросов способами GET и POST. Ответы обычно предоставляются с помощью протокола JSON.

Сервер может ответить любым из следующих кодов:

25 ● 200 OK - запрос был успешным (на некоторые вызовы интерфейса API может возвращаться код ответа 201).

● 400 Bad Request - запрос непонятен, или отсутствуют требуемые параметры.

● 403 Forbidden - запрос был понятен для сервера, но он отказался его выполнять.

Авторизация не исправит ситуацию, и запрос НЕ ДОЛЖЕН быть отправлен повторно.

30 Сервер предоставит дополнительную информацию в заголовке ответа (особенности, сопровождающие каждый соответствующий случай, при котором возможна такая ситуация).

● 404 Not Found - источник не найден.

35 ● 405 Method Not Allowed - запрашиваемый способ не поддерживается для данного источника.

● 500 Server Error - Сервер столкнулся с непредвиденной ошибкой, не позволяющей ему выполнить запрос.

Запросы, отправленные на сервер, должны включать в себя следующие заголовки HTTP:

40 ● Device-ID - Уникальный идентификатор устройства.

● Client-Version - Номер версии клиентской системы

● Client-Language - Язык, используемый клиентом

● Device-Model - Модель устройства

● Platform - Платформа устройства: iOS, Android и т.д.

45 ● Platform-Version - Версия платформы устройства

● Client-Flavor - версия/скин клиентской системы

● User-Secret - Секретный ключ, предоставленный сервером в процессе первоначальной проверки телефона. Примечание: Этот заголовок является

обязательным для всех запросов, кроме начальных проверочных запросов.

● **User-ID** - ID пользователя - в данном случае это номер мобильного абонента сети ISDN. Примечание: Этот заголовок является обязательным для всех запросов, кроме начальных проверочных запросов.

5 Интерфейс API осуществляет поддержку следующих операций:

● **Get Verification Code** - позволяет запросить новый код подтверждения для номера телефона.

○ Конечная точка запроса: `http://www.example.com/v1.0/action/code/(msisdn)/`

○ Способ: GET

10 ○ Возможные ответы сервера:

■ **200 OK** - Сервер даст пустой ответ и отправит текстовое сообщение с кодом подтверждения на указанный номер телефона. Ответ также будет содержать код, обычно 4-6 символов. Образец содержания ответа:

```

15 {
    «header»: {
        «uri»: «/v1.0/action/code/1555555555»,
        «status»: 200,
20    «code»: «ok.success»,
        «message»: «A verification code will be sent to the provided number»,
        «developerMessage»: «A verification code will be sent to the provided
25    number»,
        «moreInfo»: «mailto:support@example.com»
    },
    «payload»: {
30    «code»: {
        «length»: 4,
        «type»: «numeric»
    }
35 }
}
```

■ **400 Bad Request** - Предоставляемый ID не является действительным номером мобильного телефона. Образец содержания ответа:

40

45

```

{
  «header»: {
    «uri»: «/v1.0/action/code/1555555555»,
    «status»: 400,
    «code»: «error.parameter.illegal»,
    «message»: «The provided ID is not a valid mobile phone number»,
    «developerMessage»: «The ID is not a valid mobile phone number»,
    «moreInfo»: «mailto:support@example.com»
  },
  «payload»: null
}

```

● Confirm Verification Code - позволяет подтвердить новый код подтверждения для номера телефона.

○ Конечная точка запроса: [http://www.example.com/v1.0/action/code/\(msisdn\)/](http://www.example.com/v1.0/action/code/(msisdn)/)

○ Способ: POST

○ Параметры запроса:

■ code - Код подтверждения, предоставленный пользователем

■ push-token - Push-токен приложения

○ Образец структуры запроса:

```

{
  «code»: «12345»,
  «push-token»: «ABBC12345»
}

```

○ Возможные ответы сервера:

■ 200 OK - Сервер даст ответ (содержащий секретный ключ пользователя, который будет использоваться при следующих запросах) и отправит текстовое сообщение с кодом подтверждения на указанный номер телефона. Образец содержания ответа:

```

{

```

```

«header»: {
  «uri»: «/v1.0/action/code/1555555555»,
  «status»: 200,
  «code»: «ok.success»,
  «message»: «The provided verification code has been verified»,
  «developerMessage»: «The provided code has been verified»,
  «moreInfo»: «mailto:support@example.com»
},
«payload»: {
  «user-secret»: «ABCDEF1234567890ABCDEF123456789067890»
}

```

■ 403 Forbidden - Предоставленный код подтверждения неверен. Образец содержания ответа:

```

{
  «header»: {
    «uri»: «/v1.0/action/code/1555555555»,
    «status»: 403,
    «code»: «error.verification.wrong»,
    «message»: «The provided verification code is incorrect»,
    «developerMessage»: «The provided verification code is incorrect»,
    «moreInfo»: «mailto:support@example.com»
  },
  «payload»: null
}

```

Интерфейс API для запуска отправки подтверждения подлинности/проверки
Ниже приведен пример интерфейса API, который может осуществлять поддержку запуска отправки подтверждения подлинности клиенту представителем в соответствии с последовательностью подтверждения подлинности.

Запросы и ответы интерфейса API передаются с помощью протокола HTTP (при необходимости, через несколько протоколов) с использованием HTTP-запросов способами GET и POST. Ответы обычно предоставляются с помощью протокола JSON.

Сервер может ответить любым из следующих кодов:

- 200 OK - запрос был успешным (на некоторые вызовы интерфейса API может возвращаться код ответа 201).

- 400 Bad Request - запрос непонятен, или отсутствуют требуемые параметры.

- 403 Forbidden - запрос был понятен для сервера, но он отказался его выполнять. Авторизация не исправит ситуацию, и запрос НЕ ДОЛЖЕН быть отправлен повторно. Сервер предоставит дополнительную информацию в заголовке ответа (особенности,

сопровождающие каждый соответствующий случай, при котором возможна такая ситуация).

- 404 Not Found - источник не найден.

- 405 Method Not Allowed - запрашиваемый способ не поддерживается для данного источника.

- 500 Server Error - Сервер столкнулся с непредвиденной ошибкой, не позволяющей ему выполнить запрос.

Интерфейс API осуществляет поддержку следующих операций:

- Record Service Transaction - дает представителю возможность информировать систему СПП о сервисной транзакции с пользователем для организации представителя.

Организация представителя идентифицируется косвенным образом с помощью учетных данных представителя. Доступ к интерфейсу API ограничен пользователями, прошедшими проверку подлинности, (через наше сервисное приложение или корпоративный веб-портал с использованием единого входа) и диапазоном проверенных IP-адресов.

- Конечная точка запроса: `http://www.example.com/v1.0/action/service/{msisdn}/`

- Способ: POST

- Параметры запроса:

- `message` - Дополнительное текстовое сообщение, которое будет отправлено пользователю вместе с подтверждением подлинности

- Образец структуры запроса:

```
{
```

```
  «message»: «This is Dan from SomeCorp – I'd like to arrange a technician
```

```
  house call to service our equipment»
```

```
}
```

- Возможные ответы сервера:

- 200 OK - Сервер дополнительно предоставит код проверки и может отправить пользователю защищенное уведомление.

```
{
```

```
  «header»: {
```

```
    «uri»: «/v1.0/action/service/1555555555»,
```

```
    «status»: 200,
```

```
    «code»: «ok.success»,
```

```
    «message»: «A CoA will be sent to the provided number»,
```

```
    «developerMessage»: «A CoA will be sent to the provided number»,
```

```
    «moreInfo»: «mailto:support@example.com»
```

```
  },
```

```
  «payload»: {
```

```
    «code»: «112312»
```

```
  }
```

```
}
```

- 400 Bad Request - Предоставляемый ID не является действительным номером

мобильного телефона. Образец содержания ответа:

```
{
  «header»: {
5    «uri»: «/v1.0/action/service/1555555555»,
    «status»: 400,
    «code»: «error.parameter.illegal»,
10    «message»: «The provided ID is not a valid mobile phone number»,
    «developerMessage»: «The ID is not a valid mobile phone number»,
    «moreInfo»: «mailto:support@example.com»
  },
15  «payload»: null
}
```

- Confirm Service Transaction - Позволяет подтвердить проведение сервисной транзакции для номера телефона конкретной организации (это используется в последовательности подтверждения подлинности через веб-сайт). Организация

идентифицируется косвенным образом с помощью виджета, через который выполняется запрос (запросы выполняются через наш виджет на веб-портале организации).

- Конечная точка запроса: <http://www.example.com/v1.0/action/code/{msisdn}/>
- Способ: GET

- Возможные ответы сервера:

- 200 OK - Сервер будет предоставлено сообщение, что для данного номера телефона соответствующей организации действительно была зарегистрирована сервисная транзакция. Образец содержания ответа:

```
{
30  «header»: {
    «uri»: «/v1.0/action/code/1555555555»,
    «status»: 200,
    «code»: «ok.success»,
35    «message»: «A service transaction has been recorded for the provided
phone number 5 minutes ago»,
    «developerMessage»: «A service transaction has been recorded for the
40 provided phone number 5 minutes ago»,
    «moreInfo»: «mailto:support@example.com»
  },
  «payload»: null
45 }
```

- 400 Bad Request - Предоставляемый ID не является действительным номером мобильного телефона. Образец содержания ответа:


```

{
  «header»: {
    «uri»: «/v1.0/action/service/1555555555»,
    «status»: 400,
    «code»: «error.parameter.illegal»,
    «message»: «The provided ID is not a valid mobile phone number»,
    «developerMessage»: «The ID is not a valid mobile phone number»,
    «moreInfo»: «mailto:support@example.com»
  },
  «payload»: null
}

```

■ 404 Not Found - Для предоставленного номера телефона за последние XX минут не было зафиксировано сервисных транзакций (XX - настраиваемое значение). Образец содержания ответа:

```

{
  «header»: {
    «uri»: «/v1.0/action/service/1555555555»,
    «status»: 404,
    «code»: «error.resource.not-found»,
    «message»: «No service transaction has been recorded for the provided
phone number»,
    «developerMessage»: «No service transaction has been recorded for the
provided phone number»,
    «moreInfo»: «mailto:support@example.com»
  },
  «payload»: null
}

```

Пример процедуры интеграции, которая может выполняться интегратором, когда он/она интегрирует или регистрирует организацию x, например, при подготовке к использованию способов блок-схем 1, 2, описанной далее (следует принимать во внимание, что при регистрации каждой новой организации выполняемые операции могут меняться в зависимости от требований, определенных для этой конкретной организации). Могут выполняться некоторые или все из следующих операций:

1. Управление пользователями

а. Необходимо определить, каким образом будет осуществляться управление информацией пользователя организации, из следующих вариантов:

i. Использовать каталог организации

1. В этом случае корпоративный каталог организации используется для хранения всей необходимой информации, относящейся к пользователям (номера телефонов,

имена, предпочтительные способы уведомления, индивидуальный PIN-код и т.д.).

2. Это требует интеграции системы с корпоративным каталогом организации с доступом для чтения и записи.

ii. Использовать собственную базу данных пользователей системы СПП

5 1. В этом случае система использует свою внутреннюю базу данных для хранения всей необходимой информации, относящейся к пользователям (номера телефонов, имена, предпочтительные способы уведомления, индивидуальный PIN-код и т.д.).

2. Для этого требуется либо ручное (через веб-интерфейс командной строки системы СПП), либо пакетное предоставление (через интерфейс командной строки системы
10 СПП или веб-интерфейс) этой информации, полученной от организации.

iii. Использовать обе базы данных

1. В этом случае система использует:

15 а. Свою внутреннюю базу данных для хранения всей конфиденциальной информации, относящуюся к пользователям (предпочтительные способы уведомления, персонализированный PIN-код и т.д.).

б. Корпоративный каталог организации для хранения всей корпоративной информации, относящейся к пользователям (номера телефонов, имена и т.д.).

2. В этом случае система может быть объединена с корпоративным каталогом организации с доступом только для чтения.

20 3. Дополнительно для этого требуется либо ручное (через веб-интерфейс командной строки системы СПП), либо пакетное предоставление (через интерфейс командной строки системы СПП или веб-интерфейс) конфиденциальной информации, полученной от организации.

2. Выбор способа отправки уведомления

25 а. Необходимо определить, должна ли использоваться информация о присутствии для определения, какой способ отправки уведомления использовать. Если должна, то требуется объединить систему с сервером присутствия организации.

б. Необходимо определить, должна ли использоваться информация календаря для определения, какой способ отправки уведомления использовать. Если должна, то
30 требуется объединить систему с корпоративным сервером календарного планирования организации.

с. Необходимо определить, должна ли использоваться информация о физическом присутствии для определения, какой способ отправки уведомления использовать. Если должна, то требуется объединить систему с системой PACS организации.

35 d. Необходимо определить, какие способы отправки уведомлений должны поддерживаться:

i. Если в качестве способа отправки уведомлений должен использоваться чат-сервис, то необходимо объединить систему с системой чат-сервиса организации.

40 ii. Если в качестве способа отправки уведомлений должны использоваться push-уведомления на смартфон с помощью приложения организации для смартфона или комплект разработки ПО на смартфоне, то от организации требуется предоставить push-сертификаты для всех соответствующих платформ (APNS, GCM, т.д.) и добавить их в конфигурацию системы.

iii. Если синхронизированные по времени одноразовые пароли должны
45 использоваться как часть уведомлений, отправленных пользователям, систему необходимо объединить с сервером одноразовых паролей организации.

iv. Для всех других способов отправки уведомлений (SMS, MMS, Flash SMS и т.д.) - если для какого-то из них требуется поддержка, то ее требуется соответствующим

образом обеспечить в соответствии с системой СПП для этой организации.

3. Проверка вызова

а. Необходимо определить, следует ли извлекать информацию о вызовах из корпоративной мини АТС. Если да, то требуется объединить систему с мини АТС.

5 б. Необходимо определить, следует ли извлекать информацию о вызовах из VOIP-клиентов. Если да, то требуется объединить систему с VOIP-клиентами.

с. Необходимо определить, следует ли извлекать информацию о вызовах через корпоративное приложение для смартфона. Если да, то требуется предоставить организации комплект разработки ПО и ключ интерфейса API для этой организации в
10 системе СПП. Этот ключ интерфейса API однозначно идентифицирует запросы, отправленные на сервер системы СПП, как относящиеся к этой организации.

д. Необходимо определить, следует ли извлекать информацию о вызовах через аудиоконференцию/голосовой мост. Если да, то требуется объединить систему с сервером голосовой конференции.

15 ПРИМЕР:

Следует понимать, что конкретная реализация определенных вариантов осуществления изобретения может быть определяемой протоколом.

В следующем примере предполагается, что система СПП отправляет подтверждение подлинности в приложения чат-сервисов пользователей с помощью протокола XMPP.

20 Для других протоколов могут быть разработаны другие реализации с внесением необходимых изменений.

1. Корпоративная система чат-сервиса

Система СПП может отправлять подтверждения подлинности в приложения чат-сервисов пользователей с помощью таких протоколов, как XMPP. Для отправки
25 сообщений с помощью протокола XMPP могут выполняться некоторые или все из следующих операций.

1.1. Базовая интеграция

При начальной интеграции системы СПП определенный пользователь может быть назначен в системе СПП ответственным за связь с платформой XMPP.

30 1.2. Персональная пользовательская конфигурация

Когда в корпоративные системы добавляется новый корпоративный пользователь, системой СПП генерируется «запрос на подписку» (запрос от пользователя на авторизацию для постоянной подписки на информацию о присутствии контакта). Такие запросы будут иметь следующий вид:

35 `<presence id='xk3h1v69' to='juliet@example.com' type='subscribe'/>`

Эти заявки на подписку могут быть одобрены в одном из двух режимов:

- Перед отправкой запроса на подписку (предварительное одобрение):

- Вручную через клиентское приложение XMPP пользователя (на рабочем столе в компьютере пользователя или мобильном телефоне) с использованием предварительного
40 одобрения. Такие сообщения будут иметь следующий вид:

- `<presence id='pg81vx64' to='identity_authentication@example.com' type='subscribed'/>`

- Отправка запроса на подписку осуществляется:

- Либо автоматически с помощью сервера XMPP пользователя, если он настроен ИТ-персоналом корпорации. Такие сообщения будут иметь следующий вид:

■ `<presence from='juliet@example.com' id='xk3h1v69'
to='identity_authentication@example.com' type='subscribed'/>`

о Либо вручную через клиентское приложение XMPP пользователя (на рабочем
5 столе в компьютере пользователя или мобильном телефоне). Такие сообщения будут
иметь следующий вид:

■ `<presence id='h4v1c4kj' to='identity_authentication@example.com'
type='subscribed'/>`

1.3. Обмен данными

При возникновении необходимости отправки подтверждения подлинности
пользователю через чат-сервис система СПП инициирует сеанс «тет-а-тет» с
пользователем с атрибутом типа «заголовок» (чтобы указать, что сообщение содержит
предупреждение/уведомление, на которое не требуется давать ответ), отправив
15 сообщение формы:

`<message from='identity_authentication@example.com' id='b4vs9km4'
to='romeo@example.net' type='headline' xml:lang='en'>
20 <body>Warning: fake caller!</body>
</message>`

2. Пример корпоративной системы информирования о присутствии

Система СПП может использовать информацию о присутствии с помощью таких
протоколов, как XMPP. Для сбора информации о присутствии с помощью протокола
25 XMPP могут выполняться некоторые или все из следующих операций.

2.1. Базовая интеграция

При начальной интеграции системы СПП определенный пользователь может быть
назначен в системе СПП ответственным за связь с платформой XMPP.

2.2. Персональная пользовательская конфигурация

30 Когда в корпоративные системы добавляется новый корпоративный пользователь,
системой СПП генерируется «запрос на подписку» (запрос от пользователя на
авторизацию для постоянной подписки на информацию о присутствии контакта). Это
позволит системе СПП получить информацию о присутствии для пользователя. Такие
запросы будут иметь следующий вид:

35 `<presence id='xk3h1v69' to='juliet@example.com' type='subscribe'/>`

Эти заявки на подписку могут быть одобрены в одном из двух режимов:

● Перед отправкой запроса на подписку (предварительное одобрение)

о Вручную через клиентское приложение XMPP пользователя (на рабочем столе в
40 компьютере пользователя или мобильном телефоне) с использованием предварительного
одобрения. Такие сообщения будут иметь следующий вид:

■ `<presence id='pg81vx64' to='identity_authentication@example.com'
type='subscribed'/>`

● Отправка запроса на подписку осуществляется

о Либо автоматически с помощью сервера XMPP пользователя, если он настроен
ИТ-персоналом корпорации. Такие сообщения будут иметь следующий вид:

■ `<presence from='juliet@example.com' id='xk3h1v69'
to='identity_authentication@example.com' type='subscribed'/>`

о Либо вручную через клиентское приложение XMPP пользователя (на рабочем
столе в компьютере пользователя или мобильном телефоне). Такие сообщения будут
иметь следующий вид:

■ `<presence id='h4v1c4kj' to='identity_authentication@example.com'
type='subscribed'/>`

2.3. Обмен данными

При возникновении необходимости получения информации о присутствии
пользователя, система СПП генерирует запрос на проверку присутствия, например,
следующего вида:

`<presence from='identity_authentication@example.com' id='ign291v5'
to='romeo@example.net' type='probe'/>`

Информация о присутствии затем возвращается в систему СПП - такая информация
может иметь следующий вид:

`<presence from='romeo@example.net/bar' id='ps6t1fu3'
to='identity_authentication@example.com'>
<show>away</show>
</presence>`

3. Система управления доступом (PACS/PIAM)

Система СПП может использовать информацию Системы управления доступом для
определения, находится ли пользователь в настоящее время в помещении или нет. Для
сбора такой информации с помощью протокола LDAP могут выполняться операции,
описанные в разделе «Корпоративный каталог».

4. Корпоративная система календарного планирования

Система СПП может использовать информацию календаря с помощью таких
протоколов, как CalDAV. Обычно это делается для того, чтобы определить, занят
пользователь (находится на совещании) или нет. Для сбора такой информации с
помощью протокола CalDAV могут выполняться некоторые или все из следующих
операций.

4.1. Базовая интеграция

При начальной интеграции системы СПП определенный пользователь может быть
назначен в системе СПП ответственным за связь с сервером календарного планирования.
CALDAV: привилегия предоставления данных типа «читает-свободен-занят» должна
обеспечиваться при просмотре сборников календарей, регулярного календарного
планирования и ресурсов объектов календаря.

4.2. Персональная пользовательская конфигурация

Для того чтобы система СПП могла получить доступ к верной информации
календарного планирования для пользователя, может быть применен один из нескольких
подходов:

1. Сервер календарного планирования может быть выполнен с возможностью
использования множества псевдонимов URL-адресов для каждого ресурса, совместимого
с CalDAV. В частности, если информация календаря пользователя обычно доступна

через корпоративный электронный адрес пользователя (например, /bernard@corp.com/work/) или другой корпоративный идентификатор (например, /bernard11/work/), сервер может быть выполнен с возможностью получения доступа к тому же ресурсу по номеру телефона пользователя (например, /1555555555/work/).

2. Система СПП может быть совмещена с корпоративным каталогом (например, с помощью протокола LDAP), чтобы получить URL-адрес или идентификатор, с помощью которого можно получить информацию календаря пользователя. См. раздел «Корпоративный каталог» для получения сведений об операциях по объединению с корпоративным каталогом.

4.3. Обмен данными

Если возникает потребность в получении информации о занятости пользователя, система СПП генерирует отчет о занятости для запроса по текущей временной метке, например:

REPORT /bernard/work/ HTTP/1.1

Host: cal.example.com

Depth: 1

Content-Type: application/xml; charset="utf-8"

Content-Length: 184

<?xml version="1.0" encoding="utf-8" ?>

<C:free-busy-query xmlns:C="urn:ietf:params:xml:ns:caldav">

<C:time-range start="20150104T140000Z"

end="20150104T140100Z"/>

</C:free-busy-query>

Информация о занятости затем возвращается в систему СПП - такая информация может иметь следующий вид:

HTTP/1.1 200 OK

Дата: Sat, 11 Nov 2006 09:32:12 GMT

Content-Type: text/calendar

Content-Length: 231

BEGIN:VCALENDAR

VERSION:2.0

PRODID:-//Example Corp.//CalDAV Server//EN

BEGIN:VFREEBUSY

DTSTAMP:20150103T110000Z

DTSTART:20150104T140000Z

DTEND:20150104T140100Z

FREEBUSY;FBTYPE=BUSY:20150104T140000Z/PT1H

END:VFREEBUSY

END:VCALENDAR

5

5. Корпоративный каталог

Система СПП может извлекать пользовательские настройки и информацию из корпоративного каталога с помощью таких протоколов, как LDAP. Для сбора такой информации с помощью протокола LDAP могут выполняться некоторые или все из

10

5.1. Базовая интеграция

При начальной интеграции системы СПП определенный пользователь может быть назначен в системе СПП ответственным за связь с корпоративным каталогом. Кроме того, корпоративным ИТ-отделом могут быть предоставлены определенные параметры (например, базовое имя домена, имена атрибутов конкретной схемы LDAP), чтобы

15

система СПП могла найти информацию о пользователе в корпоративном каталоге.

5.2. Персональная пользовательская конфигурация

Пользователь системы СПП должен иметь, по меньшей мере, доступ для чтения к информации всех корпоративных пользователей, для которых должен быть активирован

20

5.3. Обмен данными

Если возникает потребность в получении информации пользователя, система СПП запрашивает эту информацию из корпоративного каталога с помощью протокола LDAP, используя некоторые или все из следующих операций:

25

1. Инициализация сеанса (например, с помощью *ldap_init()*) - Устанавливает параметры настройки сеанса по умолчанию в структуре LDAP. Состояние сеанса LDAP сохраняется в структуре LDAP. С параметрами сеанса можно ознакомиться или установить их до привязки.

30

2. Соединение с сервером (например, с помощью *ldap_connect()*) - Устанавливает соединение по протоколу LDAP с сервером LDAP.

3. Привязка к серверу (например, с помощью *ldap_simple_bind_s()*) - Сервер LDAP подтверждает подлинность клиента.

35

4. Поиск каталога для требуемого пользователя (например, с помощью *ldap_search_ext_s()*). Обычно эта операция выполняется с использованием некоторых или всех следующих параметров поиска:

a. base: базовое имя домена, предоставленное корпоративным ИТ-отделом. Обычно имеет следующий вид:

dn="dc=example;dc=com"

40

b. scope:

LDAP_SCOPE_SUBTREE

c. filter: в зависимости от конкретной схемы, используемой корпоративным ИТ-отделом. Несколько общих примеров:

45

(mobile=+1-5555555555)

(ipPhone=+15555555556)

5

(telephoneNumber=+15555555557)

d. attrs: обычно должны возвращаться все атрибуты, которые были образованы с использованием значения:

10

ЦNULL

5. Закрытие соединения с сервером LDAP по завершении (например, с помощью *ldap_unbind()*).

15

Информация, возвращаемая сервером, может содержать несколько атрибутов, которые могут использоваться системой СПП при выполнении своей роли. Несколько примеров:

- Идентификаторы

- employeeID - идентификатор сотрудника, который может использоваться для доступа к другим источникам информации (например, к системе управления доступом).

20

- Name attributes - Атрибуты имени - могут использоваться при отправке подтверждения подлинности пользователям для идентификации вызывающей стороны.

- givenName

- cn

- displayName

25

- name

- Logon/Logoff times - Время входа в систему/выхода из системы - может использоваться для определения того, находится ли пользователь по-прежнему на работе:

- lastLogoff

30

- lastLogon

- lastLogonTimestamp

- Custom attributes - Пользовательские атрибуты

- Public calendar URL - URL-адрес открытого календаря - будет использоваться для доступа к календарю пользователя

35

- IM identifier - идентификатор в чат-сервисе - идентификатор пользователя на корпоративной платформе чат-сервиса

- Last entry/exit - Последний вход в систему/выход из системы - может использоваться для определения того, находится ли пользователь в помещении. Такие атрибуты будут установлены корпоративной системой управления доступом.

40

6. Корпоративная мини АТС

Система СПП может обнаруживать исходящий или входящий вызов в системе корпоративной мини АТС. Это осуществляется путем интеграции двух платформ.

Например, интеграция с системой Cisco Unified Call Manager (CUCM) для этой цели может быть выполнена с помощью протокола JTAPI.

45

При использовании протокола JTAPI система СПП служит клиентской системой JTAPI, а система CUCM действует как сервер JTAPI. В этой схеме интеграции система СПП отслеживает события и при обнаружении исходящего вызова отправляет уведомление вызываемому абоненту в соответствии со стандартной последовательностью отправки уведомлений системы

СПП.

6.1. Базовая интеграция

Пользователь приложения может быть создан в системе CUCM с доступом к интерфейсу СТИ. Затем система СПП регистрирует как слушатель все события интерфейса

6.2. Персональная пользовательская конфигурация

Пользователю приложения может быть предоставлен доступ ко всем добавочным номерам, которые необходимо отслеживать.

6.3. Обмен данными

1. Если с использованием протокола JTAPI происходит событие, система СПП проверяет, является ли событие входящим или исходящим вызовом с помощью, например, интерфейса `CallControlConnection.getCallControlState()`. Следующие состояние, некоторые или все из которых возвращены с помощью указанного способа, могут использоваться системой СПП для определения статуса соответствующих вызовов:

- `CallControlConnection.OFFERED` - Это состояние указывает, что по адресу, связанному с соединением, предлагается принять входящий вызов.
- `CallControlConnection.NETWORK_REACHED` - Это состояние указывает, что исходящий телефонный звонок достиг сети.

2. При обнаружении вызова система СПП получит некоторые или все из следующих сведений через интерфейс `CallControlCall`. Затем эта информация используется для определения достоверности вызова:

- Адрес вызова, возвращенный с помощью способа `CallControlCall.getCallingAddress()`, - это адрес, с которого изначально был отправлен вызов.

- Терминал вызова, возвращенный с помощью способа

`CallControlCall.getCallingTerminal()`, - это терминал, с которого изначально был отправлен вызов.

- Адрес приема вызова, возвращенный с помощью способа `CallControlCall.getCalledAddress()`, - это адрес, на который изначально был отправлен вызов.

- Последний перенаправленный адрес, возвращенный с помощью способа `CallControlCall.getLastRedirectedAddress()`, - это адрес, на который был отправлен вызов перед перенаправлением на текущий адрес. Например, если вызов был перенаправлен с одного адреса на другой, то первым адресом является последний перенаправленный адрес этого вызова.

3. Если вызов может быть разъединен, система СПП выполнит через интерфейс `CallControlCall` следующую операцию:

- `CallControlCall.drop()` - сброс вызова.

Любые или все из компьютеризированных датчиков, устройств или дисплеев вывода, процессоров, устройств хранения данных и сетей могут использоваться, при необходимости, для реализации любого из способов и аппаратов, приведенных и описанных в данном документе.

Следует понимать, что некоторая терминология, например, термины «обязательный», «требуемый», «нуждается» и «должен», относится к выборам вариантов реализации, сделанным в контексте конкретной реализации или приложения, описанных в данном документе для ясности, и не предназначена для ограничения, поскольку в альтернативных вариантах те же элементы могут быть определены как не обязательные и не требуемые или даже могут быть полностью исключены.

Компоненты, описанные в данном документе как программное обеспечение, могут,

в соответствии с другим вариантом осуществления изобретения, быть, при необходимости, реализованы целиком или частично в аппаратных средствах и/или прошивке с использованием обычных технологий, и наоборот. Каждый модуль или компонент или процессор могут быть сосредоточены в одном физическом местоположении или устройстве или распределены по нескольким физическим местоположениям или устройствам.

В объем настоящего раскрытия, без ограничений, входят электромагнитные сигналы в соответствии с описанием, приведенном в настоящем документе. Они могут содержать машиночитаемые инструкции для выполнения любых или всех операций любого из способов, показанных и описанных в данном документе, в любом подходящем порядке, включая одновременное выполнение подходящих групп операций, при необходимости; машиночитаемые инструкции для выполнения любых или всех операций любого из способов, показанных и описанных в данном документе, в любом подходящем порядке; программные машиночитаемые накопительные устройства, практически воплощающие программу инструкций, исполняемых машиной, для выполнения любых или всех операций любого из способов, показанных и описанных здесь, в любом подходящем порядке; компьютерный программный продукт, содержащий пригодный для использования компьютером носитель, имеющий машиночитаемый программный код, такой как исполняемый код, воплощенный в данном случае, и/или содержащий машиночитаемый программный код для выполнения, любые или все операции любого из способов, показанных и описанных в данном документе, в любом подходящем порядке; любые технические эффекты, вызванные любой или всеми операциями любого из способов, показанных и описанных в данном документе, при выполнении в любом подходящем порядке; любой подходящий аппарат или устройство или их сочетание, запрограммированные на выполнение, отдельно или в сочетании, любых или всех операций любого из способов, показанных и описанных в данном документе, в любом подходящем порядке; электронные устройства, каждый из которых включает в себя, по меньшей мере, один процессор и/или взаимодействующее устройство ввода и/или устройство вывода, и может выполнять, например, в программном обеспечении, любые операции, показанные и описанные в данном документе; устройства хранения информации или физические записи, такие как диски или жесткие диски, вынуждая выполнять, по меньшей мере, один компьютер или другое устройство с возможностью выполнения любых или всех операций любого из способов, показанных и описанных в данном документе, в любом подходящем порядке; по меньшей мере, одну предварительно сохраненную программу, например, в накопителе или в информационной сети, такой как Интернет, до или после загрузки, которая воплощает любую или все операции любого из способов, показанных и описанных в данном документе, в любом подходящем порядке, и способ удаления или загрузки таких программ, и систему, включающую сервер(а) и/или клиентскую систему(-ы) для использования таких программ; по меньшей мере, один процессор с возможностью выполнения любого сочетания описанных операций или реализации любого сочетания описанных модулей; и аппаратное обеспечение, которое выполняет любую или все операции любого из способов, показанных и описанных в данном документе, в любом подходящем порядке, либо самостоятельное, либо в сочетании с программным обеспечением. Любые машиночитаемые носители, описанные в данном документе, включают в себя непереходные машиночитаемые носители.

Любые вычисления или другие формы анализа, описанные в данном документе, могут выполняться с помощью подходящего компьютеризованного способа. Любая

операция или функциональная возможность, описанные в данном документе, могут быть полностью или частично реализованы на базе компьютера, например, одним или несколькими процессорами. Изобретение, показанное и описанное в данном документе, может включать в себя (а) использование компьютеризованного способа для

5 идентификации решения любой из задач или для любой из целей, описанных в данном документе, решение может дополнительно включать в себя, по меньшей мере, что-то одно из следующего списка: решение, действие, продукт, услугу или любую другую информацию, описанную в данном документе, которая позитивно влияет на проблему или цели, описанные в данном документе; и (b) вывод решения.

10 При необходимости система может быть реализована как веб-система с использованием программного обеспечения, компьютеров, маршрутизаторов и телекоммуникационного оборудования.

Для обеспечения функциональности может быть использовано любое подходящее развертывание, например, программные функции, показанные и описанные в данном

15 документе. Например, сервер может хранить определенные приложения для загрузки в клиентскую систему, выполняемой на стороне клиентской системы, а серверная сторона обслуживает только хранилище. Некоторые или все функциональные возможности, например, функциональные возможности программного обеспечения, показанные и описанные в данном документе, могут быть развернуты в облачной

20 среде. Клиентские системы, например, устройства мобильной связи, такие как смартфоны, могут быть оперативно связаны с внешними облаками.

Объем настоящего изобретения не ограничивается структурами и функциями, в частности, описанными здесь, а также предназначен для включения в себя устройств, которые могут создавать структуру или выполнять описанную в данном документе

25 функцию, так что даже без задействования пользователями устройства его емкости они могут, при желании, изменить устройство для того, чтобы получить определенную структуру или функцию.

Свойства настоящего изобретения, включая операции, которые описаны в контексте отдельных вариантов осуществления изобретения, также могут быть представлены в

30 сочетании в одном варианте осуществления изобретения. Например, вариант осуществления системы подразумевает включение в себя соответствующего варианта осуществления процесса, и наоборот. Кроме того, каждый вариант осуществления системы включает в себя «вид» с централизацией относительно сервера или «вид» с централизацией относительно клиентской системы или «вид» со стороны любого другого

35 узла системы, всех функциональных возможностей системы, машиночитаемого носителя, аппаратуры, включая только те функции, которые выполняются в этом сервере, клиентской системе или узле. Свойства также могут быть объединены со свойствами, известными в данной области техники, и, без ограничений, с теми, что описаны в разделе «Уровень техники» или в публикациях, упомянутых в данном документе.

40 И наоборот, свойства изобретения, включая операции, которые описаны для краткости в контексте одного варианта осуществления или в определенном порядке, могут быть предоставлены отдельно или в любом подходящем сочетании, в том числе со свойствами, известными в данной области (без ограничений, с теми, что описаны в разделе «Уровень техники» или в упомянутых в данном документе публикациях) или

45 в другом порядке. Термин «например» используется в данном документе в смысле конкретного примера, не направленного на ограничение. Каждый способ может содержать некоторые или все проиллюстрированные или описанные операции, соответственным образом упорядоченные, например, так, как проиллюстрировано

или описано в данном документе.

Устройства, аппараты или системы, показанные на каком-либо из чертежей как взаимосвязанные, могут фактически быть интегрированы в одну платформу в определенных вариантах осуществления изобретения или могут быть связаны
 5 посредством любой соответствующей проводной или беспроводной связи, такой как, без ограничений, оптическое волокно, Ethernet, беспроводная локальная сеть, HomePNA, связь по электросети, сотовый телефон, смартфон (например, iPhone), планшет, ноутбук, КПК, Blackberry GPRS, спутник, включая GPS или другое мобильное устройство. Следует понимать, что в описании и чертежах, показанных и описанных в данном документе,
 10 функциональные возможности, описанные или проиллюстрированные как системы и их подблоки, также могут быть предоставлены как способы и операции с ними, а функциональные возможности, описанные или проиллюстрированные как способы и операции с ними, могут также предоставляться как системы и их подблоки. Шкала, используемая для иллюстрации различных элементов на чертежах, является примерной
 15 и/или подходящей для достижения ясности представления и не имеет целью ввод каких-либо ограничений.

(57) Формула изобретения

1. Система подтверждения подлинности утверждения о принадлежности к
 20 организации, содержащая следующие элементы:
 - базу данных организаций;
 - сервер/процессор, способный обеспечить доступ к базе данных; а также канал связи с конечными пользователями, позволяющий конечным пользователям получать от процессора подтверждение подлинности утверждения о принадлежности к какой-либо
 25 организации, в которой утверждение о принадлежности к какой-либо организации предъявляется заявителем, который предоставляет номер мобильного телефона и push-токен конечного пользователя в сервис подтверждения подлинности (СПП), а в ответ система СПП отправляет пользователю защищенное сообщение, действительно ли представитель связан с заявленной организацией, причем телефонный номер
 30 предоставляется через портал организации, который связывается с системой СПП через интерфейс API, а защищенное сообщение представляет собой push-уведомление.

2. Система по п. 1, в которой процессор подтверждает подлинность абонентского номера, связанного с конечным пользователем, в ответ на прием упомянутого абонентского номера от признанного законным представителя организации в
 35 упомянутой базе данных организаций.

3. Система по п. 1, в которой утверждение о принадлежности к какой-либо организации осуществляется посредством: телефонного звонка, личного посещения или текстового сообщения.

4. Система по п. 1, в которой телефонный номер предоставляется по меньшей мере
 40 одним из следующих способов:

- 1) специальный сервисный портал
- 2) специальное приложение для смартфона.

5. Система по п. 1, в которой обеспечивается последовательность, включающая в себя, по меньшей мере, некоторые из следующих операций:

- 45 1) Пользователь устанавливает приложение на свой телефон
- 2) Пользователь запускает приложение на своем телефоне
- 3) Приложение просит пользователя ввести свой номер телефона
- 4) Пользователь вводит номер телефона

5) Приложение отправляет запрос на сервер для проверки номера телефона
 6) Сервер отправляет текстовое сообщение с кодом подтверждения на указанный номер телефона

7) Пользователь вводит код из текстового сообщения в приложение

5 8) Приложение отправляет код обратно на сервер, который определяет, действителен ли он

9) Сервер оперативно записывает данные для пользователя.

6. Система по п. 5, в которой упомянутые данные содержат любое подмножество или все из следующих сведений:

- 10 a. Номер телефона
 b. Идентификатор устройства
 c. Push-токен
 d. Тип мобильной платформы
 e. Версия мобильной платформы

- 15 f. Язык пользователя
 g. Версия клиентской системы.

7. Система по п. 1, в которой обеспечивается последовательность, включающая в себя, по меньшей мере, некоторые из следующих операций:

1) Пользователь устанавливает приложение корпорации, включающее в себя комплект
 20 разработки ПО, на свой телефон

2) Пользователь запускает приложение на своем телефоне

3) Приложение просит пользователя ввести свой номер телефона

4) Пользователь вводит номер телефона

5) Приложение отправляет запрос на сервер через комплект разработки ПО для
 25 проверки номера телефона

6) Сервер отправляет текстовое сообщение с кодом подтверждения на указанный номер телефона

7) Пользователь вводит код из текстового сообщения в приложение

8) Приложение отправляет код обратно через комплект разработки ПО на сервер,
 30 который определяет, действителен ли он

9) Затем сервер оперативно записывает данные для пользователя.

8. Система по п. 7, в которой данные, характеризующие пользователя, включают в себя все или любое подмножество следующих сведений:

- 35 a. Номер телефона
 b. Идентификатор устройства
 c. Push-токен
 d. Тип мобильной платформы
 e. Версия мобильной платформы
 f. Язык пользователя

- 40 g. Версия клиентской системы.

9. Система по п. 1, в которой обеспечивается последовательность, включающая в себя, по меньшей мере, некоторые из следующих операций:

1) Пользователь добавляет специальное приложение Facebook к своей учетной записи Facebook

45 2) Пользователь запускает приложение Facebook

3) Приложение просит пользователя ввести свой номер телефона

4) Пользователь вводит номер телефона

5) Приложение отправляет запрос на сервер для проверки номера телефона (при

необходимости, через защищенное соединение). Происходит оперативная проверка, например, в соответствии с некоторыми или всеми операциями 6-9, приведенными ниже

б) Сервер отправляет текстовое сообщение с кодом подтверждения на указанный номер телефона

7) Пользователь вводит код из текстового сообщения в приложение Facebook

8) Приложение отправляет код обратно на сервер (при необходимости, через защищенное соединение), который определяет, действителен ли он, и отправляет в приложение соответствующий ответ

9) Затем сервер оперативно записывает данные для пользователя.

10. Система по п. 9, в которой данные, характеризующие пользователя, включают в себя все или любое подмножество следующих сведений:

a. Номер телефона

b. Идентификатор пользователя в Facebook

c. Язык пользователя

d. Версия приложения.

11. Система, в которой обеспечивается последовательность подтверждения подлинности при помощи системы по п. 1.

12. Система по п. 11, в которой последовательность подтверждения подлинности включает в себя, по меньшей мере, некоторые из следующих операций для случая телефонного вызова с утверждением о принадлежности к какой-либо организации:

1) Пользователь получает входящий вызов

2) Вызывающий абонент заявляет, что является представителем корпорации N

3) Пользователь просит представителя подтвердить подлинность, используя наш сервис

4) Представитель использует наше приложение виджет/портал/сервис, чтобы ввести номер телефона пользователя и (при желании) текстовое сообщение

5) Наш портал производит поиск номера телефона пользователя в базе данных и находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.)

6) Дополнительно (по желанию): представитель получает код подтверждения от нашего приложения виджет/портал/сервис

7) Наш портал отправляет защищенное уведомление на устройство пользователя со следующим содержанием:

a. Наименование корпорации

b. Код подтверждения из пункта №6 выше (по желанию)

c. Имя представителя (по желанию)

d. Текстовое сообщение, введенное представителем (по желанию)

e. Страна, в которой зарегистрирована корпорация N (по желанию)

8) Дополнительно (по желанию): пользователь может запросить у представителя код подтверждения.

13. Система по п. 11, в которой последовательность подтверждения подлинности включает в себя, по меньшей мере, некоторые из следующих операций для случая SMS-сообщения с утверждением о принадлежности к какой-либо организации:

1) Пользователь получает текстовое сообщение якобы от представителя корпорации N

2) Пользователь просит представителя подтвердить подлинность, используя наш сервис

3) Представитель использует наше приложение виджет/портал/сервис, чтобы ввести

номер телефона пользователя и (при желании) текстовое сообщение

4) Наш портал производит поиск номера телефона пользователя в базе данных и находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.)

5) Дополнительно (по желанию): представитель получает код подтверждения от нашего приложения виджет/портал/сервис

6) Наш портал отправляет защищенное уведомление на устройство пользователя со следующим содержанием:

а. Наименование корпорации

10 б. Код подтверждения из пункта №5 выше (по желанию)

с. Имя представителя (по желанию)

д. Текстовое сообщение, введенное представителем (по желанию)

е. Страна, в которой зарегистрирована корпорация N (по желанию)

15 7) Дополнительно (по желанию): пользователь может запросить у представителя код подтверждения.

14. Система по п. 11, в которой последовательность подтверждения подлинности включает в себя, по меньшей мере, некоторые из следующих операций для случая личного общения с утверждением о принадлежности к какой-либо организации:

20 1) Человек, заявляющий, что является представителем корпорации N, стучит в дверь пользователя

2) Пользователь просит представителя подтвердить подлинность, используя наш сервис

3) Представитель использует:

25 а. Наше приложение виджет/портал/сервис, чтобы ввести номер телефона пользователя и (при желании) текстовое сообщение

б. Наш биометрический сканер, установленный на объекте пользователя, для сканирования сетчатки/отпечатка пальца и т.д. Биометрический сканер отправляет эту информацию на наши серверы вместе с номером телефона пользователя или другим идентификатором установки

30 4) Наш портал производит поиск номера телефона пользователя в базе данных и находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.)

5) Дополнительно (по желанию): представитель получает код подтверждения от нашего приложения виджет/портал/сервис

35 6) Наш портал отправляет защищенное уведомление на устройство пользователя со следующим содержанием:

а. Наименование корпорации

б. Код подтверждения из пункта №5 выше (по желанию)

с. Имя представителя (по желанию)

40 д. Текстовое сообщение, введенное представителем (по желанию)

е. Страна, в которой зарегистрирована корпорация N (по желанию)

7) Дополнительно (по желанию): пользователь может запросить у представителя код подтверждения.

45 15. Система по п. 11, в которой поток подтверждения подлинности позволяет пользователю предоставлять свои контактные данные непосредственно, а не через заявителя.

16. Система по п. 12, в которой последовательность подтверждения подлинности включает в себя, по меньшей мере, некоторые из следующих операций:

- 1) Пользователь получает входящий вызов
- 2) Вызывающий абонент заявляет, что является представителем корпорации N
- 3) Пользователь просит представителя подтвердить подлинность, используя наш сервис

5 4) Представитель использует наше приложение виджет/портал/сервис, чтобы ввести номер телефона пользователя и (при желании) текстовое сообщение

5) Пользователь переходит на сайт корпорации N, и с помощью нашего виджета на сайте вводит свой номер телефона

6) Наш портал производит поиск номера телефона пользователя в базе данных и
10 находит соответствующую информацию для связи с пользователем (тип и версия платформы, идентификатор и т.д.)

7) Наш портал отправляет защищенное уведомление на устройство пользователя со следующим содержанием:

- a. Наименование корпорации
- 15 b. Имя представителя (по желанию)
- c. Текстовое сообщение, введенное представителем (по желанию)
- d. Страна, в которой зарегистрирована корпорация N (по желанию).

17. Система по п. 11, в которой заявитель использует по меньшей мере один из следующих способов для отправки подтверждения подлинности пользователям:

- 20 ☐ специальный веб-портал
- ☐ специальный виджет на своем внутреннем сервисном портале
- ☐ внутренний сервисный портал
- ☐ специальное сервисное приложение на смартфоне.

18. Система по п. 11, в которой заявитель использует по меньшей мере один из
25 следующих способов, чтобы запросить подтверждение подлинности:

- ☐ специальный виджет на веб-сайте корпорации
- ☐ расширение браузера
- ☐ приложение для смартфона
- ☐ приложение для смартфона с комплектом разработки ПО
- 30 ☐ приложение STK, установленное на SIM-карте
- ☐ исходное приложение на его мобильном телефоне
- ☐ биометрический сканер, установленный на объекте пользователя.

19. Система по п. 18, в которой конечный пользователь использует по меньшей мере один из следующих способов для получения подтверждения подлинности со
35 специального сервиса:

- ☐ приложение для смартфонов, через которое могут быть получены защищенные push-уведомления от нашего сервиса
- ☐ приложение для смартфонов с комплектом разработки ПО, через которое могут быть получены защищенные push-уведомления от нашего сервиса
- 40 ☐ приложение STK, установленное на SIM-карте, для получения зашифрованных уведомлений от нашего сервиса
- ☐ компонент аппаратных средств на его мобильном телефоне для получения зашифрованных уведомлений от нашего сервиса
- ☐ мобильный телефон, получающий защищенную идентификацию вызывающего
45 абонента через базовые протоколы мобильной сети
- ☐ веб-браузер, подключенный к веб-сервису (например, Facebook), через который могут быть получены защищенные уведомления
- ☐ стороннее приложение для смартфонов (например, приложение Facebook для

смартфонов), через которое могут быть получены защищенные push-уведомления.

20. Система, предназначенная для осуществления мониторинга связи и выявления мошенников tx, притворяющихся, что связываются с конечным пользователем gx по телефонной линии, связанной с организацией, к которой мошенник tx не имеет

5 отношения, с использованием системы по п. 11.

21. Система по п. 20, в которой связь является телефонной связью.

22. Система по п. 20, которая информирует каждого конечного пользователя gx в реальном времени обо всех случаях, при которых зарегистрированная телефонная линия в зарегистрированной организации направляла вызов на gx.

10 23. Система по п. 20, в которой упомянутое выявление происходит в реальном времени.

24. Система по п. 20, которая отслеживает входящие вызовы в сторону каждого конечного пользователя gx, включая идентификацию телефонной линии, из которой якобы возник каждый входящий вызов, и если телефонная линия, из которой каждый

15 входящий вызов якобы возник, является зарегистрированной телефонной линией в зарегистрированной организации, предупреждает gx, если телефонная линия, из которой был направлен входящий вызов, на самом деле не являлась gx.

25. По меньшей мере один процессор, выполненный с возможностью выполнения по меньшей мере одной из или любого сочетания описанных операций или для

20 выполнения любого сочетания описанных модулей.

26. Способ, предназначенный для осуществления мониторинга связи и выявления мошенников tx, притворяющихся, что связываются с конечным пользователем gx по телефонной линии, связанной с организацией, к которой мошенник tx не имеет отношения, в котором используют систему по п. 20 и процессор по п. 25.

25 27. Способ по п. 26 подтверждения подлинности утверждения о принадлежности к какой-либо организации, содержащий следующие элементы:

Предоставление базы данных организаций;

Использование сервера/процессора, способного обеспечить доступ к базе данных; а также

30 Канал связи с конечными пользователями, позволяющий конечным пользователям получать от процессора подтверждение подлинности утверждения о принадлежности к какой-либо организации.

28. Машиночитаемый носитель, содержащий машиночитаемый программный код, который при его исполнении реализует способ по п. 26, предназначенный для

35 мониторинга связи и идентификации мошенников tx, которые притворяются, чтобы связаться с конечным пользователем gx с телефонной линии, связанной с организацией, из которой мошенник tx на самом деле вовсе не звонит.

29. Машиночитаемый носитель по п. 28, содержащий машиночитаемый программный код, который при его исполнении осуществляет способ подтверждения подлинности

40 утверждения о принадлежности к какой-либо организации, включающий:

Предоставление базы данных организаций;

Использование сервера/процессора, способного обеспечить доступ к базе данных; а также

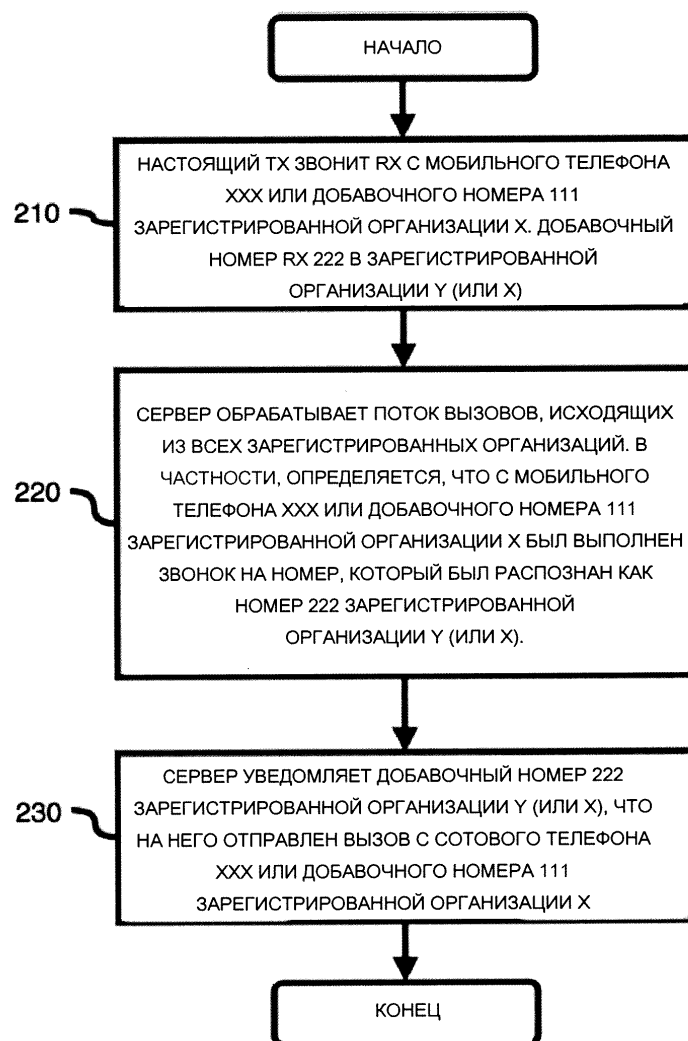
Канал связи с конечными пользователями, позволяющий конечным пользователям

45 получать от процессора подтверждение подлинности утверждения о принадлежности к какой-либо организации.

1

1/14

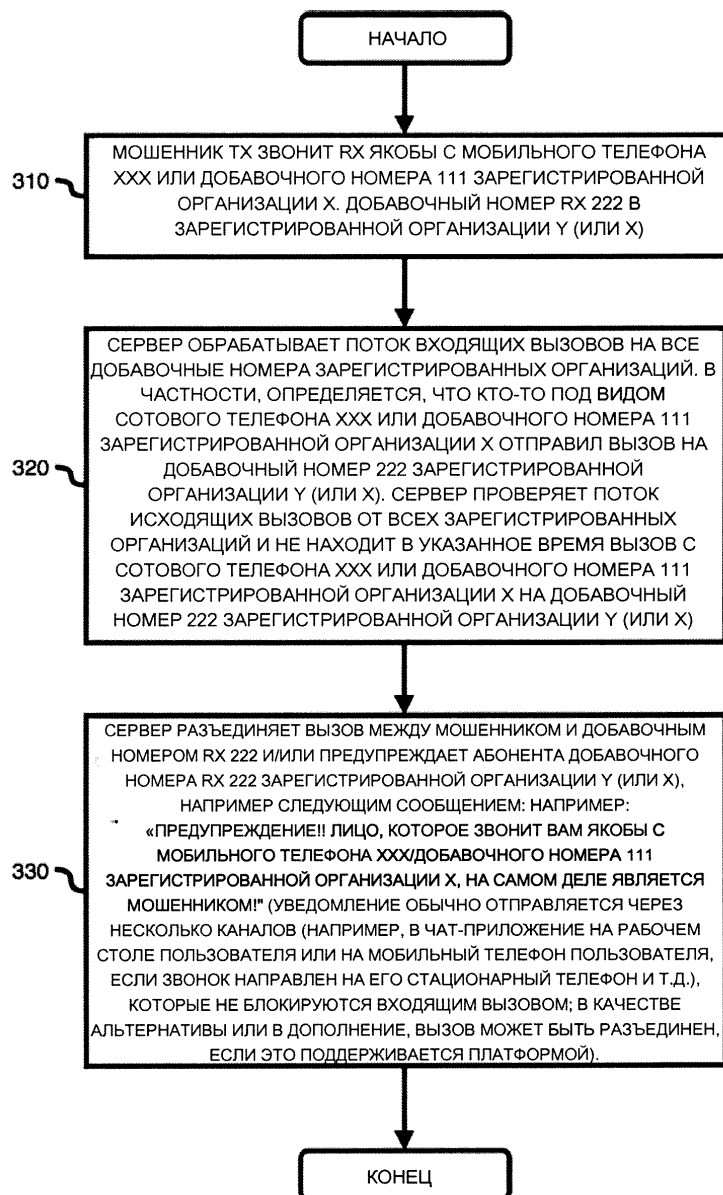
ФИГ. 1



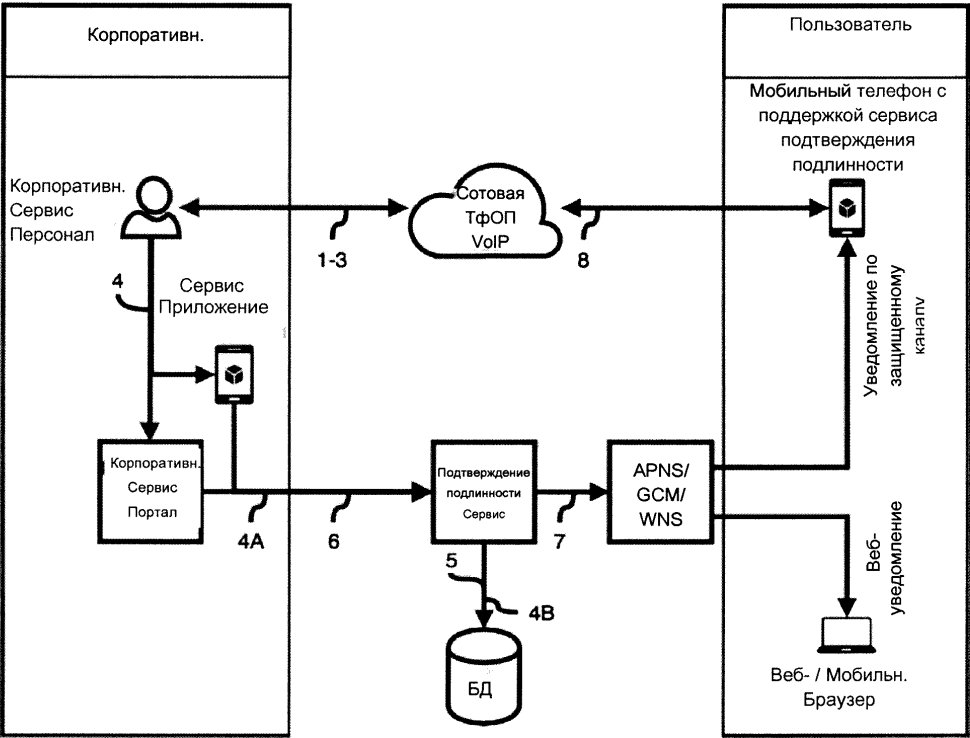
2

2/14

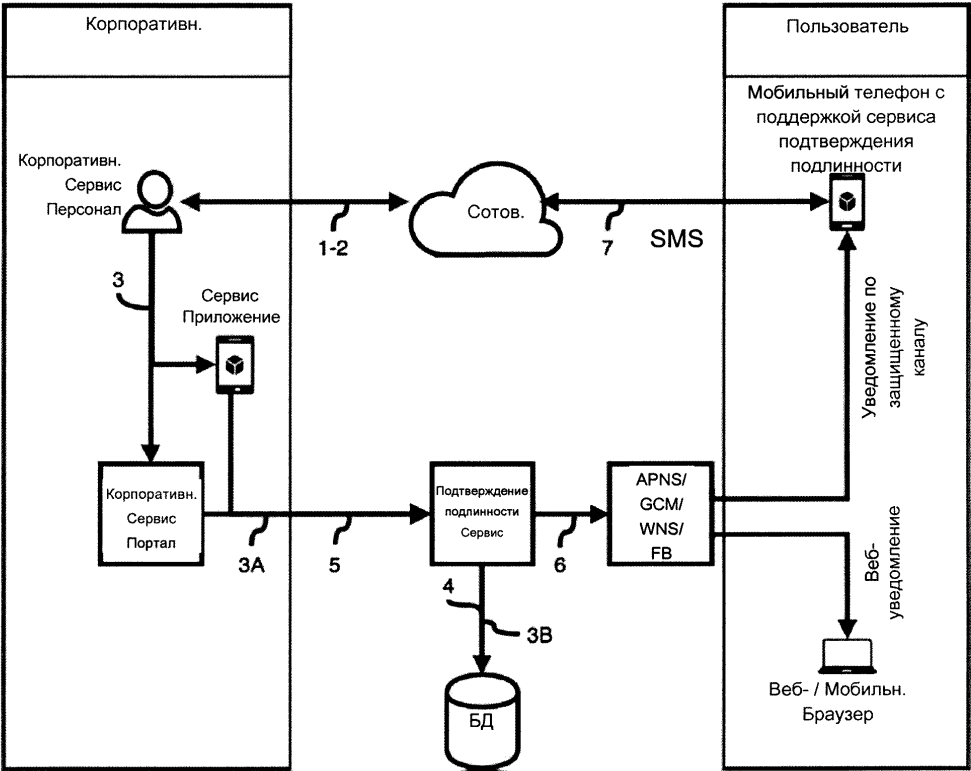
ФИГ. 2



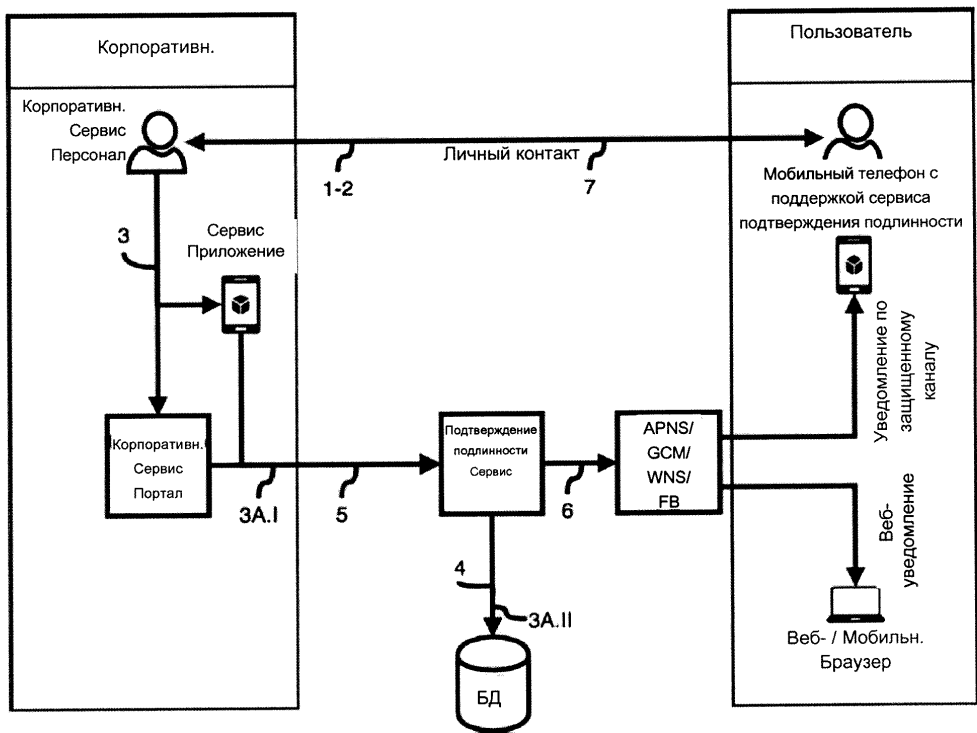
ФИГ. 3



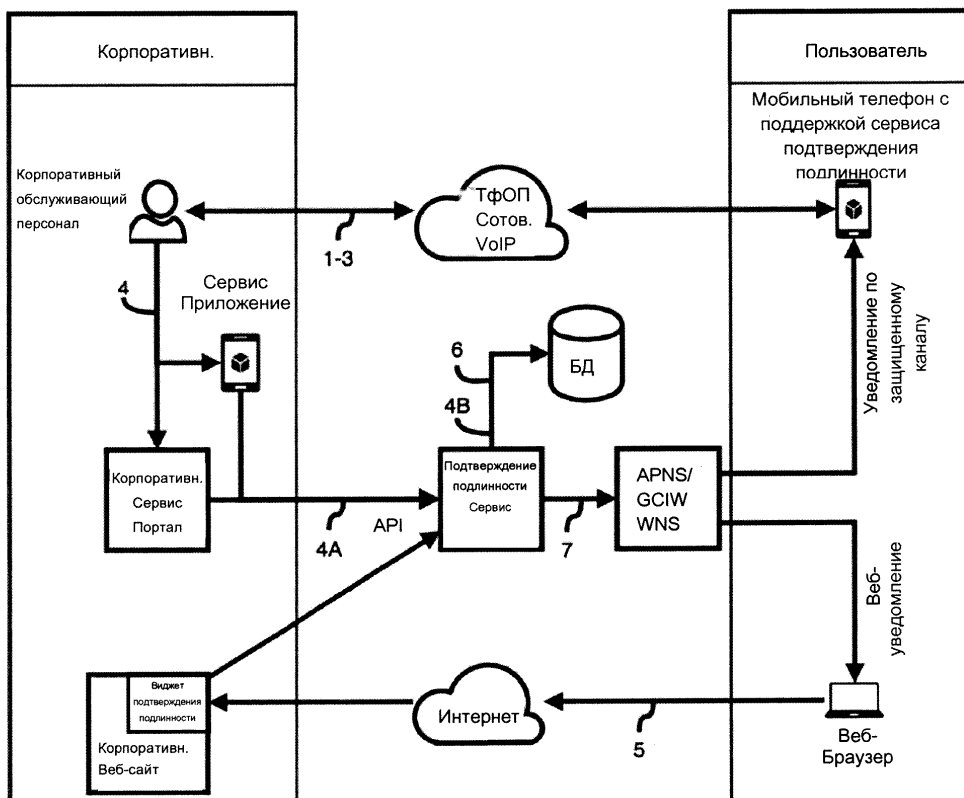
ФИГ. 4



ФИГ. 5

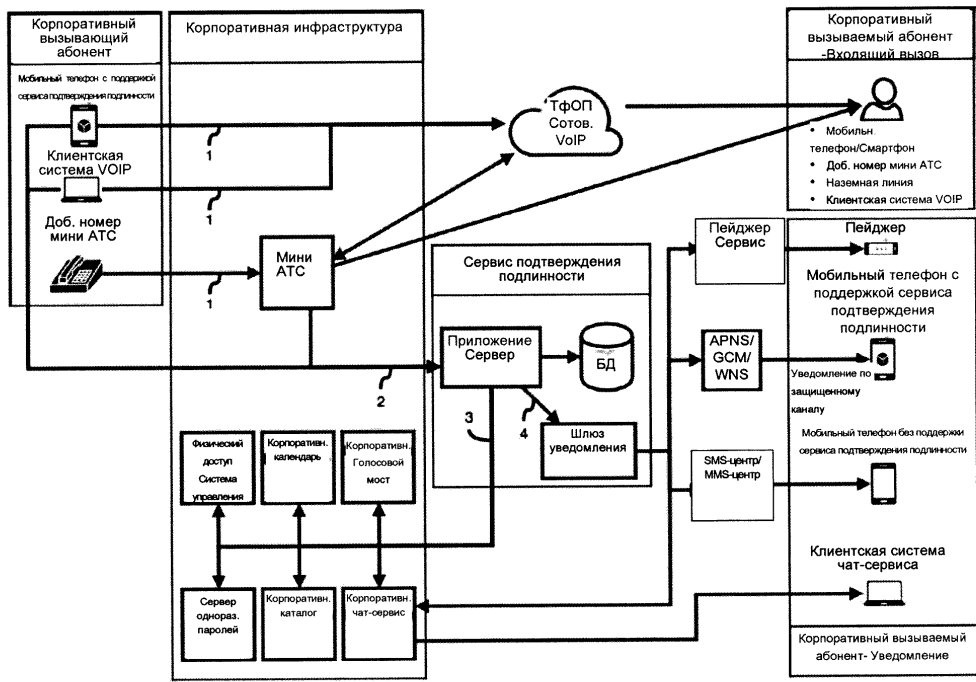


ФИГ. 6



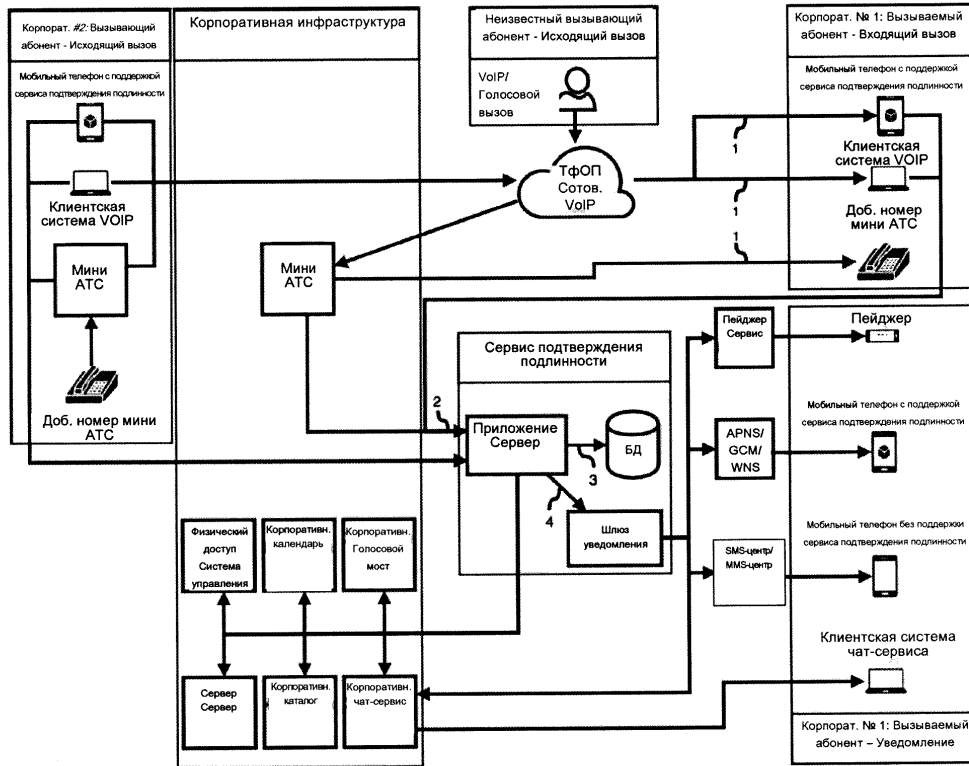
7/14

ФИГ. 7

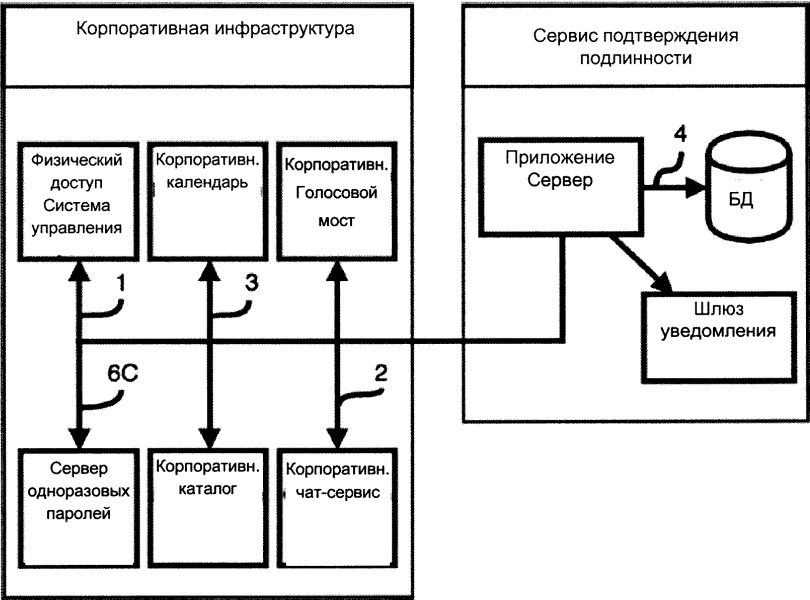


8/14

ФИГ. 8

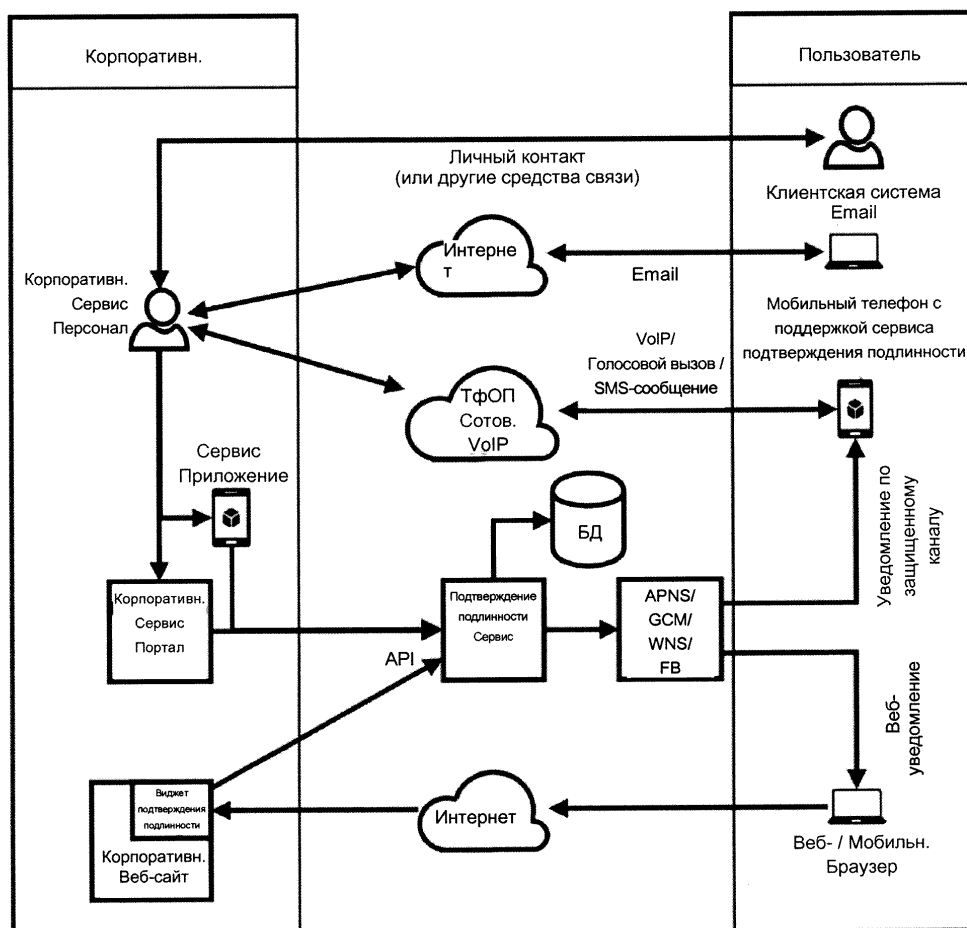


ФИГ. 9

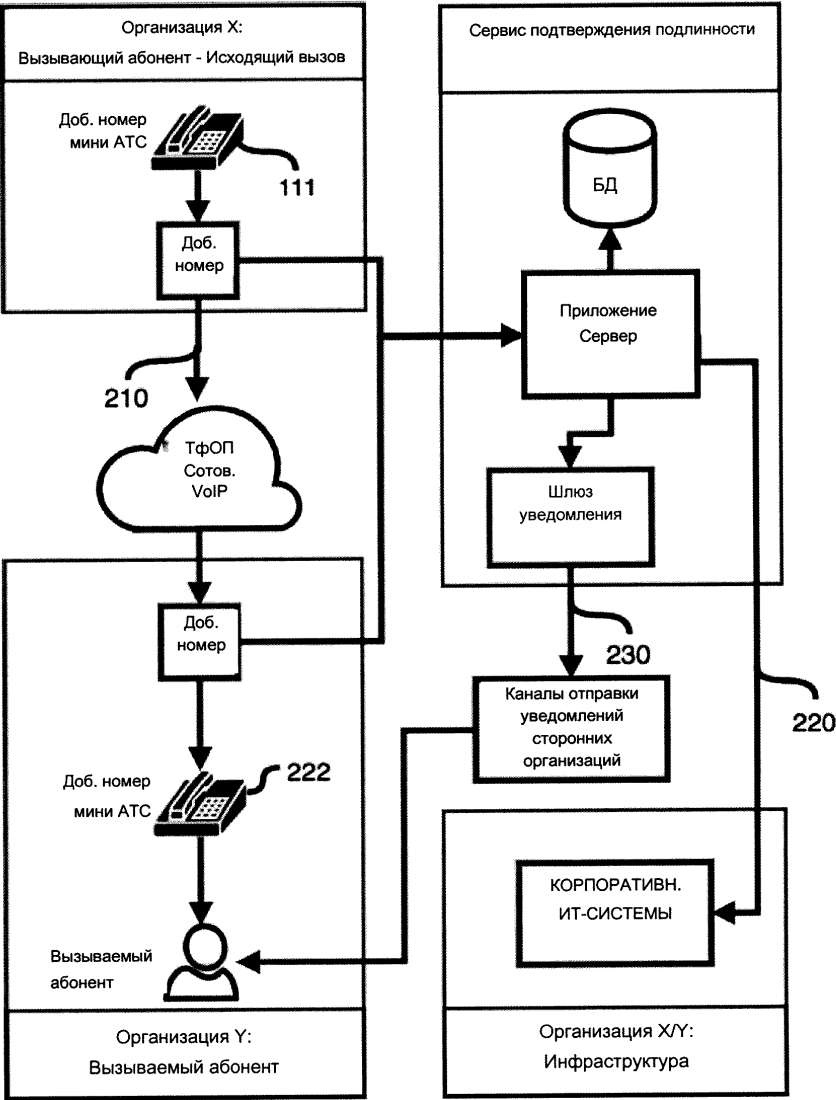


10/14

ФИГ. 10

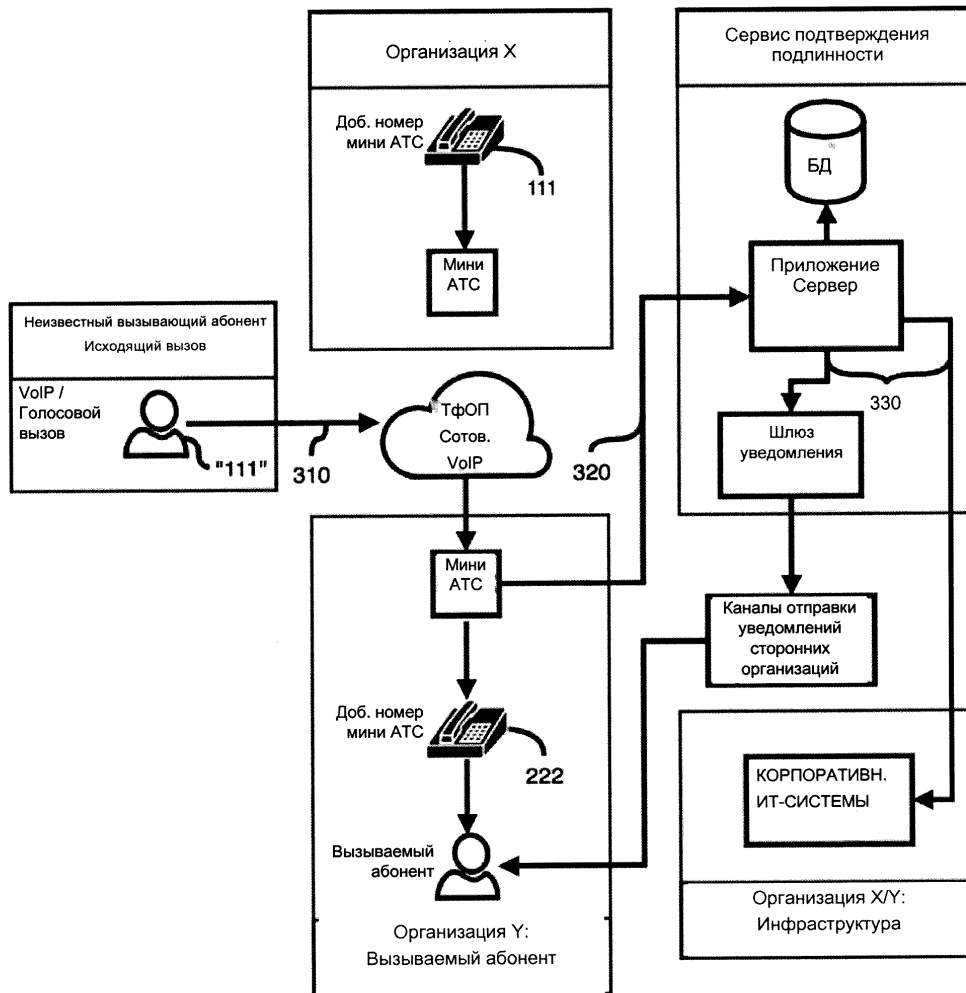


ФИГ. 11



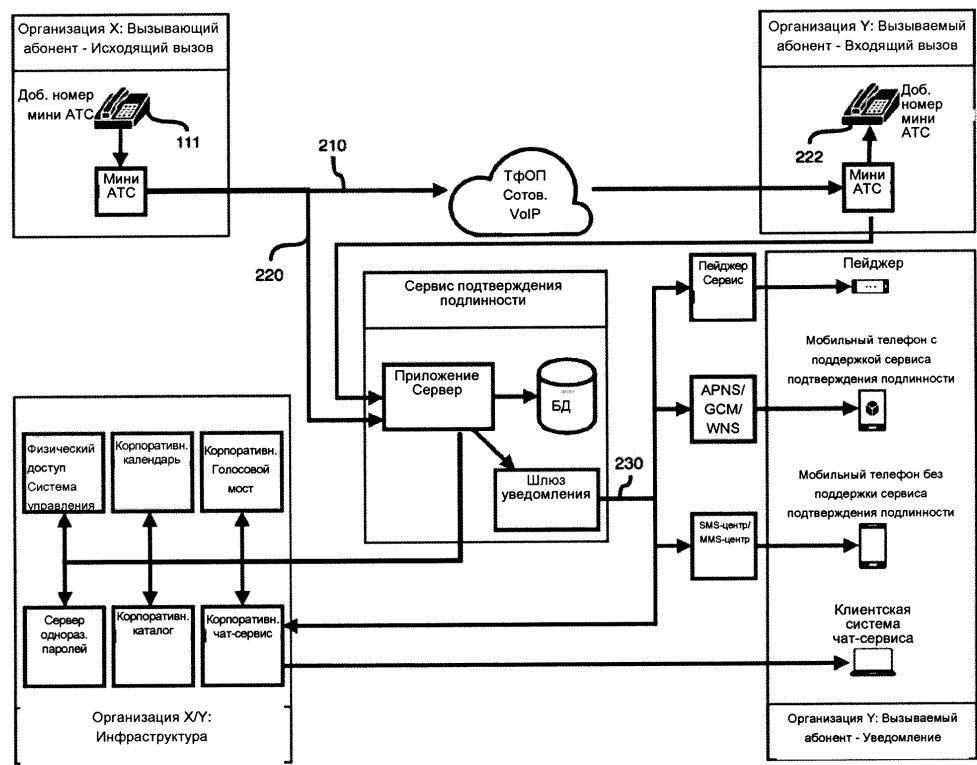
12/14

ФИГ. 12



13/14

ФИГ. 13



14/14

ФИГ. 14

