РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 557 471** (13) **C2**

(51) МПК
G10L 17/24 (2013.01)
H04W 12/12 (2009.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2012152938/08, 10.05.2011**

(24) Дата начала отсчета срока действия патента:
10.05.2011

Приоритет(ы):
(30) Конвенционный приоритет:
10.05.2010 US 12/800,173

(43) Дата публикации заявки: **20.06.2014** Бюл. № **17**

(45) Опубликовано: **20.07.2015** Бюл. № **20**

(56) Список документов, цитированных в отчете о поиске: **US 2006/0277043 A1, 07.12.2006** (см. прод.)

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **10.12.2012**

(86) Заявка PCT:
US 2011/035949 (10.05.2011)

(87) Публикация заявки PCT:
WO 2011/143235 (17.11.2011)

Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО "Союзпатент", С.В.Истомину

(72) Автор(ы):
МЕЙЛЕМАНС Марк (US),
МАРТЦ младший Гэри А. (US)

(73) Патентообладатель(и):
ИНТЕЛ КОРПОРЕЙШН (US)

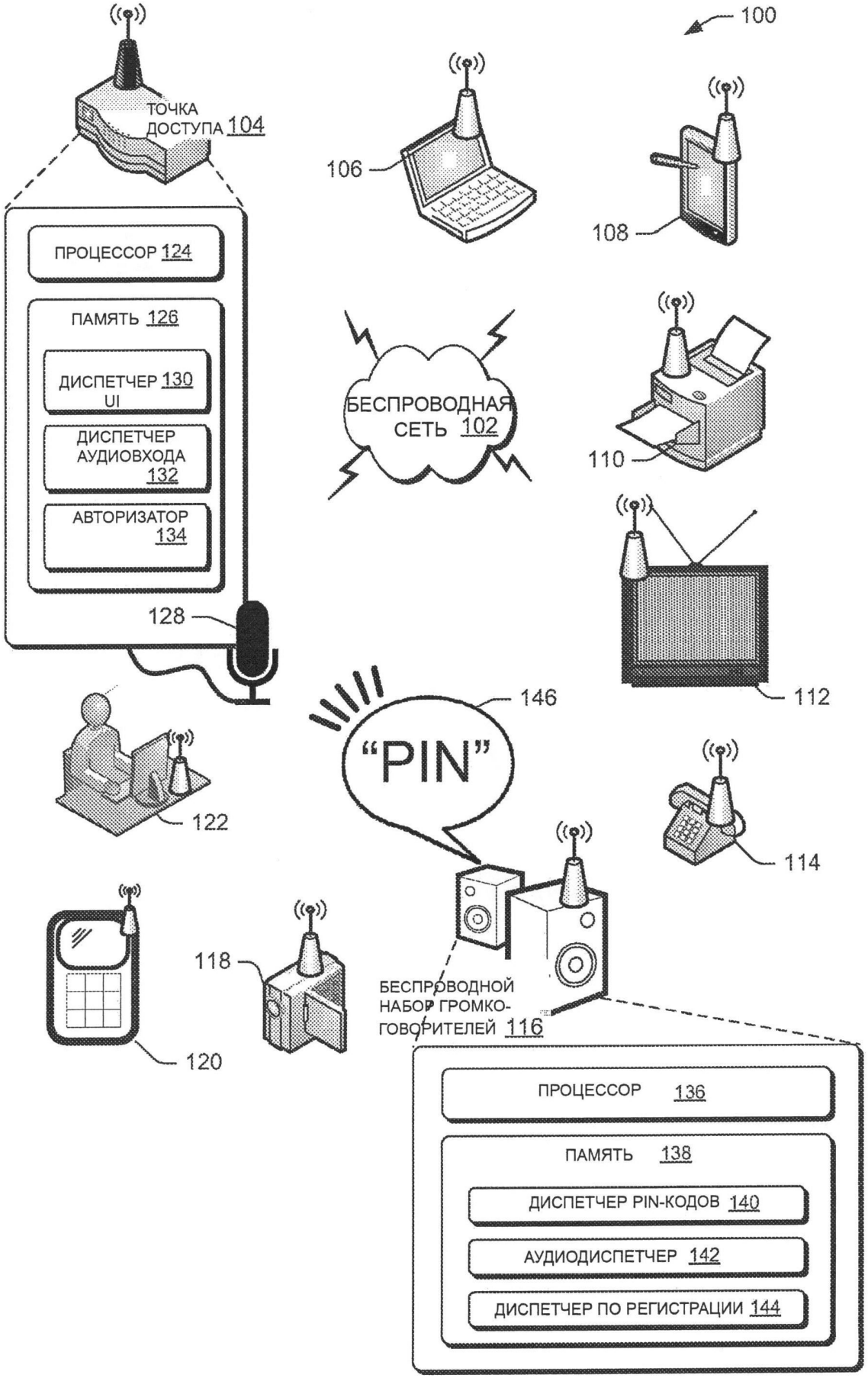
(54) ЗВУКОВАЯ АУТЕНТИФИКАЦИЯ ДЛЯ РЕГИСТРАЦИИ В БЕСПРОВОДНОЙ СЕТИ

(57) Реферат:

Изобретение относится к средствам звуковой аутентификации для регистрации в беспроводной сети. Технический результат заключается в улучшении эргономичности регистрации в защищенной беспроводной сети. Неавторизованное беспроводное устройство излучает слышимый звуковой секретный код уникальной идентификации (например, персональный идентификационный номер (PIN-код)). В некоторых реализациях пользователь слышит звуковой код и вручную вводит его через интерфейс пользователя для регистрации в сети. В других реализациях устройство авторизации в сети автоматически воспринимает звуковой код и проверяет правильность кода. Если проверка правильности прошла успешно, беспроводное устройство регистрируется в беспроводной сети. 4 н. и 11 з.п. ф-лы, 3 ил.

RU 2557471 C2

RU 2557471 C2



Фиг. 1

RU 2557471 C2

(56) (продолжение):
US 2007263577 A1, 15.11.2007 US 5450524 A, 12.09.1995 US 6088428 A, 11.07.2000RU 2326429 C2, 10.06.2008

RU 2557471 C2

RU 2557471 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 557 471** (13) **C2**

(51) Int. Cl.
G10L 17/24 (2013.01)
H04W 12/12 (2009.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2012152938/08, 10.05.2011**

(24) Effective date for property rights:
10.05.2011

Priority:
(30) Convention priority:
10.05.2010 US 12/800,173

(43) Application published: **20.06.2014** Bull. № **17**

(45) Date of publication: **20.07.2015** Bull. № **20**

(85) Commencement of national phase: **10.12.2012**

(86) PCT application:
US 2011/035949 (10.05.2011)

(87) PCT publication:
WO 2011/143235 (17.11.2011)

Mail address:
109012, Moskva, ul. Il'inka, 5/2, OOO "Sojuzpatent", S.V.Istominu

(72) Inventor(s):
MEJLEMANS Mark (US),
MARTTs mladshij Gehri A. (US)

(73) Proprietor(s):
INTEL KORPOREJShN (US)

RU 2557471 C2

(54) ACOUSTIC AUTHENTICATION FOR RECORDING IN WIRELESS NETWORK

(57) Abstract:

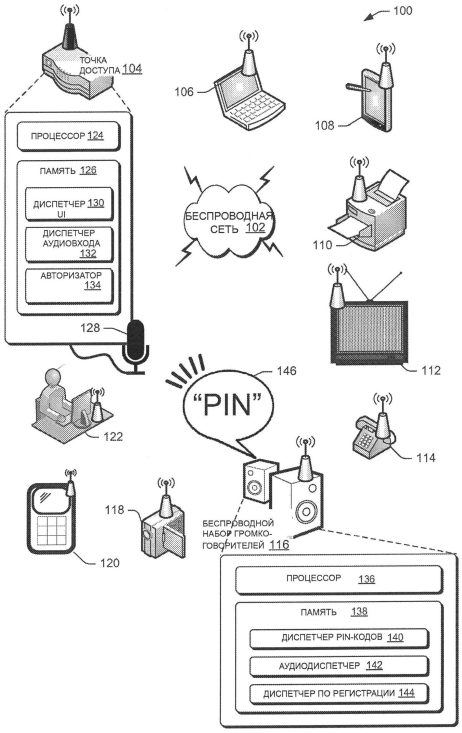
FIELD: radio engineering, communication.

SUBSTANCE: invention relates to acoustic authentication devices for recording in a wireless network. An unauthorised wireless device emits an audible acoustic secret code of unique identification (for example a personal identification number (PIN code)). In some implementations the user hears an acoustic code and enters it manually through the user interface for recording in the network. In other implementations a network authorisation device automatically receives the acoustic code and checks the code authenticity. If authenticity check is successful, the wireless device is recorded in the wireless network.

EFFECT: technical result consists in the improvement of ergonomic recording in a protected wireless network.

15 cl, 3 dwg

RU 2557471 C2



Фиг. 1

RU 2557471 C2

RU 2557471 C2

Уровень техники

Беспроводные локальные сети (WLAN) получают повсеместное распространение и используются не одними только персональными компьютерами. Для бытовых устройств нарастает тенденция обладать возможностью беспроводной связи и соединяться с WLAN. По мере роста возможностей подключения и доступности для большего количества устройств и пользователей возрастают также угрозы защищенности со стороны недопущенных к связи злоумышленников. Однако повышенные контрмеры защищенности часто смущают неискушенных пользователей беспроводных сетей.

К счастью, доступны некоторые традиционные, удобные для пользователя подходы к защищенности, пригодные для взаимодействия с сетями WLAN. Например, устройства, сертифицированные в соответствии со стандартом сертификации Wi-Fi Alliance (например, WT-FI, CERTIFIED™), способны взаимодействовать друг с другом (независимо от производителя устройства). Кроме того, Wi-Fi Alliance ввел протокол Wi-Fi Protected Setup™ (WPS), который описывает, как могут быть организованы защищенные WLAN и как сертифицированные новые беспроводные устройства могут добавляться к этим WLAN защищенным и удобным для пользователя способом. Для получения дополнительной информации обратитесь к документу ″Wi-Fi Protected Setup″ на веб-сайте Wi-Fi Alliance: .

С помощью стандартных, упрощенных и удобных для пользователя процедур установки устройства (например, WPS) пользователь может добавлять новое устройство в защищенную WLAN, вручную вводя предоставленный вместе с устройством персональный идентификационный номер (PIN-код) через интерфейс (UI) пользователя для авторизации в сети. Предоставленный вместе с устройством PIN-код действует как ключ, совместно используемый новым устройством и существующей защищенной WLAN.

Однако некоторые устройства имеют PIN-код, напечатанный на самих устройствах (например, на этикетке). Эти PIN-коды менее защищены, чем PIN-коды, динамически генерируемые другими типами устройств. Подобно ключу к замку, который никогда не изменяется, напечатанный PIN-код несет угрозу защищенности. Кроме того, одной из целей стандартных процедур регистрации в защищенной сети (например, WPS) является простота использования для пользователя. К сожалению, стандартные процедуры все еще требуют от пользователя выполнять вручную критически важные этапы. Например, с помощью WPS пользователь должен обнаружить и считать PIN-код нового устройства (который обычно имеет длину 8 знаков) и затем вручную ввести этот 8-значный PIN-код в UI, осуществляющий авторизацию для существующей защищенной сети.

Краткое описание чертежей

Подробное описание приводится со ссылкой на сопроводительные чертежи. На чертежах крайняя левая цифра(-ы) ссылочной позиции указывает чертеж, на котором эта ссылочная позиция появляется впервые. Одни и те же ссылочные позиции используются на чертежах для ссылки на схожие признаки и компоненты.

Фиг.1 - пример сетевой среды с защищенной беспроводной сетью, в рамках которой могут быть реализованы описанные здесь способы.

Фиг.2 и 3 - блок-схемы последовательностей выполнения операций описанных здесь способов звуковой аутентификации для регистрации в сети.

Подробное описание

Описанное здесь является одним или более способами использования звуковой аутентификации беспроводного устройства для регистрации в защищенной беспроводной

сети. С помощью одного или более описанных способов неавторизованное беспроводное устройство излучает звуковой сигнал, уникально идентифицирующий его секретный код (например, персональный идентификационный номер или PIN-код). В некоторых реализациях звуковой пользователь слышит код и вручную вводит его через интерфейс пользователя для сетевой регистрации. В других реализациях устройство авторизации в сети (например, беспроводная точка доступа) автоматически получает звуковой код и проверяет правильность этого кода. Если правильность кода подтверждена, беспроводное устройство регистрируется в защищенной беспроводной сети.

Описанные способы действуют как часть подходов к регистрации в защищенной сети для беспроводных локальных сетей (WLAN) и улучшают удобство пользования существующими и будущими ориентированными на пользователя и взаимодействующими подходами. Примером существующего подхода, который пригоден для использования с одной или более реализациями, описанными здесь, является Wi-Fi Protected Setup™ по протоколу Wi-Fi Alliance (WPS).

При стандартных подходах (подобных WPS) пользователь подтверждает регистрацию нового беспроводного устройства в существующей защищенной WLAN, вручную вводя предоставляемый вместе с устройством PIN-код. Когда новое устройство (например, цифровая видеокамера) обладает визуальным дисплеем, устройство показывает пользователю на этом дисплее динамически сгенерированный PIN-код. Для устройств без дисплеев стандартный подход содержит PIN-код, напечатанный на этикетке, приклеенной к устройству. Печатные PIN-коды обычно заранее генерируются и заранее печатаются изготовителем устройства. Хоть динамически генерированные PIN-коды более защищены, чем статически генерированные PIN-коды, никакой стандартный подход не предлагает устройствам без дисплеев способ предоставления динамически генерированных PIN-кодов пользователям во время процессов регистрации в защищенной сети (подобно тому, как предлагает WPS). Кроме того, стандартные подходы неприемлемы и неприменимы для пользователей со слабым зрением.

При стандартных подходах после того, как пользователь обнаруживает и считывает PIN-код на этикетке или на визуальном дисплее устройства, пользователь вводит PIN-код через интерфейс (UI) пользователя устройства авторизации (например, беспроводной точки доступа) или UI уже зарегистрированного устройства (например, персональный компьютер), действуя от имени устройства авторизации. После регистрации на WLAN новое устройство осуществляет связь через WLAN защищенным способом. Предоставляемый с устройством PIN-код действует как ключ, совместно используемый новым устройством и защищенной WLAN, и ручной ввод PIN-кода является действием, которое совместно использует этот ключ.

В отличие от стандартных подходов одна или более реализаций способов, описанных здесь, предлагает для устройств без дисплеев способ получения динамически генерированных PIN-кодов, обеспечивающий их доступность для людей со слабым зрением, и/или удобных для пользователя подходов, пригодных для взаимодействия при сетевой регистрации в защищенной сети и предназначенных для защищенных беспроводных сетей. С помощью одного или более способов, описанных здесь, устройства без дисплеев излучают слышимые динамически генерированные PIN-коды как часть процесса сетевой регистрации. Например, устройство может воспроизводить свой PIN-код через громкоговорители. Кроме того, устройство авторизации (например, сетевая точка доступа) оборудуется микрофоном, чтобы принимать и интерпретировать излучаемый слышимый PIN-код устройства. После интерпретации устройство авторизации может продолжить процесс сетевой регистрации для устройства, которое

излучило звуковой PIN-код. Таким образом, пользователь может избежать ручного и подверженного ошибкам процесса обнаружения и считывания PIN-кода устройства и последующего ручного ввода этого PIN-кода для устройства, которое должно регистрироваться в защищенной WLAN.

Пример среды беспроводной сети

На фиг.1 представлен пример среды 100 беспроводной сети. Пример сетевой среды 100 содержит беспроводную локальную сеть (WLAN) 102, которая может средствами связи (проводными, беспроводными, посредством сотовой связи, спутниковой связи и т.д.) соединяться с другими сетями, такими как Интернет или другие WLAN. Сетевая среда 100 также содержит по меньшей мере одну точку 104 доступа (AP) и много других беспроводных станций (STA) 106-122.

AP 104 функционирует как аутентификатор для WLAN 102 и AP может действовать как мост к другим сетям, осуществляемый посредством средств связи (не показаны). AP 104 может быть выделенным сетевым устройством. Альтернативно, она может быть универсальным устройством или универсальным вычислительным устройством. Например, AP 104 может быть мостом, маршрутизатором, повторителем, сервером, клиентом или любым другим сетевым устройством, которое может также функционировать как беспроводное устройство авторизации для WLAN 102. В некоторых реализациях сетевая функция аутентификации для WLAN 102 может совместно использоваться AP 104 и другими сетевыми устройствами. Также, альтернативно, AP 104 может делегировать сетевую функцию аутентификации к другим сетевым устройствам.

Как показано на чертеже, станции или STA (например, беспроводные устройства) содержат ноутбук 106, планшетный компьютер 108, сетевой принтер 110, сетевое телевидение 112, телефон 114 VoIP (передача голоса по сетям, работающим по интернет-протоколу), беспроводной набор 116 громкоговорителей, цифровую видеокамеру 118, мобильный телефон 120 и персональный компьютер 122 (показан с пользователем). Конечно, STA 106-122 являются просто иллюстрацией типов беспроводных устройств, которые могут использоваться в контексте примера среды 100 беспроводной сети. Другими подходящими беспроводными устройствами являются (для примера и без ограничений): персональные цифровые секретари (PDA), цифровые музыкальные проигрыватели, цифровые фотокамеры, офисные проекторы, цифровые фоторамки, смарт-телефоны, звуковое оборудование, навигационные системы, калькуляторы, видеооборудование, телефоны, бытовые приборы, системы нагревания и/или охлаждения, бытовая электроника, медицинское оборудование, системы обеспечения безопасности, широковещательное настраиваемое оборудование, оборудование доступа по требованию и т.п.

В примере среды 100 беспроводной набор 116 громкоговорителей в настоящий момент не зарегистрирован как часть защищенной WLAN 102. Беспроводной набор 116 громкоговорителей ищет возможность зарегистрироваться или присоединиться к WLAN 102. Устройства, ищущие возможность сетевой регистрации, подобные беспроводному набору 116 громкоговорителей, называются здесь ″претендентами″.

Подобно любому другому соответствующему беспроводному устройству и AP 104, каждая из STA 106-122 предназначена для использования при существующих или будущих удобных для пользователя подходах, пригодных для взаимодействия при регистрации в защищенной сети и предназначенных для защищенных беспроводных сетей WLAN, таких как WLAN 102. Например, STA 106-122 предназначены для использования протокола Wi-Fi Protected Setup™ (WPS) стандарта Wi-Fi Alliance для

регистрации устройства в защищенной WLAN. Аналогично, AP 104 предназначена для использования WPS при регистрации новых STA в WLAN 102. Хотя на фиг.1 явно не показано, каждая из STA 106-122 может содержать аппаратурное обеспечение, встроенное микропрограммное обеспечение, программное обеспечение или их комбинацию, выполненные с возможностью осуществления, по меньшей мере частично, описанных здесь способов.

Примером WLAN 102 может быть инфраструктура беспроводной сети, но могут использоваться и другие реализации WLAN, такие как так называемая ″специализированная″ (″ad-hoc″) или персональная сеть (PAN). WLAN 102 соответствует одному из существующих или будущих сетевых стандартов для беспроводных локальных сетей. Стандарты Института инженеров по электронике и радиотехнике (IEEE) 802.11 (например, IEEE 802.11a, 802.11b, 802.11g и 802.11n) являются примерами соответствующих сетевых стандартов для беспроводных локальных сетей, используемых для описанных здесь способов. В целом, соответствующая беспроводная сеть является сетью, имеющей сетевые устройства, предназначенные для использования существующих или будущих удобных для пользователя подходов, пригодных для взаимодействия при регистрации в защищенной сети и предназначенных для защищенных беспроводных сетей.

Как представлено на фиг.1, AP 104 имеет компоненты для реализации по меньшей мере части описанных здесь способов. AP 104 содержит один или более процессоров 124, память 126 и микрофон 128. В памяти 126 присутствуют один или более компонент, к которым относятся диспетчер 130 интерфейса (UI) пользователя, диспетчер 132 аудиовхода и авторизатор 134.

Обычно микрофон 128 является неотъемлемой частью AP 104. Альтернативно, микрофон 128 может быть внешним и подключаться проводами к AP 104. Также альтернативно, микрофон 128 может соединиться с AP 104 с помощью беспроводных технологий и может быть уже зарегистрированным устройством или частью уже зарегистрированного устройства на WLAN 102. Микрофон 128 предназначен для восприятия диапазона звуковых частот, который, как ожидается, должен излучаться. Эти частоты могут быть в пределах выше и/или ниже слухового диапазона обычного человека.

Диспетчер 130 UI управляет интерфейсом (UI) пользователя для сетевой регистрации, представляемым пользователю, который вовлекается в процесс регистрации нового устройства. Если AP 104 обладает возможностью приема ввода данных от пользователя и генерации UI, UI может быть предоставлен на самом AP 104. Как правило, UI предоставляется через отдельное и уже зарегистрированное в сети устройство, такое как персональный компьютер 122. Диспетчер 128 UI управляет входным сигналом от пользователя UI в персональном компьютере 122 и помогает генерировать выходной сигнал на этом компьютере.

Диспетчер 132 аудиовхода управляет аналоговым входным аудиосигналом, приходящим от микрофона 128. В частности, диспетчер 132 аудиовхода принимает и распознает входной аудиосигнал, который совпадает со звуковым PIN-ключом, излучаемым устройством, стремящимся зарегистрироваться в сети. Диспетчер 132 аудиовхода преобразует введенный аналоговый звуковой PIN-код в кодированную компьютером форму, которую может использовать аутентификатор 134. Здесь кодированный компьютером PIN-код сохраняется и обрабатывается способом, при котором значение и содержание PIN-кода доступны и могут использоваться компонентами компьютера. Например, кодированная компьютером форма PIN-кода

″13442GR3UT9″ может быть строкой символов или может храниться как значение с плавающей запятой.

Авторизатор 134 принимает кодированный компьютером PIN-код от диспетчера 132 аудиовхода. PIN-код действует как ключ, совместно используемый претендентом и AP 104 (и/или некоторыми из других существующих устройств в защищенной WLAN). Авторизатор 134 (например, сетевой регистратор) подтверждает достоверность PIN-кода. Авторизатор 134 может осуществлять проверку правильности посредством криптографических вычислений, таблицы поиска, консультаций с доверенной третьей стороной (например, по Интернет-соединению) или других известных процессов проверки правильности. Претенденту отказывают в регистрации, если PIN-код не может пройти проверку правильности. Как только PIN-код прошел проверку правильности, авторизатор 134 инициирует процедуру сетевой регистрации претендента, который назвал звуковой PIN-код. Такая процедура сетевой регистрации может делаться, например, в соответствии с протоколом WPS или другими удобными для пользователя подходами, пригодными для взаимодействия при сетевой регистрации в защищенной сети и предназначенными для защищенных беспроводных сетей. Примером претендента является набор 116 беспроводных громкоговорителей, являющийся устройством, не имеющим дисплея. Конечно, набор 116 беспроводных громкоговорителей является только одним примером типа устройства, у которого отсутствует электронный выходной механизм для визуального представления информации пользователю (особенно, когда такая информация обеспечивается электрическим сигналом). Здесь такие устройства называются ″бездисплейными″. Примерами различного типа визуальных дисплеев, которые не имеют бездисплейные устройства, являются (для примера, но не для ограничения): электролюминесцентные дисплеи (ELD); светодиодные дисплеи (LED); дисплеи на электронно-лучевой трубке (CRT); жидкокристаллические дисплеи (LCD); плазменные панели (PDP); органические светодиодные дисплеи (OLED); светопроцессорные дисплеи (DLP); электронные документы и невизуальные дисплеи типа электромеханических дисплеев.

Как представлено на фиг.1, беспроводной набор 116 громкоговорителей имеет компоненты для реализации по меньшей мере части описанных здесь способов. Беспроводной набор 116 громкоговорителей содержит один или более процессоров 136 и память 138. В памяти 138 находятся один или более компонентов, к которым относятся диспетчер 140 PIN-кодов, аудиодиспетчер 142 и диспетчер 144 по регистрации. Как показано на чертеже, беспроводной набор 116 громкоговорителей излучает звуковой кодовый персональный идентификационный номер (PIN) 146, показанный на выноске для надписей.

Компоненты беспроводного набора 116 громкоговорителей и компоненты AP 104 могут быть модулями исполняемых компьютером команд, причем такие команды могут исполняться на компьютере, вычислительном устройстве или процессорах таких устройств. Хотя компоненты показаны здесь как отдельные модули, компоненты могут быть реализованы в виде аппаратурного обеспечения, встроенного микропрограммного обеспечения, программного обеспечения или любой их комбинации. Способы, описанные здесь, могут быть реализованы полностью или частично в виде аппаратурного обеспечения, программного обеспечения, встроенного микропрограммного обеспечения или любой их комбинации.

Диспетчер 140 PIN-кодов управляет уникальными PIN-кодами для сетевой регистрации (например, секретным кодом регистрации в сети), которые должны быть поняты и принята сетевым авторизатором, чтобы идентифицировать и зарегистрировать

претендента в защищенной WLAN 102. Диспетчер 140 PIN-кодов также обеспечивает подачу таких PIN-кодов аудиодиспетчеру 142 так, что беспроводной набор 116 громкоговорителей может объявить PIN-код вслух. Диспетчер 140 PIN-кодов может динамически генерировать PIN-код, основываясь на предоставленной изготовителем формуле. Альтернативно, диспетчер 140 PIN-кодов может просто получить доступ к статическому PIN-коду в памяти 138.

Уникальная сетевая регистрация PIN-кода связывается с претендентом (например, беспроводным набором 116 громкоговорителей), как часть интерактивного подхода к сетевой регистрации, используемого WLAN 102 (например, WPS). PIN-код для сетевой регистрации может быть уникальным для конкретной сети (например, WLAN 102), к которой претендент пытается подключиться. Кроме того, PIN-код для сетевой регистрации может быть глобально уникальным кодом (то есть ни у какого другого беспроводного устройства такого кода нет нигде). PIN-код для сетевой регистрации обычно является многозначным числом (например, 4-8 цифр). Альтернативно, PIN-код для сетевой регистрации может быть буквенно-цифровой строкой. Кроме того, альтернативно, PIN-код для сетевой регистрации может содержать символы и другие коды, связанные с конкретными звуками, тонами или музыкой.

Аудиодиспетчер 142 принимает кодированный компьютером PIN-код от диспетчера 140 PIN-кодов. Аудиодиспетчер 142 преобразует PIN-код в его кодированном компьютером формате в электрический сигнал, который управляет громкоговорителями беспроводного набора 116 громкоговорителей. В результате беспроводной набор 116 громкоговорителей излучает слышимый звук, который показан как ″PIN″ 146 на выноске для надписей.

Звуковой PIN-код 146 может быть любым воспроизводимым звуком, тоном, музыкой и т.п. Примерами звукового PIN-кода 146 являются (только для примера и не для ограничения): произносимые слова, буквы и/или номера (возможно на выбираемых пользователем языках), тоны, щелчки, прерывистые звуковые сигналы, замечания и музыка. Звуковой PIN-код 146 может генерироваться посредством компьютера аудиодиспетчером 142. Альтернативно, звуковой PIN-код может быть одним или более хранящимися файлами (например, файл цифровой аудиозаписи), полученными из памяти 138 или системы хранения памяти и затем воспроизводимыми. Звуковой PIN-код 146 может быть в пределах, внутри и/или вне диапазона слуха обычного человека. Характер звука звукового PIN-кода 146 ограничивается способностью AP 104 получить звуковой PIN-код 146 с помощью микрофона 128, а для диспетчера 132 аудиовхода AP - способностью обнаруживать совпадение с оригинальным, уникальным PIN-кодом для сетевой регистрации, которая обеспечивается диспетчером 140 PIN-кодов беспроводного набора 116 громкоговорителей.

Пример претендента (например, беспроводного набора 116 громкоговорителей), показанный на фиг.1, по существу имеет громкоговорители, чтобы излучать слышимый PIN-код. Однако в других реализациях могут использоваться другие типы претендентов. В других реализациях Претенденты имеют аудиовозможности, встроенные в них изготовителем. Например, изготовитель беспроводного устройства может намеренно встроить интегральный громкоговоритель, может ввести гнездо для наушников, может предложить схему сети связи на короткое расстояние (например, BLUETOOTH™), чтобы соединяться с другим аудиоустройством (например, мобильным телефоном или телефоном), или может предоставить вариант связи претендента по WLAN 102 с сетевым устройством с громкоговорителем.

Диспетчер 144 по регистрации управляет сетевой процедурой регистрации с AP 104,

когда авторизатор 134 подтвердил для сетевой регистрации достоверность PIN-кода, полученного из звукового PIN-кода 146. Диспетчер 144 по регистрации управляет предоставлением сетевых учетных данных, так чтобы беспроводной набор 116 громкоговорителей становился частью защищенной WLAN 102. В целом, диспетчер 144 по регистрации выполняет процедуры сетевой регистрации в соответствии с WPS или с другими удобными для пользователя интерактивными защищенными подходами сетевой регистрации для защищенных беспроводных сетей.

Примеры процессов

На фиг.2 и 3 представлены блок-схемы последовательности выполнения операций, иллюстрирующие примеры процессов 200 и 300, которые реализуют способы, описанные здесь для звуковой аутентификации при регистрации в беспроводных сетях. Каждый из этих процессов представлен как набор этапов в логической блок-схеме, которая представляет последовательность выполнения операций, которые могут быть реализованы посредством аппаратурного обеспечения, программного обеспечения или их комбинации. В контексте программного обеспечения блоки представляют компьютерные команды, которые, когда выполняются одним или более процессорами такого компьютера, выполняют упомянутые операции. Заметим, что порядок, в котором описывается процесс, не подразумевается рассматриваемым как ограничение и любое количество описанных этапов процесса может быть объединено в любом порядке, чтобы реализовать процесс или альтернативный процесс. Дополнительно, индивидуальные блоки могут удаляться из процесса, не отступая от сущности и контекста описанного здесь предмета изобретения.

На фиг.2 представлен процесс 200 для сетевого претендента (например, беспроводного набора 116 громкоговорителей на фиг.1), чтобы совместно использовать секретный код с сетевым аутентификатором (например, AP 104), облегчая регистрацию в защищенной беспроводной сети (например, WLAN 102). Пример процесса в примере 200 начинается на этапе 202 с получения претендентом указания создать уникальный секретный код, идентифицирующий претендента для сетевых аутентификаторов, участвующих в общем стандарте/подходе к взаимодействию при сетевой регистрации в защищенной беспроводной сети. Секретный код уникален для всей защищенной беспроводной сети и, таким образом, однозначно идентифицирует претендента для сетевого аутентификатора. Дополнительно, секретный код может быть глобально уникальным и идентифицирующим. Это означает, что никакой другой претендент нигде не обладает тем же самым секретным кодом. Уникальный секретный код также называют персональным идентификационным номером (PIN-кодом).

Когда пользователь активирует претендента, претендент может искать беспроводные сети. Когда претендент обнаруживает сеть, он хочет зарегистрироваться в ней, то есть претендент может стремиться присоединиться к этой сети. На деле незарегистрированная сеть может указать, что претендент должен предоставить свой PIN-код. Альтернативно, пользователь может нажать на претенденте кнопку, которая приказывает претенденту предоставить его PIN-код.

На этапе 204 претендент получает кодированную компьютером версию PIN-кода, который уникально определяет претендента в защищенной сети или, альтернативно, определяет его глобально. Здесь претендент может динамически генерировать PIN-код, основываясь на предоставляемой изготовителем формуле и других известных подходах для создания уникально идентифицируемого секретного ключа. Альтернативно, претендент может просто получать доступ к статическому PIN-ключу, взятому из памяти (например, из памяти 138) или подсистемы хранения данных (например, с диска

или флэш-карты памяти).

На этапе 206 претендент преобразует полученный, кодированный компьютером PIN-код в электрический сигнал, способный создать звуковую версию PIN-ключа. Например, электрический сигнал может возбуждать громкоговорители беспроводного набора 116 громкоговорителей. Преобразование содержит преобразование цифр полученного PIN-кода в конкретные звуки. Звуки, являющиеся результатом преобразования, могут быть получены посредством прямого преобразования хранящихся в компьютере чисел или букв в их соответствующие звуки на определенном языке. Выполняя это, претендент может динамически создавать соответствующие звуки для каждой цифры. Альтернативно, претендент может получать доступ к хранящимся в памяти или хранилище звукам, основываясь на заданных связях между цифрами и хранящимися звуками. Например, для PIN-кода ″123″ претендент может получить доступ к трем звуковым файлам, по одному для каждой цифры ″1″, ″2″ и ″3″. Альтернативно, PIN-код может содержать понимаемые человеком слова и, возможно, предложения.

Кроме того, претендент может иметь многочисленные наборы звуков, где каждый набор имеет звуки на конкретном языке. Пользователь может выбрать конкретный язык (например, французский язык), выбирая определенные опции на устройстве претендента (например, нажимая кнопку и/или переключая переключатели). Язык по умолчанию может быть установлен изготовителем, основываясь на том, где претендент продается. Вместо понятных для человека чисел, букв и слов, звуки, получающиеся в результате преобразования, могут не быть частью обычного человеческого языка. Например, цифры PIN-кода могут преобразовываться в тона, щелчки, звуковые сигналы, замечания, музыку, взрывы, голоса животных, звуковые эффекты или другие звуки, не являющиеся частью обычного человеческого языка.

Альтернативно, вместо преобразования кодированной компьютером версии PIN-ключа (например, ″134RG34FF2W99″) в звуковую версию PIN-ключа, претендент может извлечь из памяти ранее генерированные аудиоверсии PIN-ключа [1]или частей PIN-ключа. Например, претендент мог сохранить в памяти цифровой аудиофайл, который, когда воспроизводится, создает голос женщины, говорящей ″Красный, зеленый, синий, восемь, девять, тридцать один, альфа, танго, девяносто один, оранжевый″. Звуки этой записи могут соответствовать соответствующему PIN-ключу для сетевой регистрации, посылаемому сетевому аутентификатору, который слышит этот звук или принимает этот ввод от пользователя, используя UI для сетевой регистрации.

На этапе 208 претендент создает звуковой PIN-код через громкоговорители, подобные тем, которые имеются в беспроводном наборе П6 громкоговорителей. Это показывается надписью ″PIN″ 146 в выноске для текста на фиг.1. Когда претендент не имеет встроенной возможности создания звука, претендент может выполнить промежуточный этап, чтобы упаковать и передать звуковой PIN-код устройству с громкоговорителем. Это может быть сделано через сетевую схему связи на короткое расстояние, чтобы соединиться с другим аудиоустройством (например, мобильным телефоном или телефоном), или это может быть сделано, связывая претендента с сетевым устройством с громкоговорителем через некую незащищенную сеть.

На этапе 210 претендент ждет подтверждения, что сетевой аутентификатор (например, AP 104) получил и/или подтвердил звуковой PIN-код. Сетевой аутентификатор может получить PIN-код через микрофон, чтобы иметь звуковой PIN-код. Альтернативно, аутентификатор может получить PIN-код через пользователя, который слышит звуковой PIN-код и вручную вводит PIN-код, воспринятый пользователем. В некоторых

реализациях может не быть никакого специального подтверждения. Вместо этого инициирование процесса сетевой регистрации действует как косвенное подтверждение, что PIN-код был принят и его правильность подтверждена.

На этапе 212 претендент присоединяется к защищенной беспроводной сети. Этот процесс может содержать получение претендентом сетевых учетных данных от сетевого аутентификатора. После завершения процесса регистрации претендент является установленным беспроводным устройством в защищенной беспроводной сети.

На фиг.3 представлен пример процесса 300 получения сетевым аутентификатором (например, AP 104) секретного кода от сетевого претендента (например, от беспроводного набора 116 громкоговорителей, показанного на фиг.1), чтобы облегчить регистрацию претендента в защищенной беспроводной сети (например, WLAN 102). Пример процесса 300 начинается на этапе 302 аутентификатором, принимающим уникальный секретный код, который идентифицирует претендента для аутентификатора, участвующего в общем стандарте/подходе взаимодействия для сетевой регистрации в защищенной беспроводной сети. Уникальный секретный код также называется персональным идентификационным номером (PIN-кодом).

Когда пользователь включает аутентификатор или выбирает вариант поиска, аутентификатор может искать претендентов. Когда аутентификатор обнаруживает претендента, аутентификатор спрашивает претендента, хочет ли он присоединиться к защищенной сети. Конечно, аутентификатор может конкретно просить претендента предоставить его PIN-код. Альтернативно, аутентификатор может ответить на запрос претендента о присоединении к сети или указать, что претендент отправит ему свой PIN-код. Также, альтернативно, аутентификатор может принять по сети сигнал или некоторый звуковой код, указывающий, что PIN-код появляется. Дополнительно, в некоторых реализациях аутентификатор всегда может быть готов получить звуковой PIN-код.

На этапе 304 аутентификатор получает через микрофон (например, микрофон 128) аналоговый электрический сигнал звукового PIN-кода, излучаемого претендентом. Это показывается надписью 146 ″PIN″, показанной в выноске для текста на фиг.1, приходящей от беспроводного набора 116 громкоговорителей, находящегося вблизи микрофона 128. Расстояние близости зависит от многих акустических факторов, таких как громкость звукового PIN-кода, чувствительность микрофона 128 и возможная помеха со стороны других звуковых источников (например, шум). Как правило, аутентификатор (например, AP 104) и претендент (например, беспроводной набор 116 громкоговорителей) находятся вместе в одной и той же комнате, когда создается слышимый звуковой PIN-код.

На этапе 306 аутентификатор посылает претенденту подтверждение, что аутентификатор принял звуковой PIN-код от претендента. В некоторых реализациях аутентификатор может не посылать специальное подтверждение. Вместо него инициирование процесса сетевой регистрации действует как косвенное подтверждение, что PIN-код был получен и верифицирован.

На этапе 308 аутентификатор преобразует аналоговый электрический сигнал в кодированную компьютером версию PIN-кода. Выполнение преобразования аутентификатором содержит обратное преобразование того вида преобразования, которое выполняется претендентом при создании звукового PIN и обсуждалось выше, например, в отношении этапа 206 процесса 200. Звуки звукового PIN-кода преобразуются в кодированную компьютером версию PIN-кода.

Альтернативно, вместо того, чтобы принять и преобразовать звуковой PIN-код,

аутентификатор может принять кодированную компьютером версию PIN-кода через человека в качестве посредника. В этой ситуации пользователь слышит звуковой PIN-код, выдаваемый претендентом, и вручную вводит PIN-код на UI аутентификатора. Этот UI может быть частью самого аутентификатора или может быть предоставлен через другое устройство в сети.

На этапе 310 аутентификатор подтверждает достоверность PIN-кода для регистрации в цифровой сети. Аутентификатор может сделать это посредством криптографических вычислений, таблицы поиска, консультации с доверенной третьей стороной (например, по Интернет-соединению) или других известных процессов проверки правильности. Вместо или в дополнение к подтверждению этапа 308 аутентификатор может послать претенденту подтверждение, что аутентификатор подтвердил достоверность звукового PIN-кода, полученного от претендента. В некоторых реализациях аутентификатор может не посылать специальное подтверждение. Вместо этого инициирование процесса сетевой регистрации действует как косвенное подтверждение, что PIN-код был принят и верифицирован.

Когда правильность PIN-кода проверена, аутентификатор инициирует на этапе 312 процедуру сетевой регистрации претендента, который сообщает звуковой PIN-код. Процедура может содержать посылку аутентификатором по сети сетевых учетных данных претенденту. После завершения процесса регистрации претендент является установленным беспроводным устройством в защищенной беспроводной сети. Если правильность кода не может быть проверена, то аутентификатор отказывает претенденту в доступе на вход в защищенную беспроводную сеть. Аутентификатор может послать претенденту индикацию отказа в доступе через сеть.

Заключительные замечания

Термины ″компонент″, ″модуль″, ″система″, ″интерфейс″ и т.п., как они используются в настоящей заявке, обычно подразумеваются относящимися к связанному с компьютером объекту, являющемуся аппаратурным обеспечением, комбинацией аппаратурного и программного обеспечения, программным обеспечением или исполняемым программным обеспечением. Например, компонент может быть, в частности, процессом, работающий на процессоре, процессором, объектом, исполняемым файлом, потоком выполнения, программой и/или компьютером. Например, как приложение, работающее на контроллере, так и контроллер могут быть компонентом. Один или более компонентов могут входить в состав процесса и/или потока выполнения и компонент может быть локализован на одном компьютере и/или распределен между двумя или более компьютерами.

Кроме того, заявленный предмет изобретения может быть реализован как способ, устройство или производственное изделие, используя стандартное программирование и/или технические способы для создания программного обеспечения, встроенного микропрограммного обеспечения, аппаратурного обеспечения или любой их комбинации, чтобы управлять компьютером для реализации раскрытого предмета изобретения. Термин ″производственное изделие″, как он используется здесь, подразумевается содержащим в себе компьютерную программу, доступную от любого считываемого компьютером устройства, поставщика услуг или носителя. Например, считываемый компьютером носитель может содержать, в частности, магнитные запоминающие устройства (например, жесткий диск, дискета диск, магнитные полоски…), оптические диски (например, компакт-диск (CD), цифровой универсальный диск (DVD)…), смарт-карты и устройства флэш-памяти (например, карточка, карта памяти, миниатюрное запоминающее устройство…). Конечно, специалисты в данной

области техники должны понимать, что в приведенной конфигурации могут быть сделаны многочисленные изменения, не отступая от контекста или сущности заявленного предмета изобретения.

Термин ″или″, как он используется в настоящей заявке, предназначен означать содержащее ″или″, а не исключающее ″или″. То есть, если не указано иначе или не следует четко из контекста, выражение ″X использует A или B″ подразумевает любую из естественных содержащихся перестановок. То есть, если X использует A; то X использует B; или X использует как A, так и B, то тогда ″X использует A или B″ удовлетворяется в любом из предшествующих случаев. Кроме того, неопределенные артикли, как они используются в настоящей заявке и прилагаемой формуле изобретения, должны обычно рассматриваться как означающие ″один или более″, если не указано иначе или если из контекста четко не следует, что они относятся к единственному числу. Хотя предмет изобретения был описан на языке, конкретно определенном для структурных признаков и/или методологических действий, следует понимать, что предмет изобретения, определенный в приложенной формуле изобретения, не обязательно ограничивается конкретными признаками или описанными действиями. Конкретные признаки и действия раскрываются скорее в форме примера реализации формулы изобретения.

Формула изобретения

1. Способ звуковой авторизации для регистрации в беспроводной сети, содержащий этапы, на которых:

запрашивают регистрацию в беспроводной сети с помощью беспроводного устройства, стремящегося зарегистрироваться в беспроводной сети, при этом беспроводное устройство пока еще неавторизированно беспроводной сетью;

принимают в ответ на запрос отказ в регистрации;

в ответ на получение отказа в регистрации:

получают секретный код, который уникальным образом идентифицирует беспроводное устройство;

акустически излучают секретный код с помощью беспроводного устройства;

в ответ на акустическое излучение принимают одобрение запроса регистрации через беспроводную сеть с помощью беспроводного устройства;

в ответ на прием одобрения регистрации регистрируют беспроводное устройство в беспроводной сети;

определяют выбор языка среди множества языков, доступных на беспроводном устройстве;

преобразуют кодированную компьютером версию секретного кода в звуковую версию секретного кода, в котором звуковая версия секретного кода выполнена на понятном человеку языке, соответствующем выбору определенного языка.

2. Способ по п. 1, в котором этап получения включает получение кодированной компьютером версии секретного кода, хранящегося в памяти неавторизованного беспроводного устройства.

3. Способ по п. 1, в котором этап получения включает динамически генерируемую кодированную компьютером версию секретного кода.

4. Способ по п. 1, в котором этап получения включает получение кодированной компьютером версии секретного кода и способ дополнительно содержит

преобразование кодированной компьютером версии секретного кода в звуковую версию секретного кода.

5. Способ по п. 1, дополнительно содержащий прием одних или более сетевых учетных данных для регистрации в беспроводной сети.

6. Способ по п. 1, в котором секретный код глобально идентифицирует беспроводное устройство.

7. Способ звуковой авторизации для регистрации в беспроводной сети, содержащий этапы, на которых:

получают секретный код, который уникальным образом идентифицирует беспроводное устройство, стремящееся зарегистрироваться в беспроводной сети, при этом беспроводное устройство пока еще неавторизированно беспроводной сетью;

акустически излучают секретный код с помощью беспроводного устройства;

в ответ на акустическое излучение принимают одобрение запроса регистрации через беспроводную сеть с помощью беспроводного устройства;

в ответ на прием одобрения регистрации регистрируют беспроводное устройство в беспроводной сети, и

определяют выбор языка на основании ввода пользователя;

преобразуют кодированную компьютером версию секретного кода в звуковую версию секретного кода, в котором звуковая версия секретного кода выполнена на понятном человеку языке, соответствующем выбору определенного языка.

8. Способ звуковой авторизации для регистрации в беспроводной сети, содержащий этапы, на которых:

получают звуковую версию персонального идентификационного номера (PIN-кода), который уникальным образом идентифицирует беспроводное устройство, стремящееся зарегистрироваться в беспроводной сети, при этом беспроводное устройство пока еще неавторизировано беспроводной сетью;

преобразуют звуковую версию PIN-кода в кодированную компьютером версию PIN-кода;

подтверждают достоверность кодированной компьютером версии PIN-кода;

в ответ на подтверждение, что правильность PIN-кода подтверждена, инициируют регистрацию беспроводного устройства в беспроводной сети, и

определяют выбор языка среди множества языков, доступных на беспроводном устройстве;

преобразуют кодированную компьютером версию PIN-кода в звуковую версию PIN-кода, в котором звуковая версия PIN-кода выполнена на понятном человеку языке, соответствующем выбору определенного языка.

9. Способ по п. 8, перед получением дополнительно содержащий этап, на котором принимают индикацию, что появляется звуковая версия PIN-кода.

10. Способ по п. 8, после получения дополнительно содержащий этап, на котором отправляют подтверждение приема звуковой версии PIN-кода.

11. Способ по п. 8, дополнительно содержащий после подтверждения этап, на котором посылают подтверждение, что звуковая версия PIN-кода прошла проверку.

12. Способ по п. 8, в котором получение содержит получение слышимого звука, излучаемого неавторизованным беспроводным устройством, и хранение звука в качестве звуковой версии PIN-кода.

13. Беспроводное устройство для регистрации в беспроводной сети, содержащее:

память, выполненную с возможностью хранения кодированной компьютером версии персонального идентификационного номера (PIN-кода), который уникальным образом идентифицирует беспроводное устройство, когда беспроводное устройство стремится зарегистрироваться в беспроводной сети;

один или более громкоговорителей, выполненных с возможностью акустического излучения звука;

диспетчер PIN-кодов, выполненный с возможностью получения кодированной компьютером версии PIN-кода, хранящейся в памяти и определения выбора языка среди множества языков, доступных на беспроводном устройстве;

преобразования кодированной компьютером версии PIN-кода в звуковую версию PIN-кода, в котором звуковая версия PIN-кода выполнена на понятном человеку языке, соответствующем выбору определенного языка

аудиодиспетчер, выполненный с возможностью преобразования кодированной компьютером версия PIN-кода в звуковую версию PIN-кода, при этом звуковая версия выполнена на понятном человеку языке, соответствующем выбору определенного языка, и управления излучением звуковой версии PIN-кода через один или более динамиков;

диспетчер по регистрации, выполненный с возможностью управления регистрацией беспроводного устройства в беспроводной сети и дополнительно выполненный с возможностью:

запроса регистрации в беспроводной сети с помощью беспроводного устройства;

приема в ответ на запрос отказа в регистрации;

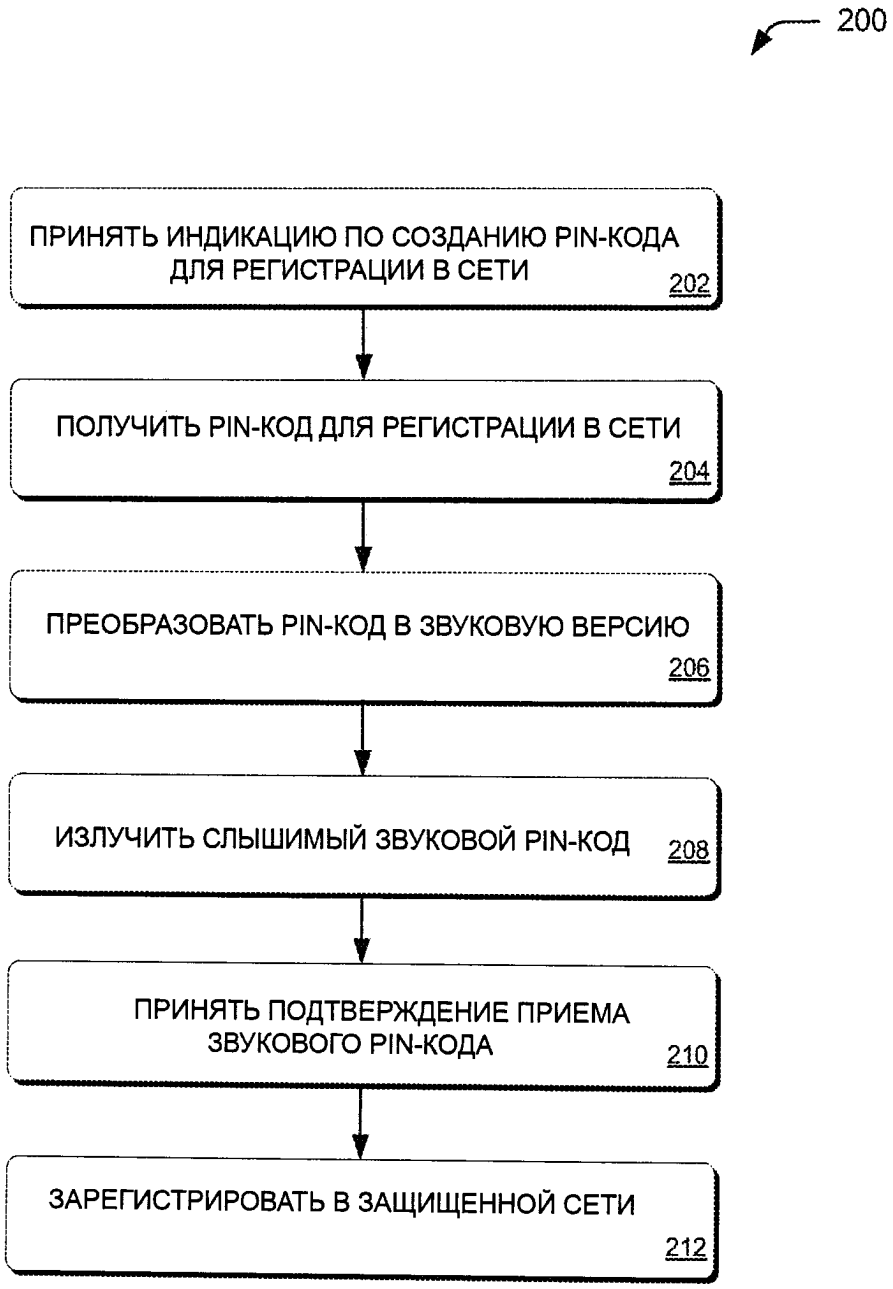
в ответ на получение отказа в регистрации запуска диспетчера PIN-кодов для получения PIN и аудиодиспетчера для преобразования кодированной компьютером версии PIN-кода в звуковую версию PIN-кода и управления акустическим излучением звуковой версии PIN-кода через один или более динамиков;

в ответ на акустическое излучение приема одобрения запроса регистрации через беспроводную сеть с помощью беспроводного устройства;

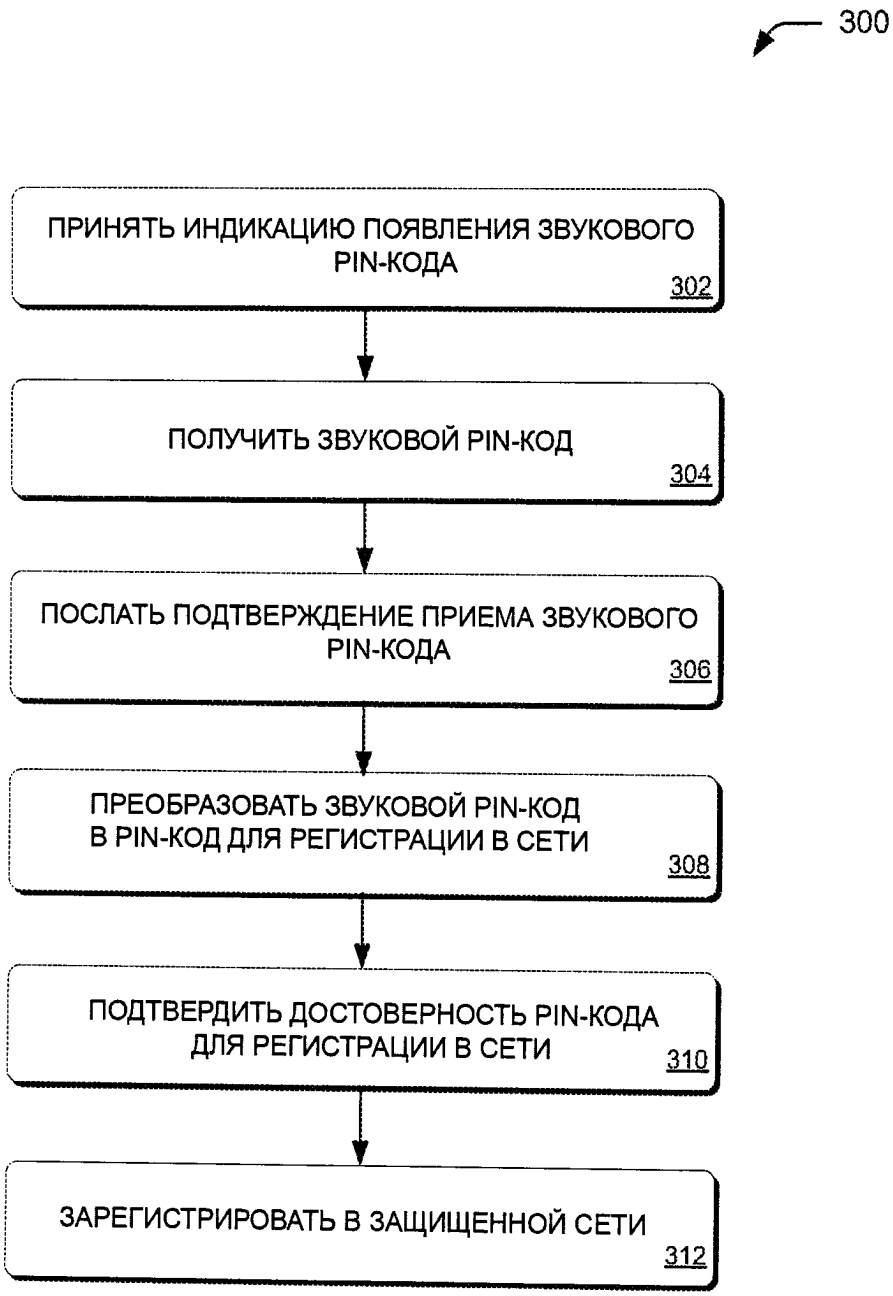
в ответ на прием одобрения регистрации регистрации беспроводного устройства в беспроводной сети.

14. Устройство по п. 13, в котором диспетчер PIN-кодов дополнительно выполнен с возможностью создания кодированной компьютером версии PIN-кода.

15. Устройство по п. 13, в котором у беспроводного устройства отсутствует визуальный дисплей для отображения PIN-кода на экране для пользователя.


200
ПРИНЯТЬ ИНДИКАЦИЮ ПО СОЗДАНИЮ PIN-КОДА ДЛЯ РЕГИСТРАЦИИ В СЕТИ
202
ПОЛУЧИТЬ PIN-КОД ДЛЯ РЕГИСТРАЦИИ В СЕТИ
204
ПРЕОБРАЗОВАТЬ PIN-КОД В ЗВУКОВУЮ ВЕРСИЮ
206
ИЗЛУЧИТЬ СЛЫШИМЫЙ ЗВУКОВОЙ PIN-КОД
208
ПРИНЯТЬ ПОДТВЕРЖДЕНИЕ ПРИЕМА ЗВУКОВОГО PIN-КОДА
210
ЗАРЕГИСТРИРОВАТЬ В ЗАЩИЩЕННОЙ СЕТИ
212

Фиг. 2


300
ПРИНЯТЬ ИНДИКАЦИЮ ПОЯВЛЕНИЯ ЗВУКОВОГО PIN-КОДА
302
ПОЛУЧИТЬ ЗВУКОВОЙ PIN-КОД
304
ПОСЛАТЬ ПОДТВЕРЖДЕНИЕ ПРИЕМА ЗВУКОВОГО PIN-КОДА
306
ПРЕОБРАЗОВАТЬ ЗВУКОВОЙ PIN-КОД В PIN-КОД ДЛЯ РЕГИСТРАЦИИ В СЕТИ
308
ПОДТВЕРДИТЬ ДОСТОВЕРНОСТЬ PIN-КОДА ДЛЯ РЕГИСТРАЦИИ В СЕТИ
310
ЗАРЕГИСТРИРОВАТЬ В ЗАЩИЩЕННОЙ СЕТИ
312

Фиг. 3