РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 739 732**(13) **C2**

(51) МПК
G06F 21/31 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/31 (2020.08)

(21)(22) Заявка: **2017138066, 01.11.2017**

(24) Дата начала отсчета срока действия патента:
01.11.2017

Дата регистрации:
28.12.2020

Приоритет(ы):
(30) Конвенционный приоритет:
04.11.2016 EP 16306445.4;
06.06.2017 EP 17305661.5

(43) Дата публикации заявки: **06.05.2019** Бюл. № 13

(45) Опубликовано: **28.12.2020** Бюл. № 1

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ЛЕ СКУАРНЕК Николя (FR),
НОЙМАНН Кристоф (FR),
ЭН Оливье (FR)

(73) Патентообладатель(и):
ИНТЕРДИДЖИТАЛ СЕ ПЭЙТЕНТ ХОЛДИНГЗ (FR)

(56) Список документов, цитированных в отчете о поиске: **IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan Area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 12.06.2003, [найдено: 13.11.2020]. Найдено в:** (см. прод.)

(54) УСТРОЙСТВА И СПОСОБЫ ДЛЯ АУТЕНТИФИКАЦИИ КЛИЕНТСКОГО УСТРОЙСТВА

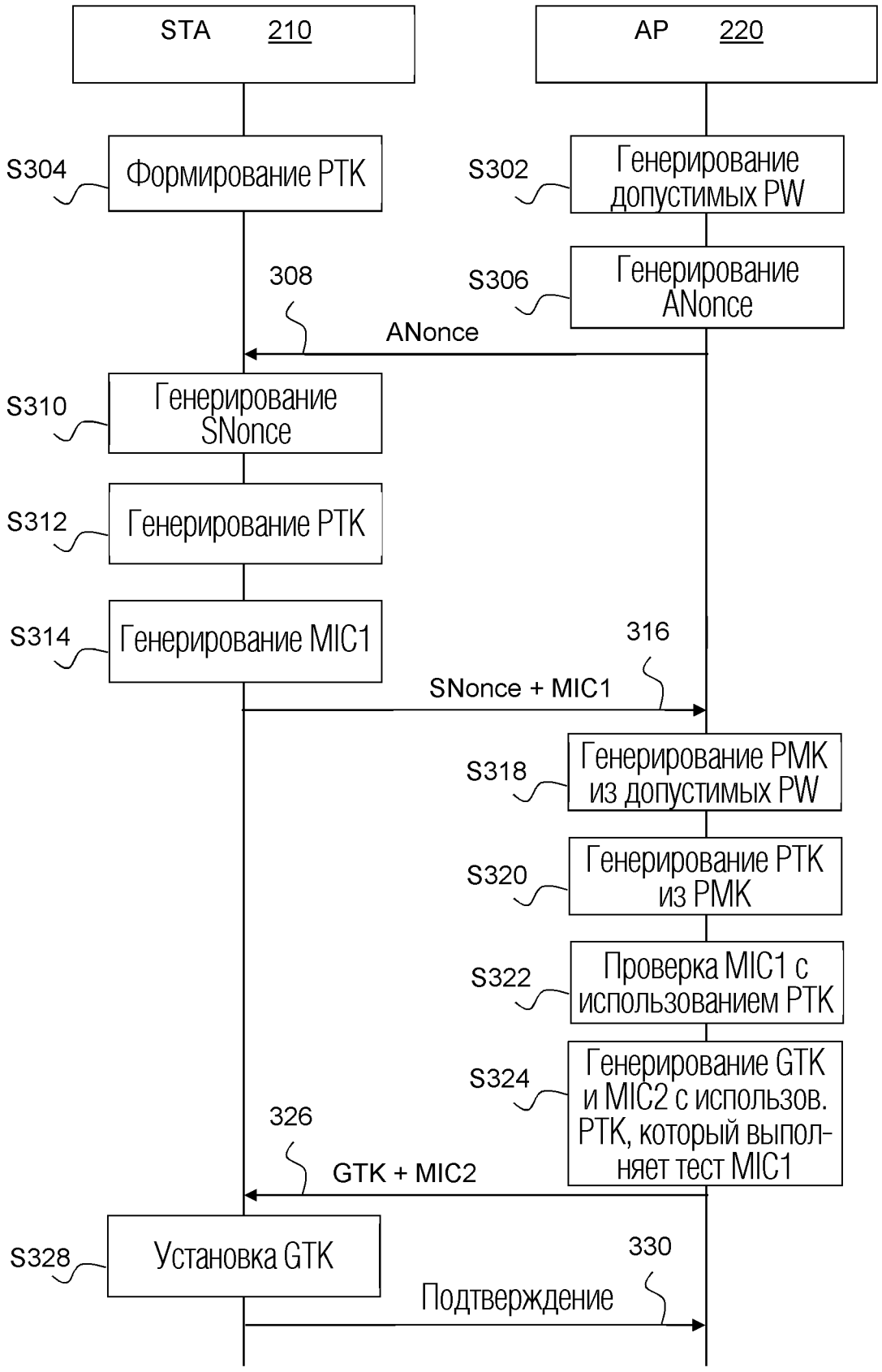
(57) Реферат:

Изобретение относится к области защиты данных в сети и, в частности, к аутентификации клиентского устройства в сетях. Техническим результатом является обеспечение доступа к точке доступа только для авторизованных клиентских устройств. Технический результат заявляемого технического решения достигается тем, что в точке доступа принимают от клиента первое контрольное слово и первую криптографическую контрольную сумму для первого контрольного слова; формируют первые ключи из каждого сохраненного первичного ввода и, по меньшей мере, одного сохраненного вторичного ввода, при этом как сохраненный первичный ввод, так и, по меньшей мере, один сохраненный вторичный ввод являются либо вторым ключом, либо парольной фразой; проверяют первую криптографическую контрольную сумму с использованием каждого сформированного первого ключа; генерируют третий ключ и вторую криптографическую контрольную сумму, используя сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы; и отправляют третий ключ и вторую криптографическую контрольную сумму клиенту. 3 н. и 9 з.п. ф-лы, 4 ил.

RU 2739732 C2

RU 2739732 C2

RU 2739732 C2



ФИГ. 3

(56) (продолжение):
"https://standards.ieee.org/standard/802_11-1999.html". US 2016/0117494 A1, 28.04.2016. US 2008/0082817 A1, 03.04.2008. CHATTERJEE R. et al.: "pASSWORD tYPOS and How to Correct Them Securely", IEEE Symposium on Security and Privacy, 2016. RU 2571576 C2, 20.12.2015.

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 739 732**(13) **C2**

(51) Int. Cl.
G06F 21/31 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/31 (2020.08)

(21)(22) Application: **2017138066, 01.11.2017**

(24) Effective date for property rights:
01.11.2017

Registration date:
28.12.2020

Priority:
(30) Convention priority:
04.11.2016 EP 16306445.4;
06.06.2017 EP 17305661.5

(43) Application published: **06.05.2019** Bull. № **13**

(45) Date of publication: **28.12.2020** Bull. № **1**

Mail address:
129090, Moskva, ul. B.Spasskaya, 25, stroenie 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
LE SKUARNEK Nikolya (FR),
NOJMANN Kristof (FR),
EN Olive (FR)

(73) Proprietor(s):
INTERDIDZHITAL SE PEJTENT KHOLDINGZ (FR)

RU 2739732 C2

(54) DEVICES AND METHODS FOR AUTHENTICATING A CLIENT DEVICE

(57) Abstract:

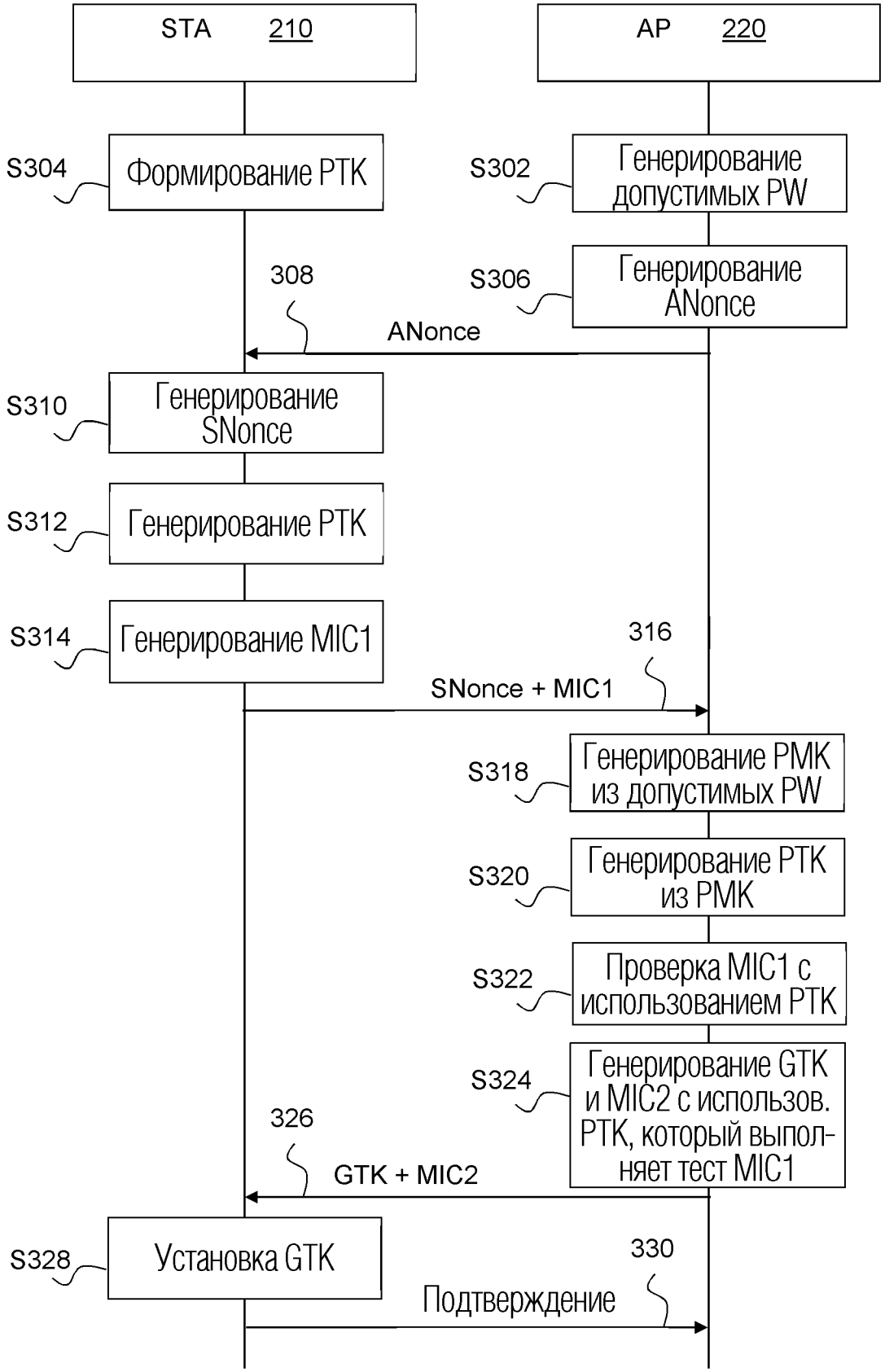
FIELD: data protection in a network.

SUBSTANCE: invention relates to authentication of a client device in networks. Technical result of the proposed technical solution is achieved by the fact that at the access point the first control word and the first cryptographic control sum for the first control word are received from the client; generating first keys from each stored primary input and at least one stored secondary input, wherein both the stored primary input and at least one stored secondary input are either a second key or a password phrase; checking a first cryptographic checksum using each generated first key; generating a third key and a second cryptographic check sum, using generated first key, which performs test of first cryptographic checksum; and sending a third key and a second cryptographic checksum to the client.

EFFECT: providing access to an access point only for authorized client devices.

12 cl, 4 dwg

RU 2739732 C2



ФИГ. 3

RU 2739732 C2

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Настоящее раскрытие изобретения в целом имеет отношение к защите данных в сети и, в частности, к аутентификации клиентского устройства в сетях.

УРОВЕНЬ ТЕХНИКИ

Этот раздел предназначен для ознакомления читателя с различными аспектами уровня техники, которые могут быть связаны с различными аспектами настоящего раскрытия изобретения, которые описываются и/или заявляются ниже. Представляется, что это обсуждение полезно для предоставления читателю справочной информации, чтобы способствовать лучшему пониманию различных аспектов настоящего раскрытия изобретения. Соответственно, следует понимать, что эти утверждения должны быть прочитаны с этой точки зрения, а не как допущение предшествующего уровня техники.

В беспроводных системах связи часто желательно ограничиваться предоставлением доступа к так называемой точке доступа только для авторизованных клиентских устройств. Технология Wi-Fi, наиболее распространенная технология беспроводной сети, будет использоваться в данном документе в качестве неограничивающего иллюстративного примера.

Первое решение для аутентификации клиентских устройств представляет собой использование сертификатов, но поскольку они требуют сложной установки и администрирования, это решение во многих случаях не подходит.

Второе решение использует общий секретный ключ, который пользователь вводит на клиентском устройстве, что становится доказательством знания общего секретного ключа для точки доступа.

Второе решение широко используется, например, в спецификации Wi-Fi Protected Access (WPA) Personal (также известной как WPA-PSK (Pre-Shared Key) - Защищенный доступ Wi-Fi для индивидуальных пользователей, с предварительно выданным общим ключом), имеющую вторую версию, именуемую WPA2 Personal, описанную в стандарте IEEE 802.11i и показанную на Фиг. 1.

На этапах S102 и S104, клиентское устройство STA и точка AP доступа независимо друг от друга формируют парный главный ключ (Pairwise Master Key - PMK), используя функцию формирования ключа под названием Функция формирования ключа на основе пароля, версия 2 (Password-Based Key Derivation Function 2 - PBKDF2), получающую в качестве входа общую парольную фразу, идентификатор сети, именуемый Идентификатор набора служб (Service Set Identifier - SSID), и длину SSID. В качестве альтернативы, PMK может быть введен как строка из 64 шестнадцатеричных цифр.

На этапе S106 AP генерирует случайное число (т.е., контрольное слово) ANonce, которое она отправляет в сообщении 108 на STA.

STA генерирует случайное число (т.е., контрольное слово) SNonce, на этапе S110, и генерирует, на этапе S112, Парный переходный ключ (Pairwise Transient Key - PTK) из контрольных слов, PMK и адресов Управления доступом к среде (Media Access Control - MAC) клиентского устройства STA и точки AP доступа. Затем STA генерирует, на этапе S114, Код целостности сообщения (Message Integrity Code - MIC) для SNonce; MIC является полученной с помощью ключа криптографической контрольной суммой (HMAC-SHA1 или AES-CMAC) для SNonce. MIC использует 128-битный PTK в качестве ключа. Затем STA отправляет SNonce и MIC в сообщении 116 на AP.

После принятия SNonce и MIC, AP формирует PTK, на этапе S118, так же, как и STA на этапе S112. На этапе S120 AP проверяет правильность MIC. На данном этапе STA и AP аутентифицированы, и они взаимно сформировали одинаковый PTK.

AP отправляет на STA сообщение 122, содержащее Групповой временный ключ

(Group Temporal Key - GTK) и порядковый номер, защищенный с использованием второго MIC (зашифрованный с использованием битов 128-256 из PTK). После принятия сообщения 122 STA, на этапе S124, устанавливает GTK, который затем может использоваться для отправки пакетов в беспроводную сеть, которую администрирует AP. В заключение, STA отправляет подтверждение 126 на AP.

Другой возможностью является WPA-Enterprise (WPA для корпоративных пользователей), который работает по-другому, чтобы предложить Расширяемый протокол аутентификации (Extensible Authentication Protocol - EAP). Среди многих протоколов EAP наиболее распространенными являются Защищенный расширяемый протокол аутентификации (Protected Extensible Authentication Protocol - PEAP), Протокол защиты транспортного уровня (Transport Layer Security - TLS) и Туннелированный протокол защиты транспортного уровня (Tunnelled Transport Layer Security - TTLS). Среди них, TLS требует сертификаты как на клиенте, так и на сервере, тогда как TTLS и PEAP довольно похожи, так как оба имеют сертификат на сервере и пароль, вводимый клиентом.

В качестве примера, PEAP использует Протокол аутентификации по квитированию вызова от компании Microsoft, версия 2 (Challenge Handshake Authentication Protocol - MS-CHAP v2) для обмена паролем следующим образом. Клиент и аутентифицирующее устройство (RADIUS-сервер) организуют туннель через AP. Аутентифицирующее устройство отправляет идентификатор сеанса и первый вызов клиенту, который в ответ отправляет имя пользователя, второй вызов и контрольную сумму вызовов, идентификатор сеанса и контрольную сумму MD4 для пароля пользователя. RADIUS-сервер выполняет тест контрольной суммы и дает в ответ успех или отказ, в зависимости от ситуации, и информирует AP о допуске клиента, что заставляет AP инициировать 4-этапное квитирование установления связи с клиентом для применения общего ключа.

Проблема с общими секретными ключами и паролями заключается в том, что их ввод является задачей, которая подвержена ошибкам, в частности, когда данные для ввода являются длинными или сложными, как это часто имеет место для Wi-Fi с целью обеспечить приемлемый уровень безопасности. В попытке устранить эту проблему было предложено использовать технологию Защищенная Установка Wi-Fi (Wi-Fi Protected Setup - WPS). Однако многие устройства, такие как устройства под управлением iOS, не поддерживают WPS, а некоторые реализации WPS наносят ущерб вопросам безопасности, что ограничивает их использование.

В работе "pASSWORD tYPOS and How to Correct Them Securely" ("оПЕЧАТКИ в пАРОЛЕ и как их безопасно исправить"), Чаттерджи (Chatterjee) и др., предлагаются способы аутентификации, которые допускают опечатки в паролях. Хотя в документе и приводится некоторый формальный анализ, но предлагаются только теоретические решения, без предоставления каких-либо реализаций или того, как внедрить такой подход в уже существующий протокол аутентификации.

Другие допускающие опечатки решения были описаны, например, в документах EP 2947591, EP 2876569, EP 3067811, US 2015/0363588 и US 2015/0363593, причем все они требуют доработки клиентского устройства, и US 9280657, в котором сервер обучается признавать ввод, когда за ошибочными паролями следует правильный пароль. Соответственно, эти традиционные решения имеют недостатки.

Другая проблема с общими секретными ключами и паролями в сетях на основе таких технологий как Wi-Fi заключается в том, что они используют один общий секретный ключ или пароль. Если нужно дать, например, гостевой доступ к сети, это тоже делается путем предоставления гостю сетевого пароля. Это означает, что гость может

продолжать получать доступ к сети до тех пор, пока сетевой пароль не будет изменен, что неудобно, так как изменение сетевого пароля требует изменения пароля на каждом устройстве, которое должно иметь доступ к сети.

С другой стороны, шлюз может использовать второй SSID, чтобы предоставить гостю, например, доступ к сети Интернет, но так как второй SSID отличается от первого SSID, это не делает возможным доступ к сети с первым SSID.

Другим решением является использование одноразовых паролей, но они, как правило, не дают гостю доступ к той же сети, которая используется пользователями.

Следует понимать, что желательно иметь решение, которое преодолевает, по меньшей мере, часть традиционных проблем, связанных с вводом общих секретных ключей в сетях беспроводной связи.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

В первом аспекте, рассматриваемые принципы направлены на способ для аутентификации клиента в точке доступа. По меньшей мере, одно аппаратное обрабатывающее устройство точки доступа принимает от клиента первое контрольное слово и первую криптографическую контрольную сумму для первого контрольного слова, при этом первая контрольная сумма вычисляется с использованием первого ключа, сформированного из второго ключа, причем второй ключ вводится на клиенте или формируется из парольной фразы, вводимой на клиенте, формирует первые ключи из каждого сохраненного первичного ввода и, по меньшей мере, одного сохраненного вторичного ввода, действительного на стадии формирования, при этом как сохраненный первичный ввод, так и, по меньшей мере, один сохраненный вторичный ввод являются либо вторым ключом, либо парольной фразой, проверяет криптографическую контрольную сумму с использованием каждого сформированного первого ключа, чтобы найти сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы, генерирует третий ключ и вторую криптографическую контрольную сумму, используя сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы, и отправляет третий ключ и вторую криптографическую контрольную сумму клиенту.

Различные варианты осуществления первого аспекта включают в себя:

Вариант, когда каждый сохраненный вторичный ввод имеет заданный, ограниченный период действия или соответствует первичному вводу, по меньшей мере, с одной ошибкой при наборе. Третий ключ может быть заменен новым, когда сохраненный вторичный ввод становится недействительным.

Вариант, когда точка доступа является точкой доступа Wi-Fi, которая также отправляет второе контрольное слово клиенту, и когда первые ключи дополнительно формируются из первого контрольного слова и второго контрольного слова.

Вариант, когда третий ключ отправляется зашифрованным с использованием ключа шифрования, сгенерированного из сформированного первого ключа, который выполняет тест первой криптографической контрольной суммы.

Во втором аспекте, рассматриваемые принципы направлены на точку доступа, которая включает в себя интерфейс связи, выполненный с возможностью приема от клиента первого контрольного слова и первой криптографической контрольной суммы для первого контрольного слова, при этом первая контрольная сумма вычисляется с использованием первого ключа, сформированного из второго ключа, причем второй ключ вводится на клиенте или формируется из парольной фразы, вводимой на клиенте, и отправки клиенту третьего ключа и второй криптографической контрольной суммы, запоминающее устройство, выполненное с возможностью хранения первичного ввода

и, по меньшей мере, одного вторичного ввода, при этом как сохраненный первичный ввод, так и, по меньшей мере, один сохраненный вторичный ввод являются либо вторым ключом, либо парольной фразой, и, по меньшей мере, одно аппаратное обрабатывающее устройство, выполненное с возможностью формирования первых ключей из каждого сохраненного первичного ввода и, по меньшей мере, одного вторичного ввода, действительного на стадии формирования, проверки криптографической контрольной суммы с использованием каждого сформированного первого ключа, чтобы найти сформированный первый ключ, который выполняет тест первой контрольной суммы, и генерирования третьего ключа и второй криптографической контрольной суммы, используя сформированный первый ключ, который выполняет тест первой контрольной суммы.

Различные варианты осуществления второго аспекта включают в себя:

Вариант, когда каждый сохраненный вторичный ввод имеет заданный, ограниченный период действия или соответствует первичному вводу, по меньшей мере, с одной ошибкой при наборе. Третий ключ может быть заменен новым, когда сохраненный вторичный ввод становится недействительным.

Вариант, когда точка доступа является точкой доступа Wi-Fi, и когда интерфейс связи выполнен с дополнительной возможностью отправки второго контрольного слова клиенту, и в котором, по меньшей мере, одно аппаратное обрабатывающее устройство выполнено с возможностью дополнительного формирования первых ключей из первого контрольного слова и второго контрольного слова. По меньшей мере, одно аппаратное обрабатывающее устройство может быть выполнено с дополнительной возможностью формирования первых ключей из сохраненного вторичного ввода только в течение периода действия для сохраненного вторичного ввода.

Вариант, когда, по меньшей мере, одно аппаратное обрабатывающее устройство выполнено с дополнительной возможностью шифрования третьего ключа с использованием ключа шифрования, сгенерированного из сформированного первого ключа, который выполняет тест первой криптографической контрольной суммы, перед передачей клиенту.

В третьем аспекте, рассматриваемые принципы направлены на способ для аутентификации клиентского устройства на аутентифицирующем устройстве, поддерживающем спецификацию Wi-Fi Protected Access 2 Enterprise, посредством отправки на клиентское устройство идентификатора сеанса и первого вызова, приема от клиентского устройства имени пользователя, второго вызова и криптографической контрольной суммы для первого вызова, второго вызова, идентификатора сеанса и парольной фразы, проверки, выполняет ли действительная сохраненная первичная парольная фраза или, по меньшей мере, одна действительная сохраненная вторичная парольная фраза тест криптографической контрольной суммы, при этом каждая сохраненная вторичная парольная фраза действительна в течение ограниченного заданного периода действия, или каждый сохраненный вторичный ввод соответствует первичному вводу, по меньшей мере, с одной ошибкой при наборе, и в случае, если парольная фраза выполняет тест криптографической контрольной суммы, отправки на клиентское устройство сообщения, сигнализирующего об успешной аутентификации, и выполнения квитирования установления связи с клиентским устройством для применения ключа.

В четвертом аспекте, рассматриваемые принципы направлены на аутентифицирующее устройство, поддерживающее спецификацию Wi-Fi Protected Access 2 Enterprise, которое включает в себя интерфейс связи, выполненный с возможностью отправки на клиентское

устройство идентификатора сеанса и первого вызова, и приема от клиентского устройства имени пользователя, второго вызова и криптографической контрольной суммы для первого вызова, второго вызова, идентификатора сеанса и парольной фразы, и, по меньшей мере, одно аппаратное обрабатывающее устройство, выполненное с возможностью проверки, выполняет ли действительная сохраненная первичная парольная фраза или, по меньшей мере, одна действительная сохраненная вторичная парольная фраза тест криптографической контрольной суммы, при этом каждая сохраненная вторичная парольная фраза действительна в течение ограниченного заданного периода действия, или каждый сохраненный вторичный ввод соответствует первичному вводу, по меньшей мере, с одной ошибкой при наборе, и в случае, если парольная фраза выполняет тест криптографической контрольной суммы, отправки на клиентское устройство, через интерфейс связи, сообщения, сигнализирующего об успешной аутентификации, и выполнения квитирования установления связи с клиентским устройством для применения ключа.

В пятом аспекте, рассматриваемые принципы направлены на компьютерную программу, содержащую инструкции в виде программного кода, исполняемые обрабатывающим устройством для реализации этапов способа в соответствии с любым вариантом осуществления первого аспекта.

В шестом аспекте, рассматриваемые принципы направлены на компьютерный программный продукт, который хранится на долговременном машиночитаемом носителе и содержит инструкции в виде программного кода, исполняемые обрабатывающим устройством для реализации этапов способа в соответствии с любым вариантом осуществления первого аспекта.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Далее будут описаны предпочтительные признаки настоящих принципов, в качестве неограничивающего примера, со ссылкой на прилагаемые чертежи, на которых:

Фиг. 1 показывает традиционный протокол Wi-Fi Protected Access (WPA) Personal;

Фиг. 2 показывает иллюстративную систему в соответствии с первым вариантом осуществления настоящих принципов;

Фиг. 3 показывает иллюстративный способ для включения в сеть устройства в соответствии с одним из вариантов осуществления настоящих принципов; и

Фиг. 4 показывает иллюстративный способ для включения в сеть устройства в соответствии с дополнительным вариантом осуществления настоящих принципов.

ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Фиг. 2 показывает иллюстративную систему 200 в соответствии с первым вариантом осуществления настоящих принципов. Система 200 содержит клиентское устройство (STA) 210, а также точку доступа (AP) 220, такую как шлюз. Точка 220 доступа выполняется с возможностью взаимодействия с локальной сетью 240 и внешней сетью 250, такой как сеть Интернет, через которые могут быть установлены соединения с устройствами в другой сети (не показано). В иллюстративной системе локальная сеть 240 является сетью Wi-Fi.

Клиентское устройство 210, как и точка 220 доступа, включает в себя, по меньшей мере, один аппаратный блок 211, 221 обработки ("обрабатывающее устройство"), запоминающее устройство 212, 222 и, по меньшей мере, один интерфейс 213, 223 связи, в этом примере интерфейс Wi-Fi, выполненный с возможностью установления связи с другими устройствами. Специалисту в данной области техники будет понятно, что показанные устройства очень упрощены для наглядности, и что реальные устройства в дополнение включают в себя такие признаки, как внутренние соединения и источники

питания. Долговременные носители 260 данных хранят инструкции, которые, при исполнении обрабатывающим устройством, выполняют функции точки 220 доступа, как дополнительно описано ниже.

Клиентское устройство 210, возможно подключенное к локальной сети 240, дополнительно включает в себя пользовательский интерфейс 214. Клиентское устройство может быть, например, дорожным компьютером, интеллектуальным телефоном или планшетным компьютером.

Точка 220 доступа выполняется с возможностью выполнения традиционных функций точки доступа, таких как обеспечение взаимодействия с локальной сетью 240 и внешней сетью 250. Множество клиентских устройств может быть подключено к локальной сети 240 или через нее, или одна локальная сеть, в качестве точки 220 доступа, может предлагать множество локальных сетей, к примеру в виде изолированных подсетей. Как правило, любому устройству, которое доказывает знание общего сетевого секретного ключа, такого как сетевой ключ, предоставляется доступ к локальной сети 240.

Внешняя сеть 250 может использоваться для подключения к серверам и другим устройствам, возможно, через другие точки доступа (не показано).

Фиг. 3 показывает иллюстративный способ для включения в сеть устройства в соответствии с одним из вариантов осуществления настоящих принципов.

На этапе S302 обрабатывающее устройство 221 точки 220 доступа ("AP") генерирует ограниченный набор ошибочных, но допустимых парольных фраз из основной парольной фразы, установленной в конфигурации точки 220 доступа, причем этот набор включает в себя основную парольную фразу. Другими словами, обрабатывающее устройство 221 генерирует и сохраняет набор парольных фраз, включающих в себя исходную, правильную, парольную фразу и некоторое количество модифицированных парольных фраз, включающих в себя, по меньшей мере, одну ошибку. Предпочтительно, если вносимые ошибки соответствуют распространенным ошибкам, например, таким (с числом модификаций, включающих в себя исходную парольную фразу для 32-символьной парольной фразы, в скобках):

пропуск символа в любой произвольной позиции (33);

инверсия регистра букв (2);

добавление пробела через каждые 4 символа (9);

замена I (i в верхнем регистре) на l (L в нижнем регистре) (2);

замена 0 (ноль) на O (2);

замена одного символа (любого) одним из 4 ближайших (4*32+1=129);

замена одного или двух символов (любых двух) одним из 4 ближайших

$$\left(\frac{32}{2} * 4 + 32 * 4 + 1 = 2113\right)$$

любая комбинация из них (произведение числа модификаций, 5020488). Отметим, что даже при принятии любой комбинации таких ошибок, это устраняет не более 23 бита энтропии. Если символ является шестнадцатеричным числом (0-9A-F), что распространено в установленных при изготовлении парольных фразах, исходная энтропия составляет 32*4=128 битов. Принятие всех этих ошибок оставляет (по меньшей мере) 105 битов энтропии, чего во многих случаях все еще достаточно.

Для одной из модификаций, обрабатывающее устройство 221 точки 220 доступа ("AP") генерирует набор допустимых парольных фраз, который включает в себя основную, используемую по умолчанию, парольную фразу и, по меньшей мере, одну действительную вторичную парольную фразу. Основная парольная фраза, как правило,

является парольной фразой, которая используется обычными пользователями сети, и она остается действительной, пока не будет изменена, например, пользователем или администратором сети. Вторая парольная фраза используется, например, гостями в сети; ее действие, как правило, ограничено по времени, но она тоже может быть действительной, пока не будет аннулирована.

Для этой модификации, обрабатывающее устройство 221 может быть выполнено с возможностью генерирования вторичных парольных фраз, каждая из которых действительна в течение одного дня. Тогда набор допустимых парольных фраз включает в себя основную парольную фразу и вторичную парольную фразу, действительную для текущего дня. Например, каждый день обрабатывающее устройство может генерировать, используя, к примеру, циклическое однонаправленное хеширование, вторичные парольные фразы для текущего дня и для следующих N дней. Эти вторичные парольные фразы могут отображаться в пользовательском интерфейсе AP (не показано) или отправляться на устройство пользователя, подключенное с использованием основной парольной фразы, для отображения в его ПИ 214, или устройство, на котором запущено специализированное приложение. Благодаря тому, что обрабатывающее устройство 221 генерирует множество вторичных парольных фраз, гостю можно сразу предоставить доступ на несколько дней.

В одном из вариантов осуществления модификации, точка доступа включает в себя "кнопку гостевой WPS". Эта кнопка реализует тот же механизм, что и WPS, за исключением того, что клиент извещается о парольной фразе дня (вместо парольной фразы по умолчанию).

В этом варианте осуществления модификации, пользователь активирует кнопку Wi-Fi Protected Setup на гостевом устройстве, активирует кнопку Wi-Fi Protected Setup на AP 220. Затем AP и гостевой устройство выполняют обмен ключами по методу Диффи-Хеллмана, после чего AP отправляет парольную фразу дня на гостевое устройство, которое использует парольную фразу во время подключения к сети, после чего AP выполняет аутентификацию, как описано выше.

Существенное отличие от традиционного протокола, описанного в отношении Фиг. 1, состоит в том, что точка 220 доступа не обязательно формирует PMK вначале, а может ожидать, пока она не примет SNonce+MIC от клиентского устройства ("STA") 210. Следует отметить, что протокол остается неизменным для клиентского устройства 210.

На этапе S304 клиентское устройство 210 принимает Парный главный ключ (PMK), используя функцию формирования ключа (в этом примере, PBKDF2), получающую в качестве входа входную парольную фразу, идентификатор сети, именуемый Идентификатор набора служб (SSID), и длину SSID. В качестве альтернативы, PMK может быть введен как строка из 64 шестнадцатеричных цифр.

На этапе S306 точка 220 доступа генерирует случайное число ANonce, которое она отправляет в сообщении 308 на клиентское устройство 210.

Клиентское устройство 210 генерирует другое случайное число SNonce, на этапе S310, и генерирует, на этапе S312, Парный переходный ключ (PTK) из контрольных слов, PMK и адресов Управления доступом к среде (MAC) клиентского устройства 210 и точки 220 доступа. Затем клиентское устройство 210 генерирует, на этапе S314, Код целостности сообщения (MIC), MIC1 на Фиг. 3, для SNonce; MIC1 является полученной с помощью ключа криптографической контрольной суммой (HMAC-SHA1 или AES-CMAC) SNonce. MIC использует 128-битный PTK в качестве ключа. Затем клиентское устройство 210 отправляет SNonce и MIC1 в сообщении 316 на точку 220 доступа.

После принятия SNonce и MIC1, точка 220 доступа формирует, на этапе S318, PMK из каждой парольной фразы в наборе допустимых парольных фраз. Сгенерированные PMK могут быть сохранены вместо набора допустимых парольных фраз, или в дополнение к нему. В качестве альтернативы, в случае, когда PMK вводится как строка из 64 шестнадцатеричных цифр, точка 220 доступа формирует и сохраняет допустимые PMK из правильного PMK. Следует отметить, что этот этап может быть выполнен заранее, например, сразу после этапа S302.

На этапе S320 точка 220 доступа генерирует PTK для каждого PMK, сгенерированного на этапе S318, используя тот же способ генерирования, что и клиентское устройство 210 на этапе S312.

На этапе S322 точка 220 доступа проверяет, что MIC1 является правильным для какого-либо PTK, сгенерированного на этапе S320. Если PTK позволяет проверить MIC1, то этот PTK задается как текущий PTK. На этой стадии точка 220 доступа и клиентское устройство 210 аутентифицируются и имеют один и тот же взаимно сформированный PTK (из основной или вторичной парольной фразы). Следует отметить, что если никакой PTK не позволяет проверить MIC, то клиентское устройство 210 не аутентифицируется, как если бы была введена неправильная парольная фраза в традиционном способе, показанном на Фиг. 1.

Точка 220 доступа генерирует, на этапе S324, Групповой временный ключ (GTK) и порядковый номер, защищенный с использованием второго MIC (зашифрованный с использованием битов 128-256 из PTK), MIC2 на Фиг. 3, которые отправляются на клиентское устройство 210 в сообщении 326. После принятия сообщения 326 клиентское устройство 210 устанавливает, на этапе S328, GTK, который затем может использоваться для отправки пакетов в беспроводную сеть, которая администрируется точкой 220 доступа. В заключение, клиентское устройство 210 отправляет подтверждение 330 на точку 220 доступа.

Как можно видеть, точка 220 доступа пытается найти парольную фразу в наборе допустимых парольных фраз, для которой принятый MIC, MIC1, является действительным. Если такая парольная фраза найдена, клиент может быть аутентифицирован, и парольная фраза используется в качестве основы для остальной части обмена (т.е., формирования PTK, шифрования GTK и подписания сообщения).

Предпочтительно, если точка доступа сохраняет PMK, используемый данным клиентским устройством (идентифицированным его MAC-адресом). Другими словами, точка доступа сохраняет PMK, из которого был сгенерирован PTK, который позволил проверить MIC. Таким образом, при следующем подключении клиентского устройства, точка доступа может выбрать сохраненный PMK, что может уменьшить количество предполагаемых паролей при повторных подключениях.

В модификации с ограниченными по времени парольными фразами предпочтительно, если точка 220 доступа аннулирует вторичные ключи, которые более не действительны, например, аннулирует ключ дня, когда день его действия закончен.

Простой подход для аннулирования вторичного ключа состоит в том, что точка 220 доступа заменяет GTK новым всякий раз, когда срок действия вторичного ключа истекает. GTK может быть заменен новым, используя так называемый механизм Квитирования с групповым ключом, заданный в IEEE 802.11i. Конечно, можно использовать и другие подходящие механизмы.

Более сложно организованный подход для аннулирования вторичного ключа состоит в том, что точка 220 доступа отслеживает, использовался ли вторичный ключ гостевым устройством. В случае если вторичный ключ не использовался, нет необходимости

заменять GTK новым при истечении срока действия вторичного ключа. GTK заменяется новым, например, используя механизм квитирования с групповым ключом, только когда вторичный ключ с истекшим сроком действия использовался во время действия этого вторичного ключа.

Настоящие принципы распространяются и на случай WPA2 Enterprise на основе пароля (PEAP/EAP-TTLS). Что касается Wi-Fi, подставляется набор допустимых паролей, чтобы определить, успешна аутентификация или нет.

Фиг. 4 показывает иллюстративный способ для включения в сеть устройства в соответствии с дополнительным вариантом осуществления настоящих принципов.

Фиг. 4 показывает клиентское устройство 210, которое может быть идентично клиентскому устройству на Фиг. 2. Чертеж также демонстрирует аутентифицирующее устройство 230, которое, хотя это и не показано для краткости, включает в себя, по меньшей мере, один аппаратный блок обработки ("обрабатывающее устройство"), запоминающее устройство и, по меньшей мере, один интерфейс связи, выполненный с возможностью установления связи с другими устройствами.

На этапе S402 клиентское устройство 210 организует, через точку доступа (220 на Фиг. 2), туннель по протоколу защиты транспортного уровня (TLS) с аутентифицирующим устройством 230, таким как RADIUS-сервер. Аутентифицирующее устройство 230 отправляет, в сообщении 404, Идентификатор сеанса (Session ID - SId) и Вызов (ACh) на клиентское устройство 210. Клиентское устройство 210 генерирует, на этапе S406, сообщение 408 с Именем пользователя, Вызовом (SCh) и контрольной суммой MD4 вызовов (Ach, SCh), Идентификатора сеанса (SId) и пароля пользователя. Сообщение 408 отправляется на аутентифицирующее устройство 230. До этого момента способ соответствует традиционному способу.

На этапе S410 аутентифицирующее устройство 230 сверяет, выполняет ли какой-либо пароль пользователя в наборе допустимых паролей пользователя для этого пользователя тест контрольной суммы H; другими словами, идентична ли вычисленная контрольная сумма MD4 вызовов (Ach, SCh), идентификатора сеанса (SId) и пароля пользователя в наборе допустимых паролей пользователя контрольной сумме H, принятой в сообщении 408.

Затем аутентифицирующее устройство 230 отправляет сообщение 412 на клиентское устройство 210. Если никакой пароль в наборе не выполняет тест контрольной суммы H, то сообщение 412 сигнализирует об отказе, клиентское устройство 210 не аутентифицируется, и способ заканчивается. Однако, если пароль выполняет тест контрольной суммы H, то сообщение 412 сигнализирует об успехе, и клиентское устройство 210 аутентифицируется. Затем клиентское устройство 210 и аутентифицирующее устройство инициируют, на этапе S414, традиционное 4-этапное квитирование для применения ключа.

Следует иметь в виду, что настоящие принципы работают с существующими клиентами и лишь требуется доработка, в зависимости от варианта осуществления, на точках доступа или RADIUS-серверах. Кроме того, поскольку исходная парольная фраза или пароль являются частью набора, способы обратно совместимы.

Следует понимать, что элементы, продемонстрированные на чертежах, могут быть реализованы в различных формах аппаратного обеспечения, программного обеспечения, или их комбинаций. Предпочтительно, если эти элементы реализованы в комбинации аппаратного и программного обеспечения на одном или нескольких соответствующим образом запрограммированных устройствах общего назначения, которые могут включать в себя обрабатывающее устройство, запоминающее устройство и интерфейсы

ввода/вывода.

Настоящее описание поясняет принципы настоящего раскрытия изобретения. Таким образом, будет понятно, что специалисты в данной области техники будут способны разработать различные конструкции, которые, хотя не описаны или продемонстрированы явно в данном документе, воплощают принципы настоящего раскрытия изобретения и входят в его объем.

Все примеры и обусловленные формулировки, приведенные в данном документе, предназначены для образовательных целей, чтобы помочь читателю в понимании принципов настоящего раскрытия изобретения и концепций, внесенных автором изобретения для развития области техники, и должны толковаться как не имеющие ограничений на такие конкретные приведенные примеры и условия.

Более того, все утверждения в данном документе, в которых излагаются принципы, аспекты и варианты осуществления настоящего раскрытия изобретения, а также их конкретные примеры, предназначены для охвата как структурных, так и функциональных их эквивалентов. Дополнительно, предполагается, что такие эквиваленты включают в себя как известные в настоящее время эквиваленты, так и эквиваленты, разработанные в будущем, т.е. любые разработанные элементы, которые выполняют ту же функцию, независимо от структуры.

Таким образом, например, специалистам в данной области техники будет понятно, что структурные схемы, представленные в данном документе, дают концептуальные представления об иллюстративных компонентах схем, воплощающих принципы настоящего раскрытия изобретения. Точно так же будет понятно, что любые блок-схемы, функциональные диаграммы, диаграммы переходов состояний, псевдокод, и т.п., представляют различные технологические процессы, которые могут быть по существу представлены на машиночитаемом носителе, а значит исполняться компьютером или обрабатывающим устройством, независимо от того, продемонстрирован такой компьютер или обрабатывающее устройство явно, или нет.

Функции различных элементов, продемонстрированных на чертежах, могут быть обеспечены посредством использования специализированного аппаратного обеспечения, а также аппаратного обеспечения, способного исполнять программное обеспечение, в сочетании с соответствующим программным обеспечением. Когда это обеспечивается обрабатывающим устройством, функции могут быть обеспечены одним специализированным обрабатывающим устройством, одним совместно используемым обрабатывающим устройством, или множеством отдельных обрабатывающих устройств, некоторые из которых могут использоваться совместно. Более того, явное использование термина "обрабатывающее устройство" или "управляющее устройство" не должно толковаться как относящееся исключительно к аппаратному обеспечению, способному исполнять программное обеспечение, и может по смыслу включать в себя, без ограничения, аппаратное обеспечение устройства цифровой обработки сигнала (ЦОС), постоянное запоминающее устройство (ПЗУ) для хранения программного обеспечения, оперативное запоминающее устройство (ОЗУ) и энергонезависимое хранилище.

Другое аппаратное обеспечение, традиционное и/или нестандартное, тоже может быть предусмотрено. Точно так же, любые переключатели, продемонстрированные на чертежах, являются только концептуальными. Их функция может выполняться посредством работы программной логики, посредством специализированной логики, посредством взаимодействия программного управления и специализированной логики, или даже вручную, при этом конкретные технические методы могут быть выбраны разработчиком, что более конкретно понято из контекста.

В формуле изобретения данного документа любой элемент, выраженный в виде средства для выполнения определенной функции, предполагает охват любого метода выполнения этой функции, в том числе, например, a) комбинация элементов схемы, которая выполняет эту функцию, или b) программное обеспечение в любой форме, в том числе, соответственно, программно-аппаратное обеспечение, набор микрокоманд или тому подобное, в сочетании с подходящей для этого схемой для исполнения этого программного обеспечения, чтобы выполнить функцию. Настоящее раскрытие изобретения, как определено такой формулой изобретения, заключается в том, что функциональные возможности, обеспечиваемые различными перечисленными средствами, объединяются и согласуются так, как предписано формулой изобретения. Таким образом, считается, что любое средство, которое может обеспечить эти функциональные возможности, эквивалентно продемонстрированному в данном документе.

(57) Формула изобретения

1. Способ для аутентификации клиента в точке (220) доступа, причем способ содержит этапы, на которых посредством, по меньшей мере, одного аппаратного обрабатывающего устройства (221) точки (220) доступа:

принимают от клиента (210) первое контрольное слово и первую криптографическую контрольную сумму для первого контрольного слова, при этом первая криптографическая контрольная сумма вычислена с использованием первого ключа, сформированного из второго ключа, причем второй ключ введен на клиенте или сформирован из парольной фразы, введенной на клиенте;

формируют (S318, S320) первые ключи из каждого сохраненного первичного ввода и, по меньшей мере, одного сохраненного вторичного ввода, при этом как сохраненный первичный ввод, так и, по меньшей мере, один сохраненный вторичный ввод являются либо вторым ключом, либо парольной фразой;

проверяют (S322) первую криптографическую контрольную сумму с использованием каждого сформированного первого ключа, чтобы найти сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы;

генерируют (S324) третий ключ и вторую криптографическую контрольную сумму, используя сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы; и

отправляют третий ключ и вторую криптографическую контрольную сумму клиенту;

при этом каждый сохраненный вторичный ввод имеет заданный, ограниченный период действия и действителен на этапе формирования.

2. Способ по п. 1, в котором точка (210) доступа является точкой доступа Wi-Fi, и способ также содержит этап, на котором отправляют (S308) второе контрольное слово клиенту (210), и в котором первые ключи также формируются из первого контрольного слова и второго контрольного слова.

3. Способ по п. 1, в котором третий ключ отправляется зашифрованным с использованием ключа шифрования, сгенерированного из сформированного первого ключа, который выполняет тест первой криптографической контрольной суммы.

4. Способ по п. 1, содержащий также этап, на котором заменяют третий ключ новым, когда сохраненный вторичный ввод становится недействительным, при этом третий ключ может быть использован для отправки пакетов в беспроводную сеть, которая администрируется точкой доступа.

5. Способ по п. 1, в котором сохраненный первичный ввод является парольной

фразой, используемой обычными пользователями сети, и сохраненный вторичный ввод используется гостями в сети.

6. Точка (220) доступа, содержащая:

интерфейс (223) связи, выполненный с возможностью:

приема от клиента (210) первого контрольного слова и первой криптографической контрольной суммы для первого контрольного слова, при этом первая криптографическая контрольная сумма вычислена с использованием первого ключа, сформированного из второго ключа, причем второй ключ введен на клиенте (210) или сформирован из парольной фразы, введенной на клиенте (210); и

отправки клиенту (210) третьего ключа и второй криптографической контрольной суммы;

запоминающее устройство (222), выполненное с возможностью хранения первичного ввода и, по меньшей мере, одного вторичного ввода, при этом как сохраненный первичный ввод, так и, по меньшей мере, один сохраненный вторичный ввод являются либо вторым ключом, либо парольной фразой; и

по меньшей мере, одно аппаратное обрабатывающее устройство (221), выполненное с возможностью:

формирования первых ключей из каждого сохраненного первичного ввода и, по меньшей мере, одного вторичного ввода;

проверки первой криптографической контрольной суммы с использованием каждого сформированного первого ключа, чтобы найти сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы; и

генерирования третьего ключа и второй криптографической контрольной суммы, используя сформированный первый ключ, который выполняет тест первой криптографической контрольной суммы;

при этом каждый сохраненный вторичный ввод имеет заданный, ограниченный период действия и действителен на этапе формирования.

7. Точка доступа по п. 6, в которой точка (210) доступа является точкой доступа Wi-Fi, и интерфейс связи (223) выполняется с дополнительной возможностью отправки второго контрольного слова клиенту (210), и в которой, по меньшей мере, одно аппаратное обрабатывающее устройство (221) выполняется с возможностью формирования первых ключей дополнительно из первого контрольного слова и второго контрольного слова.

8. Точка доступа по п. 6, в которой, по меньшей мере, одно аппаратное обрабатывающее устройство (221) выполняется с дополнительной возможностью шифрования третьего ключа с использованием ключа шифрования, сгенерированного из сформированного первого ключа, который выполняет тест первой криптографической контрольной суммы, перед передачей клиенту (210).

9. Точка доступа по п. 7, в которой, по меньшей мере, одно аппаратное обрабатывающее устройство (221) выполняется с дополнительной возможностью формирования первых ключей из сохраненного вторичного ввода только в течение периода действия для сохраненного вторичного ввода.

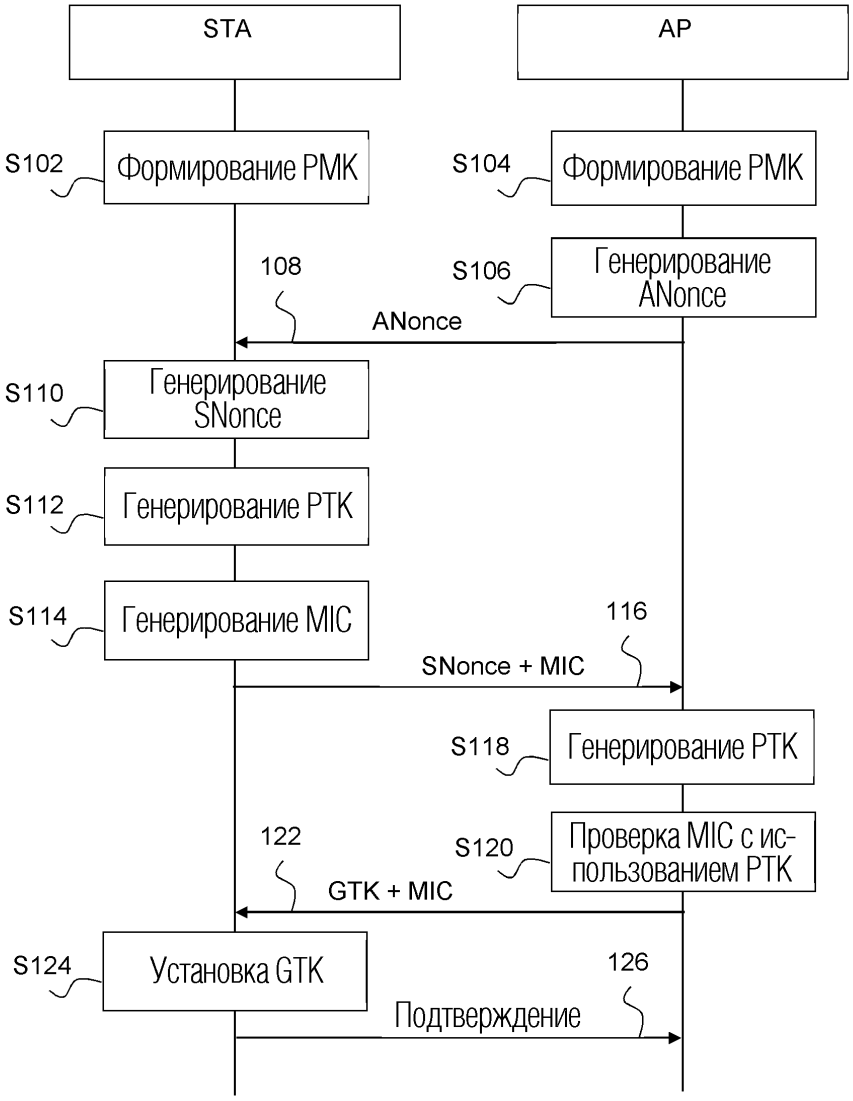
10. Точка доступа по п. 6, в которой, по меньшей мере, одно аппаратное обрабатывающее устройство (221) выполняется с дополнительной возможностью замены третьего ключа новым, когда сохраненный вторичный ввод становится недействительным, при этом третий ключ может быть использован для отправки пакетов в беспроводную сеть, которая администрируется точкой доступа.

11. Точка доступа по п. 6, в которой сохраненный первичный ввод является парольной

фразой, используемой обычными пользователями сети и сохраненный вторичный ввод используется гостями в сети.

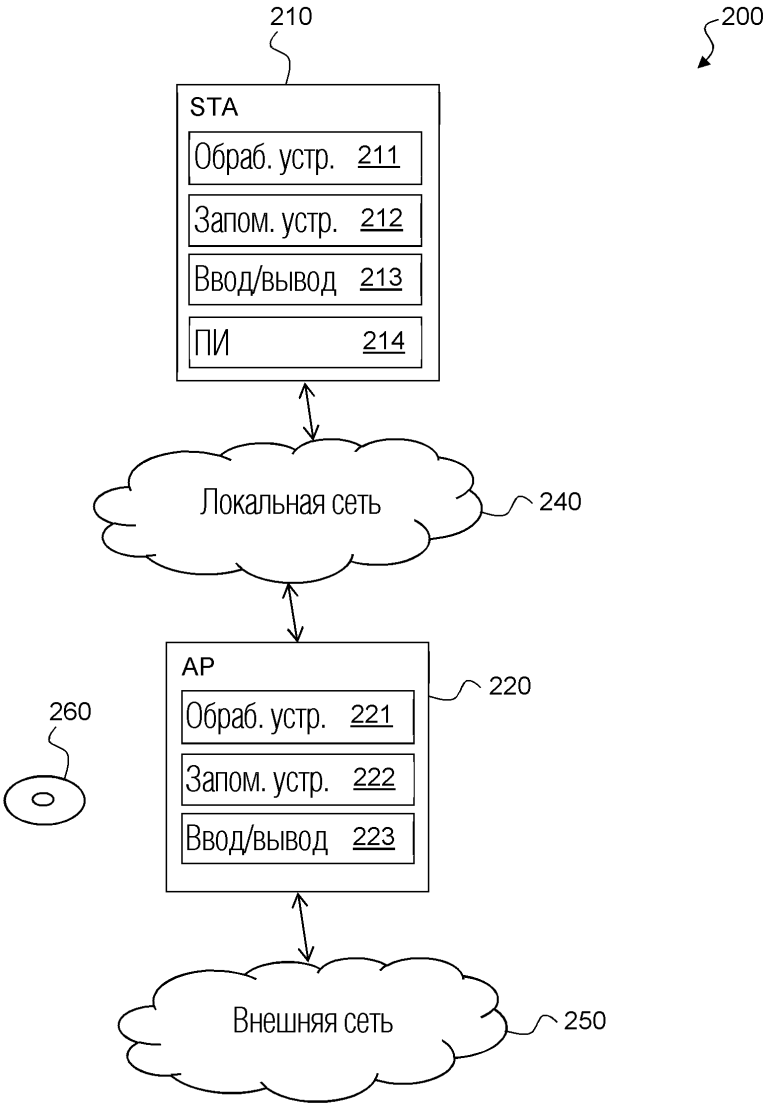
12. Долговременный машиночитаемый носитель, содержащий инструкции в виде программного кода, исполняемые обрабатывающим устройством для реализации этапов способа, по меньшей мере, по одному из пп. 1-5.

1



ФИГ. 1
(предшествующий уровень техники)

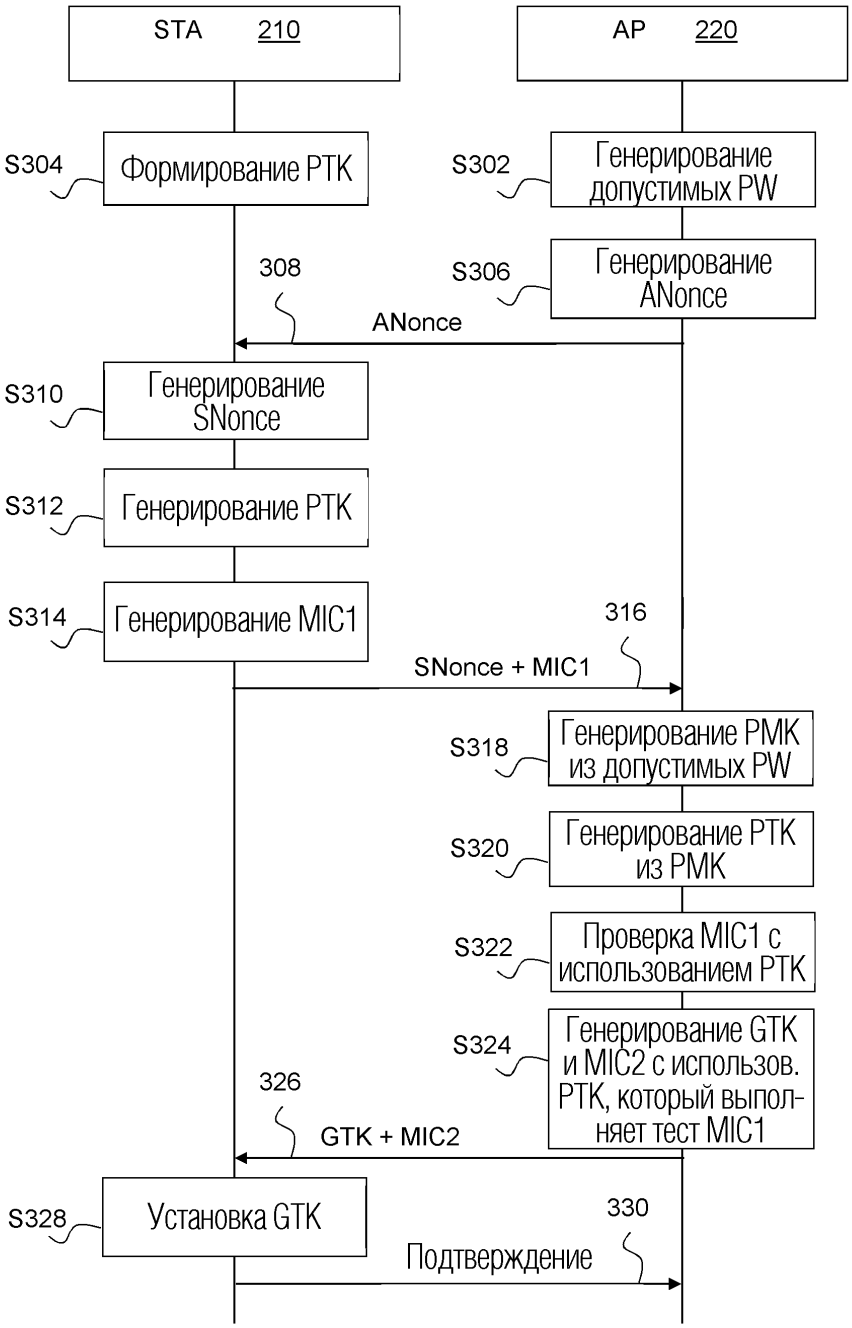
2


210
200
STA
Обраб. устр. 211
Запом. устр. 212
Ввод/вывод 213
ПИ 214
Локальная сеть
240
AP
220
260
Обраб. устр. 221
Запом. устр. 222
Ввод/вывод 223
Внешняя сеть
250

ФИГ. 2

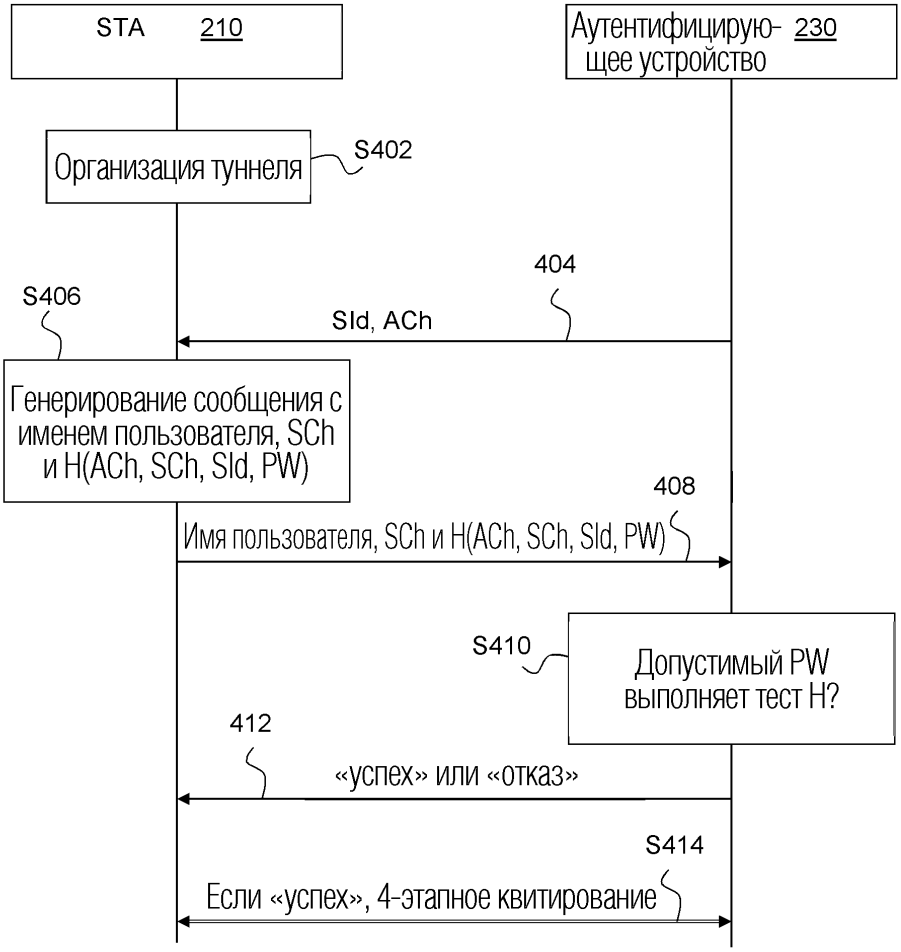
3

3/4


STA 210
AP 220
S304
Формирование PTK
S302
Генерирование допустимых PW
308
S306
Генерирование ANonce
ANonce
S310
Генерирование SNonce
S312
Генерирование PTK
S314
Генерирование MIC1
316
SNonce + MIC1
S318
Генерирование PMK из допустимых PW
S320
Генерирование PTK из PMK
S322
Проверка MIC1 с использованием PTK
S324
Генерирование GTK и MIC2 с использов. PTK, который выполняет тест MIC1
326
GTK + MIC2
S328
Установка GTK
330
Подтверждение

ФИГ. 3

4


STA 210
Аутентифицирую- 230
щее устройство
Организация туннеля
S402
404
S406
SId, ACh
Генерирование сообщения с именем пользователя, SCh и H(ACh, SCh, SId, PW)
408
Имя пользователя, SCh и H(ACh, SCh, SId, PW)
S410
Допустимый PW выполняет тест H?
412
«успех» или «отказ»
S414
Если «успех», 4-этапное квитирование

ФИГ. 4