

(19)



Евразийское  
патентное  
ведомство

(21) 202392473

(13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки  
2023.12.27

(51) Int. Cl. *H04W 12/50* (2021.01)  
*H04W 8/00* (2009.01)  
*H04L 9/40* (2022.01)  
*G06F 21/60* (2013.01)  
*H04W 84/18* (2009.01)

(22) Дата подачи заявки  
2022.02.23

(54) СИСТЕМА И СПОСОБЫ ПЕРЕДАЧИ ДАННЫХ ДАТЧИКОВ И/ИЛИ ДАННЫХ УПРАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯ

(31) 2150250-5

(72) Изобретатель:

(32) 2021.03.04

Замун Эхсан, Вестлин Самюэль (SE)

(33) SE

(74) Представитель:

(86) PCT/EP2022/054567

Тагбергенова М.М., Тагбергенова А.Т.

(87) WO 2022/184529 2022.09.09

(KZ)

(71) Заявитель:

МУНТЕРС ЕУРОП АКТИБОЛАГ  
(SE)

(57) Настоящее изобретение относится к системе (100) передачи данных датчиков и/или данных управления в пределах заданного пространства. Система содержит базовый блок, выполненный с возможностью беспроводной передачи данных с использованием открытой сети, причем базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. По меньшей мере один узел имеет сохраненные в нем указанные настройки для передачи данных по сети и идентификатор блока, опознающий узел. Базовый блок (101) и по меньшей мере один узел (102, 103, 104) выполнены с возможностью передачи данных по сети ввода. Базовый блок (101) выполнен с возможностью инициирования процедуры сопряжения по меньшей мере с одним из узлов сети ввода, указанная процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети по меньшей мере одному из узлов (102, 103, 104).



A1

202392473

202392473

A1

## **Система и способы передачи данных датчиков и/или данных управления пользователя**

### **ОБЛАСТЬ ТЕХНИКИ**

- 5 Настоящее изобретение относится к системе передачи данных датчиков и/или данных управления пользователя.
- Настоящее изобретение также относится к способам, выполняемым в указанной системе.

### 10 **ПРЕДШЕСТВУЮЩИЙ УРОВЕНЬ ТЕХНИКИ**

Приточно-вытяжные установки, такие как испарительные увлажнители и охладительные аппараты, используются для увлажнения и охлаждения различных типов помещений в зданиях. Другими типами приточно-вытяжных установок являются влагопоглотители, теплообменники или фильтрующие устройства.

- 15 Приточно-вытяжными установками можно управлять для улучшения эксплуатационных характеристик здания и/или комфорта обитателей и/или оптимизации энергопотребления. Управление приточно-вытяжной установкой может осуществляться на основе входных данных, поступающих от датчиков. Кроме того, приточно-вытяжная установка может иметь пользовательский интерфейс для ввода
- 20 параметров, предпочитаемых пользователем и/или настроек управления, чтобы осуществлять управление приточно-вытяжной установкой.

### **КРАТКОЕ ИЗЛОЖЕНИЕ СУЩНОСТИ ИЗОБРЕТЕНИЯ**

- 25 Целью изобретения является обеспечение усовершенствованной обработки данных датчиков и/или данных управления пользователя. Улучшенное управление может быть, например, обеспечено в системе мониторинга или в системе управления процессом.
- Настоящее изобретение относится к системе передачи данных датчиков и/или данных управления пользователя в пределах заранее установленного пространства. Заранее установленное пространство может быть в пределах здания или иным ограниченным
- 30 или контролируемым пространством. Система содержит базовый блок, предназначенный для беспроводной передачи данных с использованием открытой сети, причем базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между
- 35 устройствами, имеющими первый ключ шифрования. Система дополнительно содержит, по меньшей мере, один узел, содержащий блок датчиков и/или пользовательский блок управления, причем каждый указанный узел имеет сохраненные в нем указанные настройки для передачи данных по сети и идентификатор блока, однозначно идентифицирующий узел.

Базовый блок и, по меньшей мере, один узел выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и передают данные по сети ввода, используя указанный первый ключ шифрования и в соответствии с

5 указанной заранее установленной схемой передачи данных по сети.

Базовый блок выполнен с возможностью инициирования процедуры сопряжения, по меньшей мере, с одним из найденных узлов сети ввода, указанная процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из найденных узлов, указанные

10 дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования, предназначенный для использования при защищенной передаче данных по защищенной сети. Каждый сопряженный узел добавляется в защищенную сеть для передачи данных между базовым блоком и сопряженными узлами после завершения процедуры сопряжения.

15 Таким образом, система, раскрытая в настоящем изобретении, обеспечивает различные уровни защищенной передачи данных с использованием открытой сети, например ячеистой сети.

Любой базовый блок и узел, сохраняющий в себе настройки для передачи данных по сети, смогут передавать данные друг другу, используя первую, более низкую степень

20 безопасности, обеспечиваемую первым ключом шифрования для шифрования всех сообщений, и заранее установленную схему, определяющую временные интервалы передачи данных. В контексте данного описания, передача данных по открытой сети с использованием первого ключа шифрования для шифрования всех сообщений и с использованием заранее установленной схемы, определяющей временные интервалы

25 для передачи данных, относится к сети ввода. Таким образом, шифрование и заранее установленная схема, которая определяет временные интервалы для передачи данных, способствуют усложнению доступа злоумышленника к сети ввода и/или прослушиванию передачи данных между базовым блоком и узлом (узлами).

Кроме того, между базовым блоком и сопряженными узлами обеспечивается вторая

30 степень безопасности. В настоящем описании это называется защищенной сетью. В данном случае передача данных осуществляется с помощью второго ключа шифрования, который является уникальным для конкретной сети. Это обеспечивает дополнительный эффект, заключающийся в том, что возможна настройка множества защищенных сетей в пределах одного и того же пространства, без создания помех друг

35 для друга.

В соответствии с решением, определенным в настоящем описании, базовый блок выполняет функцию гейткипера (устройство контроля доступа). Именно базовый блок иницирует процедуру сопряжения, по меньшей мере, с одним из найденных узлов сети ввода. Таким образом, именно базовый блок определяет узел (узлы) для сопряжения.

Данные датчиков и/или данные управления пользователя могут передаваться как по сети ввода, так и по защищенной сети. Однако степень доверия может отличаться между данными, передаваемыми по сети ввода, и защищенной сетью. Например, базовый блок может быть выполнен с возможностью передачи контроллеру для управления технологическим процессом только данных датчиков и/или данных управления, полученных по защищенной сети. Контроллер может быть встроен в базовый блок или внешний блок. Данные датчиков и/или данные управления, полученные по сети ввода, могут использоваться для вывода на дисплей и/или мониторинга и/или регистрации.

5 В варианте осуществления, базовый блок выполнен с возможностью передачи сообщения-запроса, зашифрованного первым ключом шифрования, а соответствующий узел выполнен с возможностью приема и расшифровки сообщения-запроса, закодированного первым ключом шифрования, в результате чего базовый блок и соответствующий узел (102; 103, 104) находят друг друга, причем соответствующий найденный узел выполнен для передачи сообщения-идентификатора, зашифрованного с помощью первого ключа шифрования, указанное сообщение-идентификатор содержит идентификатор блока, и при этом базовая станция выполнена с возможностью приема и расшифровки соответствующего сообщения-идентификатора.

Базовый блок может дополнительно содержать дисплей и средства взаимодействия с пользователем. Дисплей базового блока может быть выполнен с возможностью представления списка найденных узлов на основе принятого и расшифрованного идентификатора (идентификаторов) блока. Средства взаимодействия с пользователем могут обеспечивать выбор пользователем узла (узлов) для сопряжения из списка найденных узлов, после чего выбранный пользователем узел (узлы) регистрируется в базовом блоке, и инициируется процедура сопряжения для выбранного пользователем узла (узлов). Таким образом, формирование защищенных сетей управляется пользователем с базового блока.

Дисплей базового блока может быть выполнен с возможностью отображения узлов, подключенных к защищенной сети, и средства взаимодействия с пользователем в базовом блоке могут обеспечивать управление узлами, подключенными к защищенной сети, указанное управление может включать удаление узлов.

30 В различных вариантах осуществления базовый блок выполнен с возможностью отправки времени запуска защищенной сети узлам, которые должны быть добавлены в защищенную сеть, и передача данных с использованием второго уникального ключа шифрования запускается как на базовом блоке, так и на задействованном узле (узлах) в переданное время, в результате чего узлы добавляются в защищенную сеть.

В различных вариантах осуществления, по меньшей мере, один из узлов содержит, по меньшей мере, один пользовательский блок управления, содержащий интерфейс ввода для установки параметра, относящегося к управлению технологическим процессом, причем пользовательский блок управления выполнен с возможностью передачи в

базовый блок информации, относящейся к установке параметра. Базовый блок, в свою очередь, может передавать настройку параметров для управления технологическим процессом.

5 Система может представлять собой систему мониторинга для отслеживания одного или множества датчиков.

Система может представлять собой систему для управления процессом, таким как

- инъекционное формование и печать,
- процессы производства сухого молока и других пищевых продуктов,
- производство аккумуляторных батарей, медицинских субстанций или  
10 другими химическими процессами,
- защита зданий, мостов, ветряных турбин, оборудования и исторических артефактов в музеях,
- реконструкция зданий и других сооружений, поврежденных влагой, или
- контроль процесса отверждения бетонных или склеенных изделий,  
15 созревания сыра, выдерживания фруктов и молочных продуктов.

В различных вариантах осуществления система представляет собой систему климат-контроля в помещении для управления приточно-вытяжной установкой, предназначенной для воздействия на воздух в здании. Пользовательский блок управления может содержать интерфейс ввода для установки значения температуры  
20 и/или уровня влажности, и пользовательский блок управления может быть выполнен с возможностью передачи на базовый блок информации, относящейся к заданной температуре и/или влажности. Блок управления приточно-вытяжной установкой может быть выполнен с возможностью управления на основе данных датчика и/или данных управления пользователя, передаваемых на базовый блок по защищенной сети.

25 Настоящее изобретение также относится к способу взаимодействия с, по меньшей мере, одним узлом, указанный способ осуществляется в базовом блоке системы передачи данных датчиков и/или данных управления, указанный базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее  
30 установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Способ включает

передачу по открытой беспроводной сети сообщения-запроса на подключение, причем указанное сообщение-запрос на подключение передается с использованием заранее установленной схемы и кодируется с помощью указанного  
35 первого ключа шифрования,

прием по открытой беспроводной сети, по меньшей мере, одного сообщения-идентификатора, содержащего идентификатор блока подключенного узла, причем указанное принятое сообщение-идентификатор передается с использованием

заранее установленной схемы и шифруется с использованием первого ключа шифрования и,

расшифровку полученного сообщения-ответа,

5 инициирование процедуры сопряжения, по меньшей мере, с одним из подключенных узлов, указанная процедура сопряжения включает передачу дополнительных настроек для взаимодействия по защищенной сети с, по меньшей мере, одним из подключенных узлов (102; 103, 104), указанные дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети, и

10 инициирование защищенной передачи данных с сопряженным узлом (узлами), в котором для защищенной передачи данных используется, по меньшей мере, один уникальный второй ключ шифрования для шифрования/расшифровки передаваемых сообщений.

Настоящее изобретение также относится к способу, выполняемому в узле для взаимодействия с базовым блоком системы передачи данных датчиков и/или данных управления, указанный узел имеет сохраненные в нем настройки для передачи данных по сети с использованием открытой сети и уникального идентификатора блока, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных между устройствами, имеющими первый ключ шифрования.

20 Способ включает

прием от базового блока по открытой беспроводной сети сообщения-запроса на подключение, указанное сообщение-запрос на подключение передается с использованием заранее установленной схемы передачи данных по сети и кодируется с помощью первого ключа шифрования,

25 расшифровку полученного сообщения-запроса на подключение, после успешной расшифровки сообщения-запроса на подключение, передачу (403) по открытой беспроводной сети сообщения-идентификатора, содержащего идентификатор блока узла, указанное сообщение-идентификатор передается с использованием предварительно установленной схемы передачи данных и кодируется с помощью первого ключа шифрования,

30 получение по открытой сети дополнительных настроек для передачи данных по защищенной сети, указанные дополнительные настройки для передачи данных по сети включают, по меньшей мере, один уникальный второй ключ шифрования, и

35 инициирование защищенной передачи данных, при которой для шифрования/расшифровки передаваемых сообщений используется, по меньшей мере, один уникальный второй ключ шифрования.

## **КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ**

На Фиг. 1 представлена схема сигнализации, показывающая примеры сигнализации в системе для передачи данных датчиков и/или данных управления пользователя.

Фиг. 2 представляет блок-схему, поясняющую пример способа взаимодействия с, по меньшей мере, одним узлом, причем указанный способ выполняется в базовом блоке системы передачи данных датчиков и/или данных управления пользователя.

Фиг. 3 представляет блок-схему, поясняющую пример способа, выполняемого на узле для взаимодействия с базовым блоком системы передачи данных датчиков и/или данных управления пользователя.

На Фиг. 4 представлена блок-схема, поясняющая пример системы климат-контроля в помещении для управления приточно-вытяжной установкой, предназначенной для воздействия на воздух в здании.

### **ПОДРОБНОЕ ОПИСАНИЕ**

Настоящее изобретение относится к системе передачи данных датчиков и/или данных управления пользователя в пределах заранее установленного пространства. Заранее установленное пространство может находиться внутри здания или в ином ограниченном или контролируемом пространстве. Система содержит базовый блок, выполненный для беспроводной передачи данных с использованием открытой сети, причем базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Система дополнительно содержит, по меньшей мере, один узел, содержащий блок датчиков и/или пользовательский блок управления, причем каждый указанный узел имеет сохраненные в нем указанные настройки для передачи данных по сети и идентификатор блока, однозначно идентифицирующий узел. Базовый блок и, по меньшей мере, один узел выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и взаимодействовать по сети ввода, используя указанный первый ключ шифрования и в соответствии с упомянутой заранее установленной схемой передачи данных по сети. Базовый блок выполнен с возможностью инициирования процедуры сопряжения с, по меньшей мере, одним из найденных узлов сети ввода, указанная процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из найденных узлов, указанные дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для использования при защищенной передаче данных по защищенной сети. Каждый сопряженный узел добавляется в защищенную сеть для передачи данных между базовым блоком и сопряженными узлами после завершения процедуры сопряжения.

Схема сигнализации на Фиг. 1 представляет пример сигнализации для описанной выше системы передачи данных датчика и/или данных управления пользователя в пределах заранее установленного пространства.

5 Система может представлять собой систему мониторинга для наблюдения за одним или множеством датчиков.

Система может представлять собой систему управления процессом, таким как

- инъекционное формование и печать,
- процессы производства сухого молока и других пищевых продуктов,
- производство аккумуляторных батарей, медицинских субстанций или  
10 другими химическими процессами
- защита зданий, мостов, ветряных турбин, оборудования и исторических артефактов в музеях,
- реконструкция зданий и других сооружений, поврежденных влагой, или
- контроль процесса отверждения бетонных или клеенных изделий,  
15 созревания сыра, выдерживания фруктов и молочных продуктов.

В различных вариантах осуществления система представляет собой систему климат-контроля в помещении для управления приточно-вытяжной установкой, предназначенной для воздействия на воздух в здании.

20 Схема сигнализации представляет собой схему передачи данных между базовым блоком 101 и, по меньшей мере, одним узлом 102.

Базовый блок 101 может представлять собой базовый блок, подключенный к приточно-вытяжной установке или встроенный в приточно-вытяжную установку, предназначенную для воздействия на воздух в здании. Таким образом, базовый блок 101 является частью системы климат-контроля в помещении, управляющей приточно-  
25 вытяжной установкой.

Базовый блок имеет сохраненные в нем настройки для беспроводной передачи данных по сети с использованием открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Настройки могут дополнительно  
30 содержать идентификатор сети ввода или идентификатор PAN (personal area network – персональная сеть) для сети ввода. Идентификатор сети ввода используется для однозначной идентификации сети ввода. Устройства в одной сети должны совместно использовать идентификатор (идентификаторы) сети.

Настройки являются общими для блоков, предназначенных для подключения к системе.  
35 Фактически, настройки являются уникальными для одного или нескольких производителей блоков и/или предназначены для использования с системой передачи данных датчиков и/или данных управления пользователя. Характерно, что настройки сохраняются в соответствующем блоке при его изготовлении. Настройки хранятся в секрете для предотвращения несанкционированного использования. Блоки, имеющие

настройки, размещаются таким образом, чтобы осуществлять связь друг с другом в соответствии с заранее установленной схемой в сети ввода. По меньшей мере, один узел 102 содержит, например, пользовательский блок управления и/или блок датчиков.

5 Чтобы найти узлы, предназначенные для взаимодействия с базовым блоком 101 в сети ввода, базовый блок передает сообщение-запрос на подключение M1, зашифрованное с помощью первого ключа шифрования, по открытой беспроводной сети, используя заранее установленную схему передачи данных. Узел (узлы) предназначен для приема и расшифровки сообщения-запроса на подключение, если он находится в зоне досягаемости связи по открытой беспроводной сети. Если узел способен принять и  
10 расшифровать сообщение-запрос на подключение, то узел подключен к сети ввода. После подключения узел передает сообщение-ответ M2. Сообщение-ответ M2 передается по заранее установленной схеме и шифруется с использованием первого ключа шифрования. Сообщение-ответ содержит идентификатор блока узла.

15 Предполагается, что базовый блок и узлы синхронизированы для обеспечения передачи сообщений согласно заранее установленной схеме. Такая синхронизация известна в данной области техники и не описывается подробно в настоящем документе. Например, соответствующий узел может содержать кристалл, откалиброванный с помощью сети. После приема и расшифровки сообщения-ответа M2 базовый блок 101 распознает, что подключенный узел найден.

20 Базовый блок 101 и узел 102 выполнены с возможностью передачи данных друг другу в соответствии с заранее установленной схемой, используя первый ключ шифрования для шифрования сообщений. Это показано в виде двунаправленного сообщения M3 на Фиг. 1.

25 После принятия базовым блоком решения о выполнении сопряжения с одним или несколькими из подключенных узлов для обеспечения защищенной связи, базовый блок передает сообщение M4, содержащее дополнительные настройки для передачи данных выбранным узлам по защищенной сети. Настройки содержат, по меньшей мере, второй уникальный ключ шифрования для защищенной передачи данных. Настройки могут дополнительно содержать время запуска защищенной передачи данных между узлом  
30 102 и базовым блоком 101.

Таким образом, базовый блок 101 и узел 102 подключаются для защищенной передачи данных и, следовательно, выполнены с возможностью защищенной передачи данных с использованием второго уникального ключа шифрования. Защищенная передача данных предпочтительно осуществляется по заранее установленной схеме. В другом  
35 варианте осуществления, защищенная передача данных выполняется в соответствии с другой схемой защищенной передачи данных, при этом схема защищенной передачи данных может быть предварительно сохранена в базовом блоке и узлах. Защищенная передача данных показана в виде двунаправленного сообщения M5 на Фиг. 1.

На Фиг. 2 представлен пример способа 200 для передачи данных с, по меньшей мере, одним заданным узлом. Способ 200 выполняется в базовом блоке системы передачи данных датчиков и/или данных управления пользователя, указанный базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием

5 указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования.

Способ 200 включает этап передачи 201 по открытой беспроводной сети сообщения-запроса на подключение, причем указанное сообщение-запрос на подключение

10 передается с помощью заранее установленной схемы и кодируется с использованием указанного первого ключа шифрования,

Способ 200 дополнительно включает этап 202 приема по открытой беспроводной сети, по меньшей мере, одного сообщения-ответа, содержащего идентификатор блока подключенного узла, причем указанное принятое сообщение-ответ передается с

15 помощью заранее установленной схемы и шифруется с использованием первого ключа шифрования.

Способ дополнительно включает этап 203 расшифровки принятого сообщения ответа.

Затем либо автоматически, либо вручную может инициироваться процедура сопряжения 205.

В инициированном пользователем примере подключенные узлы представлены 203 в пользовательском интерфейсе для выбора пользователем узла (узлов) для сопряжения, и обнаружен выбор пользователя, по меньшей мере, одного узла для сопряжения. Затем, по меньшей мере, один выбранный пользователем узел регистрируется в базовом блоке, и инициируется процедура сопряжения для выбранного пользователем узла (узлов).

Процедура сопряжения включает передачу 206 дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из подключенных узлов (102; 103, 104), указанные дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети.

Способ дополнительно включает этап инициирования 207 защищенной передачи данных с сопряженным узлом (узлами), в котором для защищенной передачи данных используется, по меньшей мере, один уникальный второй ключ шифрования для шифрования/расшифровки передаваемых сообщений. Инициирование 207 защищенной передачи данных может включать в себя отправку времени запуска защищенной сети

30 узлам, которые подлежат включению в защищенную сеть. Таким образом, передача данных с использованием второго уникального ключа шифрования начинается как на базовом блоке, так и на задействованном узле (узлах) в переданное время.

На Фиг.3 представлен пример способа 300, выполняемого в узле для взаимодействия с базовым блоком системы передачи данных датчиков и/или данных управления,

указанный узел имеет сохраненные в нем настройки для передачи данных по сети с использованием открытой сети и уникальный идентификатор блока, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования.

5 Узел содержит, например, по меньшей мере, один блок датчиков. Блок (блоки) датчиков может быть выполнен с возможностью определения, по меньшей мере, одного из следующих параметров:

- относительная влажность,
- точка росы,
- 10 • обычные атмосферные газы, такие как кислород, азот, углекислый газ,
- летучие органические соединения, ЛОС,
- температура,
- химическое вещество (вещества) в газообразной форме, такое как радон,
- атмосферное давление,
- 15 • уровень звукового давления,
- электромагнитные поля,
- условия освещения,
- аэрозоли, и
- частицы.

20 В примере узел содержит, по меньшей мере, один пользовательский блок управления. Пользовательский блок управления может содержать интерфейс ввода для установки параметра, относящегося к управлению технологическим процессом,

Способ включает прием 301 по открытой беспроводной сети сообщения-запроса на подключение от базового блока, при этом указанное принятое сообщение-запрос на  
25 подключение передается с использованием заранее установленной схемы передачи данных по сети и кодируется с использованием первого ключа шифрования.

Способ дополнительно включает этап 302 расшифровки принятого сообщения-запроса на подключение. После успешной расшифровки сообщения-запроса на подключение узел считается подключенным.

30 Способ дополнительно включает этап, после успешной расшифровки сообщения-запроса на подключение, передачи 303 по открытой беспроводной сети сообщения-ответа в форме сообщения-идентификатора, содержащего идентификатор блока узла. Сообщение-идентификатор передается с использованием заранее установленной схемы передачи данных по сети и кодируется с использованием первого ключа шифрования.

35 Такая процедура может повторяться с заранее установленными интервалами до тех пор, пока не будут получены настройки защищенной передачи данных.

Способ дополнительно включает этап 304 приема по открытой сети дополнительных настроек для передачи данных по защищенной сети, указанные дополнительные

настройки для передачи данных содержат, по меньшей мере, один уникальный второй ключ шифрования.

Способ дополнительно включает инициирование 305 защищенной передачи данных, в котором при защищенной передаче данных, по меньшей мере, один уникальный второй ключ шифрования используется для шифрования/расшифровки передаваемых сообщений. Инициирование 305 защищенной передачи данных может включать получение от базового блока времени для запуска защищенной сети. Таким образом, передача данных с использованием второго уникального ключа шифрования запускается как на базовом блоке, так и на узле (узлах) в переданное время.

10 Если узел содержит пользовательский блок управления, пользовательский блок управления может передавать в базовый блок информацию, относящуюся к параметрам, заданным в пользовательском блоке управления. Такие передачи могут выполняться в сети ввода и/или защищенной сети.

15 Если узел содержит блок датчиков, блок датчиков может передавать данные датчика в базовый блок. Такие передачи могут выполняться в сети ввода и/или защищенной сети. Способы, описанные в настоящем изобретении, могут быть реализованы в компьютерных программах, содержащих инструкции, которые, при выполнении программы компьютером, дают команду компьютеру выполнять способы.

20 На Фиг.4 представлена система, описанная в настоящем документе, применительно к системе 400 климат-контроля в помещении для управления приточно-вытяжной установкой 105, предназначенной для воздействия на воздух в здании.

Приточно-вытяжная установка 105 предназначена для охлаждения и/или подогрева, и/или обезвоживания, и/или осушения и/или очистки воздуха внутри здания. Приточно-вытяжная установка 105 представляет собой, например, испарительный увлажнитель и/или охладитель. Таким образом, приточно-вытяжная установка 105 используется для увлажнения и/или охлаждения помещений различных типов в зданиях. Другими видами приточно-вытяжных установок являются влагопоглотители, теплообменники или фильтрующие устройства.

30 Система 400 содержит, например, базовый блок 101, соединенный с приточно-вытяжной установкой 105. В примере базовый блок 101 является автономным базовым блоком 101. В другом варианте осуществления базовый блок может быть встроен в приточно-вытяжную установку 105.

35 Функция базового блока 101 рассчитана на предоставление данных приточно-вытяжной установке, предназначенных для управления приточно-вытяжной установкой. Базовый блок 101 функционирует как интерфейс между приточно-вытяжной установкой 105 и удаленными блоками, такими как сенсорные блоки 103 и/или пользовательские блоки управления 104.

Базовый блок 101 может содержать память 106 для хранения данных и процессор. Базовый блок 101 может содержать дисплей 107 и средства взаимодействия с пользователем 108 для ввода данных пользователя.

5 Базовый блок 101 имеет сохраненные в нем настройки, содержащие первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Настройки определяют начальный адрес системы передачи данных и, в некоторых случаях, приточно-вытяжную установку 105, к которой она подключена или в которую встроена. Настройки обычно кодируются в аппаратном или программном обеспечении базового  
10 устройства при изготовлении. По меньшей мере, часть настроек предпочтительно скрыта в аппаратном или программном обеспечении, что позволяет предотвратить несанкционированный доступ. Настройки могут храниться в памяти 106.

Базовый блок 101 выполнен с возможностью беспроводной передачи данных посредством беспроводной открытой сети и настроек, как описано в настоящем  
15 изобретении. Сеть, использующая беспроводную открытую сеть и описанные здесь настройки, называется сетью ввода. Открытая сеть может быть ячеистой сетью.

По меньшей мере, один узел 103, 104, предназначенный для взаимодействия с базовым блоком, может находиться в зоне досягаемости связи по открытой беспроводной сети с базовым блоком 101. Узел 103, 104 может содержать память 111 для хранения данных и  
20 процессор. Узел 103, 104 может содержать дисплей 109 и/или средство взаимодействия с пользователем 110 для ввода данных пользователя.

Каждый узел имеет сохраненные в нем настройки, такие же, как и в базовом блоке. Как описано выше, настройки идентифицируют начальный адрес системы передачи данных датчиков и/или данных управления пользователя и, при необходимости, приточно-вытяжную установку, для которой предназначена система передачи данных датчиков  
25 и/или данных управления пользователя. Как упоминалось выше, настройки обычно кодируются в аппаратном или программном обеспечении узла при изготовлении. По меньшей мере, часть настроек предпочтительно скрыта в аппаратном или программном обеспечении, что позволяет предотвратить несанкционированный доступ. Каждый узел  
30 дополнительно содержит сохраненный в нем идентификатор блока, опознающий узел. Настройки и идентификатор блока могут храниться в памяти 111.

Как ясно из вышеизложенного, каждый, по меньшей мере, один узел содержит блок датчиков 103 и/или пользовательский блок управления 104.

Пользовательские средства ввода 110 пользовательского блока управления 104 могут  
35 содержать интерфейс ввода для установки уровня температуры и/или влажности.

В данной заявке, по меньшей мере, один блок 103 датчиков может содержать, по меньшей мере, один датчик для определения, по меньшей мере, одного из следующих параметров:

- относительная влажность,

- точка росы, и
- температура.

Базовый блок 101 и, по меньшей мере, один узел 103, 104 выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и передачи данных по сети ввода, используя указанный первый ключ шифрования и в соответствии с заранее установленной схемой передачи данных по сети.

Более подробно, базовый блок 101 выполнен с возможностью передачи сообщения-запроса, зашифрованного первым ключом шифрования, и соответствующий узел выполнен с возможностью приема и расшифровки сообщения-запроса, закодированного первым ключом шифрования, причем базовый блок 101 и соответствующий узел (102; 103, 104) соединены. Таким образом, соответствующий подключенный узел выполнен с возможностью передачи сообщения-ответа в форме сообщения-идентификатора, зашифрованного с помощью первого ключа шифрования, причем указанное сообщение-идентификатор содержит идентификатор блока. Таким образом, базовая станция выполнена с возможностью приема и расшифровки соответствующего сообщения-идентификатора.

Передача данных осуществляется по сети ввода в соответствии с заранее установленной схемой передачи данных между устройствами, имеющими настройки, описанные в настоящем изобретении. Заранее установленная схема определяет характерные временные интервалы для передачи данных. Передача данных может, например, основываться на синхронизированном по времени переключении каналов, СВПК. Это означает, что временные интервалы передачи данных невелики, и, следовательно, система обладает высокой энергоэффективностью. Передача данных по сети ввода шифруется с помощью первого ключа шифрования.

Как описано выше, базовый блок 101 и, по меньшей мере, один узел 103, 104 выполнены с возможностью передачи данных друг другу по сети ввода. Например, пользовательский блок (блоки) управления 104 может быть выполнен с возможностью передачи информации, относящейся к заданной температуре и/или влажности, базовому блоку 101 по сети ввода. Таким образом, базовый блок 101 выполнен с возможностью приема передаваемой информации. Базовый блок 101 может быть выполнен с возможностью отображения, по меньшей мере, части принятой информации, относящейся к заданной температуре и/или влажности.

Например, блок (блоки) датчиков 103 может быть выполнен с возможностью передачи данных датчиков в базовый блок 101 по сети ввода. Таким образом, базовый блок 101 выполнен с возможностью приема переданных данных датчика. Базовый блок может быть выполнен с возможностью отображения, по меньшей мере, части принятых данных датчика.

В варианте осуществления данные, передаваемые от пользовательского блока (блоков) управления 104 и/или блока(блоков) датчиков 103 по сети ввода, не используются для управления приточно-вытяжной установкой.

5 Кроме того, базовый блок 101 выполнен с возможностью инициирования процедуры сопряжения, по меньшей мере, с одним из узлов сети ввода. Процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из подключенных узлов. Дополнительные настройки могут также называться правами доступа для защищенной передачи данных. Дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для защищенной сети и для использования при защищенной передаче 10 данных по защищенной сети. В предпочтительном варианте осуществления, по меньшей мере, один блок датчиков 103 и, по меньшей мере, один пользовательский блок управления 104 подключены к защищенной сети.

15 В приведенном примере дисплей 107 базового блока выполнен с возможностью представления перечня подключенных, несопряженных узлов. Средства взаимодействия с пользователем 108 базового блока 102 обеспечивают выбор пользователем узла (узлов) для сопряжения из списка, после чего выбранный пользователем узел (узлы) регистрируется в базовом блоке 102, и процедура сопряжения выполняется для выбранного пользователем узла (узлов).

20 Сопряжение — это процесс, используемый в компьютерных сетях, который помогает установить соединения между вычислительными устройствами для обеспечения передачи данных между ними. В контексте настоящего изобретения соединение между вычислительными устройствами уже присутствует, как описано выше, благодаря настройкам. В контексте изобретения сопряжение выполняется для настройки 25 соединения для передачи данных в защищенной сети.

В примере дополнительные настройки содержат в дополнение ко второму уникальному ключу шифрования идентификатор защищенной сети или идентификатор PAN для защищенной сети. В примере уникальный идентификатор сети используется для однозначной идентификации защищенной сети. Как упоминалось в отношении сети 30 ввода, устройства в одной сети должны совместно использовать идентификатор(ы) сети. В процессе сопряжения узлу (узлам) передается второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети. Переданный второй уникальный ключ шифрования затем сохраняется в соответствующем узле 103, 104 и используется в последующей защищенной передаче данных. Кроме того, если 35 присутствует, идентификатор защищенной сети или идентификатор PAN для защищенной сети, он также передается узлу (узлам) и хранится в нем.

Как ясно из вышеизложенного, второй уникальный ключ шифрования для передачи данных по защищенной сети передается по сети ввода с помощью заранее

установленной схемы передачи данных. То же самое применимо к идентификатору защищенной сети или идентификатору PAN для защищенной сети, при наличии.

Шифрование, используемое в защищенной передаче данных, как правило, представляет собой симметричный блочный шифр. Например, для шифрования (и последующей расшифровки) используется расширенный стандарт шифрования AES. Длина блока блочного шифра, используемого в AES, составляет, например, 128, или 192, или 256 бит. В примере второй уникальный ключ шифрования, т.е. блок, генерируется в базовом блоке при сопряжении. В соответствии с этим примером, второй уникальный ключ шифрования не хранится ни в одном из блоков до момента использования. Это повышает безопасность. Риск несанкционированного доступа ко второму ключу шифрования минимизируется. Идентификатор защищенной сети или идентификатор PAN для защищенной сети также может генерироваться на базовом блоке в связи с сопряжением таким же образом, как и второй уникальный ключ шифрования.

Защищенная передача данных начинается после завершения процедуры сопряжения. Дисплей базового блока в примере выполнен с возможностью отображения узлов, подключенных к защищенной сети. Средства взаимодействия с пользователем могут обеспечивать управление узлами, подключенными к защищенной сети, указанное управление может включать удаление узлов. Это означает, что представленные сопряженные узлы могут выбираться для разрыва сопряжения, а представленные несопряженные узлы могут выбираться для сопряжения. Удаление узла, т.е. разрыв сопряжения узла, может включать информирование узла базовым блоком о том, что он не сопряжен, и узел в ответ на это удаляет или компрометирует второй уникальный ключ шифрования, так что он больше не может использоваться.

Базовый блок может быть выполнен с возможностью отправки времени запуска защищенной сети узлам, подлежащим добавлению в защищенную сеть, и передача данных с использованием второго уникального ключа шифрования запускается как в базовом блоке, так и в задействованном узле (узлах) в переданное время, посредством чего узлы добавляются в защищенную сеть.

По меньшей мере, часть данных, передаваемых от блока (блоков) датчиков и/или блока (блоков) управления пользователя базовому блоку по защищенной сети, передается в приточно-вытяжную установку для управления ею. Таким образом, обычно базовый блок выполнен с возможностью использования данных, полученных от узла (узлов) по сети ввода, для отображения и возможных других применений, не влияющих на приточно-вытяжную установку. Базовый блок дополнительно выполнен с возможностью использования данных, полученных от узла (узлов) по защищенной сети, для передачи данных для управления приточно-вытяжной установкой. Кроме того, обновления программного обеспечения, передаваемые с базового блока на узлы, могут разрешаться только по защищенной сети.

Как правило, используемая открытая сеть представляет собой ячеистую сеть. Таким образом, решение, представленное в настоящем изобретении, обеспечивает передачу данных с подключенными узлами в сети ввода и защищенную передачу данных в защищенной сети также тогда, когда базовый блок и блок (блоки) датчиков/блок(блоки) управления пользователя не находятся в прямой связи.

5

## **Система и способы передачи данных датчиков и/или данных управления пользователя**

### **ОБЛАСТЬ ТЕХНИКИ**

- 5 Настоящее изобретение относится к системе передачи данных датчиков и/или данных управления пользователя.
- Настоящее изобретение также относится к способам, выполняемым в указанной системе.

### 10 **ПРЕДШЕСТВУЮЩИЙ УРОВЕНЬ ТЕХНИКИ**

Приточно-вытяжные установки, такие как испарительные увлажнители и охладительные аппараты, используются для увлажнения и охлаждения различных типов помещений в зданиях. Другими типами приточно-вытяжных установок являются влагопоглотители, теплообменники или фильтрующие устройства.

- 15 Приточно-вытяжными установками можно управлять для улучшения эксплуатационных характеристик здания и/или комфорта обитателей и/или оптимизации энергопотребления. Управление приточно-вытяжной установкой может осуществляться на основе входных данных, поступающих от датчиков. Кроме того, приточно-вытяжная установка может иметь пользовательский интерфейс для ввода
- 20 параметров, предпочитаемых пользователем и/или настроек управления, чтобы осуществлять управление приточно-вытяжной установкой.

### **КРАТКОЕ ИЗЛОЖЕНИЕ СУЩНОСТИ ИЗОБРЕТЕНИЯ**

- Целью изобретения является обеспечение усовершенствованной обработки данных
- 25 датчиков и/или данных управления пользователя. Улучшенное управление может быть, например, обеспечено в системе мониторинга или в системе управления процессом.
- Настоящее изобретение относится к системе передачи данных датчиков и/или данных управления пользователя в пределах заранее установленного пространства. Заранее установленное пространство может быть в пределах здания или иным ограниченным
- 30 или контролируемым пространством. Система содержит базовый блок, предназначенный для беспроводной передачи данных с использованием открытой сети, причем базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между
- 35 устройствами, имеющими первый ключ шифрования. Система дополнительно содержит, по меньшей мере, один узел, содержащий блок датчиков и/или пользовательский блок управления, причем каждый указанный узел имеет сохраненные в нем указанные настройки для передачи данных по сети и идентификатор блока, однозначно идентифицирующий узел.

Базовый блок и, по меньшей мере, один узел выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и передают данные по сети ввода, используя указанный первый ключ шифрования и в соответствии с

5 указанной заранее установленной схемой передачи данных по сети.

Базовый блок выполнен с возможностью инициирования процедуры сопряжения, по меньшей мере, с одним из найденных узлов сети ввода, указанная процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из найденных узлов, указанные

10 дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования, предназначенный для использования при защищенной передаче данных по защищенной сети. Каждый сопряженный узел добавляется в защищенную сеть для передачи данных между базовым блоком и сопряженными узлами после завершения процедуры сопряжения.

15 Таким образом, система, раскрытая в настоящем изобретении, обеспечивает различные уровни защищенной передачи данных с использованием открытой сети, например ячеистой сети.

Любой базовый блок и узел, сохраняющий в себе настройки для передачи данных по сети, смогут передавать данные друг другу, используя первую, более низкую степень

20 безопасности, обеспечиваемую первым ключом шифрования для шифрования всех сообщений, и заранее установленную схему, определяющую временные интервалы передачи данных. В контексте данного описания, передача данных по открытой сети с использованием первого ключа шифрования для шифрования всех сообщений и с использованием заранее установленной схемы, определяющей временные интервалы

25 для передачи данных, относится к сети ввода. Таким образом, шифрование и заранее установленная схема, которая определяет временные интервалы для передачи данных, способствуют усложнению доступа злоумышленника к сети ввода и/или прослушиванию передачи данных между базовым блоком и узлом (узлами).

Кроме того, между базовым блоком и сопряженными узлами обеспечивается вторая

30 степень безопасности. В настоящем описании это называется защищенной сетью. В данном случае передача данных осуществляется с помощью второго ключа шифрования, который является уникальным для конкретной сети. Это обеспечивает дополнительный эффект, заключающийся в том, что возможна настройка множества защищенных сетей в пределах одного и того же пространства, без создания помех друг

35 для друга.

В соответствии с решением, определенным в настоящем описании, базовый блок выполняет функцию гейткипера (устройство контроля доступа). Именно базовый блок инициирует процедуру сопряжения, по меньшей мере, с одним из найденных узлов сети ввода. Таким образом, именно базовый блок определяет узел (узлы) для сопряжения.

Данные датчиков и/или данные управления пользователя могут передаваться как по сети ввода, так и по защищенной сети. Однако степень доверия может отличаться между данными, передаваемыми по сети ввода, и защищенной сетью. Например, базовый блок может быть выполнен с возможностью передачи контроллеру для управления технологическим процессом только данных датчиков и/или данных управления, полученных по защищенной сети. Контроллер может быть встроен в базовый блок или внешний блок. Данные датчиков и/или данные управления, полученные по сети ввода, могут использоваться для вывода на дисплей и/или мониторинга и/или регистрации.

5 В варианте осуществления, базовый блок выполнен с возможностью передачи сообщения-запроса, зашифрованного первым ключом шифрования, а соответствующий узел выполнен с возможностью приема и расшифровки сообщения-запроса, закодированного первым ключом шифрования, в результате чего базовый блок и соответствующий узел (102; 103, 104) находят друг друга, причем соответствующий найденный узел выполнен для передачи сообщения-идентификатора, зашифрованного с помощью первого ключа шифрования, указанное сообщение-идентификатор содержит идентификатор блока, и при этом базовая станция выполнена с возможностью приема и расшифровки соответствующего сообщения-идентификатора.

10 Базовый блок может дополнительно содержать дисплей и средства взаимодействия с пользователем. Дисплей базового блока может быть выполнен с возможностью представления списка найденных узлов на основе принятого и расшифрованного идентификатора (идентификаторов) блока. Средства взаимодействия с пользователем могут обеспечивать выбор пользователем узла (узлов) для сопряжения из списка найденных узлов, после чего выбранный пользователем узел (узлы) регистрируется в базовом блоке, и инициируется процедура сопряжения для выбранного пользователем узла (узлов). Таким образом, формирование защищенных сетей управляется пользователем с базового блока.

20 Дисплей базового блока может быть выполнен с возможностью отображения узлов, подключенных к защищенной сети, и средства взаимодействия с пользователем в базовом блоке могут обеспечивать управление узлами, подключенными к защищенной сети, указанное управление может включать удаление узлов.

30 В различных вариантах осуществления базовый блок выполнен с возможностью отправки времени запуска защищенной сети узлам, которые должны быть добавлены в защищенную сеть, и передача данных с использованием второго уникального ключа шифрования запускается как на базовом блоке, так и на задействованном узле (узлах) в переданное время, в результате чего узлы добавляются в защищенную сеть.

35 В различных вариантах осуществления, по меньшей мере, один из узлов содержит, по меньшей мере, один пользовательский блок управления, содержащий интерфейс ввода для установки параметра, относящегося к управлению технологическим процессом, причем пользовательский блок управления выполнен с возможностью передачи в

базовый блок информации, относящейся к установке параметра. Базовый блок, в свою очередь, может передавать настройку параметров для управления технологическим процессом.

5 Система может представлять собой систему мониторинга для отслеживания одного или множества датчиков.

Система может представлять собой систему для управления процессом, таким как

- инъекционное формование и печать,
- процессы производства сухого молока и других пищевых продуктов,
- производство аккумуляторных батарей, медицинских субстанций или  
10 другими химическими процессами,
- защита зданий, мостов, ветряных турбин, оборудования и исторических артефактов в музеях,
- реконструкция зданий и других сооружений, поврежденных влагой, или
- контроль процесса отверждения бетонных или склеенных изделий,  
15 созревания сыра, выдерживания фруктов и молочных продуктов.

В различных вариантах осуществления система представляет собой систему климат-контроля в помещении для управления приточно-вытяжной установкой, предназначенной для воздействия на воздух в здании. Пользовательский блок управления может содержать интерфейс ввода для установки значения температуры  
20 и/или уровня влажности, и пользовательский блок управления может быть выполнен с возможностью передачи на базовый блок информации, относящейся к заданной температуре и/или влажности. Блок управления приточно-вытяжной установкой может быть выполнен с возможностью управления на основе данных датчика и/или данных управления пользователя, передаваемых на базовый блок по защищенной сети.

25 Настоящее изобретение также относится к способу взаимодействия с, по меньшей мере, одним узлом, указанный способ осуществляется в базовом блоке системы передачи данных датчиков и/или данных управления, указанный базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее  
30 установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Способ включает

передачу по открытой беспроводной сети сообщения-запроса на подключение, причем указанное сообщение-запрос на подключение передается с использованием заранее установленной схемы и кодируется с помощью указанного  
35 первого ключа шифрования,

прием по открытой беспроводной сети, по меньшей мере, одного сообщения-идентификатора, содержащего идентификатор блока подключенного узла, причем указанное принятое сообщение-идентификатор передается с использованием

заранее установленной схемы и шифруется с использованием первого ключа шифрования и,

расшифровку полученного сообщения-ответа,

5 инициирование процедуры сопряжения, по меньшей мере, с одним из подключенных узлов, указанная процедура сопряжения включает передачу дополнительных настроек для взаимодействия по защищенной сети с, по меньшей мере, одним из подключенных узлов (102; 103, 104), указанные дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети, и

10 инициирование защищенной передачи данных с сопряженным узлом (узлами), в котором для защищенной передачи данных используется, по меньшей мере, один уникальный второй ключ шифрования для шифрования/расшифровки передаваемых сообщений.

Настоящее изобретение также относится к способу, выполняемому в узле для взаимодействия с базовым блоком системы передачи данных датчиков и/или данных управления, указанный узел имеет сохраненные в нем настройки для передачи данных по сети с использованием открытой сети и уникального идентификатора блока, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных между устройствами, имеющими первый ключ шифрования.

20 Способ включает

прием от базового блока по открытой беспроводной сети сообщения-запроса на подключение, указанное сообщение-запрос на подключение передается с использованием заранее установленной схемы передачи данных по сети и кодируется с помощью первого ключа шифрования,

25 расшифровку полученного сообщения-запроса на подключение, после успешной расшифровки сообщения-запроса на подключение, передачу (403) по открытой беспроводной сети сообщения-идентификатора, содержащего идентификатор блока узла, указанное сообщение-идентификатор передается с использованием предварительно установленной схемы передачи данных и кодируется с помощью первого ключа шифрования,

30 получение по открытой сети дополнительных настроек для передачи данных по защищенной сети, указанные дополнительные настройки для передачи данных по сети включают, по меньшей мере, один уникальный второй ключ шифрования, и

35 инициирование защищенной передачи данных, при которой для шифрования/расшифровки передаваемых сообщений используется, по меньшей мере, один уникальный второй ключ шифрования.

Настоящее изобретение также относится к компьютерной программе, содержащей инструкции, которые, при выполнении программы компьютером, дают команду компьютеру выполнять любой из описанных в настоящем документе способов.

## 5 КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

На Фиг. 1 представлена схема сигнализации, показывающая примеры сигнализации в системе для передачи данных датчиков и/или данных управления пользователя.

Фиг. 2 представляет блок-схему, поясняющую пример способа взаимодействия с, по меньшей мере, одним узлом, причем указанный способ выполняется в базовом блоке системы передачи данных датчиков и/или данных управления пользователя.

Фиг. 3 представляет блок-схему, поясняющую пример способа, выполняемого на узле для взаимодействия с базовым блоком системы передачи данных датчиков и/или данных управления пользователя.

На Фиг. 4 представлена блок-схема, поясняющая пример системы климат-контроля в помещении для управления приточно-вытяжной установкой, предназначенной для воздействия на воздух в здании.

## ПОДРОБНОЕ ОПИСАНИЕ

Настоящее изобретение относится к системе передачи данных датчиков и/или данных управления пользователя в пределах заранее установленного пространства. Заранее установленное пространство может находиться внутри здания или в ином ограниченном или контролируемом пространстве. Система содержит базовый блок, выполненный для беспроводной передачи данных с использованием открытой сети, причем базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Система дополнительно содержит, по меньшей мере, один узел, содержащий блок датчиков и/или пользовательский блок управления, причем каждый указанный узел имеет сохраненные в нем указанные настройки для передачи данных по сети и идентификатор блока, однозначно идентифицирующий узел. Базовый блок и, по меньшей мере, один узел выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и взаимодействовать по сети ввода, используя указанный первый ключ шифрования и в соответствии с упомянутой заранее установленной схемой передачи данных по сети. Базовый блок выполнен с возможностью инициирования процедуры сопряжения с, по меньшей мере, одним из найденных узлов сети ввода, указанная процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из найденных узлов, указанные дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для

использования при защищенной передаче данных по защищенной сети. Каждый сопряженный узел добавляется в защищенную сеть для передачи данных между базовым блоком и сопряженными узлами после завершения процедуры сопряжения.

5 Схема сигнализации на Фиг. 1 представляет пример сигнализации для описанной выше системы передачи данных датчика и/или данных управления пользователя в пределах заранее установленного пространства.

Система может представлять собой систему мониторинга для наблюдения за одним или множеством датчиков.

Система может представлять собой систему управления процессом, таким как

- 10
- инъекционное формование и печать,
  - процессы производства сухого молока и других пищевых продуктов,
  - производство аккумуляторных батарей, медицинских субстанций или другими химическими процессами
  - защита зданий, мостов, ветряных турбин, оборудования и исторических
- 15 артефактов в музеях,
- реконструкция зданий и других сооружений, поврежденных влагой, или
  - контроль процесса отверждения бетонных или склеенных изделий, созревания сыра, выдерживания фруктов и молочных продуктов.

В различных вариантах осуществления система представляет собой систему климат-контроля в помещении для управления приточно-вытяжной установкой, предназначенной для воздействия на воздух в здании.

Схема сигнализации представляет собой схему передачи данных между базовым блоком 101 и, по меньшей мере, одним узлом 102.

25 Базовый блок 101 может представлять собой базовый блок, подключенный к приточно-вытяжной установке или встроенный в приточно-вытяжную установку, предназначенную для воздействия на воздух в здании. Таким образом, базовый блок 101 является частью системы климат-контроля в помещении, управляющей приточно-вытяжной установкой.

30 Базовый блок имеет сохраненные в нем настройки для беспроводной передачи данных по сети с использованием открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Настройки могут дополнительно содержать идентификатор сети ввода или идентификатор PAN (personal area network – персональная сеть) для сети ввода. Идентификатор сети ввода используется для

35 однозначной идентификации сети ввода. Устройства в одной сети должны совместно использовать идентификатор (идентификаторы) сети.

Настройки являются общими для блоков, предназначенных для подключения к системе. Фактически, настройки являются уникальными для одного или нескольких производителей блоков и/или предназначены для использования с системой передачи

данных датчиков и/или данных управления пользователя. Характерно, что настройки сохраняются в соответствующем блоке при его изготовлении. Настройки хранятся в секрете для предотвращения несанкционированного использования. Блоки, имеющие настройки, размещаются таким образом, чтобы осуществлять связь друг с другом в соответствии с заранее установленной схемой в сети ввода. По меньшей мере, один узел 102 содержит, например, пользовательский блок управления и/или блок датчиков.

Чтобы найти узлы, предназначенные для взаимодействия с базовым блоком 101 в сети ввода, базовый блок передает сообщение-запрос на подключение M1, зашифрованное с помощью первого ключа шифрования, по открытой беспроводной сети, используя заранее установленную схему передачи данных. Узел (узлы) предназначен для приема и расшифровки сообщения-запроса на подключение, если он находится в зоне досягаемости связи по открытой беспроводной сети. Если узел способен принять и расшифровать сообщение-запрос на подключение, то узел подключен к сети ввода. После подключения узел передает сообщение-ответ M2. Сообщение-ответ M2 передается по заранее установленной схеме и шифруется с использованием первого ключа шифрования. Сообщение-ответ содержит идентификатор блока узла.

Предполагается, что базовый блок и узлы синхронизированы для обеспечения передачи сообщений согласно заранее установленной схеме. Такая синхронизация известна в данной области техники и не описывается подробно в настоящем документе. Например, соответствующий узел может содержать кристалл, откалиброванный с помощью сети. После приема и расшифровки сообщения-ответа M2 базовый блок 101 распознает, что подключенный узел найден.

Базовый блок 101 и узел 102 выполнены с возможностью передачи данных друг другу в соответствии с заранее установленной схемой, используя первый ключ шифрования для шифрования сообщений. Это показано в виде двунаправленного сообщения M3 на Фиг. 1.

После принятия базовым блоком решения о выполнении сопряжения с одним или несколькими из подключенных узлов для обеспечения защищенной связи, базовый блок передает сообщение M4, содержащее дополнительные настройки для передачи данных выбранным узлам по защищенной сети. Настройки содержат, по меньшей мере, второй уникальный ключ шифрования для защищенной передачи данных. Настройки могут дополнительно содержать время запуска защищенной передачи данных между узлом 102 и базовым блоком 101.

Таким образом, базовый блок 101 и узел 102 подключаются для защищенной передачи данных и, следовательно, выполнены с возможностью защищенной передачи данных с использованием второго уникального ключа шифрования. Защищенная передача данных предпочтительно осуществляется по заранее установленной схеме. В другом варианте осуществления, защищенная передача данных выполняется в соответствии с другой схемой защищенной передачи данных, при этом схема защищенной передачи

данных может быть предварительно сохранена в базовом блоке и узлах. Защищенная передача данных показана в виде двунаправленного сообщения М5 на Фиг. 1.

На Фиг. 2 представлен пример способа 200 для передачи данных с, по меньшей мере, одним заданным узлом. Способ 200 выполняется в базовом блоке системы передачи данных датчиков и/или данных управления пользователя, указанный базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования.

10 Способ 200 включает этап передачи 201 по открытой беспроводной сети сообщения-запроса на подключение, причем указанное сообщение-запрос на подключение передается с помощью заранее установленной схемы и кодируется с использованием указанного первого ключа шифрования,

15 Способ 200 дополнительно включает этап 202 приема по открытой беспроводной сети, по меньшей мере, одного сообщения-ответа, содержащего идентификатор блока подключенного узла, причем указанное принятое сообщение-ответ передается с помощью заранее установленной схемы и шифруется с использованием первого ключа шифрования.

Способ дополнительно включает этап 203 расшифровки принятого сообщения ответа.

20 Затем либо автоматически, либо вручную может инициироваться процедура сопряжения 205.

В инициированном пользователем примере подключенные узлы представлены 203 в пользовательском интерфейсе для выбора пользователем узла (узлов) для сопряжения, и обнаружен выбор пользователя, по меньшей мере, одного узла для сопряжения. Затем, 25 по меньшей мере, один выбранный пользователем узел регистрируется в базовом блоке, и инициируется процедура сопряжения для выбранного пользователем узла (узлов).

Процедура сопряжения включает передачу 206 дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из подключенных узлов (102; 103, 104), указанные дополнительные настройки включают, по меньшей мере, один 30 второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети.

Способ дополнительно включает этап инициирования 207 защищенной передачи данных с сопряженным узлом (узлами), в котором для защищенной передачи данных используется, по меньшей мере, один уникальный второй ключ шифрования для 35 шифрования/расшифровки передаваемых сообщений. Инициирование 207 защищенной передачи данных может включать в себя отправку времени запуска защищенной сети узлам, которые подлежат включению в защищенную сеть. Таким образом, передача данных с использованием второго уникального ключа шифрования начинается как на базовом блоке, так и на задействованном узле (узлах) в переданное время.

На Фиг.3 представлен пример способа 300, выполняемого в узле для взаимодействия с базовым блоком системы передачи данных датчиков и/или данных управления, указанный узел имеет сохраненные в нем настройки для передачи данных по сети с использованием открытой сети и уникальный идентификатор блока, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Узел содержит, например, по меньшей мере, один блок датчиков. Блок (блоки) датчиков может быть выполнен с возможностью определения, по меньшей мере, одного из следующих параметров:

- 10                   • относительная влажность,
- точка росы,
- обычные атмосферные газы, такие как кислород, азот, углекислый газ,
- летучие органические соединения, ЛОС,
- температура,
- 15                   • химическое вещество (вещества) в газообразной форме, такое как радон,
- атмосферное давление,
- уровень звукового давления,
- электромагнитные поля,
- условия освещения,
- 20                   • аэрозоли, и
- частицы.

В примере узел содержит, по меньшей мере, один пользовательский блок управления. Пользовательский блок управления может содержать интерфейс ввода для установки параметра, относящегося к управлению технологическим процессом,

25                   Способ включает прием 301 по открытой беспроводной сети сообщения-запроса на подключение от базового блока, при этом указанное принятое сообщение-запрос на подключение передается с использованием заранее установленной схемы передачи данных по сети и кодируется с использованием первого ключа шифрования.

30                   Способ дополнительно включает этап 302 расшифровки принятого сообщения-запроса на подключение. После успешной расшифровки сообщения-запроса на подключение узел считается подключенным.

35                   Способ дополнительно включает этап, после успешной расшифровки сообщения-запроса на подключение, передачи 303 по открытой беспроводной сети сообщения-ответа в форме сообщения-идентификатора, содержащего идентификатор блока узла. Сообщение-идентификатор передается с использованием заранее установленной схемы передачи данных по сети и кодируется с использованием первого ключа шифрования. Такая процедура может повторяться с заранее установленными интервалами до тех пор, пока не будут получены настройки защищенной передачи данных.

Способ дополнительно включает этап 304 приема по открытой сети дополнительных настроек для передачи данных по защищенной сети, указанные дополнительные настройки для передачи данных содержат, по меньшей мере, один уникальный второй ключ шифрования.

5 Способ дополнительно включает инициирование 305 защищенной передачи данных, в котором при защищенной передаче данных, по меньшей мере, один уникальный второй ключ шифрования используется для шифрования/расшифровки передаваемых сообщений. Инициирование 305 защищенной передачи данных может включать  
10 получение от базового блока времени для запуска защищенной сети. Таким образом, передача данных с использованием второго уникального ключа шифрования запускается как на базовом блоке, так и на узле (узлах) в переданное время.

Если узел содержит пользовательский блок управления, пользовательский блок управления может передавать в базовый блок информацию, относящуюся к параметрам, заданным в пользовательском блоке управления. Такие передачи могут выполняться в  
15 сети ввода и/или защищенной сети.

Если узел содержит блок датчиков, блок датчиков может передавать данные датчика в базовый блок. Такие передачи могут выполняться в сети ввода и/или защищенной сети. Способы, описанные в настоящем изобретении, могут быть реализованы в компьютерных программах, содержащих инструкции, которые, при выполнении  
20 программы компьютером, дают команду компьютеру выполнять способы.

На Фиг.4 представлена система, описанная в настоящем документе, применительно к системе 400 климат-контроля в помещении для управления приточно-вытяжной установкой 105, предназначенной для воздействия на воздух в здании.

Приточно-вытяжная установка 105 предназначена для охлаждения и/или подогрева,  
25 и/или обезвоживания, и/или осушения и/или очистки воздуха внутри здания. Приточно-вытяжная установка 105 представляет собой, например, испарительный увлажнитель и/или охладитель. Таким образом, приточно-вытяжная установка 105 используется для увлажнения и/или охлаждения помещений различных типов в зданиях. Другими видами приточно-вытяжных установок являются влагопоглотители, теплообменники или  
30 фильтрующие устройства.

Система 400 содержит, например, базовый блок 101, соединенный с приточно-вытяжной установкой 105. В примере базовый блок 101 является автономным базовым блоком 101. В другом варианте осуществления базовый блок может быть встроен в приточно-вытяжную установку 105.

35 Функция базового блока 101 рассчитана на предоставление данных приточно-вытяжной установке, предназначенных для управления приточно-вытяжной установкой. Базовый блок 101 функционирует как интерфейс между приточно-вытяжной установкой 105 и удаленными блоками, такими как сенсорные блоки 103 и/или пользовательские блоки управления 104.

Базовый блок 101 может содержать память 106 для хранения данных и процессор. Базовый блок 101 может содержать дисплей 107 и средства взаимодействия с пользователем 108 для ввода данных пользователя.

5 Базовый блок 101 имеет сохраненные в нем настройки, содержащие первый ключ шифрования и заранее установленную схему передачи данных по сети между устройствами, имеющими первый ключ шифрования. Настройки определяют начальный адрес системы передачи данных и, в некоторых случаях, приточно-вытяжную установку 105, к которой она подключена или в которую встроена. Настройки обычно кодируются в аппаратном или программном обеспечении базового  
10 устройства при изготовлении. По меньшей мере, часть настроек предпочтительно скрыта в аппаратном или программном обеспечении, что позволяет предотвратить несанкционированный доступ. Настройки могут храниться в памяти 106.

Базовый блок 101 выполнен с возможностью беспроводной передачи данных посредством беспроводной открытой сети и настроек, как описано в настоящем  
15 изобретении. Сеть, использующая беспроводную открытую сеть и описанные здесь настройки, называется сетью ввода. Открытая сеть может быть ячеистой сетью.

По меньшей мере, один узел 103, 104, предназначенный для взаимодействия с базовым блоком, может находиться в зоне досягаемости связи по открытой беспроводной сети с базовым блоком 101. Узел 103, 104 может содержать память 111 для хранения данных и  
20 процессор. Узел 103, 104 может содержать дисплей 109 и/или средство взаимодействия с пользователем 110 для ввода данных пользователя.

Каждый узел имеет сохраненные в нем настройки, такие же, как и в базовом блоке. Как описано выше, настройки идентифицируют начальный адрес системы передачи данных датчиков и/или данных управления пользователя и, при необходимости, приточно-вытяжную установку, для которой предназначена система передачи данных датчиков  
25 и/или данных управления пользователя. Как упоминалось выше, настройки обычно кодируются в аппаратном или программном обеспечении узла при изготовлении. По меньшей мере, часть настроек предпочтительно скрыта в аппаратном или программном обеспечении, что позволяет предотвратить несанкционированный доступ. Каждый узел  
30 дополнительно содержит сохраненный в нем идентификатор блока, опознающий узел. Настройки и идентификатор блока могут храниться в памяти 111.

Как ясно из вышеизложенного, каждый, по меньшей мере, один узел содержит блок датчиков 103 и/или пользовательский блок управления 104.

Пользовательские средства ввода 110 пользовательского блока управления 104 могут  
35 содержать интерфейс ввода для установки уровня температуры и/или влажности.

В данной заявке, по меньшей мере, один блок 103 датчиков может содержать, по меньшей мере, один датчик для определения, по меньшей мере, одного из следующих параметров:

- относительная влажность,

- точка росы, и
- температура.

Базовый блок 101 и, по меньшей мере, один узел 103, 104 выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и  
5 передачи данных по сети ввода, используя указанный первый ключ шифрования и в соответствии с заранее установленной схемой передачи данных по сети.

Более подробно, базовый блок 101 выполнен с возможностью передачи сообщения-запроса, зашифрованного первым ключом шифрования, и соответствующий узел выполнен с возможностью приема и расшифровки сообщения-запроса, закодированного  
10 первым ключом шифрования, причем базовый блок 101 и соответствующий узел (102; 103, 104) соединены. Таким образом, соответствующий подключенный узел выполнен с возможностью передачи сообщения-ответа в форме сообщения-идентификатора, зашифрованного с помощью первого ключа шифрования, причем указанное сообщение-идентификатор содержит идентификатор блока. Таким образом, базовая станция  
15 выполнена с возможностью приема и расшифровки соответствующего сообщения-идентификатора.

Передача данных осуществляется по сети ввода в соответствии с заранее установленной схемой передачи данных между устройствами, имеющими настройки, описанные в настоящем изобретении. Заранее установленная схема определяет характерные  
20 временные интервалы для передачи данных. Передача данных может, например, основываться на синхронизированном по времени переключении каналов, СВПК. Это означает, что временные интервалы передачи данных невелики, и, следовательно, система обладает высокой энергоэффективностью. Передача данных по сети ввода шифруется с помощью первого ключа шифрования.

Как описано выше, базовый блок 101 и, по меньшей мере, один узел 103, 104 выполнены с возможностью передачи данных друг другу по сети ввода. Например, пользовательский блок (блоки) управления 104 может быть выполнен с возможностью передачи информации, относящейся к заданной температуре и/или влажности, базовому блоку 101 по сети ввода. Таким образом, базовый блок 101 выполнен с возможностью  
30 приема передаваемой информации. Базовый блок 101 может быть выполнен с возможностью отображения, по меньшей мере, части принятой информации, относящейся к заданной температуре и/или влажности.

Например, блок (блоки) датчиков 103 может быть выполнен с возможностью передачи данных датчиков в базовый блок 101 по сети ввода. Таким образом, базовый блок 101  
35 выполнен с возможностью приема переданных данных датчика. Базовый блок может быть выполнен с возможностью отображения, по меньшей мере, части принятых данных датчика.

В варианте осуществления данные, передаваемые от пользовательского блока (блоков) управления 104 и/или блока(блоков) датчиков 103 по сети ввода, не используются для управления приточно-вытяжной установкой.

5 Кроме того, базовый блок 101 выполнен с возможностью инициирования процедуры сопряжения, по меньшей мере, с одним из узлов сети ввода. Процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из подключенных узлов. Дополнительные настройки могут также называться правами доступа для защищенной передачи данных. Дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для защищенной сети и для использования при защищенной передаче 10 данных по защищенной сети. В предпочтительном варианте осуществления, по меньшей мере, один блок датчиков 103 и, по меньшей мере, один пользовательский блок управления 104 подключены к защищенной сети.

15 В приведенном примере дисплей 107 базового блока выполнен с возможностью представления перечня подключенных, несопряженных узлов. Средства взаимодействия с пользователем 108 базового блока 102 обеспечивают выбор пользователем узла (узлов) для сопряжения из списка, после чего выбранный пользователем узел (узлы) регистрируется в базовом блоке 102, и процедура сопряжения выполняется для выбранного пользователем узла (узлов).

20 Сопряжение — это процесс, используемый в компьютерных сетях, который помогает установить соединения между вычислительными устройствами для обеспечения передачи данных между ними. В контексте настоящего изобретения соединение между вычислительными устройствами уже присутствует, как описано выше, благодаря настройкам. В контексте изобретения сопряжение выполняется для настройки 25 соединения для передачи данных в защищенной сети.

В примере дополнительные настройки содержат в дополнение ко второму уникальному ключу шифрования идентификатор защищенной сети или идентификатор PAN для защищенной сети. В примере уникальный идентификатор сети используется для однозначной идентификации защищенной сети. Как упоминалось в отношении сети 30 ввода, устройства в одной сети должны совместно использовать идентификатор(ы) сети. В процессе сопряжения узлу (узлам) передается второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети. Переданный второй уникальный ключ шифрования затем сохраняется в соответствующем узле 103, 104 и используется в последующей защищенной передаче данных. Кроме того, если 35 присутствует, идентификатор защищенной сети или идентификатор PAN для защищенной сети, он также передается узлу (узлам) и хранится в нем.

Как ясно из вышеизложенного, второй уникальный ключ шифрования для передачи данных по защищенной сети передается по сети ввода с помощью заранее

установленной схемы передачи данных. То же самое применимо к идентификатору защищенной сети или идентификатору PAN для защищенной сети, при наличии.

Шифрование, используемое в защищенной передаче данных, как правило, представляет собой симметричный блочный шифр. Например, для шифрования (и последующей расшифровки) используется расширенный стандарт шифрования AES. Длина блока блочного шифра, используемого в AES, составляет, например, 128, или 192, или 256 бит. В примере второй уникальный ключ шифрования, т.е. блок, генерируется в базовом блоке при сопряжении. В соответствии с этим примером, второй уникальный ключ шифрования не хранится ни в одном из блоков до момента использования. Это повышает безопасность. Риск несанкционированного доступа ко второму ключу шифрования минимизируется. Идентификатор защищенной сети или идентификатор PAN для защищенной сети также может генерироваться на базовом блоке в связи с сопряжением таким же образом, как и второй уникальный ключ шифрования.

Защищенная передача данных начинается после завершения процедуры сопряжения. Дисплей базового блока в примере выполнен с возможностью отображения узлов, подключенных к защищенной сети. Средства взаимодействия с пользователем могут обеспечивать управление узлами, подключенными к защищенной сети, указанное управление может включать удаление узлов. Это означает, что представленные сопряженные узлы могут выбираться для разрыва сопряжения, а представленные несопряженные узлы могут выбираться для сопряжения. Удаление узла, т.е. разрыв сопряжения узла, может включать информирование узла базовым блоком о том, что он не сопряжен, и узел в ответ на это удаляет или компрометирует второй уникальный ключ шифрования, так что он больше не может использоваться.

Базовый блок может быть выполнен с возможностью отправки времени запуска защищенной сети узлам, подлежащим добавлению в защищенную сеть, и передача данных с использованием второго уникального ключа шифрования запускается как в базовом блоке, так и в задействованном узле (узлах) в переданное время, посредством чего узлы добавляются в защищенную сеть.

По меньшей мере, часть данных, передаваемых от блока (блоков) датчиков и/или блока (блоков) управления пользователя базовому блоку по защищенной сети, передается в приточно-вытяжную установку для управления ею. Таким образом, обычно базовый блок выполнен с возможностью использования данных, полученных от узла (узлов) по сети ввода, для отображения и возможных других применений, не влияющих на приточно-вытяжную установку. Базовый блок дополнительно выполнен с возможностью использования данных, полученных от узла (узлов) по защищенной сети, для передачи данных для управления приточно-вытяжной установкой. Кроме того, обновления программного обеспечения, передаваемые с базового блока на узлы, могут разрешаться только по защищенной сети.

Как правило, используемая открытая сеть представляет собой ячеистую сеть. Таким образом, решение, представленное в настоящем изобретении, обеспечивает передачу данных с подключенными узлами в сети ввода и защищенную передачу данных в защищенной сети также тогда, когда базовый блок и блок (блоки) датчиков/блок(блоки) управления пользователя не находятся в прямой связи.

5

**ФОРМУЛА ИЗОБРЕТЕНИЯ**

1. Система (100) передачи данных датчиков и/или данных управления в пределах заранее установленного пространства, система содержит

5

базовый блок (101), выполненный с возможностью беспроводной передачи данных с использованием открытой сети, при этом базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи данных по сети между

10

устройствами, имеющими первый ключ шифрования, по меньшей мере, один узел (102, 103, 104), содержащий блок датчиков и/или пользовательский блок управления, при этом указанный узел имеет сохраненные в нем указанные настройки для передачи данных по сети и идентификатор блока, идентифицирующий узел, и

15

причем базовый блок (101) и, по меньшей мере, один узел (102, 103, 104) выполнены с возможностью находить друг друга с помощью указанных настроек для передачи данных по сети, и передавать данные по сети ввода, используя указанный первый ключ шифрования и в соответствии с упомянутой заранее установленной схемой передачи данных по сети, и

20

при этом базовый блок (101) выполнен с возможностью инициирования процедуры сопряжения с, по меньшей мере, одним из найденных узлов сети ввода, указанная процедура сопряжения включает передачу дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из найденных узлов (102, 103, 104), указанные дополнительные настройки включают, по меньшей мере, один второй уникальный ключ шифрования для использования при защищенной передаче данных по защищенной сети, и

25

30

причем каждый сопряженный узел (102, 103, 104) добавляется в защищенную сеть после завершения процедуры сопряжения.

35

2. Система передачи данных датчиков и/или данных управления по п. 1, отличающаяся тем, что

базовый блок (101) выполнен с возможностью передачи сообщения-запроса, зашифрованного первым ключом шифрования, а соответствующий узел выполнен

с возможностью приема и расшифровки сообщения-запроса, закодированного первым ключом шифрования, посредством чего базовый блок (101) и соответствующий узел (102, 103, 104) находят друг друга,

- 5 соответствующий найденный узел выполнен с возможностью передачи сообщения-идентификатора, зашифрованного с помощью первого ключа шифрования, указанное сообщение-идентификатор содержит идентификатор блока, и
- 10 базовая станция выполнена с возможностью приема и расшифровки соответствующего сообщения-идентификатора.
3. Система передачи данных датчиков и/или данных управления по п. 1 или 2, отличающаяся тем, что указанный базовый блок дополнительно содержит дисплей и средства взаимодействия с пользователем.
- 15
4. Система передачи данных датчиков и/или данных управления по п. 3, отличающаяся тем, что дисплей базового блока выполнен с возможностью предоставления списка найденных узлов на основе принятого и расшифрованного идентификатора (идентификаторов) блока, при этом средства взаимодействия с пользователем предоставляют пользователю выбор узла (узлов) для сопряжения из списка найденных узлов, после чего выбранный пользователем узел (узлы) регистрируется в базовом блоке, и инициируется процедура сопряжения для выбранного пользователем узла (узлов).
- 20
- 25
5. Система передачи данных датчиков и/или данных управления по любому из пп.3 - 4, отличающаяся тем, что дисплей базового блока выполнен с возможностью отображения узлов, подключенных к защищенной сети, причем средства взаимодействия с пользователем в базовом блоке обеспечивают управление узлами, подключенными к защищенной сети, указанное управление может включать удаление узлов.
- 30
- 35
6. Система передачи данных датчиков и/или данных управления по любому из предшествующих пунктов, отличающаяся тем, что базовый блок выполнен с возможностью отправки времени запуска защищенной сети узлам для добавления в защищенную сеть, и передача данных с использованием второго уникального ключа шифрования запускается как на базовом блоке, так и на задействованном узле (узлах) в переданное время, посредством чего узлы добавляются в защищенную сеть.

7. Система передачи данных датчиков и/или данных управления по любому из предшествующих пунктов, отличающаяся тем, что, по меньшей мере, один блок датчиков и, по меньшей мере, один пользовательский блок управления  
5 подключены к защищенной сети.
8. Система передачи данных датчиков и/или данных управления по любому из предшествующих пунктов, отличающаяся тем, что, по меньшей мере, один из узлов содержит, по меньшей мере, один пользовательский блок управления,  
10 содержащий интерфейс ввода для установки параметра, относящегося к управлению технологическим процессом, причем пользовательский блок управления выполнен с возможностью передачи информации, относящейся к установке параметра, в базовый блок.
- 15 9. Система передачи данных датчиков и/или данных управления по любому из предшествующих пунктов, отличающаяся тем, что, по меньшей мере, один из узлов содержит, по меньшей мере, один блок датчиков, выполненный с возможностью определения, по меньшей мере, одного из следующих параметров:
- относительная влажность,
  - 20 • точка росы,
  - обычные атмосферные газы, такие как кислород, азот, углекислый газ,
  - летучие органические соединения, ЛОС,
  - температура,
  - химическое вещество (вещества) в газообразной форме, такое как радон,
  - 25 • атмосферное давление,
  - уровень звукового давления,
  - электромагнитные поля,
  - условия освещения,
  - аэрозоли, и
  - 30 • частицы.
10. Система передачи данных датчиков и/или данных управления по любому из предшествующих пунктов, отличающаяся тем, что базовый блок выполнен с  
35 возможностью предоставления только данных датчиков и/или данных управления, полученных по защищенной сети, контроллеру для управления технологическим процессом.

11. Система передачи данных датчиков и/или данных управления по любому из предшествующих пунктов, отличающаяся тем, что открытая сеть является ячеистой сетью.
- 5 12. Система по любому из предшествующих пунктов, отличающаяся тем, что система является системой климат-контроля в помещении (100) для управления приточно-вытяжной установкой (105), предназначенной для воздействия на воздух в здании.
- 10 13. Система климат-контроля в помещении по п. 12, отличающаяся тем, что пользовательский блок управления содержит интерфейс ввода для установки значения температуры и/или уровня влажности, причем пользовательский блок управления выполнен с возможностью передачи на базовый блок информации, относящейся к заданной температуре и/или влажности.
- 15 14. Способ (200) передачи данных, по меньшей мере, одному узлу, указанный способ осуществляется в базовом блоке системы передачи данных датчиков и/или данных управления, указанный базовый блок имеет сохраненные в нем настройки для передачи данных по сети с использованием указанной открытой сети, указанные настройки содержат первый ключ шифрования и заранее установленную схему для  
20 передачи данных по сети между устройствами, имеющими первый ключ шифрования, указанный способ включает  
передачу (201) по открытой беспроводной сети сообщения-запроса на  
25 подключение, причем указанное сообщение-запрос на подключение передается с использованием заранее установленной схемы и кодируется с помощью указанного первого ключа шифрования,  
прием (202) по открытой беспроводной сети, по меньшей мере, одного сообщения-идентификатора, содержащего идентификатор блока присоединенного узла,  
30 указанное принятое сообщение-идентификатор передается с использованием заранее установленной схемы и шифруется с использованием первого ключа шифрования, и  
расшифровку (203) полученного сообщения-ответа,  
35 инициирование (205) процедуры сопряжения с, по меньшей мере, одним из подключенных узлов, указанная процедура сопряжения включает передачу (206) дополнительных настроек для передачи данных по защищенной сети, по меньшей мере, одному из подключенных узлов (102, 103, 104), указанные дополнительные

настройки включают, по меньшей мере, один второй уникальный ключ шифрования для использования в защищенной передаче данных по защищенной сети,

5 и

10 инициирование (207) защищенной передачи данных сопряженному узлу (узлам), в котором для защищенной передачи данных используется, по меньшей мере, один уникальный второй ключ шифрования для шифрования/расшифровки передаваемых сообщений.

15 15. Способ (200) по п. 14, дополнительно включающий этап выбора узлов для сопряжения, включающий

15 представление (204) подключенных узлов посредством интерфейса пользователя для выбора пользователем узла (узлов) для сопряжения, и

20 обнаружение выбранного пользователем, по меньшей мере, одного узла для сопряжения,

20 при этом, по меньшей мере, один выбранный пользователем узел регистрируется в базовом блоке и инициируется процедура сопряжения (205) для выбранного пользователем узла (узлов).

25 16. Способ (300), выполняемый в узле для передачи данных базовому блоку системы передачи данных датчиков и/или данных управления, указанный узел имеет сохраненные в нем настройки для передачи данных по сети с использованием открытой сети и уникального идентификатора блока, указанные настройки содержат первый ключ шифрования и заранее установленную схему передачи  
30 данных по сети между устройствами, имеющими первый ключ шифрования, указанный способ включает

35 прием (401) по открытой беспроводной сети сообщения-запроса на подключение от базового блока, указанное принятое сообщение-запрос на подключение передается с использованием заранее установленной схемы передачи данных по сети и кодируется с использованием первого ключа шифрования,

расшифровку полученного сообщения-запроса на подключение,

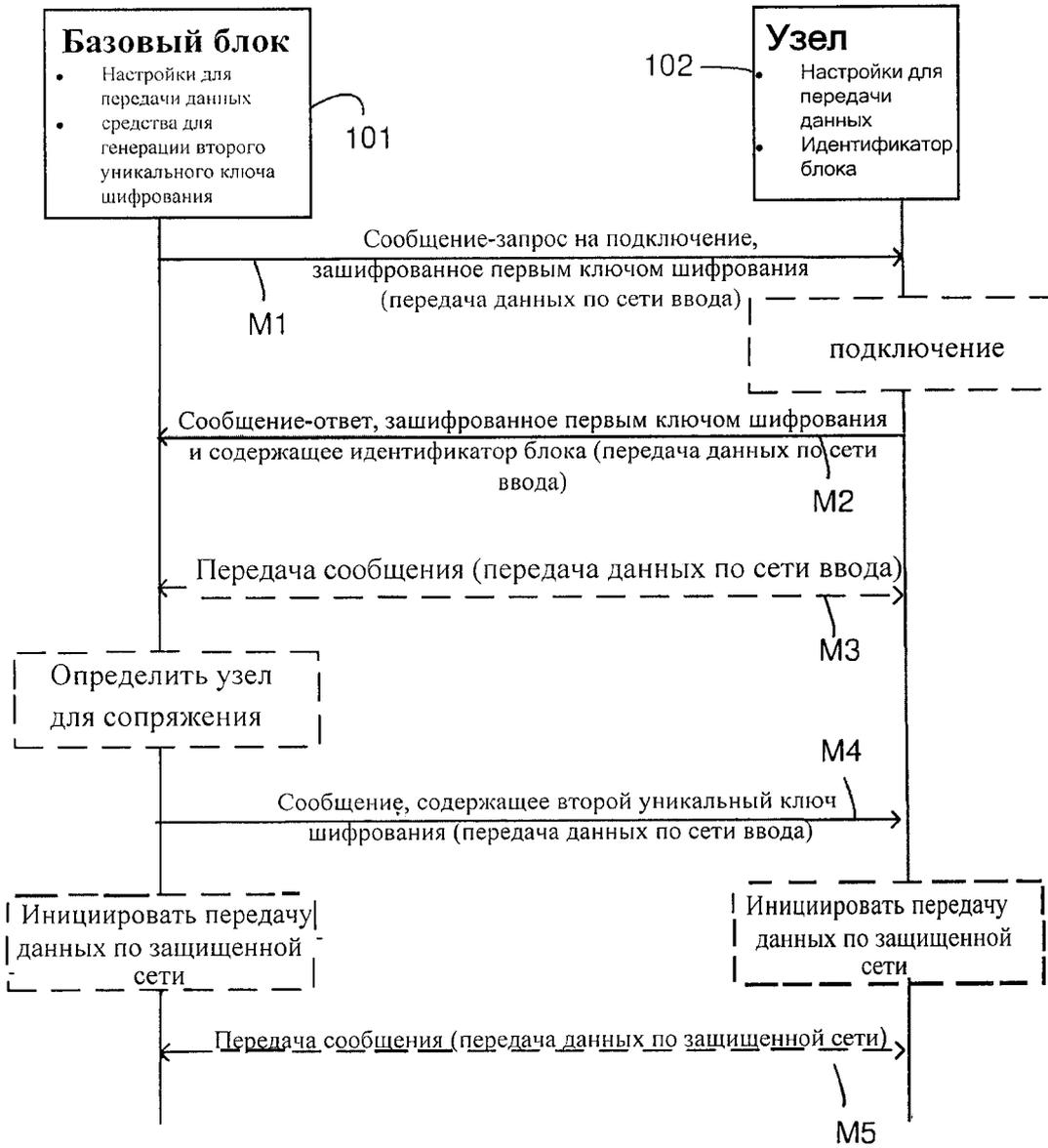
после успешной расшифровки сообщения-запроса на подключение, передачу (403) по открытой беспроводной сети сообщения-идентификатора, содержащего идентификатор блока узла, указанное сообщение-идентификатор передается с использованием заранее установленной схеме передачи данных по сети и кодируется с помощью первого ключа шифрования,

прием (404) по открытой сети дополнительных настроек для передачи данных по защищенной сети, указанные дополнительные настройки для передачи данных содержат, по меньшей мере, один уникальный второй ключ шифрования, и

инициирование (405) защищенной передачи данных, в котором при защищенной передаче данных используется, по меньшей мере, один уникальный второй ключ шифрования для шифрования/расшифровки передаваемых сообщений.

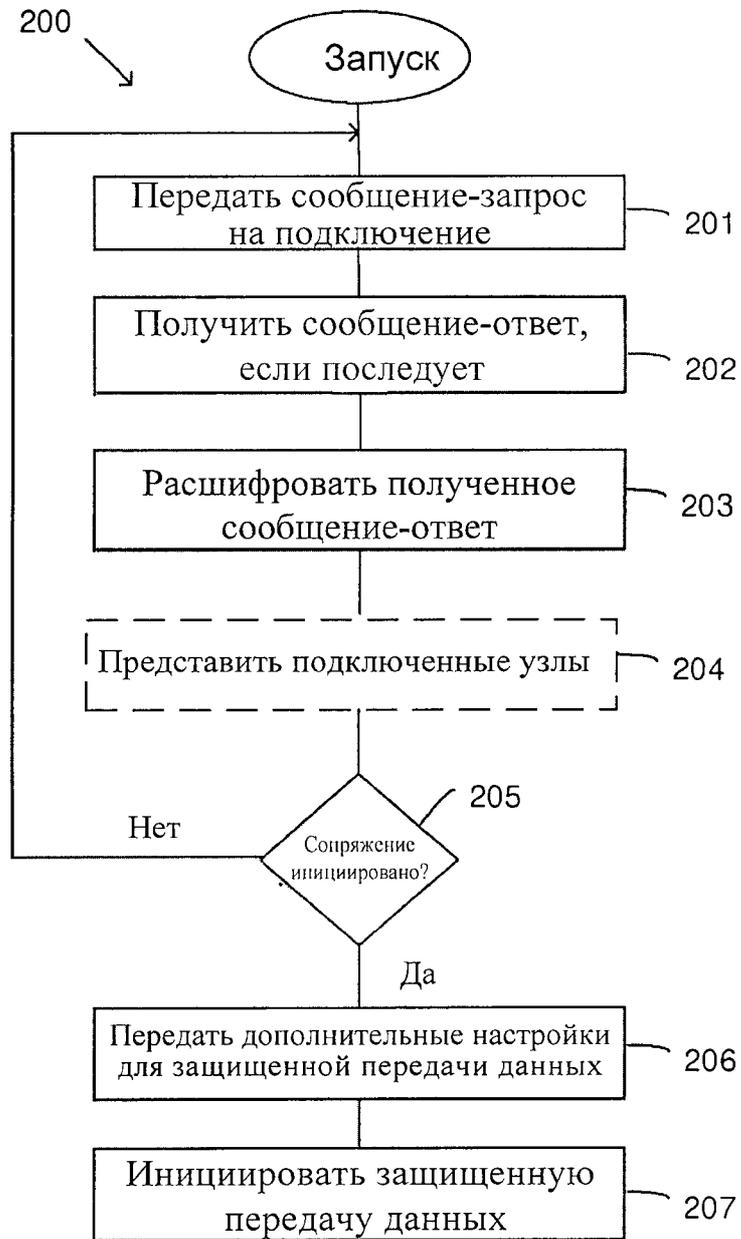
- 15 17. Компьютерная программа, содержащая инструкции, которые, при выполнении программы компьютером, влекут осуществление компьютером способа по любому из пунктов 14-16.

Фиг. 1



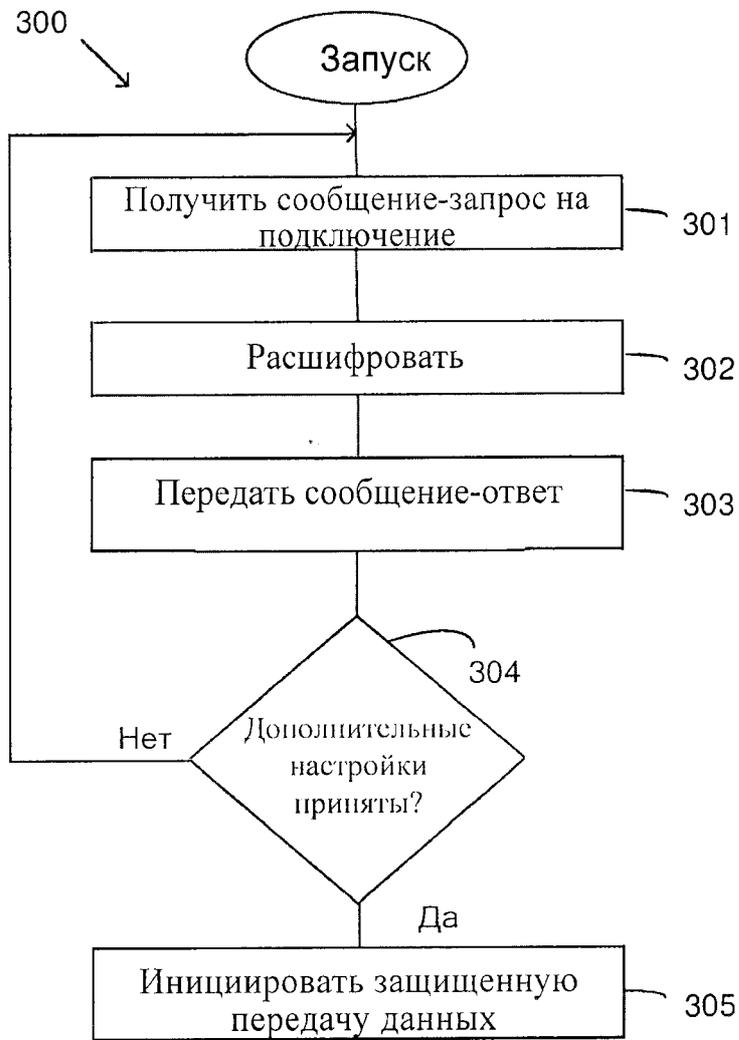
2/4

Фиг. 2



3/4

Фиг. 3



4/4

Фиг. 4

