



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК

G06F 17/00 (2019.05); H04L 12/407 (2019.05); H04L 9/08 (2019.05)

(21)(22) Заявка: 2018133842, 26.09.2018

(24) Дата начала отсчета срока действия патента:
26.09.2018

Дата регистрации:
23.07.2019

Приоритет(ы):

(22) Дата подачи заявки: 26.09.2018

(45) Опубликовано: 23.07.2019 Бюл. № 21

Адрес для переписки:

117463, Москва, а/я 38, М.А.Черняеву

(72) Автор(ы):

Гурин Олег Дмитриевич (RU)

(73) Патентообладатель(и):

Гурин Олег Дмитриевич (RU)

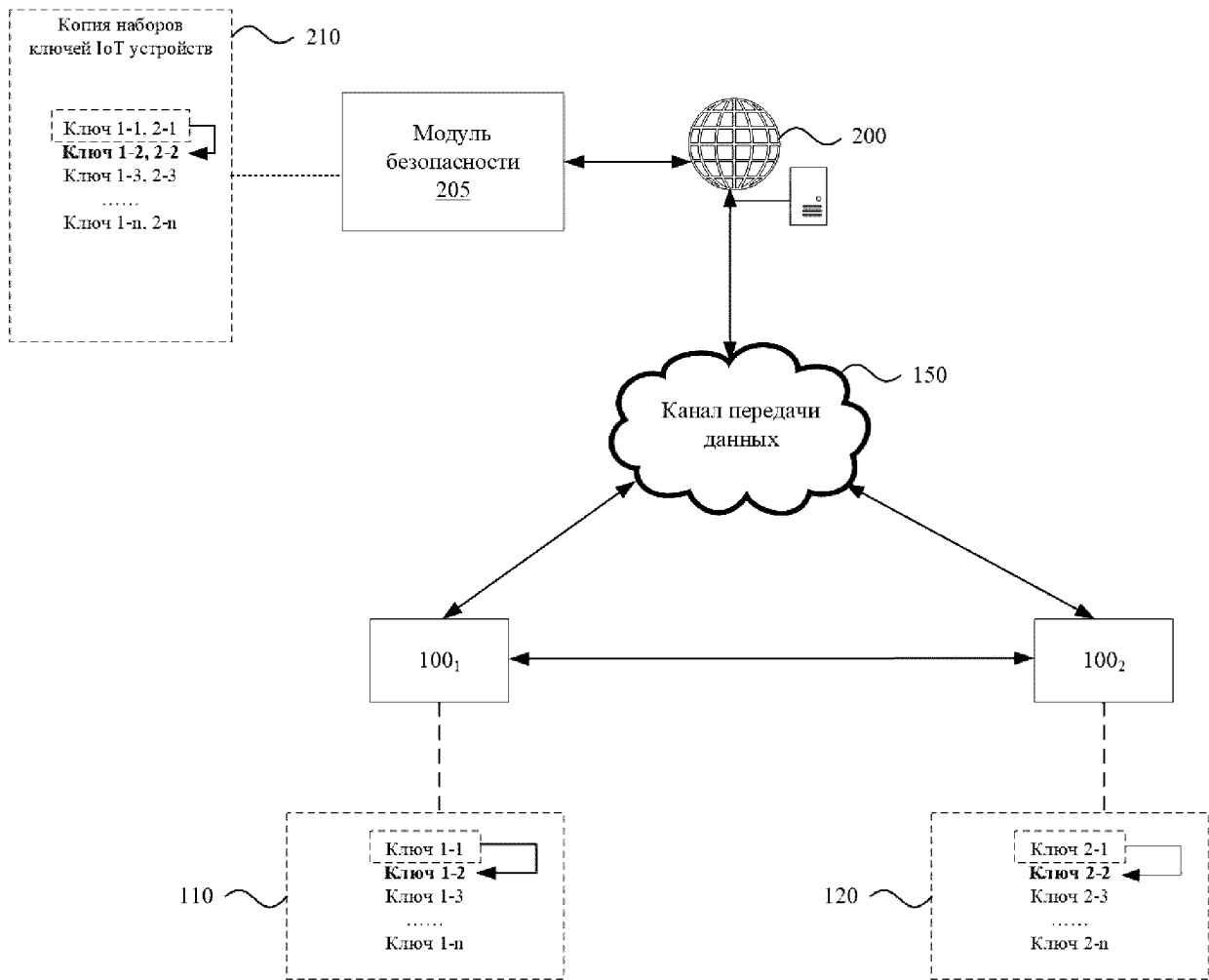
(56) Список документов, цитированных в отчете
о поиске: CN 106910367 A, 30.06.2017. CN
107682331 A, 09.02.2018. US 2018/0183587 A1,
28.06.2018. WO 2017/167741 A1, 05.10.2017. RU
2621182 C1, 31.05.2017.

(54) СПОСОБ И СИСТЕМА ОБЕСПЕЧЕНИЯ ВЗАИМОДЕЙСТВИЯ УСТРОЙСТВ ИНТЕРНЕТА
ВЕЩЕЙ (IOT)

(57) Реферат:

Изобретение относится к области организации схем сетевого обмена данными между множеством устройств, в частности для обмена данными между устройствами интернета вещей (IoT). Техническим результатом является повышение защиты информационного обмена данными между устройствами за счет организации доверенной среды взаимодействия и снабжения каждого участника информационного обмена в доверенной среде защищенным модулем безопасности, в среде которого выполняются все

необходимые операции для осуществления обмена данными с помощью набора симметричных ключей доступа. Заявленное решение осуществляется с помощью обеспечения доверенной среды обмена пакетами данных между IoT устройствами, в которой каждое из IoT устройств снабжено модулем безопасности, содержащим симметричные наборы ключей, используемых для шифрования, подписания и проверки передаваемых пакетов данных. 2 н. и 22 з.п. ф-лы, 8 ил.



Фиг. 4



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) **ABSTRACT OF INVENTION**

(52) CPC

G06F 17/00 (2019.05); *H04L 12/407* (2019.05); *H04L 9/08* (2019.05)(21)(22) Application: **2018133842, 26.09.2018**(24) Effective date for property rights:
26.09.2018Registration date:
23.07.2019

Priority:

(22) Date of filing: **26.09.2018**(45) Date of publication: **23.07.2019** Bull. № 21

Mail address:

117463, Moskva, a/ya 38, M.A.Chernyaevu

(72) Inventor(s):

Gurin Oleg Dmitrievich (RU)

(73) Proprietor(s):

Gurin Oleg Dmitrievich (RU)(54) **METHOD AND SYSTEM FOR INTERACTION OF DEVICES OF THE INTERNET OF THINGS (IOT)**

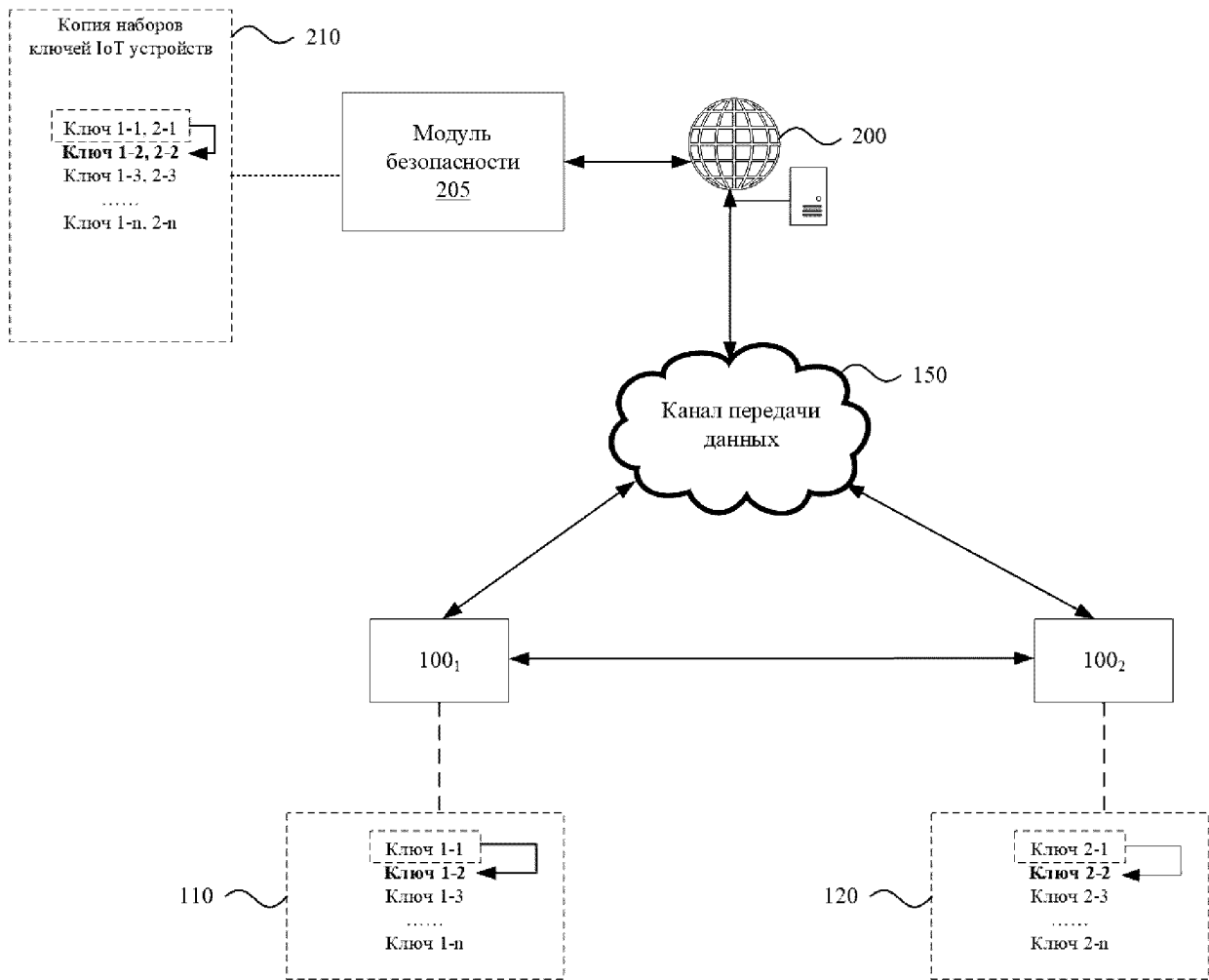
(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to arrangement of network communication schemes between multiple devices, in particular for data exchange between devices of Internet of things (IoT). Solution is carried out by providing a trusted medium for exchanging data packets between IoT devices, in which each of the IoT devices is equipped with a security module, containing symmetrical sets of keys used for encryption, signing and verification of transmitted data packets.

EFFECT: technical result is improved protection of information exchange of data between devices by organizing a trusted interaction medium and supply each participant of information exchange in a trusted environment with a secure security module, in the medium of which all necessary operations are performed to perform data exchange using a set of symmetric access keys.

24 cl, 8 dwg



Фиг. 4

Область техники

[0001] Настоящее техническое решение относится к области организации схем сетевого обмена данными между множеством устройств, в частности, для обмена данными между устройствами интернета вещей (IoT).

Уровень техники

[0002] На сегодняшний день IoT решения массово внедряются в различных областях и, как правило, такие решения жестко привязаны к программной логике контрольного устройства, осуществляющей генерирование управляющих команд для управляемых элементов.

[0003] Для IoT также существуют внедрения в области блокчейн протоколов для организации обмена данными и доверительного взаимодействия между участниками обмена в едином распределенном реестре. Например, такое решение известно из заявки US 20180183587 (VMware Inc., 28.06.2018). Сложность применения данного подхода для широкого спектра устройств является недостаточная защищенность при обмене данными IoT устройств, при применении конвенционных подходов реализации блокчейн-инфраструктуры на базе программной логики.

[0004] Для частичного нивелирования существующих проблем предлагается использовать защищенные аппаратные носители обмена данными, например, eSIM или UICC карты (чипы, смарт-карты), которые будут выполнять необходимые операции проверки/подтверждения пакетов данных, которыми IoT устройства обмениваются в процессе своей деятельности. Например, упоминание возможности таких решений изложено в заявках WO 2018066362 (NEC CORP, 12.04.2018), WO 2017082966 (Intel IP Corp., 18.05.2017).

[0005] Тем не менее существующие на текущий момент предложения по обеспечению обмена взаимодействия между IoT устройствами не предлагают прозрачного, с точки зрения защищенности, информационного обмена данными технического решения, которое бы также обеспечивало децентрализованное и универсальное управление устройствами в единой среде взаимодействия с должным обеспечением защиты и доверенным обменом данными внутри такой информационной среды.

Раскрытие изобретения

[0006] Существующей технической проблемой, на решение которой направлено заявленное техническое решение, является создание нового, безопасного и универсального способа и системы для управления множеством IoT устройств.

[0007] Техническим результатом является повышение защиты информационного обмена данными между устройствами, за счет организации доверенной среды взаимодействия и снабжения каждого участника информационного обмена в доверенной среде защищенным модулем безопасности, в среде которого выполняются все необходимые операции для осуществления обмена данными с помощью набора симметричных ключей доступа.

[0008] В предпочтительном варианте осуществления заявленного решения представлен способ обеспечения взаимодействия IoT устройств, включающий обмен информацией между множеством устройств IoT и облачной платформой, содержащий этапы, на которых

устанавливают на каждое из IoT устройств и облачную платформу по меньшей мере один модуль безопасности, обеспечивающий доверенное исполнение программ, безопасное хранение данных, а также выполнение криптографических операций для обмена данными между устройствами и/или облачной платформой;

регистрируют на облачной платформе список доверенных IoT устройств и

соответствующих им идентификаторов (ID) для осуществления информационного обмена, причем в ходе упомянутой регистрации записывают на упомянутый модуль безопасности доверенных IoT устройств набор ключей шифрования для выполнения упомянутых криптографических операций, причем указанные ключи являются

5 симметричными и одноразовыми, и копия набора ключей каждого доверенного IoT устройства хранится в модуле безопасности облачной платформы и/или доверенных IoT устройствах, участвующих в обмене данными;

при обмене данными между доверенными IoT устройствами или по меньшей мере одним IoT устройством и облачной платформой осуществляют формирование

10 информационного пакета, содержащего данные и ID IoT устройства, обрабатываемые в модуле безопасности IoT устройства с помощью ключа шифрования, передачу упомянутого пакета на принимающее пакет IoT устройство или облачную платформу, обработку упомянутого пакета с помощью упомянутой копии ключа шифрования, причем упомянутая процедура осуществляется в среде модуля безопасности облачной

15 платформы или принимающего пакет данных IoT устройства;

принимают обработанные данные из упомянутого информационного пакета на модуле безопасности принимающего IoT устройства или модуле безопасности облачной платформы;

выполняют с помощью модулей безопасности доверенных IoT устройств или по

20 меньшей мере одного модуля безопасности IoT устройства и модуля безопасности облачной платформы отметку использованных ключей шифрования, и назначают новый ключ шифрования из упомянутого набора ключей IoT устройства для подтверждения следующего информационного пакета.

[0009] В одном из частных вариантов реализации способа IoT устройства включают

25 в себя управляемые и/или управляющие устройства.

[0010] В другом частном варианте реализации способа модуль безопасности представляет собой: аппаратный, программно-аппаратный, или программный модуль, или их сочетания.

[0011] В другом частном варианте реализации способа ключи шифрования

30 формируются в модуле безопасности IoT устройства из числовой последовательности.

[0012] В другом частном варианте реализации способа каждый новый ключ набора генерируется как следующий набор чисел из числовой последовательности.

[0013] В другом частном варианте реализации способа аппаратный модуль безопасности представляет собой UICC, eUICC, iUICC или их сочетания.

[0014] В другом частном варианте реализации способа ID IoT устройств представляет собой IMEI номер, MAC-адрес, IP-адрес, Bluetooth адрес или их сочетания.

[0015] В другом частном варианте реализации способа процедура подключения и обмена данными IoT устройств между собой и облачной платформой выполняется с помощью блокчейн протокола.

[0016] В другом частном варианте реализации способа протокол представляет собой Hyperledger Fabric.

[0017] В другом частном варианте реализации способа обмен данными между IoT устройствами или IoT устройствами и облачной платформой осуществляется с помощью смарт-контрактов.

[0018] В другом частном варианте реализации способа смарт-контракты выполняются на модулях безопасности IoT доверенных устройств и облачной платформы, выполняющих обработку информационного пакета.

[0019] В другом частном варианте реализации способа при формировании

информационного пакета дополнительно записывается метка времени его создания.

[0020] В другом частном варианте реализации способа обработка информационного пакета включает в себя операции шифрования/дешифрования.

5 [0021] В другом частном варианте реализации способа обработка информационного пакета включает в себя проверку контроля целостности пакета.

[0022] В другом частном варианте реализации способа обработка информационного пакета включает в себя формирование цифровой подписи, удостоверяющей источник передачи и неизменность пакета.

10 [0023] В другом частном варианте реализации способа модуль безопасности выполнен с возможностью дополнения и/или обновления набора ключей шифрования.

[0024] В другом предпочтительном варианте осуществления заявленного решения представлена система обеспечения взаимодействия устройств интернета вещей (IoT), включающая множеством устройств IoT и облачную платформу, в которой

15 каждое из IoT устройств и облачная платформа содержат по меньшей мере один модуль безопасности, обеспечивающий доверенное исполнение программ, безопасное хранение данных, а также выполнение криптографических операций для обмена данными между устройствами и/или облачной платформой;

облачная платформа выполнена с возможностью регистрировать список доверенных IoT устройств и соответствующих им идентификаторов (ID) для осуществления
20 информационного обмена, причем в ходе упомянутой регистрации записывают на упомянутый модуль безопасности доверенных IoT устройств набор ключей шифрования для выполнения упомянутых криптографических операций, причем указанные ключи являются симметричными и одноразовыми, и копия набора ключей каждого доверенного IoT устройства хранится в модуле безопасности облачной платформы и/или доверенных
25 IoT устройствах, участвующих в обмене данными;

причем модули безопасности устройства инициатора обмена данными и принимающей стороны обеспечивают

обмен данными между доверенными IoT устройствами или по меньшей мере одним IoT устройством и облачной платформой;

30 выполнение формирования информационного пакета, содержащего данные и ID IoT устройства инициатора;

обработку упомянутого информационного пакета с помощью ключа шифрования;

передачу упомянутого пакета на принимающее пакет IoT устройство или облачную платформу;

35 обработку упомянутого пакета с помощью упомянутой копии ключа шифрования, причем упомянутая процедура осуществляется в среде модуля безопасности облачной платформы или принимающего пакет данных IoT устройства;

получение обработанных данных из упомянутого информационного пакета на модуле безопасности принимающего IoT устройства или модуле безопасности облачной
40 платформы; и

осуществлении отметки использованных ключей шифрования с назначением нового ключа шифрования из упомянутого набора ключей IoT устройства для подтверждения следующего информационного пакета.

45 [0025] В одном из частных вариантов реализации системы обмен данными между IoT устройствами и облачной платформой выполняется по протоколу беспроводной и/или проводной передачи данных.

[0026] В другом частном варианте реализации системы протокол выбирается из группы: WLAN, WAN, Wi-Fi, GSM, GPRS, LTE, 5G, ZigBee, LPWAN, LoRaWan, Bluetooth,

BLE, TCP/IP, ModBus, NB-IoT, Z-Wave, Sigfox, Ethernet.

[0027] В другом частном варианте реализации модуль безопасности выполнен с возможностью обновления и/или дополнения набора ключей шифрования.

[0028] В другом частном варианте реализации обмен данными между IoT устройствами и облачной платформой осуществляется с помощью протокола блокчейн.

[0029] В другом частном варианте реализации обмен данным между IoT устройствами или IoT устройствами и облачной платформой осуществляется с помощью смарт-контрактов.

[0030] При этом ключи шифрования являются неизвлекаемыми из модуля безопасности.

Описание чертежей

[0031] Фиг. 1 иллюстрирует общий вид IoT устройства.

[0032] Фиг. 2 иллюстрирует основные компоненты модуля безопасности.

[0033] Фиг. 3 иллюстрирует общий вид системы взаимодействия IoT устройств.

[0034] Фиг. 4 иллюстрирует пример взаимодействия устройств с использованием ключей шифрования.

[0035] Фиг. 5 иллюстрирует пример генерирования ключей шифрования.

[0036] Фиг. 6 – Фиг. 7 иллюстрируют пример работы заявленного решения с помощью смарт-контрактов.

[0037] Фиг. 8 иллюстрирует осуществление решение на примере каршеринга.

Осуществление изобретения

[0038] На Фиг. 1 представлен общий вид примера IoT устройства (100), применяемого в рамках реализации заявленного решения. Настоящее техническое решение осуществляется за счет снабжения участвующих в информационном обмене устройств Интернета вещей или IoT устройств (100) специализированным модулем безопасности (105), который обеспечивает защищенное исполнение необходимых процедур по обмену данными между участниками IoT инфраструктуры.

[0039] В общем виде устройство (100) содержит вычислительный модуль (101), одно или более средств памяти (102) или устройств оперативного или постоянного хранения данных, средства ввода/вывода информации (103), интерфейсы ввода/вывода информации (104), модуль безопасности (105) и средство сетевого взаимодействия (106). Элементы устройства (100) могут, в частности, связываться между собой посредством шины данных (110), либо же соединяться с помощью иных известных принципов, исходя из конкретной реализации и аппаратного воплощения устройства (100). При этом специалистам должно быть очевидно, что набор элементов устройства (100) может быть различным при его частных случаях реализации.

[0040] Вычислительный модуль (101) может представлять собой один или более процессоров, микроконтроллер, ПЛИС с интегрированным вычислительным средством, микросхему или иное средство, обеспечивающее обработку данных для осуществления операций и/или команд, выполняемых устройством (100).

[0041] Память (102) представляет собой одно или более средств накопления данных, например, оперативную память (RAM) и/или постоянную память (ROM). Постоянная память выбирается из такого спектра устройств, как: жесткий диск (HDD), твердотельный накопитель (SSD), флэш-память (EEPROM, NAND, SD/TF/Memory Stick -Card и т.п.), оптические накопители (CD/DVD/MD/Blue-Ray диски) и т.п. Память (102) выполняет оперативное и/или постоянное запоминание необходимых инструкций и данных для осуществления функционирования устройства (100).

[0042] Средства В/В (103) выбираются из ряда средств, которые присуще конкретному

воплощению устройства (100), например, в качестве таких средств могут выступать: дисплей (в том числе сенсорный дисплей), клавиатура, манипулятор типа мышь, трекбол, тач-пад, световое перо, сенсорный планшет, проектор, динамики, световой индикатор и т.п.

5 [0043] Также в качестве средств В/В (103) могут выступать АЦП/ЦАП для частных примеров воплощения IoT устройств (100).

[0044] Интерфейсы В/В (104) могут выбираться из следующей реализации, в зависимости от типа IoT устройства (100), например, PCI, VGA, AGP, DVI, SATA, USB (Type-C, micro-, Mini-), PS/2, RJ45, LPT, FireWire, RS232, Lightning, COM, HDMI, Display
10 Port, Audio Jack, GPIO, ЦАП/АЦП и т.п.

[0045] Модуль безопасности (105) представляет собой элемент устройства (100), обеспечивающий безопасное хранение ключей шифрования, различных данных, например, необходимых для операций информационного обмена, прошивки чипа и т.п., выполнение криптоопераций и обработки и формирования информационных
15 пакетов для взаимодействия IoT устройств (100). Детальное описание работы модуля (105) будет представлено далее.

[0046] Средство сетевого взаимодействия (106) представляет собой одно или несколько устройств, предназначенных для обеспечения приема и передачи данных посредством вычислительной сети, например, обеспечивающее передачу информации с помощью
20 протоколов WLAN, WAN, Wi-Fi, GSM, GPRS, LTE, 5G, ZigBee, LPWAN, LoRaWan, Bluetooth, BLE, TCP/IP, ModBus, NB-IoT, Z-Wave, Sigfox, Ethernet и т.п. Передача информации с помощью устройства (106) может выполняться как по проводному, так и беспроводному информационному каналу, или в комбинации известных способов обмена данными.

25 [0047] IoT устройства (100) могут выбираться из широкого спектра известных решений, участвующих в процессе информационного обмена, например, такими устройствами могут быть: датчики, актуаторы, сенсоры, смартфон, планшет, телевизор, игровая приставка, компьютер, ноутбук, терминал, мейнфрейм, различные типы измерительных устройств (термометры, монометры, счетчики и т.д.) и т.п. Очевидно,
30 что представленный спектр устройств является только примером использования в настоящем техническом решении и не ограничивается другими устройствами, которые могут быть снабженными необходимой программно-аппаратной логикой для взаимодействия в IoT среде.

[0048] Как было указано выше, в частном случае выполнения IoT устройства (100),
35 принцип его архитектуры может исключать шину данных (110). В таком примере выполнения устройства (100) логика его работы может быть реализована, например, с помощью единого чипа, который содержит необходимый набор функций.

[0049] На Фиг. 2 представлена общая концепция реализации модуля безопасности (105). Модуль безопасности (105) может выполняться в виде программного, программно-аппаратного или аппаратного решения, которое установлено на IoT устройстве (100).
40 Модуль (105) обеспечивает хранение ключей шифрования, необходимых для формирования информационных пакетов для обмена данными в среде взаимодействия IoT устройств, обеспечение доверенной защищенной среды обработки данных и выполнение необходимых криптоопераций для обмена данными между устройствами
45 (100).

[0050] Модуль безопасности (105) содержит два типа хранилища, одно для ключей шифрования, второе – для различного рода информации, например, данных, необходимых для операций информационного обмена, прошивка чипа, параметры

смарт-контрактов и т.п.

[0051] Модуль безопасности (105) может представлять собой программную логику, хранящуюся в памяти (102) устройства (100) и взаимодействующую с вычислительным модулем (101) для реализации предписанных функций.

5 [0052] В случае программно-аппаратной или аппаратной реализации модуль (105) может выполняться в виде таких решений, как UICC, eUICC, iUICC, eSIM и т.п. Примеры аналогичных решений широко известны в уровне техники, например, в документе WO 2018007461 (GEMALTO SA, 11.01.2018).

10 [0053] Модуль безопасности (105) также предназначен для хранения набора ключей шифрования для осуществления доверенного и безопасного обмена данными между IoT устройствами (100). Под модулем безопасности (105) в настоящих материалах заявки стоит также понимать элемент безопасности (например, <https://www.justaskgemalto.com/en/what-is-a-secure-element/>).

15 [0054] На Фиг. 3 представлен пример общей концепции системы взаимодействия IoT устройств (100). Устройства (100₁)-(100_n) взаимодействуют друг с другом и IoT инфраструктурой посредством облачной платформы (200) с помощью различных каналов передачи данных (150).

20 [0055] Устройства (100₁)-(100_n) при начале взаимодействия в IoT инфраструктуре осуществляют первичную регистрацию в облачной платформе (200). Регистрация выполняется с помощью, например, программного приложения, установленного на устройстве (100), с помощью заранее установленной логики в модуле безопасности (105) взаимодействия с облачной платформой (200).

25 [0056] Регистрация заключается в передаче на облачную платформу (200) идентифицирующей IoT устройство (100) информации, например, ID устройства, который может представлять собой, но не ограничиваться: UID, IMEI, SSID, MAC-адрес, Bluetooth ID, IP-адрес, PIN/PUK-код, серийный номер чипа или иного элемента устройства (100), их комбинации и т.п. На основании полученной информации устройство (100) заносится в перечень доверенных устройств. Для каждого из доверенных IoT устройств (100) с помощью облачной платформы (200) генерируется набор ключей шифрования, которые записываются в модуль безопасности (105) IoT устройства (100).

30 [0057] Облачная платформа (200) представляет собой сервер (облачный сервер) или несколько серверов (например, кластер), который также содержит модуль безопасности (205). Модуль безопасности облачной платформы (205) по своему функционалу не уступает архитектуре модуля безопасности IoT устройств (105). При каждой регистрации IoT устройства (100), в модуль безопасности (105) устройства (100) записывается набор ключей шифрования, и соответствующая копия такого набора также записывается в модуль безопасности (205) облачной платформы (200) с привязкой упомянутого набора соответствующему идентификатору регистрируемого устройства (100). Ключи шифрования являются симметричными и неизвлекаемыми из модулей безопасности (105) и (205).

40 [0058] Набор ключей может также быть заранее сформирован для устройств (100) и содержаться в модуле безопасности (105). Такой вариант применяется, если устройства (100) на заводском уровне предназначены для работы только в доверенной среде, обеспечиваемой взаимодействием с облачной платформой (200). В этом случае платформа (200) содержит соответствующие копии наборов ключей в памяти модуля безопасности (205), которые привязаны в памяти облачной платформы (200) к соответствующим идентификаторам устройств (100).

[0059] Представленный принцип взаимодействия может также содержать

дополнительную сетевую сущность в виде доверенного органа (300). Такой орган (300) может представлять собой сотового оператора, сертифицирующий орган, платформу обеспечения доступа к группе устройств, провайдера и т.п. Основная функция такого органа (300) заключается в обеспечении информационного обмена между IoT

5 устройствами (100), которые входят в контур функционирования данного органа (300), с обеспечением взаимодействия с внешними источниками посредством доверенной среды облачной платформы (200). Как пример, в части работы такого органа (300) можно рассмотреть работу сотового оператора, который содержит контур или среду работы ряда IoT устройств (100), к которым необходимо предоставить доступ внешним

10 пользователям, например, новым абонентам сети такого оператора (300).

[0060] На Фиг. 4 представлен пример взаимодействия IoT устройств (100₁)-(100₂) посредством облачной платформы (200). Как было указано выше, в каждом из модулей (105) IoT устройств содержится соответствующий набор ключей шифрования (110)-(120) для обеспечения операций по информационному обмену. Копия каждого набора

15 ключей (210) дублируется на облачной платформе (200) в модуле безопасности (205).

[0061] При обмене данными между одним из IoT устройств (110₁)-(110₂) с облачной платформой (200) или при взаимодействии устройств друг с другом (110₁)-(110₂),

20 выполняется формирование информационного пакета, который содержит как минимум идентификатор (ID) IoT устройства и данные для выполнения того или иного типа взаимодействия (команда, код, алгоритм и т.п.). Например, под типом взаимодействия может пониматься: осуществление предписанных устройством операций (открытие замка, передача данных, расчет температуры, активация устройства и т.п.), обеспечение

25 [0062] При формировании информационного пакета осуществляется использование ключей шифрования. Как показано на Фиг. 4, при формировании информационного пакета устройства (110₁)-(110₂) (или одно из устройств) использует один из набора ключ шифрования (110)-(120). Информационный пакет может шифроваться с помощью криптографических процедур в модуле безопасности (105) IoT устройства (100),

30 формирующего пакет, для последующей его передачи на одно или более получающих IoT устройств.

[0063] Информационный пакет может также проверяться получающим модулем безопасности (105) (или (205)) на предмет его целостности. Для этой процедуры может также применяться ЭЦП для устройств, осуществляющих обмен информационным

35 пакетом. В качестве известных примеров контроля целостности информационных пакетов могут также выступать известные алгоритмы, например, симметричные схемы аутентификации сообщений, основанные на блочных шифрах, алгоритмы проверки кодов аутентификации (HMAC) и др.

[0064] На принимающем устройстве (100) и/или облачной платформе (200) при

40 получении информационного пакета от устройства отправителя, упомянутый пакет обрабатывается с помощью модуля безопасности (105) (и/или (205)). При обработке информационного пакета осуществляется его дешифрование с помощью соответствующего ключа шифрования принимающего устройства (100) или устройств (100_n), в случае если информационный пакет на устройстве отправителе был зашифрован.

45 И в случае успешной обработки информационного пакета на принимающей стороне осуществляется предписанная логика информационного взаимодействия.

[0065] При использовании ключа шифрования из одного или двух наборов (110)-(120), как это представлено на Фиг. 4, с учетом их симметричности и одноразовости,

производится отметка в модуле безопасности (105) каждого из устройств, участвующих в информационном обмене, и модуле безопасности (205) облачной платформы (200) об использовании соответствующего ключа. Далее выполняется назначение следующего ключа из набора (110)-(120) взаимодействующих устройств и назначение

5 соответствующей ему копии из набора (210) модуля безопасности облачной платформы (200). Специалистам в данной области техники должно быть очевидно, что порядок использования ключей может быть различным и диктоваться логикой шифрования, заложенной в модулях безопасности (105) IoT устройств (100), приведенный пример лишь отражает частный случай использования очередности ключей шифрования.

10 [0066] В частном варианте реализации, облачная платформа может не участвовать в обмене данными между устройствами (110₁)-(110₂). В этом случае использование ключей шифрование в модулях безопасности (105) и их последующее назначение осуществляется после выполнения обмена информационными пакетами указанных устройств.

15 [0067] Данный подход применения симметричных ключей шифрования, по сравнению с широко известным ассиметричным подходом, имеет ряд преимуществ. В частности, ассиметричное шифрование является достаточно ресурсоемким, особенно в масштабах IoT инфраструктуры, в которую может входить от десятков до тысяч устройств, что обуславливается значительным увеличением размера пакета данных для обмена между

20 участниками сети. Данная проблема также очень весома при осуществлении архитектуры решения в блокчейн среде, что влияет на динамическое увеличение сложности вычислений при подтверждении транзакций. Также, ассиметричное шифрование имеет неустойчивость к квантовым компьютерам, например, для RSA – алгоритм Шора.

25 [0068] Набор ключей шифрования в модуле безопасности (105) IoT устройств (100) и модуле безопасности облачной платформы (205), может динамически обновляться в случае его исчерпания или необходимости обновления набора ключей. Данный процесс может быть частью программной логики, хранящейся на облачной платформе (200), или при участии дополнительного доверенного органа (300). При осуществлении

30 взаимодействия через доверенный орган (300), последний может содержать установленную логику в части обновления или дополнения набора ключей шифрования на IoT устройствах (100), например, при подключении новых абонентов в доверенный контур информационного обмена. В таком примере, доверенный орган (300) может выступать мобильным оператором или поставщиком иного типа услуг, с возможностью предоставления набора ключей шифрования для организации взаимодействия IoT

35 устройств (100).

[0069] На Фиг. 5 представлен пример генерирования ключей шифрования. Набор ключей может формироваться из числовой или буквенно-числовой последовательности. Принцип генерирования ключей шифрования может быть различным. Как пример, но

40 не ограничение, одним из принципов формирования ключей может являться способ выбора следующего набора символов, следующих после использованной последовательности. То есть, после применения набора для формирования Ключа 1, следующие части общей последовательности будут применяться для формирования следующих ключей. Количество символов для формирования ключа может быть различным и устанавливаться логикой алгоритма формирования ключей.

45 [0070] Заявленное техническое решение может также быть реализовано с помощью технологии блокчейн. Формируемые информационные пакеты в этом случае записываются в общий распределенный реестр, который может храниться как на IoT устройствах (100), так и на одной или более облачной платформе (200). Шифруемые

информационные пакеты представляют собой доверенные блоки для выполнения транзакционных операций.

[0071] Модуль безопасности IoT устройств (105) может также содержать логику для реализации цифрового кошелька (или криптокошелька) для обеспечения блокчейн транзакций. Под транзакциями может пониматься любое взаимодействие в рамках доверенной среды IoT устройств (100), в частности, доступ к устройству, обмен данными, отправка данных от устройства, предоставление услуги и т.п.

[0072] На Фиг. 6 – Фиг. 7 представлен процесс информационного взаимодействия IoT устройств (100) с помощью реализации на базе смарт-контрактов (СК) (400). Для данного взаимодействия целесообразно использовать блокчейн протокол, который не будет нести значимой вычислительной нагрузки на сеть, например, примером такого протокола является Hyperledger Fabric, разработанный компанией IBM™. Выполнение СК осуществляется с помощью формируемых информационных пакетов в модулях безопасности (105₁)-(105₂) IoT устройств (100₁)-(100₂), взаимодействующих в рамках блокчейн платформы (500).

[0073] Как правило, под СК (400) понимается распределенное приложение, исполняемое на блокчейн-платформе (500). СК (400) предназначен для выполнения каких-либо заранее предопределенных действий (или единого действия) при наступлении определенных условий для его реализации, например, выполнение IoT (100) устройством предопределённой условием СК (400) одной или нескольких функций. Таким образом, безопасность СК (400) (в смысле надежности и однозначности исполнения алгоритма) во многом зависит от точности данных, поступающих в СК (400), а также от точности команд, доставляемых от СК (400) на устройства.

[0074] СК (400) подходит для интеграции устройств IoT (100₁)-(100₂) друг с другом. Например, простейший сценарий, представленный на Фиг. 7, при нажатии виртуальной кнопки (120) на экране смартфона (100₁) пользователя должна загореться лампа (100₂). При повторном нажатии – потухнуть. Условие: нажатие кнопки (120), действие (команда) - изменить состояние лампы. В терминах безопасности необходимо, чтобы лампа (100₂) реагировала только на нажатие кнопки (120) на доверенном управляющем устройстве (смартфоне) (100₁) и никак другом. При нажатии кнопки (120) на экране смартфона (100₁) формируется информационный пакет, подписывается в модуле безопасности (105₁) смартфона (100₁) с использованием ключей шифрования и отправляется на облачную платформу (200). В данном примере шифрование не применяется, так как конфиденциальность не важна в данном случае. С помощью платформы (200) выполняется подтверждение условий исполнения СК (400) для передачи пакета на управляемое IoT устройство – лампочку (100₂).

[0075] На платформе (200) информационный пакет от смартфона (100₁) поступает в СК (400), и далее необходимо удостовериться, какое устройство является отправителем пакета и что пакет не изменился во время доставки, т.е., что пакет был сформирован доверенным устройством и направлен так же на доверенное устройство. Тут возможны два варианта архитектуры: 1) каждый СК (400) имеет свой модуль безопасности, который связан с модулями безопасности устройств (105₁)-(105₂), задействованных в СК (400); 2) платформа (200) имеет модуль безопасности (205), единый для всех СК на данной платформе (единый логически, он может представлять собой множество пространственно распределенных сущностей).

[0076] СК (400) обращается к модулю безопасности (на устройстве, участвующем в

процессе информационного обмена или на облачной платформе (200)). В случае положительного ответа СК (400) принимает этот пакет для исполнения алгоритма, заложенного в СК (400), в противном случае пакет отбрасывается либо подается на вход подсистемы безопасности для проведения расследования. В качестве примера

рассмотрим случай, когда проверка целостности пакета была успешной. [0077] В этом случае СК (400) формирует информационный пакет на изменение состояния лампы (100₂), который поступает в модуль безопасности СК (400) или платформы (205) для подписи, и подписанный информационный пакет отправляется на лампу (100₂). Поступив на лампу (100₂) через сетевой модуль (например, Bluetooth или Wi-Fi) пакет поступает в модуль безопасности (105₂), где проходит проверку подписи. В случае положительной проверки модуль безопасности (105₂) формирует команду чипу лампы (100₂) на изменение состояния, т.е. на исполнение команды, полученной от устройства (100₁).

[0078] Изменив состояние лампы (100₂), чип лампы (100₂) формирует пакет-отчет с актуальным состоянием лампы (100₂) (например, включено/ выключено/ нужен сервис и т.п.). Пакет-отчет проходит обратный путь через СК (400), модуль безопасности платформы (205) и поступает на вход модуля безопасности смартфона (100₁) или иного управляющего устройства.

[0079] Как пример реализации, рассмотрим вариант с шифрованием данных. В случае, когда информационный пакет содержит конфиденциальную информацию, применяется его шифрование. Пакет шифруется, подписывается и отправляется на платформу (200), где поступает в СК (400).

[0080] СК (400) отправляется пакет в модуль безопасности платформы (205), где он расшифровывается и проверяется его подпись (т.е. подпись доверенного устройства, которое инициировало его передачу), после чего СК (400) формирует информационный пакет, шифрует и подписывает его и отправляет на смартфон пользователя (100₁). На смартфоне (100₁) пакет расшифровывается и проверяется подпись, содержащаяся в нем, после чего актуальное состояние лампы (100₂) отражается на смартфоне (100₁) (например, кнопка меняет цвет).

[0081] Возможен и иной вариант: устройства (100₁)-(100₂) отправляют информационные пакеты друг другу непосредственно, а на платформу (200) отправляются копии информационных пакетов, где они обрабатываются СК (400), пишется журнал событий и фиксируются случаи нештатной работы системы.

[0082] Взаимодействие СК (400) в системе может осуществляться посредством блокчейн платформы (500) (блокчейн протокола).

[0083] На Фиг. 8 представлен пример осуществления решения на примере каршеринга. Доступ к услуге аренде автомобиля (620) осуществляется с помощью обмена данными с доверенным устройством пользователя (610). Автомобиль (620) содержит ряд IoT устройств, например, контроллер двигателя (621), контроллер центрального замка (622), контроллер управления электроникой (623) и единый вычислительный модуль (625). Модуль (625) может выступать в роде общего узла, обеспечивающего информационный обмен с устройствами автомобиля (620).

[0084] Модуль (625) может содержать модуль безопасности, который обеспечивает обмен информационными пакетами со смартфоном пользователя (610), который связан с автомобилем (610) с помощью облачной платформы (200). При регистрации устройства

пользователя (610) с помощью платформы (200) или дополнительно через доверенный орган (300), в системе предоставления услуг каршеринга, в модуль безопасности устройства (610) записывается соответствующий набор ключей шифрования для применения соответствующей услуги по аренде автомобиля (620).

5 [0085] При формировании информационного пакета с помощью устройства (610), как было описано выше, выполняются передача идентификационной информации устройства (610), преобразованной на ключе шифрования, которая впоследствии проверяется на ее валидность модулем безопасности модуля (625).

10 [0086] По аналогии с примером на Фиг. 7 для данного примера также может применяться СК (400), который будет содержать соответствующую программную логику. Организация каршеринга может осуществляться с помощью блокчейн платформы (500), которая будет осуществлять техническое взаимодействие пользователя с арендуемым автомобилем (620) посредством СК (400). СК (400) в этом случае является программным воплощением юридического договора между пользователем и владельцем 15 (арендодателем) автомобиля. В целях безопасности СК (400) делает проверку информационных пакетов на модуле безопасности по аналогии в предыдущим примером.

[0087] В этом случае, устройство пользователя (610) может в модуле безопасности содержать криптокошелок, который будет использоваться для формирования пакетов, 20 необходимых для аренды автомобиля (620).

[0088] Представленное описание заявленного решения раскрывает лишь предпочтительные примеры его реализации и не должно трактоваться как ограничивающее иные, частные примеры его осуществления, не выходящие за рамки объема правовой охраны, которые являются очевидными для специалиста 25 соответствующей области техники.

(57) Формула изобретения

1. Способ обеспечения взаимодействия устройств интернета вещей (IoT), включающий обмен информацией между множеством устройств IoT и облачной платформой, 30 содержащий этапы, на которых:

устанавливают на каждое из IoT устройств и облачную платформу по меньшей мере один модуль безопасности, обеспечивающий доверенное исполнение программ, безопасное хранение данных, а также выполнение криптографических операций для обмена данными между устройствами и/или облачной платформой;

35 регистрируют на облачной платформе список доверенных IoT устройств и соответствующих им идентификаторов (ID) для осуществления информационного обмена, причем в ходе упомянутой регистрации записывают на упомянутый модуль безопасности доверенных IoT устройств набор ключей шифрования для выполнения упомянутых криптографических операций, причем указанные ключи являются 40 симметричными и одноразовыми и копия набора ключей каждого доверенного IoT устройства хранится в модуле безопасности облачной платформы и/или доверенных IoT устройствах, участвующих в обмене данными;

при обмене данными между доверенными IoT устройствами или по меньшей мере одним IoT устройством и облачной платформой осуществляют формирование 45 информационного пакета, содержащего данные и ID IoT устройства, обрабатываемые в модуле безопасности IoT устройства с помощью ключа шифрования, передачу упомянутого пакета на принимающее пакет IoT устройство или облачную платформу, обработку упомянутого пакета с помощью упомянутой копии ключа шифрования,

причем упомянутая процедура осуществляется в среде модуля безопасности облачной платформы или принимающего пакет данных IoT устройства;

принимают обработанные данные из упомянутого информационного пакета на модуле безопасности принимающего IoT устройства или модуле безопасности облачной платформы;

выполняют с помощью модулей безопасности доверенных IoT устройств или по меньшей мере одного модуля безопасности IoT устройства и модуля безопасности облачной платформы отметку использованных ключей шифрования, и назначают новый ключ шифрования из упомянутого набора ключей IoT устройства для подтверждения следующего информационного пакета.

2. Способ по п.1, характеризующийся тем, что IoT устройства включают в себя управляемые и/или управляющие устройства.

3. Способ по п.1, характеризующийся тем, что модуль безопасности представляет собой: аппаратный, программно-аппаратный, или программный модуль, или их сочетания.

4. Способ по п.1, характеризующийся тем, что ключи шифрования формируются в модуле безопасности IoT устройства из числовой последовательности.

5. Способ по п.4, характеризующийся тем, что каждый новый ключ набора генерируется как следующий набор чисел из числовой последовательности.

6. Способ по п.3, характеризующийся тем, что аппаратный модуль безопасности представляет собой UICC, eUICC, iUICC или их сочетания.

7. Способ по п.1, характеризующийся тем, что ID IoT устройств представляет собой IMEI номер, MAC-адрес, IP-адрес, Bluetooth адрес или их сочетания.

8. Способ по п.1, характеризующийся тем, что процедура подключения и обмена данными IoT устройств между собой и облачной платформой выполняется с помощью блокчейн протокола.

9. Способ по п.8, характеризующийся тем, что протокол представляет собой Hyperledger Fabric.

10. Способ по п.8, характеризующийся тем, что обмен данными между IoT устройствами или IoT устройствами и облачной платформой осуществляется с помощью смарт-контрактов.

11. Способ по п.10, характеризующийся тем, что смарт-контракты выполняются на модулях безопасности IoT доверенных устройств и облачной платформы, выполняющих обработку информационного пакета.

12. Способ по п.1, характеризующийся тем, что при формировании информационного пакета дополнительно записывается метка времени его создания.

13. Способ по п.1, характеризующийся тем, что обработка информационного пакета включает в себя операции шифрования/дешифрования.

14. Способ по п.1, характеризующийся тем, что обработка информационного пакета включает в себя проверку контроля целостности пакета.

15. Способ по п.1, характеризующийся тем, что обработка информационного пакета включает в себя формирование цифровой подписи, удостоверяющей источник передачи и неизменность пакета.

16. Способ по п.1, характеризующийся тем, что модуль безопасности выполнен с возможностью дополнения и/или обновления набора ключей шифрования.

17. Способ по п.1, характеризующийся тем, что ключи шифрования являются неизвлекаемыми из модуля безопасности.

18. Система обеспечения взаимодействия устройств интернета вещей (IoT),

включающая множество устройств IoT и облачную платформу, в которой

каждое из IoT устройств и облачная платформа содержат по меньшей мере один модуль безопасности, обеспечивающий доверенное исполнение программ, безопасное хранение данных, а также выполнение криптографических операций для обмена данными между устройствами и/или облачной платформой;

облачная платформа выполнена с возможностью регистрировать список доверенных IoT устройств и соответствующих им идентификаторов (ID) для осуществления информационного обмена, причем в ходе упомянутой регистрации записывают на упомянутый модуль безопасности доверенных IoT устройств набор ключей шифрования для выполнения упомянутых криптографических операций, причем указанные ключи являются симметричными и одноразовыми и копия набора ключей каждого доверенного IoT устройства хранится в модуле безопасности облачной платформы и/или доверенных IoT устройствах, участвующих в обмене данными;

причем модули безопасности устройства инициатора обмена данными и принимающей стороны обеспечивают

обмен данными между доверенными IoT устройствами или по меньшей мере одним IoT устройством и облачной платформой;

выполнение формирования информационного пакета, содержащего данные и ID IoT устройства инициатора;

обработку упомянутого информационного пакета с помощью ключа шифрования; передачу упомянутого пакета на принимающее пакет IoT устройство или облачную платформу;

обработку упомянутого пакета с помощью упомянутой копии ключа шифрования, причем упомянутая процедура осуществляется в среде модуля безопасности облачной платформы или принимающего пакет данных IoT устройства;

получение обработанных данных из упомянутого информационного пакета на модуле безопасности принимающего IoT устройства или модуле безопасности облачной платформы; и

осуществлении отметки использованных ключей шифрования с назначением нового ключа шифрования из упомянутого набора ключей IoT устройства для подтверждения следующего информационного пакета.

19. Система по п.18, характеризующаяся тем, что обмен данными между IoT устройствами и облачной платформой выполняется по протоколу беспроводной и/или проводной передачи данных.

20. Система по п.19, характеризующаяся тем, что протокол выбирается из группы: WLAN, WAN, Wi-Fi, GSM, GPRS, LTE, 5G, ZigBee, LPWAN, LoRaWan, Bluetooth, BLE, TCP/IP, ModBus, NB-IoT, Z-Wave, Sigfox, Ethernet.

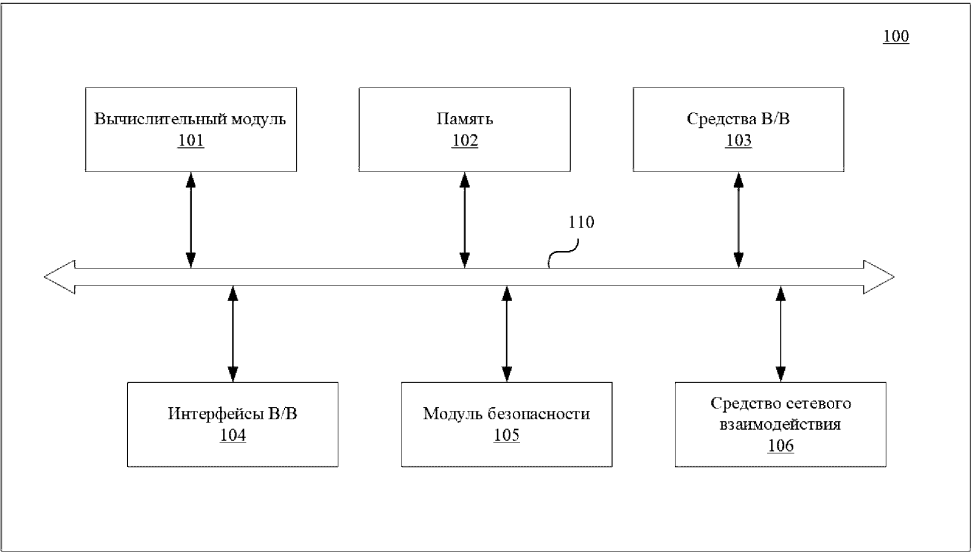
21. Система по п.18, характеризующаяся тем, что модуль безопасности выполнен с возможностью обновления и/или дополнения набора ключей шифрования.

22. Система по п.18, характеризующаяся тем, что обмен данными между IoT устройствами и облачной платформой осуществляется с помощью протокола блокчейн.

23. Система по п.22, характеризующаяся тем, что обмен данным между IoT устройствами или IoT устройствами и облачной платформой осуществляется с помощью смарт-контрактов.

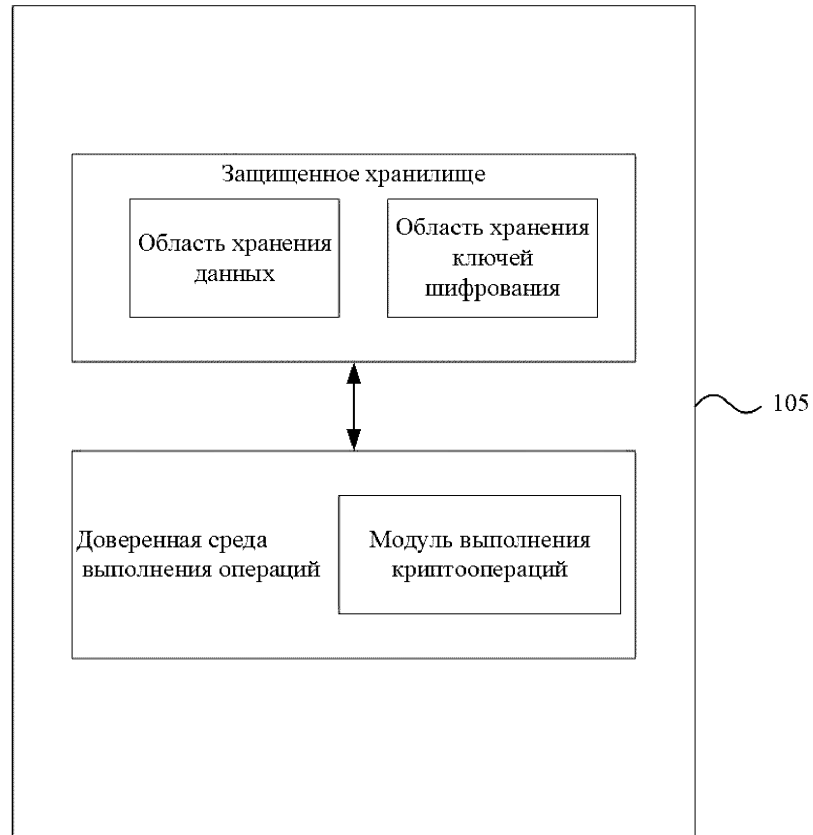
24. Система по п.18, характеризующаяся тем, что ключи шифрования являются неизвлекаемыми из модуля безопасности.

1

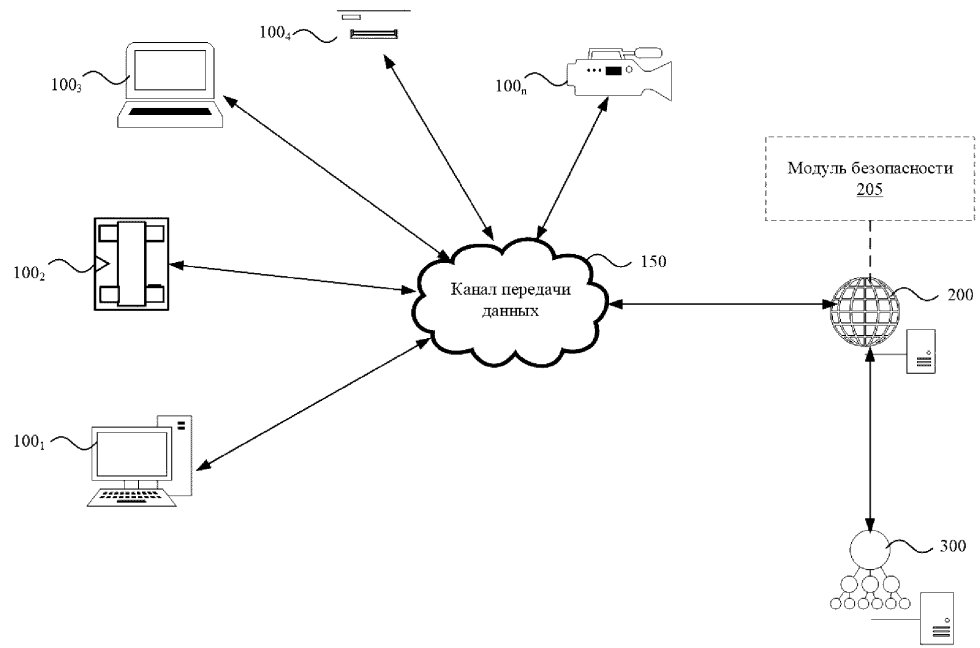


Фиг. 1

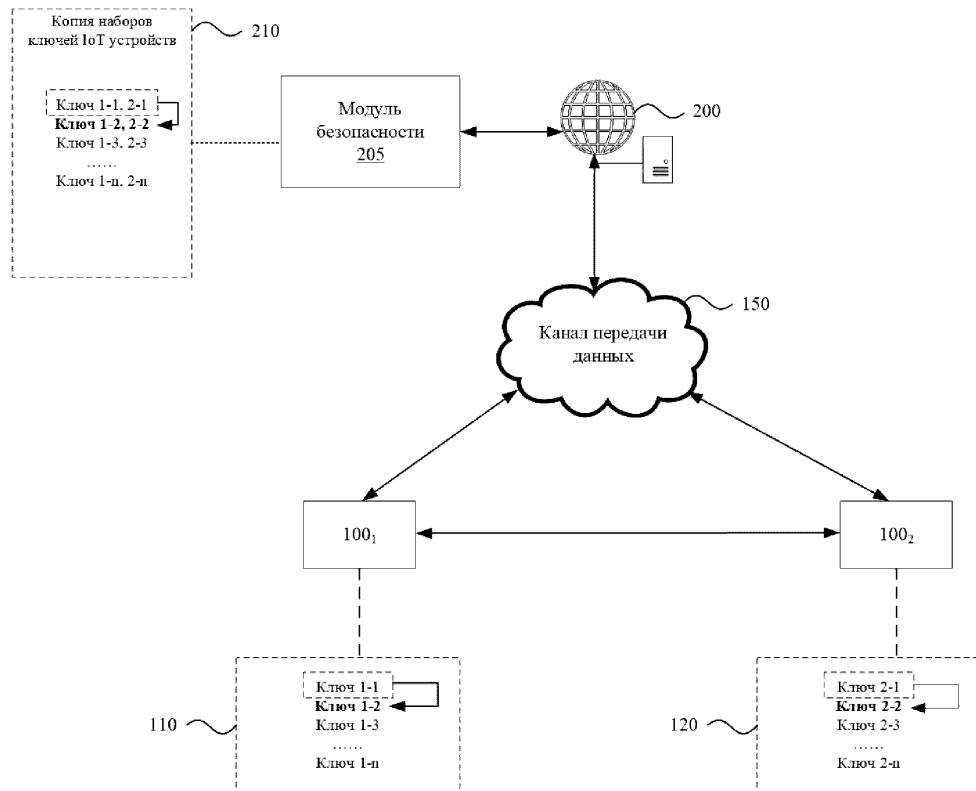
2



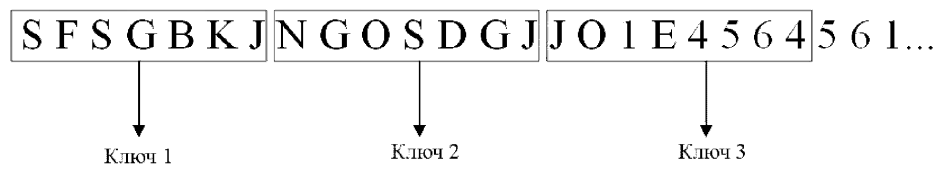
Фиг. 2



Фиг. 3



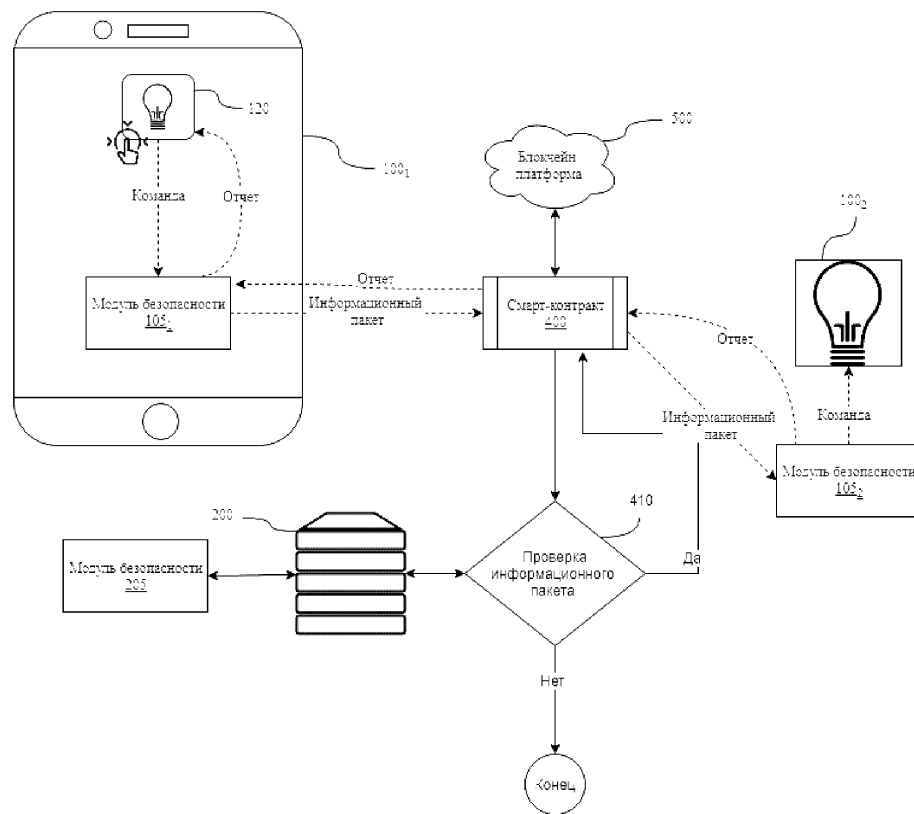
Фиг. 4



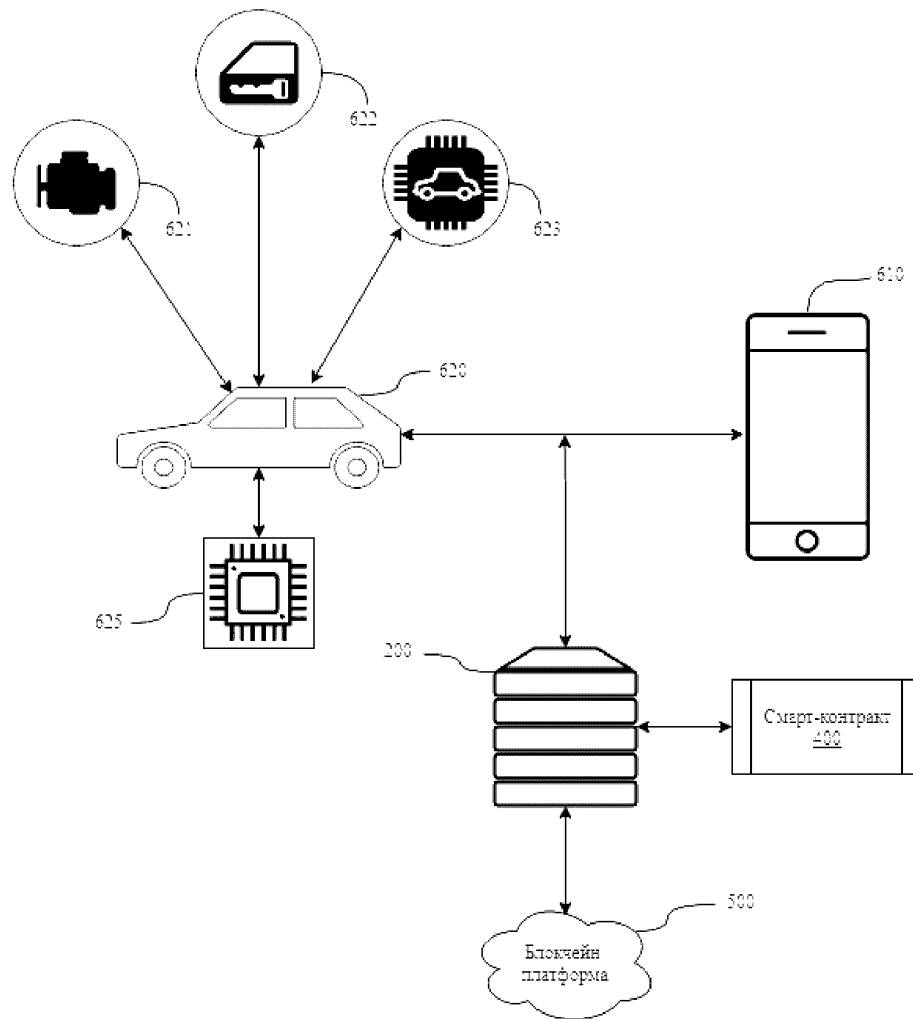
Фиг. 5



Фиг. 6



Фиг. 7



Фиг. 8