РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 634 202**(13) **C1**

(51) МПК
G06F 21/64 (2013.01)
H04B 1/38 (2015.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2016151599, 27.12.2016**

(24) Дата начала отсчета срока действия патента:
27.12.2016

Дата регистрации:
24.10.2017

Приоритет(ы):
(22) Дата подачи заявки: **27.12.2016**

(45) Опубликовано: **24.10.2017** Бюл. № **30**

Адрес для переписки:
129090, Москва, пр-кт Мира, 6, ППФ "ЮС", Ловцову С.В.

(72) Автор(ы):
Баранов Сергей Игоревич (RU),
Драгунов Виталий Анатольевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Научно-производственное объединение Ангстрем" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2512118 C2, 10.04.2014. RU 2268505 C2, 20.01.2006. RU 2599340 C2, 10.10.2016. RU 130429 U1, 20.07.2013. US 2016/0283745 A1, 29.09.2016.**

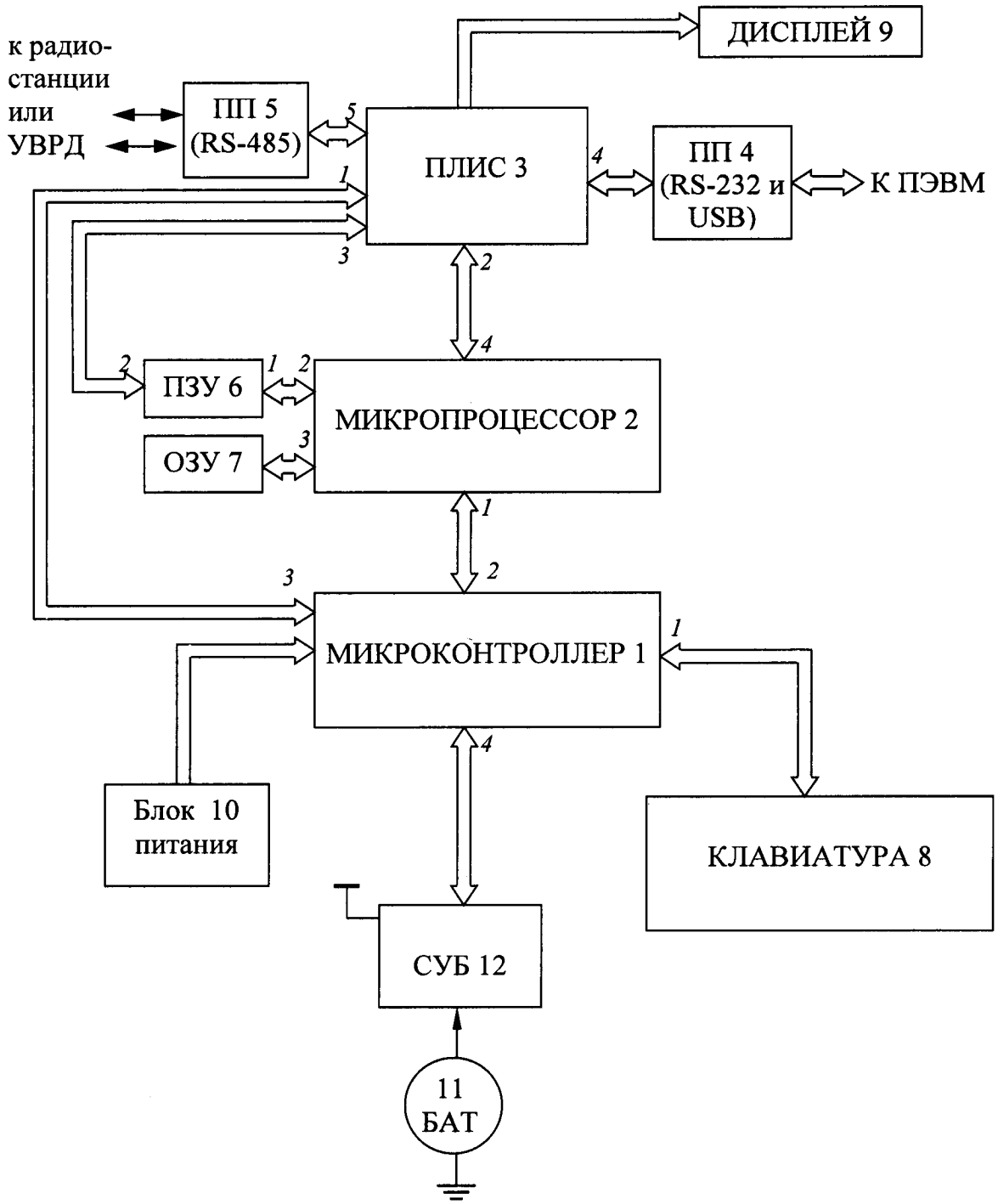
(54) УСТРОЙСТВО ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ФОРМИРОВАНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ И РАДИОДАННЫХ ДЛЯ РАДИОСТАНЦИИ

(57) Реферат:

Изобретение относится к радиотехнике и вычислительной технике. Технический результат заключается в повышение надежности защиты ключевой информации и радиоданных. Технический результат достигается за счет устройства программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции, содержащего микроконтроллер (МК), микропроцессор (МП), программируемую логическую интегральную схему (ПЛИС), по меньшей мере один первый приемопередатчик (ПП), по меньшей мере один второй приемопередатчик (ПП), постоянное запоминающее устройство (ПЗУ), оперативное запоминающее устройство (ОЗУ), клавиатуру, дисплей, блок питания. МК выполнен обеспечивающим контроль напряжений питания блока питания и управление питанием МК и ПЛИС, обеспечивающим ввод ключа расшифровки исходных данных формирования ключевой информации, ключа проверки целостности программного обеспечения ПЛИС и ключа проверки целостности программного обеспечения радиостанции посредством клавиатуры. ОЗУ выполнено обеспечивающим хранение упомянутых введенных ключей. МП выполнен обеспечивающим формирование ключевой информации и радиоданных по данным ПЗУ и ОЗУ. 1 з.п. ф-лы, 1 ил.

RU 2634202 C1

RU 2634202 C1



RU 2634202 C1

RU 2634202 C1

RUSSIAN FEDERATION

(19) **RU** (11) **2 634 202**(13) **C1**

(51) Int. Cl.
G06F 21/64 (2013.01)
H04B 1/38 (2015.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2016151599, 27.12.2016**

(24) Effective date for property rights:
27.12.2016

Registration date:
24.10.2017

Priority:
(22) Date of filing: **27.12.2016**

(45) Date of publication: **24.10.2017** Bull. № **30**

Mail address:
129090, Moskva, pr-kt Mira, 6, PPF "YUS", Lovtsovu S.V.

(72) Inventor(s):
Baranov Sergej Igorevich (RU),
Dragunov Vitalij Anatolevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Nauchno-proizvodstvennoe obedinenie Angstrem" (RU)

(54) DEVICE OF HARDWARE AND SOFTWARE COMPLEX FOR GENERATING KEY INFORMATION AND RADIO DATA FOR RADIO STATION

(57) Abstract:

FIELD: radio engineering, communication.

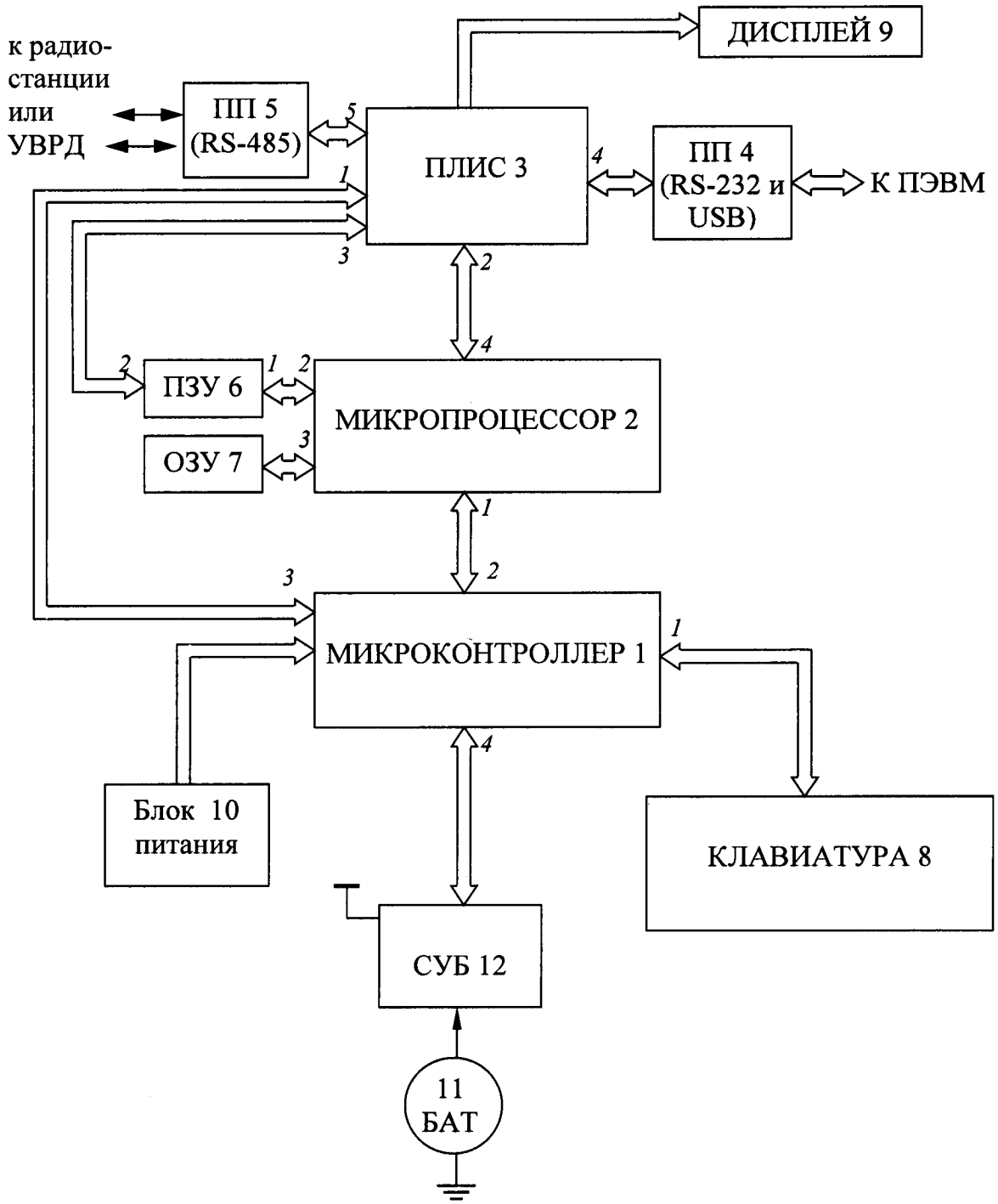
SUBSTANCE: hardware and software complex generation and radio data complex devices for the radio station comprises a microcontroller (MC), a microprocessor (MP), a programmable logic integrated circuit (PLIC), at least one first transceiver (FT), at least one second transceiver (ST), a read-only memory (ROM), a random access memory (RAM), a keyboard, a display, a power unit. The MC is provided with control for power supply voltages of the power supply unit and power supply control of the MC and the PLIC providing key input of original data decryption generation of the key information, the integrity check key of the software of the PLIC and the software integrity check key of the radio station by means of the keyboard. The RAM is provided for storing said input keys. The MP is configured to generate the key information and the radio data according to the ROM and RAM data.

EFFECT: improved protection of the key information and radio data.

2 cl, 1 dwg

RU 2634202 C1

RU 2634202 C1



RU 2634202 C1

RU 2634202 C1

Изобретение относится к радиотехнике и вычислительной технике, а именно к специализированным вычислительным средствам для радиостанции, обеспечивающим формирование, хранение, загрузку сформированных данных в радиостанцию, уничтожение ключевой информации и радиоданных, хранение и уничтожение данных конфигураций, данных исходной последовательности (ИП) и данных ключей проверки целостности программного обеспечения радиостанции (ДКРЦ), уничтожение ключевой информации (КИ) и криптографически опасной информации (КОИ) при аварийных ситуациях, несанкционированном доступе (НСД), а также по команде оператора. Заявленное устройство относится к области автоматизированных рабочих мест оператора выработки ключевой информации радиоданных для радиостанции.

Из патента РФ RU 2321055 (опубликован 27.03.2008; МПК G06F 21/20, G06F 12/14) известно устройство доверенной загрузки и защиты информации от несанкционированного доступа для компьютеров информационно-вычислительных систем. Это устройство содержит контроллер обмена информацией с компьютером, процессор идентификации и аутентификации пользователей, работающий независимо от центрального процессора компьютера, модуль блокировки шины управления и обмена данными компьютера при попытке несанкционированного доступа к нему, контроллер обмена информацией с внешним носителем информации, блоки энергонезависимой памяти с учетными данными пользователя, настройками устройства и электронным журналом, а также устройство контроля питания. Внешний магистральный вход/выход контроллера обмена информацией с компьютером соединен с шиной управления и обмена данными компьютера, его управляющий вход подключен к управляющему выходу модуля блокировки шины управления и обмена данными компьютера, а его внутренние магистральные вход/выход соединены с магистралью локальной шины устройства. Внутренние магистральные вход/выход процессора идентификации и аутентификации пользователей через магистраль локальной шины устройства подключены к магистральному входу/выходу энергонезависимой памяти и к входу модуля блокировки шины управления и обмена данными компьютера. Внешние магистральные вход/выход процессора подключены к контроллеру обмена информацией с внешним носителем информации, а сигнальный вход процессора подключен к выходу устройства контроля питания. В состав устройства введены блок интерфейсов внешних устройств, включающий межмодульный интерфейс аппаратного шифратора и интерфейс управления сетевыми адаптерами, входы которых соединены с внешними магистральными входами/выходами процессора идентификации и аутентификации, а выходы - с входами аппаратного шифратора и сетевых адаптеров соответственно. Модуль блокирования внешних устройств содержит устройства блокировки и управления жесткими дисками, электромагнитной защелкой корпуса компьютера, сигналами RESET и POWER компьютера, входы которых подключены к дополнительным управляющим выходам модуля блокировки шины управления и обмена данными компьютера и управляющему выходу процессора идентификации и аутентификации, а выходы - к входам/выходам соответствующих управляемых и блокируемых устройств. Энергонезависимая флэш-память с блоками хранения доверенной операционный системы, программного обеспечения контроля целостности компонентов устройства, удаленного администрирования и управления устройством, контроля всех критических интервалов времени процедуры запуска и загрузки компьютера, клиентской части ПО «тонкого клиента», магистральный вход/выход которой соединен с магистралью локальной шины устройства. Микроконтроллер датчиков вскрытия и извлечения компонентов компьютера с собственным независимым

источником питания, внешние входы которого подсоединены к выходам соответствующих датчиков, а выход - к сигнальному входу процессора идентификации и аутентификации. Аппаратный датчик случайных чисел, выход которого соединен с входом модуля блокировки шины управления и обмена данными компьютера. Оперативное запоминающее устройство, магистральный вход/выход которого соединен через локальную шину устройства с внутренними магистральными входом/выходом процессора идентификации и аутентификации. В состав процессора идентификации и аутентификации дополнительно введены модуль постоянной аутентификации пользователя, модуль управления загрузкой ключей аппаратного шифратора и модуль управления сетевыми адаптерами, реализующие через блок интерфейсов внешних устройств взаимодействие с внешним носителем информации, аппаратным шифратором и сетевыми адаптерами соответственно. Модуль проверки целостности и состояния аппаратных компонентов устройства защиты осуществляет их диагностику по каналам связи внутренних магистральных входов/выходов процессора идентификации и аутентификации с компонентами устройства. Модуль взаимодействия с системой разграничения доступа обеспечивает информационные связи процессора идентификации и аутентификации через локальную шину устройства, контроллер обмена информацией с компьютером и шину управления и обмена данными компьютера с системой разграничения доступа компьютера. Модуль взаимодействия с серверами информационно-вычислительной системы обеспечивает работу компьютера в режиме удаленного управления или «тонкого» клиента с использованием программного обеспечения, загружаемого в оперативную память компьютера из соответствующих блоков энергонезависимой флэш-памяти через ее магистральный вход/выход, локальную шину устройства, контроллер обмена информацией с компьютером и шину управления и обмена данными компьютера.

Указанное известное устройство предназначено для доверенной загрузки компьютера и защиты от несанкционированного доступа (НСД) к информации, обрабатываемой и хранимой в персональных компьютерах и в компьютерных информационно-вычислительных системах, и непосредственно не может использоваться устройстве программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции. Устройство не может производить уничтожение ключевой информации и радиоданных, хранение и уничтожение данных конфигураций, данных исходной последовательности (ИП) и данных ключей проверки целостности программного обеспечения радиостанции (ДКРЦ), уничтожение ключевой информации (КИ) и криптографически опасной информации (КОИ) при аварийных ситуациях, несанкционированном доступе (НСД), а также по команде оператора.

Также известно устройство создания доверенной среды и защиты информации от несанкционированного доступа для компьютеров информационно-вычислительных систем (см. патент РФ RU 2538329, опубликованный 10.01.2015; МПК G06F 21/57, G06F 12/14). Оно содержит управляющий микроконтроллер, энергонезависимую флэш-память большой емкости с блоками хранения программного обеспечения устройства, энергонезависимую быстродействующую память с электронным журналом для регистрации событий при функционировании устройства, блоком с учетными данными пользователей и блоком с настройками и с ключами удаленного управления, блок переключателей для выбора режима работы устройства, звуковое устройство для дополнительного информирования о выявленных несанкционированных действиях, блок интерфейсов внешних устройств, а также устройство блокировки питания компьютера. Управляющий микроконтроллер включает в свой состав модуль

идентификации и аутентификации пользователя, модули проверки целостности и состояния аппаратных и программных компонентов устройства защиты, модуль контроля всех критичных интервалов времени процедуры запуска и загрузки компьютера, модуль управления загрузкой ключей аппаратного шифратора, модуль взаимодействия с системой разграничения доступа, модуль взаимодействия с серверами информационно-вычислительной системы, модуль настройки устройства, датчик случайных чисел. В энергонезависимой флэш-памяти большой емкости размещаются доверенная операционная система, модули программного обеспечения контроля целостности компонентов устройства, удаленного администрирования и управления устройством, клиентская часть программного обеспечения «тонкого клиента», причем внутренние магистральные вход/выход микроконтроллера через магистраль локальной шины устройства подключены к магистральным входам/выходам энергонезависимых флэш-памяти и быстродействующей памяти, а внешние магистральные вход/выход микроконтроллера подключены к входам блока интерфейсов внешних устройств, включающего USB Host интерфейс, интерфейс iButton идентификатора типа Touch Memory и межмодульный интерфейс аппаратного шифратора. В состав устройства введены накопитель на основе микросхемы флэш-памяти с интерфейсом SPI, который подключается к шине SPI чипсета материнской платы компьютера и содержит в своей защищенной от записи области BIOS компьютера с дополнительно встроенными командами, обеспечивающими взаимодействие с управляющим микроконтроллером и проверку целостности загружаемого программного обеспечения, и управляемый быстродействующий электронный ключ, установленный на шину SPI материнской платы между чипсетом компьютера и накопителем. Микроконтроллер снабжен каналом управления электронным ключом, соединяющим управляющий выход порта ввода-вывода микроконтроллера с управляющим входом электронного ключа, а также контроллером интерфейса SPI, обеспечивающим подключение микроконтроллера к шине SPI и работу его в режиме прямого доступа к памяти накопителя и в режиме контроля команд от чипсета к накопителю по шине SPI, образуя таким образом аппаратный узел, осуществляющий контроль целостности BIOS в накопителе до ее загрузки с возможностью последующего контроля на шине SPI команд чипсета к накопителю и их блокировки с помощью электронного ключа. Для реализации каналов связи микроконтроллера с аппаратными компонентами и чипсетом он дополнительно снабжен интерфейсами USB и SMBus, а для блокировки запуска компьютера в случае нарушения целостности BIOS или других несанкционированных действий в состав микроконтроллера включен блок управления основным питанием компьютера, встроенный в соответствующий канал управления чипсета, причем само устройство подключено к дежурному источнику питания компьютера.

Это устройство, также как предыдущее, предназначено для доверенной загрузки компьютера и защиты от несанкционированного доступа (НСД) к информации, обрабатываемой и хранимой в персональных компьютерах и в компьютерных информационно-вычислительных системах, и непосредственно не может использоваться в устройстве программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции. Устройство не может производить уничтожение ключевой информации и радиоданных, хранение и уничтожение данных конфигураций, данных исходной последовательности (ИП) и данных ключей проверки целостности программного обеспечения радиостанции (ДКРЦ), уничтожение ключевой информации (КИ) и криптографически опасной информации (КОИ) при аварийных ситуациях, несанкционированном доступе (НСД), а также по команде оператора.

Аналогов заявленного устройства программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции не обнаружено.

Решаемой изобретением задачей является создание специализированного вычислительного средства (программно-аппаратного комплекса), обеспечивающего формирование, хранение, уничтожение ключевой информации и радиоданных, хранение и уничтожение данных конфигураций, данных исходной последовательности (ИП) и данных ключей проверки целостности программного обеспечения радиостанции (ДКРЦ), уничтожение ключевой информации (КИ) и криптографически опасной информации (КОИ) при аварийных ситуациях, несанкционированном доступе (НСД) и по команде оператора, а также загрузку сформированных данных в радиостанцию.

Техническое решение относится к области автоматизированных рабочих мест выработки ключевой информации для радиостанции. Решение построено на основе модульной цифровой программируемой аппаратной платформы и аппаратно-независимого модульного программного обеспечения.

Устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных (ПАК-КР) может быть использовано в радиостанциях.

Техническим результатом является повышение надежности защиты ключевой информации и радиоданных.

Для решения поставленной задачи с достижением технического результата заявленное устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции содержит микроконтроллер (МК), микропроцессор (МП), программируемую логическую интегральную схему (ПЛИС), по меньшей мере один первый приемопередатчик (ПП), по меньшей мере один второй приемопередатчик (ПП), постоянное запоминающее устройство (ПЗУ), оперативное запоминающее устройство (ОЗУ), клавиатуру, дисплей, блок питания. Шина питания от блока питания соединена с входом микроконтроллера. Первый вход/выход микроконтроллера соединен посредством шины данных с входом/выходом клавиатуры, второй вход/выход микроконтроллера соединен посредством шины данных с первым входом/выходом микропроцессора, а его третий вход/выход посредством шины данных - с первым входом/выходом программируемой логической интегральной схемы. Второй вход/выход микропроцессора соединен посредством шины данных с первым входом/выходом постоянного запоминающего устройства, третий вход/выход микропроцессора соединен посредством шины данных с входом/выходом оперативного запоминающего устройства, четвертый вход/выход микропроцессора соединен посредством шины данных со вторым входом/выходом программируемой логической интегральной схемы. Третий вход/выход ПЛИС соединен посредством шины данных со вторым входом/выходом постоянного запоминающего устройства, четвертый вход/выход ПЛИС соединен посредством шины данных с входом/выходом первого приемопередатчика, пятый вход/выход ПЛИС соединен посредством шины данных с входом/выходом второго приемопередатчика, а выход ПЛИС соединен посредством шины данных с дисплеем. Первый приемопередатчик служит для связи с персональной электронной вычислительной машиной, а второй приемопередатчик - для связи с радиостанцией или для связи с устройством ввода радиоданных. Микроконтроллер выполнен обеспечивающим контроль напряжений питания блока питания и управление питанием микропроцессора и ПЛИС, а также выполнен обеспечивающим ввод ключа расшифровки исходных данных формирования ключевой информации, ключа проверки целостности программного обеспечения программируемой логической интегральной схемы и ключа проверки целостности программного обеспечения радиостанции

посредством клавиатуры. Оперативное запоминающее устройство выполнено обеспечивающим хранение упомянутых введенных ключей. Микропроцессор выполнен обеспечивающим формирование ключевой информации и радиоданных по данным постоянного запоминающего устройства и оперативного запоминающего устройства. ПЛИС выполнена обеспечивающей контроль потока данных ключевой информации и радиоданных, обеспечивающей связь с персональной электронной вычислительной машиной посредством первого приемопередатчика, обеспечивающей связь с радиостанцией или устройством ввода радиоданных посредством второго приемопередатчика, а также обеспечивающей отображение контролируемого потока данных посредством дисплея.

Возможен дополнительный вариант выполнения устройства, в котором целесообразно, чтобы были введены внутренняя батарея и схема управления батареей, при этом внутренняя батарея соединена через схему управления батареей дополнительной шиной питания с четвертым входом/выходом микроконтроллера.

Указанные преимущества, а также особенности настоящего изобретения поясняются с помощью варианта его выполнения со ссылками на чертеж.

Чертеж изображает структурную схему заявленного устройства.

Устройство программно-аппаратного комплекса формирования ключевой информации (КИ) и радиоданных (РД) для радиостанции содержит микроконтроллер 1 (МК), микропроцессор 2 (МП), программируемую логическую интегральную схему 3 (ПЛИС), по меньшей мере один первый приемопередатчик 4 (ПП), по меньшей мере один второй приемопередатчик 5 (ПП), постоянное запоминающее устройство 6 (ПЗУ), оперативное запоминающее устройство 7 (ОЗУ), клавиатуру 8, дисплей 9, блок 10 питания. Шина питания от блока 10 питания соединена с входом микроконтроллера 1. Первый вход/выход микроконтроллера 1 соединен посредством шины данных с входом/выходом клавиатуры 8. Второй вход/выход МК 1 соединен посредством шины данных с первым входом/выходом микропроцессора 2, а его третий вход/выход посредством шины данных - с первым входом/выходом ПЛИС 3. Второй вход/выход МП 2 соединен посредством шины данных с первым входом/выходом ПЗУ 6, третий вход/выход МП 2 соединен посредством шины данных с входом/выходом ОЗУ 7, четвертый вход/выход МП 2 соединен посредством шины данных со вторым входом/выходом ПЛИС 3. Третий вход/выход ПЛИС 3 соединен посредством шины данных со вторым входом/выходом ПЗУ 6, четвертый вход/выход ПЛИС 3 соединен посредством шины данных с входом/выходом первого ПП 4, пятый вход/выход ПЛИС 3 соединен посредством шины данных с входом/выходом второго ПП 5, а выход программируемой логической интегральной схемы соединен посредством шины данных с дисплеем 9. Первый приемопередатчик 4 служит для связи с персональной электронной вычислительной машиной (ПЭВМ), а второй приемопередатчик 5 - для связи с радиостанцией или для связи с устройством ввода радиоданных (УВРД). МК 1 выполнен обеспечивающим контроль напряжений питания блока 10 питания и управление питанием МП 2 и ПЛИС 3, а также обеспечивающим ввод ключа расшифровки исходных данных формирования ключевой информации (КИ), ключа проверки целостности программного обеспечения ПЛИС 3 и ключа проверки целостности программного обеспечения радиостанции посредством клавиатуры 8. ОЗУ 7 выполнено обеспечивающим хранение упомянутых введенных ключей. МП 2 выполнен обеспечивающим формирование ключевой информации и радиоданных по данным ПЗУ 6 и ОЗУ 7. ПЛИС 3 выполнена обеспечивающей контроль потока данных ключевой информации и радиоданных, обеспечивающей связь с ПЭВМ посредством первого

приемопередатчика 4, обеспечивающей связь с радиостанцией или УВРД посредством второго приемопередатчика 5, а также обеспечивающей отображение контролируемого потока данных посредством дисплея 9.

В устройство может быть введена внутренняя батарея 11 и схема 12 управления батареей (СУБ). Внутренняя батарея 11 соединена через СУБ 12 дополнительной шиной питания с четвертым входом/выходом МК 1.

Работает устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции следующим образом.

МК 1 предназначен для ввода ключа расшифровки исходных данных формирования ключевой информации (КИ), ключа проверки целостности программного обеспечения (ПО), ключа проверки целостности ПО ПАК-КР. Ввод ключей осуществляется с ключевых блокнотов (бумажного носителя) посредством клавиатуры 8. Ключи хранятся в ОЗУ 7 МК 1 в маскированном виде и представляют собой 64-байтные массивы информации, которые передаются в МП 2 по запросу.

Взаимодействие МК 1 с МП 2 осуществляется по интерфейсу I2C. МП 2 является ведущим, а МК 1 ведомым. Заголовок и контрольная сумма посылки передаются в открытом виде (т.е. без шифрования), а информация кодируется. После обработки запроса МК 1 формирует ответ и генерирует прерывание IRQ0, по которому МП 2 запрашивает ответную информацию от МК 1. При нажатии соответствующей клавиши клавиатуры 8 МК 1 генерирует прерывание IRQ1, по которому МП 2 запрашивает состояние клавиатуры 8 от МК 1, анализирует полученные данные и вырабатывает необходимые действия.

Одной из функций МК 1 является контроль и управление питанием МП 2 и ПЛИС 3, а также контроль заряда внутренней батареи 11. Для этого у МК 1 есть встроенные АЦП и компараторы, в задачи которых входит непосредственный контроль любого отклонения напряжений в процессе работы. СУБ 12 предназначен для управления режимами заряда внутренней батареи 11. СУБ 12 корректирует токи заряда внутренней батареи 11 в зависимости от температуры окружающей среды, а также реализует 2 режима заряда - заряд током и заряд напряжением.

Пока присутствует питание на внутренней батарее 11, МК 1 находится в режиме сохранения КИ. При этом остальные основные потребители (МП 2 и ПЛИС 3) отключены. В случае наступления события НСД, или отклонения от нормы внутренних напряжений питания, или при нажатии кнопок экстренного стирания, а также по команде от МП 2 происходит уничтожение масок КИ в ОЗУ 7.

В ПЗУ 6 хранятся программы работы МП 2, исходная шумовая последовательность (ИП), схемы радиосвязи, данные КИРД, журнал работы ПАК-КР, ключи хранения ПАК-КР. Все хранимые данные в ПЗУ 6 зашифрованы.

МП 2 выполняет функцию формирования КИ и РД. Основные параметры выбираются в меню на дисплее 9 индикатора с помощью клавиатуры 8 или задаются по внешней команде от ПЭВМ. Взаимодействие с ПЭВМ обеспечивается по интерфейсу UART0, который проходит через ПЛИС 3 и преобразуется в интерфейс RS-232 или USB 2.0 в зависимости от типа подключенного кабеля. Тип кабеля распознается устройством автоматически. Между сигнальными цепями ПЛИС 3 и первым приемопередатчиком 4 (UART/RS-232 и UART/USB) используются оптические развязки и фильтры (не показаны). Фильтры блокируют попадание открытой (не зашифрованной) внутренней информации на внешние цепи, что предотвращает утечку информации по общим линиям. В ПЛИС 3 реализован контроль потока данных и блокировка передачи в случае нарушения последовательности контрольных байт. В случае возникновения ошибки,

передача данных блокируется.

В МП 2 используются два DSP-ядра для быстрой работы алгоритмов генерации КИ. Для формирования КИ и РД МП 2 необходимы данные исходной последовательности (ИП), данные ключей проверки целостности радиостанций (ДКРЦ), которые заранее вводятся в ПЭВМ посредством оптического диска, а затем передаются через первый ПП 4 и ПЛИС 3 в МП 2. При успешном формировании КИ и РД МП 2 информирует об этом через ПЛИС 3 и первый ПП 4 ПЭВМ.

Для загрузки КИ и РД в радиостанцию используется интерфейс UART1. Также он применяется для аутентификации оператора посредством УВРД. При подключении УВРД или радиостанции данные через второй приемопередатчик 5 интерфейса RS-485, оптическую развязку и фильтр (на фигуре не показано) попадают в ПЛИС 3. В ПЛИС 3 реализован контроль выходного потока данных. В случае возникновения нарушения последовательности передачи контрольных байт передача данных блокируется, а на МП 2 посылается сигнал ошибки. ПЛИС 3 обеспечивает связи МП 2 с дисплеем 9, ПЭВМ, УВРД и радиостанцией.

Таким образом, устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции позволяет осуществить:

- обмен данными с ПЭВМ по интерфейсу USB 2.0 или RS-232;
- контроль целостности программного обеспечения (ПО);
- аутентификацию оператора с использованием УВРД;
- ввод с клавиатуры 8 ключевой информации;
- получение от ПЭВМ криптограмм исходных данных для формирования КИ и РД;
- формирование ключей аутентификации оператора, формирование КИ и РД;
- отправку сформированных КИ и РД в радиостанцию по интерфейсу RS-485;
- уничтожение КИ и РД по истечении срока действия конфигурации, при вскрытии корпуса устройства, при нажатии кнопок клавиатуры 8 экстренного стирания оператором;
- получение данных проверки целостности программного обеспечения (ПО) радиостанций, их расшифровку с использованием ключей и хранение в зашифрованном и имитозащищенном виде на ключе хранения, а также инициализацию в радиостанции режима проверки целостности;
- получение от радиостанции результатов проверки целостности, их анализ и отображение на дисплее 9 эталонной и полученной от радиостанции контрольных групп проверки целостности, а также индикацию результата их сравнения.

Благодаря этому в заявленном устройстве обеспечивается достижение технического результата, заключающегося в повышении надежности защиты ключевой информации и радиоданных.

Наиболее успешно заявленное устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции промышленно применимо в радиотехнике при формировании, хранении, загрузке сформированных данных в радиостанцию, для уничтожения ключевой информации и радиоданных, для хранения и уничтожения данных конфигураций, данных исходной последовательности (ИП) и данных ключей проверки целостности программного обеспечения радиостанции (ДКРЦ), для уничтожения ключевой информации (КИ) и криптографически опасной информации (КОИ) при аварийных ситуациях и при несанкционированном доступе (НСД), а также по команде оператора.

(57) Формула изобретения

1. Устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции, содержащее микроконтроллер, микропроцессор, программируемую логическую интегральную схему, по меньшей мере один первый приемопередатчик, по меньшей мере один второй приемопередатчик, постоянное запоминающее устройство, оперативное запоминающее устройство, клавиатуру, дисплей, блок питания, причем шина питания от блока питания соединена с входом микроконтроллера, первый вход/выход микроконтроллера соединен посредством шины данных с входом/выходом клавиатуры, второй вход/выход микроконтроллера соединен посредством шины данных с первым входом/выходом микропроцессора, а его третий вход/выход посредством шины данных - с первым входом/выходом программируемой логической интегральной схемы, второй вход/выход микропроцессора соединен посредством шины данных с первым входом/выходом постоянного запоминающего устройства, третий вход/выход микропроцессора соединен посредством шины данных с входом/выходом оперативного запоминающего устройства, четвертый вход/выход микропроцессора соединен посредством шины данных со вторым входом/выходом программируемой логической интегральной схемы, третий вход/выход программируемой логической интегральной схемы соединен посредством шины данных со вторым входом/выходом постоянного запоминающего устройства, четвертый вход/выход программируемой логической интегральной схемы соединен посредством шины данных с входом/выходом первого приемопередатчика, пятый вход/выход программируемой логической интегральной схемы соединен посредством шины данных с входом/выходом второго приемопередатчика, выход программируемой логической интегральной схемы соединен посредством шины данных с дисплеем, первый приемопередатчик служит для связи с персональной электронной вычислительной машиной, а второй приемопередатчик - для связи с радиостанцией или для связи с устройством ввода радиоданных, при этом микроконтроллер выполнен обеспечивающим контроль напряжений питания блока питания и управление питанием микропроцессора и программируемой интегральной логической схемы, обеспечивающим ввод ключа расшифровки исходных данных формирования ключевой информации, ключа проверки целостности программного обеспечения программируемой логической интегральной схемы и ключа проверки целостности программного обеспечения радиостанции посредством клавиатуры, оперативное запоминающее устройство выполнено обеспечивающим хранение упомянутых введенных ключей, микропроцессор выполнен обеспечивающим формирование ключевой информации и радиоданных по данным постоянного запоминающего устройства и оперативного запоминающего устройства, программируемая интегральная логическая схема выполнена обеспечивающей контроль потока данных ключевой информации и радиоданных, обеспечивающей связь с персональной электронной вычислительной машиной посредством первого приемопередатчика, обеспечивающей связь с радиостанцией или устройством ввода радиоданных посредством второго приемопередатчика, а также обеспечивающей отображение контролируемого потока данных посредством дисплея.

2. Устройство по п. 1, отличающееся тем, что введена внутренняя батарея и схема управления батареей, при этом внутренняя батарея соединена через схему управления батареей дополнительной шиной питания с четвертым входом/выходом микроконтроллера.

1

Устройство программно-аппаратного комплекса формирования ключевой информации и радиоданных для радиостанции