РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 704 268**(13) **C1**

(51) МПК
H04L 9/08 (2006.01)
H04W 12/06 (2009.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 63/0428 (2019.05); H04L 63/0435 (2019.05); H04L 9/0819 (2019.05); H04L 9/0825 (2019.05); H04W 12/06 (2019.05)

(21)(22) Заявка: **2018118339, 18.05.2018**

(24) Дата начала отсчета срока действия патента:
18.05.2018

Дата регистрации:
25.10.2019

Приоритет(ы):
(22) Дата подачи заявки: **18.05.2018**

(45) Опубликовано: **25.10.2019** Бюл. № **30**

Адрес для переписки:
124527, Москва, Зеленоград, Солнечная аллея, 8, ООО Фирма "АНКАД", генеральному директору Романцу Ю.В.

(72) Автор(ы):
Борисов Кирилл Викторович (RU),
Любушкина Ирина Евгеньевна (RU),
Панасенко Сергей Петрович (RU),
Романец Юрий Васильевич (RU),
Сиротин Артем Владимирович (RU),
Сырчин Владимир Кимович (RU)

(73) Патентообладатель(и):
Общество с ограниченной ответственностью Фирма "АНКАД" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 9871772 B1, 16.01.2018. US 2016/0274578 A1, 22.09.2016. WO 2017/042403 A1, 16.03.2017. RU 2446606 A1, 27.03.2012.**

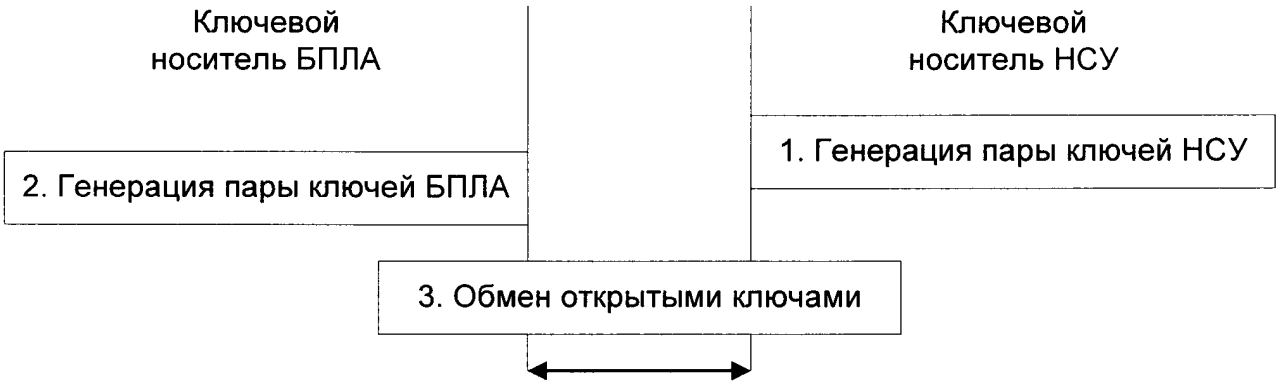
(54) Способ, система и устройство криптографической защиты каналов связи беспилотных авиационных комплексов

(57) Реферат:

Группа изобретений относится к области систем защищенной беспроводной связи и предназначена для защиты беспроводных каналов связи между беспилотным летательным аппаратом (БПЛА) или аналогичным удаленно управляемым аппаратом и наземной станцией управления (НСУ). Технический результат - обеспечение криптографической защиты каналов управления, телеметрии и передачи данных полезной нагрузки БПЛА от несанкционированного доступа (НСД) к передаваемой по данным каналам информации и от ее несанкционированной модификации. Технический результат достигается использованием ключевых носителей, оснащенных криптографическими функциями, схемы взаимной аутентификации БПЛА и НСУ на основе асимметричных криптографических ключей, совмещенной со схемой вычисления общего симметричного ключа, и схемы генерации сеансовых мастер-ключа и ключей шифрования и вычисления имитовставки для последующего формирования защищенного канала беспроводной связи между БПЛА и НСУ, обеспечивающего шифрование передаваемой информации и контроль ее целостности, при этом схемы взаимной аутентификации, вычисления общего симметричного ключа и генерации сеансовых ключей разработаны с учетом специфики применения БПЛА и формирования каналов беспроводной связи между БПЛА и НСУ. 3 н. и 46 з.п. ф-лы, 4 ил.

RU 2704268 C1

RU 2704268 C1



Фиг. 1

RU 2704268 C1

RU 2704268 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 704 268**(13) **C1**

(51) Int. Cl.
H04L 9/08 (2006.01)
H04W 12/06 (2009.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 63/0428 (2019.05); H04L 63/0435 (2019.05); H04L 9/0819 (2019.05); H04L 9/0825 (2019.05); H04W 12/06 (2019.05)

(21)(22) Application: **2018118339, 18.05.2018**

(24) Effective date for property rights:
18.05.2018

Registration date:
25.10.2019

Priority:
(22) Date of filing: **18.05.2018**

(45) Date of publication: **25.10.2019** Bull. № **30**

Mail address:
124527, Moskva, Zelenograd, Solnechnaya alleya, 8, OOO Firma "ANKAD", generalnomu direktoru Romantsu YU.V.

(72) Inventor(s):
Borisov Kirill Viktorovich (RU),
Lyubushkina Irina Evgenevna (RU),
Panasenko Sergej Petrovich (RU),
Romanets Yurij Vasilevich (RU),
Sirotin Artem Vladimirovich (RU),
Syrchin Vladimir Kimovich (RU)

(73) Proprietor(s):
Obshchestvo s ogranichennoj otvetstvennostyu Firma "ANKAD" (RU)

RU 2704268 C1

(54) METHOD, SYSTEM AND DEVICE FOR CRYPTOGRAPHIC PROTECTION OF COMMUNICATION CHANNELS OF UNMANNED AERIAL SYSTEMS

(57) Abstract:

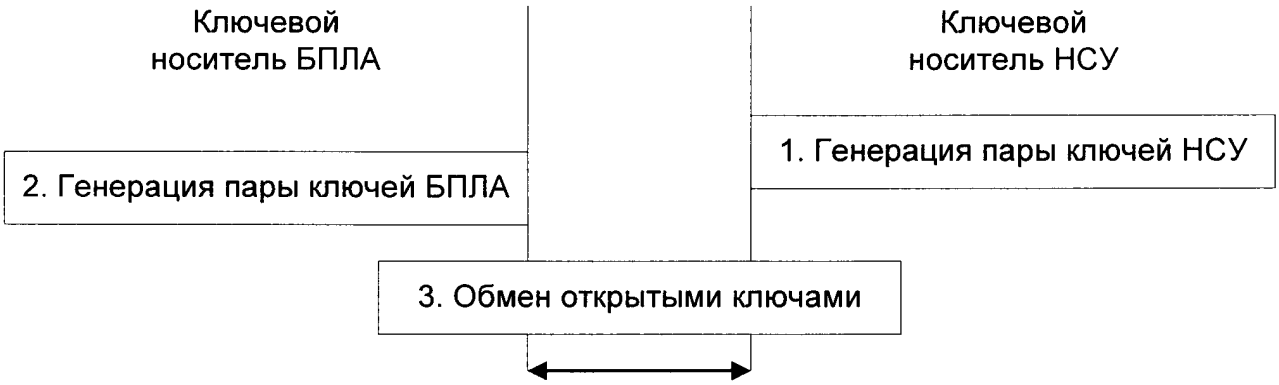
FIELD: cryptography.

SUBSTANCE: group of inventions relates to secure wireless communication systems and is intended to protect wireless communication channels between an unmanned aerial vehicle (UAV) or similar remotely controlled apparatus and a ground control station (GCS). Technical result is achieved using key carriers equipped with cryptographic functions, UAV and GCS mutual authentication scheme based on asymmetric cryptographic keys combined with common symmetric key calculation circuit, and a circuit for generating a session master key and encryption keys and calculating an simulator for subsequent generation of a secure wireless communication channel between the UAV and the GCS, which enables encryption of the transmitted information and monitoring its integrity, wherein the mutual authentication schemes, the common symmetric key calculations and the session keys generation are developed taking into account the UAV application specifics and the wireless communication channels formation between the UAV and the GCS.

EFFECT: provision of cryptographic protection of control channels, telemetry and data transfer of UAV payload from unauthorized access to data transmitted via data channels and its unauthorized modification.

49 cl, 4 dwg

RU 2704268 C1



Фиг. 1

RU 2704268 C1

RU 2704268 C1

Изобретение относится к области систем защищенной беспроводной связи и предназначено для защиты беспроводных каналов связи между беспилотным летательным аппаратом (БПЛА) или аналогичным удаленно управляемым аппаратом и наземной станцией управления (НСУ). Его использование позволит получить технический результат в виде обеспечения криптографической защиты каналов управления, телеметрии и передачи данных полезной нагрузки БПЛА от несанкционированного доступа (НСД) к передаваемой по данным каналам информации и от ее несанкционированной модификации.

Беспилотные авиационные комплексы (БАК), как правило, включают в себя наземную станцию управления, беспилотный летательный аппарат и каналы связи между ними. В зависимости от характеристик и задач БПЛА, управление им может осуществляться как автоматически, так и вручную с помощью команд, передаваемых оператором на БПЛА через пульт дистанционного управления (ПДУ), являющийся частным случаем наземной станции управления.

Защита каналов связи между НСУ и БПЛА от внешних программно-аппаратных воздействий в настоящее время является одной из наиболее актуальных проблем. Атаки на БПЛА могут быть направлены на перехват управления, вывод БПЛА из строя, получение или искажение информации, передаваемой полезной нагрузкой БПЛА, или для дальнейшей атаки на НСУ и взаимодействующие с ней системы.

В настоящее время существует множество средств защиты целостности и конфиденциальности информации, передаваемой по различным каналам связи, в т.ч. беспроводным. Однако существует определенная специфика защиты БАК, определяемая совокупностью способов несанкционированного или случайного доступа к системам БАК, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) информации. В частности, при разработке средств защиты для БАК необходимо учитывать следующие особенности (см., например, [1-3]):

1. БПЛА, как и другие роботизированные комплексы, обычно функционируют под управлением операционных систем (ОС), специально предназначенных для управления роботизированными комплексами и системами, среди которых - специализированные операционные системы реального времени (Real-Time Operation System - RTOS). В качестве одного из основных требований к таким ОС выдвигается требование обеспечения предсказуемости или детерминированности поведения системы в наихудших внешних условиях, что резко отличается от требований к ОС общего назначения, которые, в основном, относятся к их производительности и возможности применения на различных аппаратных платформах.

2. БПЛА представляет собой сложную интегрированную автоматизированную систему - аппаратура и агрегаты на борту БПЛА структурно объединены в системы, предназначенные для решения отдельных задач. Отдельные системы могут объединяться в более крупные структурные элементы - комплексы. Комплекс бортового оборудования - совокупность функционально-связанных систем, приборов, датчиков, вычислительных устройств. Система управления БПЛА обеспечивает управление и взаимодействие между всеми комплексами или системами БПЛА.

3. БПЛА в общем случае можно представить также как телекоммуникационную систему, состоящую из устройств, между которыми осуществляется обмен информацией по специальным протоколам.

Кроме того, важнейшими эксплуатационными характеристиками БПЛА являются такие их взаимосвязанные свойства, как максимальный вес полезной нагрузки БПЛА

и максимальные длительность и дальность полета. Поскольку питание бортового оборудования БПЛА обычно осуществляется от собственного источника питания, имеющего ограниченный ресурс, все функционирующие на борту БПЛА системы должны отличаться экономичностью, т.е. минимально возможным энергопотреблением.

Поэтому средства защиты информации от внешних программно-аппаратных воздействий для бортовой части БАК должны обладать небольшими массогабаритными характеристиками и низкой ресурсоемкостью. Шифрование сигналов БПЛА также не должно существенно усложнять процесс обмена данными в реальном масштабе времени, нарушать оперативность передачи команд и информационных потоков. Следовательно, системы защиты каналов связи БПЛА должны иметь минимальный вес и предъявлять минимально возможные требования к вычислительным ресурсам с целью минимизации отрицательного влияния на перечисленные выше основные эксплуатационные характеристики БПЛА.

Угроза осуществления перечисленных выше атак на БПЛА может возникнуть в результате образования канала реализации угрозы между источником угрозы и БПЛА. Поскольку БПЛА используют каналы беспроводной связи с НСУ, реализация угрозы может осуществляться путем эксплуатации атакующим существующих каналов беспроводной связи с БПЛА.

В идеальном варианте защите должны подлежать все каналы беспроводной связи БПЛА с НСУ (канал управления, канал телеметрии и канал передачи информации от полезной нагрузки БПЛА). Однако, с учетом требований минимальной ресурсоемкости систем защиты БПЛА, во многих случаях рассматривается защита только наиболее критичных каналов взаимодействия БПЛА с НСУ, к которым можно отнести следующие:

- канал управления, поскольку основные угрозы БПЛА (такие, как перехват управления или вывод из строя) наиболее просто осуществить в случае успешной эксплуатации атакующим канала управления БПЛА (см., например, [4, 5]);

- канал телеметрии, поскольку успешная подмена атакующим телеметрической информации также может привести к реализации перечисленных выше угроз БПЛА.

Стоит отметить, что в настоящее время существует достаточно большое количество методов защиты информации для стандартных протоколов беспроводной связи и их реализаций (см., например, [6]). Однако их использование напрямую для защиты каналов связи БПЛА и НСУ невозможно или нецелесообразно по следующим причинам:

1. Методы, протоколы и реализации криптографических алгоритмов зависят от организации самого радиоканала и структуры разворачиваемой беспроводной сети. Прямое копирование любого набора методов и протоколов информационной безопасности для использования в каналах связи БПЛА невозможно в силу расхождения принципов организации радиоканалов, количества объектов связи и структуры их связности.

2. Многие методы, например, организация доверенного центра аутентификации объектов, центра генерации и распределения ключей, обладают значительной избыточностью в применении к БАК.

3. Применение многих методов обеспечения безопасности приводит к значительному повышению нагрузки на каналы связи и снижает пропускную способность каналов. В системе управления БПЛА любая излишняя нагрузка на каналы связи может привести к снижению скорости передачи управляющей информации и повлиять на управляемость и динамику полета самого летательного аппарата.

4. Одними из основных принципов стандартов массовой связи являются удобство,

простота и прозрачность настроек для рядового пользователя. Данный принцип распространяется и на методы обеспечения безопасности, что приводит к тому, что производители вынуждены пользоваться настройками по умолчанию, которые позволяют подключаться к системам связи, но снижают показатели безопасности передачи данных.

5. Некорректная реализация криптографических алгоритмов и особенно систем управления криптографическими ключами, а также их разработка без учета особенностей последующего применения приводят к наличию уязвимостей в таких реализациях (см., например, [7]).

Отметим, что специфика применения БПЛА требует применения специально адаптированных для БПЛА схем генерации, распределения и использования ключевой информации, значительно отличающихся от таковых в обычных протоколах защиты беспроводной связи.

Проведенный заявителем анализ патентной и научно-технической информации показал наличие патентов на способы, устройства и системы защиты информации, основанные на применении криптографических алгоритмов и предназначенные для защиты каналов связи БПЛА или аналогичных устройств либо легко адаптируемые для использования в данных целях.

Например, в патенте США US 8219799 от 10.07.2012 г. [8] корпорацией Lockheed Martin предлагается защищенная система связи, включающая в себя процессор обработки данных, конвертер интернет-протокола, который преобразует данные, шифратор/дешифратор для обеспечения дополнительной безопасности, криптографический модуль, оценивающий уровень безопасности данных и проверяющий криптографические ключи. Процессор связи обеспечивает управление в реальном времени и может изменять источник или получатель данных, ключ шифрования, уровень безопасности, протокол связи в ответ на данные датчиков, полученные от коммуникационного объекта или от командных сигналов подключенной или дистанционной системы управления.

В патенте США US 9531689 от 27.12.2016 г. [9] предложены способ и система шифрования и дешифрования данных в устройстве памяти и в пакетах данных, передаваемых по сети связи. Система состоит из двух устройств сетевой обработки, одно из которых предназначено для приема и хранения передаваемых данных, а второе - для их передачи. При передаче проводится инкапсулирование информации в кадр пакетов данных, что является отличительным признаком передаваемых данных. Пакеты могут быть сжаты до шифрования. Запатентованная система может быть использована для защиты каналов связи в БАК.

В патенте Китая CN 105491564 от 13.04.2016 г. [10] предложен способ для установления защищенной связи в среде с несколькими БПЛА с использованием надежного протокола взаимодействия, позволяющего избежать ложных запросов и ответов. Данные шифруются с помощью закрытого ключа, что обеспечивает конфиденциальность сообщений.

Значительная часть патентов посвящена идентификации, аутентификации и авторизации объектов и субъектов доступа в системах, применяющих БПЛА.

Например, китайской фирмой SZ DJI Technology группой патентов защищены системы аутентификации и методы формирования правил полетов БПЛА, содержащие центр аутентификации и систему управления полетами, сконфигурированные для управления доступом к БПЛА на основе аутентификации БПЛА и соответствующего пользователя БПЛА по их идентификаторам (в частности, патенты США US 9412278 от 09.08.2016 г. [11], US 9805372 от 31.10.2017 г. [12], US 9805607 от 31.10.2017 г. [13], US 9870566 от

16.01.2018 г. [14]).

В международном патенте WO 2017042403 от 16.03.2017 г. [15] испанская фирма Tecteco Security Systems запатентовала способ и устройство для создания защищенных механизмов управления для воздушной навигации беспилотных транспортных средств, повышающие безопасность воздушной навигации БПЛА с помощью аутентификации, авторизации и механизмов защиты от текущих технических уязвимостей.

В патенте США US 9542850 от 10.01.2017 г. [16] предложены способ и устройство защищенной связи с БПЛА, обеспечивающие по запросу на перелет аутентификацию БПЛА. По результатам этой процедуры на основе информации о компонентах БПЛА определяется возможность перелета и рассчитывается траектория полета, передается инструкция по маршруту полета и дается разрешение на полет. В состав учетных данных БПЛА, на основе которых выполняется его аутентификация, входят, в частности, закрытый ключ шифрования, сертификат открытого ключа и идентификационный номер БПЛА.

Американской фирмой Microsoft Technology Licensing запатентована система авторизации для БПЛА, которая осуществляет контроль доступа к управлению БПЛА (патент США US 9651944 от 16.05.2017 г. [17]). Данная система содержит контроллер БПЛА, связанный по интерфейсу с блоком авторизации управления, содержащим процессор, интерфейс связи и память. Получая идентификационный код от контроллера БПЛА, который вводится оператором, средство авторизации проводит проверку его соответствия хранящемуся подписанному цифровому сертификату. Аналогичная процедура аутентификации проводится для любой принятой управляющей команды. Если цифровой сертификат недействителен, средство авторизации не разрешает оператору инициировать управляющие инструкции и не передает инструкцию управления БПЛА.

Помимо решений по обеспечению защиты каналов БПЛА с помощью криптографических алгоритмов, стоит обратить внимание и на ряд патентов, обеспечивающих защиту передаваемой информации без применения криптографии.

Например, в международном патенте WO 2005020445 от 10.11.2005 г. [18] для управления и контроля БПЛА предлагаются специальные микроволновые антенны для безопасной передачи данных, обеспечивающие надежную связь «точка-точка» в сетях беспроводной передачи данных на короткие расстояния, и транспондер с высокой направленностью сигнала и дополнительным сигналом глушения того же спектра, предотвращающие перехват передаваемых сообщений.

Представляет интерес также предложенный компанией Northrop Grumman Systems способ защиты сообщений между БПЛА и космическим аппаратом на частоте в диапазоне 50-70 ГГц по патенту США US 8594662 от 26.11.2013 г. [19], который включает в себя выбор частоты сигнала на основе высоты полета самолета и угла положения между космическим аппаратом и самолетом.

Кроме того, достаточно большое количество патентов посвящено методам и средствам распределения ключевой информации, которые могут быть использованы в БПЛА или аналогичных удаленно управляемых аппаратах.

Например, в патенте США US 5841864 от 24.11.1998 г. [20] компанией Motorola предложен метод, обеспечивающий одностороннюю аутентификацию устройства и обмен сессионными ключами на основе предварительно распределенного секрета для последующей защиты сообщений, передаваемых по каналу связи.

В патенте США US 6816970 от 09.11.2004 г. [21] корпорацией IBM предложен трехэтапный метод взаимной аутентификации и обмена сессионными симметричными

ключами на основе схемы с открытым распределением ключей, причем сессионные ключи могут быть использованы впоследствии как для защиты канала связи между субъектами аутентификации, так и для шифрования хранящихся на них данных.

Наиболее близкими к предлагаемым способу и системе криптографической защиты каналов связи БАК (прототипом) являются способ и система защищенного управления и мониторинга удаленно управляемых устройств, предложенные фирмой The Charles Stark Draper Laboratory (США) и описанные в патенте США US 9871772 от 16.01.2018 г. [22].

Система и способ, рассматриваемые в качестве прототипа, обеспечивают достаточно высокий уровень безопасности передачи данных для небольших аппаратов с ограниченными вычислительными ресурсами, которые управляются по беспроводному каналу связи. Частным случаем таких аппаратов являются БПЛА.

Основными компонентами описанной в патенте США US 9871772 системы являются следующие:

- удаленно управляемый аппарат (RCD - Remotely Controlled Device), аналогом которого является БПЛА;
- основной управляющий элемент (PCE - Primary Control Element), аналогом которого является НСУ;
- опциональный управляющий элемент - дополнительная станция управления, находящаяся впереди по предполагаемому курсу движения управляемого аппарата (FO - Forward Observer).

Описанный в патенте США US 9871772 способ заключается в выполнении следующей последовательности действий со стороны PCE:

1. PCE запрашивает и получает от RCD его параметры.
2. На основе полученных параметров PCE выбирает открытый ключ, ассоциированный с конкретным экземпляром RCD.
3. PCE генерирует основной (первый) ключевой набор, действующий в течение предстоящей миссии RCD и включающий мастер-ключ данного экземпляра RCD.
4. PCE зашифровывает сгенерированный ключевой набор с использованием открытого ключа RCD.
5. Зашифрованный ключевой набор передается на RCD по интерфейсу загрузки ключей.
6. PCE зашифровывает первую команду, предназначенную для RCD, на первом ключе шифрования, порожденном из мастер-ключа данного экземпляра RCD.
7. Первая команда и информация, необходимая для аутентификации PCE со стороны RCD (метка аутентификации), отправляется на RCD по беспроводному каналу связи.

Предполагается, что интерфейс загрузки ключей в RCD используется однократно (в рамках подготовки к выполнению конкретной миссии) и по определению является доверенным, т.е. представляет собой, например, проводной интерфейс, который задействуется только в доверенном окружении, тогда как дальнейшая отправка команд осуществляется по беспроводному интерфейсу, не являющемуся доверенным.

В свою очередь, RCD выполняет следующую последовательность действий, отвечающих на действия, инициированные со стороны PCE и описанные выше:

1. RCD получает зашифрованный ключевой набор от PCE.
2. RCD расшифровывает ключевой набор для получения из него своего мастер-ключа.
3. RCD получает первую зашифрованную команду от PCE по беспроводному каналу связи.
4. RCD аутентифицирует PCE на основе полученной метки аутентификации с

использованием предварительно загруженного ключа хэширования.

5. RCD расшифровывает первую полученную команду на первом ключе шифрования, порожденном из мастер-ключа.

В дальнейшем команды, передаваемые на RCD со стороны PCE, зашифровываются на текущем используемом ключе шифрования, который синхронно меняется на RCD и PCE через определенное количество команд (в т.ч. возможен вариант смены ключа после каждой команды) или через предопределенные интервалы времени.

Параметры RCD могут включать в себя как какой-либо идентификатор, однозначно определяющий конкретный экземпляр RCD, так и непосредственно открытый ключ RCD. Параметры могут быть нанесены на внешнюю поверхность RCD (например, в виде штрих-кода) и считываться оптическим способом или могут находиться в памяти радиочастотной метки ближнего поля (NFC - Near-Field Interface) и считываться с помощью соответствующего ридера.

При наличии одной или более дополнительных станций управления (FO) отправляемые управляющие команды на RCD со стороны FO зашифровываются с помощью дополнительного (второго) ключевого набора, содержащего дополнительный мастер-ключ, предназначенный для защиты обмена данными по беспроводному каналу связи между FO и конкретным экземпляром RCD. Механизмы порождения текущих ключей шифрования из данного мастер-ключа и их смены аналогичны таковым при взаимодействии PCE и RCD.

PCE и FO могут одновременно управлять несколькими экземплярами RCD, при этом описанные выше принципы взаимодействия компонентов системы не изменяются.

Патент США US 9871772 описывает также один из возможных вариантов реализации аппаратного модуля, обеспечивающего защиту каналов связи согласно предложенному способу (криптографического модуля). В описании патента отмечается, что криптографический модуль должен быть реализован в виде выделенного устройства, причем конкретная реализация алгоритмов, лежащих в основе запатентованного способа, может быть выполнена аппаратно (в виде специализированных микросхем) или программно (в виде программируемых логических интегральных схем или в виде программного обеспечения, выполняющегося на микропроцессорах (микроконтроллерах) общего назначения). Отметим также, что алгоритмы работы криптографического модуля несколько различаются в зависимости от его конкретного применения (на RCD, PCE или FO); тем не менее, все эти компоненты системы могут быть оснащены однотипными криптографическими модулями с возможностью их параметризации для обеспечения различных вариантов применения. Описанный в патенте США US 9871772 криптографический модуль является прототипом заявляемого устройства.

Помимо описанных выше основного (первого) и дополнительного (второго) ключевых наборов, способ допускает использование третьего ключевого набора для защиты данных, передаваемых по беспроводному каналу связи со стороны RCD на PCE, и четвертого ключевого набора для защиты данных, передаваемых по беспроводному каналу связи со стороны RCD на FO.

Отметим, что патент США US 9871772 описывает ряд вариаций способа защищенного управления и мониторинга удаленно управляемых устройств, различия между которыми заключаются в следующем:

- какие конкретно используются параметры для идентификации RCD, каким образом они хранятся и считываются;

- по какому принципу осуществляется смена текущих ключей шифрования;

- каким образом осуществляется хранение ключей шифрования на RCD;

- используются ли методы электронной подписи для защиты целостности загружаемых на RCD ключевых наборов;

- используются ли однотипные криптографические модули на всех компонентах системы;

- используется ли процедура безопасного установления соединения между PCE и FO;

- каким образом осуществляется управление ключевыми наборами и их использование при наличии нескольких FO в системе;

- допускается ли одновременное управление несколькими RCD со стороны PCE и FO;

- используются ли третий и четвертый ключевые наборы для защиты данных, передаваемых со стороны RDC по беспроводному каналу связи, соответственно, на PCE и FO.

Предлагаемый заявителями способ криптографической защиты каналов связи БАК имеет ряд преимуществ по сравнению со способом, описанном в прототипе, которые сводятся к следующим:

1. Упрощенный по сравнению с прототипом протокол распределения ключевой информации, не ухудшающий качества защиты. Кроме того, предложенный протокол распределения ключевой информации обеспечивает защиту от атак класса «человек посередине» (man-in-the middle, MITM), тогда как в описании прототипа явным образом сказано, что используемые схемы распределения ключей не обеспечивают защиту от атак данного класса.

2. Выполнение во всех случаях только взаимной аутентификации БПЛА и НСУ, тогда как в прототипе не предусмотрена аутентификация FO со стороны RCD, что может привести к потенциальному перехвату управления RCD путем внедрения в систему ложных FO.

3. Помимо криптографической защиты, в заявляемом способе предусмотрен также дополнительный фактор защиты, основанный на псевдослучайной перенастройке параметров радиосвязи между БПЛА и НСУ.

4. Заявляемый способ предполагает, помимо каналов управления и телеметрии, шифрование также информации полезной нагрузки БПЛА, передаваемой на НСУ, тогда как в прототипе шифрование канала управления является обязательным, шифрование канала телеметрии - опциональным, а из всего спектра вариантов информации полезной нагрузки БПЛА допускается только шифрование видеосигнала, причем только в том случае, если он используется для удаленного управления RCD со стороны PCE или FO и только в необходимых для такого управления объемах.

5. Заявляемый способ предполагает возможность реализации предусмотренных им алгоритмов и протоколов криптографической защиты каналов связи БАК не только в выделенном аппаратном криптографическом модуле, но и в виде программных модулей, выполняющихся непосредственно на полетном контроллере БПЛА или на вычислительных ресурсах существующего оборудования НСУ. Отсутствие необходимости установки аппаратного криптографического модуля на БПЛА, с одной стороны, не требует внесения конструктивных изменений в БПЛА и, с другой стороны, в значительно меньшей степени (только за счет дополнительного энергопотребления) ухудшает основные эксплуатационные характеристики БПЛА, т.е. максимальный вес полезной нагрузки БПЛА и/или максимальную длительность/дальность полета.

6. Заявляемый способ повышает качество защиты каналов связи БАК по сравнению с прототипом, поскольку он подразумевает шифрование сообщений целиком, тогда

как в описанной структуре сообщений прототипа существуют нешифруемые служебные поля (поля «bypass»), через которые теоретически возможна утечка информации.

7. Заявляемый способ также предполагает, что аппаратная или программная реализация криптографических преобразований оснащена дополнительными модулями, обеспечивающими контроль работоспособности модулей, выполняющих криптографические преобразования, а также их самотестирование - при старте и периодическое в процессе работы.

Предлагаемая заявителями система криптографической защиты каналов связи БАК реализует предлагаемый способ и, помимо описанных выше преимуществ способа криптографической защиты каналов связи БАК, обладает также следующими преимуществами по сравнению с системой, описанной в прототипе:

1. В отличие от прототипа, в котором жестко зафиксирована структура сообщений между компонентами системы и система команд, заявляемая система не накладывает ограничений на используемую систему команд. Это делает заявляемую систему значительно более гибкой и универсальной, поскольку система может быть построена на значительно более широком спектре оборудования, применяемого в БПЛА и НСУ, тогда как система, описанная в прототипе, может быть реализована только на оборудовании, реализующем описанные структуру сообщений и систему команд, т.е. на оборудовании, изначально разработанном с целью использования в такой системе.

2. Возможность реализации криптографического модуля в виде программных модулей, выполняющихся непосредственно на полетном контроллере БПЛА, позволяет, с одной стороны, удешевить систему в целом по сравнению с прототипом и, с другой стороны, реализовать систему с использованием более широкого спектра существующего оборудования как БПЛА, так и НСУ, поскольку не требует внесения конструктивных изменений в аппаратную часть существующих БПЛА/НСУ для обеспечения подключения аппаратного криптографического модуля, предусмотренного прототипом.

Заявляемое устройство представляет собой один из вариантов реализации заявляемого способа криптографической защиты каналов связи БАК.

Технический результат достигается следующим образом:

1. Способ криптографической защиты каналов связи между НСУ и БПЛА состоит в выполнении следующей последовательности действий:

Шаг 1) С помощью ключевого носителя НСУ, оснащенного вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями, генерируется пара асимметричных ключей НСУ: секретный и открытый ключи НСУ.

Шаг 2) С помощью ключевого носителя БПЛА, оснащенного вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями, генерируется пара асимметричных ключей БПЛА: секретный и открытый ключи БПЛА.

Шаг 3) Осуществляется копирование открытых ключей НСУ и БПЛА на, соответственно, ключевой носитель БПЛА и ключевой носитель НСУ, после которого ключевой носитель НСУ содержит секретный и открытый ключи НСУ и открытый ключ БПЛА, а ключевой носитель БПЛА содержит секретный и открытый ключи БПЛА и открытый ключ НСУ.

Шаг 4) Криптографический модуль БПЛА, оснащенный программной или аппаратной реализацией криптографических алгоритмов, возможностью инициирования передачи сообщений на НСУ и опциональной возможностью блокирования порта подключения полетного контроллера БПЛА к каналам связи, инициирует генерацию ключевым носителем БПЛА общего секретного пре-мастер-ключа (предназначенного для дальнейшей генерации на его основе мастер-ключа) на основе секретного ключа

БПЛА и открытого ключа НСУ.

Шаг 5) Криптографический модуль БПЛА считывает с ключевого носителя БПЛА открытый ключ БПЛА, открытый ключ НСУ и общий секретный пре-мастер-ключ.

Шаг 6) Криптографический модуль НСУ, оснащенный программной или аппаратной реализацией криптографических алгоритмов, возможностью инициирования передачи сообщений на БПЛА и опциональной возможностью блокирования интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА, инициирует генерацию ключевым носителем НСУ общего секретного пре-мастер-ключа на основе секретного ключа НСУ и открытого ключа БПЛА.

Шаг 7) Криптографический модуль НСУ считывает с ключевого носителя НСУ открытый ключ НСУ, открытый ключ БПЛА и общий секретный пре-мастер-ключ.

Шаг 8) Криптографический модуль БПЛА проверяет состояние своей готовности к работе.

Шаг 9) Криптографический модуль БПЛА инициирует отправку сообщения криптографическому модулю НСУ, содержащего открытый ключ БПЛА и случайное число БПЛА.

Шаг 10) Криптографический модуль НСУ, находящийся в режиме ожидания сообщений из канала связи, получает данное сообщение от БПЛА и проверяет, есть ли у него полученный открытый ключ БПЛА. Если такого открытого ключа у криптографического модуля НСУ нет, то криптографический модуль НСУ игнорирует полученное сообщение и возвращается в режим ожидания сообщений.

Шаг 11) Криптографический модуль НСУ инициирует отправку ответного сообщения криптографическому модулю БПЛА, содержащего открытый ключ НСУ и случайное число НСУ.

Шаг 12) Криптографический модуль БПЛА получает ответное сообщение от криптографического модуля НСУ и проверяет, есть ли у него полученный открытый ключ НСУ. Если такого открытого ключа у криптографического модуля НСУ нет, то криптографический модуль БПЛА игнорирует данное сообщение и возвращается к шагу 9.

Шаг 13) Криптографический модуль БПЛА вырабатывает мастер-ключ (предназначенный для дальнейшей генерации на его основе сеансовых криптографических ключей) на основе пре-мастер-ключа, случайного числа БПЛА и случайного числа НСУ.

Шаг 14) Криптографический модуль НСУ вырабатывает мастер-ключ на основе пре-мастер-ключа, случайного числа БПЛА и случайного числа НСУ.

Шаг 15) Криптографический модуль БПЛА на основе мастер-ключа вырабатывает сеансовый ключ шифрования и сеансовый ключ вычисления имитовставки.

Шаг 16) Криптографический модуль НСУ на основе мастер-ключа вырабатывает сеансовый ключ шифрования и сеансовый ключ вычисления имитовставки.

Шаг 17) Криптографический модуль БПЛА формирует тестовое сообщение, зашифрованное на выработанном сеансовом ключе шифрования, и инициирует его отправку криптографическому модулю НСУ.

Шаг 18) Криптографический модуль НСУ получает и расшифровывает тестовое сообщение от криптографического модуля БПЛА и проверяет его соответствие ожидаемому тестовому сообщению. Если тестовое сообщение не соответствует ожидаемому, то криптографический модуль НСУ считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается в режим ожидания сообщений.

Шаг 19) Криптографический модуль НСУ формирует ответное тестовое сообщение, зашифрованное на выработанном сеансовом ключе шифрования, и инициирует его отправку криптографическому модулю БПЛА.

Шаг 20) Криптографический модуль БПЛА получает и расшифровывает тестовое сообщение от криптографического модуля НСУ и проверяет его соответствие ожидаемому тестовому сообщению. Если тестовое сообщение не соответствует ожидаемому, то криптографический модуль БПЛА считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается к шагу 9.

Шаг 21) Криптографический модуль БПЛА выставляет флаг готовности к работе.

Шаг 22) Криптографический модуль НСУ выставляет флаг готовности к работе.

Шаг 23) Криптографический модуль БПЛА открывает порт подключения полетного контроллера.

Шаг 24) Криптографический модуль НСУ открывает интерфейс обмена с программным обеспечением, осуществляющим управление БПЛА.

Шаг 25) Дальнейший обмен информацией по каналам управления и телеметрии между НСУ и БПЛА ведется в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

Заявляемый способ распространяется также на различные вариации описанной выше последовательности действий, заключающиеся, в том числе, в следующем:

- используется ли псевдослучайная перенастройка параметров радиосвязи между БПЛА и НСУ;
- подразумевается ли способом оснащение криптографических модулей возможностями контроля работоспособности и самотестирования;
- возможно ли применение криптографических модулей для шифрования данных полезной нагрузки, передаваемых с БПЛА на НСУ;
- возможно ли одновременное управление нескольких БПЛА с одной НСУ и др.

2. Система криптографической защиты каналов связи между НСУ и БПЛА включает в себя следующие компоненты:

Компонент 1) Криптографический модуль НСУ, реализующий заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части НСУ, реализованный аппаратно или программно на выделенном аппаратном устройстве, оснащенном вычислительными ресурсами, интерфейсом подключения ключевого носителя НСУ и программной или аппаратной реализацией криптографических алгоритмов, функций генерации случайных или псевдослучайных чисел и функций взаимодействия с ключевым носителем НСУ, а также возможностью инициирования передачи сообщений на БПЛА и опциональной возможностью блокирования интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА, при этом выделенное аппаратное устройство подключается в разрыв между основным вычислительным модулем НСУ и приемо-передающим устройством НСУ.

Компонент 2) Криптографический модуль БПЛА, реализующий заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, реализованный аппаратно или программно на выделенном аппаратном устройстве, оснащенном вычислительными ресурсами, возможностью подключения ключевого носителя БПЛА и программной или аппаратной реализацией криптографических алгоритмов, функций генерации случайных или псевдослучайных чисел и функций взаимодействия с ключевым носителем БПЛА, а также возможностью инициирования передачи сообщений на НСУ и опциональной возможностью блокирования порта

подключения полетного контроллера БПЛА к каналам связи, при этом выделенное аппаратное устройство подключается в разрыв между полетным контроллером БПЛА и приемо-передающим устройством БПЛА.

Компонент 3) Ключевой носитель НСУ, оснащенный вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями.

Компонент 4) Ключевой носитель БПЛА, оснащенный вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями.

Криптографический модуль НСУ может быть реализован программно и выполняться непосредственно на основном вычислительном модуле НСУ, который в этом случае должен быть оснащен интерфейсом подключения ключевого носителя НСУ.

Криптографический модуль БПЛА также может быть реализован программно и выполняться непосредственно на полетном контроллере БПЛА; в этом случае БПЛА должен быть оснащен интерфейсом подключения ключевого носителя БПЛА.

Заявляемая система распространяется также на вариант с обеспечением криптографической защиты каналов связи между НСУ и БПЛА при одновременном управлении несколькими БПЛА с одной НСУ независимо от конкретного из перечисленных выше вариантов реализации криптографического модуля НСУ и криптографического модуля БПЛА.

В состав заявляемой системы может также входить ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

3. Устройство криптографической защиты каналов связи между НСУ и БПЛА выполнено на общей плате и содержит следующие элементы:

Элемент 1) Управляющий микроконтроллер, включающий в свой состав следующие программные функциональные модули, выполняющиеся на управляющем микроконтроллере:

- модуль управления, осуществляющий управление остальными программными модулями и элементами устройства;
- модуль обеспечения конфиденциальности и целостности информационного обмена;
- модуль аутентификации;
- модуль генерации и обработки ключевой информации;
- модуль генерации случайных или псевдослучайных чисел;
- модуль взаимодействия с ключевым носителем;
- модуль взаимодействия с приемо-передающим устройством.

Элемент 2) Энергонезависимая память для хранения перечисленных выше программных модулей.

Элемент 3) Интерфейс подключения к внешнему вычислительному устройству.

Элемент 4) Интерфейс взаимодействия с ключевым носителем.

Элемент 5) Интерфейс взаимодействия с приемо-передающим устройством.

Помимо перечисленных выше, в состав управляющего микроконтроллера могут быть включены следующие выполняющиеся на нем программные модули:

- модуль самотестирования устройства;
- модуль контроля целостности программного обеспечения устройства.

В результате проведенного заявителем анализа уровня техники, включая поиск по патентным и научно-техническим источникам информации и выявление источников, содержащих сведения об аналогах заявленного технического решения, не было обнаружено источника, характеризующегося признаками, тождественными всем существенным признакам заявленного технического решения, изложенным в формуле

изобретения.

Определение из перечня выявленных аналогов прототипа, как наиболее близкого по совокупности признаков аналога, позволило установить совокупность приведенных выше существенных по отношению к усматриваемому заявителем техническому результату отличительных признаков заявленных способа, системы и устройства криптографической защиты каналов связи беспилотных авиационных комплексов. Проведенный заявителем дополнительный поиск не выявил известные решения, содержащие признаки, совпадающие с отличительными от прототипа признаками заявленной системы. Следовательно, заявленное техническое решение соответствует критерию «новизна».

Заявленное техническое решение не вытекает для специалиста явным образом из известного уровня техники и не основано на изменении количественных признаков. Следовательно, заявленное техническое решение соответствует критерию «изобретательский уровень».

Графические изображения:

На фиг. 1 и фиг. 2 приведены упрощенные схемы основного алгоритма описанного выше основного варианта способа криптографической защиты каналов связи между НСУ и БПЛА, где:

- на фиг. 1 приведена схема предварительного этапа основного алгоритма;
- на фиг. 2 приведена схема этапа штатной работы основного алгоритма. Нумерация блоков на фиг. 1 и фиг. 2 соответствует номерам шагов основного алгоритма:

1 - шаг генерации пары ключей НСУ;
2 - шаг генерации пары ключей БПЛА;
3 - шаг обмена открытыми ключами;
4 - шаг генерации пре-мастер-ключа на стороне БПЛА;
5 - шаг считывания ключей с ключевого носителя БПЛА;
6 - шаг генерации пре-мастер-ключа на стороне НСУ;
7 - шаг считывания ключей с ключевого носителя НСУ;
8 - шаг проверки готовности БПЛА;
9 - шаг отправки открытого ключа и случайного числа БПЛА;
10 - шаг проверки открытого ключа БПЛА;
11 - шаг отправки открытого ключа и случайного числа НСУ;
12 - шаг проверки открытого ключа НСУ;
13 - шаг выработки мастер-ключа на стороне БПЛА;
14 - шаг выработки мастер-ключа на стороне НСУ;
15 - шаг выработки сеансовых ключей на стороне БПЛА;
16 - шаг выработки сеансовых ключей на стороне НСУ;
17 - шаг отправки тестового сообщения;
18 - шаг проверки тестового сообщения;
19 - шаг отправки ответного тестового сообщения;
20 - шаг проверки ответного тестового сообщения;
21 - шаг установки флага готовности БПЛА к работе;
22 - шаг установки флага готовности НСУ к работе;
23 - шаг открытия порта подключения полетного контроллера;
24 - шаг открытия интерфейса обмена с программами управления БПЛА;
25 - шаг обмена информацией в защищенном режиме.

На фиг. 3 приведена схема системы криптографической защиты каналов связи между НСУ и БПЛА, где:

101 - комплекс бортового оборудования БПЛА;
102 - оборудование НСУ;
103 - канал связи между БПЛА и НСУ;
104 - ключевой центр системы.

Компоненты комплекса бортового оборудования БПЛА 101:
111 - полетный контроллер;
112 - ключевой носитель БПЛА;
113 - криптографический модуль БПЛА;
114 - приемо-передающее устройство БПЛА. Компоненты оборудования НСУ 102:
121 - основной вычислительный модуль НСУ;
122 - программное обеспечение управления БПЛА;
123 - криптографический модуль НСУ;
124 - ключевой носитель НСУ;
125 - приемо-передающее устройство НСУ.

На фиг 4 представлена структурная схема устройства криптографической защиты каналов связи между НСУ и БПЛА, где: 201 - общая плата устройства;
211 - управляющий микроконтроллер;
212 - энергонезависимая память;
213 - интерфейс подключения к внешнему вычислительному устройству;
214 - интерфейс взаимодействия с ключевым носителем;
215 - интерфейс взаимодействия с приемо-передающим устройством. Программные функциональные модули, выполняющиеся на управляющем микроконтроллере 211:
221 - модуль управления;
222 - модуль обеспечения конфиденциальности и целостности информационного обмена;
223 - модуль аутентификации и установления защищенного соединения;
224 - модуль генерации и обработки ключевой информации;
225 - модуль генерации случайных или псевдослучайных чисел;
226 - модуль взаимодействия с ключевым носителем;
227 - модуль взаимодействия с приемо-передающим устройством;
228 - модуль самотестирования устройства;
229 - модуль контроля целостности программного обеспечения устройства.

В соответствии с фиг. 1 и фиг. 2 способ криптографической защиты каналов связи между НСУ и БПЛА состоит в выполнении описанной далее последовательности шагов.

На предварительном этапе осуществляется генерация асимметричных ключей и обмен открытыми ключами БПЛА и НСУ. На данном этапе основные действия выполняются ключевыми носителями БПЛА и НСУ. При этом данные действия инициируются внешними по отношению к ключевым носителям устройствами, например, криптографическими модулями БПЛА и НСУ.

Для выполнения предусмотренных способом операций ключевые носители должны представлять собой устройства, оснащенные, как минимум:
- вычислительными возможностями;
- операционной системой и/или управляющим микропрограммным обеспечением;
- оперативной и энергонезависимой памятью;
- криптографическими функциями.

В качестве ключевых носителей могут быть использованы смарт-карты с контактным или бесконтактным интерфейсом, соответствующие семействам стандартов ГОСТ Р ИСО/МЭК 7816 [23] и/или ГОСТ Р ИСО/МЭК 14443 [24]. В качестве примера подобных

смарт-карт можно привести смарт-карту на основе отечественной микросхемы MIK51SC72D производства ПАО «Микрон».

В качестве альтернативного варианта ключевого носителя могут быть использованы криптографические токены, подключаемые к порту USB и имеющие систему команд, аналогичную описанной в стандарте ГОСТ Р ИСО/МЭК 7816-4-2013 [25]. В качестве примера подобных токенов можно привести устройство «Рутокен» производства ЗАО «Актив-софт».

Более подробно варианты исполнения, возможности ключевых носителей и требования к ним будут описаны далее - в части описания заявляемой системы криптографической защиты каналов связи между НСУ и БПЛА.

Внешнее устройство, взаимодействующее с ключевыми носителями, должно иметь аппаратный и программный интерфейс подключения ключевого носителя. Например, при использовании смарт-карт в качестве ключевых носителей, внешнее устройство должно быть оснащено считывателем смарт-карт и соответствующим программным модулем, обеспечивающим взаимодействие со считывателем и смарт-картой.

Шаг 1) С помощью ключевого носителя НСУ генерируется пара асимметричных ключей НСУ: секретный и открытый ключи НСУ.

Для генерации пары ключей при использовании в качестве ключевых носителей смарт-карт или криптографических токенов может быть использована команда GENERATE ASYMMETRIC KEY PAIR стандарта ГОСТ Р ИСО/МЭК 7816-4-2013 [25]. Данная команда позволяет также получить с ключевого носителя значение сгенерированного открытого ключа, которое может использоваться на шаге 3, на котором выполняется обмен ключами.

При использовании приведенных в качестве примеров смарт-карты на основе отечественной микросхемы MIK51SC72D или устройства «Рутокен» генерируется пара ключей, соответствующих стандарту ГОСТ Р 34.10-2001 [26] и/или ГОСТ Р 34.10-2012 [27].

Шаг 2) С помощью ключевого носителя БПЛА генерируется пара асимметричных ключей БПЛА: секретный и открытый ключи БПЛА.

Шаг 3) Осуществляется копирование открытых ключей НСУ и БПЛА на, соответственно, ключевой носитель БПЛА и ключевой носитель НСУ, после которого ключевой носитель НСУ содержит секретный и открытый ключи НСУ и открытый ключ БПЛА, а ключевой носитель БПЛА содержит секретный и открытый ключи БПЛА и открытый ключ НСУ.

В результате ключевой носитель БПЛА должен содержать следующий комплект ключей:

- секретный ключ БПЛА;
- открытый ключ БПЛА;
- открытый ключ НСУ.

Ключевой носитель НСУ должен содержать следующий комплект ключей:

- секретный ключ НСУ;
- открытый ключ НСУ;
- открытый ключ БПЛА.

Поскольку некоторые варианты заявляемого способа подразумевают возможность одновременного управления несколькими БПЛА с одной НСУ, ключевой носитель НСУ в этом случае должен содержать открытые ключи всех БПЛА, управляемых с данной НСУ, т.е. в этом случае ключевой носитель НСУ должен содержать следующий комплект ключей:

- секретный ключ НСУ;
- открытый ключ НСУ;
- открытый ключ БПЛА №1;
-…
- открытый ключ БПЛА № N.

Альтернативным вариантом является применение на стороне НСУ отдельных ключевых носителей для взаимодействия с каждым из управляемых БПЛА. В этом случае n-й ключевой носитель из ключевых носителей НСУ содержит следующий комплект ключей:

- секретный ключ НСУ;
- открытый ключ НСУ;
- открытый ключ БПЛА № n.

Описанные выше варианты распределения открытых ключей БПЛА по ключевых носителям НСУ могут быть скомбинированы.

Хранение ключей, их идентификация и сопоставление с конкретным БПЛА может осуществляться различным образом. Например, каждый открытый ключ может храниться в отдельном ключевом файле в файловой системе смарт-карты, при этом имя файла представляет собой номер, соответствующий номеру конкретного БПЛА.

Таким образом, после выполнения шага 3 завершается формирование комплектов ключей на ключевых носителях БПЛА и НСУ.

Дальнейшие шаги относятся к этапу штатной работы основного алгоритма, реализующего заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА. Они выполняются после формирования комплектов ключей на ключевых носителях БПЛА и НСУ, произведенного на предварительном этапе, и осуществляются криптографическими модулями БПЛА и НСУ. Основным результатом данного этапа является установление защищенного обмена между БПЛА и НСУ.

Криптографические модули предназначены для реализации преобразований в рамках выполнения алгоритмов, предусмотренных заявляемым способом, для чего каждый криптографический модуль должен включать в себя аппаратную или программную реализацию всех необходимых для этого функций и алгоритмов. Более подробно варианты исполнения, возможности криптографических модулей и требования к ним будут описаны далее - в части описания заявляемой системы криптографической защиты каналов связи между НСУ и БПЛА.

Криптографические модули могут быть оснащены различными механизмами самотестирования и контроля работоспособности, включая, например, следующие:

- контроль целостности загружаемых и исполняемых программных модулей;
- выполнение тестовых задач (в части выполнения криптографических алгоритмов);
- контроль качества вырабатываемых случайных чисел и др.

В этом случае криптографический модуль БПЛА должен перед выполнением шага 4 выполнить процедуру самотестирования и прервать работу алгоритма с генерацией соответствующего кода/сообщения об ошибке в случае, если самотестирование показало наличие ошибочной ситуации.

Аналогичное самотестирование с аналогичными последствиями в случае обнаружения ошибочной ситуации должен выполнить криптографический модуль НСУ перед выполнением шага 6.

В дальнейшем самотестирование криптографическим модулем БПЛА и НСУ может выполняться периодически по мере выполнения защищенного обмена информацией между БПЛА и НСУ.

Шаг 4) Криптографический модуль БПЛА инициирует генерацию ключевым носителем БПЛА общего секретного пре-мастер-ключа (предназначенного для дальнейшей генерации на его основе мастер-ключа) на основе секретного ключа БПЛА и открытого ключа НСУ.

Генерация общего секретного пре-мастер-ключа на основе секретного ключа БПЛА и открытого ключа НСУ может быть выполнена различными способами. В частности, для этого может быть использован алгоритм Диффи-Хеллмана на эллиптических кривых (см., например, [28]) или алгоритм VKO_GOSTR3410_2012 [29].

Для генерации общего секретного пре-мастер-ключа при использовании в качестве ключевых носителей смарт-карт или криптографических токенов может быть использована команда GENERAL AUTHENTICATE стандарта ГОСТ Р ИСО/МЭК 7816-4-2013 [25].

Шаг 5) Криптографический модуль БПЛА считывает с ключевого носителя БПЛА открытый ключ БПЛА, открытый ключ НСУ и общий секретный пре-мастер-ключ.

Как было сказано выше, открытые ключи как БПЛА, так и НСУ могут храниться в файлах файловой системы ключевого носителя. В этом случае их считывание может быть осуществлено файловыми функциями ключевого носителя (см., например, [25]).

При использовании смарт-карт или криптографических токенов в качестве ключевого носителя общий секретный пре-мастер-ключ может быть получен от ключевого носителя как результат выполнения команды GENERAL AUTHENTICATE стандарта ГОСТ Р ИСО/МЭК 7816-4-2013 [25].

Поскольку после выполнения данного шага дальнейшее использование ключевого носителя БПЛА заявляемым способом не предусмотрено, ключевой носитель БПЛА может быть отсоединен от криптографического модуля. Кроме того, с целью минимизации веса оборудования (и, соответственно, минимизации ухудшения перечисленных выше основных эксплуатационных характеристик БПЛА), используемого для реализации заявляемого способа, аппаратная часть интерфейса подключения ключевого носителя БПЛА может быть отсоединена от криптографического модуля БПЛА. Например, при использовании в качестве ключевых носителей смарт-карт от криптографического модуля может быть отсоединен считыватель смарт-карт, который может обладать заметным весом.

Шаг 6) Криптографический модуль НСУ, оснащенный программной или аппаратной реализацией криптографических алгоритмов, возможностью инициирования передачи сообщений на БПЛА и опциональной возможностью блокирования интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА, инициирует генерацию ключевым носителем НСУ общего секретного пре-мастер-ключа на основе секретного ключа НСУ и открытого ключа БПЛА.

Шаг 7) Криптографический модуль НСУ считывает с ключевого носителя НСУ открытый ключ НСУ, открытый ключ БПЛА и общий секретный пре-мастер-ключ.

Поскольку после выполнения данного шага дальнейшее использование ключевого носителя НСУ заявляемым способом не предусмотрено, при необходимости ключевой носитель НСУ может быть отсоединен от криптографического модуля НСУ.

Шаг 8) Криптографический модуль БПЛА проверяет состояние своей готовности к работе.

Шаг 8 является опциональным и выполняется в случае, если криптографический модуль БПЛА оснащен механизмами самотестирования и контроля работоспособности.

Шаг 9) Криптографический модуль БПЛА инициирует отправку сообщения криптографическому модулю НСУ, содержащего открытый ключ БПЛА и случайное

число БПЛА.

Заявляемый способ предполагает, что инициатором описываемого процесса установления защищенной связи между БПЛА и НСУ является БПЛА, тогда как НСУ находится в режиме ожидания и вступает в активную фазу процесса, включающую совокупность дальнейших шагов алгоритма, после получения от БПЛА сообщения, предусмотренного шагом 9. При этом описанные выше шаги этапа штатной работы алгоритма, относящиеся к НСУ, могут быть выполнены на НСУ заранее: например, автоматически после включения НСУ или подключения ключевого носителя НСУ, по команде оператора НСУ и т.п. После этого НСУ переходит в режим ожидания.

В случае, когда одна НСУ используется для управления несколькими БПЛА одновременно, она должна иметь возможность параллельно для всех или части БПЛА выполнять дальнейшие шаги алгоритма по мере получения от любого из БПЛА сообщения, предусмотренного шагом 9.

В отличие от НСУ, БПЛА является инициатором активной фазы процесса установления защищенной связи между БПЛА и НСУ, поэтому режим ожидания в БПЛА не предусмотрен: этап штатной работы алгоритма может быть запущен на БПЛА автоматически при его включении или при подключении ключевого носителя БПЛА, с помощью специальной команды оператора и т.п.

Шаг 10) Криптографический модуль НСУ, находящийся в режиме ожидания сообщений из канала связи, получает данное сообщение от БПЛА и проверяет, есть ли у него полученный открытый ключ БПЛА. Если такого открытого ключа у криптографического модуля НСУ нет, то криптографический модуль НСУ игнорирует полученное сообщение и возвращается в режим ожидания сообщений.

Шаг 11) Криптографический модуль НСУ инициирует отправку ответного сообщения криптографическому модулю БПЛА, содержащего открытый ключ НСУ и случайное число НСУ.

Шаг 12) Криптографический модуль БПЛА получает ответное сообщения от криптографического модуля НСУ и проверяет, есть ли у него полученный открытый ключ НСУ. Если такого открытого ключа у криптографического модуля НСУ нет, то криптографический модуль БПЛА игнорирует данное сообщение и возвращается к шагу 9.

Таким образом, если этап установления защищенного соединения, заключающийся в выполнении шагов 9-12, прошел неуспешно, криптографический модуль БПЛА инициирует повторную попытку установления защищенного соединения.

Шаг 13) Криптографический модуль БПЛА вырабатывает мастер-ключ (предназначенный для дальнейшей генерации на его основе сеансовых криптографических ключей) на основе пре-мастер-ключа, случайного числа БПЛА и случайного числа НСУ.

Генерация мастер-ключа на основе пре-мастер-ключа может быть выполнена различными способами. В частности, для этого может быть использован напрямую алгоритм хэширования (например, ГОСТ Р 34.11-2012 [30]) или алгоритм вычисления кода аутентификации сообщений на основе алгоритмов хэширования (например, HMAC_GOSTR3411_2012_256 [29]).

Отметим, что пре-мастер-ключ является долговременным, поскольку он основан на долговременных ключах НСУ и БПЛА, тогда как мастер-ключ является сеансовым, поскольку в его генерации участвуют случайные числа БПЛА и НСУ, вырабатываемые, соответственно, на шагах 9 и 11 описанного алгоритма.

Шаг 14) Криптографический модуль НСУ вырабатывает мастер-ключ на основе

пре-мастер-ключа, случайного числа БПЛА и случайного числа НСУ.

Шаг 15) Криптографический модуль БПЛА на основе мастер-ключа вырабатывает сеансовый ключ шифрования и сеансовый ключ вычисления имитовставки.

Генерация сеансовых ключей на основе мастер-ключа также может быть выполнена различными способами. В частности, для этого может быть использован любой из алгоритмов шифрования, описанных в стандарте ГОСТ Р 34.12-2015 [31] в режиме выработки имитовставки, описанном в ГОСТ Р 34.13-2015 [32], или функция диверсификации ключей KDF_GOSTR3411_2012_256 [29].

Шаг 16) Криптографический модуль НСУ на основе мастер-ключа вырабатывает сеансовый ключ шифрования и сеансовый ключ вычисления имитовставки.

Шаг 17) Криптографический модуль БПЛА формирует тестовое сообщение, зашифрованное на выработанном сеансовом ключе шифрования, и инициирует его отправку криптографическому модулю НСУ.

Для шифрования тестового сообщение (подразумевается небольшой размер тестового сообщения) может быть применен любой режим шифрования, в частности, из описанных в стандарте ГОСТ Р 34.13-2015 [32].

При этом заявляемый способ не ограничивает набор возможных применяемых алгоритмов и режимов шифрования, а также алгоритмов хэширования, контроля целостности, генерации ключевых пар, вычисления общего ключа, диферсификации ключей и т.п., а также параметров всех перечисленных алгоритмов, алгоритмами, режимами и параметрами из какого-либо подмножества. Однако для упрощения реализации криптографического модуля не рекомендуется использование в криптографическом модуле нескольких различных криптографических алгоритмов для каждой из их категорий (алгоритмов шифрования, хэширования и т.д.).

Шаг 18) Криптографический модуль НСУ получает и расшифровывает тестовое сообщение от криптографического модуля БПЛА и проверяет его соответствие ожидаемому тестовому сообщению. Если тестовое сообщение не соответствует ожидаемому, то криптографический модуль НСУ считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается в режим ожидания сообщений.

Для упрощения реализации на шаге 17 может быть использовано константное сообщение; в этом случае контроль корректности тестового сообщения после его расшифрования сводится к бинарному или строковому сравнению полученного и ожидаемого сообщений.

В шифруемое тестовое сообщение может быть также включено значение сеансового ключа вычисления имитовставки, что позволит проконтролировать эквивалентность значений данного ключа на стороне БПЛА и на стороне НСУ. В качестве альтернативного варианта может быть рассмотрен вариант, когда на шаге 17 криптографический модуль БПЛА формирует также имитовставку тестового сообщения, вычисленную на выработанном сеансовом ключе вычисления имитовставки, и инициирует ее отправку криптографическому модулю НСУ вместе с зашифрованным тестовым сообщением. В этом случае на шаге 18 криптографический модуль НСУ получает и расшифровывает тестовое сообщение от криптографического модуля БПЛА, вычисляет на выработанном сеансовом ключе вычисления имитовставки и проверяет его имитовставку. Если имитовставка тестового сообщения неверна, то криптографический модуль НСУ считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается в режим ожидания сообщений.

Данные замечания применимы также к описанным далее шагам 19 и 20 алгоритма.

Шаг 19) Криптографический модуль НСУ формирует ответное тестовое сообщение, зашифрованное на выработанном сеансовом ключе шифрования, и инициирует его отправку криптографическому модулю БПЛА.

Временной интервал между отправкой тестового сообщения с БПЛА на НСУ (шаг 17) и получением ответного тестового сообщения (шаги 19-20) может контролироваться с помощью специального таймера, который может быть установлен на стороне БПЛА после выполнения шага 17. В этом случае, если ответное тестовое сообщение, предусмотренное шагом 19, было получено БПЛА с превышением предопределенного интервала времени, такое ответное тестовое сообщение игнорируется на стороне БПЛА, а шаги 17-19 выполняются повторно.

Шаг 20) Криптографический модуль БПЛА получает и расшифровывает тестовое сообщение от криптографического модуля НСУ и проверяет его соответствие ожидаемому тестовому сообщению. Если тестовое сообщение не соответствует ожидаемому, то криптографический модуль БПЛА считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается к шагу 9.

Таким образом, если этап установления защищенного соединения, заключающийся в выполнении шагов 9-20, прошел неуспешно, крипографический модуль БПЛА инициирует повторную попытку установления защищенного соединения.

Шаг 21) Криптографический модуль БПЛА выставляет флаг готовности к работе.

Шаг 22) Криптографический модуль НСУ выставляет флаг готовности к работе.

В случае, если с одной НСУ осуществляется управление несколькими БПЛА одновременно, флаг готовности НСУ к работе может выставляться по отношению к конкретному БПЛА, т.е. количество флагов готовности НСУ в этом случае несколько - по числу управляемых БПЛА, причем каждый флаг относится к установлению защищенного соединения НСУ с конкретным БПЛА.

Шаг 23) Криптографический модуль БПЛА открывает порт подключения полетного контроллера.

Данный шаг является опциональным и выполняется только в том случае, если криптографический модуль БПЛА имеет возможность программной или аппаратной блокировки порта подключения полетного контроллера. В этом случае заявляемый способ предполагает, что перед выполнением этапа штатной работы основного алгоритма криптографический модуль БПЛА блокирует порт подключения полетного контроллера.

Шаг 24) Криптографический модуль НСУ открывает интерфейс обмена с программным обеспечением, осуществляющим управление БПЛА.

Данный шаг является опциональным и выполняется только в том случае, если криптографический модуль НСУ имеет возможность программной или аппаратной блокировки интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА. В этом случае заявляемый способ предполагает, что перед выполнением этапа штатной работы основного алгоритма криптографический модуль НСУ блокирует данный интерфейс.

В случае, если с одной НСУ осуществляется управление несколькими БПЛА одновременно и криптографический модуль НСУ имеет возможность программной или аппаратной блокировки интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА, данный интерфейс открывается после первого успешного установления защищенного обмена информацией с любым из управляемых БПЛА.

Шаг 25) Дальнейший обмен информацией по каналам управления и телеметрии

между НСУ и БПЛА ведется в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

Заявляемый способ не накладывает каких-либо ограничений на используемые алгоритмы и режимы шифрования и контроля целостности сообщений. В частности, для шифрования сообщений могут использоваться алгоритмы шифрования, описанные в стандарте ГОСТ Р 34.12-2015 [31], в режимах работы, предназначенных для шифрования данных и описанных в стандарте ГОСТ Р 34.13-2015 [32], а для контроля целостности сообщений могут использоваться те же алгоритмы шифрования в режиме вычисления имитовставки.

В качестве дополнительной меры защиты может быть предусмотрена синхронная на стороне БПЛА и НСУ смена ключей шифрования передаваемых данных, для чего в передаваемых пакетах данных могут быть введены номера пакетов и каждый пакет может шифроваться на отдельном ключе, значение которого является зависимым от номера пакета.

Помимо обмена информацией по каналам управления и телеметрии, после выполнения шага 24 данные полезной нагрузки, передаваемые с БПЛА на НСУ, также могут передаваться в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

В случае, если с одной НСУ осуществляется управление несколькими БПЛА одновременно и ресурсов одного криптографического модуля на стороне НСУ недостаточно для выполнения предусмотренных заявляемым способом операций, на НСУ может быть установлено несколько криптографических модулей для параллельного выполнения требуемых операций. При этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

В процессе выполнения действий, предусмотренных заявляемым способом, и в рамках дальнейшего защищенного обмена данными между БПЛА и НСУ с целью дополнительной защиты радиообмена может использоваться псевдослучайная перенастройка параметров радиосвязи между БПЛА и НСУ.

Алгоритм выполнения основных действий в рамках заявляемого способа криптографической защиты каналов связи беспилотных авиационных комплексов, помимо перечисленных выше шагов, может включать в себя также ряд дополнительных действий по обработке различных ошибочных ситуаций. Выше описаны только основные ошибочные ситуации, имеющие прямое отношение к процессу установки защищенного обмена данными между БПЛА и НСУ.

Помимо них, в процессе выполнения предусмотренных заявляемым способом действий могут возникать прочие ошибки, связанные, в том числе, с потерей информационных пакетов, сигналов и другими проблемами беспроводного обмена между БПЛА и НСУ. Для их обработки в описанный выше алгоритм могут быть включены дополнительные действия, в качестве примера которых можно привести повтор отправки информационных пакетов, переустановку беспроводного соединения и аналогичные. При этом отработка ошибочных ситуаций, связанных с обменом данными между БПЛА и НСУ, может выполняться как на уровне криптографических модулей БПЛА и НСУ, так и на уровне приемо-передающих устройств, входящих в состав БПЛА и НСУ.

В соответствии с фиг. 3 заявляемая система криптографической защиты каналов

связи беспилотных авиационных комплексов содержит перечисленные далее основные компоненты:

1. Криптографический модуль БПЛА 113.
2. Ключевой носитель БПЛА 112.
3. Криптографический модуль НСУ 123.
4. Ключевой носитель НСУ 124.

Заявляемая система функционирует в соответствии с заявляемым способом криптографической защиты каналов связи беспилотных авиационных комплексов.

Криптографический модуль БПЛА 113 предназначен для выполнения на стороне БПЛА операций по установлению защищенного обмена данными между БПЛА и НСУ и по последующему шифрованию и защите целостности данных, передаваемых по беспроводным каналам связи 103 между БПЛА и НСУ.

Аналогичным образом, криптографический модуль НСУ 123 предназначен для выполнения на стороне НСУ операций по установлению защищенного обмена данными между БПЛА и НСУ и по последующему шифрованию и защите целостности данных, передаваемых по беспроводным каналам связи 103 между БПЛА и НСУ.

Возможны различные реализации криптографических модулей БПЛА и НСУ, в частности:

- криптографический модуль БПЛА/НСУ может представлять собой выделенное аппаратное устройство, подключаемое к внешнему вычислительному устройству и содержащее аппаратную и/или программную реализацию предусмотренных заявляемым способом преобразований в виде специализированных микросхем, микросхем с программируемой логикой (ПЛИС - программируемых логических интегральных схем), программных и/или микропрограммных модулей;
- криптографический модуль БПЛА/НСУ может представлять собой программную реализацию предусмотренных заявляемым способом преобразований, выполняющуюся непосредственно на вычислительных ресурсах внешнего вычислительного устройства.

Под внешним вычислительным устройством в данном случае подразумевается:

- полетный контроллер 111 в случае БПЛА;
- основной вычислительный модуль 121 НСУ, под которым подразумевается центральный процессор или аналогичное вычислительное устройство, работающее в составе основного компьютерного оборудования НСУ: сервера приложений (если рабочее место оператора НСУ выполнено в виде терминала, работающего согласно архитектуре «тонкого клиента»), персонального компьютера, переносного компьютера, смартфона и т.п.

На выбор конкретного варианта реализации криптографического модуля могут влиять, в т.ч. следующие факторы:

- возможность подключения аппаратного криптографического модуля к имеющемуся оборудованию БПЛА или НСУ;
- возможность загрузки программной реализации криптографического модуля и ее выполнение на существующих вычислительных ресурсах;
- достаточно ли ресурсов внешнего вычислительного модуля для выполнения программной реализации криптографического модуля с учетом необходимости выполнения на тех же ресурсах (полетного контроллера БПЛА или основного вычислительного модуля НСУ) программного обеспечения, предназначенного для решения основных задач полетного контроллера БПЛА или основного вычислительного модуля НСУ;
- насколько подключение аппаратного криптографического модуля БПЛА ухудшит

основные эксплуатационные характеристики БПЛА (такие, как максимальный вес полезной нагрузки и максимальная длительность/дальность полета) и др.

В криптографическом модуле БПЛА/НСУ должны быть реализованы функции, необходимые для выполнения предусмотренных заявляемым способом преобразований, в т.ч. следующих:

- криптографических алгоритмов и режимов их применения;
- функций генерации криптографических ключей;
- алгоритмов генерации случайных или псевдослучайных чисел;
- функций взаимодействия с ключевым носителем БПЛА (для криптографического модуля БПЛА) или НСУ (для криптографического модуля НСУ);
- функций взаимодействия с основным вычислительным модулем и др.

Криптографический модуль БПЛА должен иметь также возможность инициирования передачи сообщений в адрес НСУ через приемо-передающее устройство БПЛА 114. Аналогичным образом, криптографический модуль НСУ должен иметь также возможность инициирования передачи сообщений в адрес БПЛА через приемо-передающее устройство НСУ 125.

В случае программной реализации криптографического модуля все предусмотренные заявляемым способом преобразования выполняются программно непосредственно на полетном контроллере БПЛА или основном вычислительном модуле НСУ. При этом для усиления защиты при программной реализации криптографического модуля могут быть обеспечены следующие меры:

- изолированность процессов, выполняемых в рамках программной реализации криптографического модуля, от основной операционной среды вычислительного модуля;
- дублирование вычислений для обеспечения их надежности.

Возможен также вариант комбинированной программной реализации криптографического модуля, характеризующейся следующими признаками:

- в случае, если комплекс бортового оборудования БПЛА 101 или оборудование НСУ 102 уже включает в себя программную и/или аппаратную реализацию всех или части используемых криптографических алгоритмов или алгоритмов генерации случайных/псевдослучайных чисел, то криптографический модуль может не содержать реализации данных алгоритмов, которые в этом случае могут быть заменены на функции, обеспечивающие выполнение существующих в комплексе бортового оборудования БПЛА 101 или оборудования НСУ 102 реализаций криптографических алгоритмов или алгоритмов генерации случайных/псевдослучайных чисел;
- остальные требуемые алгоритмы и функции реализуются программно в криптографическом модуле БПЛА/НСУ.

В случае аппаратной реализации криптографического модуля БПЛА/НСУ криптографический модуль может подключаться к основному вычислительному устройству по любым интерфейсам, обеспечивающим достаточное для передачи требуемых данных быстродействие. В качестве примеров можно привести интерфейсы USB, PCI Express или UART, характерные как для компьютерного оборудования общего назначения (что актуально для НСУ), так и для полетных контроллеров БПЛА.

Энергопитание аппаратного криптографического модуля БПЛА/НСУ может осуществляться как по интерфейсу его подключения к полетному контроллеру БПЛА 111 или основному вычислительному модулю НСУ 121, так и от внешнего источника питания. Заявляемая система не накладывает каких-либо ограничений на способы осуществления энергопитания криптографических модулей БПЛА/НСУ.

Аппаратный криптографический модуль БПЛА 113 предпочтительно устанавливать в разрыв между полетным контроллером 111 и приемо-передающим модулем 114, но возможны и другие варианты его установки. При этом желательно, чтобы криптографический модуль БПЛА (независимо от варианта его реализации) обладал возможностью блокирования порта подключения полетного контроллера БПЛА к каналам связи, что необходимо для предотвращений потенциальной утечки незащищенных данных через приемо-передающий модуль 114 БПЛА. Однако данная возможность рассматривается как опциональная.

Аппаратный криптографический модуль НСУ 123 также предпочтительно устанавливать в разрыв между основным вычислительным модулем НСУ 121 и приемо-передающим устройством НСУ 125, но возможны и другие варианты его установки. Для криптографического модуля НСУ (независимо от варианта его реализации) желательно обеспечить возможность блокировки интерфейса обмена с программным обеспечением 122, осуществляющим управление БПЛА, что необходимо для предотвращения передачи команд в канал связи 103 между БПЛА и НСУ до завершения формирования защищенного канала обмена данными между БПЛА и НСУ. Однако данная возможность также рассматривается как опциональная.

Криптографический модуль БПЛА 113 и криптографический модуль НСУ 123 выполняют различные части алгоритма установления защищенного канала связи между БПЛА и НСУ, предусмотренного заявляемым способом, со стороны БПЛА и НСУ, соответственно. Т.е. алгоритмы, реализуемые криптографическим модулем БПЛА и криптографическим модулем НСУ, фактически различаются и поэтому криптографический модуль БПЛА и криптографический модуль НСУ могут быть реализованы в виде различных устройств или различных программных реализаций.

Но поскольку алгоритмы, выполняемые криптографическим модулем НСУ и криптографическим модулем БПЛА, имеют много общих компонентов, криптографический модуль БПЛА и криптографический модуль НСУ могут быть реализованы как единое устройство или единая программная реализация, в которых с помощью программного параметра (флага) и/или аппаратного переключателя указывается назначение конкретного экземпляра криптографического модуля, определяющее алгоритмы и/или режимы его работы, т.е. используется ли данный экземпляр криптографического модуля в качестве криптографического модуля БПЛА или криптографического модуля НСУ.

В любом из описанных выше вариантов реализации криптографических модулей БПЛА/НСУ, поскольку заявляемый способ не ограничивает применение конкретных криптографических алгоритмов, режимов и параметров их работы, необходимо в рамках одного экземпляра заявляемой системы обеспечить совместимость применяемых криптографических модулей БПЛА и криптографических модулей НСУ, т.е. использовать в них идентичные криптографические алгоритмы, режимы и параметры их применения.

При этом нет необходимости применения в рамках одного экземпляра заявляемой системы эквивалентных реализаций криптографического модуля БПЛА и криптографического модуля НСУ. Т.е. независимо от конкретного варианта аппаратной или программной реализации криптографического модуля НСУ, может быть использован любой вариант аппаратной или программной реализации криптографического модуля БПЛА с учетом необходимой совместимости криптографического модуля НСУ и криптографического модуля БПЛА. Отсутствие данного ограничения распространяется и на тот вариант, когда с одной НСУ

осуществляется управление несколькими БПЛА одновременно: в рамках такой системы криптографические модули всех БПЛА и криптографический модуль НСУ могут быть реализованы различными способами при условии обеспечения их совместимости.

Ключевой носитель БПЛА 112 и ключевой носитель НСУ 124 представляют собой устройства, оснащенные, как минимум, следующими компонентами и возможностями:

- вычислительными возможностями;

- операционной системой и/или управляющим микропрограммным обеспечением и/или другими программными/микропрограммными модулями, осуществляющими управление прочими компонентами ключевого носителя БПЛА/НСУ, а также взаимодействием как между ними, так и между ключевым носителем и криптографическим модулем БПЛА/НСУ, к которому ключевой носитель подключается;

- оперативной и энергонезависимой памятью;

- программной (микропрограммной) и/или аппаратной реализацией криптографических алгоритмов, включая алгоритмы генерации случайных или псевдослучайных чисел.

Заявляемая система не накладывает ограничений на принципы организации хранения криптографических ключей и прочих данных в энергонезависимой памяти ключевого носителя БПЛА/НСУ. Например, в энергонезависимой памяти ключевого носителя БПЛА/НСУ может быть предусмотрена файловая система согласно стандарту ГОСТ Р ИСО/МЭК 7816-4-2013 [25].

Криптографические алгоритмы, реализованные в ключевых носителях БПЛА/НСУ и применяемые в процессе установления защищенного обмена данными между БПЛА и НСУ, должны быть совместимы с криптографическими алгоритмами, реализованными в криптографических модулях БПЛА/НСУ, в том числе в части режимов и параметров их работы.

Ключевой носитель БПЛА 112 и ключевой носитель НСУ 124 подключаются, соответственно, к криптографическому модулю БПЛА 113 и криптографическому модулю НСУ 123. Следовательно, криптографические модули БПЛА/НСУ должны быть оснащены интерфейсом подключения ключевого носителя БПЛА/НСУ, включая порт для его подключения и/или необходимое внешнее устройство, взаимодействия с ключевым носителем (в зависимости от используемого типа ключевого носителя), а также необходимое для взаимодействия с ключевым носителем (и/или внешним устройством взаимодействия с ключевым носителем при его наличии) программное/микропрограммное обеспечение.

Как было сказано ранее, в качестве примеров возможных ключевых носителей БПЛА/НСУ могут быть приведены криптографические смарт-карты (смарт-карты на основе микросхем с криптографическими возможностями) или криптографические токены. При использовании криптографических токенов, подключаемых по интерфейсу USB, соответствующий криптографический модуль должен быть оснащен интерфейсом USB и соответствующим портом для подключения токена. При использовании смарт-карт соответствующий криптографический модуль должен быть оснащен не только интерфейсом USB, но и подключаемым к нему контактным или бесконтактным считывателем смарт-карт.

Заявляемая система не накладывает каких-либо ограничений на используемые типы или модели ключевых носителей БПЛА/НСУ, а также на интерфейсы их подключения и/или устройства взаимодействия с ключевыми носителями при условии их соответствия описанным требованиям. Кроме того, в рамках одного экземпляра заявляемой системы могут быть использованы различные типы/модели ключевых носителей БПЛА и НСУ

при условии выполнения сформулированного ранее требования по их совместимости с соответствующими криптографическими модулями БПЛА/НСУ.

В случае использования программной реализации криптографического модуля БПЛА 113 комплекс бортового оборудования БПЛА 101 должен быть оснащен интерфейсом подключения ключевого носителя БПЛА, включая порт для его подключения и/или необходимое внешнее устройство взаимодействия с ключевым носителем, а также необходимое для взаимодействия с ключевым носителем (и/или внешним устройством взаимодействия с ключевым носителем при его наличии) программное/микропрограммное обеспечение; при этом должна быть обеспечена возможность взаимодействия криптографического модуля БПЛА 113 и ключевого носителя БПЛА 112.

В случае использования программной реализации криптографического модуля НСУ 123 оборудование НСУ 102 должно быть также оснащено интерфейсом подключения ключевого носителя НСУ, включая порт для его подключения и/или необходимое внешнее устройство взаимодействия с ключевым носителем, а также необходимое для взаимодействия с ключевым носителем (и/или внешним устройством взаимодействия с ключевым носителем при его наличии) программное/микропрограммное обеспечение; при этом должна быть обеспечена возможность взаимодействия криптографического модуля НСУ 123 и ключевого носителя НСУ 124.

Управление ключевыми носителями БПЛА/НСУ осуществляется с внешнего устройства; ключевые носители БПЛА/НСУ являются пассивными устройствами, обеспечивающими выполнение определенных команд, инициированных внешним устройством.

Внешним (управляющим) по отношению к ключевому носителю БПЛА 112 устройством в показанном на фиг. 3 варианте заявляемой системы является криптографический модуль БПЛА 113, а внешним (управляющим) устройством по отношению к ключевому носителю НСУ 124 является криптографический модуль НСУ 123 независимо от аппаратной или программной реализации криптографического модуля БПЛА/НСУ и конкретных компонентов комплекса бортового оборудования БПЛА 101 или оборудования НСУ 102 в случае программной реализации, соответственно, криптографического модуля БПЛА и криптографического модуля НСУ.

При этом заявляемая система криптографической защиты каналов связи БАК не накладывает ограничений на управляющие устройства на подготовительном этапе заявляемого способа криптографической защиты каналов связи БАК (шаги 1-3 описанного ранее алгоритма), в рамках которого осуществляется подготовка ключевых носителей БПЛА/НСУ, включающая генерацию пар асимметричных ключей и обмен открытыми ключами. Подготовительный этап может быть выполнен заранее, причем нет необходимости подготовки ключевого носителя БПЛА при его непосредственном подключении к БПЛА: ключевой носитель БПЛА может быть подготовлен на НСУ; в этом случае внешним (управляющим) устройством по отношению к ключевому носителю БПЛА является какой-либо компонент оборудования НСУ, на котором реализовано соответствующее управляющее программное обеспечение (или присутствует аналогичная аппаратная реализация).

Более того, ключевые носители всех БПЛА (в т.ч. в случае, когда с одной НСУ осуществляется управление несколькими БПЛА одновременно) и ключевой носитель НСУ могут быть подготовлены на некотором выделенном ключевом центре 104, выполняющем централизованную подготовку ключевых носителей БПЛА и НСУ. В

этом случае ключевой центр 104 также рассматривается как часть заявляемой системы, а внешним (управляющим) устройством по отношению к ключевым носителям БПЛА/НСУ является какой-либо компонент оборудования ключевого центра, на котором реализовано соответствующее управляющее программное обеспечение (или присутствует аналогичная аппаратная реализация).

Заявляемым способом предусмотрено, что после выполнения шага считывания криптографических ключей с ключевого носителя БПЛА (шаг 5 описанного ранее алгоритма) дальнейшее использование ключевого носителя БПЛА не осуществляется.

Следовательно, после выполнения данного шага ключевой носитель БПЛА может быть отсоединен от криптографического модуля БПЛА. Кроме того, с целью минимизации веса оборудования (и, соответственно, минимизации ухудшения перечисленных выше основных эксплуатационных характеристик БПЛА), относящегося к заявляемой системе, аппаратная часть интерфейса подключения ключевого носителя БПЛА может быть отсоединена от криптографического модуля БПЛА (включая какие-либо аппаратные модули, обеспечивающие взаимодействие с ключевыми носителями, например, считыватели смарт-карт).

Заявляемое устройство криптографической защиты каналов связи БАК, структурная схема которого приведена на фиг. 4, представляет собой один из возможных примеров реализации криптографического модуля, который может использоваться в качестве криптографического модуля БАК или криптографического модуля НСУ в рамках заявляемой системы криптографической защиты каналов связи БАК.

В соответствии с фиг. 4 и выполняемыми им функциями, заявляемое устройство состоит из двух основных функциональных элементов, находящихся на общей плате устройства 201:

- управляющего микроконтроллера 211;
- энергонезависимой памяти 212.

Отметим, что управляющий микроконтроллер, в зависимости от его типа и модели, может содержать достаточный для размещения описанных далее программных модулей и прочих данных объем энергонезависимой памяти; в этом случае установка выделенной энергонезависимой памяти не требуется.

В состав управляющего микроконтроллера 211 входят программные модули, выполняющиеся на управляющем микроконтроллере в процессе работы устройства:

1. Модуль управления 221, являющийся основным программным модулем заявляемого устройства. Данный модуль обеспечивает управление всеми остальными программными модулями, выполняющимися на управляющем микроконтроллере, и взаимодействие между ними.

2. Модуль обеспечения конфиденциальности и целостности информационного обмена 222. Данный модуль обеспечивает защиту информационного обмена между БПЛА и НСУ, т.е. выполняет, в частности, шифрование сообщений и контроль их целостности. Именно в этом модуле реализуются используемые криптографические алгоритмы и режимы их работы. При необходимости выполнения криптографических операций в других программных модулях (например, в модуле аутентификации и установления защищенного соединения 223) производятся обращения к модулю обеспечения конфиденциальности и целостности информационного обмена 222 со стороны других программных модулей.

3. Модуль аутентификации и установления защищенного соединения 223. Данный модуль обеспечивает выполнение аутентификации сторон информационного обмена и основных операций по установлению защищенного соединения между БПЛА и НСУ;

именно данный модуль обеспечивает выполнение последовательности действий, предусмотренных алгоритмами заявляемого способа криптографической защиты каналов связи БАК.

Выполнение данной последовательности действий осуществляется во взаимодействии с другими программными модулями в части их функциональных возможностей.

4. Модуль генерации и обработки ключевой информации 224. Данный модуль обеспечивает выполнение преобразований над криптографическими ключами, т.е. вычисление производных ключей (в описанном выше алгоритме - вычисление мастер-ключа на основе пре-мастер-ключа) и диверсификацию ключей (в описанном выше алгоритме - вычисление ключа шифрования и ключа вычисления имитовставки на основе мастер-ключа).

Кроме того, данный модуль инициирует выполнение ключевым носителем БПЛА/НСУ, подключенным к криптографическому модулю через интерфейс 214, функций по генерации ключей (в описанном выше алгоритме - генерация пар асимметричных ключей и вычисление общего секретного пре-мастер-ключа). Взаимодействие с ключевым носителем БПЛА/НСУ данный модуль осуществляет через модуль взаимодействия с ключевым носителем 226.

Модуль генерации и обработки ключевой информации 224 отвечает также за выполнение записи ключей на ключевой носитель БПЛА/НСУ и чтения ключей с ключевого носителя БПЛА/НСУ.

5. Модуль генерации случайных или псевдослучайных чисел 225. Данный модуль отвечает за генерацию случайных чисел на основе недетерминированных физических процессов или псевдослучайных чисел на основе детерминированных алгоритмов, в т.ч. криптографических (генерация псевдослучайных чисел может выполняться, например, в соответствии с рекомендациями, изложенными в документе [33]). В данном модуле также могут выполняться процедуры контроля генерируемых случайных/псевдослучайных чисел на соответствие критериям случайности.

При использовании для генерации псевдослучайных чисел криптографических алгоритмов данный модуль осуществляет взаимодействие с модулем обеспечения конфиденциальности и целостности информационного обмена 222. Для инициализации и (при необходимости) переинициализации процесса генерации псевдослучайных чисел может использоваться какая-либо величина (например, полученная с физического датчика случайных чисел), получаемая от внешнего источника. В качестве внешнего источника может использоваться ключевой носитель БПЛА/НСУ либо любой другой источник данных (например, клавиатурный ввод пользователя). В последнем случае данная величина передается управляющему микроконтроллеру 211 внешним вычислительным устройством через интерфейс подключения к внешнему вычислительному устройству 213.

6. Модуль взаимодействия с ключевым носителем 226. Данный модуль отвечает за передачу команд, инициированных другими программными модулями (например, модулем генерации и обработки ключевой информации 224), ключевому носителю БПЛА/НСУ через интерфейс взаимодействия с ключевым носителем 214 и за получение ответов от ключевого носителя БПЛА/НСУ, их обработку и передачу полученных в ответах данных вызывающему модулю.

Заявляемое устройство допускает возможность применения различных вариантов ключевых носителей в рамках одной заявляемой системы (например, криптографических смарт-карт и криптографических токенов или криптографических смарт-карт различных моделей). Модуль взаимодействия с ключевым носителем 226 должен включать в себя

реализацию необходимых протоколов взаимодействия со всеми используемыми типами/моделями ключевых носителей БПЛА/НСУ и/или устройствами взаимодействия с ними (например, считывателями смарт-карт). Все различия в протоколах и прочих аспектах взаимодействия с различными типами/моделями ключевых носителей должны быть проработаны именно на уровне модуля взаимодействия с ключевым носителем 226, который должен предоставлять другим программным модулям единый интерфейс взаимодействия с ключевыми носителями БПЛА/НСУ, не зависящий от их конкретных типов или моделей.

7. Модуль взаимодействия с приемо-передающим устройством 227. Данный модуль отвечает за передачу информации от заявляемого устройства приемо-передающему модулю, входящему в состав комплекса бортового оборудования БПЛА или оборудования НСУ, а также за прием и обработку информации от приемо-передающего модуля. Кроме того, данный модуль может отвечать за выполнение блокировки и разблокировки приемо-передающего модуля.

Взаимодействие с приемо-передающим модулем осуществляется через интерфейс взаимодействия с приемо-передающим устройством 215.

8. Модуль самотестирования устройства 228. Данный модуль является опциональным. При его наличии он обеспечивает выполнение процедур самотестирования заявляемого устройства, причем самотестирование устройства может осуществляться как при старте устройства, так и периодически, например, через предопределенные интервалы времени, после приема или передачи определенного объема передаваемых данных с момента предыдущего самотестирования и т.п.

Выполнение самотестирования устройства не должно мешать выполнению заявляемым устройством прочих функций устройства.

9. Модуль контроля целостности программного обеспечения устройства 229. Данный модуль является опциональным. При его наличии он контролирует целостность остальных модулей устройства перед их загрузкой в управляющий микроконтроллер 211.

Контроль целостности может выполняться на основе любых типов контрольного суммирования данных, включая криптографические (например, с помощью алгоритма контрольного суммирования CRC32 [34] или с помощью алгоритма хэширования ГОСТ Р 34.11-2012 [30]) путем, например, контрольного суммирования каждого из программных модулей перед их загрузкой и последующего сравнения полученной контрольной суммы с эталонным значением, которое может храниться в энергонезависимой памяти 212 заявляемого устройства.

Заявляемое устройство имеет следующие интерфейсы:

1. Интерфейс подключения к внешнему вычислительному устройству 213. В данном случае внешним устройством может быть одно из следующих устройств:

- полетный контроллер БПЛА в случае, если заявляемое устройство функционирует в качестве криптографического модуля БПЛА;
- основной вычислительный модуль НСУ в случае, если заявляемое устройство функционирует в качестве криптографического модуля НСУ; под основным вычислительным модулем НСУ подразумевается центральный процессор или аналогичное вычислительное устройство, работающее в составе основного компьютерного оборудования НСУ: сервера, персонального компьютера, переносного компьютера, смартфона и т.п.

Заявляемое устройство может подключаться к внешнему вычислительному устройству по любым интерфейсам, обеспечивающим достаточное для передачи требуемых данных

быстродействие. В качестве примеров можно привести интерфейсы USB, PCI Express или UART, характерные как для компьютерного оборудования общего назначения (что актуально для НСУ), так и для полетных контроллеров БПЛА.

Энергопитание заявляемого устройства осуществляется также может осуществляться через интерфейс подключения к внешнему вычислительному устройству 213, но может осуществляться и любыми другими способами.

2. Интерфейс взаимодействия с ключевым носителем 214. Данный интерфейс обеспечивает подключение к заявляемому устройству ключевого носителя БПЛА (если устройство функционирует в качестве криптографического модуля БПЛА) или ключевого носителя НСУ (если устройство функционирует в качестве криптографического модуля НСУ), а также взаимодействие с подключаемым ключевым носителем БПЛА/НСУ.

Как было сказано ранее, ключевой носитель БПЛА/НСУ может подключаться не напрямую к данному интерфейсу, а через какое-либо промежуточное устройство, обеспечивающее взаимодействие с ключевым носителем используемого типа (например, промежуточным устройством может быть считыватель смарт-карт при использовании криптографических смарт-карт в качестве ключевых носителей БПЛА/НСУ).

В качестве примера интерфейса взаимодействия с ключевым носителем 214 можно привести интерфейс USB.

Энергопитание подключенного к заявляемому устройству ключевого носителя БПЛА/НСУ и/или устройства взаимодействия с ключевым носителем (при наличии такого устройства) может осуществляться через интерфейс взаимодействия с ключевым носителем 214 либо любым другим способом.

3. Интерфейс взаимодействия с приемо-передающим устройством 215. Данный интерфейс обеспечивает соединение заявляемого устройства и приемо-передающего устройства и взаимодействие между ними.

В данном случае могут использоваться любые интерфейсы, обеспечивающие достаточное для передачи требуемых данных быстродействие. В качестве примеров здесь также можно привести интерфейсы USB или UART.

Через интерфейс взаимодействия с приемо-передающим устройством 215 может осуществляться энергопитание приемо-передающего устройства, которое также может осуществляться и любым другим способом.

Заявляемое устройство функционирует в соответствии с заявляемым способом криптографической защиты каналов связи БАК, выполняя функции криптографического модуля БПЛА или криптографического модуля НСУ.

После включения устройства в управляющий микроконтроллер 211 из энергонезависимой памяти 212 загружается модуль контроля целостности программного обеспечения устройства 229 (при его наличии). Данный модуль выполняет считывание остальных программных модулей, расчет их контрольных сумм и проверку соответствия рассчитанных контрольных сумм эталонным значениям, хранящимся в энергонезависимой памяти 212 устройства.

После этого выполняется самотестирование устройства модулем самотестирования устройства 228 (при его наличии). Как было сказано выше, периодическое самотестирование устройства может выполняться и в дальнейшем в процессе работы устройства.

Если контроль целостности программного обеспечения устройства и/или самотестирование устройства выявили ошибки в его работе и/или нарушения целостности программного обеспечения, то дальнейшая работа устройства блокируется;

в этом случае устройство может выдавать соответствующее сообщение об ошибке внешнему вычислительному устройству через интерфейс подключения к внешнему вычислительному устройству 213 и/или приемо-передающему устройству через интерфейс взаимодействия с приемо-передающим устройством 215.

Если система, в составе которой функционирует заявляемое устройство, подразумевает подготовку ключевых носителей при их непосредственном подключении к заявляемому устройству (а не, например, на выделенном ключевом центре, обеспечивающем централизованную подготовку ключевых носителей) и подготовка ключевого носителя не была выполнена ранее, то устройство инициирует работу с подключенным ключевым носителем, обеспечивая выполнение предварительного этапа заявляемого способа - этапа подготовки ключевого носителя, на котором выполняется генерация пары асимметричных ключей и обмен открытыми ключами. На данном этапе задействуются модуль управления 221 и модуль генерации и обработки ключевой информации 224, которые взаимодействуют с ключевым носителем через модуль взаимодействия с ключевым носителем 226 и интерфейс взаимодействия с ключевым носителем 214.

Затем криптографический модуль выполняет действия этапа штатной работы основного алгоритма, реализующего заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА, в части действий криптографического модуля БПЛА или криптографического модуля НСУ. В результате выполнения данного этапа формируется защищенный канал обмена данными между БПЛА и НСУ.

На данном этапе задействуются модуль управления 221, модуль обеспечения конфиденциальности и целостности информационного обмена 222, модуль аутентификации и установления защищенного соединения 223, модуль генерации и обработки ключевой информации 224 и модуль генерации случайных или псевдослучайных чисел 225. При этом данные модули могут инициировать взаимодействие со следующими внешними устройствами по отношению к заявляемому устройству:

- с внешним вычислительным устройством через модуль управления 221 и интерфейс подключения к внешнему вычислительному устройству 213;
- с ключевым носителем через модуль взаимодействия с ключевым носителем 226 и интерфейс взаимодействия с ключевым носителем 214;
- с приемо-передающим устройством через модуль взаимодействия с приемо-передающим устройством 227 и интерфейс взаимодействия с приемо-передающим устройством 215.

После установления защищенного обмена данными между БПЛА и НСУ заявляемое устройство функционирует следующим образом:

- информация, предназначенная для передачи в канал беспроводной радиосвязи и дальнейшей передачи на БПЛА (со стороны НСУ) или на НСУ (со стороны БПЛА), передается внешним вычислительным устройством через интерфейс подключения к внешнему вычислительному устройству 213 и модуль управления 221, затем зашифровывается и снабжается необходимой для контроля целостности информацией в модуле обеспечения конфиденциальности и целостности информационного обмена 222 (который также при необходимости может задействовать модуль генерации случайных или псевдослучайных чисел 225), после чего результат обработки информации модулем 222 передается приемо-передающему устройству через модуль взаимодействия с приемо-передающим устройством 227 и интерфейс взаимодействия с приемо-передающим устройством 215;

- зашифрованная информация, получаемая из канала беспроводной радиосвязи, передается приемо-передающим устройством через интерфейс взаимодействия с приемо-передающим устройством 215 и модуль взаимодействия с приемо-передающим устройством 227, затем модулем обеспечения конфиденциальности и целостности информационного обмена 222 информация расшифровывается и проверяется ее целостность, после чего расшифрованная информация передается внешнему вычислительному устройству через модуль управления 221 и интерфейс подключения к внешнему вычислительному устройству 213.

В случае невозможности по каким-либо причинам расшифрования полученного из канала беспроводной связи сообщения и/или обнаружения нарушения его целостности полученное сообщение игнорируется. В этом случае устройство может выдавать соответствующее сообщение об ошибке внешнему вычислительному устройству через интерфейс подключения к внешнему вычислительному устройству 213 и/или приемо-передающему устройству через интерфейс взаимодействия с приемо-передающим устройством 215.

Остальные компоненты заявляемого устройства на этапе обмена данными между БПЛА и НСУ после установления защищенного канала связи не используются, за исключением модуля самотестирования устройства 228 (при его наличии), который может выполнять периодическое самотестирование устройства в процессе его работы.

Заявляемое устройство криптографической защиты каналов связи БАК может быть реализовано на базе известных покупных комплектующих изделий. Заявителем разработан экспериментальный образец заявляемого устройства, основанный на использовании следующих комплектующих и модулей:

- макетной платы Core746I, содержащей управляющий микроконтроллер STM32F746IGT6 (Cortex-M7), обладающий большим объемом энергонезависимой памяти;

- программные модули (модуль управления, модуль обеспечения конфиденциальности и целостности информационного обмена, модуль аутентификации и установления защищенного соединения, модуль генерации и обработки ключевой информации, модуль генерации случайных или псевдослучайных чисел, модуль взаимодействия с ключевым носителем и модуль взаимодействия с приемо-передающим устройством) написаны на языке программирования Си и выполнены в виде микропрограмм прошивки микроконтроллера;

- в качестве интерфейса подключения внешнего вычислительного устройства и интерфейса взаимодействия с приемо-передающим устройством используется интерфейс UART;

- в качестве интерфейса подключения ключевого носителя используется интерфейс USB в форм-факторе microUSB;

- в качестве ключевых носителей экспериментальный образец может использовать криптографические смарт-карты на основе отечественной микросхемы MIK51SC72D и ее вариантов; взаимодействие со смарт-картами осуществляется через считыватель смарт-карт КРИПТОН-ССК, подключаемый к экспериментальному образцу через переходник microUSB-USB;

- энергопитание экспериментального образца осуществляется по выделенному интерфейсу от внешнего вычислительного устройства;

- экспериментальный образец содержит выделенный интерфейс для энергопитания приемо-передающего устройства.

В программных модулях устройства реализованы следующие криптографические алгоритмы:

- в качестве алгоритма шифрования сообщений используется алгоритм «Магма» ГОСТ Р 34.12-2015 [31] в режиме гаммирования с обратной связью по шифртексту согласно ГОСТ Р 34.13-2015 [32];

- в качестве алгоритма контроля целостности сообщений используется алгоритм «Магма» ГОСТ Р 34.12-2015 [31] в режиме вычисления имитовставки согласно ГОСТ Р 34.13-2015 [32];

- в качестве алгоритмов вычисления общего ключа и диверсификации ключей используются алгоритмы VKO_GOSTR3410_2012 [29] и ГОСТ Р 34.11-2012 [30].

Дополнительно экспериментальный образец устройства оснащен кнопкой сброса питания RESET, индикаторами питания и подключения по интерфейсу USB, а также переключателями режимов работы.

Кроме того, в экспериментальном образце реализован тестовый режим его работы с повышенным быстродействием обработки данных.

Проведенное нагрузочное тестирование экспериментального образца показало эффективность операций шифрования на скорости 115200 кбит/с в режиме full duplex (одновременная обработка данных, поступающих на прием и передачу), чего более чем достаточно для реализации защиты командно-телеметрического канала при максимальной генерации телеметрических данных полетным контроллером. При активации реализованного в экспериментальном образце тестового режима с повышенным быстродействием обработки данных может быть также реализована защита информации канала передачи данных полезной нагрузки с БПЛА на НСУ с рядом ограничений.

Заявителем разработан также экспериментальный образец заявляемой системы, основанный на применении следующих компонентов и решений:

- НСУ построена на базе персонального компьютера, оснащенного процессором Intel i5, 4 ГБ оперативной памяти SSD 240 ГБ, необходимым количеством портов USB и свободно распространяемой операционной системой Ubuntu Linux 16.04;

- в качестве программного обеспечения управления БПЛА используется установленное на компьютер НСУ свободно распространяемое программное обеспечение QGroundControl;

- в системе присутствует один управляемый БПЛА, собранный заявителем на основе полетного контроллера Pixhawk 2.4.8 и других покупных компонентов;

- в качестве приемо-передающих модулей НСУ используется 3DR Telemetry Kit 433 МГц;

- описанный выше экспериментальный образец заявляемого устройства в различных режимах работы используется в качестве криптографического модуля БПЛА и криптографического модуля НСУ;

- криптографический модуль НСУ подключается к порту USB компьютера НСУ через переходник USB-UART и получает энергопитание от внешнего блока питания через выделенный разъем;

- приемо-передающее устройство НСУ подключается к порту UART криптографического модуля НСУ и получает энергопитание от выделенного разъема криптографического модуля НСУ;

- криптографический модуль БПЛА подключается к полетному контроллеру БПЛА через интерфейс UART и получает энергопитание от полетного контроллера БПЛА через выделенный разъем;

- приемо-передающее устройство БПЛА подключается к порту UART криптографического модуля БПЛА и получает энергопитание от выделенного разъема

криптографического модуля БПЛА;

- в качестве ключевых носителей БПЛА и НСУ используются криптографические смарт-карты на основе отечественной микросхемы MIK51SC72D;

- в качестве устройства взаимодействия с ключевыми носителями БПЛА/НСУ используется контактный считыватель смарт-карт КРИПТОН-ССК, который подключается к портам USB криптографических модулей БПЛА/НСУ через переходник microUSB-USB.

Проведенное тестирование экспериментального образца заявляемой системы показало возможность достижения поставленной цели в виде создания криптографически стойкой системы защиты каналов информационного обмена БАК, а также корректность и эффективность заявляемого способа криптографической защиты каналов связи БАК, лежащего в основе заявляемой системы.

Изложенные выше сведения свидетельствуют, что для заявляемых системы и устройства криптографической защиты каналов связи БАК в том виде, как они охарактеризованы в соответствующих пунктах изложенной формулы изобретения, подтверждена возможность осуществления изобретения с помощью описанных средств.

Следовательно, заявляемое техническое решение соответствует критерию «промышленная применимость».

Заявляемую систему криптографической защиты каналов связи БАК или аналогичные системы, основанные на реализации заявляемого способа криптографической защиты каналов связи БАК, рекомендуется использовать для защиты каналов связи между БПЛА и НСУ (каналов управления, телеметрии и передачи данных полезной нагрузки БПЛА) во всех случаях, когда требуется обеспечение целостности и конфиденциальности информации, передаваемой по данным каналам связи.

Заявляемое устройство криптографической защиты каналов связи БАК, основанное на реализации криптографически стойких отечественных стандартов на криптографические преобразования, может использоваться в системах криптографической защиты каналов связи БАК в качестве основных компонентов - криптографических модулей БПЛА и/или криптографических модулей НСУ.

Источники информации:

1. Боев Н. М., Шаршавин П. В., Нигруца И. В. Построение систем связи беспилотных летательных аппаратов для передачи информации на большие расстояния. // Известия ЮФУ. Технические науки. Раздел IV. Комплексы с БЛА.

2. Прокопьев И. В. Бецков А. В. Структура системы управления беспилотных летательных аппаратов специального назначения. // Труды Международного симпозиума «Надежность и качество», 2012, том 1.

3. Шилов К. Е. Разработка системы автоматического управления беспилотным летательным аппаратом мультироторного типа. // Труды МФТИ, 2014, Том 6, №4.

4. Kamkar S. SkyJack. // http://samy.pl - Private Blog - Dec 2, 2013.

5. Агаджанов М. Сложно ли угнать коптер? Несколько уже реализованных способов перехвата управления. // https://geektimes.ru/post/281934/.

6. Sigma Design. Software Design Specification. Security 2 Command Class, version 0.9, 2016.

7. Anderson R. Why Cryptosystems Fail. // http://www.cl.cam.ac.uk - University Computer Laboratory, Cambridge.

8. Patent No. US 8219799. Secure Communication System. - Jul. 10, 2012.

9. Patent No. US 9531689. System and Method for Encryption of Network Data. -Dec. 27, 2016.

10. Patent No. CN 105491564. Method for Establishing a Secure Communication Link in a Multi-UAV Environment. - Apr. 13, 2016.

11. Patent No. US 9412278. Authentication Systems and Methods for Generating Flight Regulations. - Aug. 9, 2016.

12. Patent No. US 9805372. Authentication Systems and Methods for Generating Flight Regulations. - Oct. 31, 2017.

13. Patent No. US 9805607. Authentication Systems and Methods for Generating Flight Regulations. - Oct. 31, 2017.

14. Patent No. US 9870566. Authentication Systems and Methods for Generating Flight Regulations. - Jan. 16, 2018.

15. Patent No. WO 2017042403. Secure Control of Unmanned Vehicles. - Mar. 16, 2017.

16. Patent No. US 9542850. Secure Communications with Unmanned Aerial Vehicles. -Jan. 10, 2017.

17. Patent No. US 9651944. Unmanned Aerial Vehicle Piloting Authorization. -May 16, 2017.

18. Patent No. WO 2005020445. Microwave Self-Phasing Antenna Arrays for Secure Data Transmission & Satellite Networks Crosslinks. - Nov. 10, 2005.

19. Patent No. US 8594662. Method and Apparatus for Protected Communications to High Altitude Aircraft. - Nov. 26, 2013.

20. Patent No. US 5841864. Apparatus and Method for Authentication and Session Key Exchange in a Communication System. - Nov. 24, 1998.

21. Patent No. US 6816970. Security Method and System for Persistent Storage and Communications on Computer Network Systems and Computer Network Systems Employing the Same.-Nov. 9, 2004.

22. Patent No. US 9871772. Cryptographic System for Secure Command and Control of Remotely Controlled Devices. - Jan. 16, 2018 - прототип.

23. ГОСТ Р ИСО/МЭК 7816. Карты идентификационные. Карты на интегральных схемах.

24. ГОСТ Р ИСО/МЭК 14443. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия.

25. ГОСТ Р ИСО/МЭК 7816-4-2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

26. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

27. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

28. Barker E., Chen L., Roginsky A., Smid M. NIST Special Publication 800-56A Revision 2. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. // http://csrc.nist.gov - National Institute of Standards and Technology -May 2013.

29. Рекомендации по стандартизации Р 50.1.113-2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования.

30. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.

31. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.

32. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита

информации. Режимы работы блочных шифров.

33. Barker E., Kelsey J. NIST Special Publication 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised). // http://csrc.nist.gov - National Institute of Standards and Technology - March 2007.

34. Koopman P. 32-Bit Cyclic Redundancy Codes for Internet Applications. // http://www.ece.cmu.edu - 2002 - Carnegie Mellon University, Pittsburgh, USA.

(57) Формула изобретения

1. Способ криптографической защиты каналов связи между наземной станцией управления и беспилотным летательным аппаратом, заключающийся в выполнении следующей последовательности действий: на первом шаге с помощью ключевого носителя наземной станции управления (НСУ), оснащенного вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями, генерируется пара асимметричных ключей НСУ, включающая секретный и открытый ключи НСУ; на втором шаге с помощью ключевого носителя беспилотного летательного аппарата (БПЛА), оснащенного вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями, генерируется пара асимметричных ключей БПЛА, включающая секретный и открытый ключи БПЛА; на третьем шаге осуществляется копирование открытых ключей НСУ и БПЛА на, соответственно, ключевой носитель БПЛА и ключевой носитель НСУ, после которого ключевой носитель НСУ содержит секретный и открытый ключи НСУ и открытый ключ БПЛА, а ключевой носитель БПЛА содержит секретный и открытый ключи БПЛА и открытый ключ НСУ; на четвертом шаге криптографический модуль БПЛА, оснащенный программной или аппаратной реализацией криптографических алгоритмов, возможностью инициирования передачи сообщений на НСУ и опциональной возможностью блокирования порта подключения полетного контроллера к каналам связи, инициирует генерацию ключевым носителем БПЛА общего секретного пре-мастер-ключа, предназначенного для дальнейшей генерации на его основе мастер-ключа, на основе секретного ключа БПЛА и открытого ключа НСУ; на пятом шаге криптографический модуль БПЛА считывает с ключевого носителя БПЛА открытый ключ БПЛА, открытый ключ НСУ и общий секретный пре-мастер-ключ; на шестом шаге криптографический модуль НСУ, оснащенный программной или аппаратной реализацией криптографических алгоритмов, возможностью инициирования передачи сообщений на БПЛА и потенциальной возможностью блокирования интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА, инициирует генерацию ключевым носителем НСУ общего секретного пре-мастер-ключа на основе секретного ключа НСУ и открытого ключа БПЛА; на седьмом шаге криптографический модуль НСУ считывает с ключевого носителя НСУ открытый ключ НСУ, открытый ключ БПЛА и общий секретный пре-мастер-ключ; на восьмом шаге криптографический модуль БПЛА проверяет состояние своей готовности к работе; на девятом шаге криптографический модуль БПЛА инициирует отправку сообщения криптографическому модулю НСУ, содержащего открытый ключ БПЛА и случайное число БПЛА; на десятом шаге криптографический модуль НСУ, находящийся в режиме ожидания сообщений из канала связи, получает данное сообщение от БПЛА и проверяет, есть ли у него полученный открытый ключ БПЛА, при этом если такого открытого ключа у криптографического модуля НСУ нет, то криптографический модуль НСУ игнорирует полученное сообщение и возвращается в режим ожидания сообщений; на одиннадцатом шаге криптографический модуль НСУ инициирует отправку ответного сообщения

криптографическому модулю БПЛА, содержащего открытый ключ НСУ и случайное число НСУ; на двенадцатом шаге криптографический модуль БПЛА получает ответное сообщение от криптографического модуля НСУ и проверяет, есть ли у него полученный открытый ключ НСУ, при этом если такого открытого ключа у криптографического модуля НСУ нет, то криптографический модуль БПЛА игнорирует данное сообщение и возвращается к действию девятого шага; на тринадцатом шаге криптографический модуль БПЛА вырабатывает мастер-ключ, предназначенный для дальнейшей генерации на его основе сеансовых криптографических ключей, на основе пре-мастер-ключа, случайного числа БПЛА и случайного числа НСУ; на четырнадцатом шаге криптографический модуль НСУ вырабатывает мастер-ключ на основе пре-мастер-ключа, случайного числа БПЛА и случайного числа НСУ; на пятнадцатом шаге криптографический модуль БПЛА на основе мастер-ключа вырабатывает сеансовый ключ шифрования и сеансовый ключ вычисления имитовставки; на шестнадцатом шаге криптографический модуль НСУ на основе мастер-ключа вырабатывает сеансовый ключ шифрования и сеансовый ключ вычисления имитовставки; на семнадцатом шаге криптографический модуль БПЛА формирует тестовое сообщение, зашифрованное на выработанном сеансовом ключе шифрования, и инициирует его отправку криптографическому модулю НСУ; на восемнадцатом шаге криптографический модуль НСУ получает и расшифровывает тестовое сообщение от криптографического модуля БПЛА и проверяет его соответствие ожидаемому тестовому сообщению, при этом если тестовое сообщение не соответствует ожидаемому, то криптографический модуль НСУ считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается в режим ожидания сообщений; на девятнадцатом шаге криптографический модуль НСУ формирует ответное тестовое сообщение, зашифрованное на выработанном сеансовом ключе шифрования, и инициирует его отправку криптографическому модулю БПЛА; на двадцатом шаге криптографический модуль БПЛА получает и расшифровывает тестовое сообщение от криптографического модуля НСУ и проверяет его соответствие ожидаемому тестовому сообщению, при этом если тестовое сообщение не соответствует ожидаемому, то криптографический модуль БПЛА считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается к действию девятого шага; на двадцать первом шаге криптографический модуль БПЛА выставляет флаг готовности к работе; на двадцать втором шаге криптографический модуль НСУ выставляет флаг готовности к работе; на двадцать третьем шаге криптографический модуль БПЛА открывает порт подключения полетного контроллера; на двадцать четвертом шаге криптографический модуль НСУ открывает интерфейс обмена с программным обеспечением, осуществляющим управление БПЛА; дальнейший обмен информацией по каналам управления и телеметрии между НСУ и БПЛА ведется в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки, при этом в процессе выполнения описанной выше последовательности действий и в рамках дальнейшего обмена информацией между НСУ и БПЛА с целью дополнительной защиты радиообмена может использоваться псевдослучайная перенастройка параметров радиосвязи между БПЛА и НСУ.

2. Способ по п. 1, отличающийся тем, что: на семнадцатом шаге криптографический модуль БПЛА формирует также имитовставку тестового сообщения, вычисленную на выработанном сеансовом ключе вычисления имитовставки, и инициирует ее отправку криптографическому модулю НСУ вместе с зашифрованным тестовым сообщением;

на восемнадцатом шаге криптографический модуль НСУ получает и расшифровывает тестовое сообщение от криптографического модуля БПЛА, вычисляет на выработанном сеансовом ключе вычисления имитовставки и проверяет его имитовставку, при этом если имитовставка тестового сообщения неверна, то криптографический модуль НСУ считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается в режим ожидания сообщений; на девятнадцатом шаге криптографический модуль НСУ формирует также имитовставку ответного тестового сообщения, вычисленную на выработанном сеансовом ключе вычисления имитовставки, и инициирует ее отправку криптографическому модулю БПЛА вместе с зашифрованным ответным тестовым сообщением; на двадцатом шаге криптографический модуль БПЛА получает и расшифровывает тестовое сообщение от криптографического модуля НСУ, вычисляет на выработанном сеансовом ключе вычисления имитовставки и проверяет его имитовставку, при этом если имитовставка ответного тестового сообщения неверна, то криптографический модуль БПЛА считает, что произошла ошибка установления сеансовых криптографических ключей, и возвращается к действию девятого шага.

3. Способ по п. 1, отличающийся тем, что: до выполнения четвертого шага криптографический модуль БПЛА выполняет самотестирование, которое также может выполняться периодически по мере обмена информацией между БПЛА и НСУ через различные промежутки времени и/или через определенное количество переданных сообщений и/или по командам НСУ; до выполнения шестого шага криптографический модуль НСУ выполняет самотестирование, которое также может выполняться периодически по мере обмена информацией между БПЛА и НСУ через различные промежутки времени и/или через определенное количество переданных сообщений и/или по командам оператора НСУ.

4. Способ по п. 2, отличающийся тем, что: до выполнения четвертого шага криптографический модуль БПЛА выполняет самотестирование, которое также может выполняться периодически по мере обмена информацией между БПЛА и НСУ через различные промежутки времени и/или через определенное количество переданных сообщений и/или по командам НСУ; до выполнения шестого шага криптографический модуль НСУ выполняет самотестирование, которое также может выполняться периодически по мере обмена информацией между БПЛА и НСУ через различные промежутки времени и/или через определенное количество переданных сообщений и/или по командам оператора НСУ.

5. Способ по п. 1, отличающийся тем, что после выполнения двадцать четвертого шага данные полезной нагрузки, передаваемые с БПЛА на НСУ, также передаются в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

6. Способ по п. 2, отличающийся тем, что после выполнения двадцать четвертого шага данные полезной нагрузки, передаваемые с БПЛА на НСУ, также передаются в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

7. Способ по п. 3, отличающийся тем, что после выполнения двадцать четвертого шага данные полезной нагрузки, передаваемые с БПЛА на НСУ, также передаются в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

8. Способ по п. 4, отличающийся тем, что после выполнения двадцать четвертого шага данные полезной нагрузки, передаваемые с БПЛА на НСУ, также передаются в защищенном режиме с использованием шифрования на основе выработанного сеансового ключа шифрования и с контролем целостности на основе выработанного сеансового ключа вычисления имитовставки.

9. Способ по п. 1, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

10. Способ по п. 2, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

11. Способ по п. 3, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

12. Способ по п. 4, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

13. Способ по п. 5, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

14. Способ по п. 6, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

15. Способ по п. 7, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

16. Способ по п. 8, отличающийся тем, что криптографическая защита каналов связи между НСУ и БПЛА по указанному способу может осуществляться между одной НСУ и одновременно несколькими управляемыми с нее БПЛА.

17. Система криптографической защиты каналов связи между наземной станцией управления и беспилотным летательным аппаратом, в составе четырех компонентов, где: компонент 1 представляет собой криптографический модуль наземной станции управления (НСУ), реализующий заявляемый способ криптографической защиты каналов связи между НСУ и беспилотным летательным аппаратом (БПЛА) в части НСУ, реализованный аппаратно или программно на выделенном аппаратном устройстве, оснащенном вычислительными ресурсами, интерфейсом подключения ключевого носителя НСУ и программной или аппаратной реализацией криптографических алгоритмов, функций генерации случайных или псевдослучайных чисел и функций взаимодействия с ключевым носителем НСУ, а также возможностью инициирования передачи сообщений на БПЛА и опциональной возможностью блокирования интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА, при этом выделенное аппаратное устройство подключается в разрыв между основным вычислительным модулем НСУ и приемо-передающим устройством НСУ, которое может поддерживать псевдослучайную перенастройку параметров радиосвязи между БПЛА и НСУ; компонент 2 представляет собой криптографический модуль БПЛА, реализующий заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, реализованный аппаратно или программно на выделенном аппаратном устройстве, оснащенном вычислительными ресурсами,

фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА и программной или аппаратной реализацией криптографических алгоритмов, функций генерации случайных или псевдослучайных чисел и функций взаимодействия с ключевым носителем БПЛА, а также возможностью инициирования передачи сообщений на НСУ и опциональной возможностью блокирования порта подключения полетного контроллера БПЛА к каналам связи, при этом выделенное аппаратное устройство подключается в разрыв между полетным контроллером БПЛА и приемо-передающим устройством БПЛА, которое может поддерживать псевдослучайную перенастройку параметров радиосвязи между БПЛА и НСУ; компонент 3 представляет собой ключевой носитель НСУ, оснащенный вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями; компонент 4 представляет собой ключевой носитель БПЛА, оснащенный вычислительными ресурсами и энергонезависимой памятью, а также криптографическими функциями.

18. Система по п. 17, в которой компонент 1 представляет собой криптографический модуль НСУ, реализующий заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части НСУ, реализованный программно и выполняющийся непосредственно на основном вычислительном модуле НСУ, оснащенном интерфейсом подключения ключевого носителя НСУ, при этом программная реализация криптографического модуля НСУ включает в себя реализацию криптографических алгоритмов, включая алгоритмы генерации псевдослучайных чисел, или функций использования криптографических алгоритмов, включая алгоритмы генерации случайных или псевдослучайных чисел, реализованных аппаратно в основном вычислительном модуле НСУ, а также реализацию функций взаимодействия с ключевым носителем НСУ, инициирования передачи сообщений на БПЛА и (опционально) блокирования интерфейса обмена с программным обеспечением, осуществляющим управление БПЛА.

19. Система по п. 17, в которой компонент 2 представляет собой криптографический модуль БПЛА, реализующий заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, реализованный программно и выполняющийся непосредственно на полетном контроллере БПЛА, при этом БПЛА оснащен фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА, а программная реализация криптографического модуля БПЛА включает в себя реализацию криптографических алгоритмов, включая алгоритмы генерации псевдослучайных чисел, или функций использования криптографических алгоритмов, включая алгоритмы генерации случайных или псевдослучайных чисел, реализованных аппаратно в комплексе бортового оборудования БПЛА, а также реализацию функций взаимодействия с ключевым носителем БПЛА, инициирования передачи сообщений на НСУ и (опционально) блокирования порта подключения полетного контроллера БПЛА к каналам связи.

20. Система по п. 18, в которой компонент 2 представляет собой криптографический модуль БПЛА, реализующий заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, реализованный программно и выполняющийся непосредственно на полетном контроллере БПЛА, при этом БПЛА оснащен фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА, а программная реализация криптографического модуля БПЛА включает в себя реализацию криптографических алгоритмов, включая алгоритмы генерации псевдослучайных чисел, или функций использования криптографических алгоритмов, включая алгоритмы генерации случайных или псевдослучайных чисел, реализованных

аппаратно в комплексе бортового оборудования БПЛА, а также реализацию функций взаимодействия с ключевым носителем БПЛА, инициирования передачи сообщений на НСУ и (опционально) блокирования порта подключения полетного контроллера БПЛА к каналам связи.

21. Система по п. 17, отличающаяся тем, что в ее составе: компонентов 2 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ; компонентов 4 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ.

22. Система по п. 18, отличающаяся тем, что в ее составе: компонентов 2 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ; компонентов 4 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ.

23. Система по п. 19, отличающаяся тем, что в ее составе: компонентов 2 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ; компонентов 4 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ.

24. Система по п. 20, отличающаяся тем, что в ее составе: компонентов 2 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ; компонентов 4 может быть несколько в соответствии с количеством БПЛА, управление которыми осуществляется одновременно с одной НСУ.

25. Система по п. 21, отличающаяся тем, что в ее составе некоторое количество криптографических модулей БПЛА (компонентов 2), реализующих заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, может быть реализовано аппаратно или программно на выделенных аппаратных устройствах, каждое из которых оснащено вычислительными ресурсами, фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА и программной или аппаратной реализацией криптографических алгоритмов и функций взаимодействия с ключевым носителем БПЛА, а также возможностью инициирования передачи сообщений на НСУ и опциональной возможностью блокирования порта подключения полетного контроллера БПЛА к каналам связи, при этом каждое из выделенных аппаратных устройств подключается в разрыв между полетным контроллером БПЛА и приемо-передающим устройством БПЛА, тогда как оставшееся количество криптографических модулей БПЛА, реализующих заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, реализовано программно и выполняется непосредственно на полетных контроллерах БПЛА, при этом каждый из БПЛА оснащен фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА, а программная реализация криптографического модуля БПЛА включает в себя реализацию криптографических алгоритмов, включая алгоритмы генерации псевдослучайных чисел, или функций использования криптографических алгоритмов, включая алгоритмы генерации случайных или псевдослучайных чисел, реализованных аппаратно в комплексе бортового оборудования БПЛА, а также реализацию функций взаимодействия с ключевым носителем БПЛА, инициирования передачи сообщений на НСУ и (опционально) блокирования порта подключения полетного контроллера БПЛА к каналам связи.

26. Система по п. 22, отличающаяся тем, что в ее составе некоторое количество криптографических модулей БПЛА (компонентов 2), реализующих заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, может быть реализовано аппаратно или программно на выделенных аппаратных устройствах, каждое из которых оснащено вычислительными ресурсами, фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА и программной или аппаратной реализацией криптографических алгоритмов и функций взаимодействия с ключевым носителем БПЛА, а также возможностью инициирования передачи сообщений на НСУ и опциональной возможностью блокирования порта подключения полетного контроллера БПЛА к каналам связи, при этом каждое из выделенных аппаратных устройств подключается в разрыв между полетным контроллером БПЛА и приемо-передающим устройством БПЛА, тогда как оставшееся количество криптографических модулей БПЛА, реализующих заявляемый способ криптографической защиты каналов связи между НСУ и БПЛА в части БПЛА, реализовано программно и выполняется непосредственно на полетных контроллерах БПЛА, при этом каждый из БПЛА оснащен фиксированным или съемным интерфейсом подключения ключевого носителя БПЛА, а программная реализация криптографического модуля БПЛА включает в себя реализацию криптографических алгоритмов, включая алгоритмы генерации псевдослучайных чисел, или функций использования криптографических алгоритмов, включая алгоритмы генерации случайных или псевдослучайных чисел, реализованных аппаратно в комплексе бортового оборудования БПЛА, а также реализацию функций взаимодействия с ключевым носителем БПЛА, инициирования передачи сообщений на НСУ и (опционально) блокирования порта подключения полетного контроллера БПЛА к каналам связи.

27. Система по п. 21, отличающаяся тем, что в ее составе криптографических модулей НСУ (компонентов 1) может быть несколько, при этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

28. Система по п. 22, отличающаяся тем, что в ее составе криптографических модулей НСУ (компонентов 1) может быть несколько, при этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

29. Система по п. 23, отличающаяся тем, что в ее составе криптографических модулей НСУ (компонентов 1) может быть несколько, при этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

30. Система по п. 24, отличающаяся тем, что в ее составе криптографических модулей НСУ (компонентов 1) может быть несколько, при этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

31. Система по п. 25, отличающаяся тем, что в ее составе криптографических модулей НСУ (компонентов 1) может быть несколько, при этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

32. Система по п. 26, отличающаяся тем, что в ее составе криптографических модулей НСУ (компонентов 1) может быть несколько, при этом программное обеспечение НСУ может включать в себя реализацию механизмов статической или динамической балансировки нагрузки между криптографическими модулями НСУ.

33. Система по п. 17, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевого носителя БПЛА и ключевого носителя НСУ.

34. Система по п. 18, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевого носителя БПЛА и ключевого носителя НСУ.

35. Система по п. 19, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевого носителя БПЛА и ключевого носителя НСУ.

36. Система по п. 20, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевого носителя БПЛА и ключевого носителя НСУ.

37. Система по п. 21, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

38. Система по п. 22, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

39. Система по п. 23, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

40. Система по п. 24, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

41. Система по п. 25, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

42. Система по п. 26, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

43. Система по п. 27, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

44. Система по п. 28, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

45. Система по п. 29, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

46. Система по п. 30, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

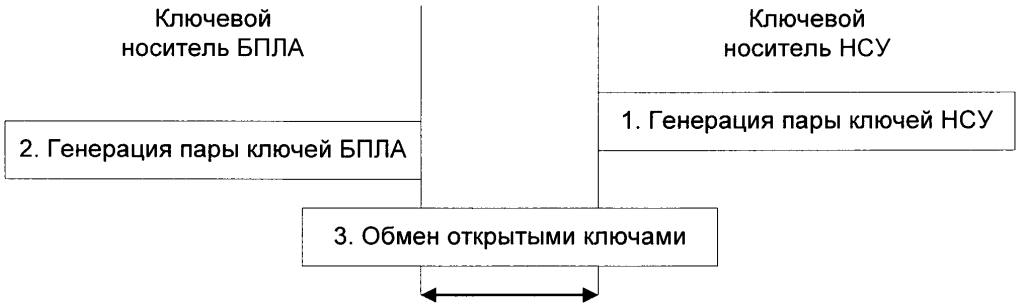
47. Система по п. 31, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

48. Система по п. 32, отличающаяся тем, что в состав системы входит компонент 5, представляющий собой ключевой центр, обеспечивающий централизованную генерацию криптографических ключей и подготовку ключевых носителей БПЛА и ключевого носителя НСУ.

49. Устройство криптографической защиты каналов связи между наземной станцией управления и беспилотным летательным аппаратом, выполненное на общей плате и содержащее пять элементов, где: элемент 1 представляет собой управляющий микроконтроллер, включающий в свой состав следующие программные функциональные модули, выполняющиеся на управляющем микроконтроллере в процессе работы устройства: модуль управления, осуществляющий управление остальными элементами устройства и программными модулями, выполняющимися на управляющем микроконтроллере, а также взаимодействие между ними; модуль обеспечения конфиденциальности и целостности информационного обмена, обеспечивающий защиту информационного обмена между беспилотным летательным аппаратом (БПЛА) и наземной станцией управления (НСУ) путем шифрования сообщений и осуществления контроля их целостности и включающий в себя реализации используемых криптографических алгоритмов и режимов их работы, в том числе для использования другими программными модулями; модуль аутентификации и установления защищенного соединения, обеспечивающий выполнение последовательности действий по аутентификации сторон информационного обмена и установлению защищенного соединения между БПЛА и НСУ, предусмотренной заявляемым способом криптографической защиты каналов связи между НСУ и БПЛА, причем выполнение данной последовательности может осуществляться во взаимодействии с другими элементами устройства в части их функциональных возможностей; модуль генерации и обработки ключевой информации, обеспечивающий выполнение преобразований над криптографическими ключами, включая вычисление производных ключей (в том числе вычисление мастер-ключа на основе пре-мастер-ключа) и диверсификацию ключей (в том числе вычисление ключа шифрования и ключа вычисления имитовставки на основе мастер-ключа), а также инициирование выполнения ключевым носителем функций по генерации ключей (генерации пар асимметричных ключей и вычисления общего секретного пре-мастер-ключа) и функций записи ключей на ключевой носитель и чтения ключей с ключевого носителя; модуль генерации случайных или псевдослучайных чисел, обеспечивающий генерацию случайных чисел на основе недетерминированных физических процессов или псевдослучайных чисел на основе детерминированных алгоритмов (в том числе криптографических), а также (опционально) выполнение процедур контроля генерируемых случайных или псевдослучайных чисел на соответствие

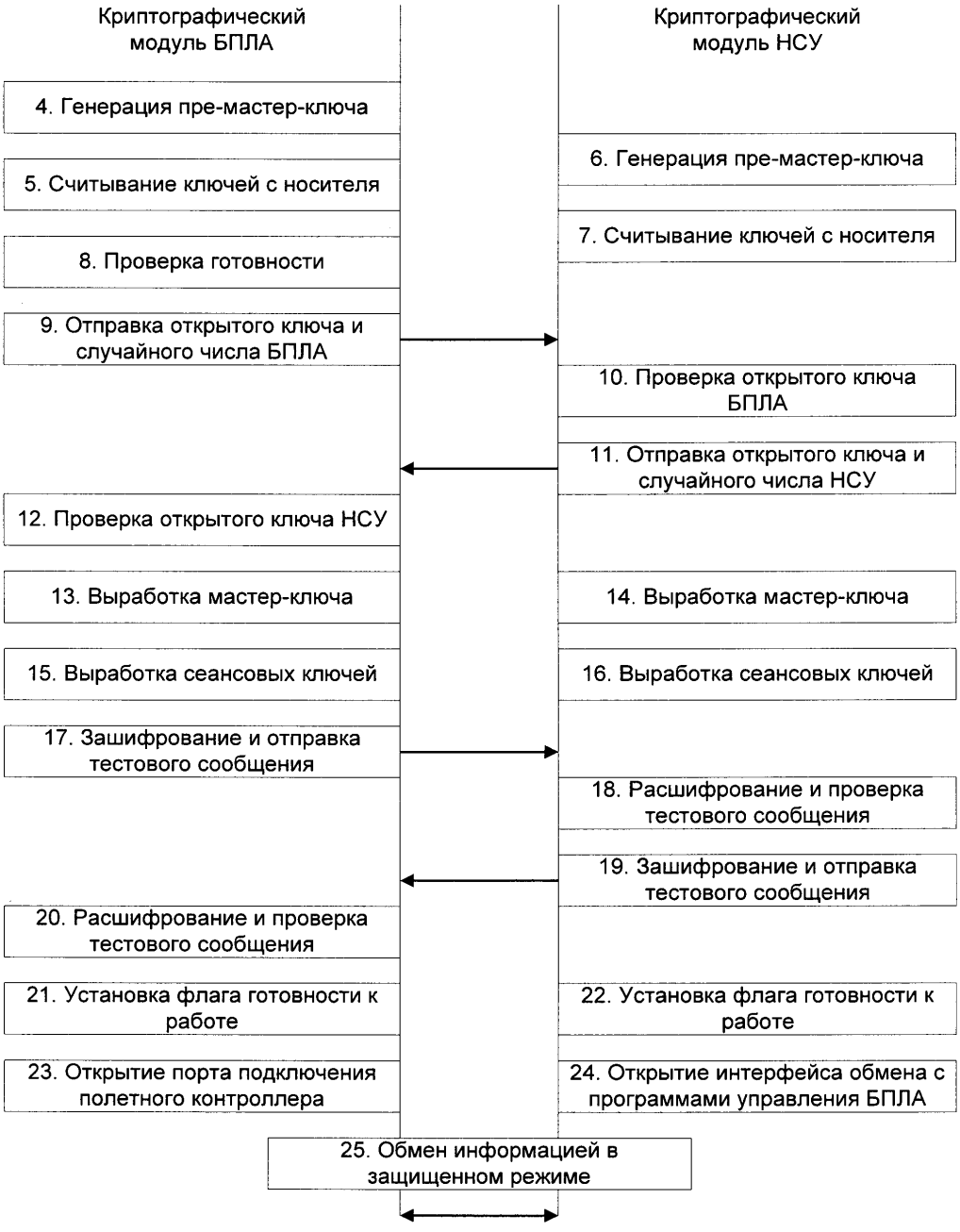
критериям случайности, причем генерация псевдослучайных чисел на основе криптографических алгоритмов выполняется данным модулем во взаимодействии с модулем обеспечения конфиденциальности и целостности информационного обмена, а для инициализации и (при необходимости) переинициализации процесса генерации псевдослучайных чисел может использоваться случайная величина, получаемая от внешнего источника, в том числе ключевого носителя; модуль взаимодействия с ключевым носителем, обеспечивающий передачу (через интерфейс взаимодействия с ключевым носителем) ключевому носителю команд, инициированных другими программными модулями, а также обработку ответов на команды, получаемых от ключевого носителя, и передачу получаемых от ключевого носителя данных инициировавшему команды модулю; модуль взаимодействия с приемо-передающим устройством, обеспечивающий передачу информации (через интерфейс взаимодействия с приемо-передающим устройством) приемо-передающему устройству и прием и обработку информации, получаемой от приемо-передающего устройства, а также (опционально) блокировку и разблокировку приемо-передающего устройства при необходимости; опциональный модуль самотестирования устройства, обеспечивающий выполнение процедур самотестирования устройства, которое может осуществляться как при старте устройства, так и периодически в процессе его работы; опциональный модуль контроля целостности программного обеспечения, обеспечивающий контроль целостности остальных программных модулей устройства; элемент 2 представляет собой энергонезависимую память для долговременного хранения программных модулей, выполняющихся на элементе 1; элемент 3 представляет собой интерфейс подключения к внешнему вычислительному устройству; элемент 4 представляет собой интерфейс взаимодействия с ключевым носителем; элемент 5 представляет собой интерфейс взаимодействия с приемо-передающим устройством.

1


Ключевой носитель БПЛА
Ключевой носитель НСУ
1. Генерация пары ключей НСУ
2. Генерация пары ключей БПЛА
3. Обмен открытыми ключами

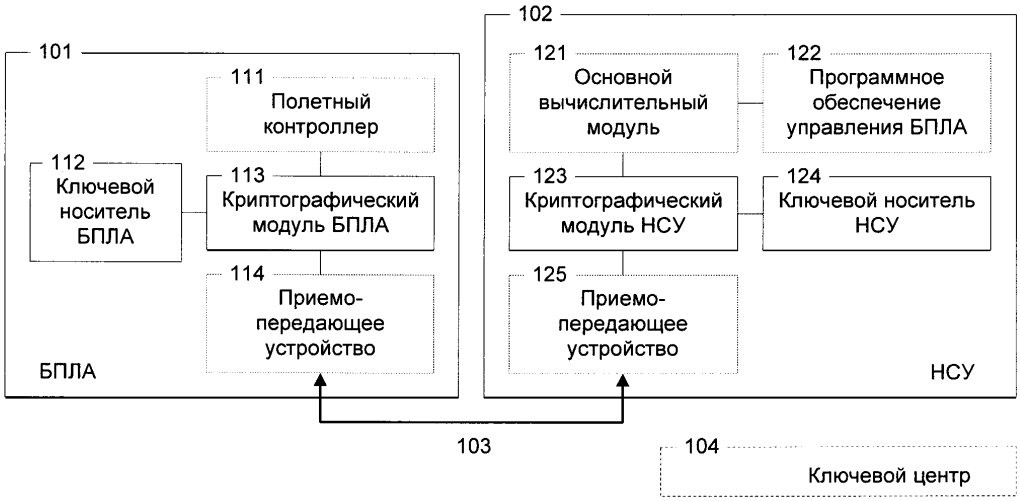
Фиг. 1

2

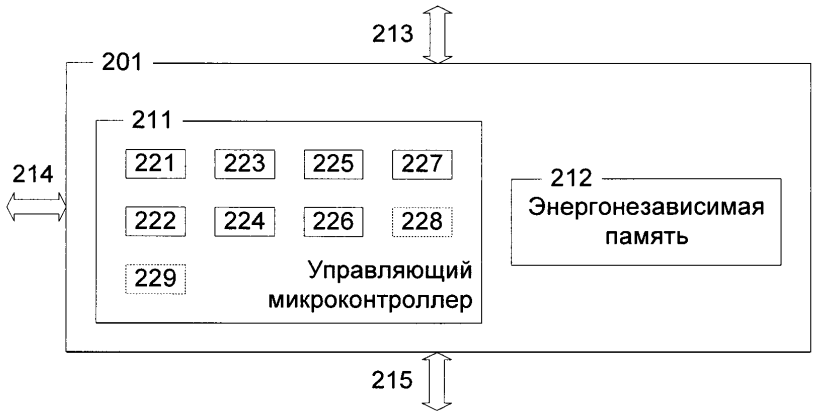

Криптографический модуль БПЛА
Криптографический модуль НСУ
4. Генерация пре-мастер-ключа
6. Генерация пре-мастер-ключа
5. Считывание ключей с носителя
7. Считывание ключей с носителя
8. Проверка готовности
9. Отправка открытого ключа и случайного числа БПЛА
10. Проверка открытого ключа БПЛА
11. Отправка открытого ключа и случайного числа НСУ
12. Проверка открытого ключа НСУ
13. Выработка мастер-ключа
14. Выработка мастер-ключа
15. Выработка сеансовых ключей
16. Выработка сеансовых ключей
17. Зашифрование и отправка тестового сообщения
18. Расшифрование и проверка тестового сообщения
19. Зашифрование и отправка тестового сообщения
20. Расшифрование и проверка тестового сообщения
21. Установка флага готовности к работе
22. Установка флага готовности к работе
23. Открытие порта подключения полетного контроллера
24. Открытие интерфейса обмена с программами управления БПЛА
25. Обмен информацией в защищенном режиме

Фиг. 2

3


101
111
Полетный контроллер
112
Ключевой носитель БПЛА
113
Криптографический модуль БПЛА
114
Приемо-передающее устройство
БПЛА
102
121
Основной вычислительный модуль
122
Программное обеспечение управления БПЛА
123
Криптографический модуль НСУ
124
Ключевой носитель НСУ
125
Приемо-передающее устройство
НСУ
103
104
Ключевой центр

Фиг. 3


213
201
211
221
223
225
227
222
224
226
228
229
Управляющий микроконтроллер
214
212
Энергонезависимая память
215

Фиг. 4