ООО Фирма «АНКАД»

УТВЕРЖДЕН

КБДЖ.01384-01 13 01 - ЛУ

Комплекс программного обеспечения шифратора БПЛА

Шифратор БПЛА

Описание программы

КБДЖ. 01384-01 13 01

Листов 28

2018 г

Подп. и дата	
Инв.№ дубл.	
Взам. инв.№	
Подп. и дата	
Инв.№ дубл.	

Аннотация

Настоящий документ содержит сведения о внутренней организации и логике работы программного обеспечения защиты (ПОЗ) беспилотных летательных аппаратов (БПЛА). Шифратор БПЛА предназначен для оперативной криптографической защиты командно-телеметрической радиолинии между наземной станцией управления (НСУ) и БПЛА. Шифратор БПЛА может функционировать на базе программного шифратора или на базе аппаратного шифратора. Отличия в работе Шифратора БПЛА программного и аппаратного шифратора приведены в данном документе. Приведена подробная информация о структуре защищенного комплекса управления БПЛА, приведены этапы подготовки комплекса к штатной эксплуатации. Также в документе дана подробная информация о входных, выходных данных, способе обмена данными между Шифратором БПЛА и другими программными и аппаратными компонентами и о технических средствах, необходимых для штатного функционирования Шифратора БПЛА.

Оглавление

Перечень сокращений

АРМ	—	автоматизированное рабочее место;
ОЗУ	—	оперативное запоминающее устройство;
НСУ	—	наземная станция управления;
ПО	—	программное обеспечение;
ПЗУ	—	постоянно запоминающее устройство;
ППУ	—	приемо-передающее устройство;
CBC	—	Cipher Block Chaining (режим зацепления по шифртексту);
FHSS	—	Frequency-hopping Spread Spectrum (псевдослучайная перестройка рабочей частоты);
HMAC	—	Keyed-Hash Message Authentication Code (хэш-код аутентификации сообщений);
KDF	—	Key Derivation Function (функция формирования ключа);
MAC	—	Message Authentication Code (уникальный код аутентификации или имитовставка сообщения);
MAVLink	—	Micro Air Vehicle Link (протокол обмена данными в инфраструктуре БПЛА);
RTOS	—	Real Time Operation System (операционная система реального времени);
TLS	—	Transport Layer Security (криптографический протокол передачи данных для транспортного уровня);
UART	—	Universal Asynchronous Receiver-Transmitter (универсальный асинхронный приёмопередатчик);
USB	—	Universal Serial Bus (универсальная последовательная шина);

1. Общие сведения

1.1 Наименование, назначение и область применения

Комплекс программного обеспечения шифратора БПЛА (Шифратор БПЛА) является разработкой ООО Фирма «АНКАД». Шифратор БПЛА разрабатывается в рамках НИОКР по теме «Исследование и разработка алгоритмов и протоколов обеспечения защищенной передачи данных в рамках информационного обмена беспилотных авиационных систем между собой и с наземной инфраструктурой».

Шифратор БПЛА предназначен для обеспечения оперативной криптографической защиты радиолинии и наземной станцией управления (НСУ). Шифратор БПЛА не предназначен для применения в качестве самостоятельного программного обеспечения. Шифратор БПЛА функционирует в составе программного средства защиты (программного шифратора) или программно-аппаратного средства защиты (аппаратного шифратора).

Программный шифратор функционирует на аппаратной платформе НСУ. Также в аппаратную часть НСУ может встраиваться аппаратный шифратор с встроенным в него ПО Шифратора БПЛА. В составе БПЛА функционирует только аппаратный шифратор с встроенным ПО Шифратора БПЛА.

1.2 Язык программирования и среда разработки

Шифратор БПЛА разрабатывался с применением языка C/C++. ПО Шифратора БПЛА применяется как в программном так и в аппаратном шифраторе.

Программный шифратор

Программный шифратор представляет собой ПО Шифратора БПЛА с интерфейсной пользовательской надстройкой. Пользовательский интерфейс разработан с помощью библиотек Qt5.

Программный шифратор предназначен для работы только в составе НСУ. Программный шифратор предназначен для функционирования на компьютере, работающем под операционными системами:

- ОС семейства deb-based linux;

– ОС Windows-7 и выше.

Программный шифратор для ОС семейства deb-based linux

Среда разработки программного шифратора под ОС семейства deb-based linux – Qt Creator. Для успешной сборки на компьютер должны быть установлены следующие программные компоненты:

– cryptec – проприетарная библиотека криптографических функций ООО Фирма «АНКАД»;
– mavlink v2 – библиотека функций для протокола MAVlink, сгенерированная для языка C/C++;
– mavlink-crypto-helper – надстройка над библиотекой mavlink разработки ООО Фирма «АНКАД», которая осуществляет конвертирование данных и их криптографическую защиту с помощью библиотеки cryptec;
– libpcsclite1-dev – пакет для сборки драйвера для подключения к смарт-картам через PC/SC;
– qt5-dev-tools, libqt5-dev, libqt5-core – dev-пакеты для qt;
– cmake (версии не ниже 3.7) – кроссплатформенная система автоматизации сборки ПО;
– gcc – набор компиляторов.

В среде разработки Qt Creator создается исполняемый файл, который является программным шифратором со встроенным ПО Шифратора БПЛА для ОС семейства deb-based linux.

Программный шифратор для ОС Windows-7 и выше

Среда разработки программного шифратора под ОС Windows-7 и выше – Qt Creator и Visual Studio 2015. Для успешной сборки на компьютер должны быть установлены следующие программные компоненты:

– cryptec – проприетарная библиотека криптографических функций ООО Фирма «АНКАД»;

- mavlink v2 – библиотека функций для протокола MAVlink, сгенерированная для языка C/C++;
- mavlink-crypto-helper – надстройка над библиотекой mavlink разработки ООО Фирма «АНКАД», которая осуществляет конвертирование данных и их криптографическую защиту с помощью библиотеки cryptec.

В среде разработки Visual Studio 2015 делается подготовка библиотек cryptec, mavlink v2, mavlink-crypto-helper для дальнейшей сборки исполняемого файла в среде Qt Creator. В среде разработки Qt Creator создается исполняемый файл с расширением .exe, который является программным шифратором со встроенным ПО Шифратора БПЛА для ОС Windows-7 и выше.

Аппаратный шифратор

Аппаратный шифратор реализуется на основе микроконтроллера STM32F7. Аппаратный шифратор предназначен для применения в НСУ и в БПЛА. Для применения в БПЛА подходит только аппаратный шифратор.

Шифратор БПЛА, функционирующий на базе микроконтроллера STM32F7, представляет собой прошивку для данного микроконтроллера. Прошивка аппаратного шифратора создается в среде разработки IAR Embedded Workbench IDE 8.11.3. Для успешной сборки прошивки на компьютер должны быть установлены следующие программные компоненты:

- cryptec – проприетарная библиотека криптографических функций ООО Фирма «АНКАД»;
- mavlink v2 – библиотека функций для протокола MAVlink, сгенерированная для языка C/C++;
- mavlink-crypto-helper – надстройка над библиотекой mavlink разработки ООО Фирма «АНКАД», которая осуществляет конвертирование данных и их криптографическую защиту с помощью библиотеки cryptec;
- Free RTOS v.10.0.0 – исходные коды ядра операционной системы реального времени Free RTOS.

Функции Шифратора БПЛА встраиваются в ОС Free RTOS. В среде разработки IAR Embedded Workbench IDE 8.11.3 создается единый файл прошивки с расширением *.bin, который при запуске микроконтроллера запускает ОС Free RTOS, которая в свою очередь запускает функции Шифратора БПЛА.

Программа для прошивки микроконтроллера - STM32 ST-LINK Utility. После прошивки микроконтроллера аппаратный шифратор считается готовым к началу эксплуатации.

1.3 Программное обеспечение необходимое для функционирования программы

Программный шифратор

Программный шифратор функционирует на компьютерах под управлением ОС семейства deb-based linux или Windows-7 и выше. Компьютер, на котором запускается Шифратор БПЛА должен обладать следующими техническими характеристиками:

- Процессор— 2 ядра или больше, тактовая частота на одно ядро минимум 1,8 GHz;
- Оперативная память (RAM) — не менее 2 Гб;
- Жесткий диск (HDD/SSD) — минимум 100 Мб свободного места.

Для полнофункциональной работы ПО Шифратора БПЛА, написанного под ОС семейства deb-based linux, на компьютере должны быть установлены следующие программные компоненты:

- pcscd – фоновый процесс (демон), предназначенный для подключения смарт-картам через PC/SC;
- libpcsclite1 – промежуточное ПО (библиотека) для доступа к смарт-картам через PC/SC;
- libccid – библиотека-драйвер, поддерживающая USB CCID устройства через PC/SC;
- модули qml и serialport – модули системы qt5;

– tty0tty –программный драйвер виртуальных COM-портов, соединенных нуль модемным кабелем для linux.

Для полнофункциональной работы ПО Шифратора БПЛА, написанного под ОС Windows 7, на компьютере должны быть установлены следующие программные компоненты:

– модули qml и serialport – модули системы разработки qt5;
– com0com – программный драйвер виртуальных COM-портов, соединенных нуль модемным кабелем для Windows.

Аппаратный шифратор

ПО Шифратора БПЛА, разработанное для аппаратного шифратора, функционирует на базе ОС FreeRTOS. ПО Шифратора БПЛА интегрировано в ОС FreeRTOS в единой прошивке.

ОС FreeRTOS с встроеннам Шифратором БПЛА предназначен для работы на микроконтроллера STM32F7. Минимальное количество свободной оперативной памяти, которое должно присутствовать в микроконтроллере, составляет 200 Кбайт.

2. Функциональное назначение

Шифратор БПЛА предназначен для обеспечения оперативной криптографической защиты радиолинии между БПЛА и наземной станцией управления (НСУ). Шифратор БПЛА не предназначен для применения в качестве самостоятельного программного обеспечения. Шифратор БПЛА функционирует в составе программного или аппаратного шифратора. Программный и аппаратный шифратор предназначены для защиты командно-телеметрической радиолинии обмена данными между БПЛА и НСУ.

Программный шифратор представляет собой исполняемый модуль, запускаемый на аппаратной платформе НСУ. Программный шифратор состоит из ПО Шифратора БПЛА и пользовательского интерфейса, с помощью которого оператор НСУ может вызывать функции Шифратора БПЛА. Программный шифратор подключается к аппаратному последовательному порту USB или UART, к которому подключается приемо-передающее

устройство (ППУ). Также программный шифратор подключается к порту USB для связи со считывателем смарт-карт. Считыватель смарт-карт применяется для подключения к шифратору ключевого носителя для записи начальной ключевой информации.

К программе управления полетами программный шифратор подключается через один из пары виртуальных портов, соединенных нуль модемным кабелем с помощью специализированного драйвера (tty0tty для linux-систем, com0com для ОС Windows). Драйвер создает пары связанных виртуальных COM-портов, позволяющих осуществлять подключение пары программ к одному физическому соединению, что при стандартном использовании не возможно, ввиду того что процедуры операционной системы позволяют занимать свободный порт только одной программе одновременно. В качестве программы управления полетами используется свободно распространяемая программа QGroundControl. В качестве программы управления полетами может применяться любая другая программа, осуществляющая взаимодействие с БПЛА по протоколу MAVLink.

Аппаратный шифратор представляет собой законченное изделие, выполненное на одной плате. Центральным вычислительным элементом, на котором запускается ПО Шифратора БПЛА, является микроконтроллер STM32F746. В аппаратном шифраторе оно интегрировано в ОС FreeRTOS. После запуска и начальной инициализации микроконтроллера загружается FreeRTOS, которая вызывает функции Шифратора БПЛА.

Аппаратный шифратор может применяться как в составе НСУ, так и в составе БПЛА. В конструкции БПЛА должно быть предусмотрено место для монтирования аппаратного шифратора.

Аппаратный шифратор включается в разрыв между портом USB/UART и ППУ на НСУ или в разрыв между полетным контроллером и ППУ на БПЛА.

Внедрение аппаратного шифратора в структуру БПЛА не ухудшает его эксплуатационные характеристики.

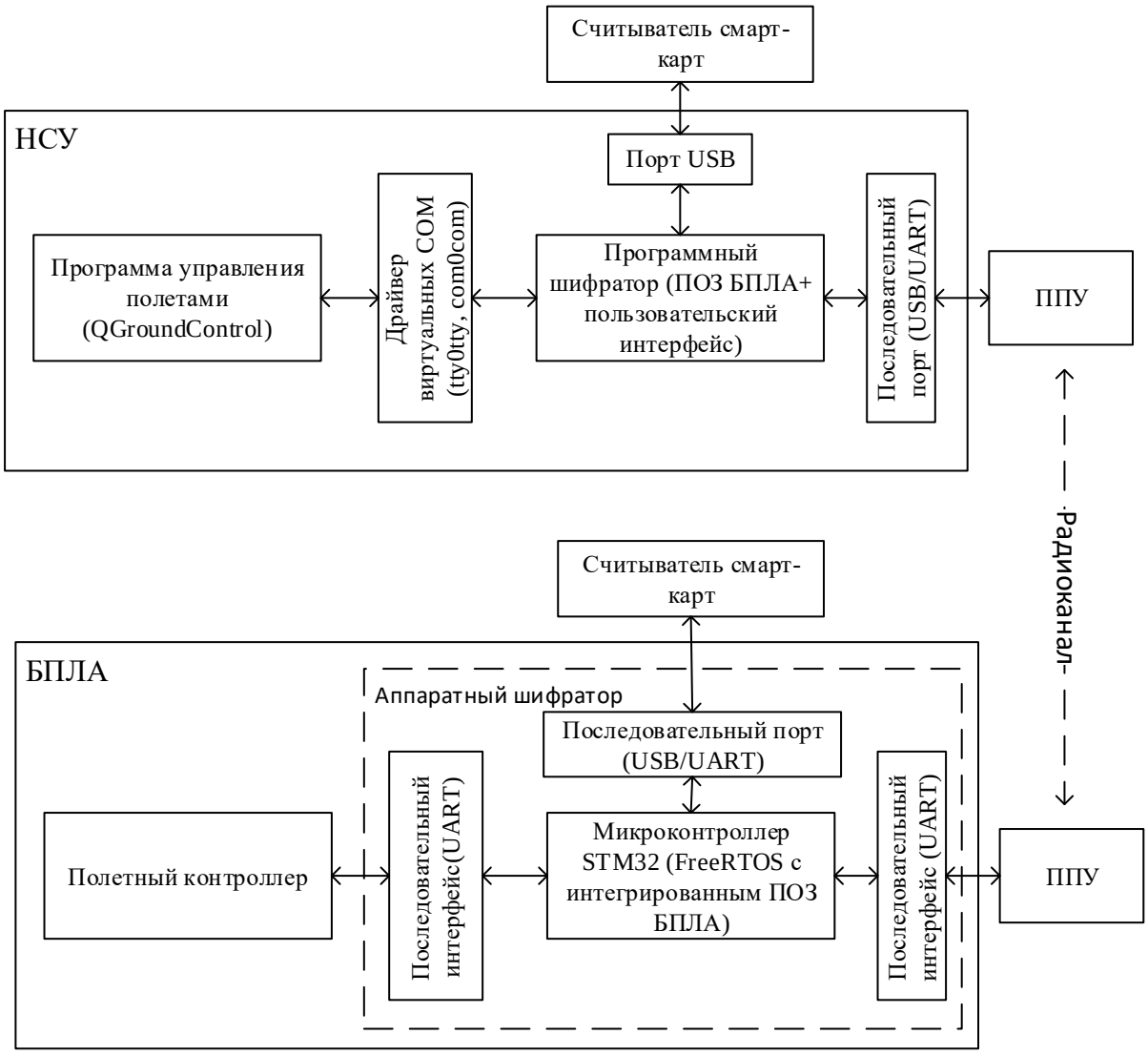
Аппаратный шифратор имеет физические разъемы для подключения ППУ, считывателя смарт-карт и стыковки либо с последовательным интерфейсом НСУ либо с полетным контроллером БПЛА. В состав Шифратора БПЛА входят драйвера последовательных интерфейсов USB/UART.

Оба шифратора, программный и аппаратный, осуществляют:

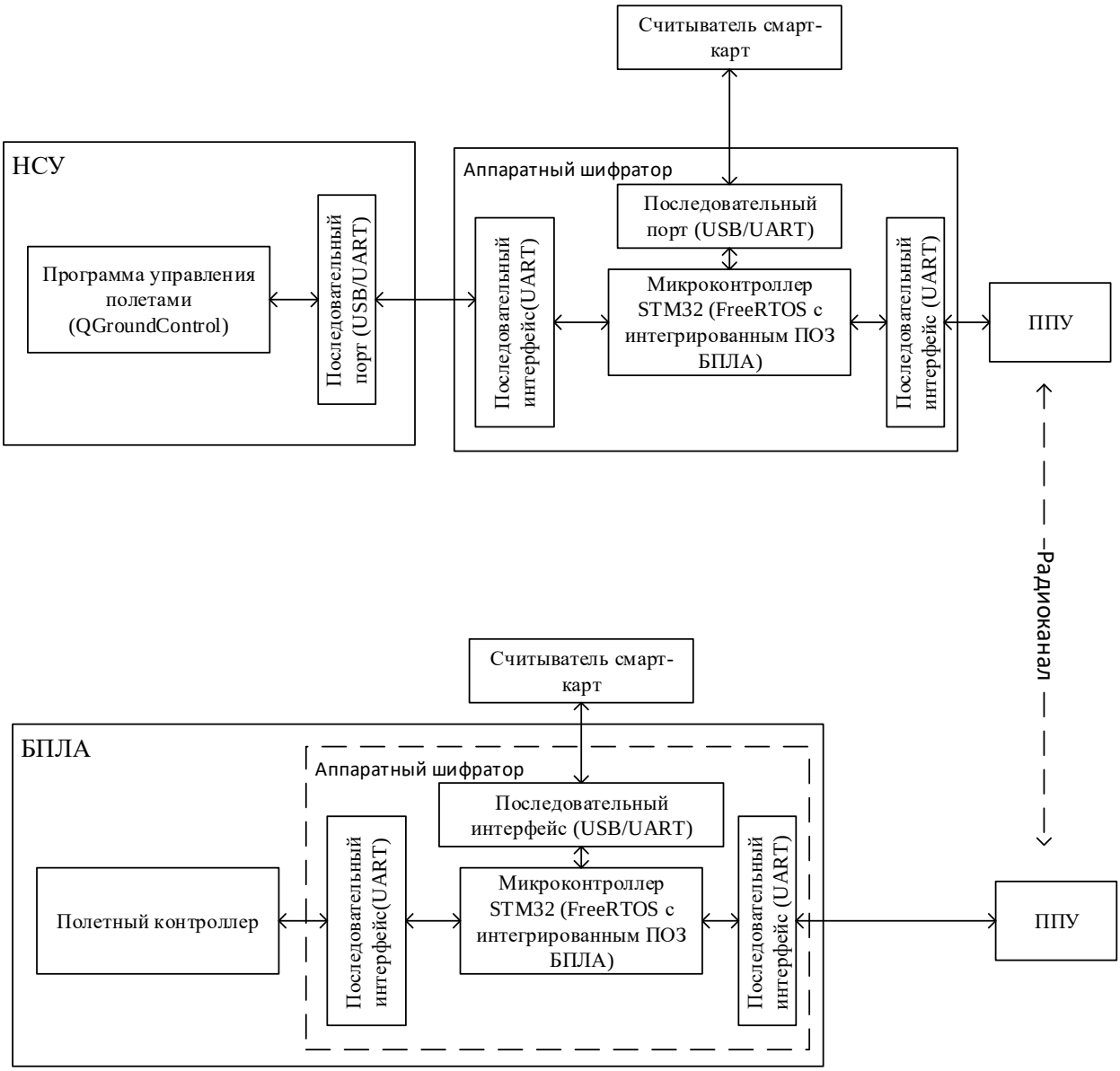
- взаимную аутентификацию НСУ и БПЛА;
- загрузку начальной ключевой информации;
- генерацию сеансовой ключевой информации;
- шифрование сообщений, генерируемых полетным контроллером и программой управления полетами по протоколу MAVLink;
- защиту целостности сообщений, генерируемых полетным контроллером и программой управления полетами по протоколу MAVLink;
- смену сеансовых ключей для каждого пакета на основе номера данного пакета.

Аппаратный шифратор дополнительно производит проверку целостности прошивки при старте микроконтроллера.

Схема подключения шифраторов и организации защищенной инфраструктуры БПЛА показана на рисунке 1.


Считыватель смарт-карт
НСУ
Порт USB
Драйвер виртуальных COM (tty0tty, com0com)
Программный шифратор (ПОЗ БПЛА+ пользовательский интерфейс)
Последовательный порт (USB/UART)
ППУ
Программа управления полетами (QGroundControl)
Радиоканал
Считыватель смарт-карт
БПЛА
Аппаратный шифратор
Последовательный порт (USB/UART)
Последовательный интерфейс(UART)
Микроконтроллер STM32 (FreeRTOS с интегрированным ПОЗ БПЛА)
Последовательный интерфейс (UART)
Полетный контроллер
ППУ

а)



б)

Рисунок 1 – Схема организации защищенной инфраструктуры БПЛА; а) В НСУ используется программный шифратор, в БПЛА – аппаратный шифратор; б) В НСУ и в БПЛА используются аппаратные шифраторы.

При установке шифраторов должен быть обеспечен свободный доступ к интерфейсам подключения считывателей смарт-карт. Подключение считывателей смарт-

карт производится каждый раз при предполетной подготовке и отключение после загрузки начальных ключей и установки соединения.

До запуска криптографических функций необходимо провести многофакторную взаимную аутентификацию и генерацию сеансовых ключей. Для этого требуется подключить к шифратору на стороне НСУ и к шифратору на стороне БПЛА считыватель смарт-карт с микропроцессором. Смарт-карты генерируют открытые ключи, производится обмен этими ключами между сторонами по открытому радиоканалу посредством шифраторов, после этого микроконтроллер шифратора производит генерацию сеансовых мастер-ключей. После генерации и загрузки в шифраторы сеансовых мастер-ключей считыватель смарт-карт может быть отключен от шифраторов.

После успешной аутентификации производится псевдо случайная настройка параметров работы приемо-передающего устройства в целях сеансовой смены сетки рабочих частот скачкообразной перестройки частоты FHSS (или иных параметров) и устанавливается защищенное соединения между управляющими компонентами БПЛА и НСУ, производится инициализация и запуск всех систем БПЛА. Дальнейший процесс управления и мониторинга за состоянием БПЛА производится при помощи штатных аппаратных и программных средств, применимых в данной инфраструктуре.

Шифратор БПЛА настроен для применения в конкретном аппаратно-программном окружении, описанном выше. Для применения ПО Шифратора БПЛА в других аппаратных конфигурациях необходима адаптация ПО Шифратора БПЛА под заданное программно-аппаратное окружение.

3. Описание логической структуры программы

3.1 Структура программы и описание функций составных частей

Шифратор БПЛА содержит программные модули, которые реализуют все функциональные задачи криптографической защиты радиолинии между НСУ и БПЛА. В состав программных модулей входят:

- Блок аутентификации участников информационного обмена;
- Блок генерации и распределения ключевой информации;
- Блок обеспечения конфиденциальности информационного обмена;
- Блок обработки данных последовательного порта;
- Блоки работы с параметрами приемо-передающего устройства;
- Блок обеспечения целостности компонентов модуля.

Блок обеспечения аутентификации участников информационного обмена используется для обмена открытыми ключами, сгенерированными микропроцессором на смарт-карте посредством их приема по интерфейсу подключения считывателя и отправки посредством блока обработки данных последовательного порта.

Блок генерации и распределения ключевой информации используется для приема с смарт-карты по интерфейсу подключения считывателя начальной ключевой информации и генерации сеансовых ключей для использования в блоке обеспечения конфиденциальности информационного обмена.

Блок обеспечения конфиденциальности информационного обмена используется для выполнения шифрования сообщений и просчета имитовставки. Процедуры шифрования и просчета имитовставки зависят от счетчика пакетов.

Блок обработки данных последовательного порта используется для приема и отправки пакетных сообщений.

Блок работы с параметрами приемо-передающего устройства используется для индивидуальной настройки параметров каждого из приемо-передающих устройств с целью смены параметров работы канала передачи данных для каждого сеанса.

Блок обеспечения целостности компонентов используется для проверки целостности программного обеспечения перед его непосредственным запуском с целью контроля неизменности программного обеспечения.

Логическая структура программы приведена на рисунке 2.

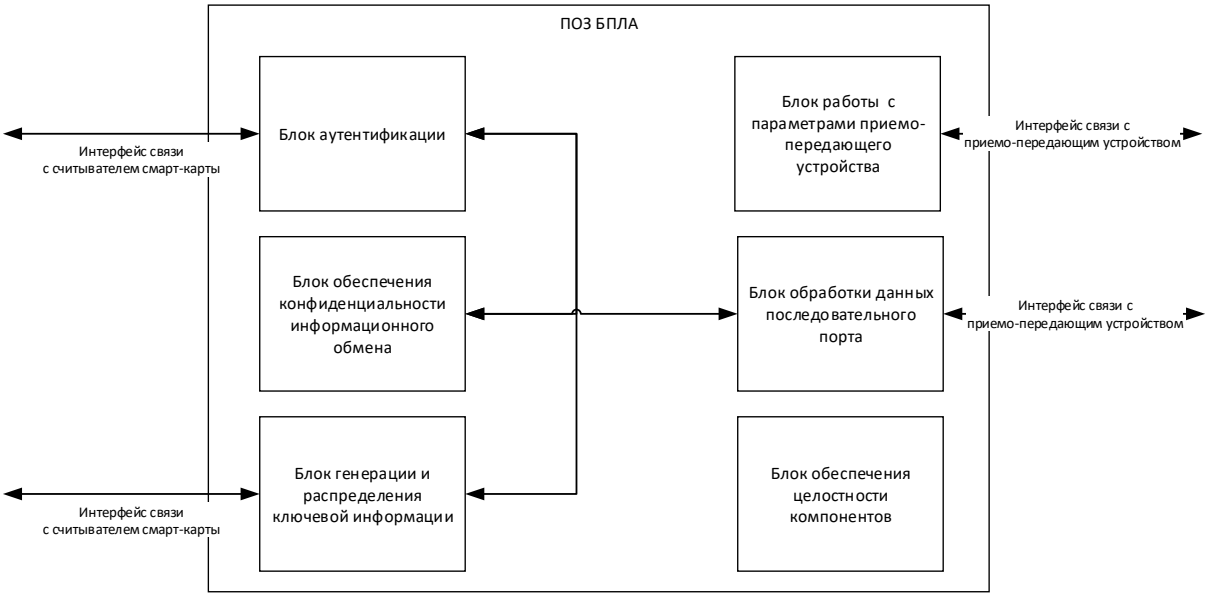


Рисунок 2 – Логическая структура программы

3.2 Алгоритм работы защищенного комплекса БПЛА

Алгоритм работы защищенного комплекса БПЛА включает несколько этапов/шагов:

- Шаг 1: Создание ключевых носителей.
- Шаг 2: Двухсторонняя аутентификация, установление защищенного соединения, формирование сеансовых ключей.
- Шаг 3: Обмен защищенными данными.

Для подготовки БПЛА к выполнению полетного задания необходимо выполнить последовательно все шаги.

3.2.1 Шаг 1: Создание ключевых носителей

Начальное распределение ключей осуществляется в соответствии с протоколу Диффи-Хэллмана. В соответствии с данным протоколов у обоих участников обмена должны быть личный секретный ключ, личный публичный ключ. Публичные ключи предназначены для обмена по каналам связи для формирования сеансовых ключей индивидуальной парно-выборочной связи.

Для уменьшения вероятности проведения атаки «человек по середине», возможной в обмене публичными ключами по протоколу Диффи-Хэллмана, введено требование, в соответствии с которым обе стороны должны заранее иметь публичные ключи друг друга. Во время обмена публичными ключами по протоколу обе стороны сравнивают полученный публичный ключ с имеющимся. При совпадении ключей стороны считают, что обмен ведется с легальным пользователем, а не с несанкционированной третьей стороной.

Таким образом, начальная ключевая информация, хранящаяся на ключевом носителе (смарт-карте) должна включать:

1. Собственный секретный ключ;
2. Собственный публичный ключ;
3. Публичные ключи всех абонентов, с которыми необходимо организовать защищенную связь.

Создание ключевого носителя для каждого абонента состоит из двух этапов:

1. Создание собственной пары «открытый ключ-секретный ключ».
2. Запись на ключевой носитель открытых ключей других абонентов.

Для генерации ключевой пары «секретный ключ – открытый ключ» используется микропроцессорная смарт-карта отечественного производства, на которой установлен карточный микроконтроллер семейства MIK51. На базе микроконтроллера MIK51 функционирует проприетарная операционная система, выполняющая набор команд в

соответствии с ГОСТ Р ИСО/МЭК 7816-8 «Карты на интегральных схемах. Часть 8. Команды для операций по защите информации».

Смарт-карты на базе микроконтроллера MIK51 работают по контактному интерфейсу. Для работы со смарт-картой необходимо иметь следующие программно-аппаратные компоненты:

- Считыватель смарт-карт;
- Кабель подключения смарт карты к шифратору БПЛА/НКУ (как правило, USB A – USB B):
- Драйвер поддержки работы со считывателем.

Схема подключения считывателя к компьютеру приведена на рисунке 4.

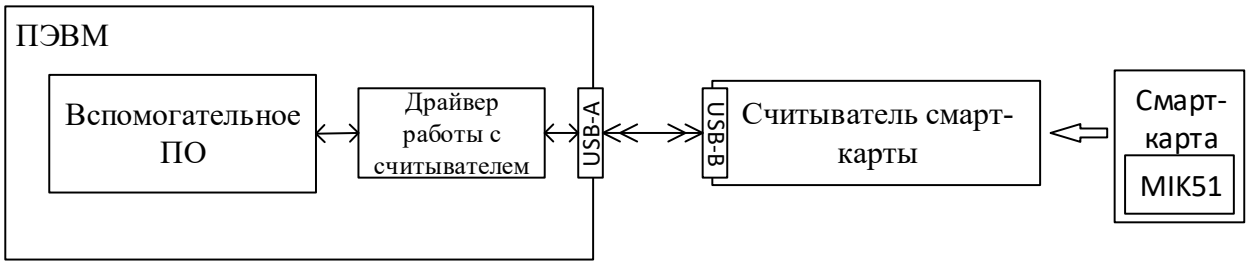


Рисунок 4 – Схема подключения считывателя смарт-карты и ПЭВМ.

Для генерации пары «секретный ключ – открытый ключ» используется команда GENERATE KEY PAIR. С помощью данной команды генерируется пара ключей в соответствии с алгоритмом ГОСТ Р 34.10-2001. Формируется секретный ключ размеров 32 байт и открытый ключ размером 64 байт. Открытый и секретный ключ сохраняются на смарт-карте. Открытый ключ возвращается в ответе на команду.

3.2.2 Шаг 2: Двухсторонняя аутентификация, установление защищенного соединения, формирование сеансовых ключей.

Процесс формирования сеансовых ключей разделен на несколько этапов:

1. Обмен публичными ключами и проведение двухсторонней аутентификации.
2. Создание общего секретного пре-мастер ключа на основе собственного секретного и публичного второго участника обмена в соответствии с алгоритмом Диффи-Хэллмана.
3. Создание сеансовых ключей.

Для проведения установки защищенного соединения, двухсторонней аутентификации и формирования сеансовых ключей необходимо иметь следующие компоненты:

- НКУ;
- БПЛА;
- Считыватель смарт-карт, подключенный к шифратору НКУ;
- Считыватель смарт-карт, подключенный к шифратору БПЛА;
- Смарт-карта НКУ;
- Смарт-карта БПЛА.

Схема подключения считывателя к программному и аппаратному шифратору приведена на рисунке 5.

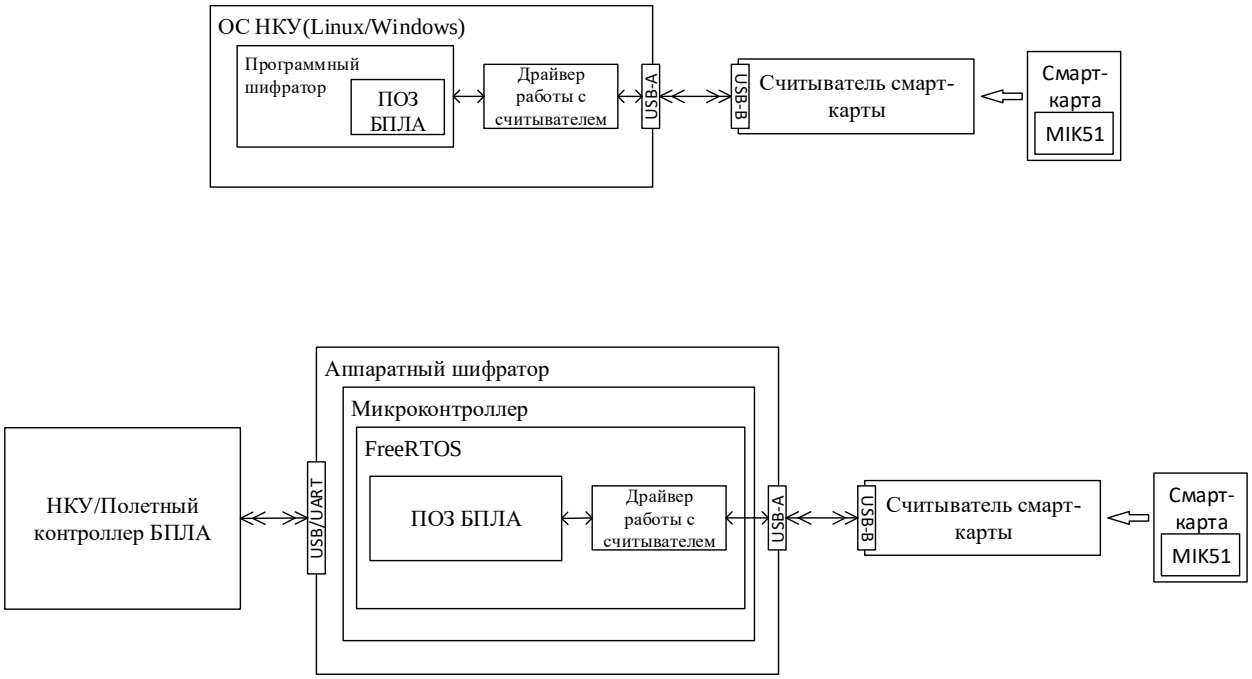


Рисунок 5 – Подключение считывателя смарт-карт к программному и аппаратному шифратору.

Формирование общего секретного пре-мастер ключа осуществляется с помощью команды GENERAL AUTHENTICATE. На карте должен быть секретный ключ. В формате команды на карту передается открытый ключ, на основе которого формируется общий секретный ключ в соответствии с алгоритмом Диффи-Хэллмана на эллиптических кривых. Для формирования общего секретного ключа используется режим VKO (RFC 4357) с передачей случайного числа (8 байт) на карту. В ответе от карты содержится общий секретный ключ (64 байта).

Команда подается на смарт-карту подключенную к шифратору БПЛА и на смарт-карту подключенную к шифратору НКУ. Шифратор БПЛА и шифратор НКУ обмениваются открытыми ключами.

Подготовка к проведению аутентификации и выработке сеансовых ключей:

1. Подключаем считыватель к шифратору БПЛА №i и вставляем в слот подготовленную смарт-карту БПЛА №i.
2. Подключаем считыватель к шифратору НКУ и вставляем в слот подготовленную смарт-карту НКУ. Включаем НКУ. Шифратор НКУ находится в режиме ожидания.
3. Включаем питание БПЛА. Инициатором обмена сообщениями является БПЛА.

Обмен сообщениями происходит по беспроводному каналу связи с помощью приемопередатчиков. Протокол аутентификации при установлении соединения и выработки сеансового мастер-ключа основан на протоколе TLS (Transport Layer Security) и является его аналогом, адаптированным под инфраструктуру БПЛА.

Сформированные сеансовые ключи хранятся в оперативной памяти до момента перезагрузки. При следующем включении питания процедура установки безопасного соединения и выработки сеансовых ключей повторяется.

3.2.3 Шаг 3: Обмен защищенными данными.

Как программный, так и аппаратный шифратор включается в разрыв между приемо-передающим устройством и устройством, генерирующим командно-телеметрическую информацию. В НКУ таким устройством является программа управления полетами QGroundControl, а в БПЛА – полетный контроллер.

Командно-телеметрическая информация формируется в соответствии с протоколом MAVLink. После установки защищенного соединения и настройки всех необходимых параметров на шаге 2 шифратор осуществляет прием открытых сообщений MAVLink от полетного контроллера/программы управления, зашифровывает их и передает в ППУ.

В обратную сторону шифратор принимает зашифрованные сообщения MAVLink от ППУ, расшифровывает их и передает в полетный контроллер/программу управления. Открытые сообщения от ППУ передаются в неизменном виде.

В защищенном комплексе БПЛА присутствует счетчик пакетов. Каждый шифратор ведет счетчик отправленных и счетчик принятых пакетов. Каждому отправленному пакету присваивается свой порядковый номер. Номер очередного пакета на 1 больше предыдущего. Нумерация пакетов в каждом направлении 0, 1, 2, 3, 4, …, N. Номер каждого

принятого пакета считывается и фиксируется. Приему и расшифровке подлежат только пакеты с порядковым номером больше, чем предыдущий принятый.

Для каждого пакета формируется свой сеансовый ключ шифрования и свой сеансовый ключ просчета имитовставки, которые обновляются в зависимости от номера пакета. Таким образом, пакеты с одинаковым содержанием, но с разными порядковыми номерами, защищаются разными криптографическими ключами, что приводит к качественной рандомизации данных попадающих в радиоканал.

3.3 Алгоритм работы Шифратора БПЛА

После запуска Шифратор БПЛА работает по следующему алгоритму:

1. Проверяет целостность ПО (только для аппаратного шифратора).
2. Запускает процедуру проведения аутентификации, обмена ключами и выработки сеансовых ключей.
3. Работает в режиме защищенного обмена сообщениями.

В аппаратном шифраторе проверка целостности производится сразу после старта микроконтроллера. Алгоритм проверки целостности приведен в п. 3.4.1.

Запуск процедуры аутентификации осуществляется в соответствии с п.3.3.2. Сеансовые ключи, сформированные на данном этапе, хранятся в оперативной памяти до момента выключения питания или перезагрузки. При новом старте происходит выработка новых сеансовых ключей.

Защищенный обмен производится в соответствии с п.3.3.3.

3.3.1 Проверка целостности ПО

В время старта после инициализации микроконтроллера аппаратный шифратор производит проверку целостности прошивки.

ПО аппаратного шифратора разрабатывается в специализированной среде разработки IAR Embedded Workbench IDE. На этапе компиляции прошивки для микропроцессора STM32F7 среда разработки вычисляет контрольную сумму CRC32 (4

байта). Контрольная сумма рассчитывается по стандартному алгоритму, основанному на полиноме 0xEDB88320 или его зеркальном отражении 0x04C11DB7.

Алгоритм проверки целостности прошивки аппаратного шифратора:

1. Шифратор считывает адрес начала и адрес конца прошитого в него ПО.
2. Шифратор вычисляет контрольную сумма и сравнивает со значением, хранимым в константе «просчитанное значение CRC32».
3. Если значение, просчитанное шифратором, совпадает со значение, хранимым в константе, тогда шифратор считает, что его прошивка не повреждена. Шифратор продолжает работу.
4. Если значение, просчитанное шифратором, не совпадает со значением, хранимым в константе, тогда шифратор считает, что его прошивка повреждена и выдает ошибку в виде световой индикации (частое моргание светодиода).

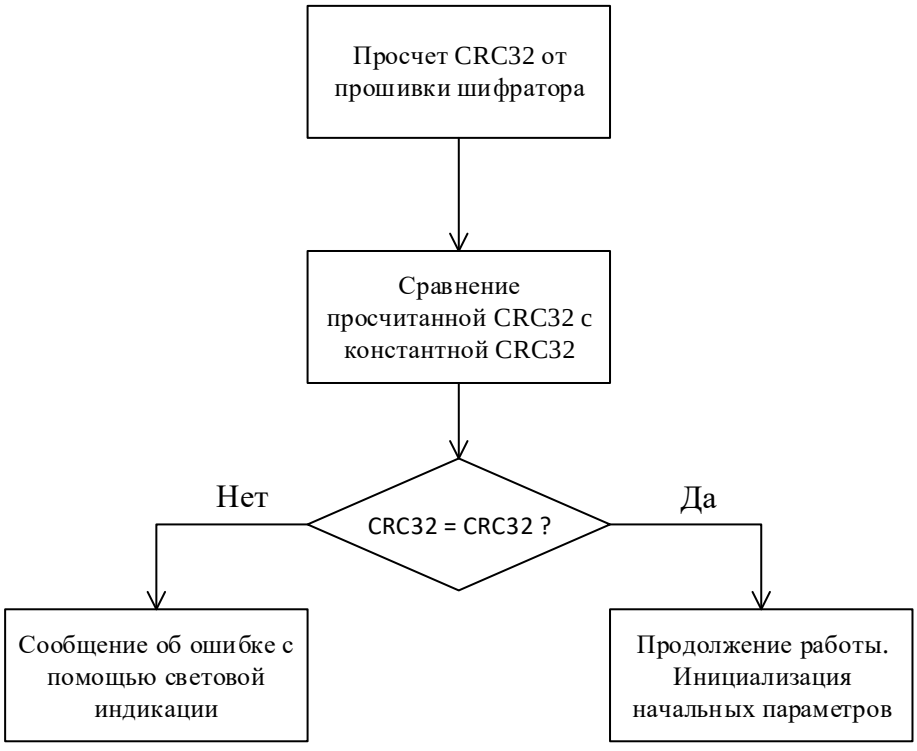


Рисунок 8 – Алгоритм проверки целостности прошивки шифратора.

3.4 Используемые криптографические алгоритмы

3.4.1 Иерархия ключей и методы формирования ключей

Сеансовый пре-мастер ключ формируется микроконтроллером смарт-карты на основе алгоритма ГОСТ Р 34.10. На основе сеансового пре-мастер-ключа формируется мастер-ключ. На основе мастер-ключа формируются сеансовые криптографические ключи. В состав сеансовых криптографических ключей входят ключ шифрования и ключ просчета имитовставки.

Для генерации мастер-ключа и сеансовых криптографических ключей используется проприетарная библиотека криптографических функций ООО Фирма «АНКАД» Cryptec.

Для генерации мастер-ключа из сессионного пре-мастер-ключа используются алгоритм выработки имитовставки HMAC на основе функции хэширования с длиной хэш-кода 512 бит из ГОСТ Р 34.11-2012 ("Стрибог").

3.4.2 Алгоритм шифрования командно-телеметрической информации

Для шифрования командно-телеметрических сообщений MAVLink используется блочный шифр "Магма" в режиме гаммирования с обратной связью по шифртексту.

4. Используемые технические средства

Программный шифратор

Программный шифратор представляет собой исполняемый модуль, который запускается на ПЭВМ под управление ОС Linux (deb-based) или ОС Windows 7 и выше. На ПЭВМ должны быть установлены все программные компоненты, которые использует Шифратор БПЛА в своей работе (см. п. 1.3).

Требования к ПЭВМ:

- Процессор — 2 ядра или больше, тактовая частота на одно ядро минимум 1,8 GHz;

- Оперативная память (RAM) — не менее 2 Гб;
- Жесткий диск (HDD/SSD) — минимум 100 Мб свободного места;
- Два свободных порта USB.

Используемые приемо-передающие устройства – 3DR telemetry kit, RFD 900 и их производные. ППУ подключаются по порту USB через переходник USB-UART CP2102.

Считыватель смарт-карт подключается по порту USB.

Аппаратный шифратор

Аппаратный шифратор реализуется на единой плате. Шифратор БПЛА функционирует под управлением ОС FreeRTOS. Основной вычислитель, на котором построен аппаратный шифратор микропроцессор STM32F746IGT6. На плате аппаратного шифратора должны присутствовать интерфейсы для подключения считывателя смарт-карт (USB/UART), интерфейс для подключения к полетному контроллеру или НКУ UART и интерфейс для подключения к ППУ UART.

Макет аппаратного шифратора выполнен на макетной плате, содержащей микроконтроллер STM32F746IGT6. Разведенные и выведенные для подключения пины – PA9, PA10, GND, PD5, PD6, 5Vin, 5Vout, PH5, PE3.

Соединение с БПЛА

Аппаратный шифратор предназначен для работы в составе БПЛА любого типа, функционирующего на основании полетного контроллера семейства APM 2.6 или Pixhawk 1 (включая модификации PX4, Pixracer и т.д.) с подключением приемо-передающих устройств (командно-телеметрическая связь) при помощи порта UART. Полетный стек – ArduPilot или PX4.

Используемые приемо-передающие устройства – 3DR telemetry kit, RFD 900 и их производные ППУ подключаются по порту UART.

В БПЛА должно быть предусмотрено свободное место для установки шифратора.

Соединение с НКУ

При соединении с НКУ аппаратный шифратор подключается к порту USB через переходник USB-UART CP2102. ППУ подключаются посредством порта UART.

5. Вызов и загрузка

Программный шифратор, в составе которого функционирует Шифратор БПЛА, представляет собой исполняемый модуль. Входная точка в программу функция main. Функция загружает пользовательский интерфейс и ожидает команд оператора.

Прошивка аппаратного шифратор хранится в ПЗУ микроконтроллера. При включении питания микроконтроллер начинает выполнять самотестирование и начальную инициализацию. Вызывается функция Reset_Handler, которая устанавливает начальные значения регистров, разбивает оперативную память, выставляет режимы работы микроконтроллера. Далее функция Reset_Handler вызывает функцию main программы. Функция main проводит проверку целостности прошивки, хранящейся в ПЗУ. В случае успешной проверки функция main проводит инициализацию параметров Шифратора БПЛА и вызывает загрузку ОС FreeRTOS. После загрузки ОС FreeRTOS управление передается ей. Далее в процессе работы ОС FreeRTOS вызывает необходимые функции Шифратора БПЛА как свои задачи.

6. Входные данные

Входные данные для ПО Шифратора БПЛА программного и аппаратного шифратора идентичны.

Входные данные со стороны программы управления полетом или со стороны полетного контроллера – это сообщения в формате базового пакета протокола MAVLink v2, предназначенные для отправки в радиоканал.

Входные данные со стороны ППУ – это зашифрованные пакеты протокола MAVLink v2, полученные из радиоканала.

7. Выходные данные

Выходные данные для Шифратора БПЛА программного и аппаратного шифратора идентичны.

Выходные данные для программы управления полетом или для полетного контроллера – это сообщения в формате базового пакета протокола MAVLink v2,

8. Обмен данными между компонентами

Процесс передачи данных между шифраторами и компонентами (полетный контроллер/управляющая программа и ППУ) производится для зашифрованных и открытых данных идентично.

Лист регистрации изменений									
	Номера листов (страниц)								
	изменён-ных	заменён-ных	новых	аннули-рованных					

Инв. N подл	Подпись и дата	Взам. инв. N	Инв. N дубл	Подпись и дата