ООО «Фирма «АНКАД»

УТВЕРЖДЕН

КБДЖ.01384-01 31 01- ЛУ

Комплекс программного обеспечения шифратора БПЛА

Шифратор БПЛА

Описание применения

КБДЖ. 01384-01 31 01

Листов 15

2018 г

Аннотация

Настоящий документ содержит сведения о назначении программного продукта и его функциональных возможностях, список минимальных технических и программных средств, необходимых для применения Шифратора БПЛА в инфраструктуре беспилотных авиационных систем, а также основную задачу, на решение которой направлено применение Шифратора БПЛА и методы, примененные для ее решения. Помимо этого приведено описание входных и выходных данных Шифратора БПЛА.

Оглавление

1. Назначение программы

Программное обеспечение применяется для защиты беспроводных каналов связи в беспилотных авиационных системах (далее БАС) ближнего радиуса управления с использованием сверхмалых и малых беспилотных летательных аппаратов (далее БПЛА) коптерного типа. Программное обеспечение предназначено для организации защищенного канала передачи командно-телеметрической информации между БПЛА и наземной станцией управления (далее НСУ) по открытым каналам беспроводной цифровой связи.

Аппаратные и программно-аппаратные модули защиты с программным обеспечением Шифратора БПЛА встраиваются в разрыв цепи беспроводной связи беспилотных авиационных систем. Функции обоих (аппаратного и программного) типа реализации одинаковы и полностью совместимы. Аппаратные модули защиты устанавливаются при проектировании и сборке беспилотных систем посредством интерфейсов взаимодействия БПЛА или НСУ с приемо-передающими устройствами. При этом со стороны НСУ модуль защиты может быть установлен на аппаратном обеспечении НСУ, без использования выделенных аппаратных средств. При установке модулей защиты должно быть соблюдено условие возможности свободного подключения и отключения аутентифицирующего носителя. Подключение аутентифицирующего носителя производится каждый раз при предполетной подготовке и отключение после загрузки ключевой информации.

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.

2. Условия применения

Для функционирования программы, как минимум, необходимо наличие следующих аппаратных и программных средств:

2.1 Аппаратные средства.

- Беспилотный летательный аппарат (далее БПЛА) на полетном контроллере Pixhawk 2.4.8 (произвольного типа)
- Комплект приемо-передающих устройств 3DR Telemetry Kit
- Комплект аутентифицирующих носителей типа смарт-карта на микроконтроллере МИКРОН в количестве двух штук

- Считыватель смарт-карт Криптон-ССК
- Соединительный кабель MicroUSB(папа)-USB(мама)
- Шифратор в аппаратном исполнении на подготовленной макетной плате Core746I в количестве двух штук
- Электронная вычислительная машина (далее ЭВМ) наземной станции управления (далее НСУ) (двухядерный процессор Intel с тактовой частотой не ниже 1.8 ГГц, оперативная память не меньше 2Гб, жесткий диск не меньше 32Гб, монитор, клавиатура, мышь, не менее 2ух свободных USB-портов)
- Конвертер интерфейсов USB-UART на микроконтроллере CP2102 в количестве двух штук.
- Комплект соединительных проводов.

2.2 Программные средства.

Требования наличия программных зависят от типа операционной системы, используемой на НСУ.

Операционная система Windows с предустановленным программным обеспечением:

- Драйвер виртуальных ком портов, соединенных нуль-модемным кабелем COM0COM;
- Драйвер считывателя смарт-карт Криптон-ССК;
- Драйвер конвертера интерфейсов USB-USRT CP2102;
- Программное обеспечение управления полетами, осуществляющее взаимодействие по протоколу MAVLink.

Операционная система Linux с предустановленным программным обеспечением:

- Пакеты pcscd и libpcsclite1 для обеспечения взаимодействия со смарт-картами;
- Модули qml и serialport среды разработки QT5;
- Драйвер виртуальных ком портов, соединенных нуль-модемным кабелем TTY0TTY;
- Драйвер считывателя смарт-карт libccid;
- Драйвер конвертера интерфейсов USB-USRT CP2102;

– Программное обеспечение управления полетами, осуществляющее взаимодействие по протоколу MAVLink.

3. Описание задачи

3.1 Определение задачи

Основным каналом передачи данных, подлежащим защите в беспилотных системах, является канал обмена командно-телеметрической информацией на линии БПЛА-НСУ. При этом БАС находится в режиме автоматического пилотирования. Данный канал основан на приемопередающих модулях с рабочими нелицензируемыми частотами 433 МГц и 900 МГц.

Соединение и прием/передача данных на приемо-передающие устройства с полетного контроллера производятся посредством стандартизованного последовательного порта UART. Связь приемо-передающего устройства с наземной станцией управления, в роли которой обычно выступает ЭВМ, также осуществляется посредством последовательного порта UART напрямую (практически не используется) либо посредством дополнительного преобразователя USB-UART основанного на преобразующих микрочипах, для подключения к повсеместно распространенной шине передачи данных USB.

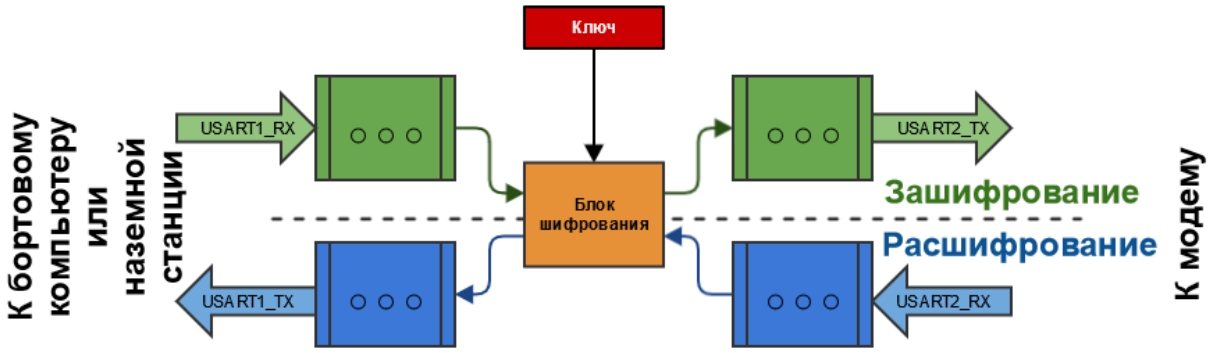
При этом данные соединения находятся непосредственно на объектах, в следствие чего считается, что они защищены от несанкционированного доступа, который становится возможным только при прямом физическом контакте с атакуемыми объектами. В следствие этого наиболее высока вероятность проведения ряда противоправных действий, направленных на проникновение в каналы информационного обмена посредством атаки на линии беспроводной передачи данных.

К таким атакам, в первую очередь, относятся атаки типа человек посередине (MitM) и повторная отправка пакетов (Replay). Ключевыми механизмами защиты от данных атак являются:

– обеспечение конфиденциальности передаваемой информации (шифрование);
– целостность сообщений (имитовставка);

– аутентификация участников информационного обмена и сообщений.

Для обеспечения защиты необходимо применять специализированное программное обеспечение направленное на реализацию данных механизмов. В первую очередь должно быть определено условие о недопустимости появления в радиоэфире незакодированных сообщений управляющих и информационных воздействий, т.е. по радиоэфиру должны передаваться модифицированные, защищённые пакеты данных. При этом, ввиду ограниченности ресурсов приемо-передающих устройств, на их вход должны подаваться уже закодированные пакеты данных, где в последствии они переупаковываются в пакеты предназначенные для передачи по радиоканалу. Приёмо-передающее устройство принимающей стороны должно напротив получать пакеты данных по радиоканалу и распаковывать их в зашифрованное сообщение, предназначенное для дальнейшей расшифровки (рисунок 1).



– Рисунок 1 - Общая схема работы средств защиты

Данное условие определяет, что непосредственная обработка пакетов данных должна производиться либо посредством собственных вычислительных мощностей полетного контроллера и станции наземного управления, либо, если это невозможно или нецелесообразно, с применением отдельных аппаратных компонентов с собственными вычислительными ресурсами.

Комплекс программного обеспечения БПЛА направлен на решение данной задачи и реализацию указанных выше механизмов защиты.

3.2 Методы решения задачи

В целях решения поставленной задачи Шифратор БПЛА осуществляет выполнение комплекса операций по обеспечению защиты информации циркулирующей в телекоммуникационных каналах БАС:

- Аутентификация участников информационного обмена с использованием алгоритмов в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.11-2012, ГОСТ Р 34.13-2015 посредством аутентифицирующих носителей, изготовленных в соответствии с ГОСТ Р ИСО/МЭК 7816-8 «Карты на интегральных схемах. Часть 8. Команды для операций по защите информации».
- Шифрование в соответствии с алгоритмом «Магма» по ГОСТ Р 34.12-2015;
- Целостность и аутентификация сообщений в соответствии с алгоритмом ГОСТ Р 34.13-2015;

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». 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.

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.

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.

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.

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

В обратную сторону шифратор принимает зашифрованные сообщения MAVLink от приемо-передающего устройства, расшифровывает их и передает в полетный

контроллер/программу управления. Открытые сообщения от приемо-передающего устройства передаются в неизменном виде.

В блоке обеспечения конфиденциальности Шифратора 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.

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").

Для генерации сеансовых криптографических ключей используется алгоритм выработки имитовставки CMAC (режим выработки имитовставки ГОСТ Р 34.13-2015 на основе алгоритма «Кузнечик»).

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

4. Входные и выходные данные

4.1 Входные данные

Входные данные для ПОЗ 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.

Формат зашифрованного пакета:

Флаг начала пакета данных (1 байт)
Тип пакета (1 байт)
Длина данных в пакете (2 байта)
Номер пакета (8 байт)
Номер ключа, использованного для шифрования данных пакета (4 байта)
Зашифрованные данные (512 байт)
CMAC (8 байт)
Флаг конца пакета (1 байт)

Описание полей:

Флаг начала – константное значение;

Тип пакета – тип полученного пакета. Используются три типа пакетов:

Тип 0 – данные протокола MAVLink. В зависимости от того, из какого буфера шифратор считал данные (см. раздел 8), их нужно либо расшифровать либо зашифровать;

Тип 1 – сообщение Hello протокола аутентификации TLS;

Тип 2 – сообщение Finished протокола аутентификации TLS.

Длина данных в пакете – Длина данных, которые передаются в пакете, минимум 0 байт, максимум 512 байт. Таким образом, общая длина пакета может быть минимум 25 байт

(все поля, кроме поля данных; при этом имитовставка считается от полей Тип пакета, Длина данных в пакете, Номер пакета, Номер ключа, использованного для шифрования данных пакета) и максимум 537 байт.

Номер пакета – номер пакета. В ПОЗ БПЛА ведется счет пакетов.

Номер ключа, использованного для шифрования данных пакета – номер текущего ключа шифрования и ключа просчета имитовставки. Каждые 100 Кбайт в процессе обмена данными между НСУ и БПЛА производится обновление криптографических ключей. Новые криптографические ключи получают новый номер. Этот номер заносится в данное поле. По этому полю шифратор на приемной стороне знает, что произошло обновление ключей и расшифровывает пакет на обновленном ключе.

Зашифрованные данные – полезная нагрузка пакета. В данном поле находится зашифрованный пакет протокола MAVLink.

CMAC – имитовставка просчитанная от полей Тип пакета, Длина данных в пакете, Номер пакета, Номер ключа, использованного для шифрования данных пакета, и Зашифрованные данные;

Флаг конца пакета – константное значение.

4.2 Выходные данные

Выходные данные для ПОЗ 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, пришедшие из радиоканала.

Выходные данные для ППУ:

1. Зашифрованные пакеты протокола MAVLink v2, предназначенные для отправки в радиоканал. Формат зашифрованного сообщения приведен в разделе 6.
2. Текстовые команды AT для настройки параметров ППУ.

AT- команды используются для настройки параметров ППУ. AT-команды передаются в открытом виде для ППУ. ППУ не передает данные команды в беспроводной канал. Для настройки параметров ППУ ПОЗ БПЛА использует три команды:

ATS3 – установка идентификатора сети или номера сети. Номер сети записывается в ОЗУ;

AT&W – запись установленных параметров в ПЗУ ППУ;

ATZ – перезагрузка ППУ с новыми параметрами.

Три команды используются последовательно для установки номера сети после успешной выработки сеансовых криптографических ключей.

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