ООО Фирма «АНКАД»

УТВЕРЖДЕН

КБДЖ.01384-01 34 01- ЛУ

Комплекс программного обеспечения шифратора БПЛА

Шифратор БПЛА

Руководство оператора

КБДЖ. 01384-01 34 01

Листов 19

2018 г

Аннотация

Настоящий документ предназначен для организаций действий оператора по запуску и осуществлению деятельности оператора при работе с программой. Документ содержит сведения о назначении программного продукта и его функциональных возможностях, список минимальных технических и программных средств, необходимых для выполнения программы, а также последовательность действию, необходимую для выполнения оператором для осуществления заупска, управления и завершения работы программы. Аспекты работы с прогарммой рассмотремы с точки зрения выполнения всех типов реализуемых средств защиты: аппаратной и прогарммно-аппаратной. Помимо этого документ содержит возможные сообщения оператору, выдаваемые в ходе выполнения программы, описание их содержания и соответствующие действия оператора в случае их возникновения.

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 ПОЗ 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.

2. Условия выполнения программы

Для выполнения 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 2,2 ГГц, оперативная память 2Гб, твердотельный накопитель 32Гб, монитор, клавиатура, мышь, не менее 2ух свободных USB-портов)
- Конвертер интерфейсов USB-UART на микроконтроллере CP2102 в количестве двух штук.
- Комплект содеинительных 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. Выполнение программы

3.1 Аппаратная реализация защиты

При реализации аппаратной защиты канала передачи данных между БПЛА и НСУ выполняется установка и подключение аппаратных шифраторов и считывателей смарт-карт в соответствии со схемой стандартной сборки аппаратных средств для организации аппаратной защиты канала связи (рисунок 1).

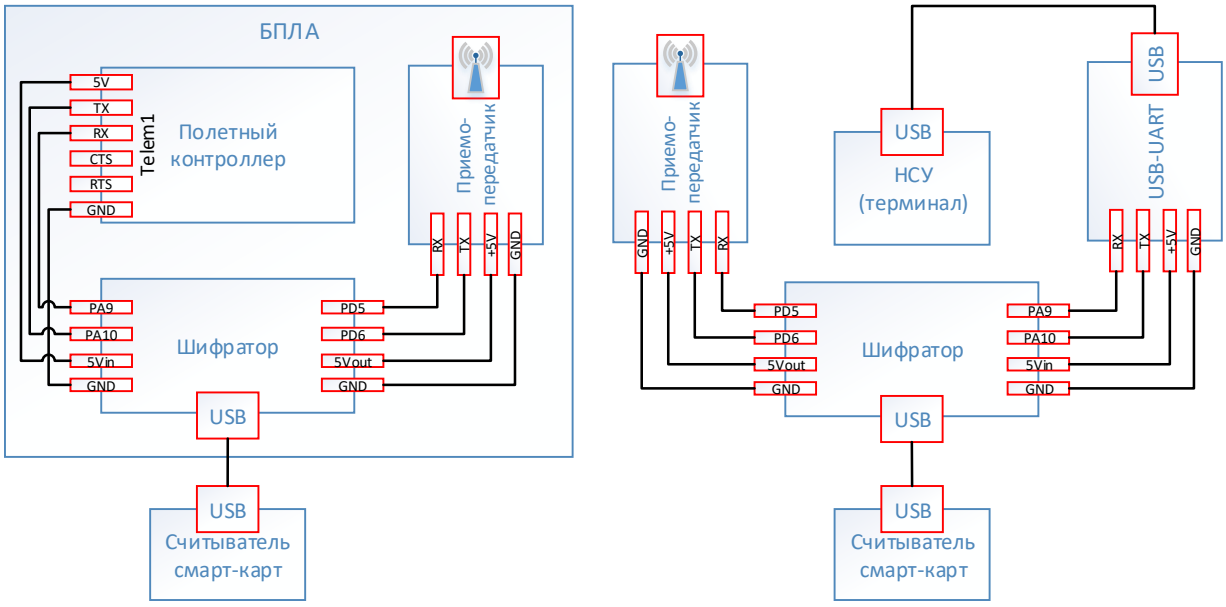

Рисунок 1. Схема стандартной сборки аппаратных средств для организации аппаратной защиты канала связи

Для запуска средств шифрования необходимо осуществить следующую последовательность действий:

1) В соответствии с руководством по эксплуатации на БПЛА осуществить подачу питания на полетный контроллер. Питание на аппаратный шифратор будет подано автоматически. Светодиод на плате шифратора примет состояние «Постоянное мигание с периодом 300мс» (см раздел 4 настоящего документа «Сообщения оператору»).

2) Вставить в слот считывателя смарт-карт, подключенного к аппаратному шифратору БПЛА, подготовленную смарт-карту. Должна начаться генерация и загрузка ключей со смарт-карты, данный процесс может сопровождаться изменением индикации светодиода состояния считывателя смарт-карт.

3) После успешной загрузки ключей светодиод на плате шифратора примет состояние Постоянное мигание с периодом 1000мс (см раздел 4 настоящего документа «Сообщения оператору»). После этого смарт-карту можно извлечь, а считыватель отключить от шифратора.

4) В соответствии с руководством по эксплуатации на НСУ осуществить подачу питания на аппаратный шифратор (USB-порт). Светодиод на плате шифратора примет состояние «Постоянное мигание с периодом 300мс» (см раздел 4 настоящего документа «Сообщения оператору»).

5) Вставить в слот считывателя смарт-карт, подключенного к аппаратному шифратору НСУ, подготовленную смарт-карту. Должна начаться генерация и загрузка ключей со смарт-карты, данный процесс может сопровождаться изменением индикации светодиода состояния считывателя смарт-карт.

6) После успешной загрузки ключей светодиод на плате шифратора примет состояние Постоянное мигание с периодом 1000мс (см раздел 4 настоящего документа «Сообщения оператору»). После этого смарт-карту можно извлечь, а считыватель отключить от шифратора.

7). Начнется информационный обмен (о чем может свидетельствовать индикация на приемо-передающем устройстве (красный светодиод)) и осуществление процесса аутентификации.

8) После завершения информационного обмена между БПЛА и НСУ в автоматическом режиме будет осуществлена перенастройка параметров работы обоих приемо-передающих устройств, о чем может свидетельствовать смена индикации питания приемо-передающих устройств (зеленый светодиод погаснет и зажжется на обоих устройствах).

9) Если процесс аутентификации и перенастройки приемо-передающих устройств пройдет успешно, то светодиод на плате обоих шифраторов примет состояние Постоянно горит (см раздел 4 настоящего документа «Сообщения оператору»).

10) Осуществить запуск штатных средств управления БПЛА на НСУ в соовтетствии с руководством по эксплуатации на средства управления БПЛА и выполнить подключение

БПЛА в штатном режиме, выбрав COM-порт приемо-передающего устройства в операционной системе НСУ (Windows или Linux).

3.2 Программно-аппаратная реализация защиты

При реализации программно-аппаратной защиты канала передачи данных между БПЛА и НСУ на стороне БПЛА выполняется установка и подключение аппаратного шифратора и считывателя смарт-карт в соответствии со схемой стандартной сборки аппаратных средств для организации программно-аппаратной защиты канала связи (рисунок 2).

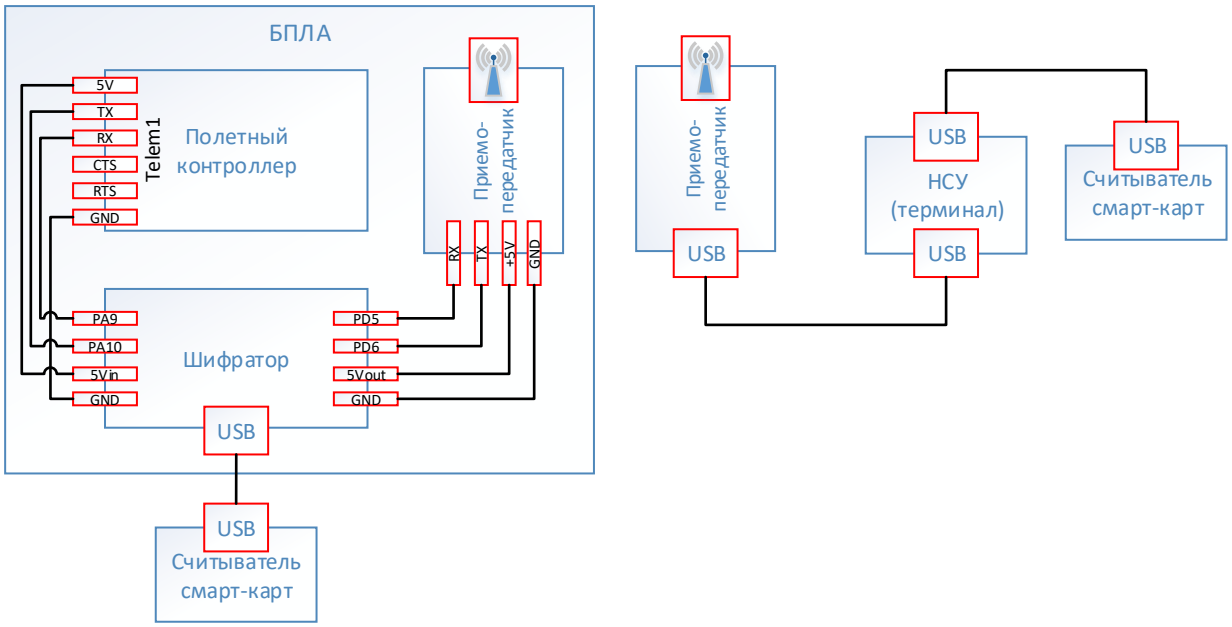

Рисунок 2. Схема стандартной сборки аппаратных средств для организации программно-аппаратной защиты канала связи

Для запуска средств шифрования необходимо осуществить следующую последовательность действий:

1) В соответствии с руководством по эксплуатации на БПЛА осуществить подачу питания на полетный контроллер. Питание на аппаратный шифратор будет подано автоматически. Светодиод на плате шифратора примет состояние «Постоянное мигание с периодом 300мс» (см раздел 4 настоящего документа «Сообщения оператору»).

2) Вставить в слот считывателя смарт-карт, подключенного к аппаратному шифратору БПЛА, подготовленную смарт-карту. Должна начаться генерация и загрузка

ключей со смарт-карты, данный процесс может сопровождаться изменением индикации светодиода состояния считывателя смарт-карт.

3) После успешной загрузки ключей светодиод на плате шифратора примет состояние Постоянное мигание с периодом 1000мс (см раздел 4 настоящего документа «Сообщения оператору»). После этого смарт-карту можно извлечь, а считыватель отключить от шифратора.

Дальнейшие действия осуществляются в зависимости от среды операционной системы, установленной на НСУ: Windows (пп 3.2.1 настоящего Руководства) или Linux (пп 3.2.2 настоящего Руководства).

3.2.1 В среде операционной системы Windows

4) Перейти в рабочую дирректорию средств шифрования в Проводнике Windows.

5) Двойным нажатием на левую кнопку мыши осуществить запуск программы “yae.exe”. Откроектся окно настройки шифратора (рисунок 3).

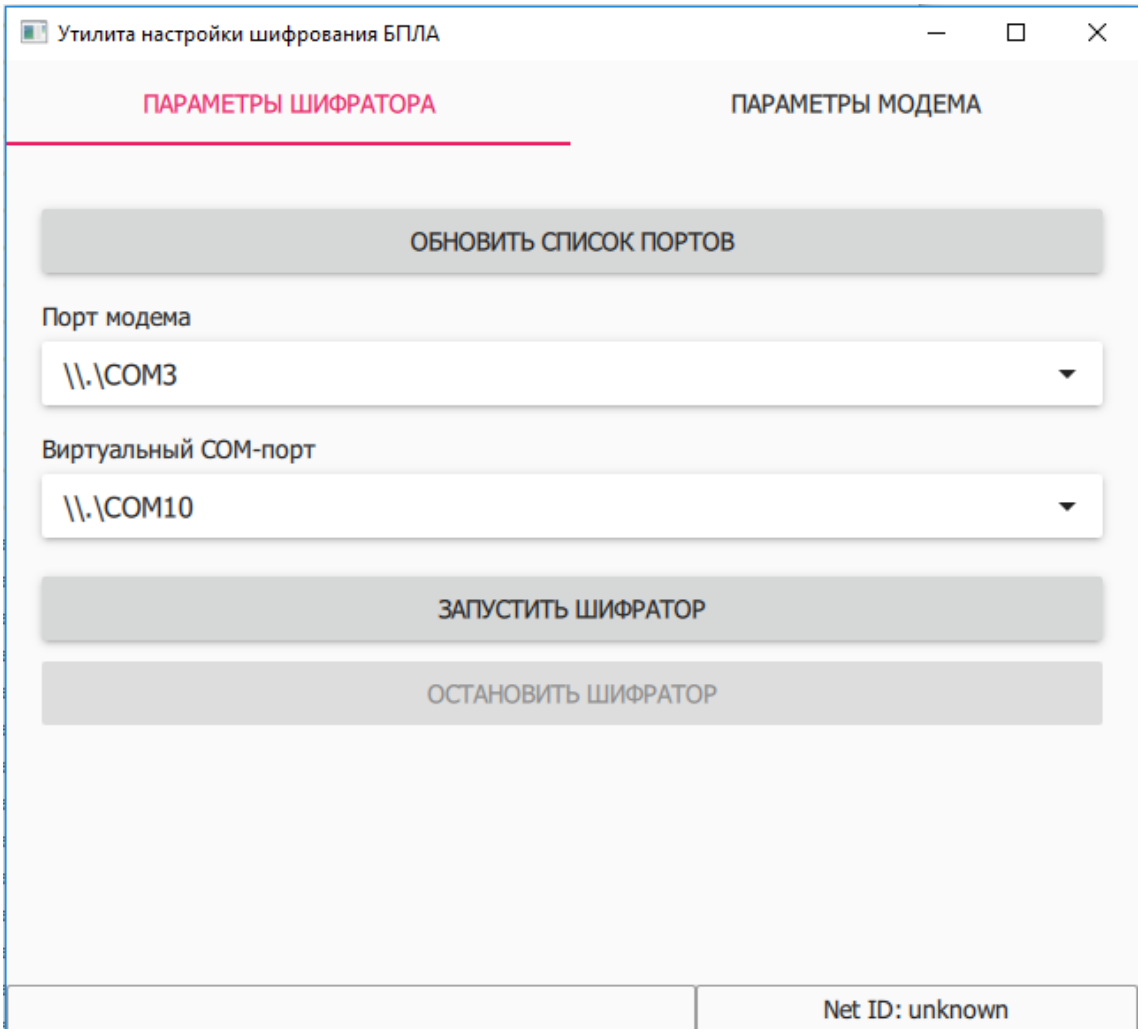

Рисунок 3. Окно настройки шифратора в ОС Windows

6. В поле «Порт модема» из выпадающего списка выбрать наименование COM-порта к которому осуществлено подключение приемо-передающего устройства. Наименование COM-порта можно определить в Диспетчере устройств операционнной системы Windows.

7. В поле «Виртуальный COM-порт» из выпадающего списка выбрать наименование одного из виртуальных COM-портов, созданных при установке драйвера com0com. Наименование COM-порта можно определить в Диспетчере устройств операционнной системы Windows.

8. Левой кнопкой мыши нажать кнопку «Запустить шифратор». В строке состояния долно отобразиться сообщение «Выполняется загрузка ключей…» (см раздел 4 настоящего документа «Сообщения оператору»).

9. Вставить в слот считывателя смарт-карт, подключенного к НСУ, подготовленную смарт-карту. Должна начаться генерация и загрузка ключей со смарт-карты, данный процесс может сопровождаться изменением индикации светодиода состояния считывателя смарт-карт.

10. После загрузки ключей в строке состояния должно отобразиться сообщение «Выполняется аутентификация…» (см раздел 4 настоящего документа «Сообщения оператору»). После этого смарт-карту можно извлечь, а считыватель отключить от НСУ.

11. Начнется информационный обмен (о чем может свидетельствовать индикация на приемо-передающем устройстве (красный светодиод)) и осуществление процесса аутентификации.

12. После завершения информационного обмена между БПЛА и НСУ в автоматическом режиме будет осуществлена перенастройка параметров работы обоих приемо-передающих устройств, о чем может свидетельствовать смена индикации питания приемо-передающих устройств (зеленый светодиод погаснет и зажжется на обоих устройствах).

13. Если процесс аутентификации и перенастройки приемо-передающих устройств пройдет успешно, то: а) светодиод на плате шифратора примет состояние Постоянно горит (см раздел 4 настоящего документа «Сообщения оператору»); б) в строке состояния отобразится сообщение «Аутентификация успешно завершена» (см раздел 4 настоящего документа «Сообщения оператору»). При эток кнопка «Запустить шифратор» станет неактивна, а кнопка «Остановить шифратор» станет активной (рисунок 4).

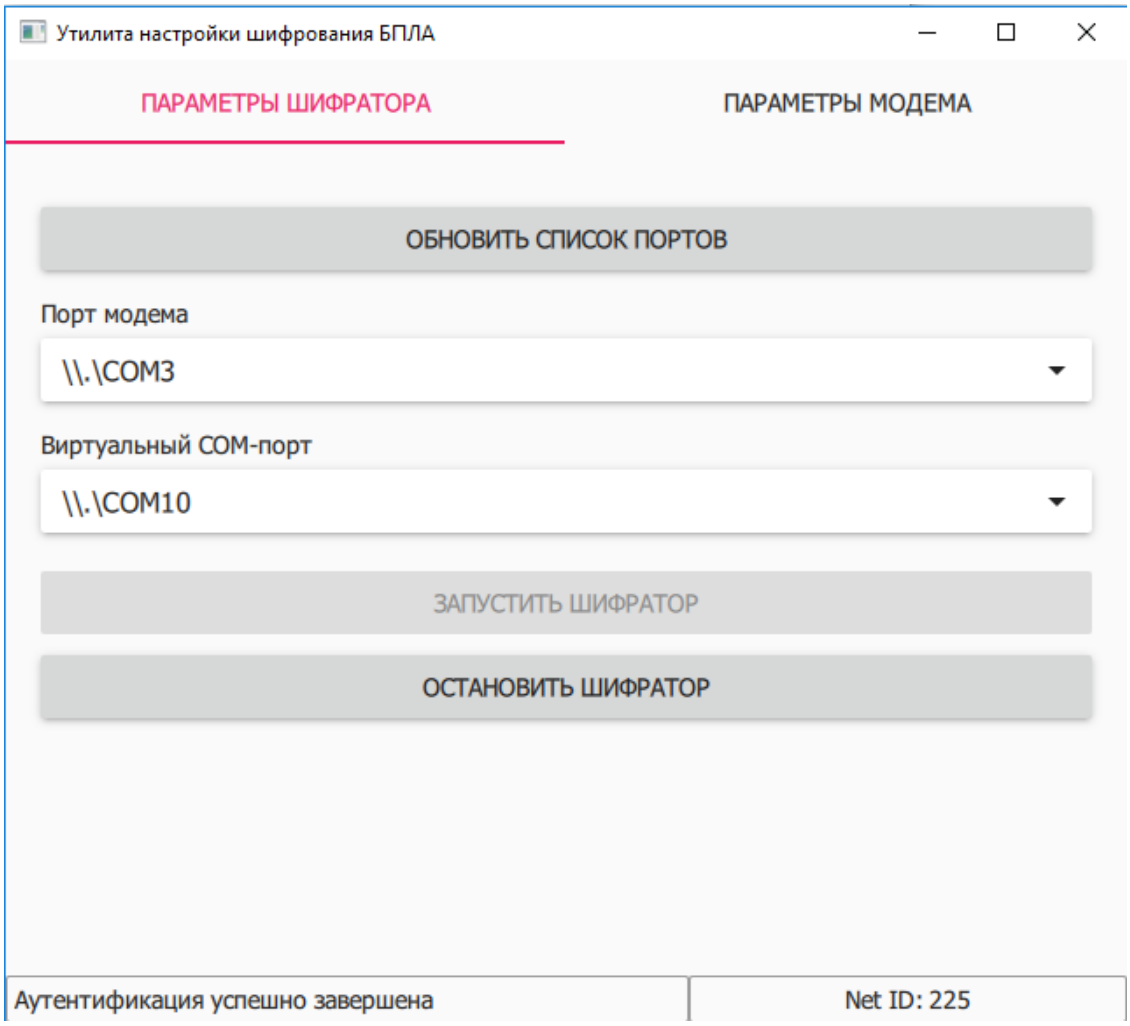

Рисунок 4. Изображение окна шифратора после успешно проведенной аутентификации в ОС Windows

14. Осуществить запуск штатных средств управления БПЛА на НСУ в соответствии с руководством по эксплуатации на средства управления БПЛА и осуществить подключение БПЛА в штатном режиме, выбрав в качестве COM-порта приемо-передающего устройства второй виртуальный COM-порт из пары, созданных в результате установки драйвера com0com.

15. Остановка работы средств шифрования осуществляется: а) на аппаратном шифраторе при помощи отключения питания БПЛА в соответствии с Руководством по эксплуатации на БПЛА; б) нажатием левой кнопкой мыши кнопки «Остановить шифратор» в окне программны шифратора на НСУ.

3.2.2 В среде операционной системы Linux

4) Перейти в рабочую дирректорию средств шифрования в терминале Linux Ubuntu используя команду “cd”.

5) При помощи команды “./yae” осуществить запуск программы. Откроектся окно настройки шифратора (рисунок 5).

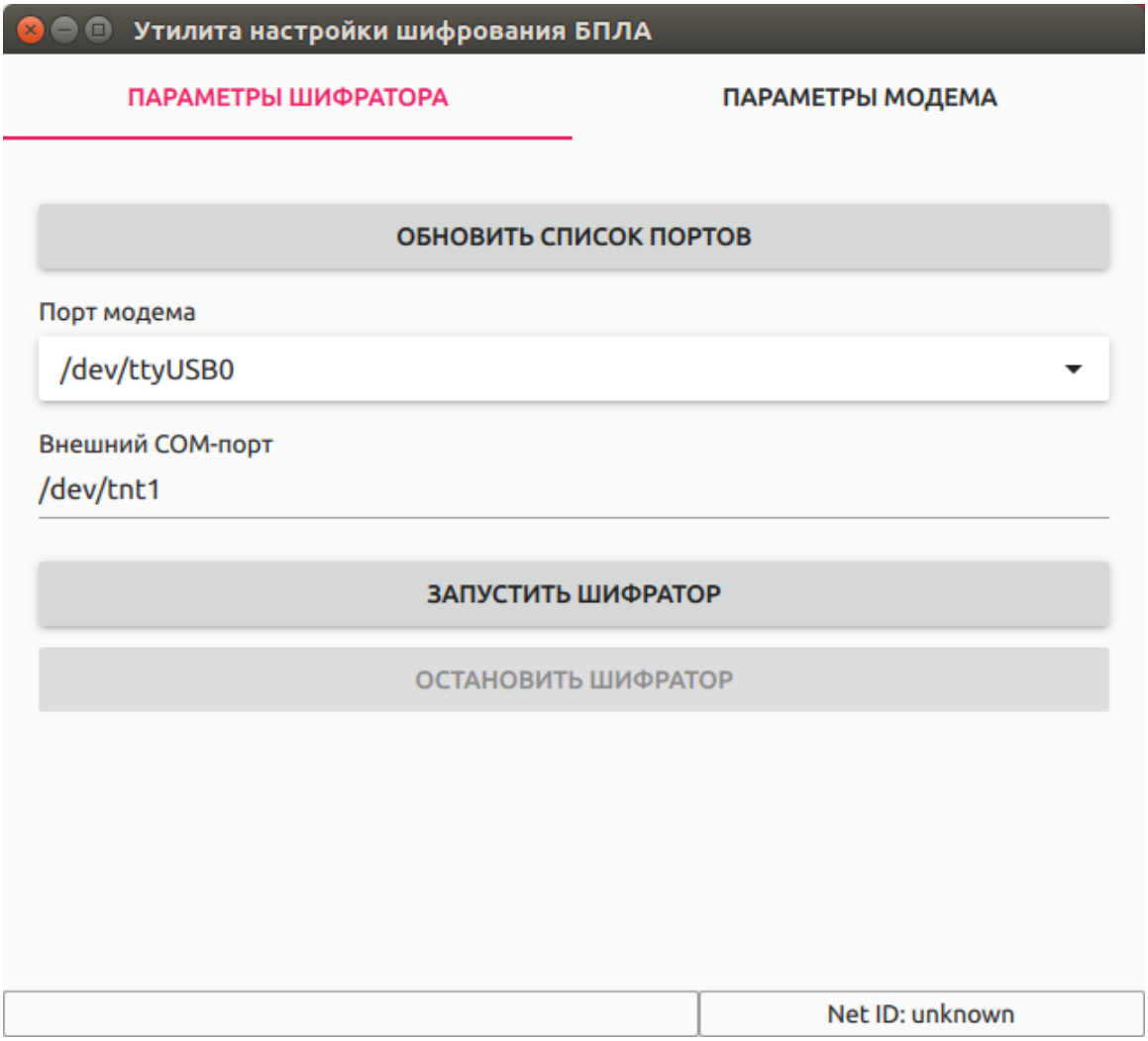

Рисунок 5. Окно настройки шифратора в ОС Linux

6. В поле «Порт модема» из выпадающего списка выбрать наименование tty-порта к которому осуществлено подключение приемо-передающего устройства. Наименование tty-порта можно определить при помощи выполнения команды “dmesg | grep attached” в терминале операционной системы.

7. В поле «Внешний COM-порт» из выпадающего списка выбрать наименование одного из пары виртуальных tnt-портов, созданных при установке драйвера tty0tty. Наименование tty-порта можно определить при помощи выполнения команды “ls /dev/” в терминале операционной системы.

8. Левой кнопкой мыши нажать кнопку «Запустить шифратор». В строке состояния долно отобразиться сообщение «Выполняется загрузка ключей…» (см раздел 4 настоящего документа «Сообщения оператору»).

9. Вставить в слот считывателя смарт-карт, подключенного к НСУ, подготовленную смарт-карту. Должна начаться генерация и загрузка ключей со смарт-карты, данный процесс может сопровождаться изменением индикации светодиода состояния считывателя смарт-карт.

10. После загрузки ключей в строке состояния должно отобразиться сообщение «Выполняется аутентификация…» (см раздел 4 настоящего документа «Сообщения оператору»). После этого смарт-карту можно извлечь, а считыватель отключить от НСУ.

11. Начнется информационный обмен (о чем может свидетельствовать индикация на приемо-передающем устройстве (красный светодиод)) и осуществление процесса аутентификации.

12. После завершения информационного обмена между БПЛА и НСУ в автоматическом режиме будет осуществлена перенастройка параметров работы обоих приемо-передающих устройств, о чем может свидетельствовать смена индикации питания приемо-передающих устройств (зеленый светодиод погаснет и зажжется на обоих устройствах).

13. Если процесс аутентификации и перенастройки приемо-передающих устройств пройдет успешно, то: а) светодиод на плате шифратора примет состояние Постоянно горит (см раздел 4 настоящего документа «Сообщения оператору»); б) в строке состояния отобразится сообщение «Аутентификация успешно завершена» (см раздел 4 настоящего документа «Сообщения оператору»). При эток кнопка «Запустить шифратор» станет неактивна, а кнопка «Остановить шифратор» станет активной (рисунок 6).

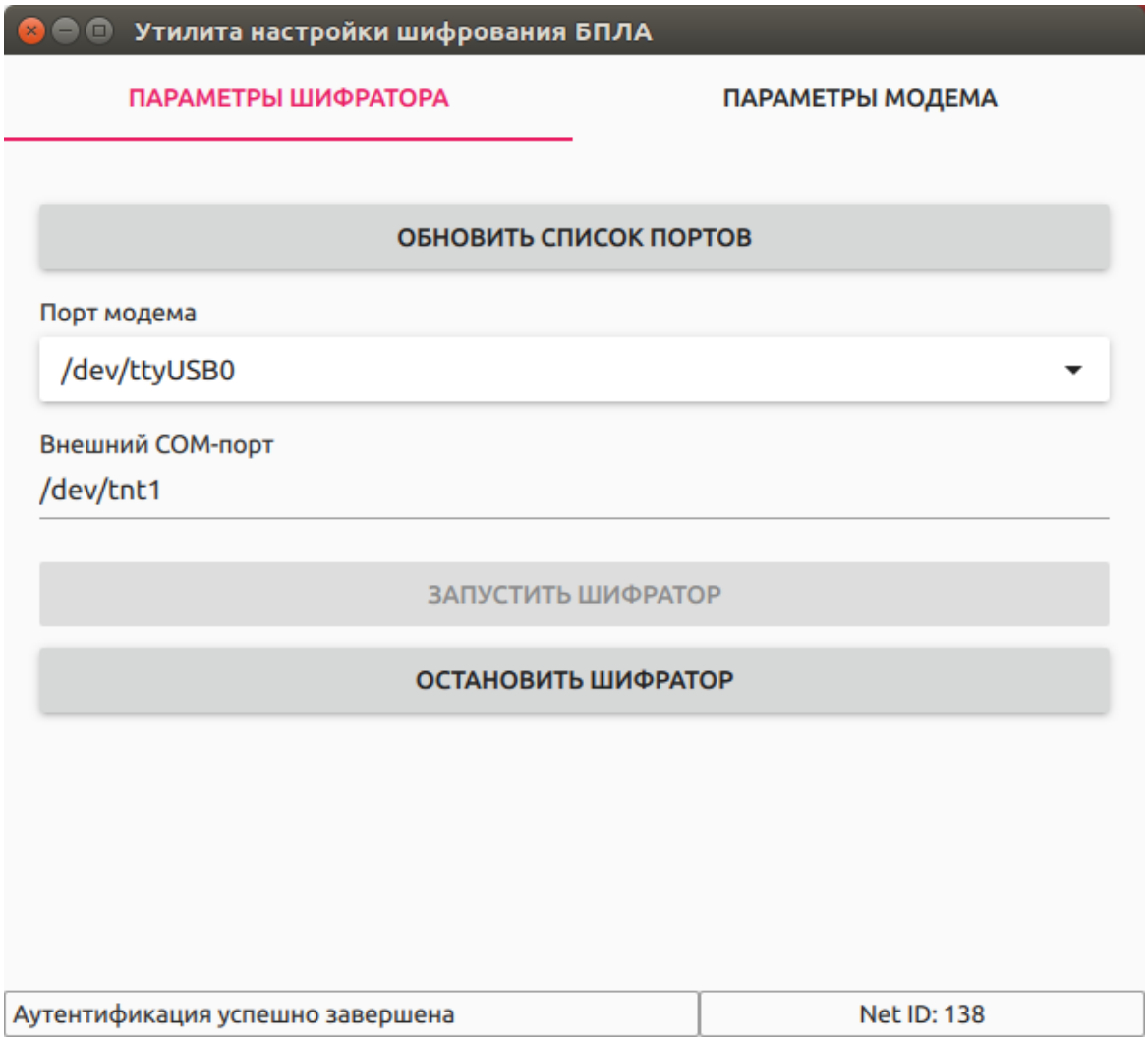

Рисунок 6. Изображение окна шифратора после успешно проведенной аутентификации в ОС Linux

14. Осуществить запуск штатных средств управления БПЛА на НСУ в соответствии с руководством по эксплуатации на средства управления БПЛА и осуществить подключение БПЛА в штатном режиме, выбрав в качестве COM-порта приемо-передающего устройства второй виртуальный tnt-порт из пары, созданных в результате установки драйвера tty0tty.

15. Остановка работы средств шифрования осуществляется: а) на аппаратном шифраторе при помощи отключения питания БПЛА в соответствии с Руководством по эксплуатации на БПЛА; б) нажатием левой кнопкой мыши кнопки «Остановить шифратор» в окне программны шифратора на НСУ.

4. Сообщения оператору

Сообщения оператору различаются в зависимости от типа реализации средств защиты (программного и аппаратного) и подразделяются на 2 типа: сообщения аппаратного шифратора и сообщения программного шифратора.

4.1 Аппаратный шифратор.

При использовании одного или нескольких аппаратных шифраторов сообщения оператору реализуются посредством световой индикации светодиода состояния.

Световая индикация имеет 5 состояний:

Постоянное мигание с периодом 300мс – ожидается загрузка ключевой информации. Данное сообщение обычно наблюдается сразу после включения при нормальной работе всех компонентов и обозначает готовность к дальнейшей работе. Необходимо произвести подключение считывателя смарт-карт к шифратору и осуществить установку в него аутентифицирующего носителя (смарт-карта).

Постоянное мигание с периодом 1000мс – ключи загружены, ожидается обмен ключами и аутентификация. Данное сообщение наблюдается после загрузки ключей с аутентифицирующего носителя и обозначает готовность к проведению информационного обмена ключами и прочей информации с вторым шифратором (программным или аппаратным) по организованной линии связи. Информационный обмен и аутентификация со вторым устройством будет произведена только после загрузки ключей в ответное устройство. Если оба шифратора находятся в состоянии ожидания обмена и световая индикация не меняется в течении 60 секунд, необходимо осуществить сброс питания на шифраторах и повторить процедуру аутентификации. При повторении ситуации необходимо обратиться к системному программисту.

Постоянно горит – аутентификация прошла успешно, соединение установлено. Данное сообщение отображает штатную работу устройств: аутентификация осуществлена, соединение установлено, мастер-ключи сгенерированы, канал проходного шифрования открыт, шифрование работает в штатном режиме. Сообщение позволяет начать работу беспилотной системы в штатном режиме с использованием стандартных прогарммных средств управления и наблюдения за БПЛА.

Короткое мигание с длительными интервалами (50мс/1000мс) – ошибка инициализации или несоответствие контрольной суммы прошивки. Данное сообщение отображает критический сбой в работе программных компонентов, не позволяющих продолжить работу в штатном режиме. При возникновении данной ситуации необходимо обратиться к системному программисту.

Не горит – тотальный сбой работы системы. Данное сообщение означает нарушение работы цепей питания или поломку центрального микроконтроллера шифратора. При возникновении данного сообщения необходимо обратиться к системному администратору.

4.2 Программный шифратор:

При использовании программного шифратора на имеющихся аппаратных средствах НСУ сообщения оператору отображаются визуально на экране НСУ в виде текстовых сообщений в строке состояния (рисунок 7).

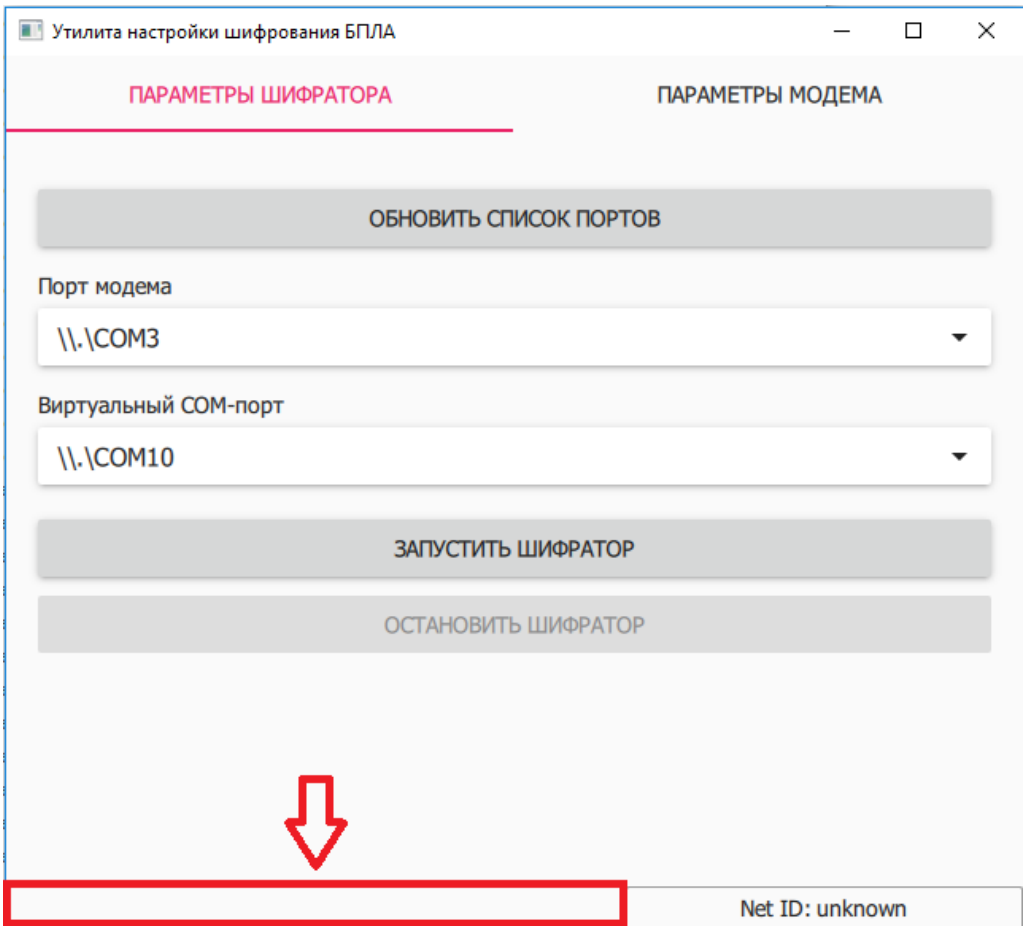

Рисунок 7. Строка состояия в окне настройки программного шифратора

Возможны следующие сообщения:

«Выполняется загрузка ключей…» (рисунок 8) - данное сообщение обычно наблюдается сразу после включения при нормальной работе всех компонентов и обозначает готовность к дальнейшей работе. Необходимо произвести подключение считывателя смарт-карт к НСУ и осуществить установку в него аутентифицирующего носителя (смарт-карту).

Рисунок 8. Сообщение "Выполняется загрузка ключей…"

«Выполняется аутентификация…» (рисунок 9) - данное сообщение наблюдается после загрузки ключей с аутентифицирующего носителя и обозначает готовность к проведению информационного обмена ключами и прочей информации с аппаратным шифратором БПЛА по организованной линии связи. Информационный обмен и аутентификация со вторым устройством будет произведена только после загрузки ключей в ответное устройство. Если оба шифратора (программный на НСУ и аппаратный на БПЛА) находятся в состоянии ожидания обмена и статус сообщений не меняется в течении 60 секунд необходимо: а) осуществить сброс питания на аппаратном шифраторе; б) осуществить повторный запуск программных средств шифрования.Повторить процедуру аутентификации. При повторении ситуации необходимо обратиться к системному программисту.

Рисунок 9. Сообщение "Выполняется аутентификация..."

«Аутентификация успешно завершена» (рисунок 10) - Данное сообщение отображает штатную работу устройств: аутентификация осуществлена, соединение установлено, мастер-ключи сгенерированы, канал проходного шифрования открыт, шифрование работает в штатном режиме. Сообщение позволяет начать работу беспилотной системы в штатном режиме с использованием стандартных прогарммных средств управления и наблюдения за БПЛА.

Рисунок 10. Сообщение "Аутентификация успешно завершена"

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