

УТВЕРЖДЕН
ДАКЖ.467239.002 РА - ЛУ

Программное обеспечение для
программно-аппаратного комплекса
«Переключатель накопителя данных»

РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА

ДАКЖ.467239.002 РА

Листов 34

Аннотация

Настоящее руководство системного администратора разработано в рамках ОКР «Разработка программно-аппаратного комплекса «Переключатель накопителя данных».

Руководство содержит условия выполнения, состав дистрибутива, инструкции по установке, настройке и эксплуатации программного обеспечения изделия АПК «Переключатель накопителя данных».

Обозначение изделия: ДАКЖ.467239.002.

Документ предназначен для системных администраторов, обслуживающих АПК «Переключатель накопителя данных».

Содержание

Термины, определения и сокращения.....	5
1. Введение.....	7
1.1. Общие сведения.....	7
1.2. Область применения.....	7
1.3. Краткое описание возможностей.....	8
1.4. Уровень подготовки системного администратора.....	8
1.5. Перечень эксплуатационных документов для ознакомления.....	9
2. Назначение и условия применения.....	10
2.1. Вид деятельности, функции, для автоматизации которых предназначен АПК	10
2.2. Требования к рабочему месту системного администратора.....	10
2.3. Требования к программно-техническому обеспечению.....	10
3. Действия по безопасной установке и настройке АПК.....	12
4. Действия по реализации функций безопасности среды функционирования.....	13
5. Подготовка к работе.....	16
5.1. Сборка АПК.....	16
5.2. Требования к ПЭВМ.....	17
5.3. Требования к накопителю данных.....	17
5.4. Состав дистрибутива.....	17
5.5. Установка ПО.....	19
5.6. Описание конфигурации.....	20
5.7. Настройка регистрации событий безопасности.....	20
6. Порядок проверки работоспособности.....	23
6.1. Автоматизированная проверка.....	23
6.2. Ручная проверка.....	24
6.3. Проверки для периодических и приёмо-сдаточных испытаний.....	24
6.3.1. Проверка круглосуточной работы.....	24
6.3.2. Проверка отсутствия цепи между ПЭВМ.....	25

7. Описание операций.....	27
7.1. Функциональные задачи администратора.....	27
7.2. Управление политиками безопасности.....	27
7.3. Сборка АПК.....	27
7.4. Установка ОС и ПО.....	27
7.5. Мониторинг событий безопасности.....	27
7.6. Диагностика и мониторинг работоспособности ПО и АПК.....	29

Термины, определения и сокращения

В настоящем документе применены следующие термины:

Администратор системы	Лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.
Контроль целостности	Контроль за сохранением неизменности информации в условиях случайного и (или) преднамеренного искажения (разрушения).
Пароль	Секретный набор символов, используемый субъектом доступа для аутентификации в системе.
Объект доступа	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
Учетная запись пользователя	Запись, содержащая информацию о пользователе системы, необходимую для его работы в системе, в том числе сведения, используемые для идентификации и аутентификации пользователя при его подключении (регистрации) к системе.

В настоящем документе применены следующие сокращения:

ОКР	опытно-конструкторская работа,
АПК	программно-аппаратный комплекс,
ОС	операционная система,
ПО	программное обеспечение,
ПЭВМ	персональная электронно-вычислительная машина,
ЛВС	локальная вычислительная сеть
ФСТЭК	Федеральная служба по техническому и экспортному контролю
КИИ	критическая информационная инфраструктура
ИСПДн	информационная системы персональных данных
ГИС	государственная информационная система;
ИС	информационная система
РА.1	руководство администратора операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 95 01-1, часть 1
РКСЗ.1	руководство по комплексу средств защиты (КСЗ) операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 97 01-1, часть 1

1. Введение

1.1. Общие сведения

Наименование разработки — программное обеспечение для программно-аппаратного комплекса «Переключатель накопителя данных» (далее — ПО).

Краткое наименование разработки — ПО для АПК «Переключатель накопителя данных».

ПО обеспечивает функционирование изделия «Переключатель» (ДАКЖ.465219.001) и реализует программный механизм для переноса информации между двумя ПЭВМ, подключенными к изделию.

Гриф секретности — несекретно.

1.2. Область применения

АПК предназначен для автоматизации процесса переноса информации между двумя ПЭВМ, изолированными друг от друга. АПК реализует перенос информации между ПЭВМ поочередным переключением накопителя данных от одной ПЭВМ к другой, при условии отсутствия сетевых и других соединений между указанными ПЭВМ.

АПК «Переключатель накопителя данных» может применяться в значимых объектах КИИ до 1 категории значимости включительно (приказ ФСТЭК России от 25.12.2017 г. №239), в ГИС до 1 класса защищенности включительно (приказ ФСТЭК России от 11.02.2013 г. №17), в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно (приказ ФСТЭК России от 14.03.2014 г. №31), в ИСПДн до 1 уровня защищенности включительно (приказ ФСТЭК России от 18.02.2013 г. №21), в информационных системах управления производством ОПК до 1 класса защищенности включительно (приказ ФСТЭК России от 28.02.2017 №31дсп).

АПК может использоваться для переноса информации между изолированными ИС без сетевого соединения между ними, в том числе для переноса в

указанные ИС обновлений антивирусных и справочно-правовых систем, обновлений ПО, включая обновления безопасности, и т.д.

1.3. Краткое описание возможностей

ПО обеспечивает функционирование изделия «Переключатель» (ДАКЖ.465219.001) и реализует программный механизм передачи информации (файлов и каталогов) между двумя изолированными друг от друга ПЭВМ, подключенными к изделию «Переключатель», посредством этого изделия. В любой момент времени передачи информации ПЭВМ остаются изолированными между собой.

ПО предназначено для реализации следующих функций:

- 1) Управление изделием «Переключатель» (ДАКЖ.465219.001).
- 2) Передача информации (файлов и каталогов) между двумя изолированными ПЭВМ, подключенными к изделию «Переключатель» через Накопитель данных:
 - передача информации с ПЭВМ РС1 на Накопитель данных и с Накопителя данных на ПЭВМ РС2;
 - передача информации с ПЭВМ РС2 на Накопитель данных и с Накопителя данных на ПЭВМ РС1.
- 3) Диагностика АПК «Переключатель накопителя данных» для проверки работоспособности и проведения приёмо-сдаточных испытаний.

1.4. Уровень подготовки системного администратора

Системный администратор АПК «Переключатель накопителя данных» должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке и настройке системного и прикладного программного обеспечения, применяемых в АПК.

Квалификация системного администратора должна позволять:

- осуществлять управление политиками безопасности в системе;
- устанавливать правила доступа к ресурсам системы (приложения, устройства, каталоги и т.п.);
- проводить мониторинг событий безопасности;
- настраивать ПО;
- диагностировать работу АПК.

Системный администратор АПК «Переключатель накопителя данных» должен ознакомиться с комплектом эксплуатационной документации.

1.5. Перечень эксплуатационных документов для ознакомления

Для работы с АПК системному администратору необходимо ознакомиться с настоящим документом и со следующими документами:

- 1) Формуляр ДАКЖ.467239.002 ФО.
- 2) Руководство по эксплуатации ДАКЖ.467239.002 РЭ.
- 3) Описание применения ДАКЖ.467239.002 ОП.

2. Назначение и условия применения

2.1. Вид деятельности, функции, для автоматизации которых предназначен АПК

Описание видов деятельности приведено в разделе 1.2 настоящего документа, описание функций приведено в разделе 1.3 настоящего документа.

2.2. Требования к рабочему месту системного администратора

Системное администрирование осуществляется непосредственно на подключенных к АПК ПЭВМ.

2.3. Требования к программно-техническому обеспечению

АПК «Переключатель накопителя данных» использует программно-техническое обеспечение со следующими минимальными системными требованиями, указанными в таблице 1.

Таблица 1: Системные требования к программно-техническому обеспечению АПК

№	Программно-техническое обеспечение АПК	Кол-во, шт.	Системные требования	Входит в поставку АПК
1	Устройство «Переключатель» ДАКЖ.465219.001	1	-	да
2	Кабель питания для устройства	2	-	да
3	Кабель для USB-порта	2	USB 2.0 тип А – В	да
4	Кабель для COM-порта	2	Тип GCR-DB9CF2F	да
5	ПЭВМ	2	Состав ПЭВМ: системный блок, монитор, клавиатура. Минимальные аппаратные требования ПЭВМ должны соответствовать минимальным аппаратным требованиям используемой ОС	нет
6	ОС Astra Linux SE	2	Версия не ниже 1.6 с обновлениями безопасности, должна быть	нет

№	Программно-техническое обеспечение АПК	Кол-во, шт.	Системные требования	Входит в поставку АПК
			установлена в консольном режиме без графики	
7	Накопитель данных	1	Интерфейс USB 2.0 и выше, объём накопителя данных не должен превышать объём свободного места на ПЭВМ, накопитель данных должен быть с созданным и отформатированным разделом в файловой системе ext4	нет

3. Действия по безопасной установке и настройке АПК

При установке и настройке АПК «Переключатель накопителя данных» для обеспечения безопасности необходимо выполнение следующих условий:

- 1) Использование сертифицированной операционной системы Astra Linux SE и сертифицированных средств защиты информации при применении изделия для защиты информации конфиденциального характера.
- 2) Обеспечение физической охраны технических средств, на которых развернут АПК, а также наличие надежных препятствий для несанкционированного проникновения в помещение с АПК.
- 3) Периодическая проверка программной среды подключенных к АПК ПЭВМ на наличие вредоносного программного обеспечения, использование средств периодического контроля за целостностью программной части АПК, регистрация результатов тестирования и проверок АПК в формуляре.
- 4) Периодичность технического обслуживания АПК должна быть не реже одного раза в 6 месяцев.
- 5) Должен быть назначен администратор информационной безопасности, отвечающий за соблюдение мер безопасности при эксплуатации и настройку политик безопасности;
- 6) Установка, обслуживание, восстановление работоспособности и администрирование АПК должны осуществляться персоналом, прошедшим подготовку в объеме изучения эксплуатационной документации на АПК и обладающим достаточной квалификацией для работы и администрирования АПК.
- 7) АПК собран и сконфигурирован таким образом, чтобы в ходе установки правильно применялись все необходимые меры и политики безопасности, которые предотвращают возможность реализации существующих угроз безопасности. Для поддержания данного состояния необходимо после установки АПК настраивать параметры среды функционирования АПК, перечисленные в п.4.

4. Действия по реализации функций безопасности среды функционирования

Для реализации функций безопасности среды функционирования АПК «Переключатель накопителя данных» должны выполняться следующие действия:

- 1) АПК и ПЭВМ, подключенные к АПК, должны находиться в контролируемой зоне в отдельном помещении, в котором исключен несанкционированный доступ.
- 2) Требования к характеристикам безопасности паролей системного администратора и администратора информационной безопасности должны быть определены организационно-распорядительными документами.
- 3) При работе с АПК должна быть обеспечена конфиденциальность аутентификационных данных (логина и пароля) системного администратора и администратора информационной безопасности ПЭВМ, подключенных к АПК.
- 4) Все работы в помещении с АПК должны производиться в присутствии ответственного за эксплуатацию АПК.
- 5) Перед первым подключением накопителя данных к АПК, системный администратор должен произвести форматирование накопителя данных, а также выполнить проверку на наличие вредоносного программного обеспечения на накопителе данных.
- 6) В случае необходимости передачи накопителя данных между пользователями или в сторонние организации для ремонта машинных носителей информации, необходимо обеспечить уничтожение (стирание) информации на накопителе.
- 7) Для учета машинных носителей информации (накопителей данных, подключаемых к АПК) ответственный за эксплуатацию АПК должен вести журнал учета машинных носителей информации.
- 8) При работе с АПК системные администраторы должны обеспечить хранение системных журналов безопасности сроком не менее 3 (трёх) месяцев.

- 9) Для правильной работы механизмов безопасности ОС Astra Linux SE должны быть установлены актуальные обновления безопасности.
- 10) Для осуществления контроля целостности ПО АПК в ОС Astra Linux SE необходимо включить механизм проверки контроля целостности и настроить его для проверки исполняемых файлов ПО АПК в соответствии с РКСЗ.1 (пункт 9.4).
- 11) Для контроля подключения и запрета несанкционированного подключения машинных носителей информации необходимо использовать механизмы разграничения доступа к USB-носителям ОС Astra Linux SE в соответствии с РКСЗ.1 (раздел 13) и РА.1 (раздел 16).
- 12) Для обнаружения в системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации на ПЭВМ, подключенные к АПК, должны быть установлены средства антивирусной защиты. Правила и процедуры обновления базы данных средств антивирусной защиты должны регламентироваться в организационно-распорядительных документах.
- 13) Контроль доступа к каталогам, расположенным на ПЭВМ, с помощью которых происходит обмен информацией через АПК, должен обеспечиваться механизмом разграничения доступа ОС Astra Linux SE в соответствии с РКСЗ.1 (разделы 3 и 4).
- 14) Для исключения несанкционированного доступа к ПЭВМ необходимо настроить правила фильтрации, таким образом, чтобы разрешались только необходимые сетевые взаимодействия в соответствии с РКСЗ.1 (раздел 11). Целесообразно предусмотреть использование межсетевого экрана, установленного в виде программного комплекса на ПЭВМ либо в виде программно-аппаратного комплекса между ПЭВМ и ЛВС.

- 15) В ОС Astra Linux SE должен быть включен механизм регистрации действия системных администраторов и администраторов информационной безопасности в соответствии с РКСЗ.1 (раздел 6), а именно:
- вход (выход), а также попытки входа субъектов доступа в ОС;
 - подключение машинных носителей информации и вывод информации на носители информации.
- 16) Для запрета несанкционированного доступа в ОС в ПЭВМ на базовую систему ввода/вывода (BIOS) и загрузчик GRUB должны быть установлены пароли.
- 17) Для входа в ОС системные администраторы и администраторы информационной безопасности должны использовать пароли, удовлетворяющие заданными организационно-распорядительными документами характеристиками безопасности в соответствии с РКСЗ.1 (пункт 17.2).

5. Подготовка к работе

5.1. Сборка АПК

Сборка АПК осуществляется подключением устройства «Переключатель» к ПЭВМ PC1 и PC2, и Накопителя данных к устройству «Переключатель», согласно рисунку 1.

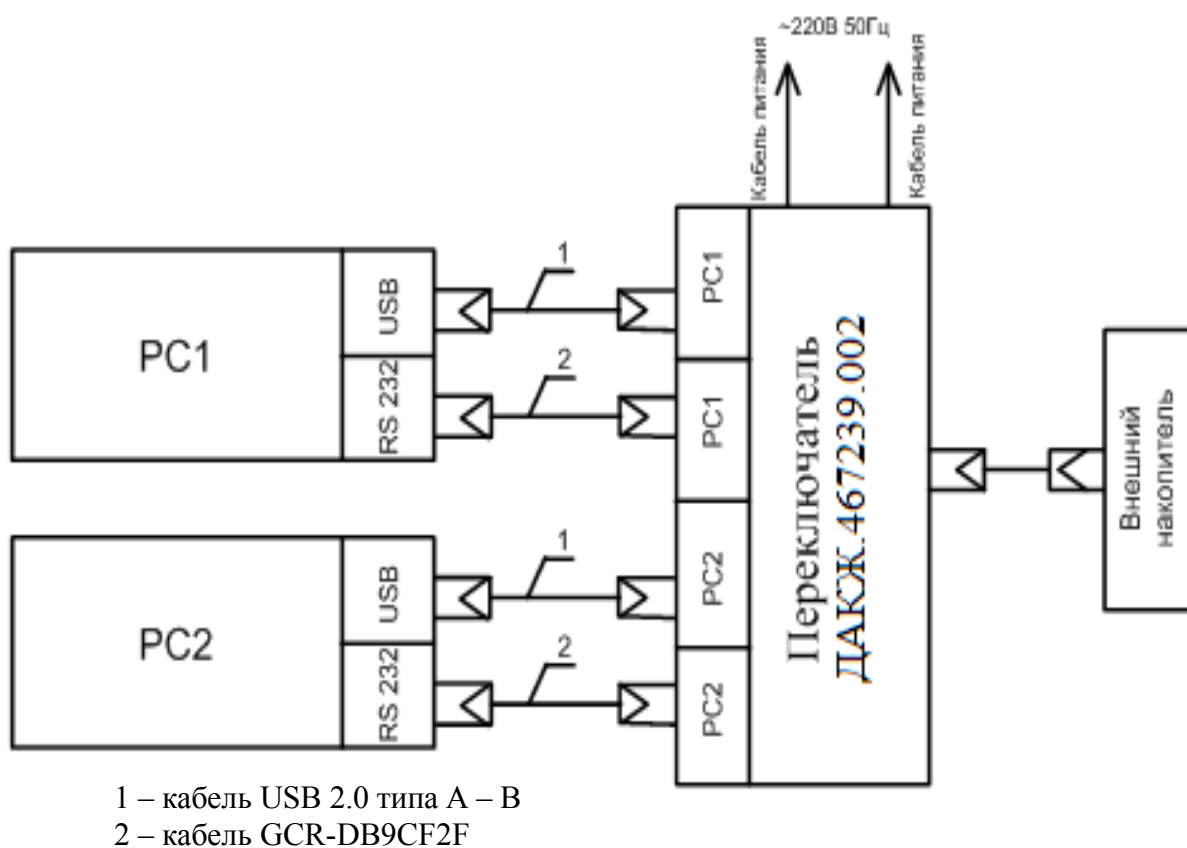


Рисунок 1: Схема электрического соединения АПК

Для сборки АПК необходимо:

- 1) Подключить «Переключатель» к сети 220В двумя кабелями питания.
- 2) Подключить кабели USB и COM от переключателя к двум ПЭВМ. Кабели от разъемов с подписью PC1 подключить к ПЭВМ PC1, а от разъемов с подписью PC2 к ПЭВМ PC2. Имена ПЭВМ могут отличаться от «PC1» и «PC2», в этом

случае необходимо указать правильную настройку при инсталляции пакета в соответствии с подключением ПЭВМ к разъёмам АПК (п. 5.5).

- 3) Вставить Накопитель данных (на рисунке обозначен как Внешний накопитель) в разъём «Переключателя».
- 4) Включить питание на «Переключателе» и включить ПЭВМ.

5.2. Требования к ПЭВМ

ПЭВМ должны состоять из системного блока, монитора и клавиатуры. На ПЭВМ PC1 и PC2 должны быть установлены ОС Astra Linux SE версии не ниже 1.6 со всеми обновлениями безопасности, в консольном режиме без графики. Минимальные системные требования ПЭВМ должны соответствовать минимальным системным требованиям используемой ОС в соответствии с эксплуатационной документацией ОС.

5.3. Требования к накопителю данных

Накопитель данных должен иметь USB интерфейс 2.0 и выше, объём накопителя не должен превышать объём свободного места на ПЭВМ.

Перед началом работы накопитель данных необходимо отформатировать, форматирование необходимо выполнить с помощью команды:

```
mkfs -t ext4 /dev/<устройство накопителя>.
```

5.4. Состав дистрибутива

В состав дистрибутива ПО входит:

1) Драйвер:

- */usr/lib/biorobot/driver_pc1* и */usr/lib/biorobot/driver_pc2* — драйверы для обеспечения работы Переключателя для PC1 и PC2, устанавливаются на ПЭВМ в */usr/bin/biorobot_driver*.

- */lib/systemd/system/biorobot_driver.system* — сервис, отвечающий за запуск драйвера переключателя.

2) Скрипт копирования:

- */usr/bin/biorobot_script* — программа для копирования файлов на Накопитель данных и с Накопителя данных, а также для автоматического тестирования работоспособности.

- */lib/systemd/system/biorobot_switch@.service* — сервис, запускающий программу копирования информации.

- */etc/biorobot.conf* — файл конфигурации ПО.

3) Диагностическое ПО:

- */lib/systemd/system/biorobot_test.service* — сервис, запускающий тестирование работоспособности при загрузке сервиса драйвера.

- */usr/bin/biorobot_autotest* — программа для тестирования круглосуточной работы АПК.

- */usr/lib/biorobot/isolationtest1* и */usr/lib/biorobot/isolationtest2* — программы для проверки отсутствия цепи между PC1 и PC2, устанавливается в */usr/bin/biorobot_isolationtest*.

4) Настройки для *udev*:

- */etc/udev/rules.d/automount.rules* — правило для *udev*, запускающее программу копирования при подключении Накопителя данных.

5) Настройка для регистрации событий *rsyslog*:

- */etc/rsyslog.d/90-biorobot.conf* — файл настроек журналирования *rsyslog*.

- */etc/logrotate.d/biorobot* — файл настроек ротации файлов журнала.

6) Прочие настройки:

- */etc/sysctl.d/90-biorobot.conf* — конфигурация для отключения режима вывода отладочной информации на консоль при подключении носителя информации.

5.5. Установка ПО

Установка пакета производится командой:

```
dpkg -i biorobot-<версия>.deb
```

При установке пакета необходимо выбрать, на какой ПЭВМ он устанавливается: «PC1» или «PC2», см. рисунок 2:

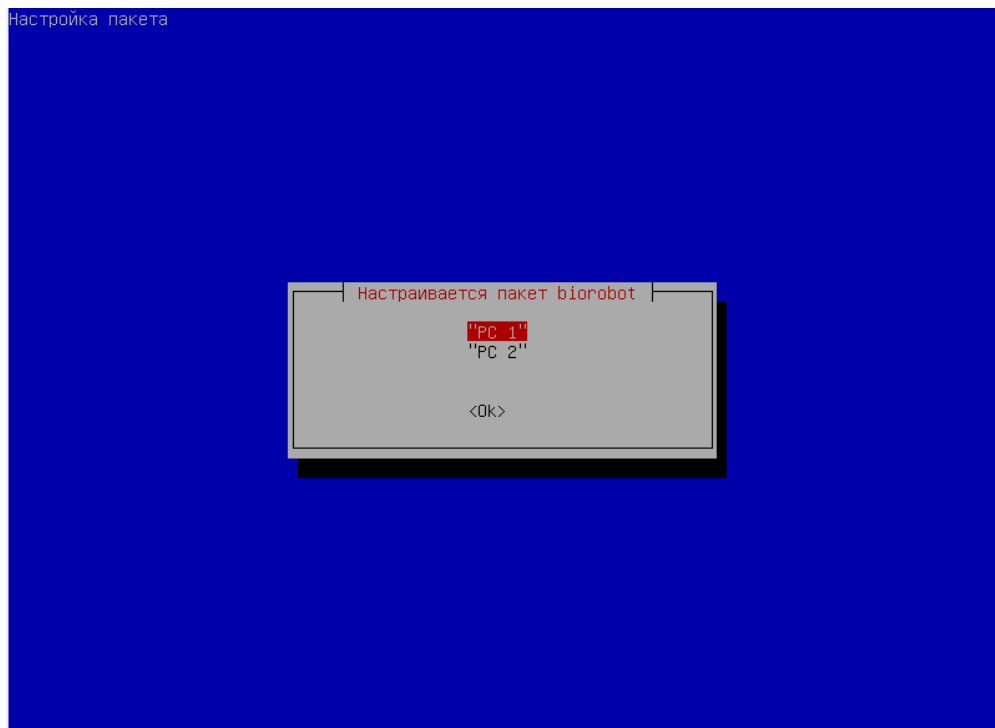


Рисунок 2: Установка пакета

В случае, если имена ПЭВМ отличаются от «PC1» и «PC2», важно указать правильную настройку при установке пакета в соответствии с подключением ПЭВМ к разъёмам АПК («PC1» и «PC2»).

При настройке АПК в случае подключения устройства к ПЭВМ через конвертеры интерфейса RS-232 необходимо проверить имя устройства, определяемое операционной системой (например, с помощью команды *dmesg*). Если имя устройства отличается от */dev/ttyS0* или */dev/ttyUSB0*, необходимо указать его в настройках ПО.

Для настройки имени устройства в драйвере отредактировать файл `/lib/systemd/system/biorobot_driver.service`, в строке `ExecStart` в параметре `-d` указать имя устройства. Например так:

```
ExecStart=/usr/bin/biorobot_driver -d /dev/ttyUSB1
```

Затем выполнить команды:

```
systemctl daemon-reload
```

```
systemctl restart biorobot_driver
```

Если параметр `-d` драйвера не указан, сначала опрашивается `/dev/ttyUSB0`, затем `/dev/ttyS0`.

При корректном подключении Переключателя к ПЭВМ PC1 и PC2 в процессе работы ПО должны быть слышны характерные щелчки со стороны Переключателя.

5.6. Описание конфигурации

В конфигурационном файле `/etc/biorobot.conf` следующие настройки:

1) *wait_timeout* — устанавливает время одного цикла ожидания исходящих файлов.

2) *twait* — количество циклов ожидания исходящих файлов.

3) *lock_wait* — время ожидания для проверки поступления новых данных.

4) *umount_timeout* — таймаут после размонтирования накопителя.

5) *this_pc* — абонентский пункт (pc1 или pc2).

5.7. Настройка регистрации событий безопасности

В ПО предусмотрена регистрация следующих типов событий безопасности:

Таблица 2: Типы событий безопасности

№	Тип события	Источники событий
0	Запуск программы	biorobot_driver
1	Завершение программы	biorobot_script

		biorobot_autotest biorobot_isolationtest
2	Подключение накопителя данных	biorobot_script
3	Отключение накопителя данных	
4	Перенос файлов и каталогов на накопитель данных	
5	Перенос файлов и каталогов с накопителя данных	
6	Нарушение доступности накопителя данных	
7	Нарушение целостности переносимых файлов	
8	Нарушение штатного функционирования программы	
9	Режим проверки работоспособности	biorobot_script -t
10	Режим проверки гальванической развязки	biorobot_isolationtest
11	Режим проверки круглосуточной работы	biorobot_autotest
12	Отправка управляющей команды	biorobot_driver

Для выбора типов событий безопасности для регистрации необходимо произвести следующие действия:

1) Отредактировать файл */lib/systemd/system/biorobot_driver.service*, в строке *ExecStart* в параметре *-e* указать номера типов событий для регистрации через запятую, например для регистрации всех событий программы:

```
ExecStart=/usr/bin/biorobot_driver -e 0,1,8,12
```

Если параметр *-e* драйвера не указывать, регистрируются все события. Для отключения регистрации всех событий драйвера необходимо в параметре *-e* передать *-1*: *ExecStart=/usr/bin/biorobot_driver -e -1*

2) Отредактировать файл */lib/systemd/system/biorobot_switch@.service*, в строке *ExecStart* вторым параметром указать номера типов событий для регистрации через запятую, например для регистрации всех событий программы:

```
ExecStart=/usr/bin/biorobot_script %I 0,1,2,3,4,5,6,7,8,9
```

Если второй параметр скрипта копирования не указывать, регистрируются все события. Для отключения регистрации всех событий скрипта копирования необходимо вторым параметром передать *-1: ExecStart=/usr/bin/biorobot_script %I -1*

3) Отредактировать файл */lib/systemd/system/biorobot_test.service*, в строке *ExecStart* вторым параметром указать номера типов событий для регистрации через запятую, например для регистрации всех событий программы проверки работоспособности:

```
ExecStart=/usr/bin/biorobot_script -t 9
```

Если второй параметр скрипта копирования не указывать, регистрируются все события. Для отключения регистрации всех событий необходимо вторым параметром передать *-1: ExecStart=/usr/bin/biorobot_script -t -1*

Если второй параметр скрипта копирования не указывать,

4) Выполнить команды:

```
systemctl daemon-reload
```

```
systemctl restart biorobot_driver
```

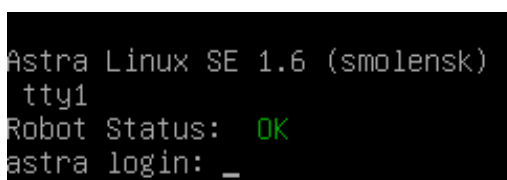
6. Порядок проверки работоспособности

6.1. Автоматизированная проверка

Автоматизированная проверка работоспособности запускается при загрузке ОС, после установки пакета, либо при ручной перезагрузке сервиса драйвера командой:

```
systemctl restart biorobot_driver
```

Результат успешной проверки работоспособности отображается на всех свободных консолях ПЭВМ PC1 и PC2 в строке «*Robot Status:*», см. рисунок 3:



```
Astra Linux SE 1.6 (smolensk)
tty1
Robot Status: OK
astra login: _
```

Рисунок 3: Статус ПО (после проверки работоспособности)

АПК признается функционирующим, если на консолях ПЭВМ PC1 и PC2 появляется надпись «*Robot Status: OK*» в пределах времени, установленного в технических условиях ДАКЖ.467239.002 ТУ, см. таблица 3.

Таблица 3: Временные показатели установления работоспособности АПК

Показатель	Описание показателя	Алгоритм измерения	Время (не менее), мин
Время готовности к работе	Период между включением АПК и началом выполнения АПК теста на работоспособность	Время между включением АПК и появлением сообщения «Biorobot status: Warning (UNKNOWN status)» на ПЭВМ PC1 и PC2 (рис. 6)	1
Время подготовки к работе	Период между началом выполнения АПК теста на	Время между появлением сообщения «Biorobot status: Warning (UNKNOWN	10

Показатель	Описание показателя	Алгоритм измерения	Время (не менее), мин
	работоспособность и установлением работоспособности АПК	status)» и появлением сообщения «Biorobot status: ОК» на ПЭВМ PC1 и PC2 (рис. 7)	

6.2. Ручная проверка

Режим ручной проверки работоспособности выполняется командой:

```
/usr/bin/biorobot_script -t
```

```
root@pc1:~/biorobot_script# biorobot_script -t
Запуск автоматической проверки работоспособности
Контрольная сумма (отправлено): 381038c1ce99f156ffd3b77c11c40e2decb5863ea8cac1745bd092d59982feb5
Ожидаем ответ...
Контрольная сумма (доставлено): 381038c1ce99f156ffd3b77c11c40e2decb5863ea8cac1745bd092d59982feb5
Проверка пройдена
```

Рисунок 4: Проверка работоспособности

В данном режиме проверки будет создан тестовый файл и подготовлен для передачи на другой ПЭВМ. На обеих сторонах с файла снимутся контрольные суммы и сравнятся. Если значения совпадают, то выведется сообщение «Проверка пройдена», иначе, выведется сообщение «Проверка НЕ пройдена». Система считается работоспособной при совпадении контрольных сумм, см. рисунок 4.

Результат ручной проверки работоспособности также отображается на всех свободных консолях ПЭВМ PC1 и PC2 в строке «*Robot Status:*», см. рисунок 3.

6.3. Проверки для периодических и приёмо-сдаточных испытаний

6.3.1. Проверка круглосуточной работы

Режим тестирования круглосуточной работы АПК представляет собой непрерывное автоматическое создание файлов и передачу их на другой ПЭВМ. Запуск данного режима выполняется командой на ПЭВМ PC1 и PC2 одновременно:

biorobot_autotest

Во время работы программы нельзя выполнять какие либо действий по передаче информации через АПК.

Работа программы выполняется непрерывно до нажатия комбинации клавиш Ctrl+C одновременно на ПЭВМ PC1 и PC2. В процессе работы программы будут создаваться файлы случайного размера со случайными именами и передаваться на другой ПЭВМ. С генерируемых и принятых файлов снимаются контрольные суммы и записываются в файл */tmp/autotest.stat*. По завершении работы снимается контрольные суммы с принятых файлов, выводится результирующая контрольная сумма полученного файла */tmp/autotest.stat* с каждой стороны. АПК считается выдержавшим проверку, если не менее, чем за 24 ч в работе программы «*biorobot_autotest*» не было отказов и сбоев и результирующие контрольные суммы на ПЭВМ PC1 и PC2 совпали, см. рисунок 5.

```
administrator@relay-test1:~$ sudo biorobot_autotest
Программа для проверки АПК в круглосуточном режиме работы (версия 1.6 для pc1)
Программа должна запускаться синхронно на ПЭВМ PC1 и PC2
ВНИМАНИЕ: будут удалены все файлы на передачу и все ранее принятые файлы!!!
Для продолжения нажмите любую клавишу, для отмены нажмите Ctrl+C...
Запущен процесс генерации файлов для передачи через Переключатель...
Для завершения генерации файлов нажмите Ctrl+C синхронно на ПЭВМ PC1 и PC2
Сформирован файл с md5 суммой: d77b94eee8ad01c4e4b804fe9ecd26a2 niMesjUd
^Снажатие Ctrl+C...Идёт остановка генерации файлов...
Результирующая контрольная сумма будет рассчитана через 5 минут...
Результирующая контрольная сумма: 7261be644627a5b35c3ee7cb947fa812
```

Рисунок 5: Проверка круглосуточной работы АПК

6.3.2. Проверка отсутствия цепи между ПЭВМ

Режим проверки отсутствия цепи между ПЭВМ представляет собой пошаговую процедуру. Запуск данного режима выполняется командой на ПЭВМ PC1 и PC2 одновременно:

biorobot_isolationtest

Программа представляет собой пошаговый алгоритм работы ПО на ПЭВМ РС1 и РС2. В процессе работы программы необходимо следовать инструкциям и синхронно переключать шаги на ПЭВМ РС1 и РС2, на каждом шаге производить измерения на отсутствие цепей между контактами в режиме измерения сопротивления. Для выполнения теста необходимо дополнительное оборудование (мультиметр). АПК считается выдержавшим испытания, если при проверке отсутствует цепь между всеми одноимёнными контактами кабелей USB и кабелей связи по RS232 на всех шагах работы АПК, более подробно данное испытание описано в технических условиях ДАКЖ.467239.002 ТУ.

7. Описание операций

7.1. Функциональные задачи администратора

В функции системного администратора входит:

- 1) Управление политиками безопасности в системе;
- 2) Сборка АПК;
- 3) Установка и настройка ОС на ПЭВМ;
- 4) Установка и настройка ПО для АПК на ПЭВМ;
- 5) Мониторинг событий безопасности;
- 6) Диагностика и мониторинг работоспособности ПО и АПК.

7.2. Управление политиками безопасности

Требования к политикам безопасности описаны в п.п. 3, 4, 5.7 настоящего документа.

7.3. Сборка АПК

Сборка АПК описана в п.п. 5.1-5.3 настоящего документа.

7.4. Установка ОС и ПО

Установка ОС осуществляется в соответствии с инструкциями для ОС Astra Linux. Требования к ОС описаны в п.п. 2.3 настоящего документа. Установка ПО описана в п.п. 5.4-5.6 настоящего документа.

7.5. Мониторинг событий безопасности

Журнал регистрации событий безопасности ведётся в файле */var/log/biorobot.log*.

Состав и содержание записей журнала регистрации событий:

- 1) дата и время;
- 2) программный компонент источника события (имя ПЭВМ и компонента ПО);
- 3) тип события (из таблицы 2);

- 4) результат события (OK, ERROR, WARNING);
- 5) для событий запуска и завершения программы: наименование и версия программы;
- 6) для событий регистрации подключения и отключения накопителя данных: логическое имя подключаемого носителя информации;
- 7) для событий регистрации переноса файлов и каталогов: логическое имя файла, контрольная сумма.

Пример записей журнала регистрации событий безопасности:

```
Feb 15 19:19:47 pc2 biorobot_driver: OK <Запуск программы> Запуск программы управления переключателем
на PC2 версия 1.8
Feb 15 19:19:48 pc2 biorobot_script: OK <Запуск программы> Запущен скрипт версии 1.8 для pc2
Feb 15 19:19:48 pc2 biorobot_script: OK <Режим проверки работоспособности> Запуск автоматической
проверки работоспособности
Feb 15 19:19:48 pc2 biorobot_script: WARNING <Режим проверки работоспособности> Изменение статуса:
WARNING (UNKNOWN status)
Feb 15 19:19:48 pc2 biorobot_script: OK <Подключение накопителя данных> Монтируем /dev/sda1
Feb 15 19:19:48 pc2 biorobot_script: OK <Перенос файлов и каталогов на накопитель данных>
Файл .biorobot_test.9M9UHEp0 принят успешно 24d4568a60fd5ba6bfe886c749a2afe4492a947cac4ec896ee3ff7
Feb 15 19:19:48 pc2 biorobot_script: OK <Перенос файлов и каталогов на накопитель данных> Удаление
файлов с носителя
Feb 15 19:19:48 pc2 biorobot_script: OK <Перенос файлов и каталогов на накопитель данных> Были
отправлены файлы с pc1: ".biorobot_test.9M9UHEp0",
Feb 15 19:19:48 pc2 biorobot_script: OK <Перенос файлов и каталогов с накопителя данных> Ожидание
данных для копирования
Feb 15 19:20:05 pc2 biorobot_script: OK <Перенос файлов и каталогов с накопителя данных> Скопирован
файл ".biorobot_test.juNgXxC9" с контрольной суммой 987f15a3b66c09b6939d3f99c117262a375
Feb 15 19:20:05 pc2 biorobot_script: OK <Отключение накопителя данных> Размонтирование /dev/sda1
Feb 15 19:20:20 pc2 biorobot_script: OK <Завершение программы> Сигнал на переключение процессу драйвера
(PID=431)
Feb 15 19:20:20 pc2 biorobot_script: OK <Завершение программы> Завершение работы скрипта
Feb 15 19:20:20 pc2 biorobot_driver: OK <Отправка управляющей команды> Отправка сигнала переключателю
от PC2 на переключение
Feb 15 19:21:13 pc2 biorobot_script: OK <Запуск программы> Запущен скрипт версии 1.8 для pc2
Feb 15 19:21:13 pc2 biorobot_script: OK <Подключение накопителя данных> Монтируем /dev/sda1
Feb 15 19:21:13 pc2 biorobot_script: OK <Перенос файлов и каталогов с накопителя данных> На pc1 были
переданы файлы: ".biorobot_test.juNgXxC9",
Feb 15 19:21:13 pc2 biorobot_script: OK <Перенос файлов и каталогов на накопитель данных> Файл
".biorobot_test.juNgXxC9" с контрольной суммой 987f15a3b66c09b6939d3f99c117262a3751c1c98ad8c
Feb 15 19:21:13 pc2 biorobot_script: OK <Режим проверки работоспособности> Файл
".biorobot_test.juNgXxC9" успешно доставлен
Feb 15 19:21:13 pc2 biorobot_script: OK <Перенос файлов и каталогов с накопителя данных> Ожидание
данных для копирования
Feb 15 19:21:14 pc2 biorobot_script: OK <Режим проверки работоспособности> Проверка прошла успешно
Feb 15 19:21:14 pc2 biorobot_script: OK <Режим проверки работоспособности> Изменение статуса: OK
Feb 15 19:21:14 pc2 biorobot_script: OK <Режим проверки работоспособности> Завершение автоматической
проверки работоспособности
```

Для просмотра журнала можно использовать любые встроенные в ОС средства просмотра журналов, например:

```
less /var/log/biorobot.log
```

```
tail -f /var/log/biorobot.log
```

Настройки журналирования осуществляются с помощью сервисов ОС `rsyslog` и `logrotate`. Настройки журналирования устанавливаются при установке ПО и менять их нежелательно.

Содержимое файла настройки ротации журнала и его сжатия `/etc/logrotate.d/biorobot`:

```
/var/log/biorobot.log rotate 12 {  
    monthly  
    compress  
    missingok  
    notifempty }
```

Описание настроек файла ротации:

- `/var/log/biorobot.log` — имя файла журнала;
- `rotate 12` — количество хранимых старых файлов журналов;
- `monthly` — частота ротации файлов журнала, допустимые значения: `hourly`, `daily`, `weekly`, `yearly`;
- `compress` — сжатие файлов журналов;
- `missingok` — не выводить ошибки при отсутствии файла журнала;
- `notifempty` — не ротировать пустой файл журнала.

При настройках ротации по умолчанию, в каталоге `/var/log` создаются каждый месяц сжатые файлы журналов `/var/log/biorobot.log.1.gz`, `/var/log/biorobot.log.2.gz` и т. д., сжатые файлы хранятся в течении года.

Для того, что бы обратиться к сжатым файлам, можно использовать стандартны утилиты ОС, например:

```
zcat /var/log/biorobot.log.1.gz | less
```

7.6. Диагностика и мониторинг работоспособности ПО и АПК

Текущий статус работы ПО выводится на все текстовые консоли ОС в строке *Robot Status*:

После загрузки ОС на ПЭВМ PC1 и PC2 запускается проверка работоспособности АПК, которая устанавливает статус работы ПО на ПЭВМ.

Также можно запустить ручную проверку работоспособности с помощью команды *biorobot_script -t*, которая также устанавливает статус работы ПО на ПЭВМ.

На рисунке 6 — статус после загрузки ОС до запуска проверки работоспособности:

```
Astra Linux SE 1.6 (smolensk)
tty1
Robot Status:  WARNING (UNKNOWN status)
astra login: _
```

Рисунок 6: Статус ПО (при включении)

На рисунке 7 — статус после успешной проверки работоспособности:

```
Astra Linux SE 1.6 (smolensk)
tty1
Robot Status:  OK
astra login: _
```

Рисунок 7: Статус ПО (после проверки работоспособности)

Текущий статус работы драйвера можно проверить командой:

```
systemctl status biorobot_driver
```

Текущий статус работы скрипта проверки работоспособности можно проверить командой:

```
systemctl status biorobot_test
```

Текущий статус работы ПО (который также отображается на всех консолях в строке *Robot Status:*) можно проверить командой:

```
biorobot_script -s
```

Список всех статусов работы ПО и действий администратора приведены в таблице 4:

Таблица 4: Статусы работы ПО

Статус работы	Описание статуса	Действие администратора
ОК	ПО АПК работает исправно, последнее автоматизированное тестирование работоспособности успешно выполнено (<i>biorobot_script -t</i>)	-
WARNING (UNKNOWN status)	Выполняется процедура автоматизированного тестирования работоспособности ПО АПК (<i>biorobot_script -t</i>)	<p>В случае долгого сохранения статуса (более 5 минут) и присутствия характерных щелчков со стороны Переключателя необходимо проверить файловую систему и работоспособность накопителя данных и в случае неисправности заменить накопитель данных или произвести ремонт, проверить работоспособность ПЭВМ и файловую систему ПЭВМ и произвести замену или ремонт ПЭВМ, проверить исправность кабеля соединения USB и RS232 и заменить неисправный кабель.</p> <p>В случае отсутствия характерных щелчков со стороны устройства Переключатель необходимо проверить схему сборки АПК, настройки ПО, проверить исправность Переключателя и в случае неисправности Переключателя провести ремонт согласно руководству по эксплуатации ДАКЖ.467239.002 РЭ (п.5) или замену Переключателя. Повторно включить АПК и ПЭВМ.</p>
ERROR (Self diagnostic failed)	Процедура автоматизированного тестирования работоспособности ПО АПК	Необходимо проверить схему сборки АПК, настройки ПО, проверить файловую систему и работоспособность накопителя

	(<i>biorobot_script -t</i>) выполнена неуспешно	данных и в случае неисправности заменить накопитель данных или произвести ремонт, проверить работоспособность ПЭВМ и файловую систему ПЭВМ и произвести замену или ремонт ПЭВМ, проверить исправность кабеля соединения USB и RS232 и заменить неисправный кабель, проверить исправность Переключателя и в случае неисправности Переключателя провести ремонт согласно руководству по эксплуатации ДАКЖ.467239.002 РЭ (п.5) или замену Переключателя. Повторно включить АПК и ПЭВМ.
ERROR (Integrity violation)	Сбой передачи файла в процессе работы АПК (несоответствие контрольных сумм при передаче)	Проверить файловую систему и работоспособность накопителя данных и в случае неисправности заменить накопитель данных или произвести ремонт, проверить работоспособность ПЭВМ и файловую систему ПЭВМ и произвести замену или ремонт ПЭВМ, проверить исправность кабеля соединения USB и RS232 и заменить неисправный кабель, проверить исправность Переключателя и в случае неисправности Переключателя провести ремонт согласно руководству по эксплуатации ДАКЖ.467239.002 РЭ (п.5) или замену Переключателя. Повторно включить АПК и ПЭВМ.
ERROR (USB drive failed)	Сбой при обращении к накопителю данных в процессе работы АПК	Проверить файловую систему и работоспособность накопителя данных и в случае неисправности заменить накопитель данных или произвести ремонт, проверить исправность кабеля соединения USB и заменить неисправный кабель. Повторно включить АПК и

		ПЭВМ.
ERROR (Biorobot script failed)	Сбой ПО копирования данных в процессе работы АПК	Проверить исправность кабеля соединения RS232 и USB и заменить неисправный кабель, проверить файловую систему и работоспособность накопителя данных и в случае неисправности заменить накопитель данных или произвести ремонт, проверить исправность Переключателя и в случае неисправности Переключателя провести ремонт согласно руководству по эксплуатации ДАКЖ.467239.002 РЭ (п.5) или замену Переключателя. Повторно включить АПК и ПЭВМ.

