

ПРОГРАММА СЕРВИСНОГО УСТРОЙСТВА КИТП-КОНФИГУРАТОР

Инструкция по эксплуатации

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящий документ содержит информацию, необходимую для эксплуатации программы сервисного устройства КИТП-конфигуратор (далее – программа, программное обеспечение, ПО)
- 1.2. Исключительные права на программу принадлежат ООО «Элтех», г. Тверь (далее - компания).
- 1.3. Программа встраивается в сервисное устройство для обслуживания и настройки телеметрических систем (далее сервисное устройство, СУ) и не распространяется отдельно от него.
- 1.4. Настоящий документ подлежит размещению на официальном сайте компании в сети интернет, расположенном по адресу <https://eltech-tver.ru>.

2 ОБЩИЕ СВЕДЕНИЯ

Настоящее руководство по эксплуатации предназначено для изучения обслуживающим персоналом устройства, порядка подготовки к работе и правил эксплуатации программы сервисного устройства КИТП-конфигуратор.

В настоящем руководстве приведены сведения, необходимые для настройки операционной системы РЕД ОС, работы с модулем связи «UA-Modem», антивирусной защиты, взаимодействия программы с контроллерами телеметрии КИТП-01 и КИТП-02, проведения инвентаризации, обновления и восстановления программного обеспечения.

3 НАЗНАЧЕНИЕ

ПО предназначено для локального конфигурирования, диагностики, технического обслуживания и обновления встроенного программного обеспечения устройств телеметрии без использования каналов связи и подключения к информационно-телекоммуникационным сетям.

ПО не выполняет обработку или преобразование результатов измерений и используется исключительно для конфигурирования, отображения, диагностики и технического обслуживания устройств телеметрии.

3 СОСТАВ

Сервисное устройство, на котором исполняется программа, представляет собой программно-аппаратный комплекс, предназначенный для локального взаимодействия с устройствами телеметрии производства ООО «Элтех».

В состав сервисного устройства входят:

- аппаратная платформа;
- операционная система РЕД ОС;
- программное обеспечение сервисного устройства;
- драйверы устройств;
- кабель подключения к устройствам телеметрии;
- комплект эксплуатационной документации.

4 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Аппаратной платформой сервисного устройства является переносной персональный компьютер. Конкретное исполнение аппаратной платформы определяется комплектом поставки и спецификацией сервисного устройства.

Наименование параметра	Значение
Тип аппаратной платформы	Переносной персональный компьютер (ноутбук)
Операционная система	РЕД ОС
Интерфейс локального подключения к устройствам телеметрии	USB
Поддерживаемые устройства	КИТП-01; КИТП-02*
Режим работы	Периодический, при выполнении настройки, диагностики и технического обслуживания

5 ПОДГОТОВКА К ЭКСПЛУАТАЦИИ

Перед началом эксплуатации необходимо проверить комплектность СУ, исправность аппаратной платформы и кабелей подключения, наличие установленной операционной системы РЕД ОС, программного обеспечения и необходимых драйверов.

Настройку учетных записей, режима киоска и средств регистрации событий информационной безопасности выполнить в соответствии с разделом 6 настоящего руководства.

Антивирусное программное обеспечение должно быть установлено и настроено в операционной системе СУ. Конкретное наименование и версия антивирусного программного обеспечения указываются в комплекте программной документации и должны быть совместимы с применяемой версией РЕД ОС.

При эксплуатации СУ подключение к сети Интернет не допускается. В составе программного обеспечения СУ не должны использоваться сервисы электронной почты. Сетевые интерфейсы и службы, не требуемые для выполнения функций СУ, должны быть отключены или заблокированы.

6 НАСТРОЙКА ОПЕРАЦИОННОЙ СИСТЕМЫ РЕД ОС

6.1 Общие сведения

Настоящий раздел содержит порядок настройки учетных записей пользователей, разграничения прав доступа, ограничения доступа пользователей в режиме киоска, а также порядок просмотра журналов событий информационной безопасности средствами операционной системы РЕД ОС.

Для эксплуатации сервисного устройства предусматриваются учетные записи администратора и пользователей программы конфигурирования КИТП. Пользователи программы конфигурирования КИТП в зависимости от предоставленных полномочий подразделяются на три типа.

Тип пользователя	Группа разграничения доступа	Назначение
Администратор	GRP_Installer	Пользователь с правами администратора
Супервизор	GRP_Supervisor	Пользователь с правами супервизора
Оператор	GRP_Worker	Пользователь с правами оператора

Конкретный состав доступных функций прикладного программного обеспечения определяется группой разграничения доступа, в которую включена учетная запись пользователя.

Каждый пользователь, предназначенный для работы с программой конфигурирования КИТП, должен входить в одну и только одну группу разграничения доступа из перечня GRP_Installer, GRP_Supervisor, GRP_Worker.

При необходимости перечень групп разграничения доступа может быть расширен. Наименование дополнительной группы должно начинаться с префикса GRP_. При расширении перечня пользователь также должен входить в одну и только одну группу разграничения доступа с префиксом GRP_.

Независимо от типа пользователя все учетные записи, предназначенные для работы с программой конфигурирования КИТП, должны входить в группы dialout и kiosk_users.

Пользователи программы конфигурирования КИТП не должны входить в группы wheel и root. Выполнение данного требования исключает предоставление пользователю административных полномочий операционной системы.

Учетная запись администратора предназначена для настройки операционной системы РЕД ОС, управления учетными записями, настройки программного обеспечения и выполнения иных административных функций. Администратор должен входить в группу `wheel`. В зависимости от выполняемых функций администратор может дополнительно входить в группы `desktop_users`, `dialout`, `kfladmin`, `kfluser` и другие группы, необходимые для выполнения возложенных на него функций.

Прикладное программное обеспечение сервисного устройства запускается для пользователей программы конфигурирования КИТП в режиме киоска с ограниченным доступом к функциям операционной системы РЕД ОС.

6.2 Создание учетной записи администратора

Создание учетной записи администратора может выполняться средствами графического окружения MATE либо из терминала.

6.3 Создание администратора средствами графического интерфейса MATE

- 1) Открыть Главное меню и перейти в раздел «Администрирование» → «Менеджер Пользователей MATE» (рисунок 1). При запросе ввести пароль текущего администратора (`root`).
- 2) В открывшемся окне нажать кнопку «Добавить пользователя». Ввести имя пользователя (логин латинскими символами), полное имя и задать пароль.
- 3) Выделить созданную учетную запись и открыть настройку групп.
- 4) Включить пользователя в группу `wheel`. При необходимости выполнения дополнительных функций включить администратора также в требуемые группы, например `desktop_users`, `dialout`, `kfladmin`, `kfluser`.
- 5) Сохранить внесенные изменения.

6.4 Создание администратора из терминала

Для создания учетной записи администратора из терминала MATE выполнить команду:

```
sudo useradd -m -G wheel <имя_пользователя>
```

Для назначения пароля созданной учетной записи выполнить команду:

```
sudo passwd <имя_пользователя>
```

После выполнения команды система запросит ввод и повторное подтверждение пароля. Вводимые символы пароля на экране не отображаются.

6.5 Создание учетной записи пользователя программы конфигурирования КИТП

Учетная запись пользователя программы конфигурирования КИТП предназначена для штатной работы с прикладным программным обеспечением сервисного устройства в режиме киоска.

При создании учетной записи пользователю должен быть назначен один из предусмотренных типов доступа путем включения в одну и только одну группу разграничения доступа.

Тип пользователя	Группа
Администратор	GRP_Installer
Супервизор	GRP_Supervisor
Оператор	GRP_Worker

Дополнительно пользователь должен быть включен в группы `kiosk_users` и `dialout`.

Включение пользователя одновременно в две или более группы, наименования которых начинаются с `GRP_`, не допускается.

Пользователь не должен входить в группы `wheel` и `root`.

Таким образом, состав групп должен включать:

- для пользователя типа «Администратор» — `GRP_Installer`, `kiosk_users`, `dialout`;
- для пользователя типа «Супервизор» — `GRP_Supervisor`, `kiosk_users`, `dialout`;
- для пользователя типа «Оператор» — `GRP_Worker`, `kiosk_users`, `dialout`.

6.6 Создание пользователя программы конфигурирования КИТП средствами графического интерфейса MATE

1. Открыть Главное меню → «Система» → «Администрирование» → «Менеджер Пользователей MATE» и ввести пароль администратора (рисунок 1).

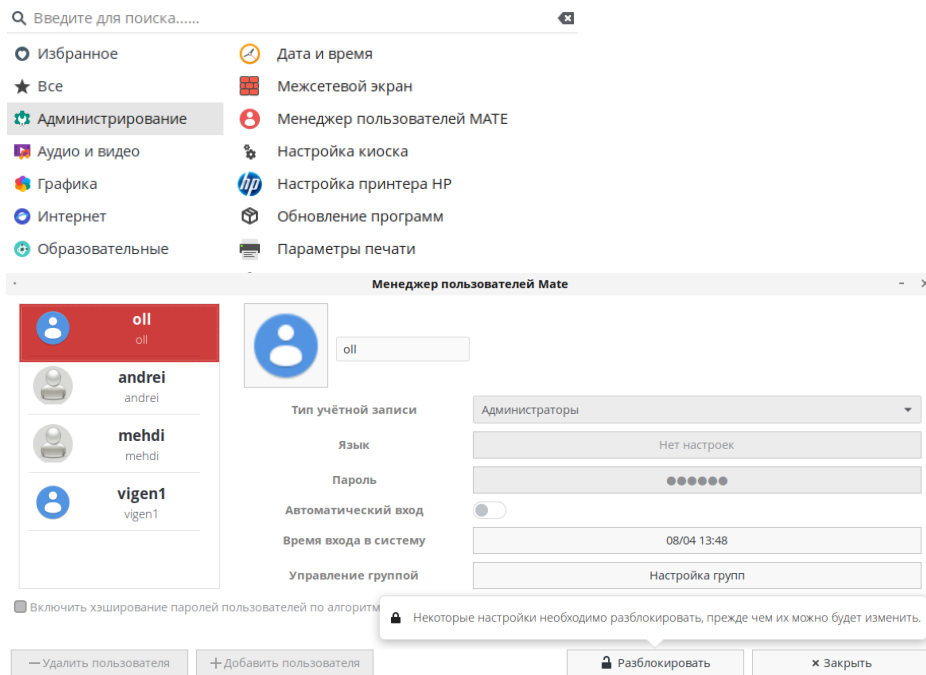


Рисунок 1. Администрирование пользователей

2. Нажать кнопку «Добавить пользователя». Ввести имя пользователя (логин латинскими символами) и задать пароль (рисунок 2).

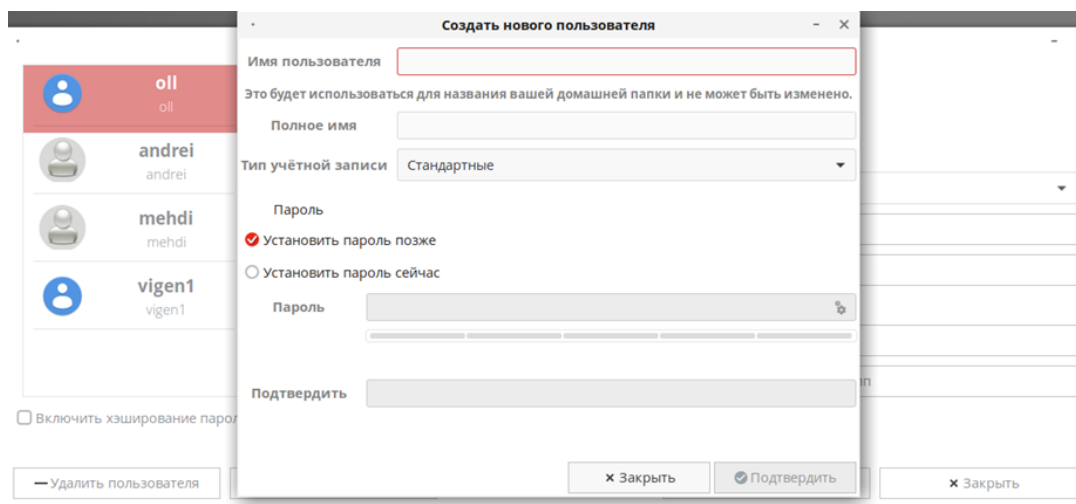


Рисунок 2. Создание пользователя

3. Открыть свойства созданной учетной записи и перейти к настройке групп (рисунок 3).

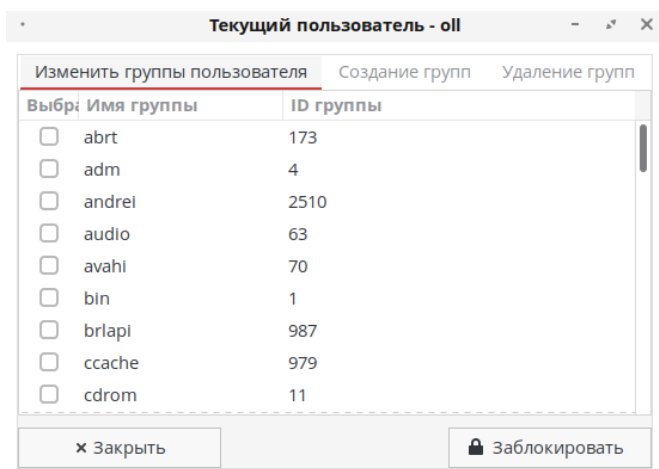


Рисунок 3. Настройка группы пользователя

4. Убедиться, что пользователь не включен в группы wheel и root.
 5. Включить пользователя в группы kiosk_users, dialout и в одну из групп разграничения доступа: GRP_Installer, GRP_Supervisor или GRP_Worker (рисунок 4). Одновременное включение пользователя в несколько групп с префиксом GRP_ не допускается.

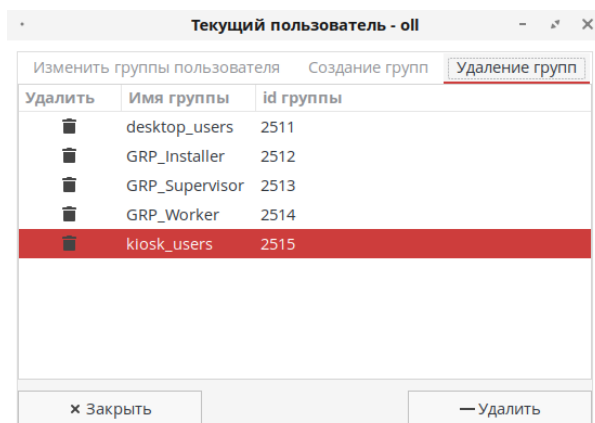


Рисунок 4. Выбор групп пользователя

6. Сохранить внесенные изменения.

6.7 Создание пользователя программы конфигурирования КИТП из терминала

Для создания учетной записи необходимо выбрать тип пользователя и выполнить соответствующую команду.

Пользователь типа «Администратор»:

```
sudo useradd -m -G kiosk_users,dialout,GRP_Installer
<имя_пользователя>
```

Пользователь типа «Супервизор»:

```
sudo useradd -m -G kiosk_users,dialout,GRP_Supervisor
```

<имя_пользователя>

Пользователь типа «Оператор»:

```
sudo useradd -m -G kiosk_users,dialout,GRP_Worker
```

<имя_пользователя>

Для назначения пароля созданной учетной записи выполнить команду:

```
sudo passwd <имя_пользователя>
```

После создания учетной записи необходимо проверить ее членство в группах. Пользователь должен входить в `kiosk_users`, `dialout` и только одну группу с префиксом `GRP_`; членство в группах `wheel` и `root` не допускается.

6.8 Настройка режима киоска

Для пользователей программы конфигурирования КИТП сервисного устройства должен быть активирован режим киоска. Дополнительно необходимо исключить возможность запуска терминала стандартным сочетанием клавиш.

6.9 Отключение сочетания клавиш запуска терминала

Настройка выполняется в графическом сеансе соответствующего пользователя программы конфигурирования КИТП.

1. Открыть Главное меню → «Параметры» → «Сочетания клавиш и клавиатуры» (рисунок 5).

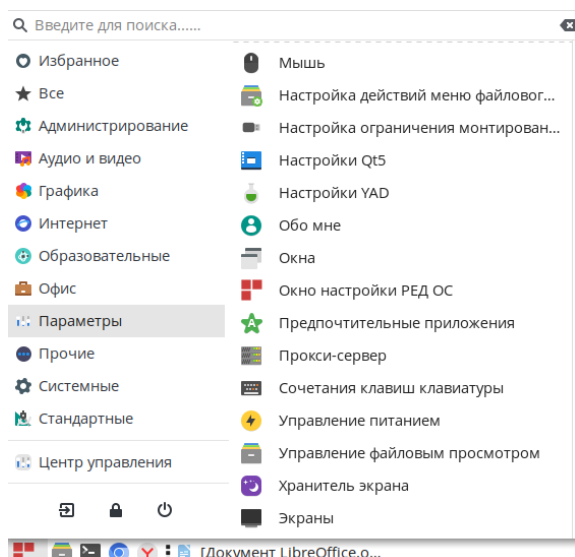


Рисунок 5. Сочетания клавиш

2. В списке действий открыть категорию «Рабочий стол».
3. Найти действие «Открыть терминал», для которого назначено сочетание `Ctrl+Alt+T` (рисунок 6).

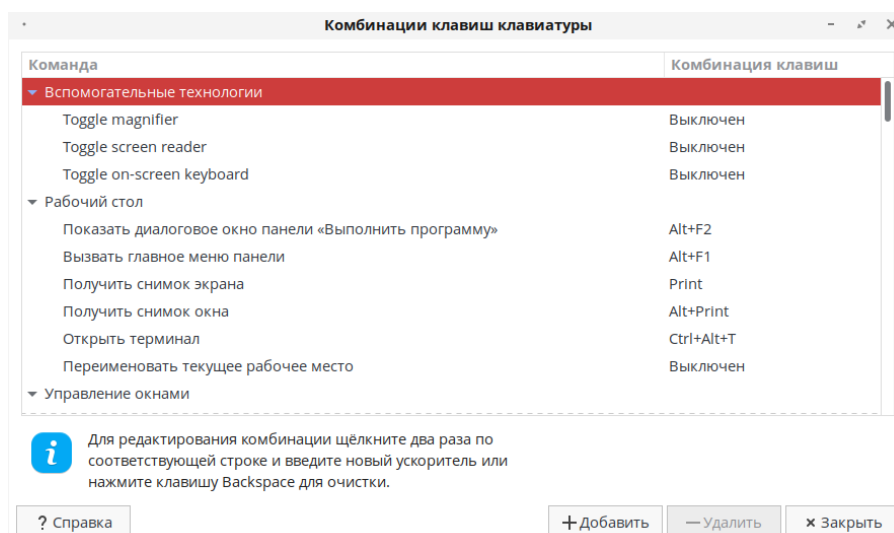


Рисунок 6. Открыть терминал

4. Выбрать указанное действие. После появления режима ввода нового сочетания нажать клавишу Backspace.
5. Убедиться, что для действия «Открыть терминал» установлено состояние «Выкл.».
6. Закрывать окно настройки.

6.10 Назначение сеанса киоска

Для выбора сеанса киоска в качестве сеанса по умолчанию необходимо от имени администратора открыть файл учетной записи пользователя:

```
sudo nano /var/lib/AccountsService/users/<USERNAME>
```

где <USERNAME> — имя пользователя программы конфигурирования КИТП.

В файле учетной записи установить параметр:

```
Session=single
```

Сохранить изменения сочетанием клавиш Ctrl+O, подтвердить сохранение клавишей Enter и закрыть редактор сочетанием Ctrl+X.

6.11 Просмотр журналов событий информационной безопасности

Регистрация событий информационной безопасности сервисного устройства выполняется средствами операционной системы РЕД ОС. Для просмотра записей журнала используется утилита ausearch.

Основные журналы, формируемые средствами РЕД ОС при работе конфигуратора на СУ, расположены по следующим путям:

/var/log/audit/audit.log – журналирование событий информационной безопасности.

`/var/log/messages` – журналирование событий работы программного обеспечения.

Примечание. Указанные журналы используются для просмотра и анализа событий, связанных с работой СУ и прикладного программного обеспечения.

6.12 Просмотр событий по типу

Для просмотра событий заданного типа выполнить команду:

```
sudo ausearch -m <тип_события> -i
```

При необходимости результаты могут быть дополнительно отфильтрованы по ключевому слову, например по имени пользователя:

```
sudo ausearch -m <тип_события> -i | grep <ключевое_слово>
```

Основные типы событий приведены в таблице.

Тип события	Назначение
USER_AUTH	События аутентификации пользователя, включая успешные и неуспешные попытки.
USER_START	Начало пользовательского сеанса.
USER_END	Завершение пользовательского сеанса.
ADD_GROUP	Создание группы пользователей.
DEL_GROUP	Удаление группы пользователей.
GRP_MGMT	Изменение состава или параметров группы пользователей.
USER_MGMT	Операции, связанные с группами и правами доступа (ролями).
USER	Регистрация события аудита о заполнении жесткого диска на 75 %.

6.13 Просмотр событий по ключу правила аудита

Для просмотра событий, зарегистрированных определенным правилом аудита, выполнить команду:

```
sudo ausearch -k <ключ_правила>
```

Используемые в конфигурации ключи правил аудита приведены в таблице.

Ключ правила	Назначение
конфигуратор	Регистрация запуска и завершения работы конфигуратора, а также результатов периодической проверки его целостности
changed_politics_passwd	Контроль изменения файла политики паролей
changed_audit_conf	Контроль изменения конфигурационных файлов auditd
changed_audit_rules	Контроль изменения правил auditd
read_audit_log	Регистрация чтения основного журнала аудита
changed_crc	Контроль изменения контрольной суммы целостности
cleared_audit_log	Регистрация очистки журнала событий информационной безопасности
roles_modifications	Регистрация изменения правил (ролей/групп) разграничения доступа учетных записей РЕД ОС

Для просмотра записей, связанных с запуском и завершением работы ПО конфигулятора, периодической проверкой целостности файла ПО конфигулятора (configurator.jar), а также сообщениями о возможном переполнении журнала ИБ, выполнить команду:

```
sudo grep "конфигуратор" /var/log/messages
```

6.14 Очистка журнала событий информационной безопасности

Очистка журнала событий информационной безопасности допускается только уполномоченным администратором. Удаление или редактирование отдельных записей журнала не допускается. Перед очисткой журнал должен быть сохранен в отдельный файл для последующего хранения и анализа.

Для сохранения текущего журнала в файл выполнить команду (путь и имя архивного файла задаются администратором):

```
sudo cp /var/log/audit/audit.log <путь_к_архиву>/audit_YYYY-MM-DD.log
```

После подтверждения сохранения архивной копии очистить основной файл журнала командой:

```
sudo truncate -s 0 /var/log/audit/audit.log
```

После очистки убедиться, что событие очистки зарегистрировано в новом журнале. Для контроля записи использовать ключ `cleared_audit_log`:

```
sudo ausearch -k cleared_audit_log -i
```

6.15 Ограничение взаимодействия с сетью Интернет

Штатная эксплуатация СУ не предусматривает подключения к сети Интернет. Доступ к ресурсам сети Интернет и использование сервисов электронной почты должны быть исключены.

После настройки СУ администратор должен убедиться в отсутствии доступа к сети Интернет. Проверка может быть выполнена встроенными средствами РЕД ОС, например командами `ping` и `traceroute`. Попытки обращения к внешним ресурсам должны завершаться неуспешно.

В эталонном перечне программного обеспечения СУ не должны присутствовать почтовые клиенты и серверные сервисы электронной почты, не требуемые для выполнения функций СУ.

6.16 Отключение небезопасных сетевых протоколов и служб

На СУ не допускается использование сетевых служб и сервисов, реализующих небезопасные протоколы, если они не требуются для выполнения

штатных функций изделия. Службы `ftpd`, `telnetd`, `rlogin` и `http` должны отсутствовать либо быть отключены (заблокированы).

После установки и обновления программного обеспечения администратор должен контролировать состав активных сетевых служб средствами РЕД ОС и отключать службы, не предусмотренные эксплуатационной документацией и эталонным перечнем программного обеспечения СУ.

6.17 Контроль целостности программного обеспечения СУ

Контроль целостности прикладного программного обеспечения СУ выполняется автоматически при запуске пользовательского сеанса в режиме киоска и периодически в процессе работы программы.

При входе в систему под учетной записью пользователя программы конфигурирования КИТП выполняется проверка соответствия файла `licence` контрольной сумме файла `configurator.jar`. При положительном результате проверки прикладное программное обеспечение СУ запускается автоматически. Событие запуска регистрируется в системном журнале `/var/log/messages` с меткой «конфигуратор» и описанием события.

При штатном завершении работы прикладного программного обеспечения соответствующее событие также регистрируется в `/var/log/messages` с меткой «конфигуратор».

Если при запуске обнаружено нарушение целостности, прикладное программное обеспечение СУ не запускается, событие регистрируется в `/var/log/messages` с меткой «конфигуратор», после чего пользовательский сеанс завершается.

Во время работы контроль целостности выполняется с периодичностью 60 с. При выявлении нарушения целостности пользователю выводится сообщение, пользовательский сеанс завершается, а событие регистрируется в `/var/log/messages` с меткой «конфигуратор».

Для просмотра записей, относящихся к запуску, завершению работы и результатам контроля целостности прикладного программного обеспечения, выполнить команду:

```
sudo grep "конфигуратор" /var/log/messages
```

Эксплуатация прикладного программного обеспечения при нарушении его целостности не допускается. Перед повторным запуском должна быть восстановлена эталонная версия программных файлов.

6.18 Контроль событий изменения паролей

События изменения паролей учетных записей пользователей СУ регистрируются средствами операционной системы РЕД ОС. После выполнения процедуры смены пароля администратор должен убедиться в наличии соответствующей записи в системном журнале безопасности `/var/log/secure`.

6.19 Настройка политики блокировки учетной записи

Для настройки политики времени блокировки и количества последовательных неуспешных попыток запуска сеанса работы в прикладном (специальном) ПО, а также других связанных с идентификацией и аутентификацией параметров необходимо следовать руководству РЕД ОС и настроить файл:

`/etc/security/faillock.conf`

Для просмотра статуса пользователя и сброса блокировки после неудачной авторизации пользователя выполнить в терминале:

`sudo faillock --user имя_пользователя --reset` – сбросить блокировку пользователя.

`sudo faillock --user имя_пользователя` – просмотреть статус пользователя.

6.20 Блокировка и разблокировка учетной записи пользователя

Для блокировки и разблокировки учетной записи пользователя по запросу администратора выполнить в терминале:

`sudo usermod -L имя_пользователя`

`sudo usermod -U имя_пользователя`

Команда `usermod -L` блокирует учетную запись, команда `usermod -U` снимает блокировку.

6.21 Принудительная смена пароля пользователя

Для сброса пароля учетной записи пользователя и требования от пользователя выполнить смену пароля, назначенного администратором, при запуске сеанса работы выполнить команду:

`sudo passwd -e имя_пользователя`

6.22 Настройка политики паролей

Для настройки политики паролей и связанных с ней параметров необходимо следовать руководству РЕД ОС и настроить файл:

`/etc/security/pwquality.conf`

6.23 Журналирование средствами прикладного программного обеспечения

Прикладное программное обеспечение СУ ведет собственный журнал действий, связанных с конфигурированием и обслуживанием контроллеров КИТП. Просмотр и экспорт журнала выполняются администратором с помощью программы Configurator.jar.

Для просмотра журнала необходимо войти в операционную систему под учетной записью администратора и запустить файл Configurator.jar. В главном окне программы доступны кнопки «Open», «Save», «Настроить права пользователей», «Настроить интервалы», «Протокол» и «О программе».

Кнопка «Настроить права пользователей» предназначена для просмотра предусмотренных групп разграничения доступа и настройки доступных для них функций прикладного программного обеспечения. Кнопка «Настроить интервалы» используется для настройки соответствующих параметров работы программы.

Для загрузки журнала действий с контроллером нажать кнопку «Open». После загрузки в рабочей области программы отображаются зарегистрированные действия, в том числе операции конфигурирования, просмотра конфигурации и зарегистрированные тревоги. Для каждой записи указываются метка времени и пользователь, от имени которого выполнено действие.

Журнал хранится в каталоге /opt/configurator в файле «Журнал настройки.txt» в зашифрованном виде. Непосредственное использование данного файла для просмотра записей не предусмотрено.

Для сохранения журнала в читаемом текстовом виде нажать кнопку «Save». В открывшемся диалоговом окне выбрать каталог и имя файла, после чего подтвердить сохранение. Программа сохраняет расшифрованное содержимое журнала в файл формата TXT.

Для просмотра истории действий, выполненных непосредственно в программе Configurator.jar, нажать кнопку «Протокол». В рабочей области отображается протокол работы с настройками программы, содержащий сведения о выполненных операциях, времени их выполнения и пользователе.

6.24 Контроль изменения параметров управления сеансами пользователей

Изменение параметров управления сеансами пользователей РЕД ОС регистрируется правилом аудита с ключом changed_systemd_logind_conf. Для просмотра зарегистрированных событий выполнить команду:

```
sudo ausearch -k changed_systemd_logind_conf -i
```

6.25 Контроль события смены пароля

Смена пароля пользователя регистрируется событием `USER_CHAUTHNOK`. Для проверки регистрации события выполнить команду:

```
sudo ausearch -m USER_CHAUTHNOK -i
```

6.26 Смена пароля стандартным пользователем в режиме киоска

Для смены собственного пароля стандартным пользователем без выхода из режима киоска в программе «Терминал» предусмотрен вызов формы смены пароля клавишей F5.

После нажатия F5 пользователь должен ввести текущий пароль, новый пароль и подтверждение нового пароля. Новый пароль должен соответствовать политике паролей РЕД ОС. После успешной смены пароля программа выводит сообщение об успешном завершении операции, а событие регистрируется средствами РЕД ОС как `USER_CHAUTHNOK`.

6.27 Инвентаризация программно-аппаратных средств СУ

Инвентаризация выполняется уполномоченным администратором при вводе СУ в эксплуатацию, после изменения состава аппаратных или программных средств и далее периодически в соответствии с установленным порядком эксплуатации. Результаты инвентаризации сопоставляются с паспортом СУ и эталонным перечнем программного обеспечения.

При проведении инвентаризации необходимо:

1. Проверить фактический состав СУ, наличие аппаратной платформы, кабелей подключения и иных средств, указанных в разделе «Комплектность» паспорта.
2. Получить сведения об установленном программном обеспечении РЕД ОС и сопоставить их с эталонным перечнем ПО СУ. Для формирования перечня установленных пакетов может использоваться команда: `rpm -qa | sort`.
3. Проверить подключенные USB-устройства командой `lsusb`. В составе СУ не должно быть неучтенных съемных устройств.
4. Проверить сетевые интерфейсы командой `ip link show` и активные сетевые порты командой `ss -tulpen`. Состав активных интерфейсов и портов должен соответствовать эксплуатационной документации; неиспользуемые интерфейсы и службы должны быть отключены.
5. Проверить отсутствие программно-аппаратных средств и ПО, не предусмотренных эксплуатационной документацией и не используемых для выполнения штатных функций СУ.

6. Зафиксировать дату инвентаризации, фактический состав аппаратных и программных средств, выявленные отклонения и принятые меры. При выявлении неучтенного оборудования или ПО эксплуатацию СУ в штатном режиме прекратить до устранения несоответствия.

Примечание. Процедура обеспечивает выполнение проверки состава программно-аппаратных средств и возможность периодической инвентаризации программного обеспечения, сетевых портов и портов подключения съемных устройств.

6.28 Параметры и контроль заполнения журнала событий ИБ

Основной журнал событий информационной безопасности РЕД ОС формируется службой аудита и расположен по пути `/var/log/audit/audit.log`. Доступ к журналу предоставляется только уполномоченному администратору.

При каждом входе в учетную запись администратора выполняется оценка текущего состояния журнала ИБ и прогноз времени до его возможного переполнения. Поскольку доступ к `audit.log` осуществляется с административными правами, для выполнения расчета автоматически выводится диалоговое окно запроса пароля администратора.

После ввода пароля выполняется расчет прогнозируемого времени до возможного переполнения журнала ИБ в часах. Факт уведомления администратора регистрируется в журнале событий информационной безопасности.

Если изменение объема журнала относительно предыдущего контроля не позволяет сформировать существенный прогноз переполнения, отдельное предупреждающее окно не выводится. Это означает, что скорость роста объема журнала незначительна либо его объем практически не изменился.

При достижении установленного предельного размера файла `audit.log` служба аудита выполняет ротацию: текущий файл журнала переименовывается с присвоением номера, после чего создается новый файл `audit.log`. Ранее сформированные журналы при этом сохраняются.

Для предотвращения заполнения накопителя контролируется занятое дисковое пространство. При достижении уровня заполнения 75 % администратору выводится всплывающее уведомление. Одновременно событие о достижении уровня заполнения диска 75 % регистрируется в журнале событий информационной безопасности.

Редактирование и удаление отдельных записей журнала не допускается. Сохранение и очистка журнала выполняются в порядке, приведенном в п. 6.14 настоящего руководства.

7 НАСТРОЙКА МОДУЛЯ СВЯЗИ UA MODEM

7.1 Общие сведения

Программный модуль UA-Modem-Terminal предназначена для диагностики, настройки и обслуживания модуля связи «UA Модем». Основное окно программы содержит область вывода сообщений терминала и командную строку, расположенную в нижней части окна (рисунок 7).

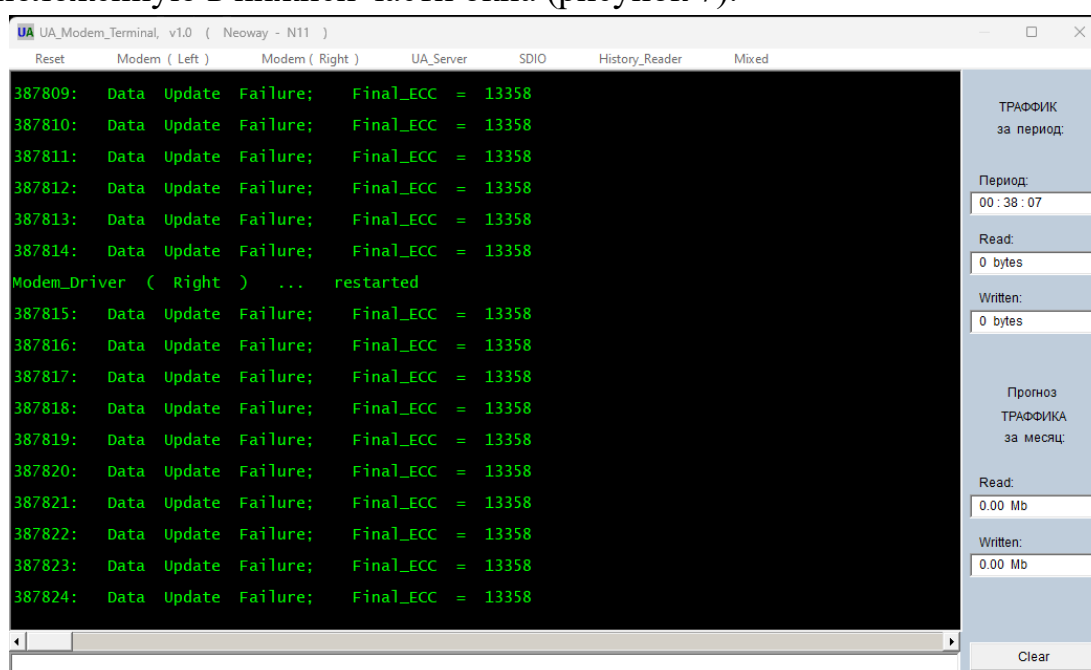


Рисунок 7: внешний вид главного окна UA-Modem-Terminal

Команды вводятся вручную в командной строке с последующим нажатием клавиши Enter. Для перехода по ранее введенным и предустановленным командам используется клавиша «Вверх».

Команда из истории	Назначение
Help	Вывод общего списка доступных сервисных команд.
MODBUS Slave Address	Просмотр текущего Modbus-адреса опрашиваемого устройства.
MODBUS F1 x81_x81	Тестовое чтение регистров Coil по функции Modbus 01.
MODBUS F2 x1_x8	Тестовое чтение дискретных входов по функции Modbus 02.
MODBUS F3 x81_x84	Тестовое чтение регистров Holding Register по функции Modbus 03.
MODBUS F4 x1_x10	Тестовое чтение регистров Input Register по функции Modbus 04.

Dynamic Memory Summary	Вывод информации о текущем состоянии динамической памяти устройства.
Modem_Driver (Left): Summary	Вывод текущих параметров левого GSM-модема.
Modem_Driver (Right): Summary	Вывод текущих параметров правого GSM-модема.

7.2 Получение справочной информации

В программном модуле UA-modem-terminal, в разделе Mixed предусмотрен набор готовых команд, для получения информации о работе UA-Modem (рисунок 8).

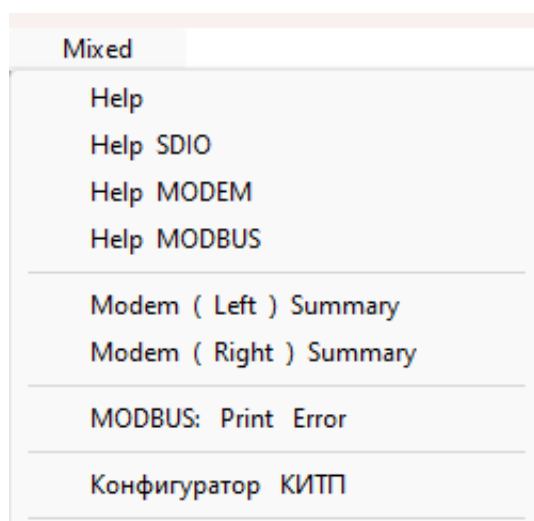


Рисунок 8: команды раздела Mixed

Также все эти команды доступны и для ввода в командную строку. Для получения списка доступных команд необходимо выполнить команду:

Help

Для вывода справки по отдельным подсистемам используются команды **Help MODEM**, **Help MODBUS** и **Help SDIO**.

Команда	Назначение
Help	Вывод общего списка команд.
Help MODEM	Вывод списка команд GSM-модемов.
Help MODBUS	Вывод списка команд Modbus.
Help SDIO	Вывод списка команд подсистемы SDIO.

7.3 Команды GSM-модемов

UA Modem содержит два независимых GSM-модуля: левый (Left) и правый (Right). Для каждого GSM-модуля доступен одинаковый набор команд. Полные команды содержат префикс конкретного модема, например:

Modem_Driver (Left): Summary

Modem_Driver (Right): Summary

7.3.1 Просмотр текущих параметров GSM-модема

Команда Summary выводит текущую конфигурацию выбранного GSM-модема.

Параметр	Назначение
AP Name	Имя точки доступа оператора связи (APN).
AP Login	Имя пользователя APN. Если авторизация не используется, поле может быть пустым.
AP Password	Пароль APN. Если авторизация не используется, поле может быть пустым.
Reverse IP	IP-адрес удалённого узла, к которому модем инициирует исходящее TCP-соединение.
Reverse Port	TCP-порт удалённого узла, к которому модем инициирует исходящее TCP-соединение.

7.3.2 Настройка параметров GSM-модема

Команда	Назначение
AP Name	Просмотр APN.
AP Name = <значение>	Установка APN.
AP Login	Просмотр имени пользователя APN.
AP Login = <значение>	Установка имени пользователя APN.
AP Password	Просмотр пароля APN.
AP Password = <значение>	Установка пароля APN.
Reverse IP	Просмотр IP-адреса удалённого узла.
Reverse IP = <A>..<C>.<D>	Установка IP-адреса удалённого узла. Каждый октет должен находиться в диапазоне 0...255.
Reverse Port	Просмотр TCP-порта удалённого узла.
Reverse Port = <порт>	Установка TCP-порта удалённого узла. Допустимый диапазон: 0...65535.

7.3.3 Команды Reverse IP и Reverse Port

Команды Reverse IP и Reverse Port задают параметры исходящего TCP-соединения GSM-модема. В прошивке предусмотрена логика автоматической попытки открытия локального сокета после регистрации модема в сети, установки соединения и перехода модема в режим прослушивания (OPC TCP данных) или в режим передачи (Reverse). Если параметр Reverse IP равен 0.0.0.0, попытка открытия Reverse-соединения не выполняется.

При заданном Reverse IP модем периодически пытается открыть TCP-соединение командой модема вида:

+tcpsetup=<номер_сокета>,<Reverse IP>,<Reverse Port>

После успешного открытия такого сокета он передаётся подсистеме встроенного OPC UA сервера. В диагностическом выводе прошивки такое соединение обозначается как reverse.

Пример настройки:

Modem_Driver (Left): Reverse IP = 0.0.0.0

Modem_Driver (Left): Reverse Port = 4840

Примечание. Значения по умолчанию для обоих модемов заданы как AP Name = fixedip.nw, AP Login и AP Password пустые, Reverse M = 0.0.0.0, Reverse Port = 0.

7.3.4 Диагностические команды GSM-модема

Команда	Назначение
Restart at 115200	Перезапуск драйвера модема на скорости 115200 бит/с
Debug at 115200	Переход в диагностический режим на скорости 115200 бит/с
Debug at 57600	Переход в диагностический режим на скорости 57600 бит/с
Debug at 38400	Переход в диагностический режим на скорости 38400 бит/с
Debug at 19200	Переход в диагностический режим на скорости 19200 бит/с
Debug at 9600	Переход в диагностический режим на скорости 9600 бит/с
Show TCP Load Statistic	Включение отображения статистики загрузки TCP-соединения
Hide TCP Load Statistic	Отключение отображения статистики загрузки TCP-соединения

7.4 Команды подсистемы буферизации данных SDIO

Подсистема SDIO обеспечивает работу устройства с внутренней памятью. Для просмотра списка команд используется команда Help SDIO.

Команда	Назначение
SDIO_Manager: Restart	Перезапуск подсистемы SDIO
SDIO_Manager: Debug SD_Card	Вывод расширенной диагностической информации по внутренней памяти
SDIO_Manager: Erase only SD_Card	Удаление содержимого внутренней памяти без дополнительной инициализации
SDIO_Manager: Clear SD_Card	Очистка внутренней памяти
SDIO_Manager: Format SD_Card	Форматирование внутренней памяти
SDIO_Manager: Read block @	Чтение блока данных по указанному номеру блока
SDIO_Manager: Card CSD	Вывод регистра CSD внутренней памяти
SDIO_Manager: Card SCR	Вывод регистра SCR внутренней памяти
SDIO_Manager: Card STATUS	Вывод текущего состояния внутренней памяти
SDIO_Manager: Glitch	Служебная диагностическая команда

7.5 Команды Modbus

Команды Modbus предназначены для настройки и диагностики обмена с подключённым устройством по интерфейсу RS485/RS422. Для просмотра списка команд используется команда `Help MODBUS`.

Команда	Назначение
MODBUS Slave Address	Просмотр текущего адреса опрашиваемого Modbus-устройства
MODBUS Slave Address = <адрес>	Установка адреса опрашиваемого Modbus-устройства
MODBUS F1 x81_x81	Тест чтения регистров Coil по функции 01
MODBUS F2 x1_x8	Тест чтения Discrete Input по функции 02
MODBUS F3 x81_x84	Тест чтения Holding Register по функции 03
MODBUS F4 x1_x10	Тест чтения Input Register по функции 04
MODBUS: Print Error	Вывод статистики ошибок обмена Modbus

Если текущая конфигурация RS485/RS422 не использует протокол Modbus, при выполнении команды `MODBUS: Print Error` терминал может вывести сообщение:

```
RS485_Protocol is not __MODBUS
```

Данное сообщение означает, что в текущей конфигурации устройства протокол Modbus не используется и статистика ошибок Modbus недоступна.

7.6 Команды идентификации устройства и URL

Команда	Назначение
Hardware GUID	Просмотр аппаратного идентификатора устройства
Hardware GUID = <значение>	Установка аппаратного идентификатора устройства Значение используется при формировании Endpoint URL
URL Base	Просмотр дополнительной части имени Endpoint URL
URL Base = <значение>	Установка дополнительной части имени Endpoint URL
URL	Вывод полного Endpoint URL встроенного OPC UA сервера

Полный URL формируется по шаблону:

```
opc.tcp://<Hardware GUID>[.<URL Base>]:4840
```

Если URL Base не задан, в URL используется только Hardware GUID и порт 4840.

8 АНТИВИРУСНАЯ ЗАЩИТА

Для защиты СУ от вредоносного программного обеспечения в операционной системе РЕД ОС должно быть установлено и настроено лицензионное антивирусное программное обеспечение, совместимое с применяемой версией операционной системы.

Антивирусная защита должна обеспечивать проверку файлов, исполняемых файлов и информации на подключаемых съемных носителях, а также регистрацию результатов антивирусной проверки.

Перед эксплуатацией СУ необходимо убедиться в работоспособности антивирусной защиты и актуальности используемых антивирусных баз в соответствии с установленным на предприятии порядком обновления.

Наименование, версия и параметры настройки применяемого антивирусного программного обеспечения уточняются после выбора конкретного средства защиты информации.

9 ВЗАИМОДЕЙСТВИЕ СЕРВИСНОГО УСТРОЙСТВА С КОНТРОЛЛЕРАМИ КИТП

9.1 Взаимодействие сервисного устройства с КИТП-01

КИТП-01 является сетевым контроллером. Взаимодействие сервисного устройства (СУ) с КИТП-01 осуществляется посредством команд, вводимых пользователем в прикладном программном обеспечении КИТП-Конфигуратор СУ, работающем в режиме киоска.

Команды предназначены для просмотра и изменения конфигурации контроллера, настройки аналоговых и дискретных каналов. Команды «КОНФИГУРАЦИЯ» и «СБРОС» вводятся на кириллице.

При вводе команд необходимо соблюдать приведенный ниже синтаксис, включая обозначения каналов, круглые скобки и последовательность параметров.

9.1.1 Контроль текущих технологических параметров и состояния КИТП-01

После подключения СУ к КИТП-01 и запуска прикладного программного обеспечения на экране СУ должны отображаться текущие технологические параметры объекта, получаемые контроллером.

Для контроля работоспособности КИТП-01 убедиться, что значения параметров отображаются без ошибок, изменяются при изменении соответствующих входных сигналов и соответствуют текущей конфигурации

контроллера. Наличие устойчивого обмена данными и отсутствие диагностических сообщений об ошибках являются признаком штатной работы программного обеспечения КИТП-01.

9.1.2 Просмотр конфигурации контроллера

Для вывода текущей конфигурации контроллера выполнить команду:

Конфигурация

После выполнения команды на экране СУ отображается текущая конфигурация контроллера.

9.1.3 Сброс конфигурации контроллера

Для сброса конфигурации контроллера к значениям по умолчанию выполнить команду:

Сброс

После выполнения команды отображается сообщение «Сброс настроек выполнен», после чего выводится конфигурация контроллера, установленная по умолчанию.

9.1.4 Конфигурирование аналоговых каналов

Для конфигурирования аналогового канала используется команда следующего вида:

Аn тип роутер = предел1 предел2 предел3 предел4 предел5 предел6

где:

- **Аn** — номер аналогового канала; n принимает значения от 1 до 12;
- **тип** — тип входного аналогового сигнала;
- **роутер** — назначение аналогового канала;
- **предел1...предел6** — значения диапазона измерения и границ зон контроля параметра.

Если аналоговый канал не используется, для него задается значение:

Аn = NULL

9.1.4.1 Типы аналогового сигнала

Значение	Описание
4-20	Токовый сигнал 4–20 мА
0-20	Токовый сигнал 0–20 мА
0-5	Токовый сигнал 0–5 мА

9.1.4.2 Назначение аналогового канала (роутера)

Роутер	Назначение
NULL	Канал не используется
Pin(1)...Pin(4)	Давление на входе, каналы 1–4
Pout(1)...Pout(4)	Давление на выходе, каналы 1–4
Pdif(1)...Pdif(4)	Перепад давления, каналы 1–4
Tin(1)...Tin(4)	Температура газа на входе, каналы 1–4
Tout(1)...Tout(4)	Температура газа на выходе, каналы 1–4
Tcool	Температура теплоносителя отопления
CH4(1)...CH4(3)	Параметр CH4, помещения 1–3
CHO(1)...CHO(3)	Параметр CHO, помещения 1–3
Tamb(1)...Tamb(3)	Температура воздуха в помещениях 1–3
Toutdoor	Температура наружного воздуха

9.1.4.3 Пределы аналогового канала

Параметр	Назначение
предел1	Нижний предел измерения
предел2	Нижняя граница красной зоны
предел3	Нижняя граница желтой зоны
предел4	Верхняя граница желтой зоны
предел5	Верхняя граница красной зоны
предел6	Верхний предел измерения

9.1.4.4 Пример конфигурирования аналогового канала

Пример настройки аналогового канала A1 для измерения давления на входе Pin(1) с типом входного сигнала 4–20 мА:

A1 4-20 Pin(1) = -1.5 0 3 6 8 10

В приведенном примере для канала A1 заданы: нижний предел измерения минус 1,5; нижняя граница красной зоны 0; нижняя граница желтой зоны 3; верхняя граница желтой зоны 6; верхняя граница красной зоны 8; верхний предел измерения 10.

9.1.5 Конфигурирование дискретных каналов (роутера)

Для конфигурирования дискретного канала используется команда следующего вида:

Dn роутер = нормальное состояние

где:

- Dn — номер дискретного канала; n принимает значения от 1 до 16;
- тип — назначение дискретного канала;
- нормальное состояние — нормальное состояние подключенного дискретного сигнала: NC или NO.

Если дискретный канал не используется, для него задается значение:

$Dn = NULL$

9.1.5.1 Нормальное состояние дискретного канала

Значение	Описание
NC	Нормально замкнутое состояние
NO	Нормально разомкнутое состояние
NULL	Канал не используется

9.1.5.2 Назначение дискретного канала (роутера)

Роутер	Назначение
NULL	Канал не используется
Pdif(1)...Pdif(4)	Перепад давления, каналы 1–4
PZK(1)...PZK(4)	ПЗК, каналы 1–4
PSK(1)...PSK(4)	ПСК, каналы 1–4
HeatValve	Клапан отопителя
FAlarm	Сигнал пожарной сигнализации «Пожар»
FAttent	Сигнал пожарной сигнализации «Внимание»
FFault	Сигнал пожарной сигнализации «Неисправность»
UpsFault	Сигнал неисправности ИБП
R1D1...R1D5	Дискретные сигналы помещения 1
R2D1...R2D5	Дискретные сигналы помещения 2
R3D1...R3D5	Дискретные сигналы помещения 3
SecP1...SecP3	Сигналы поста охраны

9.1.5.3 Пример конфигурирования дискретного канала

Пример настройки дискретного канала D1 для сигнала PZK(1) с нормально замкнутым состоянием:

D1 PZK(1) = NC

9.1.6 Отключение неиспользуемых каналов

Для исключения неиспользуемого аналогового или дискретного канала из конфигурации используется значение NULL.

Для аналогового канала команда имеет вид:

An = NULL

Для дискретного канала команда имеет вид:

Dn = NULL

После изменения конфигурации рекомендуется выполнить команду «Конфигурация» и убедиться, что введенные параметры сохранены и отображаются корректно.

9.1.7 Настройка УИРГ

Для записи состава среды в УИРГ используется команда:

УИРГ <пароль> N2=<значение> CO2=<значение>

Плотность=<значение>

Пример: УИРГ 0000 N2=0.2 CO2=0.3 Плотность=0.6

Параметры команды: <пароль> — пароль доступа к УИРГ; N2 — процентное содержание азота; CO2 — процентное содержание диоксида углерода; Плотность — плотность газа при стандартных условиях, кг/м³.

9.1.8 Резервный источник питания КИТП-01

Неавтономный КП ТМ на базе КИТП-01 питается от сети переменного тока 220/230 В и предусматривает резервный источник питания с аккумуляторной батареей. При пропадании основного сетевого питания контроллер автоматически, без вмешательства оператора, переключается на резервный источник питания. После восстановления сетевого питания выполняется автоматический возврат на основной источник.

Резервный источник питания должен обеспечивать автономную работу оборудования КП ТМ не менее 24 часов. Подтверждение времени автономной работы выполняется расчетом путем сопоставления расчетной емкости аккумуляторной батареи и параметров энергопотребления шкафа КП ТМ, указанных в технической документации.

При проверке резервирования питания необходимо отключить основной источник питания, убедиться в сохранении работоспособности КИТП-01 и наличии сообщения о пропадании сетевого питания, затем восстановить основное питание и убедиться в автоматическом обратном переключении и формировании сообщения о восстановлении сетевого питания.

9.2 Взаимодействие сервисного устройства с КИТП-02

КИТП-02 является автономным контроллером. Взаимодействие сервисного устройства (СУ) с КИТП-02 осуществляется посредством команд, вводимых пользователем в прикладном программном обеспечении СУ, работающем в режиме киоска. В отличие от КИТП-01, для измерительных каналов КИТП-02 используются цифровые датчики.

При вводе команд необходимо соблюдать приведенный ниже синтаксис, включая обозначение канала, тип датчика, назначение канала (роутер), круглые скобки и последовательность параметров.

9.2.1 Контроль текущих технологических параметров и состояния КИТП-02

После подключения КИТП-02 к СУ оператор должен убедиться в наличии обмена с контроллером и возможности получения его текущей конфигурации. Контроль корректности внесенных изменений выполняется повторным чтением конфигурации после записи параметров.

9.2.2 Просмотр конфигурации контроллера

Для вывода текущей конфигурации КИТП-02 выполнить команду:

Конфигурация

После выполнения команды на экране СУ отображается текущая конфигурация контроллера.

9.2.3 Сброс конфигурации контроллера

Для сброса конфигурации КИТП-02 к значениям по умолчанию выполнить команду:

Сброс

После выполнения команды отображается сообщение «Сброс настроек выполнен», после чего выводится конфигурация контроллера, установленная по умолчанию.

9.2.4 Конфигурирование каналов цифровых датчиков

Для конфигурирования измерительного канала КИТП-02 используется команда следующего вида:

Ап тип роутер = предел1 предел2 предел3 предел4 предел5 предел6

где:

- Ап — номер канала; n принимает значения от 1 до 12;
- тип — тип подключенного цифрового датчика;
- роутер — назначение измерительного канала;
- предел1...предел6 — значения диапазона измерения и границ зон

контроля параметра.

9.2.4.1 Типы цифровых датчиков

Примечание. Расшифровка обозначений AIR, TPU, SDV и OPT в исходном перечне команд разработчика не приведена; в настоящем руководстве сохранены фактические обозначения, используемые программным обеспечением.

Значение	Описание
NULL	Канал не используется.
AIR	Допустимый тип цифрового датчика КИТП-02
TPU	Допустимый тип цифрового датчика КИТП-02
SDV	Допустимый тип цифрового датчика КИТП-02
OPT	Допустимый тип цифрового датчика КИТП-02

9.2.4.2 Назначение измерительного канала (роутера)

Роутер	Назначение
NULL	Канал не используется.
Pin(1)...Pin(4)	Давление газа на входе, каналы 1–4.
Pout(1)...Pout(4)	Давление газа на выходе, каналы 1–4.
Pdif(1)...Pdif(4)	Перепад давления, каналы 1–4.
Tin(1)...Tin(4)	Температура газа на входе, каналы 1–4.
Tout(1)...Tout(4)	Температура газа на выходе, каналы 1–4.
Tcool	Температура теплоносителя отопления.
CH4(1)...CH4(3)	Параметр CH4, помещения 1–3.
CHO(1)...CHO(3)	Параметр CHO, помещения 1–3.
Tamb(1)...Tamb(3)	Температура воздуха в помещениях 1–3.
Toutdoor	Температура наружного воздуха.

9.2.5 Конфигурирование дискретных каналов

Для конфигурирования дискретного канала КИТП-02 используется команда следующего вида:

Dn роутер = нормальное состояние

где:

- Dn — номер дискретного канала; n принимает значения от 1 до 16;
- роутер — назначение дискретного канала;
- нормальное состояние — нормальное состояние подключенного дискретного сигнала: NC или NO.

9.2.5.1 Нормальное состояние дискретного канала

Значение	Описание
NC	Нормально замкнутое состояние
NO	Нормально разомкнутое состояние
NULL	Канал не используется

9.2.5.2 Назначение дискретного канала (роутера)

Роутер	Назначение
NULL	Канал не используется
Pdif(1)...Pdif(4)	Перепад давления, каналы 1–4
PZK(1)...PZK(4)	ПЗК, каналы 1–4
PSK(1)...PSK(4)	ПСК, каналы 1–4
HeatValve	Клапан отопителя
FAlarm	Сигнал пожарной сигнализации «Тревога»
FAttent	Сигнал пожарной сигнализации
FFault	Сигнал пожарной сигнализации «Неисправность»
UpsFault	Сигнал неисправности ИБП
R1D1...R1D5	Дискретные сигналы помещения 1
R2D1...R2D5	Дискретные сигналы помещения 2
R3D1...R3D5	Дискретные сигналы помещения 3
SecP1...SecP3	Сигналы поста охраны

9.2.6 Отключение неиспользуемых каналов

Для исключения неиспользуемого измерительного или дискретного канала из конфигурации используется значение NULL.

Для измерительного канала команда имеет вид:

$A_n = \text{NULL}$

Для дискретного канала команда имеет вид:

$D_n = \text{NULL}$

После изменения конфигурации рекомендуется выполнить команду «Конфигурация» и убедиться, что введенные параметры сохранены и отображаются корректно.

10 ВОЗМОЖНЫЕ НЕИСПРАВНОСТИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

При возникновении неисправности следует использовать рекомендации таблицы. Если после выполнения указанных действий работоспособность не восстановлена, дальнейшую эксплуатацию СУ прекратить и передать изделие ответственному специалисту.

Признак неисправности	Возможная причина	Способ устранения
СУ не включается	Разряжена аккумуляторная батарея аппаратной платформы; неисправен адаптер питания	Подключить штатный адаптер питания, проверить наличие питания и повторить включение
КИТП не определяется СУ	Неисправен или не подключен кабель USB; отсутствует необходимый драйвер; недостаточны права пользователя	Проверить кабель и подключение, наличие драйвера, включение пользователя в группу dialout, повторить подключение
Прикладное ПО СУ не запускается	Нарушена целостность программных файлов; некорректное обновление	Проверить события контроля целостности. При необходимости восстановить утвержденную версию ПО.
Не отображаются текущие параметры КИТП	Отсутствует обмен с контроллером; неверное подключение; контроллер не включен	Проверить питание КИТП, кабель подключения, состояние интерфейса и повторить установление соединения
Измененные параметры не сохраняются	Команда введена с ошибкой или нарушен синтаксис	Проверить синтаксис команды, повторить ввод и выполнить команду «Конфигурация» для контроля результата
Антивирусная защита неактивна	Антивирусное ПО остановлено или требует обновления	Запустить/восстановить работу антивирусного ПО и проверить состояние защиты до продолжения эксплуатации
Журнал событий ИБ недоступен	Недостаточны права учетной записи	Выполнить просмотр под учетной записью администратора с использованием sudo.

11 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

Техническое обслуживание СУ направлено на поддержание исправности аппаратной платформы, кабелей подключения, программного обеспечения и средств защиты информации. Специальная разборка аппаратной платформы при проведении технического обслуживания не допускается.

Ремонт аппаратной платформы СУ выполняется в соответствии с эксплуатационной документацией изготовителя и должен осуществляться уполномоченной организацией. Восстановление программного обеспечения выполняется ответственным специалистом путем установки утвержденного комплекта ПО.

Вид обслуживания	Периодичность	Содержание работ
Контроль перед применением	Перед каждым использованием СУ	Внешний осмотр аппаратной платформы и кабелей; проверка уровня заряда/питания; запуск РЕД ОС и ПО СУ; контроль работоспособности антивирусной защиты; проверка подключения к КИТП
Контроль после обновления ПО	После каждого обновления ПО СУ или РЕД ОС	Проверка запуска ПО; контроль целостности; проверка журналирования событий; пробное подключение к КИТП и проверка чтения конфигурации
Плановое обслуживание аппаратной платформы	С периодичностью, установленной эксплуатационной документацией изготовителя аппаратной платформы	Очистка внешних поверхностей и вентиляционных отверстий без разборки; проверка состояния аккумуляторной батареи и штатного адаптера питания; иные работы по документации изготовителя
Контроль средств защиты информации	При каждом плановом обслуживании и после изменения конфигурации ПО	Проверка учетных записей и групп доступа; режима киоска; активности антивирусной защиты; состава сетевых служб; наличия и доступности журналов событий ИБ

В рамках технического обслуживания необходимо периодически проводить инвентаризацию программно-аппаратных средств СУ в соответствии с п. 6.27, контролировать отсутствие неучтенного ПО и устройств, а также состояние ограничений доступа к USB-накопителям.