

УТВЕРЖДЕН  
RU.EMTЦ.000020-ЛУ

Программный комплекс «RDW GUARDOS»

Руководство оператора  
RU.EMTЦ.000020 34

Листов 14

2024

Литера

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

## **АННОТАЦИЯ**

Настоящий документ содержит сведения для проверки, обеспечения функционирования и настройки программного комплекса «**RDW GUARDOS**» (**RU.EMTЦ.000020**) (далее **ПК «RDW GUARDOS»**).

В документе приводятся сведения о выполнении программных компонентов **ПК «RDW GUARDOS»**.

## Содержание

1. Назначение программного комплекса .....	4
2. Условия выполнения программного комплекса .....	5
3. Выполнение программного комплекса .....	4
4. Режим администратора .....	10
5. Управление включением УВМ .....	12
6. Сообщения оператору .....	12
<b>ПЕРЕЧЕНЬ СОКРАЩЕНИЙ .....</b>	<b>14</b>

## 1. НАЗНАЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

1.1. ПК «RDW GUARDOS» предназначен для мониторинга персонального компьютера или сервера.

1.2. ПК «RDW GUARDOS» состоит из следующих компонентов:  
– компонент программное обеспечение «RDW GUARDOS Back» (RU.EMTЦ.000010) (далее ПО «RDW GUARDOS Back»);  
– компонент программное обеспечение «RDW GUARDOS Front» (RU.EMTЦ.000011) (далее ПО «RDW GUARDOS Front»).

1.3. ПО «RDW GUARDOS Back» предназначено для функционирования в изделиях: плата защиты персонального компьютера (EMTЦ.431431.004), плата защиты и мониторинга сервера (EMTЦ.431431.006) (далее **Изделия**), для обеспечения работы периферийных устройств и сбора статистической информации о состоянии наблюдаемой рабочей станции.

1.4. ПО «RDW GUARDOS Front» предназначено для получения информации от ПО «RDW GUARDOS Back», имеет графический интерфейс пользователя с набором элементов управления и отображения пользовательской информации.

## 2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО КОМПЛЕКСА

2.1. Функционирование ПО «RDW GUARDOS Back» происходит внутри ядра микроконтроллера STM32F103C8 с тактовой частотой 8 МГц.

2.2. ПО «RDW GUARDOS Back» записывается во внутреннюю память **Изделия** один раз при изготовлении устройства и не имеет интерфейса пользователя.

2.3. Установка и функционирование ПО «RDW GUARDOS Front» осуществляется на УВМ с минимальной конфигурацией для платформы Intel:

- платформа на базе процессора Intel с тактовой частотой 3 ГГц;
- ОЗУ - 4 ГБ;
- жесткий диск объемом 80 ГБ;
- видеокарта с объемом памяти 32 МБ;
- монитор 15” SVGA с разрешением 1024x768;
- 1 порт USB 2.0 или выше.

2.4. Для установки ПО «RDW GUARDOS Front» необходимо наличие свободного дискового пространства на УВМ, которое будет использовано в процессе установки, не менее 220 Мбайт.

2.5. Машинное время на технических средствах, на которых выполняются компоненты ПК «RDW GUARDOS», должно быть синхронизировано.

2.6. Для функционирования компонента ПО «RDW GUARDOS Front» на соответствующих УВМ необходимо наличие ОС Windows 7 и выше, а также Linux-версий: Astra Linux, RedOS, Alt Linux для рабочих станций.

## 3. ВЫПОЛНЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА

### 3.1. Общие правила

3.1.1. Работа **ПО «RDW GUARDOS Back»** происходит внутри ядра микроконтроллера **STM32F103C8**, запускается автоматически при включении **Изделия** и не требует дальнейшего пользовательского сопровождения.

3.1.2. Интерфейс пользователя, предоставляемый **ПО «RDW GUARDOS Front»**, состоит из элементов, которыми являются основные экранные формы **ПО «RDW GUARDOS Front»**. Они отображаются сразу после запуска **ПО «RDW GUARDOS Front»** и являются его рабочей областью. Все остальные экранные формы являются диалоговыми или вспомогательными.

3.1.3. Экранные формы **ПО «RDW GUARDOS Front»** содержат различные графические элементы управления, отвечающие за функционирование программы и отображение данных – кнопки, поля ввода, списки, таблицы и т.д.

3.1.4. Для выполнения операции, доступной пользователю, для управления работой приложения, необходимо нажать на соответствующую кнопку с соответствующей пиктограммой при помощи графического манипулятора типа «мышь» (далее, «мышь»).

## **3.2. Запуск и использование ПО «RDW GUARDOS Front»**

3.2.1. Для запуска **ПО «RDW GUARDOS Front»** на УВМ необходимо:

- 1) скопировать содержимое **ПО «RDW GUARDOS Front»** на жесткий диск УВМ;
- 2) подключить **Изделие** к USB-порту УВМ;
- 3) перейти в папку \GUARDOSAPP и запустить файл **GUARDOS.exe**.

Во время запуска программы происходит соединение с **Изделием**, а также автоматическая синхронизация времени **Изделия** и системного времени УВМ.

Запуск программы произойдет только при наличии устойчивой связи с **Изделием**.

После запуска программы появится окно Авторизации (Рис.1):

управление и сбор статистики  
с модуля защиты ПК

Имя

Способ авторизации

смарт-карта

Нажмите "Вход" и приложите  
свой ключ "смарт-карта"

Вход

Рис. 1

- 4) В поле «Имя» ввести Имя пользователя
- 5) выбрать необходимый способ авторизации, выбрав его в выпадающем списке:

– способ «смарт-карта» Рис.2:

Имя

Способ авторизации

смарт-карта

Нажмите "Вход" и приложите  
свой ключ "смарт-карта"

Рис. 2

Данный способ авторизации требует ввода Имени пользователя, нажать кнопку «Вход», после чего необходимо поднести смарт-карту к устройству считывания.

– способ «отпечаток пальца» Рис.3:

Имя

Способ авторизации

отпечаток пальца

Нажмите "Вход" и приложите свой ключ "отпечаток пальца"

Рис.3

Данный способ авторизации требует ввода Имени пользователя, нажать кнопку «Вход», после чего необходимо приложить один палец к устройству считывания.

**– способ «iButton» Рис.4:**

Имя

Способ авторизации

iButton

Нажмите "Вход" и приложите свой ключ "iButton"

Рис.4

Данный способ авторизации требует ввода Имени пользователя, нажать кнопку «Вход», после чего необходимо приложить ключ iButton к устройству считывания.

**– способ «пароль» Рис.5:**

Имя

Способ авторизации

пароль

Пароль

Рис.5

Данный способ авторизации требует ввода Имени пользователя, после чего необходимо ввести пароль пользователя в появившемся поле «Пароль» и нажать кнопку «Вход».

После успешной авторизации будет произведён немедленный переход в основное окно.

### 3.3. Экранные формы ПО «RDW GUARDOS Front»

3.3.1. Вид основной экранной формы приложения пользователя показан на Рис. 6.

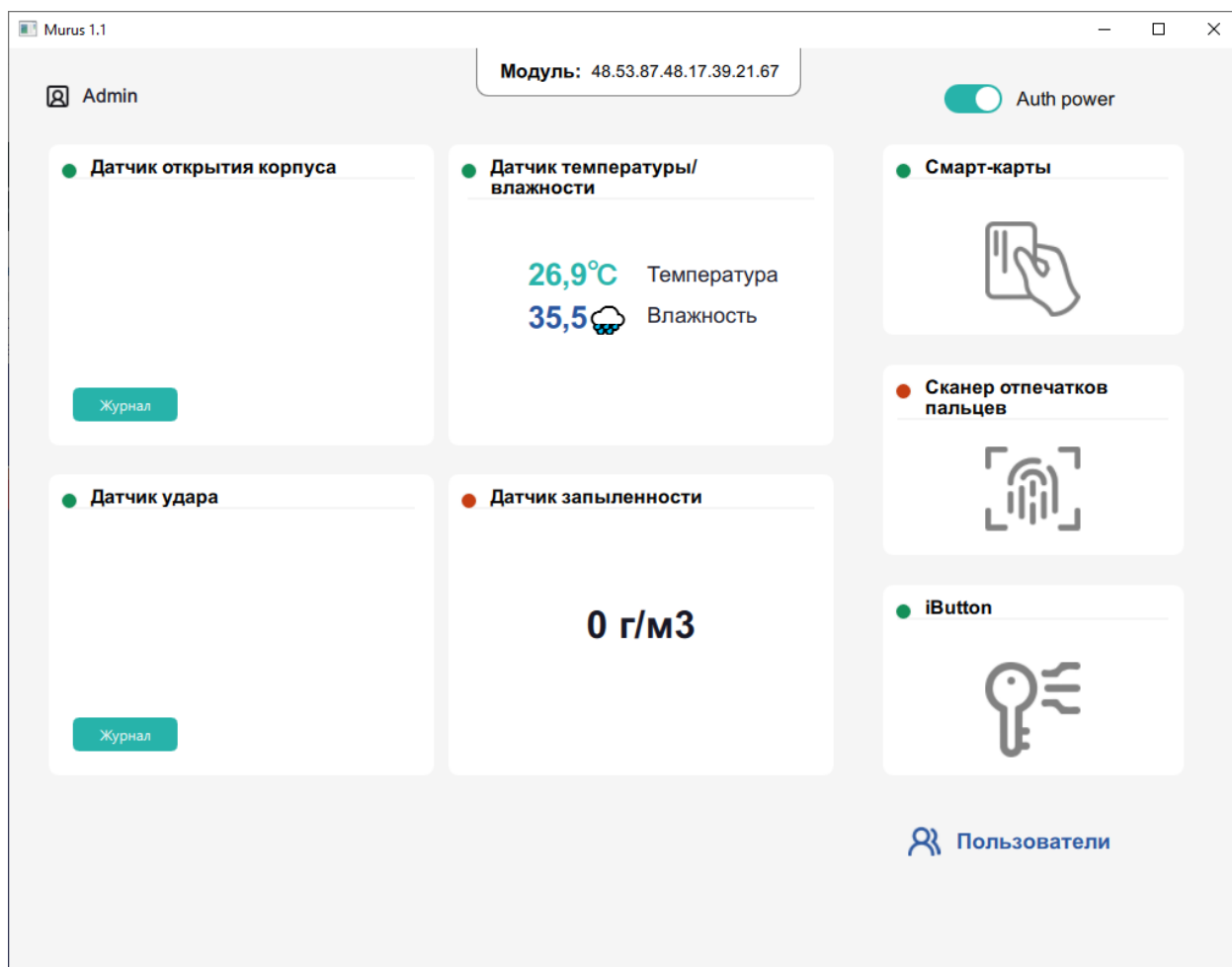


Рис. 6

Основная экранная форма содержит следующие области:

- Идентификационный номер **Изделия**;
- Имя авторизовавшего пользователя;
- Датчик открытия корпуса;
- Датчик температуры и влажности - текущая температура и влажность;
- Датчик запылённости – текущая запылённость.

Показания значений «Текущая температура и влажность» и «Текущая запылённость» обновляются при изменении реальных значений датчиков.

Если авторизованный пользователь имеет статус Администратора, появится дополнительный элемент управления «Пользователи».

Области «Датчик открытия корпуса» и «Датчик удара» имеют кнопку «Журнал», при нажатии на которую осуществляется переход в дополнительное окно - «Журнал датчика открытия корпуса» (Рис.7):

< Журнал датчика открытия корпуса

№	Дата и время
---	--------------

Рис.7.

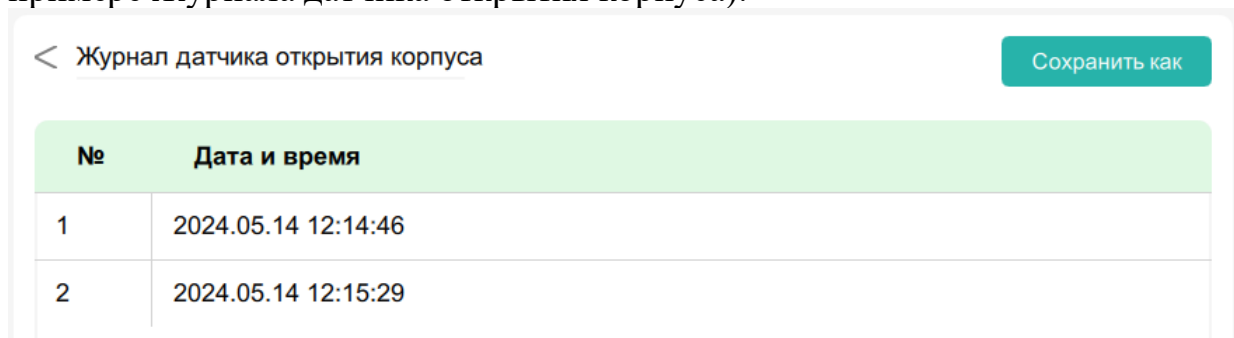
и «Журнал датчика удара» (Рис.8):

< Журнал датчика удара

№	Дата и время	Сила
---	--------------	------

Рис.8.

Если «Журнал датчика открытия корпуса» (Рис.7) или «Журнал датчика удара» (Рис.8) имеют записи о событиях, тогда, в соответствующем окне, отобразится кнопка «Сохранить как» (Рис. 9 - на примере Журнала датчика открытия корпуса):



< Журнал датчика открытия корпуса Сохранить как

№	Дата и время
1	2024.05.14 12:14:46
2	2024.05.14 12:15:29

Рис.9.

Для сохранения журнала на локальный диск нужно нажать кнопку «Сохранить как».

Появится окно выбора файла сохранения Рис.10:

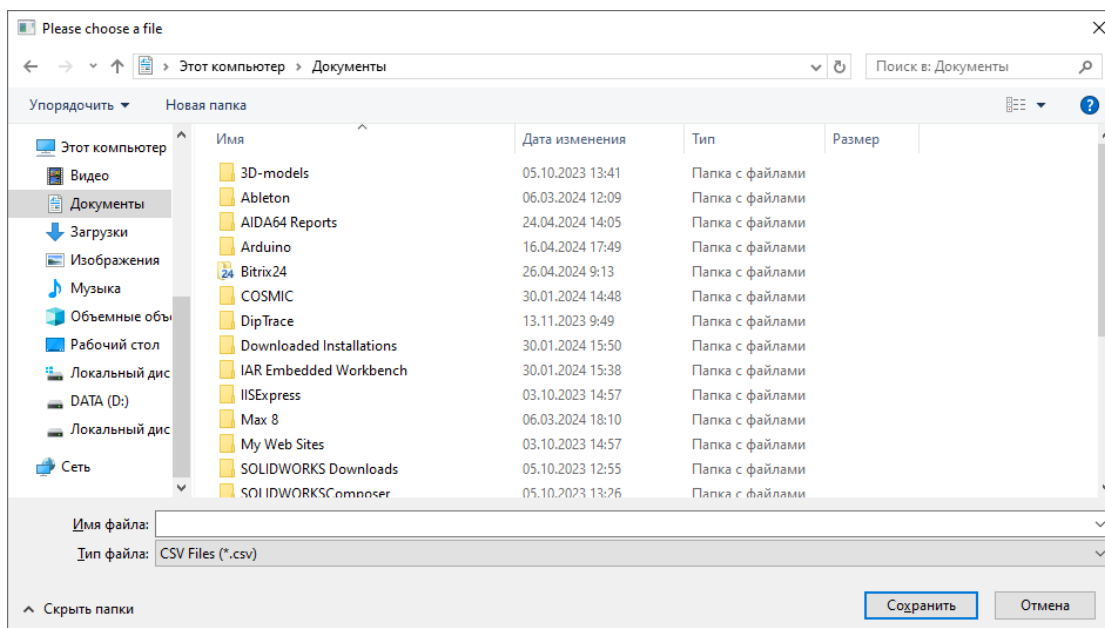


Рис.10.

Выбрать путь сохранения. В поле «Имя файла» ввести желаемое имя сохраняемого файла. Нажать кнопку «Сохранить».

Данные сохраняются в файле «имя.csv», в универсальном формате «Comma-Separated Values» с разделителем «;» (точка-с-запятой).

#### 4. РЕЖИМ АДМИНИСТРАТОРА

Некоторые пользователи могут обладать правами Администратора.

4.1. Режим Администратора является расширенным режимом и добавляет возможность добавления, редактирования и удаления Пользователей.

4.2. Для управления списком пользователей необходимо выбрать раздел «Пользователи» (Рис.11):



Рис.11.

Произойдёт переход в окно редактора пользователей (Рис.12):

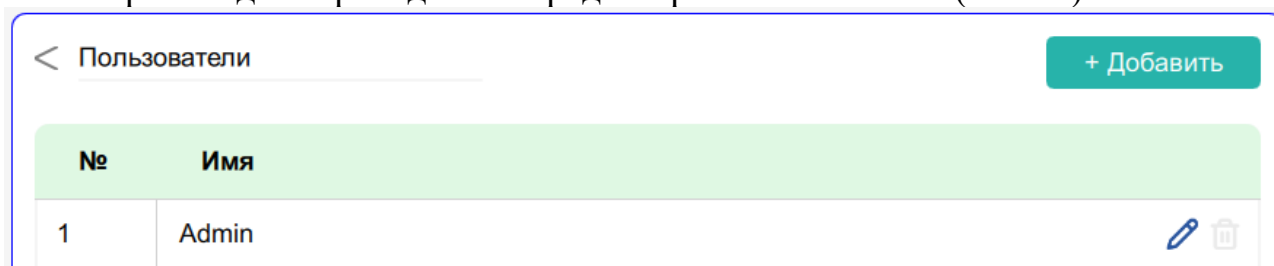


Рис.12.

4.2.1. Для добавления нового пользователя нужно нажать кнопку «Добавить». Отобразится форма создания нового пользователя (Рис.13):

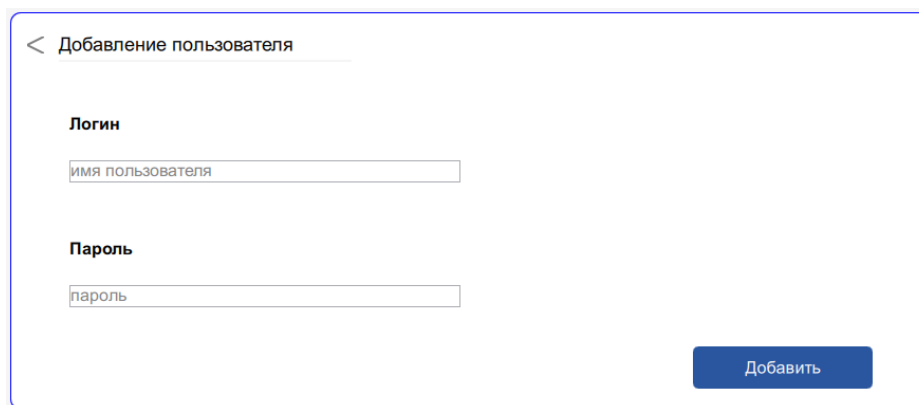


Рис.13.

Необходимо заполнить поле «Имя пользователя» и поле «Пароль». Нажав кнопку «Добавить» произойдёт создание нового пользователя и автоматическая запись данных о новом пользователе в память **Изделия**. Информация о новом пользователе появится в списке пользователей предыдущего окна.

4.2.2. Для удаления пользователя используйте символ удаления (Рис.14):



Рис 14.

4.2.3. Для изменения идентификационных данных пользователя необходимо перейти в соответствующий раздел нажатием на символ редактирования, напротив соответствующего пользователя (Рис.15):



Рис.15

Откроется окно редактора (Рис.16):

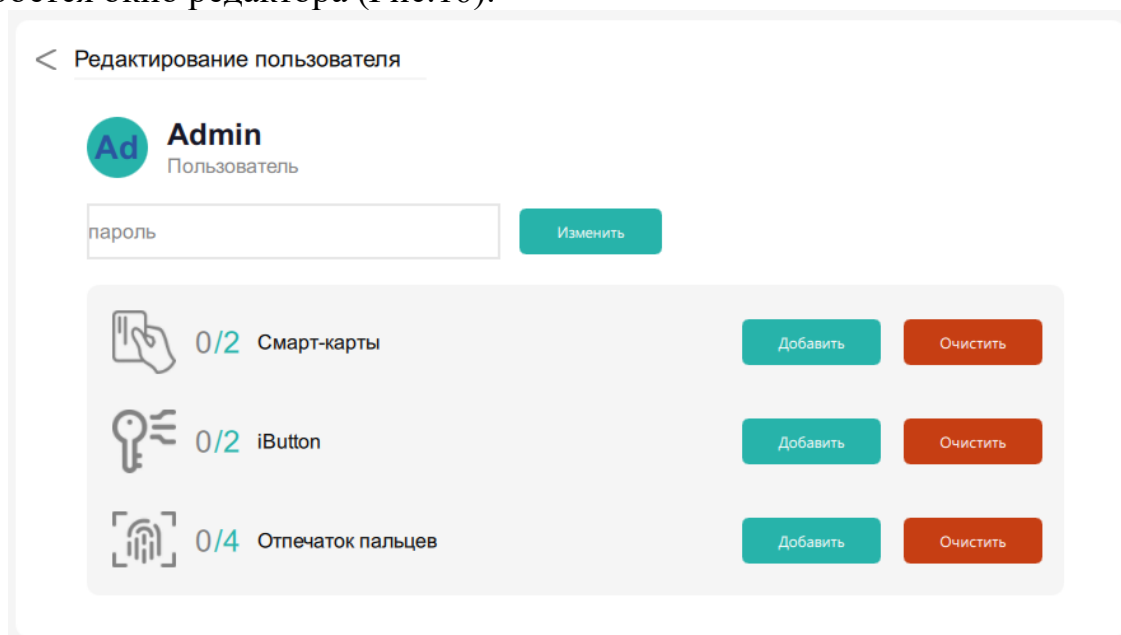


Рис.16.

Элементы управления данного окна позволяют производить:

- изменение пароля пользователя,
- добавление и удаление смарт-карты,

- добавление и удаление ключа iButton,
- добавление и удаление отпечатков пальцев.

## 5. Управление включением УВМ

**Изделие** предоставляет два режима включения УВМ:

- обычное включение;
- включение УВМ с обязательной авторизацией пользователя, при помощи устройств идентификации пользователя (смарт-карты, ключа iButton, отпечатка пальца).

### 5.1. Активация режима обязательной авторизации пользователя

Если положение управляющего элемента такое, как указано на Рис.17

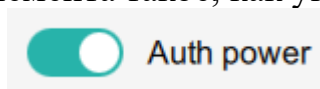


Рис.17

это означает, что УВМ может быть включен только авторизованным пользователем, чей ключ iButton, смарт-карта или отпечаток пальца зарегистрирован в памяти **Изделия**. Для включения УВМ необходимо подтвердить авторизацию одним из выше указанных способов. Без такого подтверждения УВМ не включится.

### 5.2. Деактивация режима обязательной авторизации пользователя

Если положение управляющего элемента такое, как указано на Рис.18

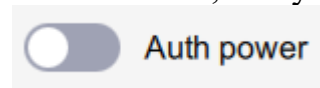


Рис.18.

это означает, что УВМ может включаться обычным способом, без подтверждения авторизации пользователя.

5.3. Переключение элемента управления из одного положения в другое производит автоматическое сохранение режима в **Изделии** без дополнительного подтверждения.

## 6. СООБЩЕНИЯ ОПЕРАТОРУ

6.1. В процессе функционирования приложения пользователя на экран монитора выдаются сообщения о состоянии датчиков **Изделия**. В случае изменения состояния **Изделия** показания изменяются автоматически.

6.2. При переходе в режим просмотра журналов выводятся данные о записях, содержащихся в конкретном журнале. В момент открытия окна журнала, данные обновляются автоматически, оператор видит последнюю обновлённую информацию.

6.3. Если во время работы программы будет потеряна связь с **Изделием**, оператор получит сообщение (Рис.19):

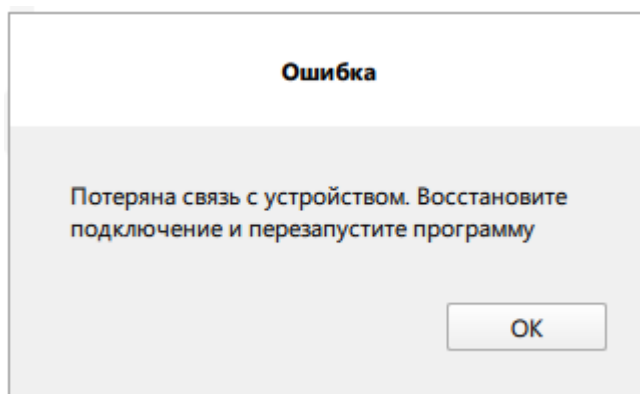


Рис.19.

Для восстановления работы программы необходимо проверить соединение с **Изделием** и перезапустить программу. Нажатие кнопки «ОК» приведёт к автоматическому закрытию программы.

## 7. ТРЕБОВАНИЯ К ПЕРСОНАЛУ

Обслуживающий персонал должен иметь следующий уровень специальной подготовки - в части обслуживания программного обеспечения:

- знание основных правил работы в среде операционных систем;
- знание основ ОС Linux;
- опыт системного администрирования ОС Linux;
- ознакомление с информацией настоящего руководства.

## 8. СПОСОБ И МЕСТО ХРАНЕНИЯ ИСХОДНЫХ КОДОВ ПО

Адрес нахождения технических средств хранения исходного текста и объектного кода программного обеспечения, а также технических средств компиляции исходного текста в объектный код программного обеспечения:

Способ хранения на flash-накопителе

Место хранения: по фактическому адресу офиса компании разработчика:

ООО «АйТиАй», 236006, Калининградская обл., г. Калининград, Ленинский пр-т, д. 30, помещение 8 (офис № 402)

Тел. + 909 933 82 14

Электронная почта: [info@i-t-i.ru](mailto:info@i-t-i.ru)

Технические средства для формирования и хранения лицензионных ключей не требуются.

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОС	- операционная система;
ПК	- программный комплекс;
ПП	- приложение пользователя;
ТЗ	- техническое задание;
УВМ	- универсальная вычислительная машина;
ПЗПК	- плата защиты персонального компьютера;
ПЗМС	- плата защиты и мониторинга сервера.