

**Руководство пользователя**  
**Программное обеспечение**  
**ЭНТ Контроль доступа**  
**ПОДТВЕРЖДЕНИЕ ДОСТУПА**

**Сделано в России**

Редакция от 24.02.2026 г.

## ОГЛАВЛЕНИЕ

1	ВВЕДЕНИЕ.....	3
1.1	Общие сведения о программе .....	3
2	РАБОТА С ПРОГРАММОЙ.....	4
2.1	Установка.....	4
2.2	Настройка .....	5
2.3	Запуск/остановка.....	7
2.4	Сценарии.....	7
2.5	Веб-интерфейс .....	8
3	НАСТРОЙКИ В ПРОГРАММЕ «ЭНТ Контроль доступа – Клиент».....	9
4	ПРИМЕРЫ НАСТРОЙКИ В ПО «ЭНТ Контроль доступа».....	11
5	ОБОЗНАЧЕНИЯ, ТЕРМИНЫ И СОКРАЩЕНИЯ.....	13
5.1	Условные обозначения, принятые в руководстве.....	13
5.2	Список принятых сокращений .....	13

# 1 ВВЕДЕНИЕ

## 1.1 Общие сведения о программе

Программа «Подтверждение доступа» является специализированным программным обеспечением, предназначенным для реализации нестандартных решений в системе контроля и управления доступом (СКУД) «ЭНТ Контроль доступа». После установки программа функционирует в фоновом режиме как служба, автоматически запускаемая вместе с операционной системой Windows. Она интегрируется с другими программами серии «ЭНТ Контроль Доступа – Сервер» и «Клиент».

Программа предоставляет три предварительно настроенных сценария с различными алгоритмами подтверждения доступа:

1. Запрещение повторного прохода пользователя в одном направлении.
2. Запрещение доступа при нулевом или отрицательном значении в поле «Баланс».
3. Однократный доступ в течение 24-часового периода.

Программа может поддерживать сценарии гибкого пропускного режима, которые могут быть настроены в соответствии с требованиями пользователя.

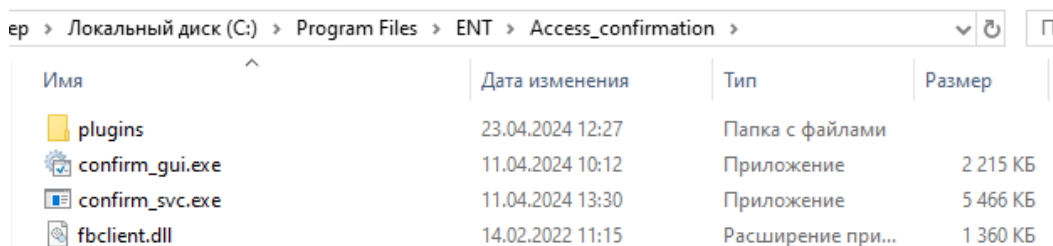
Для реализации специфических сценариев подтверждения доступа на конкретные объекты, наши специалисты могут разработать индивидуальные решения за дополнительную плату. Процесс разработки осуществляется на основании предварительного технического задания, учитывая режим функционирования и особенности объекта.

Программное обеспечение «ЭНТ Контроль Доступа» совместимо только с контроллерами серии «ЭРА» производства компании «ЭРА НОВЫХ ТЕХНОЛОГИЙ» и не поддерживает работу с контроллерами других производителей.

## 2 РАБОТА С ПРОГРАММОЙ

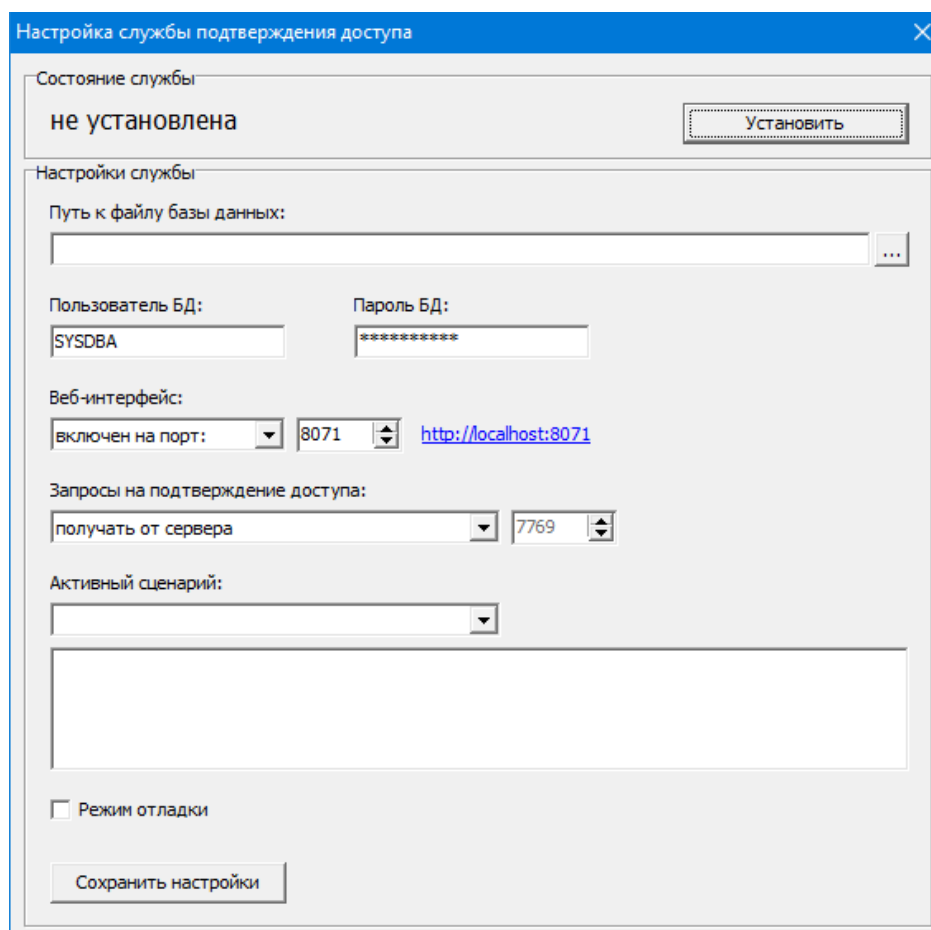
### 2.1 Установка

Произведите распаковку содержимого скачанной папки в директорию ...\\ENT\\.

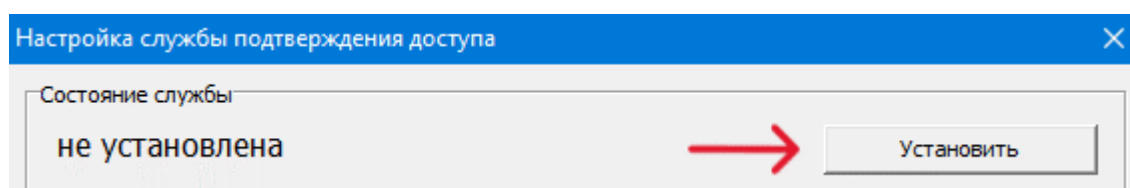


Имя	Дата изменения	Тип	Размер
plugins	23.04.2024 12:27	Папка с файлами	
confirm_gui.exe	11.04.2024 10:12	Приложение	2 215 КБ
confirm_svc.exe	11.04.2024 13:30	Приложение	5 466 КБ
fbclient.dll	14.02.2022 11:15	Расширение при...	1 360 КБ

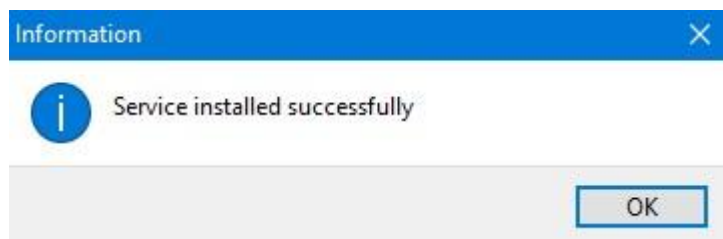
Для удобства использования программы, создан графический интерфейс. Чтобы его открыть, щелкните правой кнопкой мыши на файле `confirm_gui.exe` и выберите пункт «Запуск от имени администратора».



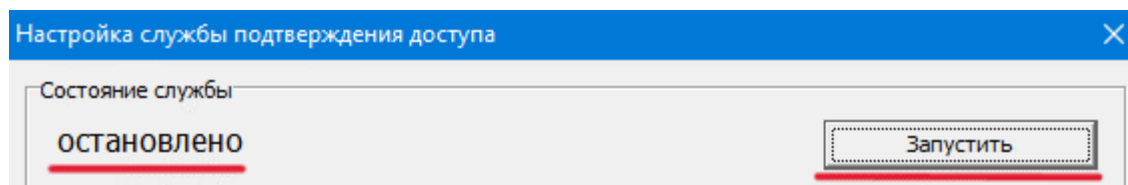
Для установки службы нажмите кнопку «**Установить**».



После успешной установки появится информационное окно с подтверждением:

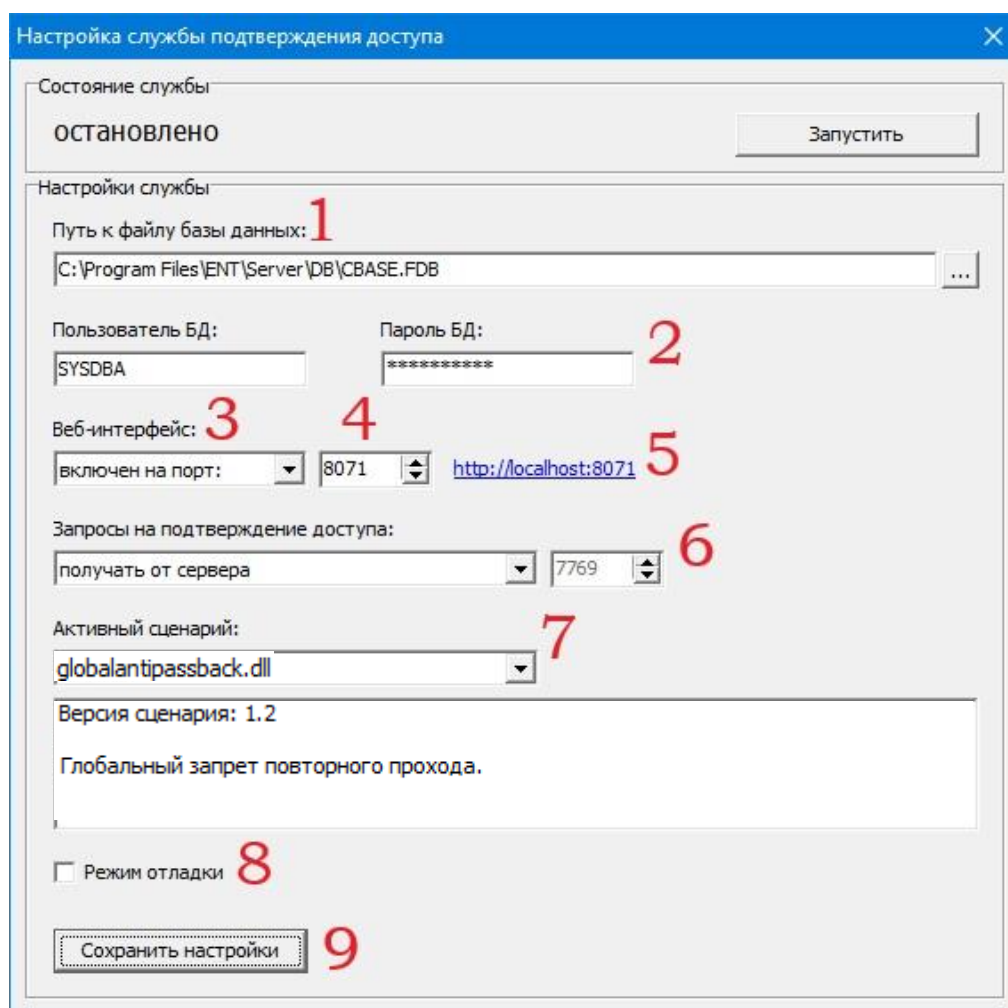


Нажмите «**ОК**». Служба установлена. Состояние службы при этом измениться на «остановлено», а кнопка «Установить» на «Запустить».



## 2.2 Настройка

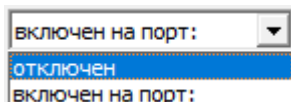
Перед запуском необходимо отредактировать параметры службы.



**1. Путь к файлу базы данных.** Укажите путь до файла CBASE.FDB, расположенный в папке ...\ENT\Server\DB.

**2. Пользователь БД и пароль БД.** По умолчанию в СУБД «Firebird»: SYSDBA и masterkey соответственно.

**3. Веб-интерфейс.** Включите или отключите веб-интерфейс сервиса, выбрав соответствующий параметр в настройках. *Для получения дополнительной информации обратитесь к разделу [«Веб-интерфейс»](#).*



**4.** При выборе опции «**включен на порт**» необходимо указать порт, через который программа будет взаимодействовать с веб-браузером. По умолчанию программа использует программный порт 8071. Если этот порт не занят другими приложениями в системе, его можно оставить неизменным. В случае, если указанный порт уже используется или требуется выбрать другой, следует указать любой доступный свободный программный порт.

**5.** Для доступа к веб-интерфейсу можно воспользоваться следующей гиперссылкой, предназначенной для открытия страницы в веб-браузере.

**6. Запросы на подтверждение доступа.** Выберите метод получения запросов на подтверждение доступа:

1) «**Получать от сервера**»:

- Функционирование системы в данном режиме может быть представлено следующей архитектурой: программа – сервер – контроллер. Контроллер должен поддерживать непрерывное соединение с функционирующим сервером, который, в свою очередь, должен быть подключен к программе. В случае выхода из строя одного из компонентов системы, её функциональность может быть нарушена.

2) «**Получать от контроллеров на указанный порт**»:

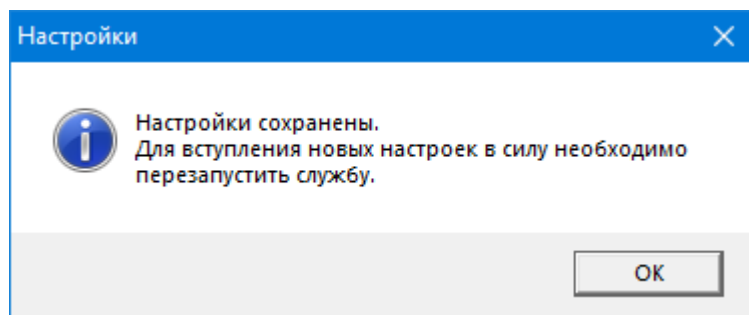
- Работа системы в данном режиме характеризуется архитектурой: программа – контроллер. Контроллер должен обеспечивать постоянное соединение с функционирующей программой. По умолчанию программой используется порт 7769 для взаимодействия с контроллером. Если данный порт занят другими приложениями или требуется выбрать альтернативный, необходимо указать любой другой доступный свободный программный порт.

**7. Активный сценарий.** Выберите необходимый сценарий. Описание предустановленных сценариев представлено в разделе [2.4 «Сценарии»](#) данного руководства.

**8. Режим отладки.** Установите флажок для отображения дополнительной информации в файле с логами *confirm\_svc.log*, который будет создан при запуске службы и появится в папке с файлами службы.

**9.** После ввода параметров необходимо их сохранить. Для этого нажмите кнопку «**Сохранить настройки**».

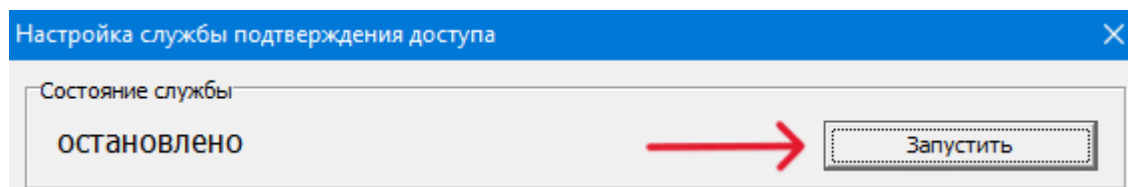
Появится информационное окно. Нажмите «**ОК**».



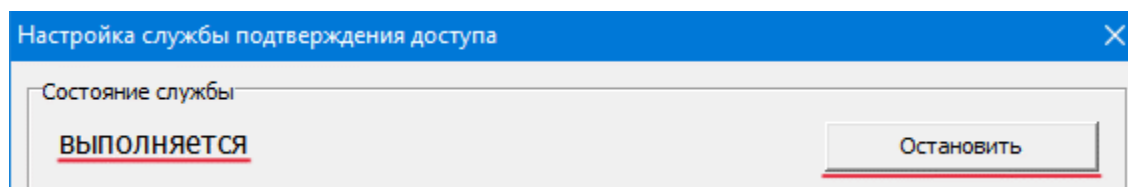
В папке с файлами службы появится конфигурационный файл *settings.ini*.

## 2.3 Запуск/остановка

Для запуска службы можно использовать её графический интерфейс. Для этого щелкните правой кнопкой мыши на файле *confirm\_gui.exe* и выберите пункт «Запуск от имени администратора». Откроется окно «Настройка службы подтверждения доступа». Нажмите кнопку «**Запустить**».



После запуска состояние службы изменится на «выполняется», а кнопка «Запустить» на «Остановить».



Для остановки службы нажмите «**Остановить**».

Окно для настройки службы можно закрыть. Служба будет работать в фоновом режиме и по умолчанию запускаться вместе с ОС Windows.

 **При изменении параметров службы и вступлении их в силу, необходимо перезапустить работу службы.**

## 2.4 Сценарии

Файлы сценариев располагаются в директории *plugins* совместно с файлами службы. В стандартной конфигурации предусмотрено три сценария для подтверждения доступа:

- *globalantipassback.dll* (версия: 3.0) — реализует функцию предотвращения повторного прохода, которая исключает возможность повторного использования одного и того же ключа для входа или выхода без обязательного прохода в обратном направлении. Максимальная длина ключа составляет 8 байт;

- `posbalance.dll` (версия: 2.0) — данный сценарий подтверждает доступ пользователям, имеющим положительный баланс. Максимальная длина ключа составляет 8 байт;
- `once_0to24h.dll` (версия 2.1) – сценарий предоставляет однократный доступ в течение 24-часового периода, начиная с 00:00 и заканчивая 23:59. Каждый новый день доступ автоматически обновляется. В настройках ключа предусмотрена опция «всегда разрешать повторный проход», которая, при активации, обеспечивает постоянное подтверждение доступа.

При выборе соответствующего сценария отображается его краткое описание.

## 2.5 Веб-интерфейс

В веб-интерфейсе отображается системная информация.



```
Версия программы: 3.5.3 сборка 14
Время запуска программы: 26.04.2024 15:39:59
Активный сценарий: globalantipassback.dll
Тип запросов: через сервер на порт 7769
Время последнего запроса: 26.04.2024 15:40:23
Пакетов получено: 3
Доступ подтвержден: 2
Доступ не подтвержден: 1
Ошибок: 0
```


- **Версия программы.**
- **Время запуска программы Подтверждение доступа.**
- **Активный сценарий.**
- **Тип запросов.**
- **Время последнего запроса.**
- **Пакетов получено.** Количество запросов на подтверждение доступа, полученные программой.
- **Доступ подтвержден.** Количество успешных подтверждений прохода.
- **Доступ не подтвержден.** Количество отказов в доступе по определенным причинам, указанным в алгоритме сценария.
- **Ошибок.** Количество ошибок в результате работы алгоритма.

### 3 НАСТРОЙКИ В ПРОГРАММЕ «ЭНТ Контроль доступа – Клиент».

Основные параметры	Дополнительные параметры	Подтверждение доступа	Пожарная тревога
	Считыватель №1 (вход)	Считыватель №2 (выход)	
Время ожидания подтверждения (секунд):	3 <input type="text"/> 0 = <a href="#">отключить</a>	3 <input type="text"/> 0 = <a href="#">отключить</a>	
Ожидать подтверждение для:	<input type="text" value="всех ключей"/>	<input type="text" value="всех ключей"/>	
По окончании ожидания (таймаут):	<input type="text" value="доступ запретить"/>	<input type="text" value="доступ запретить"/>	
Кнопка во время ожидания:	<input type="text" value="не используется"/>	<input type="text" value="не используется"/>	
Термодатчик во время ожидания:	<input type="text" value="не используется"/>	<input type="text" value="не используется"/>	
Отправлять запрос на UDP-порт:	7714 <input type="text"/> <input checked="" type="checkbox"/>	7714 <input type="text"/> <input checked="" type="checkbox"/>	

В программе «Клиент» в конфигурации контроллера необходимо активировать подтверждение доступа. Для этого выберите пункт «Конфигурация» > «Устройства». В таблице добавленных контроллеров выберите контроллер, настройки которого хотите изменить. Откройте закладку «Изменить/удалить выбранный контроллер» > «Подтверждение доступа» и в параметрах ниже укажите необходимые значения.

**Время ожидания подтверждения.** Укажите время в секундах для необходимого считывателя (направления прохода), ожидающего управляющей команды. По истечении заданного времени, если команда не будет получена, контроллер самостоятельно примет решение в соответствии с пунктом "По окончании ожидания".


 Для отключения подтверждения доступа укажите значение времени ожидания подтверждения – 0 или нажмите «отключить».

	Считыватель №1 (вход)	Считыватель №2 (выход)
Время ожидания подтверждения (секунд):	0 <input type="text"/> 0 = <a href="#">отключить</a>	0 <input type="text"/> 0 = <a href="#">отключить</a>

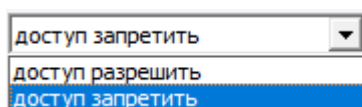
**Ожидать подтверждения для.** Выберите для каких ключей использовать функцию подтверждения доступа. Остальные ключи будут работать по стандартному сценарию.

- всех ключей
- изымаемых ключей
- не изымаемых ключей
- неизвестных ключей

- «**всех ключей**» - для типа ключа «обычный» и «гостевой».
- «**изымаемых ключей**» - только для типа «гостевой ключ».
- «**не изымаемых ключей**» - только для типа «обычный ключ».
- «**неизвестных ключей**» - только для «неизвестных ключей».

 Тип ключа выбирается при добавлении в программу «Клиент» (см. [Руководство пользователя ПО «ЭНТ Контроль доступа – Клиент»](#) > раздел 4.2.2 «Ключи»).

**По окончании ожидания (таймаут).** Если программа по каким-либо причинам не приняла решения о подтверждении доступа за указанное время в параметре **«Время ожидания подтверждения»** контроллер самостоятельно примет решение в соответствии с выбранным значением.



- *«Доступ запретить»* - контроллер запретит доступ.
- *«Доступ разрешить»* - контроллер разрешит доступ.

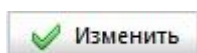
**Кнопка во время ожидания подтверждения.** Выберите *«не используется»*.

**Термодатчик во время ожидания.** Выберите *«не используется»*.

**Отправлять запрос на UDP-порт.** Для активации функции отправки запросов на указанный UDP-порт необходимо установить отметку в соответствующем поле и указать программный порт, на который контроллером будет осуществляться отправка запросов для подтверждения данных.

- Если в настройках программы **«Подтверждение доступа»** в параметре **«Запросы на подтверждение доступа»** выбрано **«Получать от сервера»**, то укажите порт **7714**.
- Если же в настройках программы **«Подтверждение доступа»** выбран параметр **«Получать от контроллеров на указанный порт»**, укажите такой же порт, что указан в параметре **«Получать от контроллеров на указанный порт»** программы **«Подтверждение доступа»**.

После ввода параметров для их применения, нажмите на кнопку **«Изменить»**.



**!** *Указанный для запросов UDP-порт необходимо добавить в правило для входящих подключений брандмауэра Защитника Windows, программы-антивирусы (если установлены), настраиваемые коммутаторы (switch) или маршрутизаторы (если присутствуют в сети). Подробности по настройке стороннего программного обеспечения и/или оборудования смотрите в соответствующих руководствах производителя или обратитесь к системному администратору.*

## 4 ПРИМЕРЫ НАСТРОЙКИ В ПО «ЭНТ Контроль доступа».

Для работы через «Сервер».

Настройки в ПО «Подтверждение доступа»:

Настройка службы подтверждения доступа

Состояние службы  
**ВЫПОЛНЯЕТСЯ** Остановить

Настройки службы

Путь к файлу базы данных:  
C:\Program Files\ENT\Server\DB\CBASE.FDB

Пользователь БД: SYSDBA      Пароль БД: \*\*\*\*\*

Веб-интерфейс:  
включен на порт: 8071      <http://localhost:8071>

Запросы на подтверждение доступа:  
получать от сервера      7769

Активный сценарий:  
globalantipassback.dll

Версия сценария: 1.2  
Глобальный запрет повторного прохода.

Режим отладки

Сохранить настройки

Настройки в ПО «Клиент»:

Основные параметры	Дополнительные параметры	Подтверждение доступа	Пожарная тревога
	Считыватель №1 (вход)		Считыватель №2 (выход)
Время ожидания подтверждения (секунд):	3      0 = отключить		3      0 = отключить
Ожидать подтверждение для:	всех ключей		всех ключей
По окончании ожидания (таймаут):	доступ запретить		доступ запретить
Кнопка во время ожидания:	не используется		не используется
Термодатчик во время ожидания:	не используется		не используется
Отправлять запрос на UDP-порт:	7714 <input checked="" type="checkbox"/>		7714 <input checked="" type="checkbox"/>

Для работы напрямую от контроллеров.

Настройки в ПО «Подтверждение доступа»:

Настройка службы подтверждения доступа

Состояние службы: **Выполняется** Остановить

Настройки службы:

Путь к файлу базы данных: C:\Program Files\ENT\Server\DB\CBASE.FDB

Пользователь БД: SYSDBA      Пароль БД: \*\*\*\*\*

Веб-интерфейс: включен на порт: 8071 <http://localhost:8071>

Запросы на подтверждение доступа: получать от контроллеров на указанный порт: 7769

Активный сценарий: globalantipassback.dll

Версия сценария: 1.2  
Глобальный запрет повторного прохода.

Режим отладки


Сохранить настройки


Настройки в ПО «Клиент»:

Основные параметры	Дополнительные параметры	Подтверждение доступа	Пожарная тревога
		Считыватель №1 (вход)	Считыватель №2 (выход)
Время ожидания подтверждения (секунд):	3	0 = отключить	3
Ожидать подтверждение для:	всех ключей		всех ключей
По окончании ожидания (таймаут):	доступ запретить		доступ запретить
Кнопка во время ожидания:	не используется		не используется
Термодатчик во время ожидания:	не используется		не используется
Отправлять запрос на UDP-порт:	7769 <input checked="" type="checkbox"/>		7769 <input checked="" type="checkbox"/>

## 5 ОБОЗНАЧЕНИЯ, ТЕРМИНЫ И СОКРАЩЕНИЯ

### 5.1 Условные обозначения, принятые в руководстве.

 - *этим знаком отмечены крайне важные предложения. Не соблюдение правил и условий абзацев, помеченных данным знаком, приведет к неработоспособности системы.*

 - *абзацы, выделенные данным знаком, составляют важную информацию о системе, которая облегчит работу с ней.*

 - *справочная информация, разъясняющая некоторые понятия системы.*

### 5.2 Список принятых сокращений

БД – база данных.

СКУД – система контроля и управления доступом.

ОС – операционная система.

ПО – программное обеспечение.

ПК – персональный компьютер.

Клиент – ПО «ЭНТ Контроль доступа – Клиент».

Сервер – ПО «ЭНТ Контроль доступа – Сервер».