



БИОМЕТРИЧЕСКИЙ ТЕРМИНАЛ  
УЧЕТА РАБОЧЕГО ВРЕМЕНИ И КОНТРОЛЯ ДОСТУПА

**BioTime FingerPass T5**



Инструкция настройке и эксплуатации

Москва 2018



## **Биометрический терминал учета рабочего времени и контроля доступа BioTime FingerPassT5:**

Инструкция по настройке и эксплуатации / ООО «Биолинк Солюшенс». – М., 2018. – 32 с.

© ООО «Биолинк Солюшенс», 2018

BioLink, BioTime — зарегистрированные товарные знаки ООО «Биолинк Солюшенс». Другие товарные знаки, упомянутые в документе, являются или могут являться собственностью их правообладателей.

### **О данной инструкции**

- ООО «Биолинк Солюшенс» (далее — компания BioLink) оставляет за собой право вносить изменения в содержание инструкции без предварительного уведомления.
- Некоторые функции, описанные в инструкции, могут отсутствовать в Вашем терминале BioTime FingerPass T5 (далее — терминал) – это зависит от версии микропрограммы.
- Изображения в меню и названия команд в инструкции могут отличаться от изображений и команд в Вашей модели.
- Не все опции, перечисленные в инструкции, поддерживаются программным обеспечением системы BioTime.
- Работоспособность некоторых функций может зависеть от версии используемого программного обеспечения.
- По всем возникшим вопросам обращайтесь в службу технической поддержки компании BioLink.

**Система BioTime и входящие в ее состав биометрические терминалы постоянно совершенствуются. По этой причине технические параметры, приведенные в данной инструкции, могут быть изменены без предварительного уведомления. Упомянутые параметры носят исключительно справочный характер и ни при каких обстоятельствах не могут служить основанием для претензий.**

Для получения актуальной информации о системе BioTime и входящих в ее состав биометрических терминалах посетите ее сайт — [www.biotime.ru](http://www.biotime.ru)

## СОДЕРЖАНИЕ

<b>1. Использование устройства</b> .....	<b>4</b>
1.1. Как сканировать отпечаток пальца.....	4
1.2. Режимы проверки.....	5
<b>2. Главное меню</b> .....	<b>6</b>
<b>3. Управление пользователями</b> .....	<b>8</b>
3.1. Добавление нового пользователя.....	8
3.2. Поиск пользователей.....	9
3.3. Редактирование и удаление пользователей .....	10
<b>4. Управление доступом</b> .....	<b>11</b>
<b>5. Настройка связи</b> .....	<b>12</b>
5.1. Сеть .....	12
5.2. Безопасность соединения.....	12
5.3. Настройки Wiegand.....	13
<b>6. Настройка системы</b> .....	<b>14</b>
<b>7. Управление данными</b> .....	<b>14</b>
<b>8. Управление USB-устройством</b> .....	<b>15</b>
<b>9. Подключение исполнительных устройств</b> .....	<b>15</b>
9.1. Подключение датчика двери.....	17
9.2. Подключение кнопки входа/выхода .....	17
9.3. Подключение системы сигнализации .....	18
9.4. Подключение дверного замка.....	18
<b>10. Эксплуатация терминала</b> .....	<b>23</b>
10.1. Условия использования.....	23
10.2. Действия при обнаружении неисправности.....	24
10.3. Обязательства и условия гарантийного обслуживания .....	25
Гарантийный талон .....	28

# 1. Использование устройства

## 1.1. Как сканировать отпечаток пальца

Для идентификации используйте отпечатки указательного, среднего и безымянного пальцев (большой и мизинец не подходят для идентификации).

Сканер отпечатка пальца расположен справа от дисплея устройства.

- 1) Правильный способ прикладывать палец:

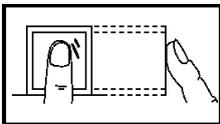


Прикладывайте палец  
к центральной части окна сканирования

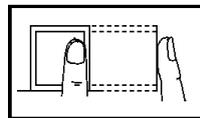
Сканер отпечатков пальцев

- 2) Неправильный способ прикладывать палец:

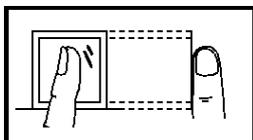
Вертикально



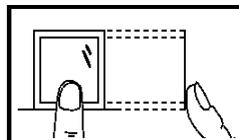
С боковым смещением



С поворотом



Со смещением вниз



Внимательно изучите, как правильно прикладывать палец к сканеру. Неправильное прикладывание пальца может привести к затруднению распознавания.

После идентификации появится сообщение об успешном подтверждении личности.

## 1.2. Режимы проверки

### 1.2.1. Проверка по отпечатку пальца 1:N

Терминал сравнивает цифровую модель вновь отсканированного отпечатка пальца с моделями этих биометрических идентификаторов, хранящимися в памяти терминала.

### 1.2.2. Проверка по отпечатку пальца 1:1

В режиме «Распознавания по отпечатку пальца 1:1» терминал сравнивает цифровую модель вновь отсканированного отпечатка пальца с моделью отпечатка пальца, «прикрепленного» к ID пользователя (ID вводится с клавиатуры). Рекомендуется подключать этот режим, только если трудно распознать отпечаток пальца.

### 1.2.3. Проверка по паролю

В режиме проверки по паролю терминал сравнивает введенный пароль с паролем, прикрепленным к ID пользователя.

Нажмите  на дисплее. Введите ID пользователя и нажмите ОК.

Затем введите пароль пользователя и нажмите ОК.

Введите корректный пароль и нажмите ОК. В результате появится сообщение об успешном подтверждении личности.

#### 1.2.4. Проверка по ID-картам

Проведите картой над датчиком. В результате появится сообщение об успешном подтверждении личности.

## 2. Главное меню

Чтобы открыть главное меню, если терминал находится в режиме ожидания, коснитесь иконки меню  на сенсорном экране.



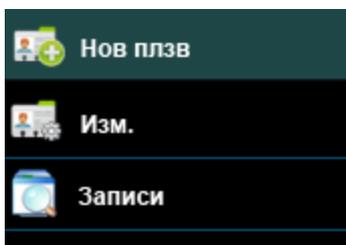
В главном меню доступны следующие опции:

- Управление пользователями (пункт **Упр плзв**) позволяет регистрировать новых пользователей, редактировать и удалять профили, а также искать записи о конкретном пользователе в системе за выбранный месяц.
- Управление доступом (пункт **Доступ**) позволяет назначать права доступа, включая учет временных зон, код разблокировки терминала, параметры замков и сигнализации.
- Настройка связи (пункт **Связь**) позволяет ввести настройки сети для связи устройства с компьютером (IP-адрес, шлюз, пароль входа и т.д.), а также задать Wiegand-функции.
- Настройка системы (пункт **Система**) позволяет сконфигурировать поведение системы, задать системное время, откалибровать сенсорный экран и вернуть состояние системы к стандартным параметрам.
- Управление данными (пункт **Дата**) позволяет удалять логи устройства.
- USB-устройство (пункт **USB-Disk**) позволяет загружать данные (пользовательские логи) с подключенного USB-устройства или закачивать их на него, а также обновлять устройство с USB-носителя.

Нажмите , чтобы выйти из меню.

### 3. Управление пользователями

Основная информация о пользователе на устройстве включает в себя отпечаток пальца, пароль и права доступа. Эта информация может быть добавлена, проверена, изменена или удалена непосредственно на устройстве. Для управления пользователями выберите пункт **Упр плзв** в главном меню.



#### 3.1. Добавление нового пользователя

Выберите пункт **Нов плзв**.

В форме создания нового пользователя введите следующие данные:

- ID (максимум 9 символов);
- пароль (максимум 6 символов);
- роль (стандартный User или Administrator).

Администратор (Administrator): Администратор имеет права доступа ко всем функциям меню.

Пользователь (User): Если в системе зарегистрирован администратор, пользователь может только отмечаться по отпечатку, паролю или карте. Если в системе нет администратора, то пользователь имеет все права.

Чтобы ввести в систему отпечаток пальца пользователя, нажмите **FP**. Будет отображен интерфейс сканирования отпечатка пальца. Пользователю необходимо трижды приложить палец к сканеру (справа от экрана), руководствуясь подсказками на экране. В случае успешного сканирования появится подтверждающее сообщение.

Нажмите  , чтобы вернуться к форме редактирования нового пользователя.

Чтобы ввести в систему данные об ID-карте пользователя, нажмите **Card**.

Пользователю необходимо провести карту над устройством считывания (сканер отпечатка пальца). В случае успешной регистрации ID-карты, терминал автоматически вернется к форме редактирования нового пользователя.

## 3.2. Поиск пользователей

Выберите пункт **Поиск польз.**

С помощью цифровой клавиатуры введите ID искомого пользователя и нажмите **OK**. Если требуется удалить последний введенный символ, нажмите .

В случае успешного поиска информация о пользователе отобразится на экране.

Терминал также позволяет выводить информацию обо всех записях о пользователе в системе за указанный месяц. Для этого перейдите из главного меню в **Упр. Польз.** → **Запись**, введите ID искомого пользователя и выберите месяц, за который нужно отобразить записи.

### 3.3. Редактирование и удаление пользователей

Чтобы отредактировать или удалить профиль пользователя, сначала необходимо найти его профиль по ID (см. пункт 3.2. «Поиск пользователей»).

Нажмите **Изменить.**, чтобы отредактировать пользователя. Поля формы редактирования пользователя соответствуют тем, что указываются при его создании (см. пункт 3.1. «Добавление нового пользователя»).

Отредактируйте пользователя по своему усмотрению и нажмите , чтобы вернуться в предыдущее окно.

Чтобы удалить пользователя, нажмите **Удалить польз.** внизу окна редактирования. Доступны четыре режима удаления:

- Удалить пароль (**Удалить пароль.**);
- Удалить только ID-карту (**Удалить ID карту**);
- Удалить отпечаток (**Удалить ОП**);
- Удалить пользователя (**Удалить Польз.**) – удаляет всю информацию о пользователе.

Выберите требуемый режим и нажмите ОК. Если какой-то параметр (например, пароль) не зарегистрирован для пользователя, соответствующая опция удаления будет недоступна.

Чтобы настроить права доступа пользователя, найдите его в системе и нажмите (**Доступ плзв**). Перейти к настройке доступа можно также из основного меню управления пользователями.

В открывшемся меню вы можете добавить выбранного пользователя в какую-то из групп доступа (по номеру), задать использование временных зон и настроить обязательный ввод отпечатка пальца.

## 4. Управление доступом

Для управления доступом выберите пункт **Доступ** в главном меню.

Для настройки доступны следующие параметры:

- **Временная зона (Зона врем.)** – добавьте временные зоны (интервалы времени для доступа в помещение), которые впоследствии будут привязаны к группам пользователей и другим настройкам.
- **Праздники (Праздники)** – добавьте праздники, чтобы ограничить доступ в праздничные дни, и укажите требуемые временные зоны.

Если время доступа в праздники настроено, в праздники временные зоны пользователя будут определяться этим временем доступа.

- **Группа доступа (Группа. Доступа.)** – создайте группы доступа, которым будут присвоены одна или несколько конкретных временных зон. Сотрудники включаются в ту или иную группу доступа в зависимости от того, в какой интервал времени им должен быть разрешен доступ в помещение. Каждой группе могут быть присвоены до 5 сотрудников.
- **Возврат к стандартным настройкам (Reset A&C Sett.)** – верните все настройки устройства к заводским.

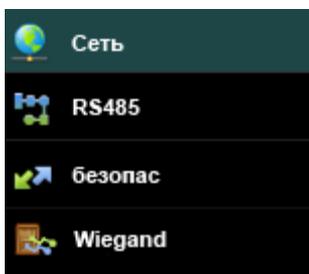
*Замечание:* Профили пользователей и записи посещений удалены не будут.

## 5. Настройка связи

Перед обменом данными между устройством и компьютером настройте параметры соединения.

**Внимание:** настройки связи должны соответствовать настройкам программы на компьютере.

Для настройки связи выберите пункт **Связь** в главном меню.



### 5.1. Сеть

При использовании Ethernet задайте следующие параметры для подсоединения к компьютеру:

- IP-адрес (IP address). По умолчанию, *192.168.1.201*.
- Маска сети (Subnet Mask). По умолчанию, *255.255.255.0*.
- Шлюз (GateWay). По умолчанию, *192.168.1.254*.

### 5.2. Безопасность соединения

Для защиты доступа к записям посещений, необходимо задать пароль для соединения между устройством и компьютером. Пароль вводится, когда устройство подключается для считывания информации.

Пароль по умолчанию: 0. Может быть задано другое значение. После

настройки, при подключении к устройству потребуется ввести пароль или подключение не удастся. Длина пароля – до 6 цифр.

Также в данном меню задается ID устройства. Если Вы используете последовательный порт RS232/RS485, задайте ID от 1 до 254. При использовании RS232/RS485 этот ID необходимо ввести в окне настройки соединения на компьютере.

### 5.3. Настройки Wiegand

Настройте параметры интерфейса Wiegand:

- Формат (26 или 34 бита).
- Биты (количество битов, занятых данными Wiegand).
- Длительность импульса (от 20 до 100 мкс). По умолчанию, 100 мкс.
- Интервал между импульсами (от 200 до 20000 мкс). По умолчанию, 100 мкс.
- Тип ID. Определяет, что будет подаваться на вход Wiegand: ID работника или номер карты.
- Сведения о формате Wiegand.
- Wiegand-выход.
- ID ошибки. Определяет выходное значение для ошибочных идентификаций пользователя. Выходной формат определяется настройками формата Wiegand – от 0 до 65535.
- Код места. Аналогично ID устройства. Код настраивается пользователем. Разные устройства могут иметь одинаковый код (от 0 до 255).

## 6. Настройка системы

Для настройки системы выберите пункт **Система** в главном меню.

Для настройки и просмотра доступны следующие параметры:

- Параметры системы (**Система**).
  - Порог при сравнении 1:1.
  - Порог при сравнении 1:N.
  - Формат даты.
  - Время до перехода в режим сна.
  - Звуки и громкость сигналов.
- Системная информация (**Информация о системе**) – просмотрите информацию о системе, включая номер прошивки устройства.
- Дата и время (**Дата**) – настройте дату и время на терминале.
- Автотест (**Автотест**) – проведите тест дисплея, датчика и работы часов реального времени.
- Калибровка – откалибруйте сенсорный дисплей.
- Системный сброс – автоматический возврат настроек системы к заводским.

## 7. Управление данными

Для управления данными выберите пункт **Дата** в главном меню.

Доступны следующие действия:

- Удалить все логи посещения
- Удалить все логи посещения, информацию о пользователях,

временные зоны, праздники, группы и комбинацию разблокировки терминала

- Присвоить всем администраторам роли стандартных пользователей

## 8. Управление USB-устройством

Для управления подключенным USB-устройством выберите пункт **USB-диск** в главном меню.

Доступны следующие действия:

- Загрузить все логи посещения на USB-носитель, с поддержкой Access-отчёта
- Загрузить всю информацию о пользователях на USB-носитель
- Закачать информацию о пользователях, содержащуюся на USB-устройстве, на терминал.
- Обновить ПО терминала с помощью файла обновления, содержащегося на USB-устройстве

## 9. Подключение исполнительных устройств

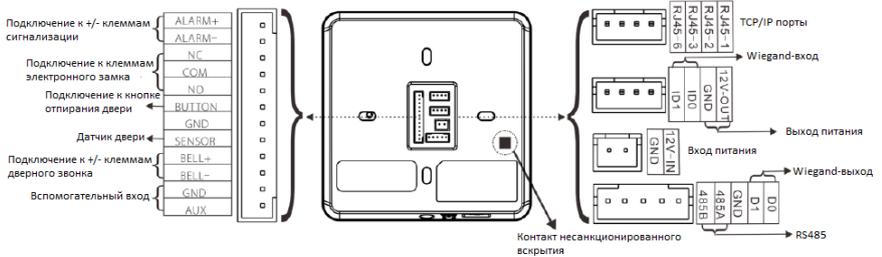
Внимание: не подключайте исполнительные устройства при включенном питании терминала. В противном случае терминал может быть серьезно поврежден.

Следуйте инструкциям ниже для подключения следующих исполнительных устройств:

1. Подключение датчика двери
2. Подключение кнопки входа/выхода

3. Подключение сигнализации
4. Подключение дверного замка
5. Подключение сетевого кабеля Ethernet
6. Подключение кабеля RS485

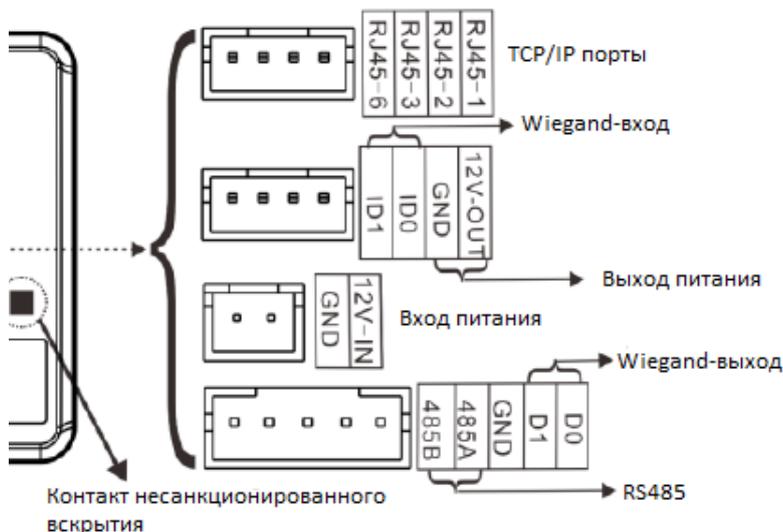
Ниже представлено описание разъемов, расположенных на задней панели биометрического терминала.



Левая часть:



Правая часть:



## 9.1. Подключение датчика двери

Датчик двери используется для определения положения двери (закрыта/открыта). С помощью датчика терминал может установить неавторизованное открытие двери, подавая при этом сигнал тревоги.

## 9.2. Подключение кнопки входа/выхода

Кнопка входа/выхода устанавливается внутри помещения. Когда кнопочный выключатель замкнут, дверь открывается. Расстояние от кнопки до пола составляет примерно 1,4 м. Удостоверьтесь, что кнопка установлена правильно и прямо, а подключение выполнено точно и

надежно. (Неиспользуемые оголенные части провода должны быть отрезаны и изолированы лентой.) Необходимо принимать во внимание электромагнитные помехи (создаваемые, например, включением компьютеров, световых приборов и т.д.).

### **9.3. Подключение системы сигнализации**

Выход на сигнализацию терминала представляет собой сигнал переключения. Он может подключаться к обычной сигнализации с помощью последовательной сети.

### **9.4. Подключение дверного замка**

Способ установки дверного замка зависит от типа замка и конкретных условий эксплуатации. При выборе кабеля электропитания необходимо учитывать использование встроенного резистора для передачи данных на большие расстояния. Дверной замок должен быть установлен надежно и устойчиво. Удостоверьтесь в правильности подключения проводки. Для замков-защелок и электромагнитных замков будьте предельно внимательны при подключении положительного и отрицательного проводов. Неиспользуемую оголенную часть провода необходимо отрезать и изолировать лентой. Время срабатывания замка-защелки настраивается в зависимости от конкретных требований. Выбор электрического замка: для стеклянной двери, открывающейся в двух направлениях, рекомендуется использовать электрический накладной замок; для деревянной двери, открывающейся в одном направлении, мы рекомендуем использовать электромагнитный замок.

Электромагнитный замок более надежен, чем электрический накладной замок, но последний более безопасен. В помещениях небольших размеров рекомендуется использовать электрический накладной замок и электромагнитный замок. Электрические замки производят больше шума при работе; они часто используются внутри зданий. Но теперь появились новые бесшумные электрические замки. Обратите внимание, что замок изготовлен из железа и подвержен образованию ржавчины, поэтому необходимо предотвратить воздействие водной среды или тяжелых условий эксплуатации.

Входной разъем кнопки открытия двери (Button, GND). Входной порт кнопки отпирания двери принимает сигнал, поступающий от нормально разомкнутого контакта, означающего, что кто-то хочет выйти наружу. В этом случае входные устройства, такие как кнопка входа/выхода, выступают в качестве источника передачи сигнала. Когда кнопка отпирания двери не нажата, электрическая сеть оборвана, а при ее нажатии создается замкнутый контур.

*Примечание:* процесс отпирания двери управляется реле при установке дверного замка. При этом необходимо выбрать один из следующих принципов работы замка: сохранность или безопасность. Иными словами, все зависит от того, что должно произойти в результате потери управления дверью: если вы теряете управление дверью, но дверь остается в сохранности – это принцип «потеря управления, но обеспечение сохранности»; если вы теряете управление дверью, но дверь остается в безопасности – это принцип «потеря управления, но обеспечение безопасности».

«Потеря управления, но обеспечение сохранности» означает, что при отключении питания (по причине прекращения подачи питания или

выхода из строя контроллера) дверь автоматически открывается и любой может свободно войти или выйти из помещения. Дверь не закроется до тех пор, пока питание вновь не будет включено. Такие двери устанавливаются в защитных зонах, обеспечивая возможность входа и выхода при отключении питания. Этот принцип действует при использовании электромагнитного замка: при нормальном питании дверь управляется контроллером; как только питание отключается, электромагнитный замок перестает действовать, и дверь открывается и остается открытой.

«Потеря управления, но обеспечение безопасности» - при отключении питания дверь автоматически блокируется, запрещая доступ в помещение снаружи, но позволяя покинуть помещение изнутри. Дверь остается заблокированной до тех пор, пока питание вновь не будет включено. Данный принцип целесообразно применять в случаях, когда речь идет о территории, которая должна быть надежно защищена от неавторизованного доступа в любой ситуации. Указанный принцип действует при использовании электрического замка: при отключении питания дверь невозможно открыть извне, но ее можно открыть изнутри вручную.

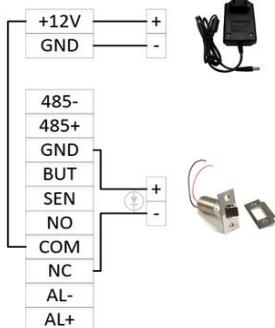
Мы рекомендуем обеспечить отдельное подключение питания биометрического терминала и дверного замка в следующих трех случаях.

- 1) Рабочее напряжение замка составляет 12 В, но разница потребляемого тока терминала и замка не превышает 1 А.
- 2) Напряжение замка отлично от 12 В.
- 3) Расстояние между замком и биометрическим терминалом слишком велико.

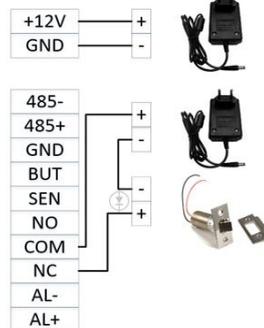
Также рекомендуется использование импульсного диода FR107 (входит в комплект поставки).

### Терминал и замок питаются от одного источника питания

Нормально - открытый замок

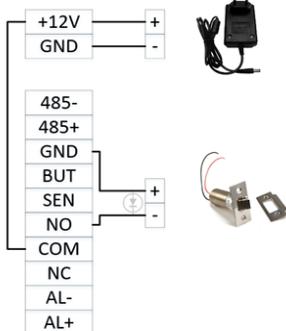


Нормально - открытый замок

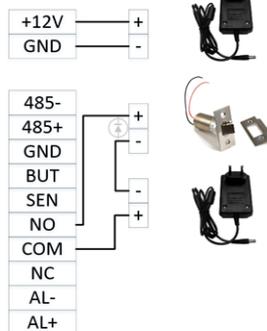


### Терминал и замок питаются от разных источников питания

Нормально - закрытый замок



Нормально - закрытый замок

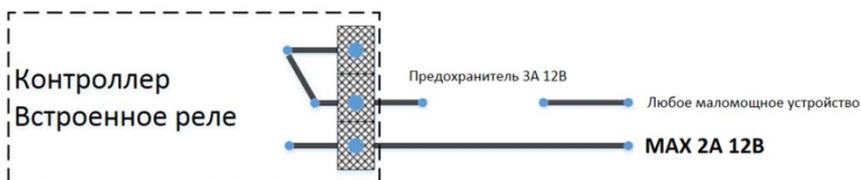


Встроенные в контроллер реле позволяют управлять различными устройствами в цепях постоянного тока напряжением до **MAX 2A 12B**.

Реле поддерживает два состояния NO и NC, для подключения

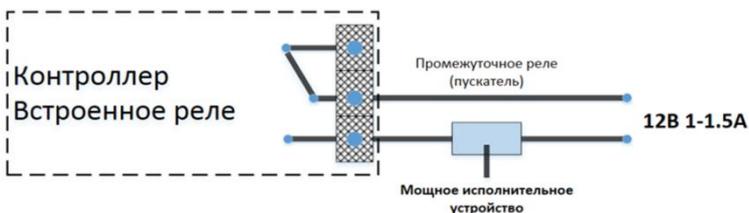
нормально открытых и нормально закрытых устройств, а также один общий контакт (COM).

В качестве примера подключения исполнительных устройств можно воспользоваться приведенными ниже вариантами:



**Во избежание необратимых повреждений печатной платы контроллера, в случае ошибок при монтаже, полезно хотя бы один из проводов в цепи исполнительного устройства в непосредственной близости от клемм блока пропустить через плавкий предохранитель стоком срабатывания до 3А.**

Если необходимо управлять мощными устройствами, а также увеличить срок службы исполнительного реле терминала, то следует использовать промежуточные реле или пускатели соответствующего типа.



## 10. Эксплуатация терминала

Помните, что терминал является высокоточным оптическим устройством и требует бережного отношения. Учтите, что несоблюдение изложенных в данном разделе требований по обеспечению безопасности может создать угрозу Вашей жизни и здоровью, а также привести к прекращению действия гарантийных обязательств.

### 10.1. Условия использования

#### **Категорически ЗАПРЕЩАЕТСЯ:**

- нарушать температурный режим и другие условия эксплуатации терминала;
- применять терминал в помещениях с повышенной опасностью, где присутствует хотя бы один из перечисленных далее факторов: химически активная среда (постоянно или длительно присутствуют пары кислот, щелочей, или других агрессивных соединений); токопроводящая пыль; токопроводящие полы (металлические, земляные, железобетонные, кирпичные и т.п.) без изоляционного покрытия;
- производить любые работы с терминалом при открытой крышке его корпуса, не отключив предварительно электропитание терминала или сетевого преобразователя питания;
- включать блок питания терминала в сеть ~220В (50Гц) при открытой крышке корпуса терминала;
- загрязнять окно сканирования, воздействовать на него колющими и режущими предметами, абразивными и агрессивными веществами,

а также красящими и едкими субстанциями (бензином, нефтью и т.п.);

- опускать терминал в воду и прочие жидкости;
- распылять на терминал и/или вблизи него жидкости и аэрозоли;
- допускать попадание внутрь насекомых и других посторонних веществ, существ и предметов;
- допускать падения и удары терминала и его механические повреждения;
- пытаться самостоятельно вносить изменения в конструкцию терминала;
- изменять, стирать, удалять серийный номер терминала, нарушать целостность заводских пломб;
- передавать терминал для тестирования, ремонта и обслуживания в предприятия и организации, не уполномоченные компанией BioLink на проведение упомянутых работ (список официальных партнеров компании BioLink с указанием их статуса и предоставляемых ими услуг приведен на сайте [www.biotime.ru](http://www.biotime.ru));
- эксплуатировать терминал в телекоммуникационных и кабельных сетях и/или с оборудованием, параметры которых не удовлетворяют требованиям соответствующих стандартов;
- брать за терминал мокрыми руками;
- подносить глаза к окну сканирования.

## **10.2. Действия при обнаружении неисправности**

При обнаружении неисправности незамедлительно прекратите использование терминала и отключите его питание. Обратитесь к поставщику или в службу технической поддержки компании BioLink.

При обращении к поставщику или в службу технической поддержки компании BioLink сообщите сведения о модели терминала и его серийном номере (указаны в Гарантийном талоне или на самом устройстве), представьте копию Гарантийного талона вместе с полным описанием обстоятельств, предшествовавших возникновению неисправности, и предпринятых Вами действий.

После того, как получение Вашего обращения подтверждено, действуйте в соответствии с рекомендациями, поступающими от поставщика или специалистов службы технической поддержки компании BioLink.

### **10.3. Обязательства и условия гарантийного обслуживания**

1. Действие обязательств по гарантийному обслуживанию распространяется на терминалы, приобретенные и эксплуатируемые на территории Российской Федерации.
2. Установка и/или использование терминала означает, что Вы полностью принимаете и согласны с условиями гарантийного обслуживания.
3. Гарантийное обслуживание предоставляется в течение 12 месяцев с даты продажи терминала.
4. Гарантийное обслуживание осуществляется по предъявлении Гарантийного талона с отметкой о дате продажи и подписью уполномоченного представителя покупателя. Если отметка о дате продажи в Гарантийном талоне отсутствует, срок гарантийного обслуживания исчисляется с указанной в талоне даты изготовления терминала. **При отсутствии гарантийного талона гарантийное обслуживание не производится.**

5. Компания BioLink гарантирует, что терминал прошел выходной контроль, соответствует техническим характеристикам, приведенным в данной Инструкции, и признан годным к эксплуатации. Никаких других гарантий (ни явно выраженных, не подразумеваемых) не предоставляется.
6. Компания BioLink не несет никакой ответственности за какой-либо ущерб (включая все, без исключения, случаи потери прибыли, прерывания деловой активности, потери деловой информации, либо других потерь), связанный с использованием или невозможностью использования терминала.
7. Компания BioLink не гарантирует совместную работу терминала с оборудованием других производителей и каким-либо другим программным обеспечением.
8. Заявки на гарантийное обслуживание должны подаваться в письменном виде до истечения гарантийного срока.
9. **Доставка терминала для гарантийного обслуживания поставщику или в компанию BioLink осуществляется за счет потребителя.**
10. Заявки на гарантийное обслуживание должны подтверждаться достаточными для компании BioLink свидетельствами неисправности.

**Гарантийное обслуживание НЕ ПРОИЗВОДИТСЯ, если:**

11. неисправность терминала явилась следствием небрежного обращения, применения терминала не по назначению, нарушения условий эксплуатации и требований обеспечения безопасности;
12. сканирование отпечатков пальцев пользователя невозможно вследствие естественных (природных) особенностей папиллярных узоров отпечатков пальцев отдельных людей.

13. Было произведено изменение или замена существующего программного обеспечения: попытки модификации и установка сторонней прошивки.
14. Неисправности терминала, обнаруженные в период срока его службы, устраняются компанией BioLink или уполномоченными ею ремонтными организациями (авторизованными сервисными центрами). В течение гарантийного срока устранение неисправностей производится бесплатно (при соблюдении потребителем всех условий, приведенных в данном разделе).
15. Компания BioLink может по своему усмотрению произвести гарантийный ремонт неисправного терминала или предоставить потребителю взамен неисправного терминала новый, аналогичный по своим техническим характеристикам неисправному.
16. Дополнительные услуги по установке, техническому обслуживанию, консультированию пользователей, сопровождению терминала и т.п. оказываются в соответствии с планом технической поддержки, выбранным покупателем при приобретении терминала.
17. Производитель имеет право вносить изменения в настоящие условия гарантийного обслуживания путем размещения новой редакции на официальных ресурсах компании. Обязанность самостоятельного ознакомления с актуальной редакцией гарантийных условий лежит на пользователе.
18. Гарантия не распространяется на износ покрытия сканирующего модуля, повреждения корпусов оборудования (в том числе и износ), повреждения соединительных проводов и контактов.
19. По истечении срока действия гарантийных обязательств покупатель вправе заключить с компанией BioLink или уполномоченным ею сервисным центром договор на платное послегарантийное обслуживание терминала.
20. **Срок службы терминала — два года.**



ООО «Биолинк Солюшенс»  
125493, г. Москва  
ул. Авангардная, д. 3  
+7 (499) 281-69-35  
help@biotime.ru

[www.biotime.ru](http://www.biotime.ru)