

Биометрический замок. Руководство

Версия: 1.0

Дата: декабрь 2011

Об этом руководстве

В этом руководстве описывается интерфейс биометрического замка и работа с меню. Установка самого замка показана в анимированном виде отдельным файлом.



Наша продукция время от времени обновляется, поэтому интерфейс системы может не полностью совпадать с описанным в данном руководстве, но принципы работы значительно изменяться не будут.

Содержание

1. Инструкция по использованию	3
1.1 Основные особенности биометрического замка	3
1.2 Комплект поставки	4
1.3 Требования по монтажу	6
1.4 Передний и задний виды	9
1.5 Меры предосторожности	12
1.6 Права пользователей	13
1.7 Установка времени	13
2. Ввод пользователей и верификация	15
2.1 Ввод администратора	15
2.1.1 Регистрация отпечатка	16
2.1.2 Регистрация кода	17
2.1.3 Регистрация RFID-карты	18
2.2 Регистрация рядового пользователя	20
2.3 Дополнительная регистрация	22
2.4 Проверка пользователей и разблокировка замка	23
2.5 Управление FP-картами *	24
2.5.1 Создание ПИН-карты	25
2.5.2 Регистрация FP-карты	27
2.5.3 Создание FP-карты	29
2.5.4 Очистка FP-карты	30
2.6 Удаление данных пользователя	31
3. Информация о замке, настройки системы	33
3.1 Настройки	33

3.2	Выбор языка.....	35
3.3	Код для FP-карты.....	36
3.4	Расширенные настройки.....	36
3.5	Просмотр системной информации.....	37
3.6	Просмотр журнала.....	38
3.7	Работа с USB-устройствами.....	39
4.	Другие функции.....	42
4.1	Индикация.....	42
4.2	Предотвращение утраты администраторских полномочий.....	42
4.3	Защита от разряда батареек.....	42
4.4	Автоматический выход из программы и отключение системы ..	43
4.5	Использование внешнего питания.....	43
4.6	Открытие замка механическим ключом.....	44
Приложение.....		46
	Спецификации.....	46

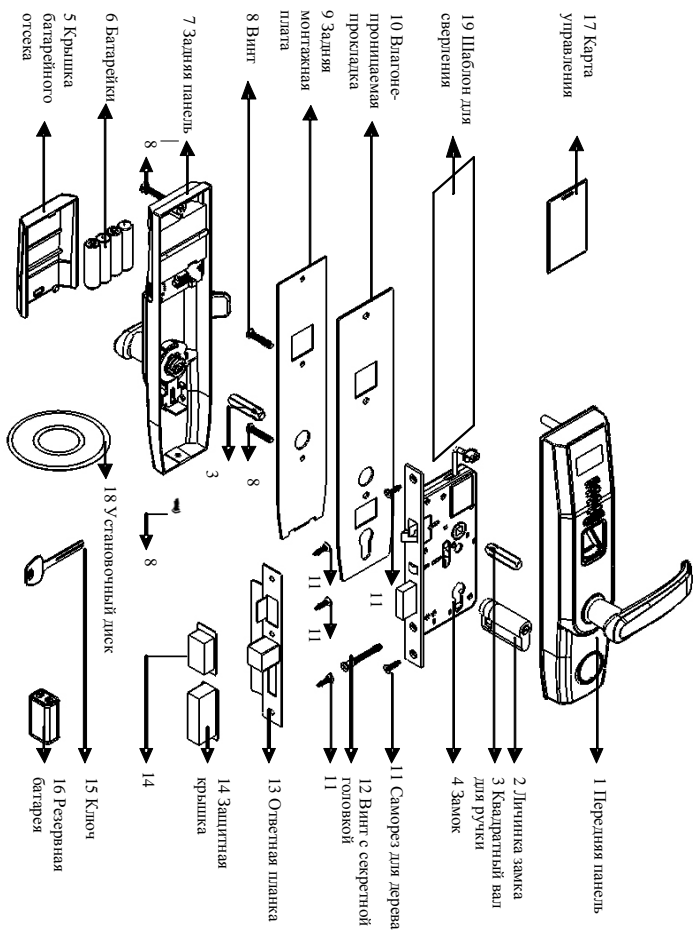
1. Инструкция по использованию

Функции, помеченные в руководстве звёздочкой, поддерживаются не во всех продуктах.

1.1 Основные особенности биометрического замка

1. Комбинация биометрии и криптографии даёт замечательный результат при использовании отпечатков совместно с кодами.
2. Современный дисплей на органических светодиодах (OLED) позволяет выводить чёткое изображение для простого использования замка. Вы сможете легко его эксплуатировать, прочитав данное руководство.
3. Поддержка различных привилегий пользователей: администратор, менеджер, рядовой пользователь.
4. Поддержка частичного и полного удаления данных.
5. Обновление прошивки, загрузка/выгрузка данных пользователей и журналов посещений на USB-накопитель.
6. Возможность просмотра журнала посещений без использования компьютера.
7. Отображение даты и времени с погрешностью менее двух минут в год.
8. Возможность подключения внешней батареи.
9. При необходимости замок можно перевести в состояние разблокировки.
10. Отображение уровня заряда батареи и тревоги при низком заряде.
11. Специальный дизайн, предотвращающий повреждение внутренней структуры биометрического замка в результате резкого воздействия на ручку.

1.2 Комплект поставки

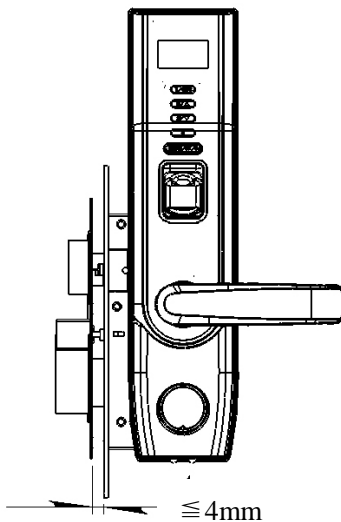


Комплект поставки

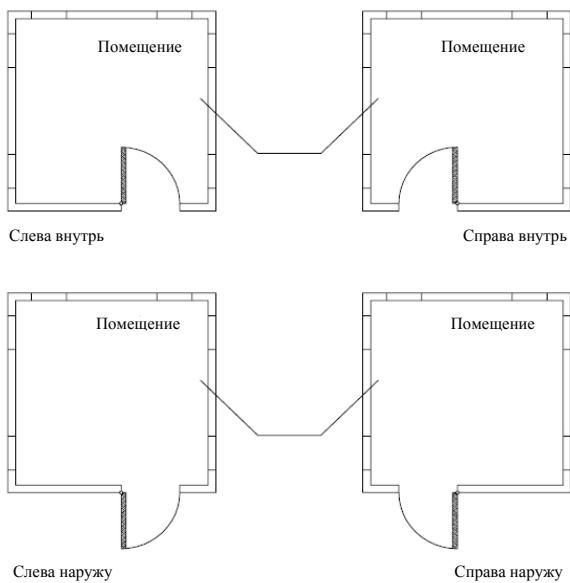
№	Название	Кол-во, шт.	Примечание
01	Передняя панель	1	
02	Личинка замка	1	
03	Квадратный вал ручки	2	
04	Замок	1	
05	Крышка батарейного отсека	1	
06	Батарейки	4	Четыре щелочные батарейки AA
07	Задняя панель	1	
08	Винт	6	Два винта запасные. Выбирайте винты в соответствии с толщиной двери.
09	Задняя монтажная плата	1	
10	Влагонепроницаемая прокладка	2	Для передней и задней панели
11	Саморез для дерева	5	
12	Винт с секретной головкой	1	
13	Ответная планка	1	
14	Защитная крышка	2	
15	Ключ	2	
16	Резервная батарейка	1	9V
17	Карта управления	1	Опционально
18	Установочный диск	1	
19	Шаблон для сверления	1	

1.3 Требования по монтажу

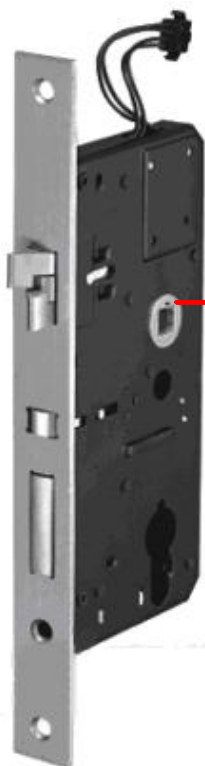
1. Биометрический замок может быть установлен на двери толщиной от 35 до 50 мм.
2. Зазор между замком и защитными крышками не может быть больше 4 мм, в ином случае вам придётся что-то придумывать для его уменьшения:



3. Дверь может открываться в четырёх направлениях: внутрь слева, наружу слева, внутрь справа, наружу справа. Вам нужно выбрать соответствующий замок – левый или правый:



4. Центральная точка ручки должна быть примерно на 1 м от пола.
5. Отмеченная точка зажимного механизма должна быть правее и выше самого зажимного механизма.



Маркерная точка
правее и выше
зажимного механизма

6. Руководствуйтесь анимированной инструкцией по установке замка.

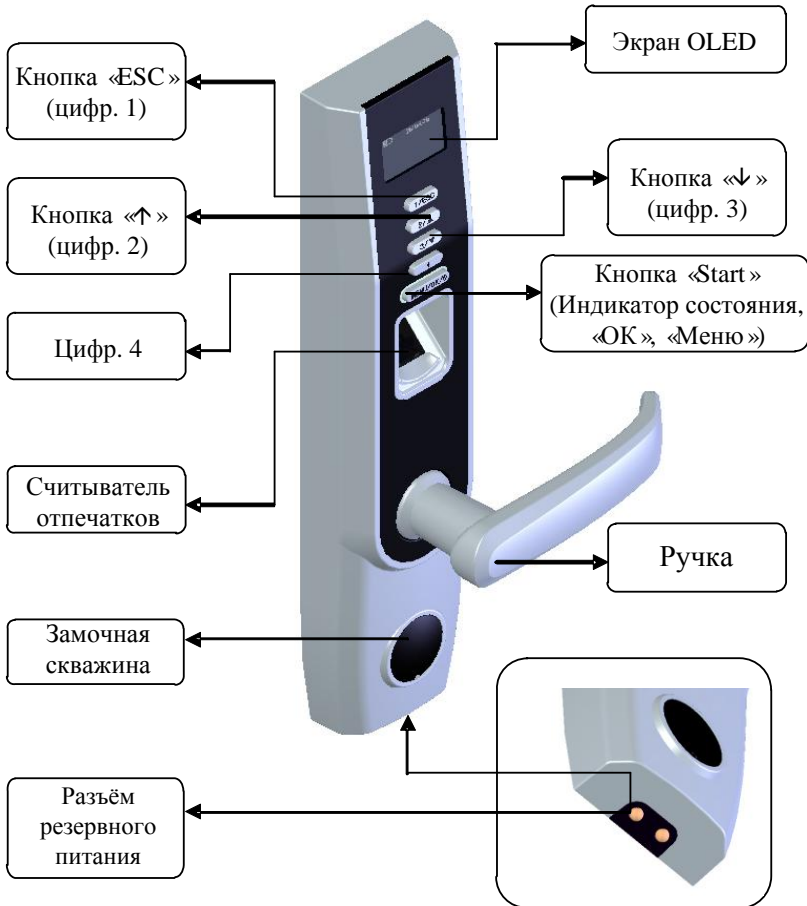
Монтажные инструменты

Для монтажа замка вам понадобятся следующие инструменты:

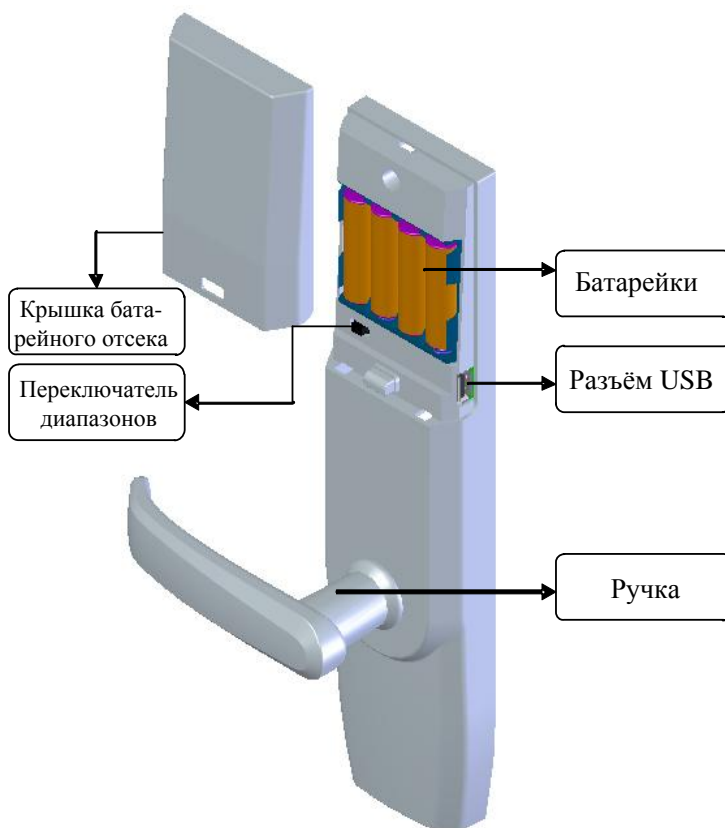
- Рулетка
- Карандаш
- Дрель
- Крестовая отвёртка

1.4 Передний и задний виды

Передний вид



Задний вид



Кнопка «ESC»: Нажатие на эту кнопку завершает текущее действие. Длительное нажатие выключает замок. Также эта кнопка отвечает за ввод цифры «1».

Кнопка «↑»: Эта кнопка увеличивает числовое значение в настройках (длительное нажатие – быстрое увеличение). В меню она перемещает курсор вверх. При вводе кода отвечает за цифру «2».

-
- Кнопка «**↓**»: Кнопка уменьшает числовое значение в настройках (длительное нажатие – быстрое уменьшение). В меню она перемещает курсор вниз. При вводе кода отвечает за цифру «3».
- Кнопка «**Start**»: Кнопка используется для запуска замка. Удержание её в течение трёх секунд на главном экране открывает меню. Также кнопка используется для подтверждения выбора («OK»).
- Переключатель «**Band**»: Если вы по какой-то причине утратили администраторский доступ и не можете войти в меню, выполните следующие действия: нажмите и удерживайте кнопку «**Menu**» в течение трёх секунд для отображения экрана проверки администратора, после чего воспользуйтесь переключателем **Band** на задней стороне замка, чтобы войти в меню в качестве администратора.
- Индикатор статуса: Перевод замка в режим ожидания осуществляется нажатием кнопки «**Start**». Если замок работает корректно, светодиод будет моргать зелёным цветом. В случае возникновения ошибок индикатор будет гореть красным цветом в течение трёх секунд. В качестве подтверждения успешности операции, светодиод будет гореть зелёным в течение трёх секунд.
- OLED-экран: Монохромный OLED-экран может отображать белый текст или графику на чёрном фоне.
- Считыватель отпечатков: Когда считыватель подсвечивается, вы можете вводить отпечатки в базу данных, либо осуществлять проверку

пользователей. При отключенной подсветке приложенный палец не вызовет никакого ответного действия.



Примечание: Если вы не можете выключить замок из-за программной ошибки, нажмите и удерживайте кнопку «ESC», пока замок не перезагрузится. При нормальном функционировании данной возможностью лучше не пользоваться.

Резервные интерфейсы

Замочная скважина: Вы можете открыть дверь механическим ключом в случае особой необходимости.

Внешний интерфейс резервного питания: Вы можете подключить внешнее питание для открытия замка, если встроенные батареи не могут обеспечить работу устройства.

Интерфейс USB

USB-интерфейс используется для обновления прошивки и обмена данными с USB-накопителем (информация о пользователях, журнал посещений).

1.5 Меры предосторожности

1. Настоятельно рекомендуется зарегистрировать хотя бы одного администратора после установки биометрического замка. В любом случае нужно будет регистрировать администратора до регистрации рядовых пользователей.
2. Не вытаскивайте батарейки во время сравнения, ввода или удаления отпечатков, поскольку неожиданное отключение питания может привести к потере данных в системе. Прежде, чем заменить батарейки, выключите замок.

-
3. Рекомендуется заменять батарейки в замке как минимум раз в полгода во избежание повреждения схем в результате утечки электролита. Не используйте некачественные батарейки.
 4. При установке замка подключайте разъёмы правильно. Неправильное подключение может вызвать повреждение устройства.

1.6 Права пользователей

В системе предусмотрено три типа пользователей: администраторы, менеджеры и рядовые пользователи.

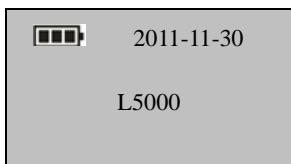
Администраторы имеют доступ ко всем функциям системы и могут изменять все настройки.

Менеджеры могут делать в системе всё, кроме некоторых расширенных функций и ввода администраторов.


Рядовые пользователи имеют доступ только к функциям считывания отпечатков и разблокировки замка.

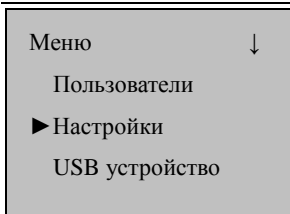
1.7 Установка времени

Перед началом использования замка вам следует установить дату и время. Для этого выполните следующие действия:

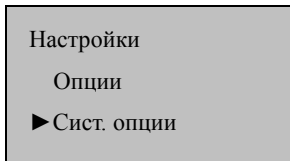


1) Включите замок, нажав кнопку «**Start**». Вы увидите стартовый экран как показано на изображении слева.

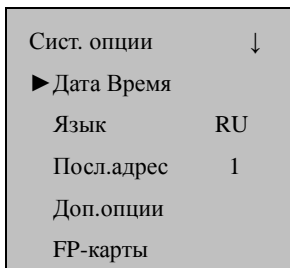
Примечание: Значок  на стартовом экране показывает уровень заряда батареи. В правом верхнем углу отображается дата и время (с интервалом переключения в 5 секунд).



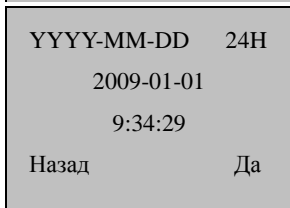
2) Нажмите и удерживайте кнопку **«Меню»** в течение трёх секунд для доступа в меню. Выберите **«Настройки»**, нажимая **▼**. Затем нажмите **«ОК»** для перехода к настройкам.




3) Нажмите **▼** для выбора пункта **«Сист. опции»** и **«ОК»** для входа.



4) Нажмите **«ОК»** для выбора **«Дата Время»**.



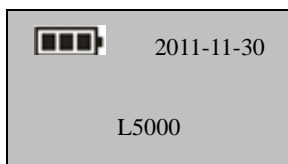
5) Для изменения даты или времени нажимайте кнопки **▲/▼** для перемещения курсора к нужному пункту. Теми же кнопками вводится непосредственно дата и время. Нажимайте **«ОК»** для сохранения настроек.

 **Примечание:** Дата должна попадать в интервал с 1 января 2003 года по 31 декабря 2032 года. Чтобы установить дату за пределами этого диапазона, проконсультируйтесь со своим поставщиком или технической поддержкой.

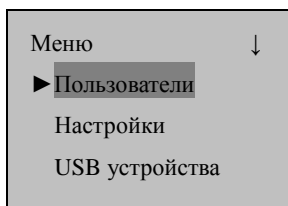
2. Ввод пользователей и верификация

2.1 Ввод администратора

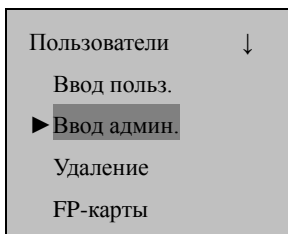
Если в биометрическом замке отсутствует учётная запись администратора, вам следует задать её до ввода рядовых пользователей. Для ввода администратора следует выполнить следующие шаги:



1) Включите биометрический замок, нажав кнопку **«Start»**. Затем нажмите и удерживайте кнопку **«Menu»** до появления меню.



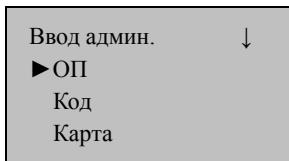
2) Нажмите кнопку **«OK»** для входа в интерфейс управления пользователями.



3) Нажмите **▼**, чтобы выбрать **«Ввод админ.»**. Подтвердите выбор нажатием **«OK»**.

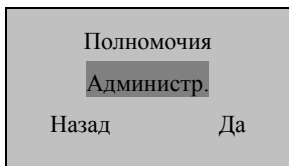
Теперь вы можете зарегистрировать отпечаток, код или RFID-карту для администратора.

2.1.1 Регистрация отпечатка



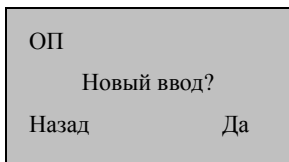
Ввод админ. ↓
▶ ОП
Код
Карта

4) Выберите пункт **«ОП»** и нажмите **«ОК»**.



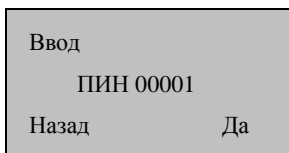
Полномочия
Администр.
Назад Да

5) Нажимая кнопки **▲/▼**, выберите **«Ввод админ.»**, после чего укажите уровень полномочий **«Администр.»** или **«Менеджер»**. Кнопкой **«ОК»** подтвердите свой выбор.



ОП
Новый ввод?
Назад Да

6) На вопрос о вводе нового отпечатка ответьте утвердительно, нажав **«ОК»**.



Ввод
ПИН 00001
Назад Да

7) Система назначает неиспользованные идентификаторы по порядку, но вы можете ввести незадействованный номер вручную.




00001-0
Приложите палец...
Назад (Выход)

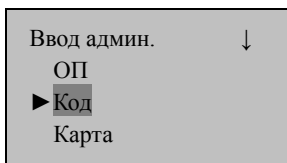
Каждое успешное считывание отпечатка будет отображаться на данном индикаторе.

8) Определитесь, какой палец вы хотите зарегистрировать, и приложите его три раза к считывателю. В случае успешного считывания система выдаст запрос на сохранение отпечатка. В случае неудачи – попросит повторить ввод. По окончании ввода система вернётся к интерфейсу

ввода нового отпечатка. Вы можете зарегистрировать ещё один палец для администратора, либо закончить на этом.

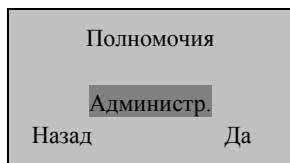
 **Примечание:** последняя цифра в строке «00001-0» ссылается на зарегистрированные отпечатки, начиная с нуля. Например, «0» - первый отпечаток, «1» - второй и т.д.

2.1.2 Регистрация кода



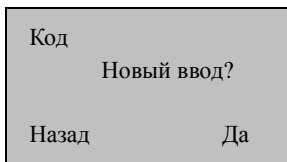
Ввод админ. ↓
ОП
▶ **Код**
Карта

4) Выберите пункт «**Код**» и нажмите «**ОК**».



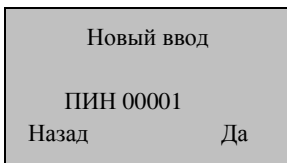
Полномочия
Администр.
Назад Да

5) Нажимая кнопки ▲/▼, выберите «**Ввод админ.**», после чего укажите уровень полномочий «**Администр.**» или «**Менеджер**». Кнопкой «**ОК**» подтвердите свой выбор.



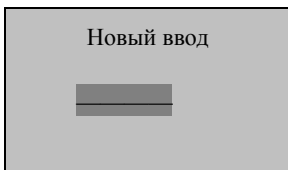
Код
Новый ввод?
Назад Да

6) На вопрос о вводе нового кода ответьте утвердительно, нажав «**ОК**».

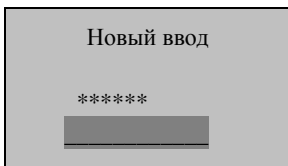


Новый ввод
ПИН 00001
Назад Да

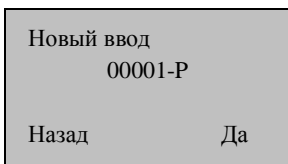
7) Система назначает неиспользованные идентификаторы по порядку, но вы можете ввести незадействованный номер вручную.




8) Введите код, нажимая кнопки с цифрами. Затем нажмите **«ОК»** для завершения ввода.




9) Введите код ещё раз и нажмите **«ОК»** для подтверждения. Затем нажмите **«ОК»** для выхода в меню нового ввода.

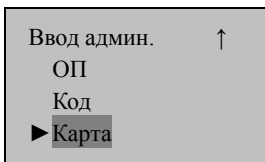


10) Нажмите **«ОК»** для сохранения введённых данных и выхода из меню ввода кода.

 **Примечание:** Код может содержать от 6 до 10 цифр. Вы можете ввести только один код для каждого пользователя системы. Повторяющиеся коды допускаются.

2.1.3 Регистрация RFID-карты

 **Примечание:** Функция реализована только в биометрических замках со считывателем RFID-карт.



4) Выберите **«Карта»** и нажмите **«ОК»**.

Полномочия	
Администр.	
Назад	Да

5) Нажимая кнопки ▲/▼, выберите «Ввод админ.», после чего укажите уровень полномочий «Администр.» или «Менеджер». Кнопкой «ОК» подтвердите свой выбор.

Карта	
Новый ввод?	
Назад	Да

6) На вопрос о считывании новой карты ответьте утвердительно, нажав «ОК».

Новый ввод	
ПИН 00010	
Назад	Да

7) Введите идентификатор пользователя (число в диапазоне от 1 до 65534) и нажмите «ОК» для продолжения.

Новый ввод	
Считыв. карты	
ПИН 00010	
Назад	Да

8) Приложите карту в ответ на соответствующий запрос.

Новый ввод	
Карта: 16650449	
ПИН 00010	
Назад	Да

9) Номер карты отобразится на экране.

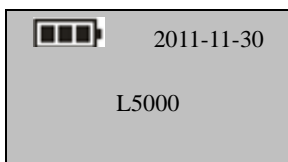
Новый ввод	
000010-С	
Назад	Да

10) Для перехода к следующему шагу нажмите **ОК**.
Буква «С» в строке «00010-С» обозначает привязанную RFID-карту.

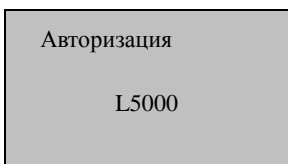
11) Нажмите «**OK**» для сохранения считанных данных и выхода из режима считывания карты.

2.2 Регистрация рядового пользователя

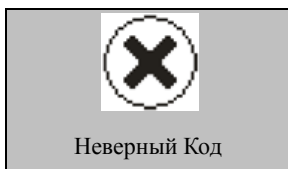
Менеджер может заводить только рядовых пользователей, для чего нужно выполнить следующие действия:



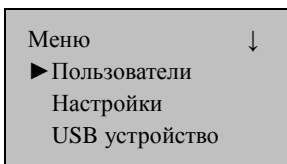
1) Включите замок, нажав кнопку «**Start**».



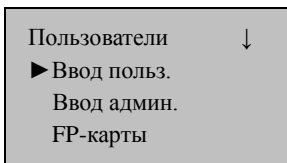
2) Нажмите и удерживайте кнопку «**Menu**» для входа в меню. Система запросит подтверждения администраторских полномочий. Введите администраторский код или приложите палец к считывателю. Если авторизация прошла успешно, переходите к шагу 4.



3) В случае ошибки авторизации отобразится сообщение «**Неверный код**», после чего система вернется к экрану «**Авторизация**» для повторной авторизации.



4) Нажмите **«ОК»** для входа в интерфейс управления пользователями.

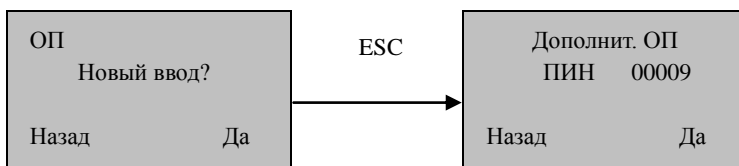


5) Нажмите **▼** для выбора пункта **«Ввод польз.»** и подтвердите выбор кнопкой **«ОК»**.

Теперь можно начать считывание отпечатков, RFID-карт и ввод кодов. Порядок действий тот же, что и при регистрации администратора (см. п. 2.1) за тем исключением, что не нужно выбирать привилегии.

2.3 Дополнительная регистрация

Если вы нажмёте «ESC» на экране новой регистрации, отобразится экран дополнительной регистрации.

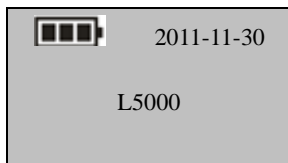


Последовательность шагов при дополнительной регистрации в целом совпадает с обычной регистрацией, за исключением того, что в верхней части экрана отображается другая надпись.



- Примечание:**
1. Рекомендуется зарегистрировать как минимум два отпечатка для пользователей, которые планируют пользоваться системой в течение продолжительного срока.
 2. Если вы хотите изменить код после его ввода, вы можете заменить оригинальный код с помощью резервного.
 3. Дополнительную RFID-карту создать нельзя. Новая карта заменит собой старую.

2.4 Проверка пользователей и разблокировка замка



1) Нажмите кнопку «Start» для включения замка.

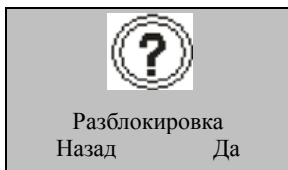
2) Приложите ранее зарегистрированный палец к считывателю или введите свой код / приложите карту.

Примечание: В режиме разблокировки замок не обрабатывает идентификационные данные, поскольку он и так открыт.

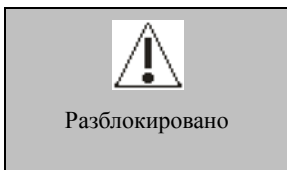


3) После успешной идентификации ваш номер отобразится на экране, и вы услышите соответствующий звук. Для открытия замка нужно повернуть ручку в течение 4 секунд.

Если функция разблокировки включена в меню (см. п. 3.1), будет выдан запрос на разблокировку (см. шаг 4 и 5).




4) Нажмите «ESC» в ответ на запрос разблокировки, и замок будет закрыт. Значок «Открыто» на экране сменится на «Закрыто», после чего замок выключится.




5) Если вы нажмёте **«ОК»**, замок перейдёт в режим разблокировки с отображением соответствующего сообщения и тройным звуковым сигналом.

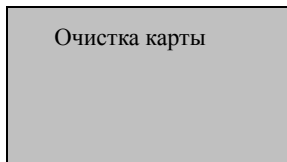
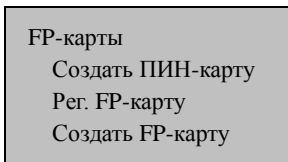
Если код или отпечаток не опознаны системой, будет выдано сообщение **«Попробуйте ещё»** или **«Неверный Код»**. Параметры **«Счетчик»** и **«Тревога»** устанавливаются администратором. Система выдаст тревогу после достижения заданного количества ошибочных попыток. Подробнее об этом в разделе 3.1.

 **Примечание:** Если значение параметра **«Счетчик»** - более 6, система автоматически отключится при совершении 6 ошибок подряд.

2.5 Управление FP-картами *

 **Примечания:** 1) Эта функция присутствует в замках со считывателем карт Mifare.
2) При отсутствии в системе администратора будет выдан запрос на его регистрацию.

Выберите **«FP-карты»** из меню **«Пользователи»**:



Создать ПИН-карту: Вы можете создать ID-карту для пользователя, уже зарегистрированного в системе. Данная карта будет

использоваться вместо отпечатка (если установлен параметр «Только карта». Подробнее в разделе 3.1).

Зарег. FP-карту: Вы можете сохранить считанный отпечаток прямо в FP-карте, а не в замке. Верификацию пользователя можно производить в виде «FP-карта + отпечаток». В этом случае карту нужно прикладывать перед пальцем.

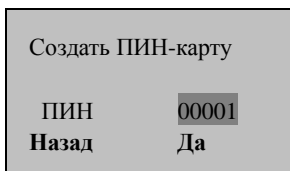
Создать FP-карту: Эта функция используется для создания дубликата считанных отпечатков (сохранённых в биометрическом замке) в FP-карте. Вы можете производить проверку пользователей как по отпечатку, так и в виде «FP-карта + отпечаток».

Очистить карту: Эта функция используется для удаления всех данных (отпечатков и чисел), сохранённых в FP-карте.

2.5.1 Создание ПИН-карты

1. Создание ПИН-карты

Каждому пользователю, регистрируемому в замке, назначается идентификационный номер, например, 00001.



1) Выберите в главном меню **Пользователи** → **FP-карты** → **Создать ПИН-карту**. Отобразится экран, как показано на снимке слева.

Создать ПИН-карту
Приложите карту

2) Когда система спросит ПИН пользователя, нажмите ▲/▼ для выбора желаемого ПИН и подтвердите выбор кнопкой **ОК**. Будет выдан запрос на считывание карты (если ПИН пользователя не существует, вы увидите сообщение «**Не зарегистрир.**»).

Создать ПИН-карту
Завершено

3) Приложите карту к считывателю. При удачной записи в карту система сообщит «**Завершено**». Вы можете заменить верификацию по отпечатку на верификацию по ПИНу.

Создать ПИН-карту
Ошибка -7

Если вы видите такое сообщение, значит, запись карты не удалась.

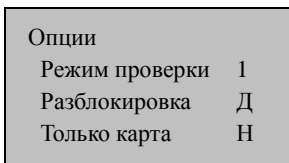
Примечание: Чтобы создать ПИН-карту, нужно убедиться, что пользователь с указанным ПИН уже существует в системе, иначе система выдаст сообщение «**Не зарегистрир.**». После успешной регистрации ПИН будет записан в ПИН-карту.

2 Проверка ПИН-карты

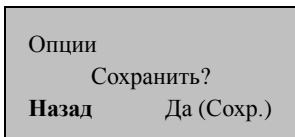


Примечание: Установите параметру «**Только карта**» значение «**Да**».

Если вы поставите значение «**Нет**», проверка с помощью ПИН-карты будет невозможна.



1) Выберите в главном меню **«Настройки»** → **«Опции»**. Вы увидите интерфейс, показанный на снимке слева.



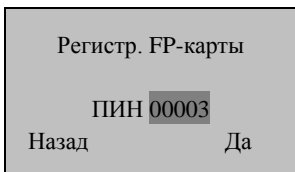
2) Выберите **«Только карта»** и нажмите **«ОК»**. С помощью кнопок **▲/▼** выберите **«Да»** и подтвердите изменение нажатием **ОК**. Теперь вы можете выполнять проверку пользователей с помощью ПИН-карты.



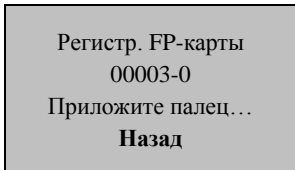
3) Приложите ПИН-карту к считывателю, когда система будет находиться на стартовом экране. Если замок успешно разблокируется, ПИН-карта создана и действует.

2.5.2 Регистрация FP-карты

1. Регистрация FP-карты



1) Выберите в главном меню **«Пользователи»** → **FP-карты** → **Регистр. FP-карты**.



2) Нажимая **▲/▼**, выберите ПИН пользователя и нажмите **«ОК»** для перехода к следующему шагу. На соответствующий запрос системы приложите палец к считывателю.

<p>Регистр. FP-карты 00003-0 Приложите 2 раз Назад</p>	<p>3) Приложите тот же палец повторно.</p>
<p>Регистр. FP-карты 00003-0 Приложите 3 раз Назад</p>	<p>4) И, наконец, приложите палец в третий раз.</p>
<p>Регистр. FP-карты 00003: 1 Приложите карту</p>	<p>Далее система запросит карту.</p>
<p>Регистр. FP-карты 00003: 1 Завершено</p>	<p>5) Приложите карту к считывателю. Если вы увидите сообщение, как показано на снимке слева, карта успешно записана.</p>

2. Проверка зарегистрированной FP-карты


Примечание: Установите параметру «Только карта» значение «Нет», иначе замок будет осуществлять проверку только по ПИН-картам.



1) На стартовом экране приложите FP-карту к считывателю. Будет выдан запрос как на снимке слева.



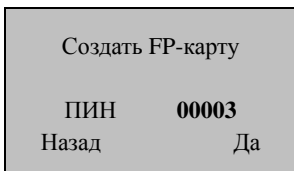
2) Приложите один из ранее зарегистрированных пальцев к считывателю отпечатков. Если будет показано сообщение как на снимке слева, FP-карта успешно прошла проверку.

 **Примечание:** Выполняя вышеприведённые операции, помните, что отпечатки сохраняются в вашей карте, а не в памяти замка. Таким образом, вам необходимо сначала приложить карту, а потом палец, иначе распознавание работать не будет.

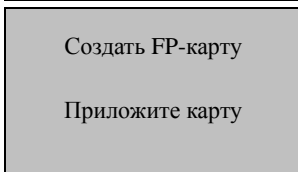
2.5.3 Создание FP-карты

1. Создание FP-карты

Каждый пользователь системы во время регистрации отпечатка получает свой идентификатор, например, 00003.



1) Выберите в главном меню **«Пользователи»** → **FP-карты** → **Создать FP-карту**. Вы увидите сообщение, показанное на снимке слева.



2) Нажмите **«ОК»**. Отобразится запрос на карту.

Создать FP-карту

Завершено

3) Приложите карту к считывателю. Если вы увидите сообщение, показанное на снимке слева, FP-карта успешно создана.

2. Проверка созданной FP-карты

Примечание: Установите параметру «Только карта» значение «Нет».

Операция проверки созданной FP-карты аналогична операции проверки зарегистрированной.



Примечание: Выполнив вышеприведённые операции, вы создадите копию отпечатка в FP-карте. Таким образом, отпечаток сохранится и в карте, и в замке. Вы сможете выполнять открывать замок как по отпечатку, так и в режиме «карта + отпечаток».

2.5.4 Очистка FP-карты

Для удаления всей информации из FP-карты, выполните следующие действия:

Очистка карты

Приложите карту

1) Выберите в главном меню **Пользователи** → **FP-карты** → **Очистка карты**.

Очистка карты

Завершено

2) Поднесите карту к считывателю. Вы увидите сообщение, показанное на снимке слева. Это означает успешное стирание данных из карты.

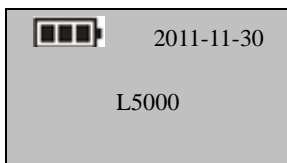
2.6 Удаление данных пользователя



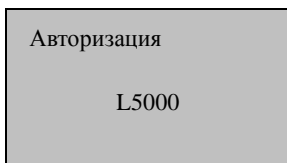
Важно:

Ни в коем случае не отключайте питание биометрического замка во время удаления данных пользователя, иначе могут быть потеряны данные и других пользователей.

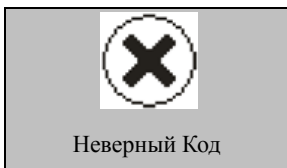
Для удаления данных пользователя выполните следующие действия:



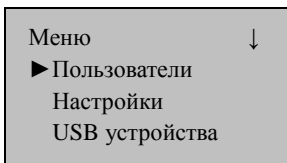
1) Включите замок нажатием клавиши **«Start»**.



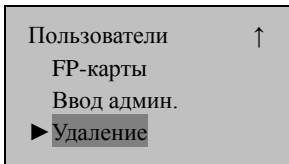
2) Введите код администратора, либо приложите соответствующий палец. Если проверка выполнена успешно, переходите к шагу 4, иначе – к шагу 3.



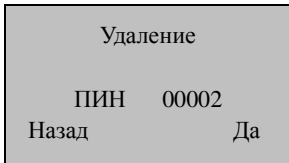
3) Отобразится сообщение **«Неверный Код»**, после чего система вернётся к интерфейсу повторной проверки администратора. В результате успешной проверки вы получите доступ к меню.



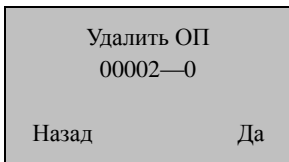
4) Нажмите **«OK»** для перехода к меню управления пользователями.



5) Нажимая **▼**, выберите **«Удаление»**.
Подтвердите свой выбор кнопкой **«ОК»**.

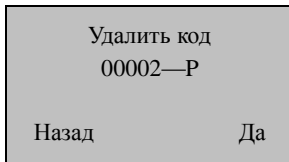


6) Кнопками **▲/▼** выберите ПИН пользователя, который вы хотите удалить, и нажмите **«ОК»**.



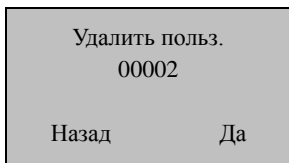
Если для пользователя были зарегистрированы отпечатки,

7) Нажмите **«ОК»** для удаления отпечатков.



Если для пользователя был зарегистрирован код,

8) Нажмите **«ОК»** для удаления кода.



9) И, наконец, нажмите **«ОК»** для удаления пользовательской учётной записи, либо **«ESC»** для возврата в меню **«Пользователи»** без удаления записи.

10) После удаления данных пользователя вы можете перезапустить замок и убедиться, что его в систему больше не пускают.



Примечание: Менеджеры (а также администраторы) могут удалять только рядовых пользователей. Для удаления администратора вам нужно

выбрать в меню **«Настройки»** → **«Сист.опции»** → **«Доп.опции»** → **«Удал.адм.прав»**, после чего следует выполнить действия по удалению рядового пользователя.

3. Информация о замке, настройки системы

3.1 Настройки

Выберите **«Настройки»** → **«Опции»** из главного меню. На экране отобразится следующая информация:

Опции	
Тревога	Д
Счетчик	10
Замок	5

Режим	1
Разблокировка	Д
Только карта	Н

«Опции» включают в себя:


Тревога: Биометрический замок отключится автоматически при достижении заданного количества ошибочных входов. После перезагрузки он будет пищать в течение 30 секунд, а затем отключится.

Счетчик: Параметр устанавливает допустимое количество ошибочных входов до перехода в режим тревоги. Диапазон значений: от 3 до 99. Значение по умолчанию: 10.

 **Примечание:** Счётчик ошибок накапливается между включениями замка.

При достижении заданного значения генерируется событие тревоги. После успешной разблокировки счётчик сбрасывается.

Замок: Параметр определяет продолжительность разблокировки замка после успешной верификации пользователя. Выберите пункт «**Замок**» и нажмите «**ОК**» для перехода в интерфейс установки значения. Нажимайте ▲/▼ для изменения времени (в секундах). Нажмите «**ESC**» для сохранения. Допустимы значения в интервале от 3 до 15 секунд.

 **Примечание:** Если вам необходимо установить большее значение разблокировки, свяжитесь со своим поставщиком или тех. поддержкой.

Режим проверки: Нажмите **ОК** для отображения интерфейса «**Режим проверки**». Кнопками ▲/▼ выберите значение. Имеется три варианта, отвечающих за различные режимы (по умолчанию – 1).

- 0:** Только администратор сможет открыть замок. Разблокировка рядовым пользователям недоступна.
- 1:** Значение по умолчанию. Пользователи могут открывать замок, если их отпечаток зарегистрирован в системе.
- 2:** Режим двойной проверки. Администратор может открыть замок по отпечатку, но рядовому пользователю нужно пройти проверку двумя разными способами (нужно чтобы эти данные были зарегистрированы на один и тот же ID).

Разблокировка: Нажмите «**ОК**» для входа в меню «**Разблокировка**» и кнопками ▲/▼ выберите «**Да**» или «**Нет**». Если вы выберете «**Да**», после проверки пользователя будет отображаться запрос на разблокировку. Нажмёте «**ОК**» – система разблокирует замок и выключит питание. Ниже показан интерфейс запроса на разблокировку:

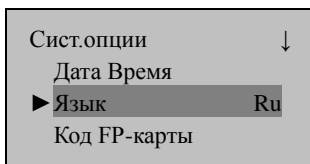


Чтобы снова закрыть замок, включите его и нажмите **«ОК»** за запрос закрытия.


Только карта: Нажмите **«ОК»** для изменения параметра и кнопками **▲/▼** выберите **«Да»** или **«Нет»**. Если вы выберете **«Да»**, то для проверки нужна будет только ID-карта. Если вы выберете **«Нет»**, то для проверки нужно будет предъявлять и карту, и отпечаток.

3.2 Выбор языка

В главном меню выберите **«Настройки»** → **«Сист.опции»** → **«Язык»**:



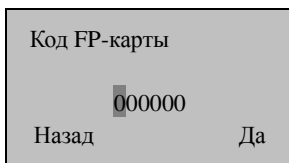
Нажмите **«ОК»** для отображения интерфейса выбора языка и выберите нужный язык с помощью кнопок **▲/▼**. Кнопкой **«ОК»** подтвердите свой выбор и нажмите **«ESC»** для выхода в **«Сист.опции»**. Когда система спросит, желаете ли вы сохранить изменения, нажмите **«ОК»**. Новый язык отобразится после перезагрузки замка.

 **Примечание:** Выбор языка не является базовой функцией. Если вам необходимо воспользоваться ею, свяжитесь со своим поставщиком или технической поддержкой.

3.3 Код для FP-карты


После установки кода для вашей FP-карты, биометрический замок пропишет его в карту Mifare при регистрации или создании вашей FP-карты.

Выберите **«Настройки»** → **«Сист.опции»** → **«Код FP-карты»** из главного меню. На экране отобразится следующая информация:



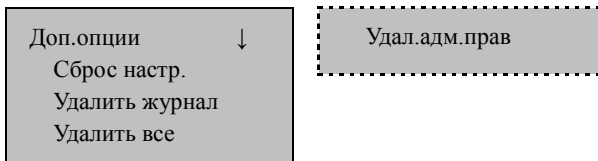
Код FP-карты состоит из 6 цифр. Для ввода кода выберите цифру от 0 до 9, нажимая **↑** или **↓**, и нажмите **«ОК»** для подтверждения. Аналогично – для всех остальных цифр. По окончании ввода нажмите **«ОК»** для сохранения кода и возвращения в меню системных настроек.

3.4 Расширенные настройки

 **Примечание:** С расширенными настройками могут работать только администраторы.

Выберите **«Настройки»** → **«Сист.опции»** → **«Доп.опции»** из главного меню.

На экране отобразится следующая информация:



«Доп.опции» включают в себя:

Сброс настр.: используется для восстановления заводских настроек замка.

Удалить журнал: используется для удаления всех записей журнала из памяти.

Удалить все: используется для удаления всех зарегистрированных отпечатков, кодов и записей.

Удал.адм.прав: используется для разжалования администратора до рядового пользователя. Используйте эту функцию с осторожностью. Следует зарегистрировать как минимум одного нового администратора, прежде чем разжаловать кого-либо.

3.5 Просмотр системной информации


Вы можете просматривать информацию о системе, включающую в себя количество считанных отпечатков, кодов, карт, зарегистрированных пользователей и информацию об устройстве. Выберите **«Информация»** в главном меню и нажмите **«ОК»** для перехода к следующему экрану:

Информация	↓
Просм.журн	
Польз.	5
ОП	1

Журнал	85
Администр.	2
Код	3
Карта	12
Свободно	
Устройство	

Выберите пункт **«Свободно»**, чтобы увидеть количество доступных для регистрации отпечатков, RFID-карт и недействующих записей журнала:

Свободно	
ОП	499
Журнал	29915
Сист.журн.	488

 **Примечание:** Данную информацию можно посмотреть лишь в работающих с RFID-картами замках.

В меню «**Устройство**» можно увидеть следующую информацию (расширенная информация доступна по нажатию «**ОК**»):

Устройство ↓		SN
ОП (x100)	5	Поставщик
Журнал (x10к)	3	Тип
Сист.журн.	4095	Алгоритм
Дата произв.		Прошивка

3.6 Просмотр журнала

Биометрические замки поддерживают просмотр событий разблокировки без компьютера.

Выберите «**Просмотр журн.**» в главном меню:

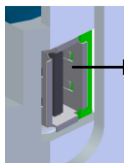
Просмотр журн.	
ПИН	0001
Назад	Да

Нажимая ▲/▼, выберите идентификатор пользователя, журнал событий которого вы хотите просмотреть, и нажмите «**ОК**» для подтверждения:

2--1	
ПИН:	0001
2011-11-30	14: 49
Назад	Да

Первая цифра означает общее количество записей. Вторая – номер текущей записи.

3.7 Работа с USB-устройствами



USB-порт

1) Вставьте USB-накопитель в USB-порт, скрытый за батарейным отсеком.



USB устройство
Назад Да

2) Выберите **«USB устройство»** в главном меню и нажмите **«ОК»**. Вы увидите запрос, показанный на снимке слева.

USB устройство
Скачать журнал
Скачать польз.
Загр-ть польз.

3) Нажмите **«ОК»** и перед вами предстанет следующее меню.

Обн. прошивки

1. Загрузка журнала посещений



Завершено

1) Нажимая **▲/▼**, выберите **«Скачать журнал»**. Подтвердите выбор кнопкой **«ОК»**. Когда загрузка будет завершена, вы увидите такое сообщение.

2) Нажмите **«ESC»** для возврата на стартовый

экран, после чего USB-накопитель можно будет отключить. На USB-накопителе будут созданы два файла: X_attlog.dat (журнал посещений) и X_user (список пользователей). «X» означает номер устройства.



Примечание: Если вместо сообщения об успешной загрузке данных будет выдано сообщение **«Нет устройства»**, убедитесь, что вы вставили накопитель правильно.

2. Загрузка данных пользователей с устройства

Загрузка данных пользователей схожа с загрузкой журнала посещений. Выберите в меню **«USB устройство»** пункт **«Скачать польз.»**. Будут созданы два файла – user.dat (информация о пользователях) и template.dat (шаблоны отпечатков).

3. Выгрузка данных пользователей на устройство

В меню **«USB устройство»** выберите **«Загр-ть польз.»** и нажмите **«ОК»**. Файлы user.dat (информация о пользователях) и template.dat (шаблоны отпечатков), сохранённые ранее на USB-накопителе будут выгружены в память биометрического замка.



Примечание: Если вы будете выгружать пользователей с ПИН, уже зарегистрированными в системе, данные в замке будут заменены новыми (с USB-накопителя).

4. Обновление прошивки

Выберите **«Обн. прошивки»** для обновления микропрограммы биометрического замка с сохранённого на USB-накопителе файла.



Примечание: Если у вас возникла необходимость в обновлении прошивки, свяжитесь с тех.поддержкой. Обычно обновление прошивки не требуется.

Примечание: Не проводите экспериментов с USB-накопителем (например, не переподключайте его слишком часто в обычном режиме работы и, тем более, во время выгрузки-загрузки данных), поскольку это может вызвать нестабильную работу системы. Во время работы с USB-устройством рекомендуется держать дверь открытой.

4. Другие функции

4.1 Индикация

Успешное действие пользователя: Однократный звуковой сигнал и зелёная подсветка в течение трёх секунд.

Неверное действие пользователя: Двойной звуковой сигнал и красная подсветка в течение трёх секунд.

Тревога: Пятикратный повторяющийся звуковой сигнал.

4.2 Предотвращение утраты администраторских полномочий

Чтобы попасть в меню после утраты администраторских полномочий, выполните следующие действия: Нажмите и удерживайте кнопку **Menu** в течение трёх секунд для входа в режим проверки администратора. Передвиньте переключатель на задней стороне замка влево или вправо. Теперь у вас есть права доступа к замку с привилегиями администратора.

4.3 Защита от разряда батареек

Когда индикатор заряда батарей покажет одно деление, система попросит заменить батарейки, а значок будет моргать. Если вы будете удерживать кнопку **Menu**, система сообщит о невозможности доступа к меню. Более того, меню будет недоступно и при использовании внешнего питания во избежание потери данных в результате внезапного отключения. Если уровень заряда упадёт до нуля, система будет отключена автоматически.

4.4 Автоматический выход из программы и отключение системы

Биометрический замок автоматически отключается:

- в результате успешного распознавания и разблокировки.
- когда вы устанавливаете режим разблокировки.
- по достижении заданного количества ошибочных попыток разблокировки. После перезапуска замок выдаст тревогу в течение 30 секунд и выключится автоматически.
- при снижении напряжения ниже определённого значения.
- при отсутствии активности в течение 10 секунд после включения.

4.5 Использование внешнего питания

Биометрический замок поддерживает внешнее питание для кратковременного распознавания отпечатков или сравнения кодов и последующей разблокировки. Но при использовании внешнего питания во избежание потери данных недоступны такие функции как регистрация, удаление и настройка.

На рисунке ниже показан способ подключения батарейки 9В – к двум контактам на нижней части замка. Полярность значения не имеет.

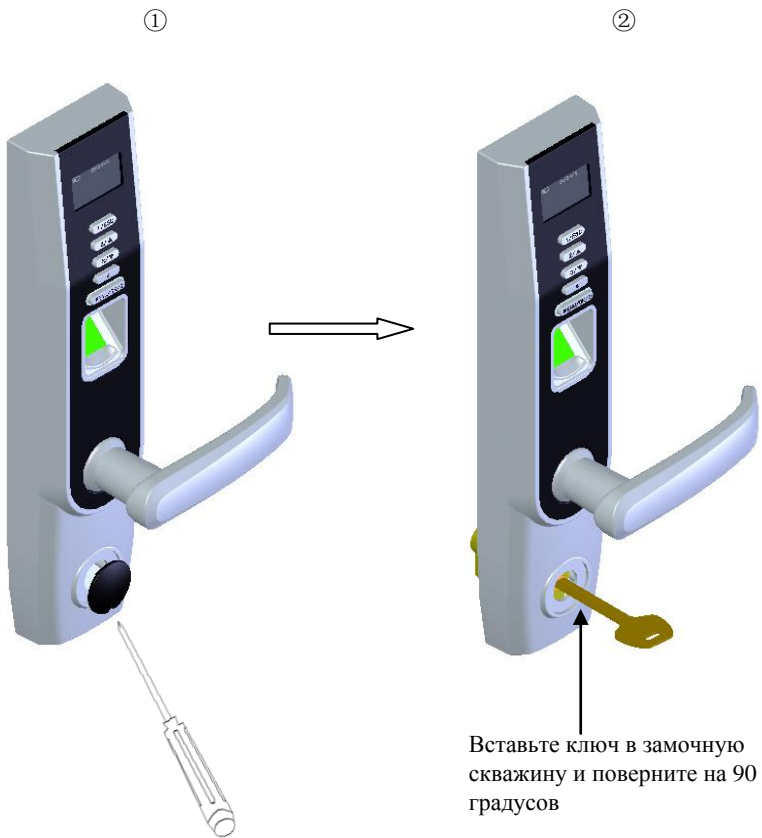


Если при использовании внешнего питания вы выключите замок, не закрывая дверь, блокировочный цилиндр не вернётся автоматически в исходное положение. Т.е. замок останется в состоянии разблокировки. Для решения проблемы замените батарейки и откройте замок однократно.

4.6 Открытие замка механическим ключом

Если электронная часть замка не функционирует, вы можете открыть его механическим ключом.

- (1) Удалите заглушку в нижней части замка с помощью какого-нибудь острого предмета, например, отвёртки.
- (2) Вставьте ключ в замочную скважину и поверните на 90 градусов для разблокировки.



Приложение

Спецификации

- Сенсор: оптический, без дополнительного слоя
- Ёмкость: 500 образов отпечатков; 100 кодов; 500 пользователей.
- Режимы проверки: сравнение отпечатков, кодов, RFID-карт и Mifare.
- Количество записей: 30000
- Разрешение сенсора: 500 DPI
- Скорость распознавания: ≤ 2 сек.
- Вероятность ошибок ложного доступа: $\leq 0.0001\%$
- Вероятность ошибок ложного недопуска: $\leq 1\%$
- Питание: четыре батарейки AA, рабочее напряжение: 4.2В–6В.
- Количество срабатываний: ≥ 4000 (от четырёх щелочных батареек)
- Рабочая температура: 0–45 °C
- Рабочая влажность: 10%–80%

Этот документ может быть изменён без предварительного уведомления
Перевод выполнен ООО "Стратегия безопасности" www.bio5.ru