

Терминал BioSmart PV-WTC

Руководство по эксплуатации



Оглавление

1. ВВЕДЕНИЕ	4
2. МЕРЫ ПРЕДОСТОРОЖНОСТИ	4
3. ВНЕШНИЙ ВИД И ЭЛЕМЕНТЫ УПРАВЛЕНИЯ ТЕРМИНАЛА.....	5
3.1. Описание лицевой панели терминала	5
3.2. Управление терминалом посредством клавиатуры	6
4. РЕЖИМ ОЖИДАНИЯ И ДОСТУП К ОСНОВНОМУ МЕНЮ	7
5. РАЗДЕЛ «МЕНЮ»	8
5.1 Настройки	8
5.1.1. Система.....	9
5.1.2. Сеть.....	18
5.1.3. Экран	18
5.1.4. Дата и время	19
5.1.5. Интеграция	20
5.2 Сотрудники	20
5.2.1. Фильтр поиска сотрудников	20
5.2.2. Редактирование данных сотрудника.....	21
5.2.3. Добавление нового сотрудника.....	26
6. РАЗДЕЛ «ИНФО»	27
7. РАЗДЕЛ «ОШИБКИ»	27
8. РАБОТА ТЕРМИНАЛА С СЕЙФОВЫМИ ЯЧЕЙКАМИ	28
9. WEB-ИНТЕРФЕЙС ТЕРМИНАЛА	29
9.1. Доступ к веб-интерфейсу	29
9.2. Главное меню	30
9.2.1. Overview	30
9.2.2. Settings.....	30
9.3. Work model	31
9.3.1. Создание и редактирование режимов работы	33
9.3.2. Создание простого сценария работы.....	41

9.3.3. Создание более сложного сценария работы.....	44
9.3.4. Создание сценария работы с использованием реле/кнопки.....	50
10. НЕИСПРАВНОСТИ ТЕРМИНАЛА И МЕТОДЫ ИХ УСТРАНЕНИЯ.....	57
11. ОБСЛУЖИВАНИЕ ТЕРМИНАЛА.....	59
11.1 Проверка физического состояния терминала.....	59
11.2 Проверка наличия ошибок в работе терминала.....	60
11.3 Проверка наличия ошибок в работе с сейфовыми ячейками.....	60
12. ХРАНЕНИЕ	61
13. ТРАНСПОРТИРОВАНИЕ.....	61
14. УТИЛИЗАЦИЯ	61

Уважаемые покупатели!

Благодарим Вас за приобретение нашей продукции. При соблюдении правил монтажа и эксплуатации данное устройство прослужит долгие годы.

1. Введение

Настоящий документ описывает работу терминала **BioSmart PV-WTC**.

Руководство по монтажу терминала BioSmart PV-WTC и программное обеспечение находятся по адресу www.bio-smart.ru в разделе «Поддержка».

Используемые сокращения:

ЖК – жидкокристаллический;

ПО – программное обеспечение;

СКУД – система контроля и управления доступом;



- так выделена важная информация, на которую следует обратить внимание.

2. Меры предосторожности

- Используйте терминал только по назначению, как указано в руководстве по эксплуатации;
- Установка и обслуживание терминала осуществляется только квалифицированным и обученным персоналом;
- Не используйте для очистки или обеззараживания средства за исключением тех, что рекомендуются производителем;
- Терминал должен располагаться на ровной поверхности и быть сохранен от ударов;
- Подсоединяйте только к источнику питания с напряжением, соответствующим напряжению, указанному на маркировке;
- Источник питания должен соответствовать классу II по электробезопасности;
- Регулярно проверяйте оболочку соединительных кабелей. В случае повреждения оболочки немедленно замените кабель.

3. Внешний вид и элементы управления терминала

Терминал **BioSmart PV-WTC** предназначен для работы в составе системы контроля и управления доступом **BioSmart**. Терминал позволяет организовать учет рабочего времени посредством идентификации пользователей по рисунку вен ладони и бесконтактным RFID картам, а также осуществлять контроль и управление доступом.

3.1. Описание лицевой панели терминала

Внешний вид терминала представлен на рисунке 1.



Рисунок 1. Внешний вид терминала BioSmart PV-WTC

1. Поле для считывания пластиковых карт
2. ЖК экран
3. Клавиатура
4. Сканер вен ладони

3.2. Управление терминалом посредством клавиатуры

Навигация по экранному меню осуществляется с помощью кнопок клавиатуры (рисунок 2):



Рисунок 2. Клавиатура

2 – переход вверх по списку;

6 – переход вправо или переход от списка к функциональным кнопкам. В меню «Пользователи» используется для постраничной навигации;

4 – переход влево или переход от функциональных кнопок к списку, в меню «Пользователи» используется для постраничной навигации;

5 – переход для подтверждения в меню «Сотрудники»;

8 – переход вниз по списку;

 – выполняет функции выбора и подтверждения;

 – выполняет функции возврата в предыдущий раздел меню или удаления последней введенной цифры.

Все числовые настройки также вводятся с клавиатуры.

4. Режим ожидания и доступ к основному меню

В режиме ожидания экран терминала имеет вид, соответствующий установленному на нем режиму работы (подробно о режимах работы см. п.5.1.1). Один из вариантов вида приведен на рисунке 3. На экране, как правило, выводится тип действия, которое ожидается терминалом («Нажмите кнопку», «Приложите ладонь» и т.д.).

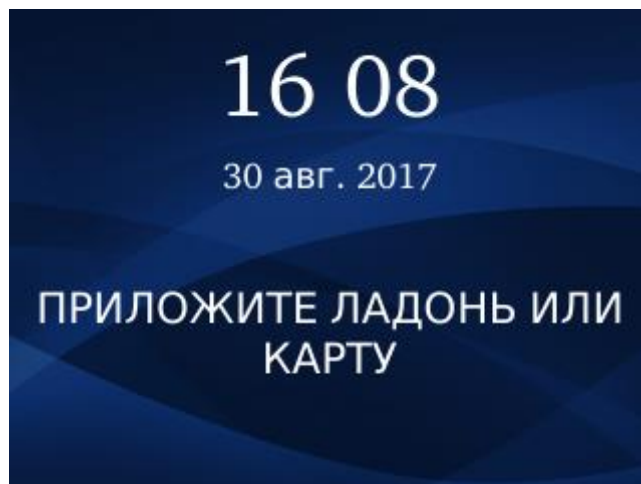


Рисунок 3. Экран терминала в режиме ожидания

Основное меню терминала позволяет пользователю получить доступ к настройкам терминала, данным о сотрудниках, информацию об ошибках.

- Для входа в основное меню нажмите клавишу «Ввод» ();
- Введите пароль администратора в появившемся поле;

После первого входа рекомендуется установить новый пароль, в целях исключения в дальнейшем несанкционированного доступа к настройкам терминала. Процедура смены пароля описана в пункте 5.1.1



Заводские настройки пароля администратора – пустой пароль.

Вид основного меню представлен на рисунке 4



Рисунок 4. Экран терминала в режиме доступа к основному меню

5. Раздел «Меню»

Данный раздел позволяет получить доступ к системному меню. Он содержит следующие пункты (рисунок 5):

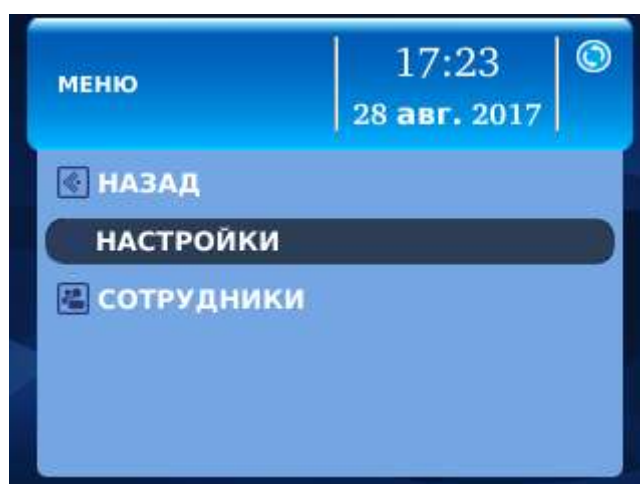


Рисунок 5. Выбор «Настройки»

5.1 Настройки

Позволяет получить доступ к системным и сетевым настройкам терминала. Содержит следующие подпункты:

5.1.1. Система



Рисунок 6. Система

Позволяет произвести конфигурацию системных параметров терминала

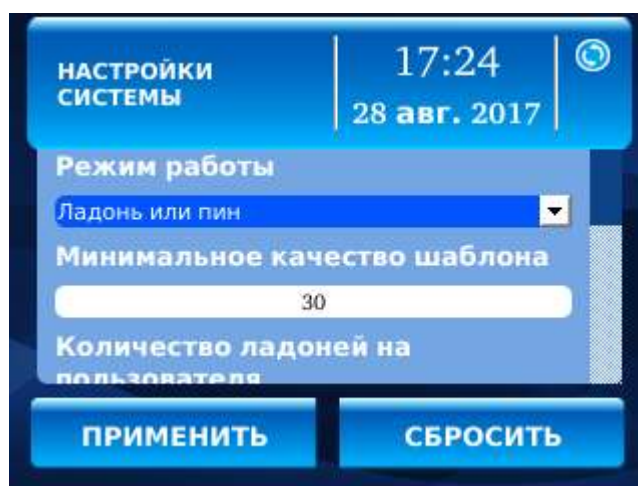


Рисунок 7. Вид меню «Настройки системы»

- **Режим работы** (рисунок 7) – параметр, определяющий, какие алгоритмы идентификации будут использоваться терминалом:

- Ладонь или карта (рисунок 8)



Рисунок 8. Экран терминала в режиме «Ладонь или карта»

В данном режиме терминал ожидает поднесенной карты или приложенной ладони. При предъявлении любого идентификатора будет формироваться событие «Идентификация успешна» и фиксироваться в журнале событий.

- Карта + ладонь (рисунок 9)

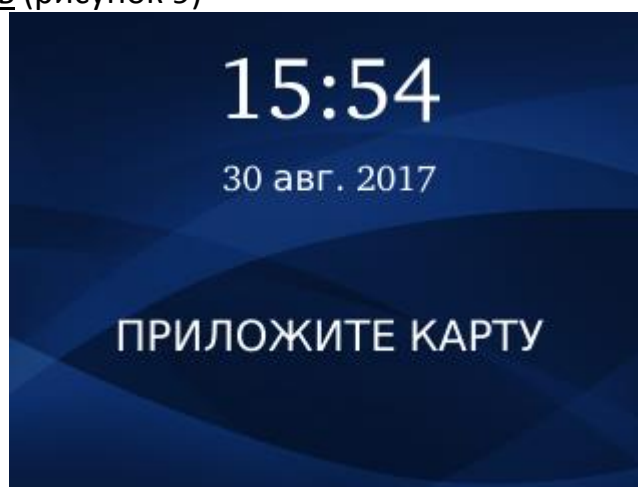


Рисунок 9. Экран терминала в режиме «Карта+ладонь»

В данном режиме терминал ожидает приложенной карты. При предъявлении карты и ее успешной идентификации требуется дополнительная идентификация по ладони. При успешной идентификации будет формироваться событие «Идентификация успешна» и фиксироваться в журнале событий.

- Ладонь или пин (рисунок 10)



Рисунок 10. Экран терминала в режиме «Ладонь или пин»

В данном режиме терминал ожидает приложенной ладони или ввода пин-кода. При предъявлении любого идентификатора будет формироваться событие «Идентификация успешна» и фиксироваться в журнале событий.

- Пин + ладонь (рисунок 11)



Рисунок 11. Экран терминала в режиме «Пин+ладонь»

В данном режиме терминал ожидает ввода пин-кода. При вводе кода и его успешной идентификации требуется дополнительная идентификация по ладони. При успешной идентификации будет формироваться событие «Идентификация успешна» и фиксироваться в журнале событий.

- Кнопка входа/выхода + код группы + ладонь/карта (рисунок 12)



Рисунок 12. Экран терминала в режиме «Кнопка входа/выхода + код группы + ладонь/карта»

В данном режиме терминал ожидает нажатия соответствующей клавиши на клавиатуре терминала. В случае нажатия клавиш 1-3 требуется ввод кода группы, затем идентификация по ладони или карте. В случае нажатия клавиш 4-6 ввод кода группы не требуется (он берется из настроек терминала в BioSmart Studio v5), затем также требуется идентификация по ладони или карте. При успешной идентификации будет формироваться событие «Идентификация успешна» и фиксироваться в журнале событий.

- Кнопка входа/выхода + ладонь или карта (рисунок 13)

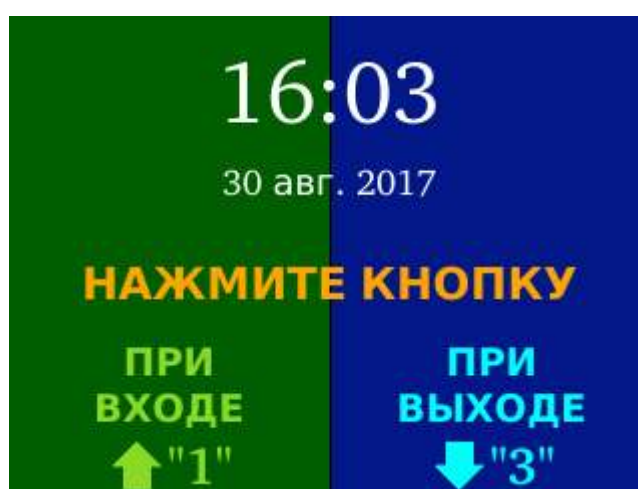


Рисунок 13. Экран терминала в режиме «Кнопка входа/выхода + ладонь или карта»

В данном режиме терминал ожидает нажатия соответствующей клавиши на клавиатуре терминала. После нажатия требуется идентификация по ладони или карте. При успешной идентификации будет формироваться событие «Идентификация на входе успешна» или «Идентификация на выходе успешна», и фиксироваться в журнале событий.

- Ладонь или карта или кнопка (рисунок 14)

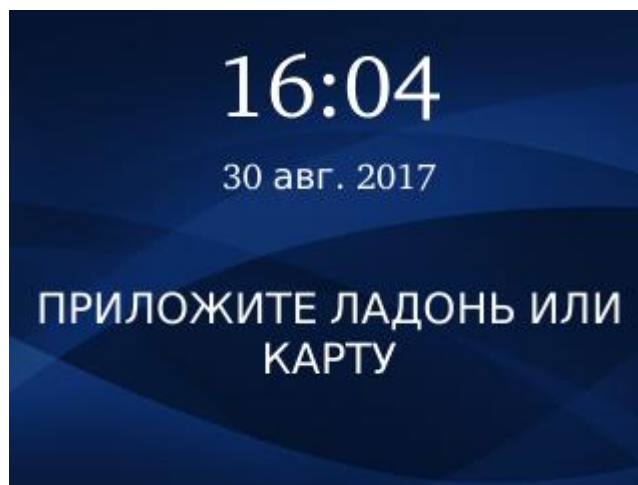


Рисунок 14. Экран терминала в режиме «Ладонь или карта или кнопка»

В данном режиме терминал ожидает приложенной ладони или карты, либо нажатой кнопки выхода, подключенной к входу «In 0». В случае успешной идентификации ладони или карты, либо нажатия кнопки будет формироваться событие «Идентификация успешна» либо «Нажата кнопка» и фиксироваться в журнале событий, а также будет разомкнуто бортовое реле.

- Кнопка входа/выхода + обед + ладонь или карта (рисунок 15)

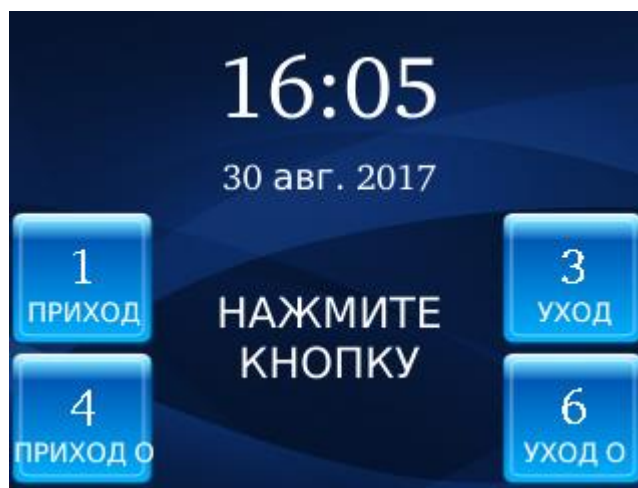


Рисунок 15. Экран терминала в режиме «Кнопка входа/выхода + обед + ладонь или карта»

В данном режиме терминал ожидает нажатия соответствующей клавиши на клавиатуре терминала. Доступны варианты «Приход»/«Уход» и «Приход обед»/«Уход обед». После нажатия требуется идентификация по ладони или карте. При успешной идентификации будут формироваться события «Идентификация на входе/выходе успешна» и «Идентификация ухода на обед/возвращения с обеда успешна» и фиксироваться в журнале событий.

- Карта + ладонь или кнопка (рисунок 16)

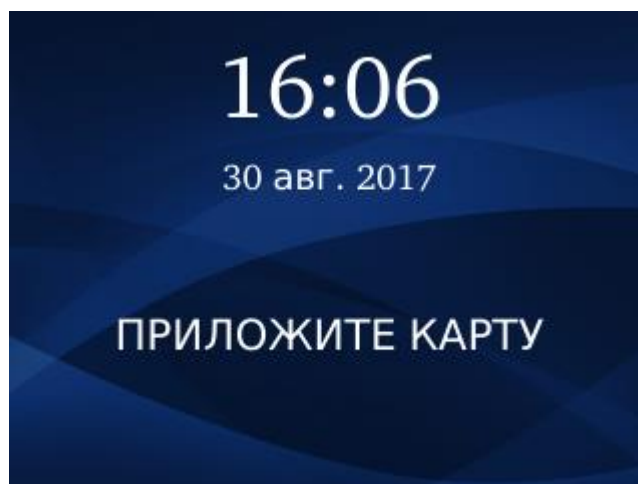


Рисунок 16. Экран терминала в режиме «Карта + ладонь или кнопка»

В данном режиме терминал ожидает приложенной карты, либо нажатой кнопки выхода. В случае успешной идентификации по карте, требуется идентификация по ладони. При успешной идентификации ладони и карты будет формироваться событие «Идентификация успешна» и фиксироваться в журнале

событий.

После этого, размыкается выходное реле. Также, реле размыкается при нажатии кнопки.

- Отметка на вход (рисунок 17)

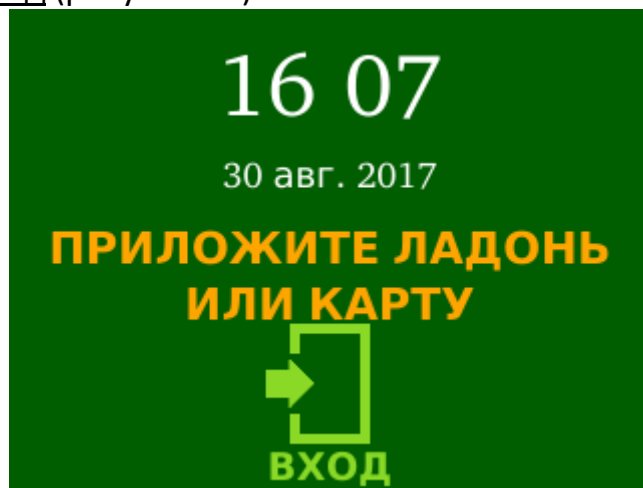


Рисунок 17. Экран терминала в режиме «Отметка на вход»

В данном режиме терминал ожидает приложенной ладони или карты. При успешной идентификации будет формироваться событие «Идентификация на входе успешна» и фиксироваться в журнале событий.

- Отметка на выход (рисунок 18)

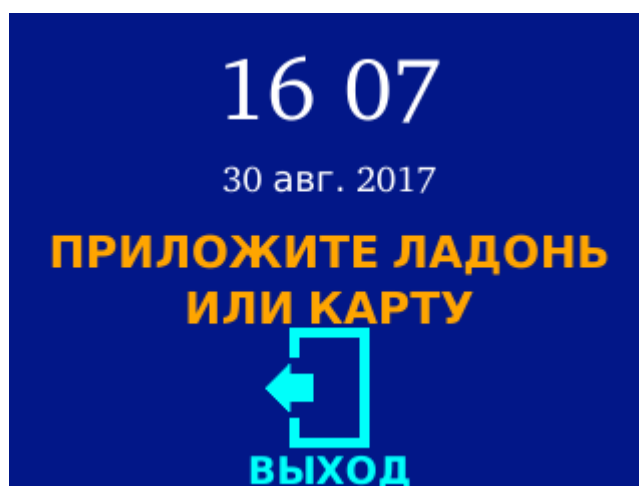


Рисунок 18. Экран терминала в режиме «Отметка на выход»

В данном режиме терминал ожидает приложенной ладони или карты. При успешной идентификации будет формироваться событие «Идентификация на выходе успешна» и фиксироваться в журнале событий.

Пользователь может создавать собственные режимы работы через web-интерфейс терминала (см. п.9.3.1).

- **Минимальное качество шаблона** (рисунок 19) – численное значение, определяющее минимальный уровень качества при регистрации скана ладони. Не рекомендуется изменять данное значение.

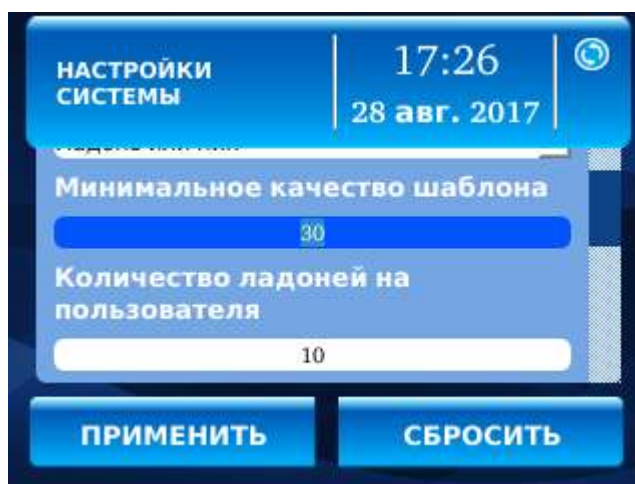


Рисунок 19. Вид меню «Настройки системы»

- **Количество ладоней на пользователя** (рисунок 19) - задает количество шаблонов рисунка вен ладони для каждого пользователя. Можно задать от 0 до 10 шаблонов. На одну ладонь создается два шаблона. (при сканировании из BioSmart Studio v5 – один шаблон).

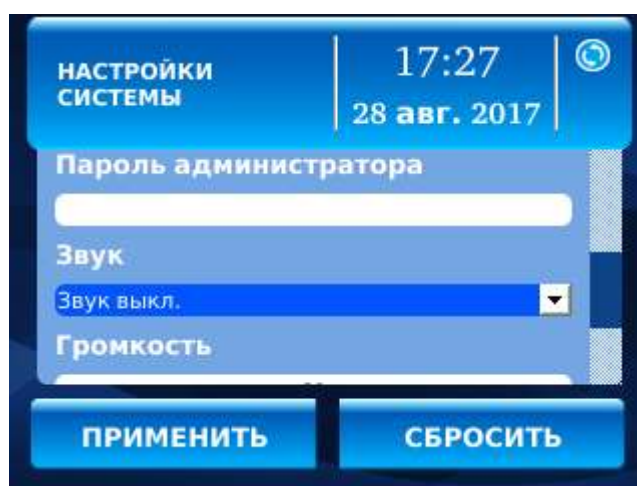


Рисунок 20. Вид меню «Настройки системы»

- **Пароль администратора** (рисунок 20) - задает цифровой пароль администратора для входа в меню настроек терминала с клавиатуры. Максимальное количество цифр в пароле - 9. По умолчанию пароль отсутствует. Если пароль неизвестен, его можно изменить или убрать с помощью BioSmart Studio v5.

Для того чтобы установить пустой пароль, введите в поле значение «0».

- **Звук** (рисунок 20) - позволяет выбрать и настроить режим работы звукового источника терминала (бипер/спикер/отключить звук).

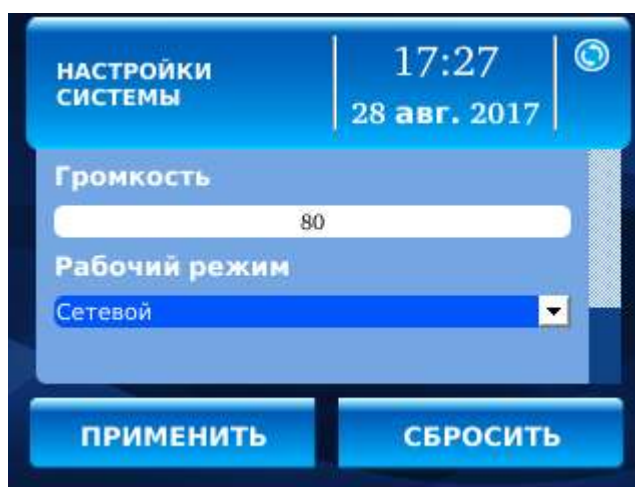


Рисунок 21. Вид меню «Настройки системы»

- **Громкость** (рисунок 21) - позволяет настроить громкость звукового источника терминала.
- **Рабочий режим** (рисунок 21) - позволяет выбрать режим работы терминала:
 - Сетевой – режим работы, при котором доступ на терминал для пользователей назначается из BioSmart Studio v5. Сканы ладоней при этом хранятся в памяти терминала.
 - Локальный – режим работы, при котором доступ на терминал назначается непосредственно с терминала.



Внимание! В режиме «Локальный» из BioSmart Studio v5 можно изменить только рабочий режим. Другие настройки не меняются, журналы событий не передаются

- Серверный – режим работы, при котором сканы ладоней хранятся

на внешнем сервере биометрической идентификации, а не в локальной памяти. В этом режиме сравнение биометрических данных производится на внешнем сервере, что позволяет расширить количество сканов в базе данных и увеличить скорость идентификации.

5.1.2. Сеть



Рисунок 22. Меню сетевых настроек

В меню отображаются сетевые параметры терминала с возможностью их настройки.

5.1.3. Экран

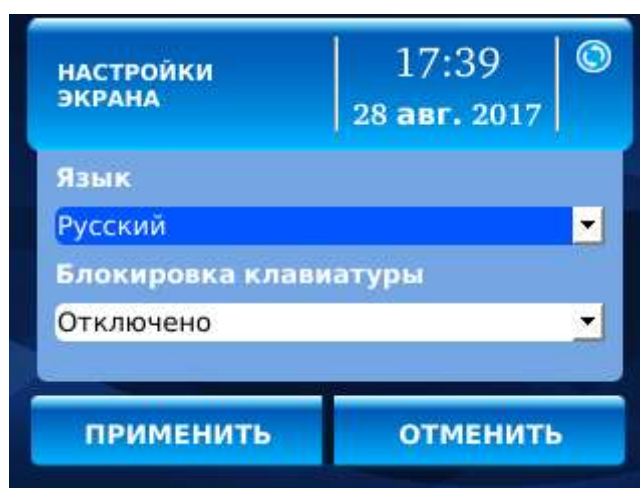


Рисунок 23. Меню настроек экрана

В меню регулируются следующие параметры:

- **Язык** - настройка устанавливает язык интерфейса экрана (русский или английский).
- **Блокировка клавиатуры** - настройка позволяет заблокировать или разблокировать клавиатуру терминала. Блокировка позволяет предотвратить несанкционированный вход в меню терминала и другие действия при случайном нажатии клавиш клавиатуры. При заблокированной клавиатуре последовательное нажатие клавиш «7» и «9» временно разблокирует клавиатуру, а на дисплее появятся кнопки «Меню» и «Инфо».

5.1.4. Дата и время

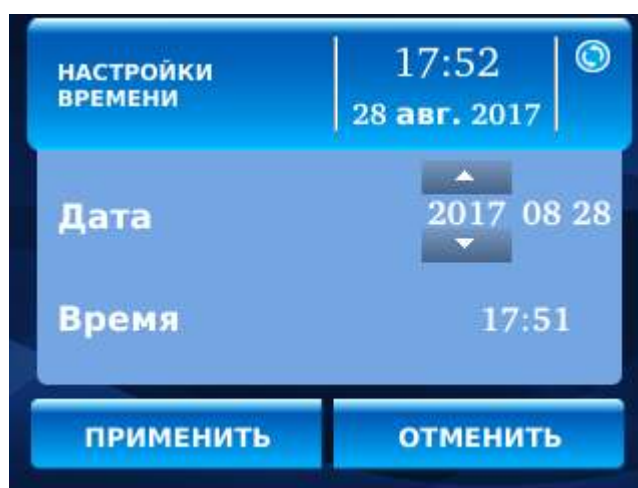


Рисунок 24. Меню настройки даты и времени

В меню устанавливаются текущие дата и время. В сетевом режиме время синхронизируется со временем сервера ПО BioSmart Studio v5.

5.1.5. Интеграция

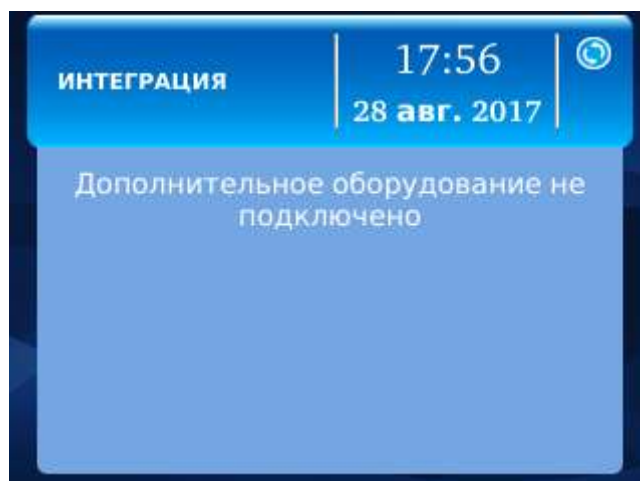


Рисунок 25. Меню настроек интеграции

В меню отображается информация о подключенном стороннем оборудовании.

5.2 Сотрудники

5.2.1. Фильтр поиска сотрудников

Меню позволяет добавлять/удалять рисунки вен ладоней/карт для сотрудников в сетевом режиме работы терминала, а также добавлять/удалять сотрудников, добавлять/удалять рисунки вен ладоней/карт для сотрудников в локальном режиме работы терминала.

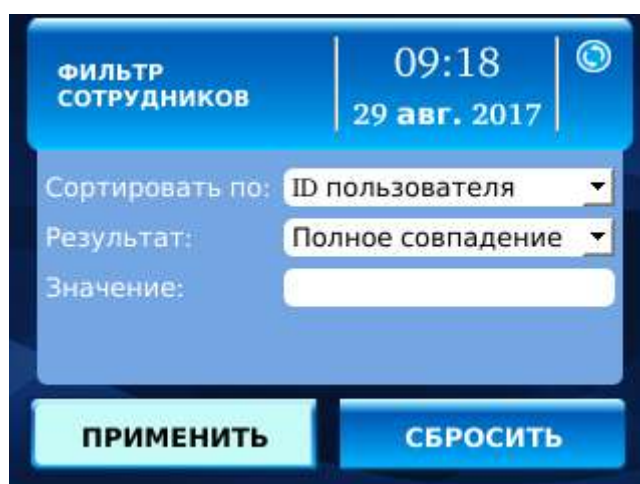


Рисунок 26. Меню «Сотрудники».

В сетевом режиме работы доступ сотрудникам на терминал должен быть предварительно назначен из ПО BioSmart Studio v5. Подробнее процедура

назначения доступа описана в [Руководстве пользователя BioSmart Studio v5](#).

В меню «Сотрудники» (рисунок 26) присутствуют три фильтра, позволяющие производить поиск по сотрудникам.

- **Сортировать по:** - данное поле позволяет выбрать, по какому критерию будет производиться сортировка списка сотрудников. Доступны варианты - фамилия, имя, код группы, ID пользователя.
- **Результат:** - устанавливает, требуется ли полное совпадение введенного значения (фамилия, имя, код группы, ID пользователя) тому, что хранится в базе терминала или достаточно вхождения введенного значения в то, что хранится в базе.
- **Значение:** - точные имя/фамилия сотрудника.



Для быстрого поиска в больших базах рекомендуется устанавливать фильтры «Сортировать по: ФИО, Результат: вхождение»

После применения фильтров и нажатия клавиши «Применить» на экране отобразится список сотрудников (рисунок 27).

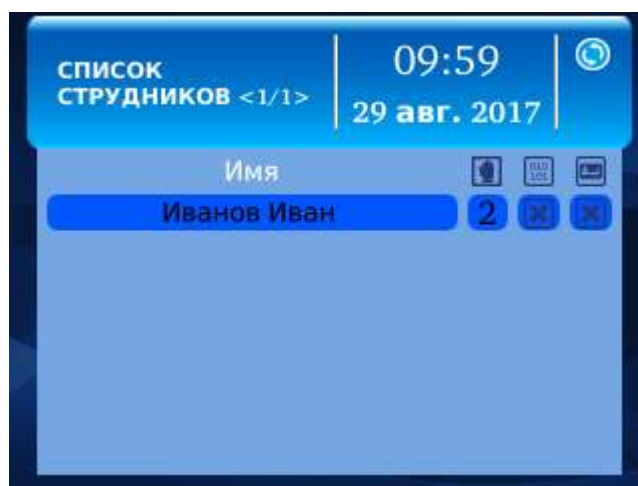


Рисунок 27. Список сотрудников

Иконки справа указывают на наличие в базе терминала данных о шаблонах вен ладони, кода карты, пин-кода сотрудника.

5.2.2. Редактирование данных сотрудника

Если терминал находится в локальном режиме (см. п.5.1.1), то нажатие клавиши «5» откроет меню редактирования данных сотрудника (рисунок 28).



Рисунок 28. Меню редактирования данных сотрудников

Доступны следующие пункты:

Фильтр - возврат к настройкам фильтров поиска;

Изменить – изменение данных выбранного сотрудника (рисунок 29)

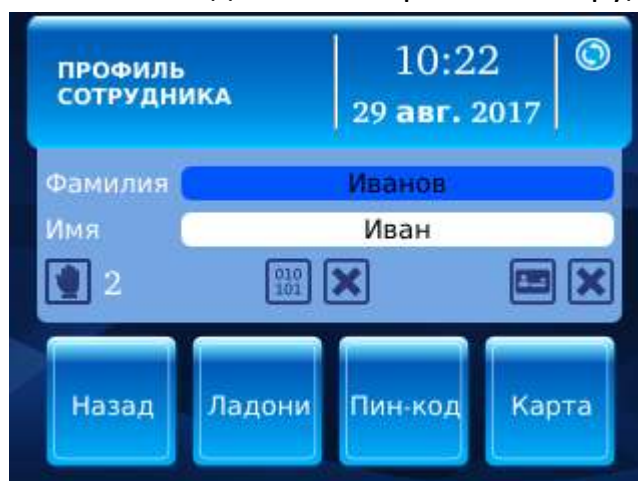


Рисунок 29. Изменение данных о сотруднике

В данном разделе можно редактировать следующие данные:

- **Фамилию, имя сотрудника.**

При выборе соответствующего поля на экране отобразится клавиатура для ввода имени/фамилии сотрудника (рисунок 30).

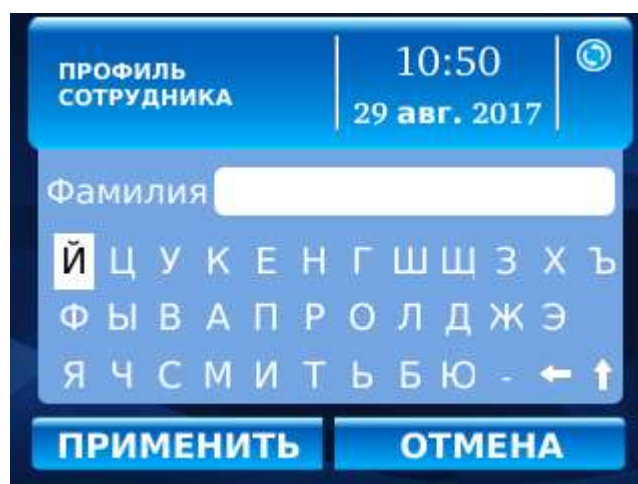


Рисунок 30. Ввод фамилии сотрудника

- **Шаблоны рисунков вен ладони.**

Для добавления (обновления) шаблона выберите «**Ладони**» (рисунок 31).



Рисунок 31. Редактирование шаблонов ладони

Для добавления новых шаблонов нажмите клавишу «**Добавить ладони**». Прозвучат короткие звуковые сигналы, на дисплее появится надпись: «**Приложите ладонь**».



Внимание! Для корректной регистрации и распознавания сканов ладони придерживайтесь правил, указанных ниже. Несоблюдение данных правил может привести к ошибкам и проблемам со сканированием

- Ладонь должна быть раскрыта и находиться в вертикальном состоянии;
- Пальцы должны быть распрямлены естественным образом, без

напряжения и должны находиться на направляющих для пальцев;

- Запястье должно находиться на направляющей для запястья.
- Середина ладони должна находиться точно над сканером.

Правильное положение ладони при сканировании указано на рисунке 32



Рисунок 32. Расположение ладони на считывателе

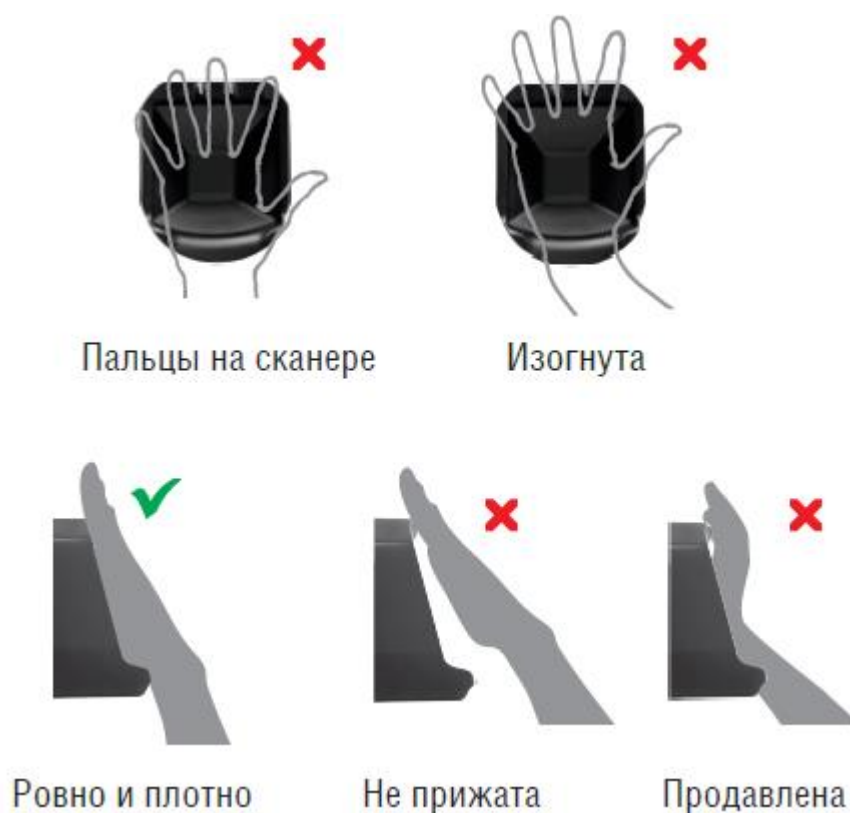


Рисунок 33. Расположение ладони на считывателе

Если ладонь располагается правильно, то на дисплее появится надпись «**Не двигайте ладонь**», а затем, через несколько секунд «**Уберите ладонь**». После этого терминал попросит ещё раз приложить ладонь для завершения процесса регистрации. Если ладонь расположена неправильно, то на дисплее появится надпись «**Неправильное расположение ладони**» и последующая ошибка при регистрации ладони.

При успешной регистрации отпечатка прозвучит длинный звуковой сигнал и появится надпись «**Регистрация успешна**» (рисунок 34).



Рисунок 34. Окончание процесса добавления шаблона

Для удаления шаблонов выберите пункт «**Удалить ладони**».

- Код карты

Для добавления (обновления) кода карты выберите «обновить карту» (рисунок 35). Прозвучат короткие звуковые сигналы и на дисплее появится надпись: «**Приложите карту**».



Рисунок 35. Процесс регистрации кода карты

Приложите карту к терминалу. При успешной регистрации кода карты прозвучит длинный звуковой сигнал и появится надпись: «**Код карты изменен**» (рисунок 36).



Рисунок 36. Окончание процесса регистрации кода карты

Для удаления кода карты выберите «Удалить карту».

- Пин-код

Для добавления (обновления) пин-кода выберите «**Обновить пин-код**» (рисунок 37).



Рисунок 37. Редактирование пин-кода

Введите новый пин-код. При успешной регистрации пин-кода прозвучит длинный звуковой сигнал и появится надпись: «**Пин-код изменен**».

5.2.3. Добавление нового сотрудника

Для добавления сотрудника в локальном режиме работы нажмите клавишу

«5» на клавиатуре терминала в списке сотрудников (рисунок 27). В открывшемся выберите «**Добавить**». При этом созданному сотруднику будут определены имя и фамилия по умолчанию (текущие день, месяц, год, время).

Нажмите клавишу «5» клавиатуры терминала. Выберите вновь добавленного сотрудника в списке и отредактируйте его свойства аналогично пункту 5.2.2.

Для удаления сотрудника выберите его в списке, нажмите клавишу «5» на клавиатуре и нажмите «**Удалить**».

6. Раздел «Инфо»

В данном разделе представлена основная информация о терминале (рисунок 38). IP хоста – это IP адрес сервера BioSmart Studio v5.

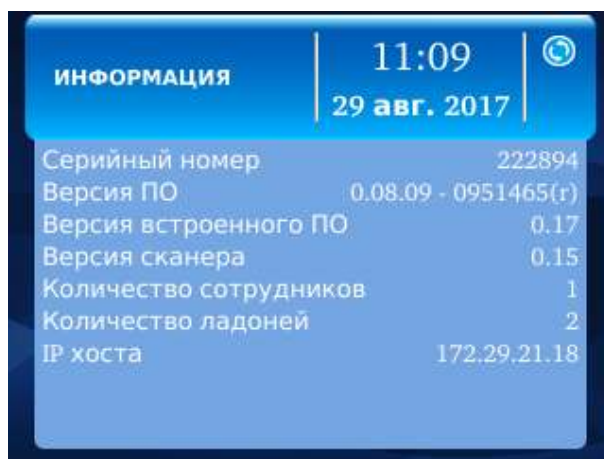


Рисунок 38. Раздел «Инфо»

7. Раздел «Ошибки»

В данном разделе выводится информация об ошибках в работе терминала (рисунок 39).

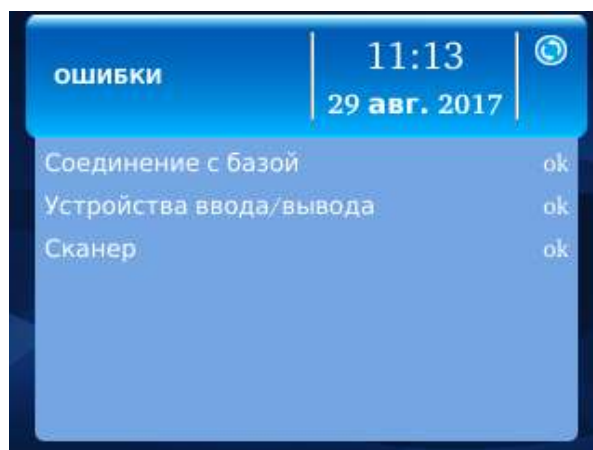


Рисунок 39. Раздел «Ошибки»

8. Работа терминала с сейфовыми ячейками ПРОМЕТ



Внимание! Не все модели терминала поддерживают работу с сейфовыми ячейками! Уточните возможность подключения к депозитарию в службе технической поддержки

Режим работы терминала с сейфовыми ячейками настраивается из ПО BioSmart Studio v5.

При работе терминала в данном режиме, стандартный фон экрана имеет вид, представленный на рисунке 40.

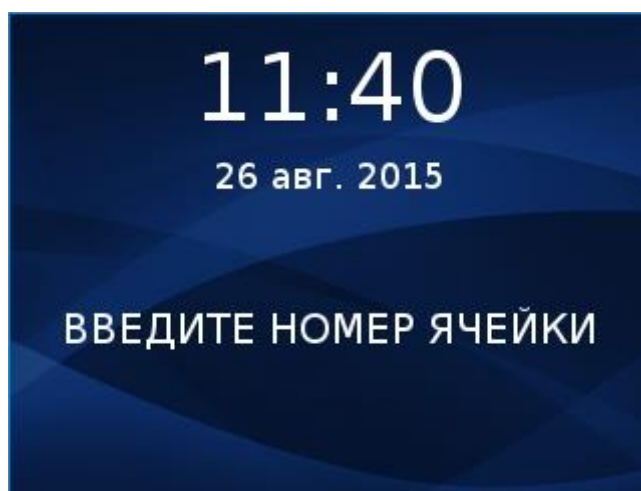


Рисунок 40. Стандартный фон экрана в режиме работы с сейфовыми ячейками

Для корректной работы в данном режиме, наберите на клавиатуре номер назначенной ячейки. Если заданный номер существует, то на экране появится надпись, соответствующая типу идентификации назначенному данной ячейке. При отсутствии такой ячейки, появится соответствующая ошибка (рисунок 41)

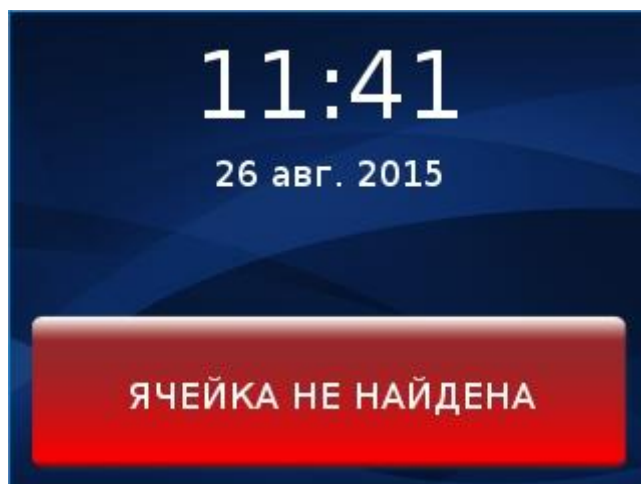


Рисунок 41. Ячейка не найдена

При удачном нахождении номера ячейки, предъявите соответствующий идентификатор. При успешной идентификации появится соответствующая надпись (рисунок 42).

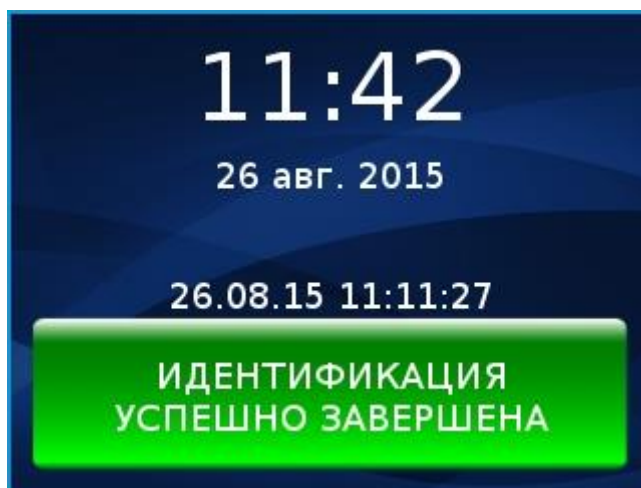


Рисунок 42. Успешная идентификация

После этого должна открыться назначенная ячейка. На экране терминала появится надпись «**Ячейка открыта**».

При неудачном открытии ячейки, на экране появится надпись «**Ячейка не была открыта**».

9. WEB-интерфейс терминала

9.1. Доступ к веб-интерфейсу

Для конфигурирования терминала посредством веб-интерфейса потребуется компьютер с веб-браузером. Убедитесь, что между компьютером и терминалом настроена маршрутизация, открыт TCP порт 8082. Сетевые настройки терминала, заданные по умолчанию, приведены в следующей таблице:

IP-адрес	172.25.110.71
Имя пользователя	root
Пароль	bioroot

Для получения доступа к веб-интерфейсу устройства:

1. Откройте на компьютере веб-браузер (Chrome, Firefox, Internet Explorer)
2. В строке браузера введите IP-адрес устройства в виде: **IP_address:8082**
3. Введите логин и пароль



Рисунок 43. Экран ввода логина и пароля

9.2. Главное меню

Главное меню веб-интерфейса состоит из трех разделов (рисунок 44):

Overview — общая информация

Settings — настройки

Work model — описания возможных режимов работы

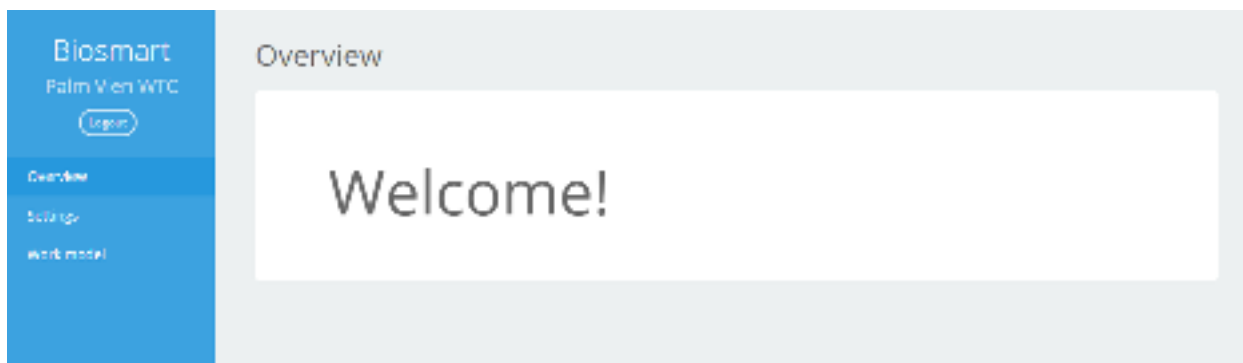


Рисунок 44. Главное меню веб-интерфейса

9.2.1. Overview

В этом разделе будет представлена информация об устройстве.

9.2.2. Settings

В этом разделе можно просматривать, и изменять настройки устройства.



Рисунок 45. Раздел Settings

Доступные настройки:

System – общие настройки устройства

- **Work Model** - режим работы устройства. Можно выбрать предварительно настроенный режим или создать свой. После выбора режима, нажмите кнопку «Save», чтобы изменения вступили в силу. Предварительно настроенные режимы описаны в п.5.1.1

Пользователь может добавлять собственные режимы работы (см.п.9.3.1).

Palm Vein Scanner – настройки сканера вен ладони.

- **Anti-Fake** – Включение проверки на фальшивую ладонь (лист бумаги и т.д.). Рекомендуется значение **Enable anti fake check white paper**.
- **Auto FAR** – опция включает, либо отключает алгоритм автоматического подбора порога сравнения шаблонов. Позволяет оптимизировать качество идентификации.



Внимание! Auto FAR не работает на базах, содержащих более 200 шаблонов.

- **Minimal quality** – устанавливает минимальный уровень качества для вносимого скана ладони.

Для сохранения изменений нажмите «**Save**»; для отмены – «**Cancel**». Также можно вернуться в раздел «**Overview**», нажав кнопку «**Back To Overview**» в правой верхней части экрана.

9.3. Work model

В разделе «**Work Model**» можно просмотра интересующий режим работы или

создать новый, нажав кнопку «**New**».

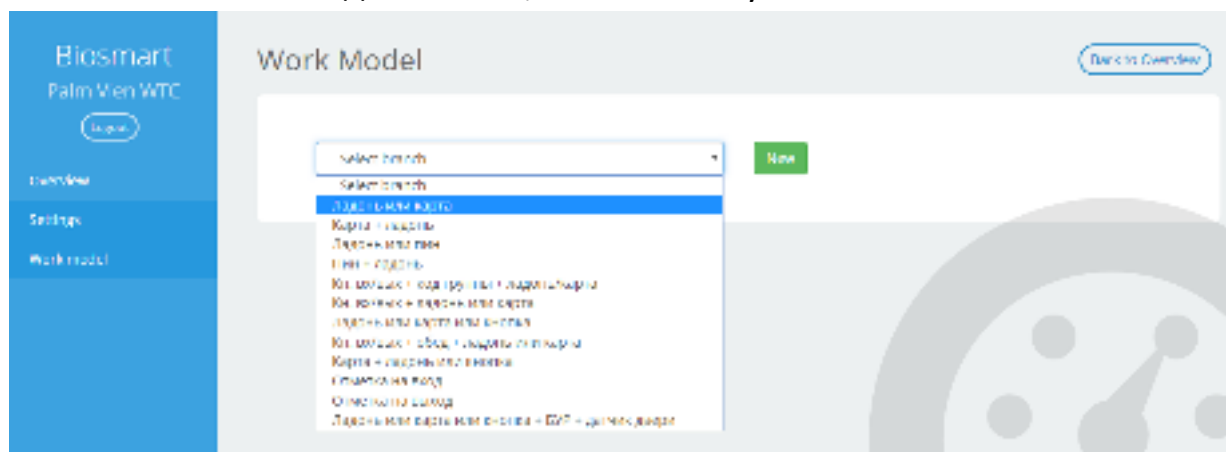


Рисунок 46. Выбор рабочей модели

Для быстрой настройки терминала можно скопировать существующий режим и отредактировать его под свои нужды, нажав кнопку «**Copy**». Созданные пользователем новые режимы и копии существующих можно также редактировать («**Edit**») или удалить («**Delete**»).

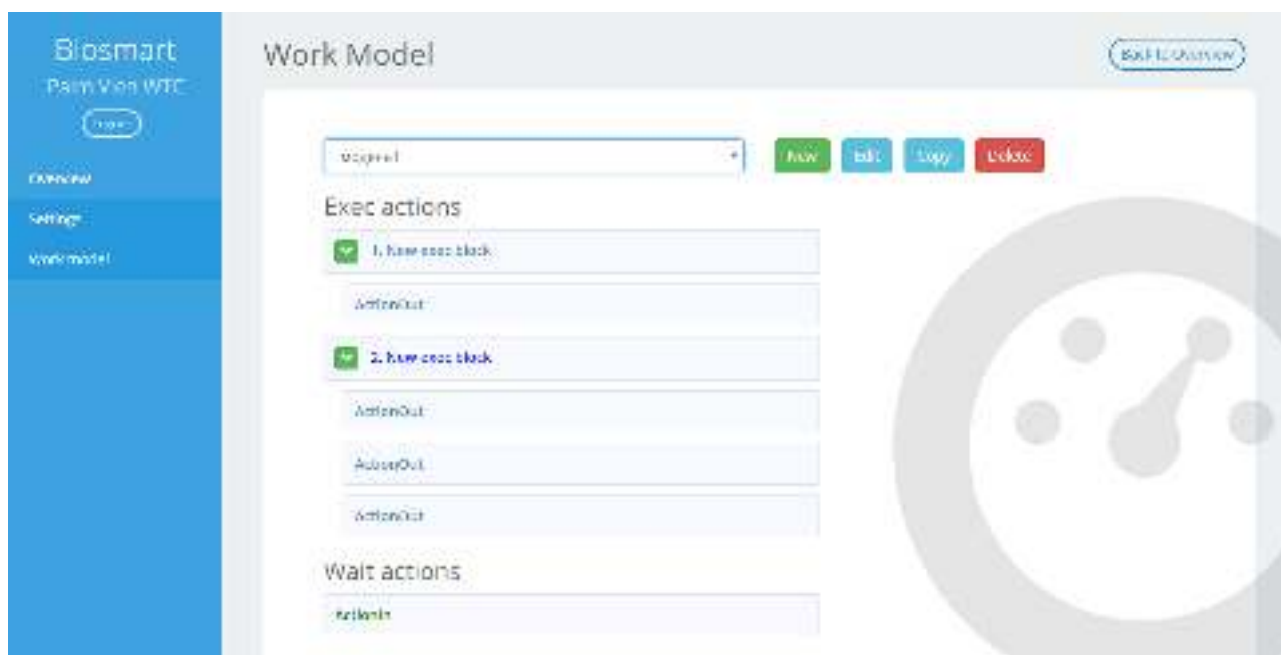


Рисунок 47. Выбор рабочей модели



Внимание! Удалить и отредактировать предварительно настроенные режимы нельзя!

Логика работы режима описана в блоках «**Exec actions**» и «**Wait actions**». Терминал ожидает (или проверяет) выбранные типы событий в секции «**Wait actions**», реагирует на них действием (-ями) из блока (-ов) «**Exec action**» и

переходит к ожиданию следующего события (или к началу, если событие было последним). Подробное описание возможных действий приведено в пункте

9.3.1. Создание и редактирование режимов работы

Для добавления нового режима нажмите кнопку «**New**». По умолчанию для редактирования доступно одно возможное событие в блоке «**Wait actions**» и одно действие в блоке «**Exec actions**». Пользователь может добавлять другие события и действия путем нажатия кнопки «**New**» в соответствующей секции. Для сохранения изменений нажмите «**Save**», для отмены - «**Cancel**». Также можно ввести название новой модели (New model по умолчанию). После окончания редактирования модели и сохранения изменений она будет доступна для применения в меню **Settings** → **Work model**

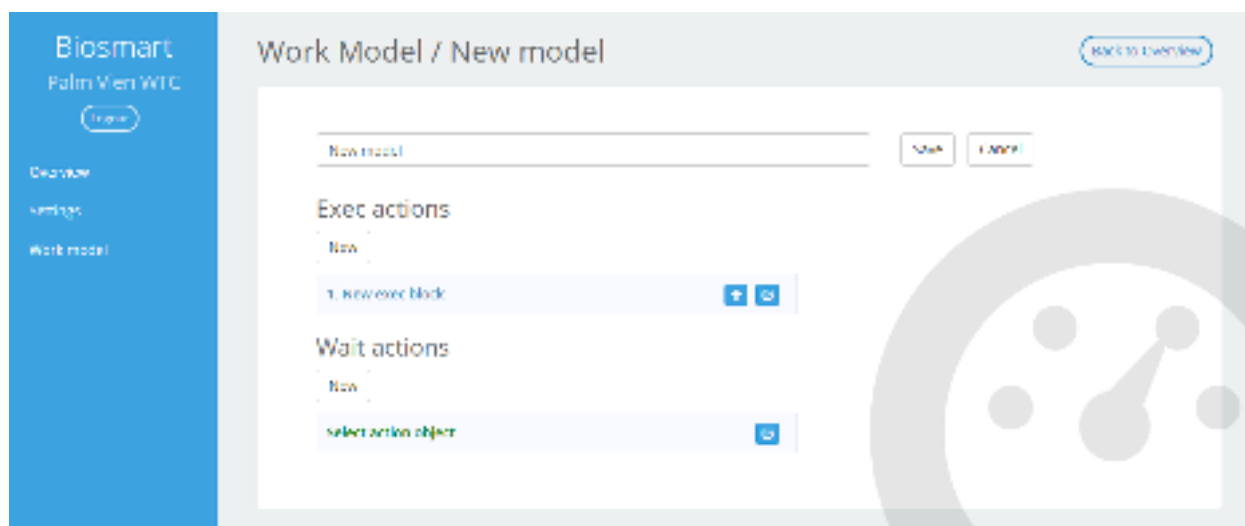


Рисунок 48. Создание новой модели

Блоки имеют следующие кнопки управления:

-  - Добавить новый элемент в блок
-  - Редактировать выбранный элемент
-  - Удалить выбранный элемент

- **Блок событий (Wait actions)**

В блоке доступны для выбора следующие типы событий

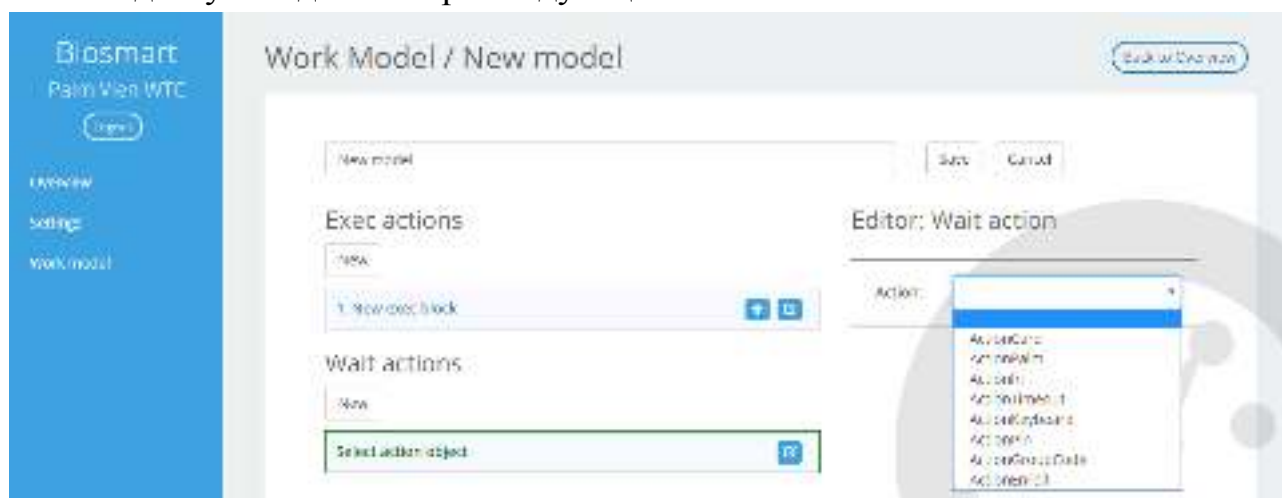


Рисунок 49. Блок событий

ActionCard — ожидание идентификации по карте

ActionPalm — ожидание идентификации по ладони

ActionIn — ожидание события по дискретному входу

ActionTimeout — ожидание окончания временного интервала

ActionKeyboard — ожидание нажатия кнопки на клавиатуре

ActionPin — ожидание ввода ПИН-кода

ActionGroupCode — ожидание ввода кода группы

ActionEnroll — ожидание внесения новых данных (карта/ладонь/пин-код)

Для событий доступны следующие параметры:

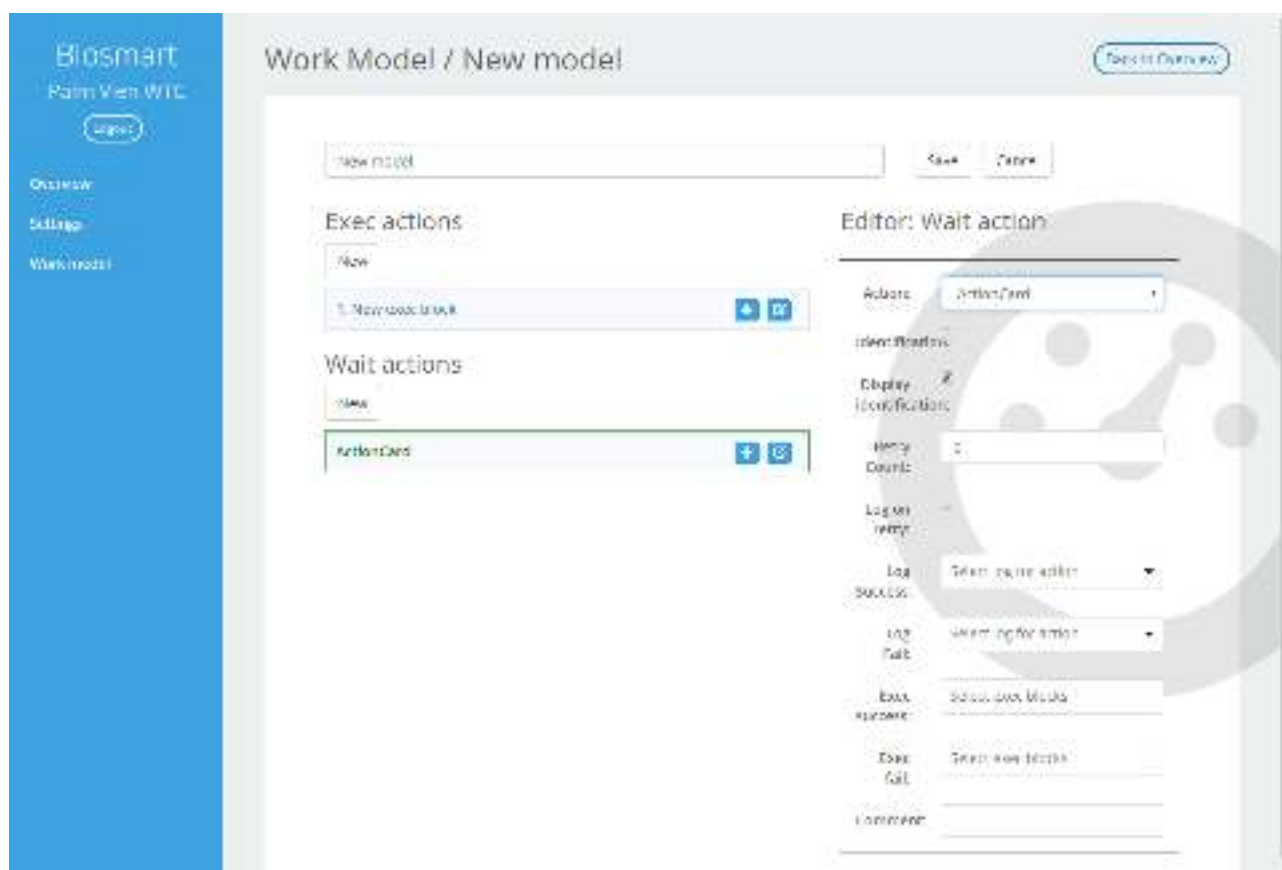


Рисунок 50. Блок событий

Identification

(Идентификация)

При включении данного пункта терминал будет производить идентификацию человека по выбранному признаку, при отсутствии - запоминать поступившие данные. По умолчанию отключено.

Display identification(Отображение
идентификации)

При включении данного пункта терминал будет отображать на экране результат идентификации. По умолчанию включено.

Log on retry(Запись лога при
попытке повтора)

При включении данного пункта терминал фиксирует в логе факт попытки повторного получения доступа. По умолчанию отключено.

Log Success\Fail(Запись лога при
успешной\неудачной
идентификации)

При наличии числового значения в поле будет произведена запись лога для дальнейшей передачи в ПО верхнего уровня.

Retry Count (Количество повторов действия при неудачном исходе действия) При отсутствии информации на устройстве о сотруднике с выбранным типом идентификатора, терминал предложит ещё N раз повторить процедуру.

Exec success\fail (Блоки действий на выполнение) При успешном\неудачном (success\fail) исходе выбранного действия будут произведены действия, описанные в выбранном блоке (блоках).

Comment (Комментарии) Текстовое описание действия. Будет отображаться рядом с названием.

Дополнительно для отдельных событий можно настроить следующие параметры:

ActionIn	Number	Номер входа
	Level	Уровень сигнала
ActionTimeout	Interval	Длительность ожидания (мс.)
ActionKeyboard	Key	Ожидаемая клавиша (0-9)
ActionGroupCode	Default	Если установлена галочка, будет использован код группы по умолчанию
ActionEnroll	Type	Определяет тип сведений, которые будут занесены (Palm – скан ладони, Card – данные карты, Pin – пин-код)

- **Блоки действий (Exec actions)**

Для блока можно задать название блока и добавить действия в этом блоке, действия будут выполняться последовательно, в том порядке, в котором они были добавлены. Обратите внимание, что порядок действий внутри одного блока после их добавления изменить будет нельзя.

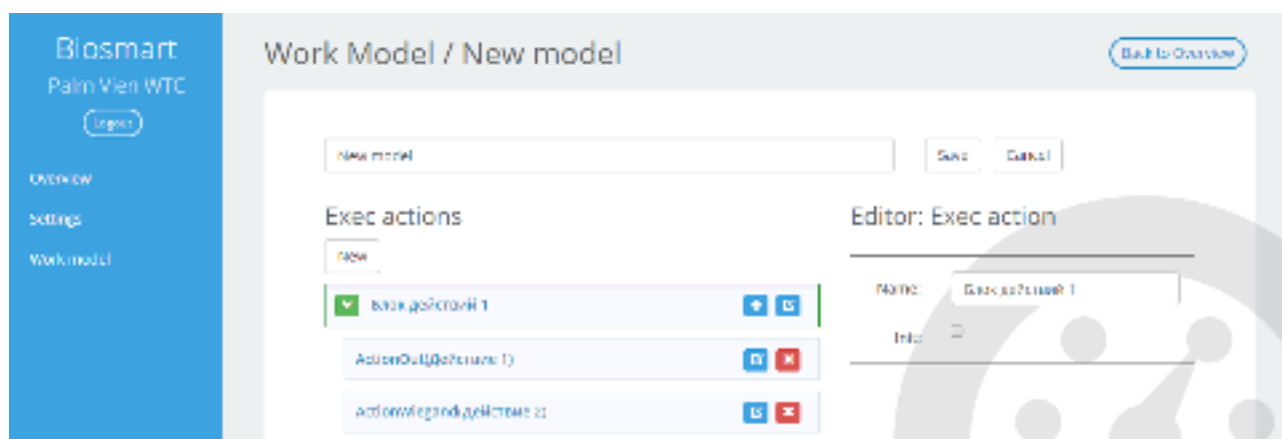


Рисунок 51. Блок действий

Блок действий имеет следующие параметры:

Name – Название блока

Init – При включении данного пункта, выбранный блок будет выполняться безусловно, при активации данной рабочей модели.

Типы возможных действий:

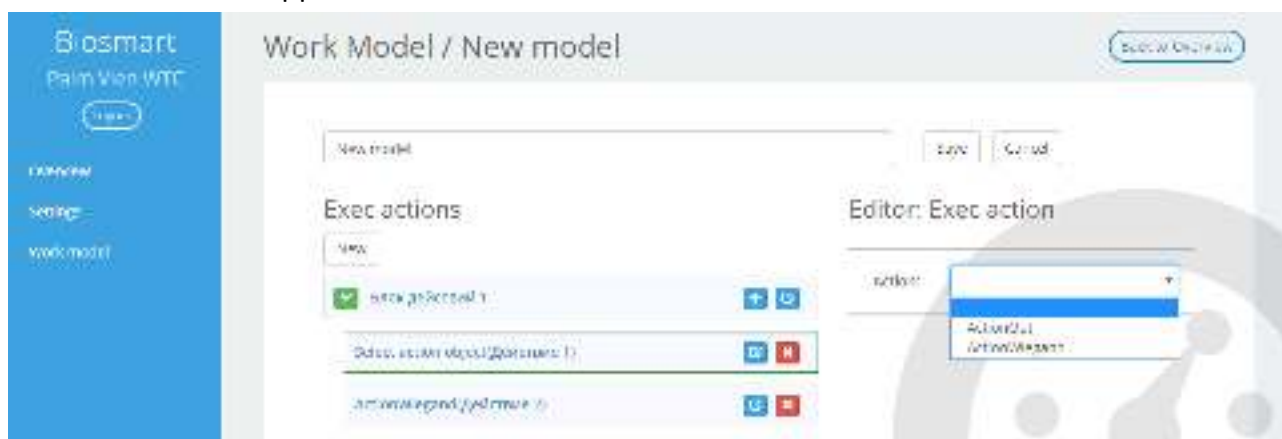


Рисунок 52. Блок действий

ActionOut — управление дискретными выходами

ActionWiegand — управление wiegand-выходом

Для действий можно настроить следующие параметры:

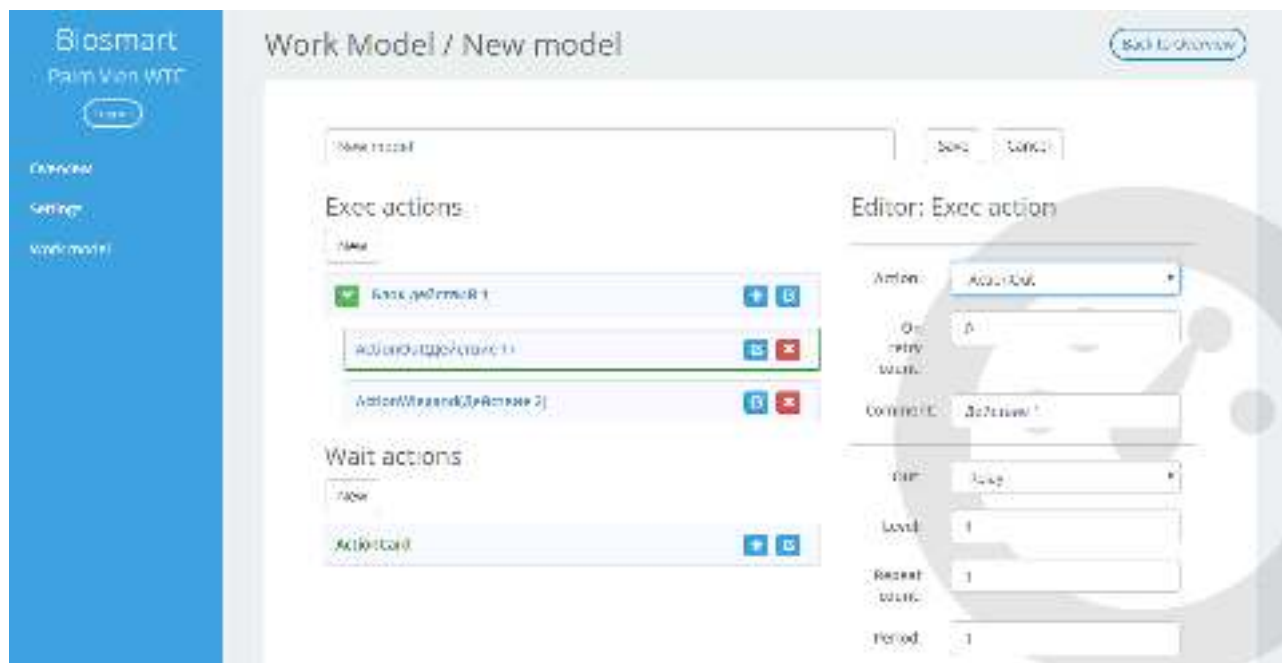


Рисунок 53. Параметры блока действий

ActionOut	Out	Номер дискретного выхода (Relay – бортовое реле; Bur 1, Bur 2 – выходы блока управления реле (БУР))
	Level	Начальный уровень воздействия (0-откл., 1- вкл.)
	Repeat count	Число повторов (0-32767)
	Period	Время включения/отключения реле в миллисекундах (0-32767)
ActionWiegand	Number	Номер wiegand-выхода (доступен «Num 0»)
	Type	Тип wiegand-выхода (26 bits, 32 bits)
	Length pulse	Длина импульса (микросекунды)
	Length interval	Длина интервала (микросекунды)

Role

Тип посылаемых данных:

Employee ID - внутренний

идентификатор идентифицируемого сотрудника;

Employee Card - номер карты идентифицируемого сотрудника;

Employee Pin – пин-код идентифицируемого сотрудника;

Code – любое число не более 4х байт

Также для всех видов действий доступны следующие общие параметры:

On retry count (Счетчик повторов) Количество попыток исполнения данного действия при неудачной попытке.

Comment (Комментарии) Текстовое описание действия. Будет отображаться рядом с названием.

- **Логи событий**

IdentPalmEnter	Вход сотрудника по ладони
IdentPalmLeave	Выход сотрудника по ладони
IdentPalmSuccess	Успешная идентификация по ладони
IdentPalmFail	Неудачная идентификация по ладони
IdentPalmDinnerLeave	Идентификация ладони сотрудника, ушедшего на обед
IdentPalmDinnerEnter	Идентификация ладони сотрудника, вернувшегося с обеда
IdentCardEnter	Карта была приложена к сканеру
IdentCardLeave	Карта была удалена от сканера
IdentCardSuccess	Успешная идентификация по карте
IdentCardFail	Неудачная идентификация по карте
IdentCardDinnerLeave	Идентификация карты сотрудника, ушедшего на обед

IdentCardDinnerEnter	Идентификация карты сотрудника, вернувшегося с обеда
IdentPinEnter	Введен пин-код
IdentPinLeave	Прекращен ввод пин-кода
IdentPinSuccess	Успешная идентификация по пин-коду
IdentPinFail	Неудачная идентификация по пин-коду
IdentPinDinnerLeave	Идентификация по пин-коду сотрудника, ушедшего на обед
IdentPinDinnerEnter	Идентификация по пин-коду сотрудника, вернувшегося с обеда
IdentBlockStudio	Запрет прохода из ПО Biosmart Studio v5
IdentBlockAntiPassBack	Запрет повторного прохода в одном направлении
IdentBlockHoliday	Запрет прохода (выходные, праздники)
IdentBlockShedule	Запрет прохода (расписание)
IdentTimeout	Таймаут идентификации
IdentUnknownError	Неизвестная ошибка идентификации
DeviceInitialization	Инициализация устройства
DeviceRestart	Перезапуск устройства
LogSaveError	Ошибка сохранения лога
EmployeeAddOK	Добавление сотрудника успешно
EmployeeAddError	Ошибка добавления сотрудника
EmployeeUpdateError	Ошибка обновления данных сотрудника
EmployeeUpdateOK	Обновление данных сотрудника успешно
EmployeeDeleteOk	Удаление данных сотрудника успешно
EmployeeDeleteError	Ошибка удаления данных сотрудника
EmployeeBlockOK	Блокировка сотрудника успешна
EmployeeBlockError	Ошибка блокировки сотрудника
EmployeeUnblockOK	Разблокировка сотрудника успешна

EmployeeUnblockError	Ошибка разблокировки сотрудника
UnblockFail	Ошибка разблокировки
HardwareUnknownError	Неизвестная ошибка оборудования
HardwareErrorScanner	Ошибка сканера
HardwareErrorCoprocc	Ошибка процессора
LeaveButton	Нажата кнопка выхода
NotPass	Проход не выполнен
TryCrackByPalm	Попытка взлома
ServerIdentSuccess	Успешная идентификация сервера
ServerIdentFail	Неудачная идентификация сервера
MobieEmployeeEnter	Вход мобильного сотрудника
MobileEmployeeExit	Выход мобильного сотрудника
MobileEmployeeSuccess	Идентификация мобильного сотрудника

9.3.2. Создание простого сценария работы.

Рассмотрим в качестве примера создание типового сценария работы системы (рабочей модели): идентификация пользователя по карте.

- Для редактирования доступны также различные параметры данного действия. Обратите внимание, что параметры для разных действий могут отличаться. Подробный список с описанием параметров каждого действия приведен в пункте
2. Создадим блоки действий, выполняемых при успешной либо неудачной идентификации.

- В блоке «**Exec actions**» нажмите кнопку «**Редактировать**» 
- В правой части экрана введите название выбранного действия в меню «**Editor: Exec action**». В данном примере это будет блок действий при успешной идентификации (**Success indication**)

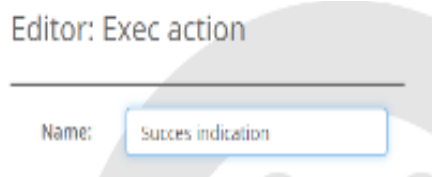


Рисунок 56. Создание блока действий

- Добавим также блок действий, выполняющихся при неудачной идентификации пользователя. Нажмите кнопку «**New**» в блоке «**Exec action**»



Рисунок 57. Создание блока действий

- Отредактируйте название созданного блока аналогично первому блоку.



Рисунок 58. Создание блока действий

3. Свяжем блок события и блоки действий.

- В блоке «**Wait actions**» нажмите кнопку «**Редактировать**» 
- В меню «**Editor: Wait action**» выберите пункт «**Exec success**». Выберите из выпадающего списка пункт «**Success indication**».

Аналогично выберите пункт «**Fail indication**» в поле «**Exec fail**».



Рисунок 59. Создание блока действий

9.3.3. Создание более сложного сценария работы.

Рассмотрим более сложный сценарий работы: в начальный момент времени терминал ожидает приложенной ладони или карты.

- В случае успешной идентификации по ладони терминал отправляет код карты сотрудника на wiegand
- В случае успешной идентификации по карте отправляет код карты сотрудника на wiegand
- В случае неудачной идентификации по ладони отправляет код «23» на wiegand
- В случае неудачной идентификации по карте отправляет код карты на wiegand

Готовый сценарий выглядит следующим образом:



Рисунок 60. Готовый сценарий

1. Создадим первый блок – **«Успешная идентификация ладони»**. Он используется при успешной идентификации по ладони. Итогом его выполнения станет отправка ID карты сотрудника на wiegand

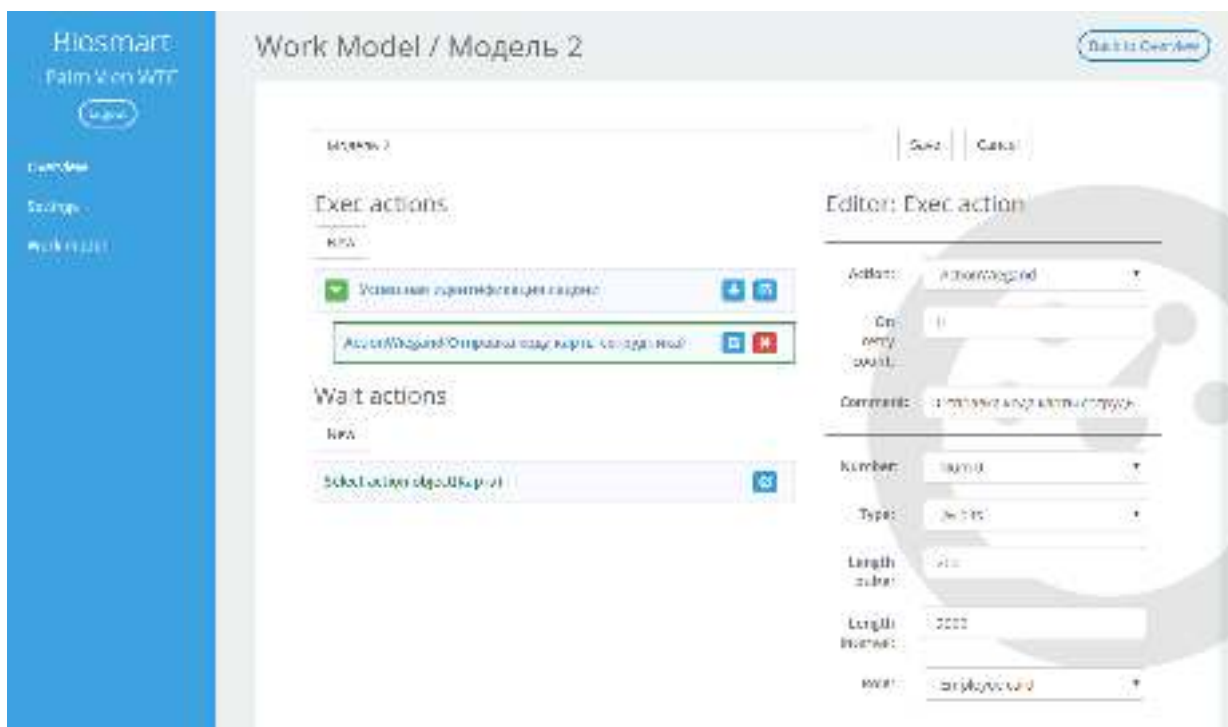


Рисунок 61. Создание сценария

Добавим действие «Отправка кода карты сотрудника» (ActionWiegand) со следующими параметрами:

- Один wiegand-выход (Number 0), типа wiegand-26 (Type: 26);
- Длины импульса и интервала 200 и 2000 (Length pulse и Length interval соответственно), средние из допустимого;
- Тип данных - карта пользователя (Role: Employee card).

2. Создадим следующий блок – **«Успешная идентификация карты»**. Он используется при успешной идентификации по карте. Итогом его выполнения станет отправка кода карты сотрудника на wiegand

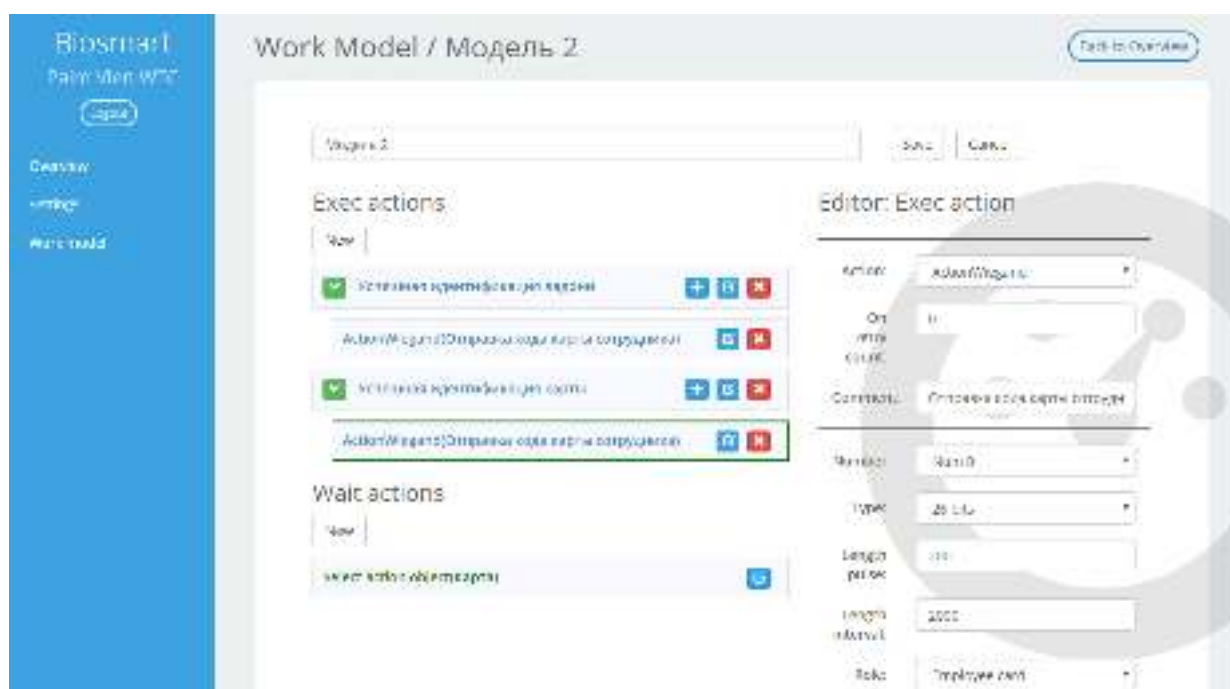


Рисунок 62. Создание сценария

Добавим действие «Отправка кода карты сотрудника». Параметры зададим аналогично предыдущему пункту.

3. Создадим третий блок – **«Неудачная идентификация ладони»**. Он используется, если ладонь не была идентифицирована. Итогом его выполнения станет отправка статичного кода «23» на wiegand.

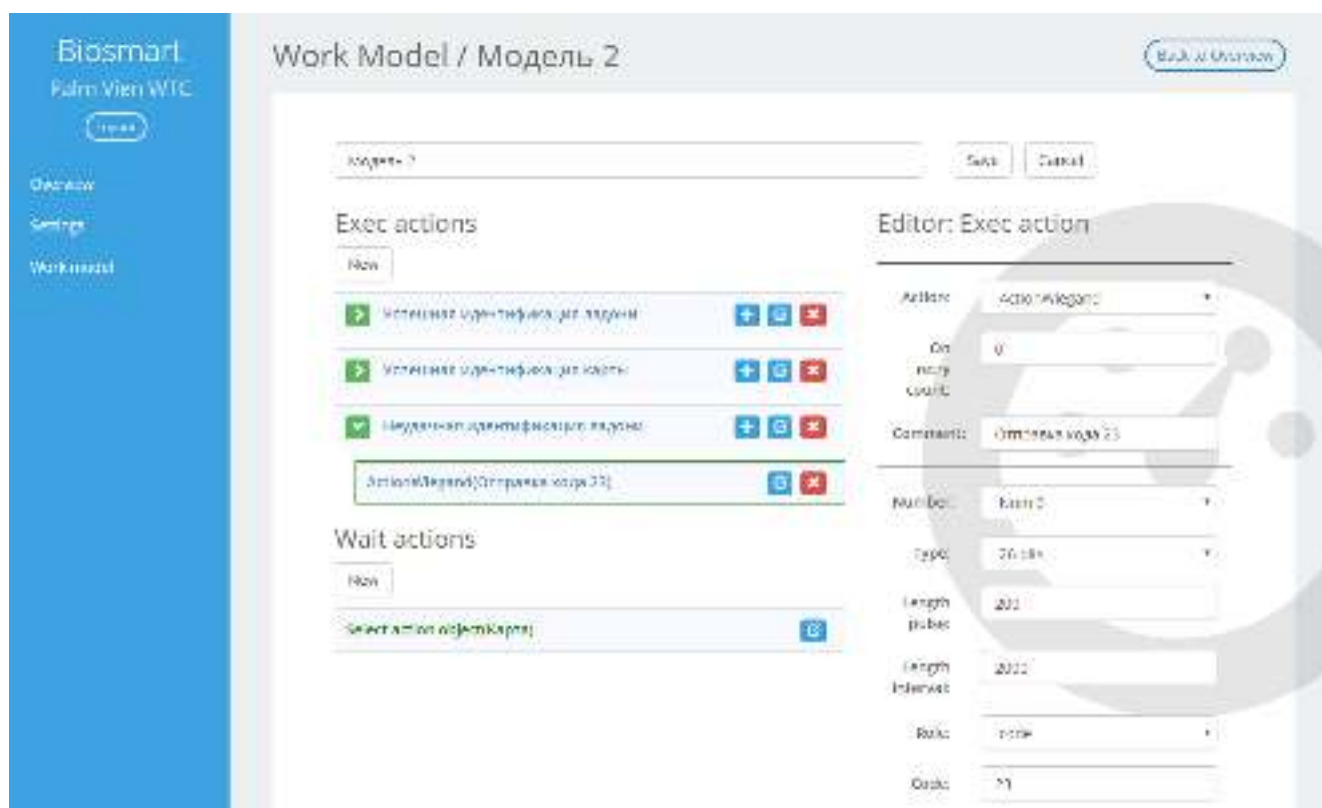


Рисунок 63. Создание сценария

Добавим действие «Отправка кода 23». Выберем режим отправки статического кода (Role:code) и зададим его значение (Code:23).

4. Создадим последний блок – **«Неудачная идентификация карты»**. Он используется, если карта не была идентифицирована. Итогом его выполнения станет отправка кода приложенной карты на wiegand.

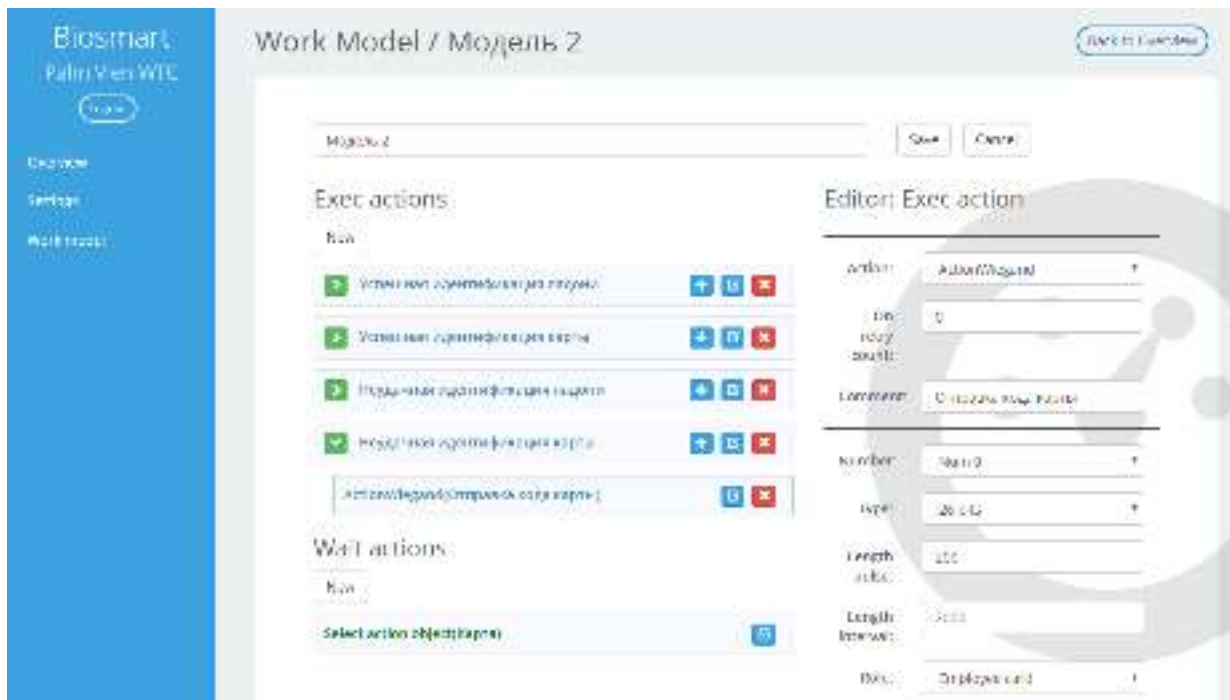


Рисунок 64. Создание сценария

Добавим действие «Отправка кода карты». Выберем режим отправки кода карты (Role: Employee card).

Теперь определим события, которые будут вызывать описанные выше действия. Создадим событие «Карта» типа ActionCard. Оно будет отвечать приложению карты.

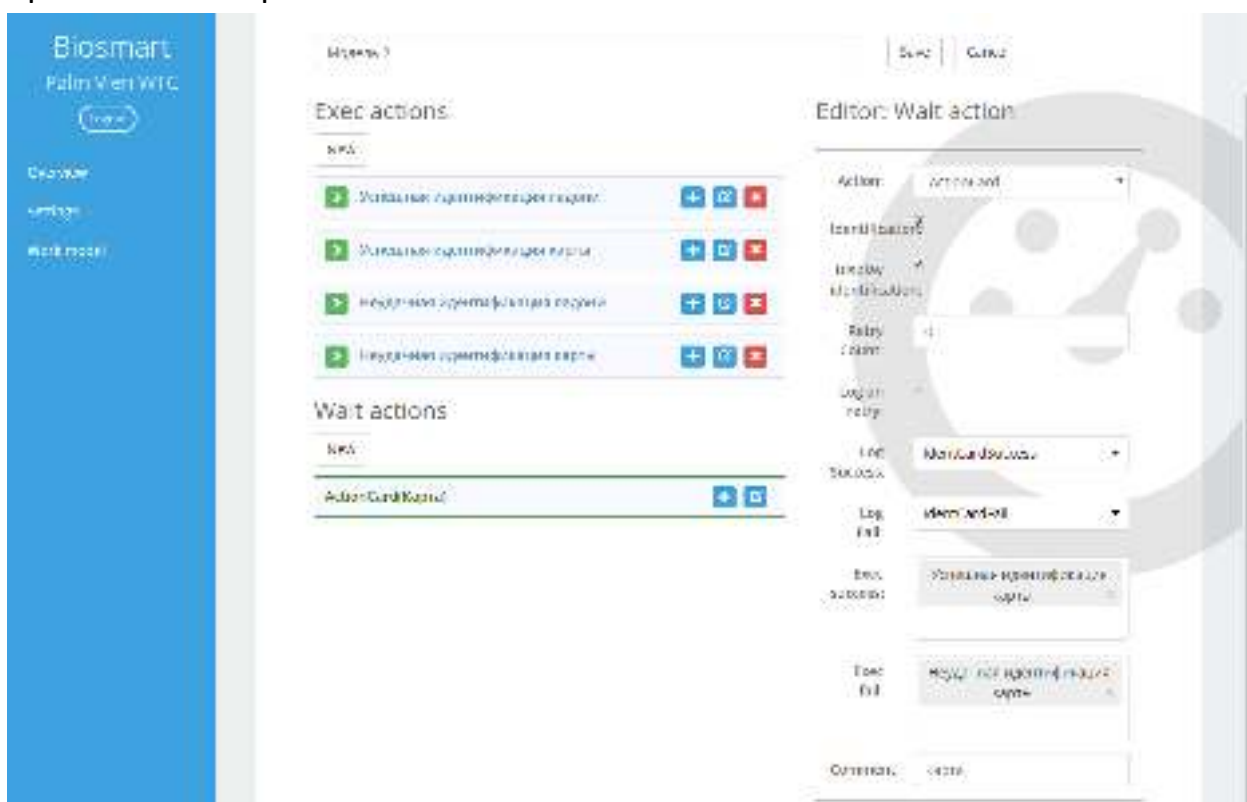


Рисунок 65. Создание сценария

Установим следующие параметры данного события:

- Производить идентификацию и отображать результат на дисплее (установить галочки в **Identification** и **Display Identification**);
- Добавляем логирование для сохранения журнала по производимым действиям (**Log success: IdentCardSuccess** и **Log fail:IdentCardFail**);
- В случае успешной идентификации отправляем ID сотрудника на wiegand – указываем обработчик события «**Успешная идентификация карты**» в поле **Exec success**;
- В случае неудачной идентификации отправляем код карты на wiegand – указываем обработчик события «**Неудачная идентификация карты**» в поле **Exec fail**.

Создадим событие «**Ладонь**», которое будет отвечать приложенной ладони. Выберем соответствующий тип – **ActionPalm**.

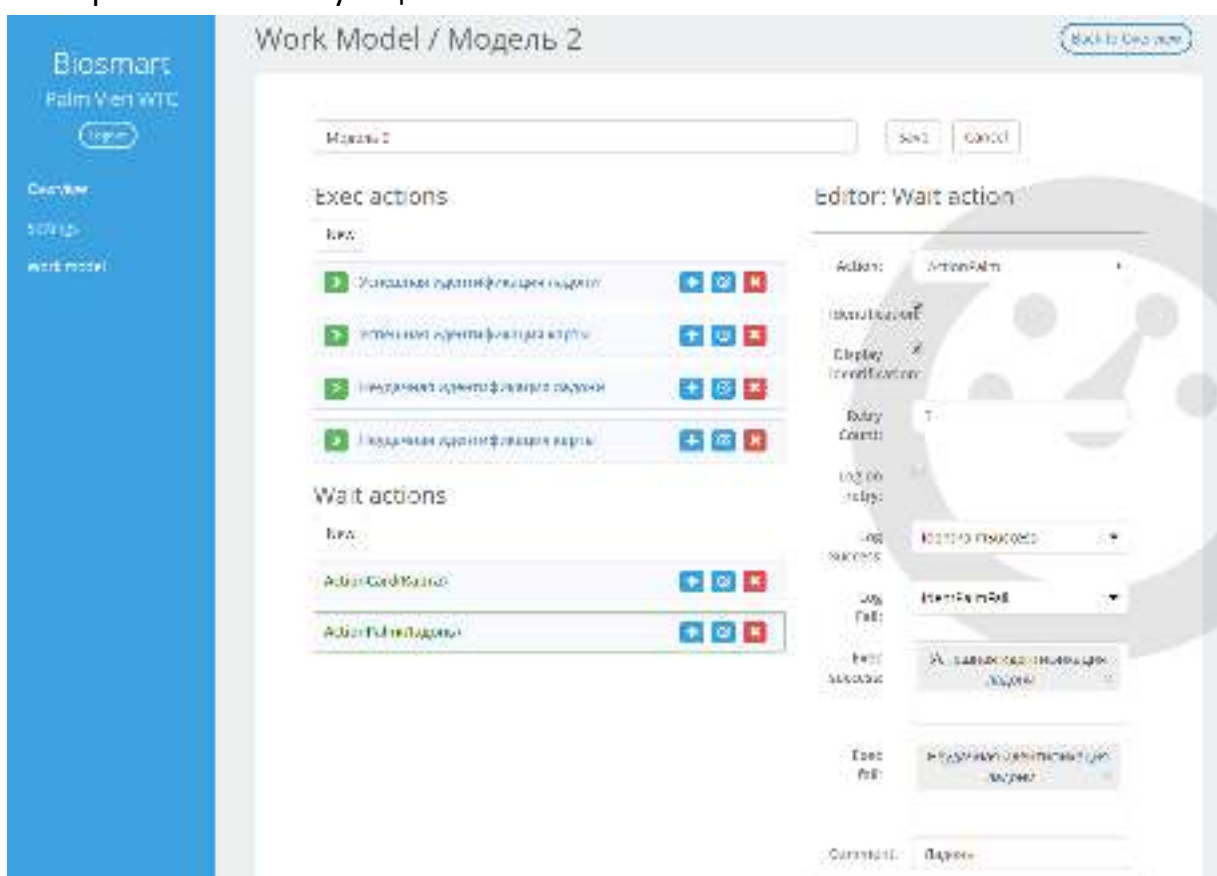


Рисунок 66. Создание сценария

Параметры события определим следующим образом:

- Производить идентификацию и отображать результат на дисплее

- (установить галочки в **Identification** и **Display Identification**;
- Установим три попытки идентификации (**Retry Count:3**);
 - Добавляем логирование для сохранения журнала по производимым действиям (**Log success: IdentPalmSuccess** и **Log fail:IdentPalmFail**);
 - В случае неудачной идентификации отправляем статичный код 23 на wiegand – указываем обработчик события «**Неудачная идентификация ладони**» в поле **Exec fail**;
 - В случае успешной идентификации отправляем номер карты сотрудника на wiegand – указываем обработчик события «**Успешная идентификация ладони**» в поле **Exec Success**.

9.3.4. Создание сценария работы с использованием реле/кнопки.

В начальный момент времени терминал ожидает приложенной карты или нажатой кнопки.

- При нажатии кнопки должно срабатывать бортовое реле на 7 секунд
- При успешной идентификации по карте ожидается идентификация по ладони в течение 10 секунд
- При успешной идентификации по ладони включить реле на 7 секунд
- При неудачной идентификации по ладони выдать код ранее приложенной карты на wiegand
- При неудачной идентификации по карте выдать код wiegand «23»

Готовый сценарий выглядит следующим образом:

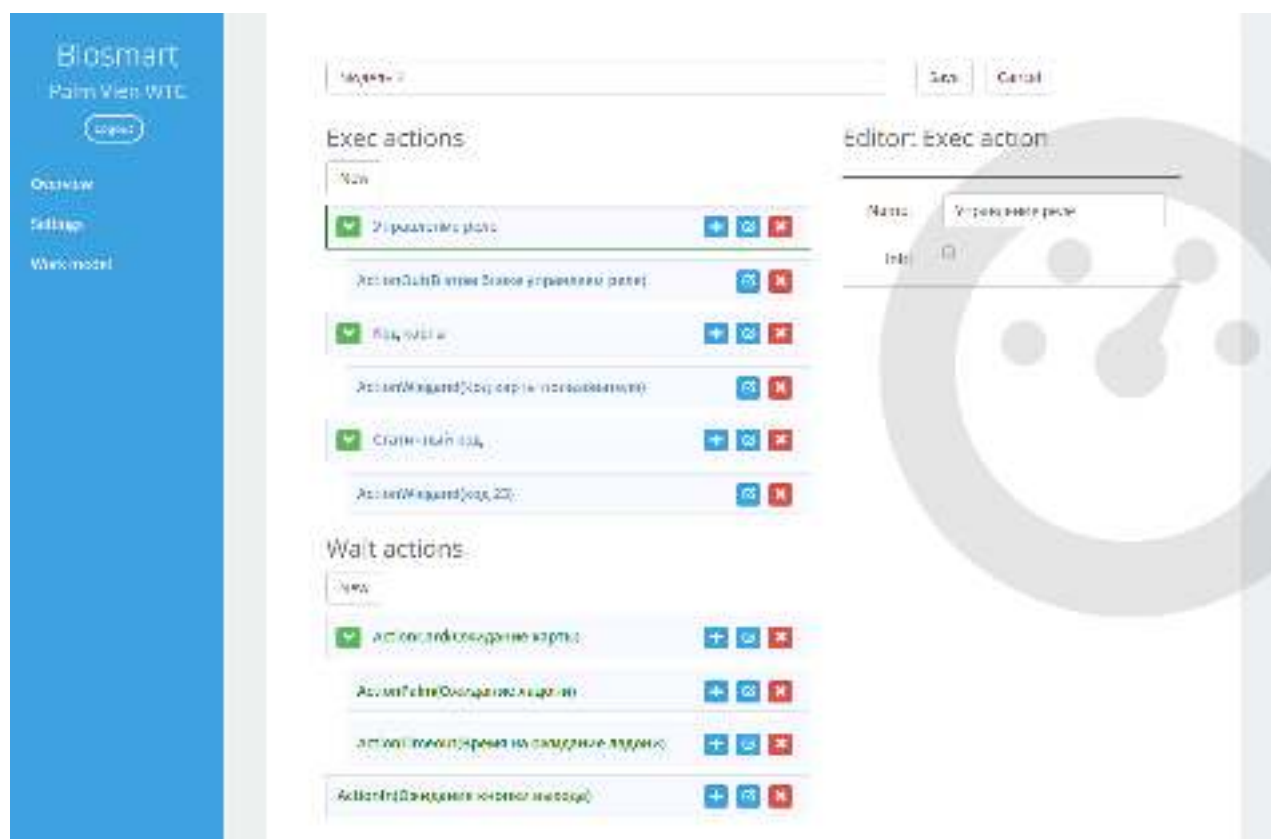


Рисунок 67. Готовый сценарий

Ожидаемые действия расположены на одном уровне, уровне, следующие за событием - с отступами.

Нам потребуются три различных блока действий: блок для включения реле и блоки для отправки разных кодов на wiegand-выход

5. Создадим первый блок - **«Управление реле»**. Он используется при нажатии на кнопку и при успешной идентификации по ладони:

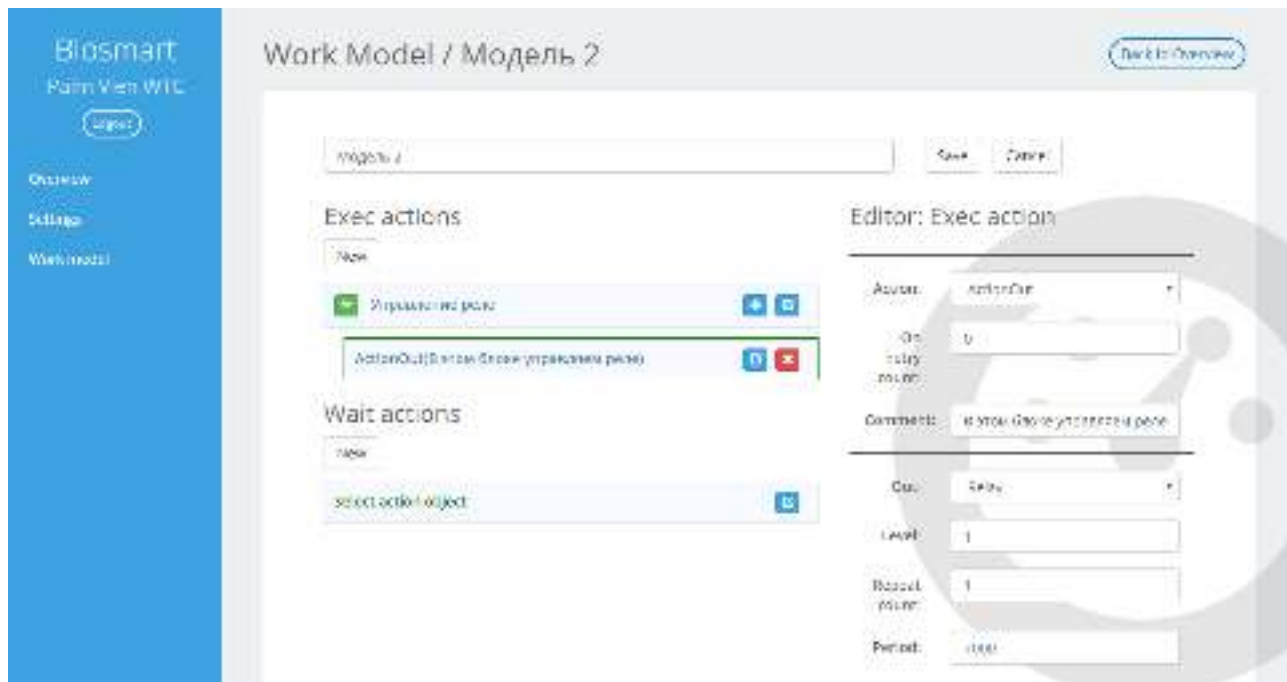


Рисунок 68. Создание сценария.

Добавим в блок действие «Управление выходом» (**ActionOut**). Нам необходимо включить реле (**Out: relay**) один раз (**Repeat count: 1**) на 7 секунд (**Period: 7000**).

6. Следующий блок – «**Код карты**». Он используется при неудачной идентификации по ладони.

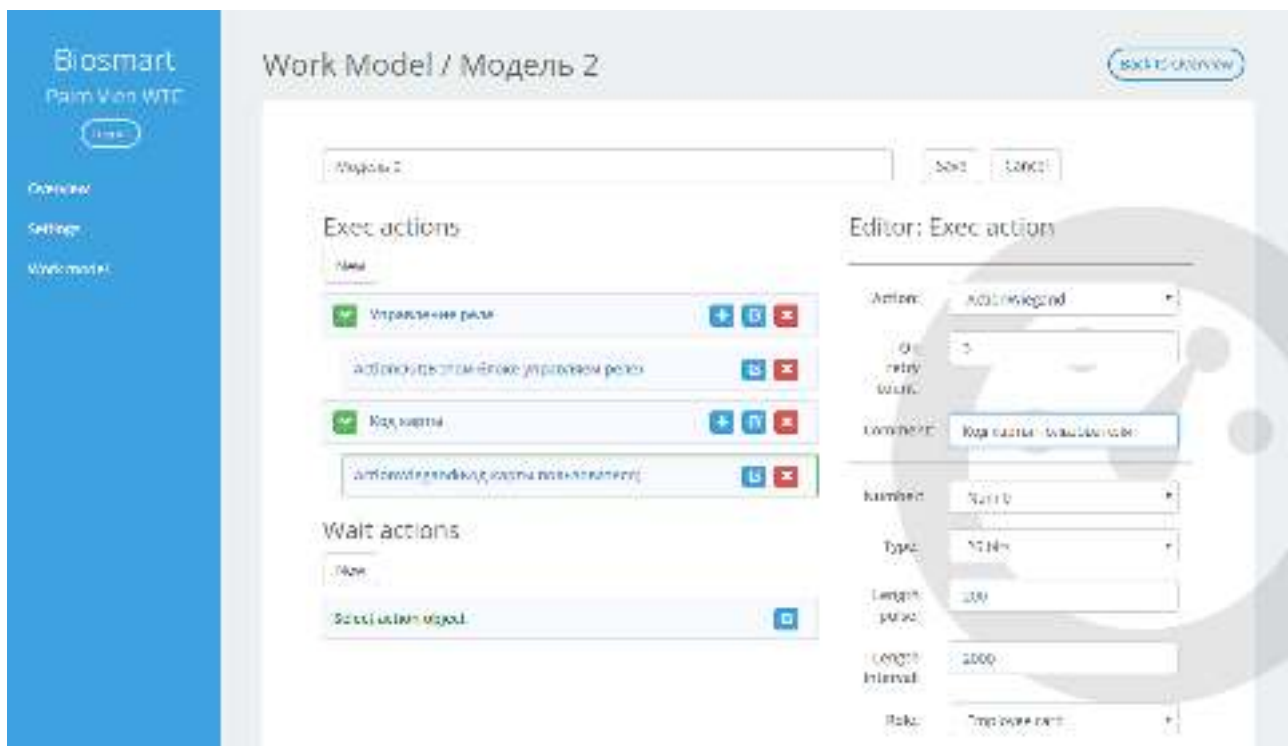


Рисунок 69. Создание сценария.

Добавляем действие «Код карты пользователя» (**ActionWiegand**) со следующими параметрами:

- Один wiegand-выход (**Number 0**), типа wiegand-26 (**Type: 26**);
- Длины импульса и интервала 200 и 2000 (**Length pulse** и **Length interval** соответственно), средние из допустимого;
- Тип данных - карта пользователя (**Role: Employee card**);
- Устанавливаем три попытки идентификации, т.е. после третьей неудачной попытки будет отправлен код (**On retry count: 3**).

7. Последний необходимый блок – «**Статичный код**». Он отвечает за отправку кода «23» на wiegand-выход.

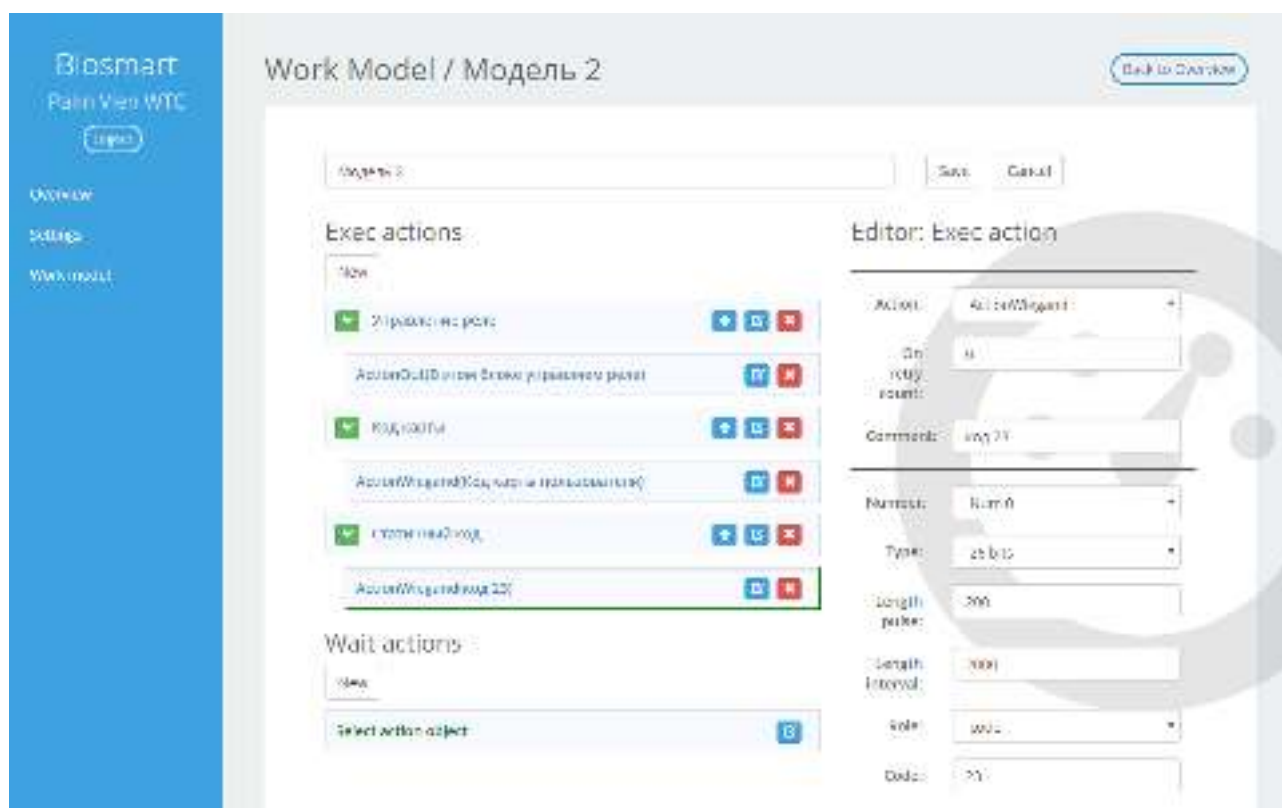


Рисунок 70. Создание сценария

Настраиваем параметры действия следующим образом:

- Один wiegand-выход (**Number 0**), типа wiegand-26 (**Type: 26**);
- Длины импульса и интервала 200 и 2000 (**Length pulse** и **Length interval** соответственно), средние из допустимого;
- Тип данных - статичный код (**Role: Code**);
- Значение кода – 23 (**Code: 23**);
- Т.к. идентификация по карте только одна, поле «On retry count»

Далее необходимо добавить действия для идентификации по ладони:

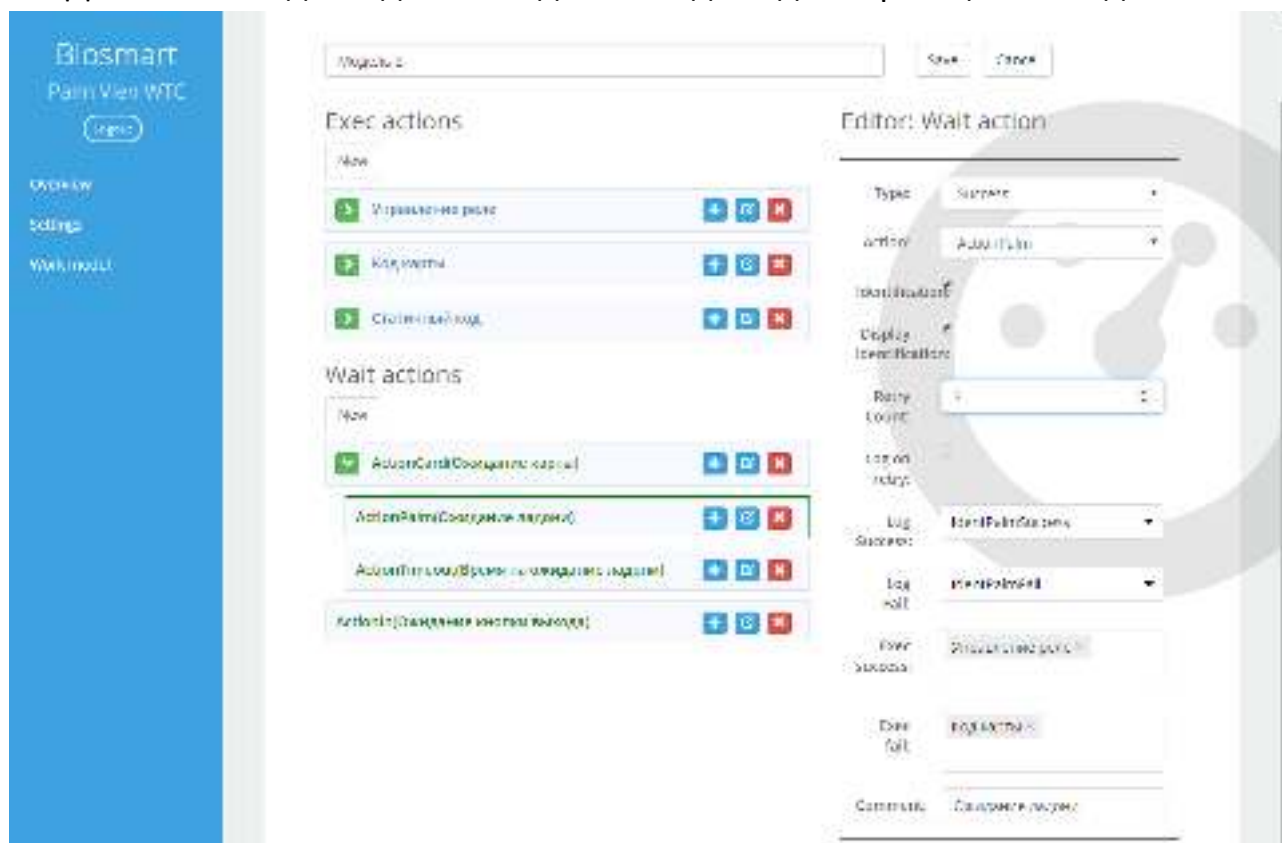


Рисунок 72. Создание сценария

- Добавляем логирование для сохранения журнала по производимым действиям (**Log success: IdentPalmSuccess** и **Log fail:IdentPalmFail**);
- Добавляем действия, исполняемые при удачной и неудачной идентификации по исходам действия (**Exec success – Управление реле, Exec fail – Код карты**);
- Дадим возможность трех попыток идентификации по ладони (**Retry count: 3**).

Для того, чтобы ограничить время идентификации по ладони (например, для ожидания другой карты, если предыдущий пользователь приложил карту и ушел, забыв отметиться рукой) зададим время ожидания идентификации по ладони:

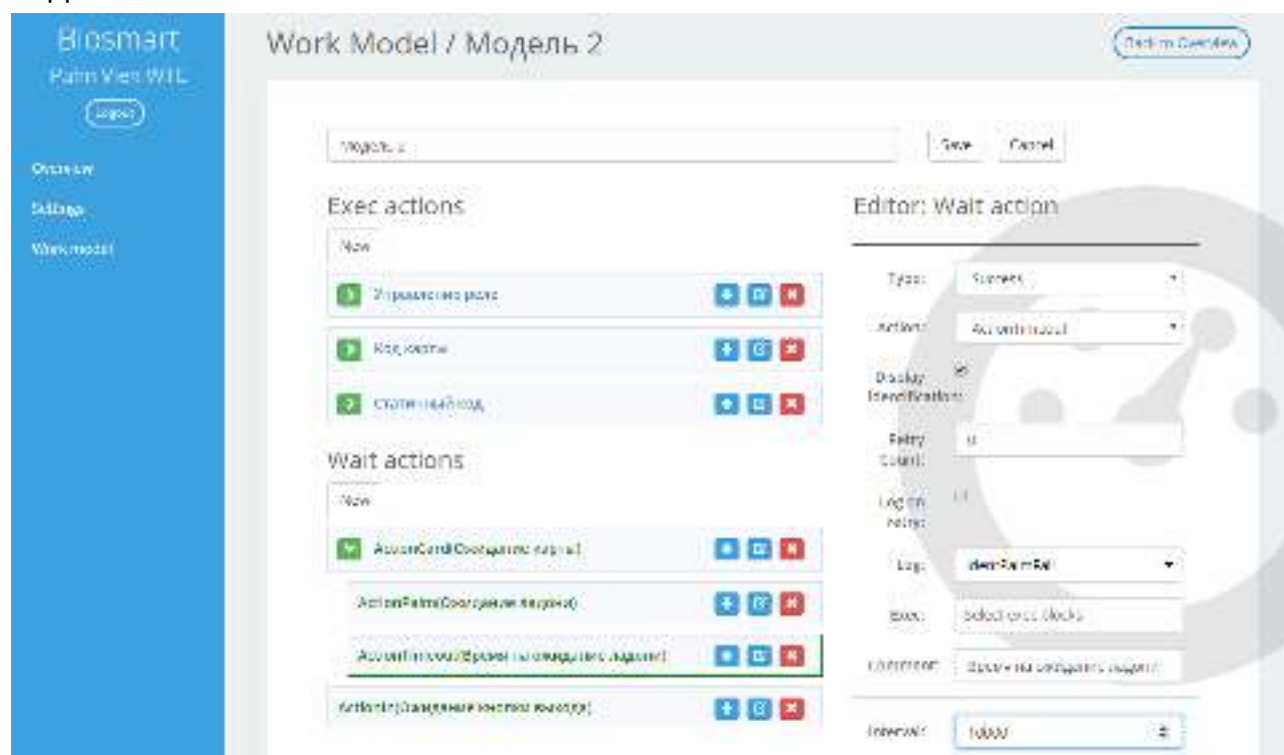


Рисунок 73. Создание сценария

- Зададим параметр “**interval**” 10000, что равно 10 сек - время на идентификацию по ладони;
- Если интервал закончится, а идентификация по ладони не будет произведена, запишем лог об этом событии (**Log: IdentPalmFail**).

Последнее событие - нажатие кнопки:

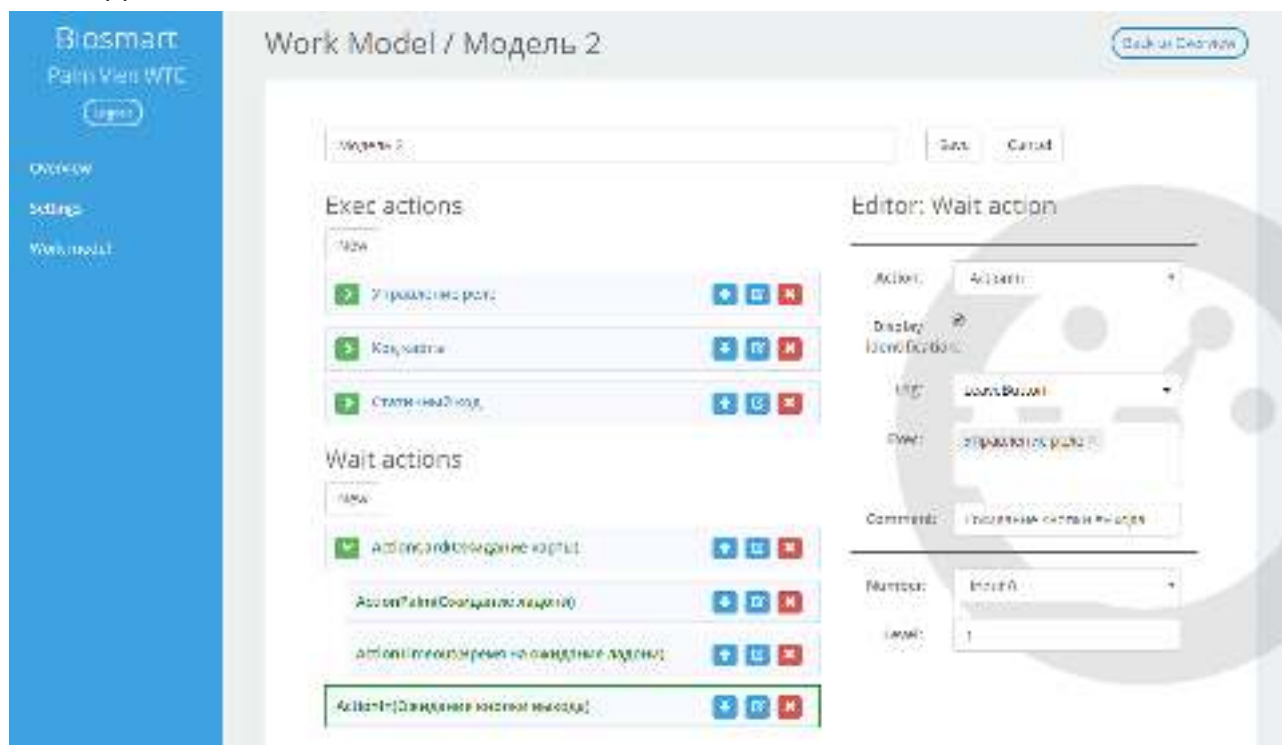


Рисунок 74. Создание сценария

- Указываем вход, с которым соединена кнопка (**Number: Input 0**) и уровень сигнала - 1;
- Логируем событие (**Log: LeaveButton**);
- В качестве исполнительного действия указываем управление реле (**Exec: Управление реле**).

10. Неисправности терминала и методы их устранения

Методы устранения некоторых неисправностей терминала представлены в таблице 1.

Таблица 1. Неисправности терминала и методы их устранения

№	Описание неисправности	Возможная причина	Методы устранения
1	При подаче питания не загорается экран	Отсутствие контакта	• Выключите питание. • Проверьте, надежно ли закреплен провод питания в клеммнике. • Включите питание.

3	На экране появился значок ошибки в работе терминала. Устройство в целом работает, но нет информации во вкладке "Инфо" полностью или частично.	В результате внутренней автоматической диагностики выявлена ошибка работы терминала, которая отображена в меню «Ошибки»: Соединение с базой (ошибка соединения с базой данных терминала, неисправна файловая система).	• Выключите питание. • Подождите 1 минуту. • Включите питание.
4	На экране появился значок ошибки в работе терминала. Могут не работать все или одно/несколько нижеперечисленных устройств: - клавиатура; - считыватель карт; - дискретный вход; - реле; - wiegand выход.	В результате внутренней автоматической диагностики выявлена ошибка работы терминала, которая отображена в меню «Ошибки»: Устройства ввода/вывода (неисправна файловая система, неисправность во внутренних соединениях, неисправность шлейфов и подключений)	• Визуально проверьте шлейфы и плату терминала на наличие повреждений. • Выключите питание. • Подождите 1 минуту. • Включите питание.

5	На экране появился значок ошибки в работе терминала. Не работает сканер.	В результате внутренней автоматической диагностики выявлена ошибка работы терминала, которая отображена в меню «Ошибки»: Сканер (неисправность USB кабеля сканера, ненадежный контакт)	• Выключите питание; • Осмотрите на наличие повреждений сканер и USB кабель сканера. Все разъемы должны стоять без перекосов; • Подключите сканер ко второму входу USB терминала; • Включите питание.
---	--	---	--

Если содержащаяся в данном разделе информация не помогла вам в установлении причины неисправности, свяжитесь со службой технической поддержки.

11. Обслуживание терминала

Терминал рассчитан на непрерывную работу без постороннего вмешательства, однако, для обеспечения исправности терминала необходимо проводить некоторые операции профилактического обслуживания.

11.1 Проверка физического состояния терминала

Проводится раз в 3 месяца.

Для проверки физического состояния терминала выполните следующее:

- проверьте узлы терминала на загрязнение, коррозию, влажность и пыль.
- при необходимости очистки сканера, продуйте его сжатым воздухом, затем аккуратно очистите поверхность сухой мягкой тканью;
- проверьте на предмет выявления несанкционированных доработок и визуально заметных повреждений, таких как не подсоединенные провода и поврежденная изоляция.

11.2 Проверка наличия ошибок в работе терминала

Проводится раз в месяц, или по необходимости.

Для проверки выполните следующее:

- проверьте наличие значка ошибки в работе терминала. При отсутствии значка проверку можно прекратить;
- откройте меню «**Ошибки**» терминала

Если ошибки имеются (рисунок 75), действуйте согласно пунктам 3-5 таблицы 1.

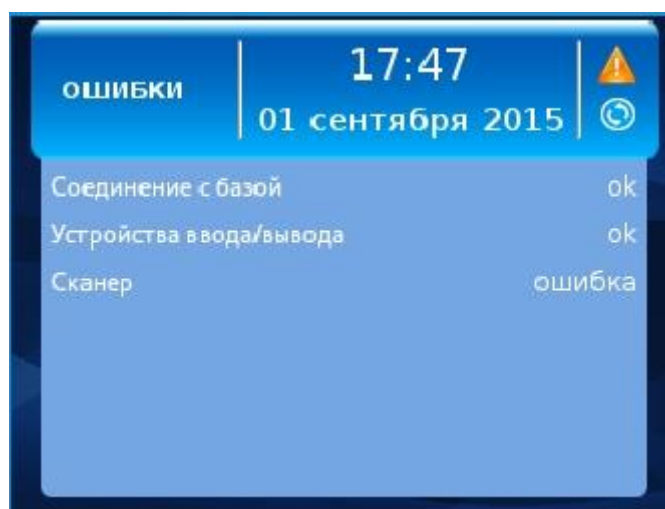


Рисунок 75. Ошибка сканера

11.3 Проверка наличия ошибок в работе с сейфовыми ячейками

Проводится раз в месяц, или по необходимости.

В режиме работы терминала с сейфовыми ячейками, в списке проверяемых ошибок работы терминала в меню «**Ошибки**» появляются дополнительные пункты «**Контроллер ПРОМЕТ**», «**Незакрытая ячейка**», «**Дублированные ячейки**» (рисунок 76).

При наличии какой-либо ошибки из списка, в правом углу экрана появляется значок ошибки в работе терминала.

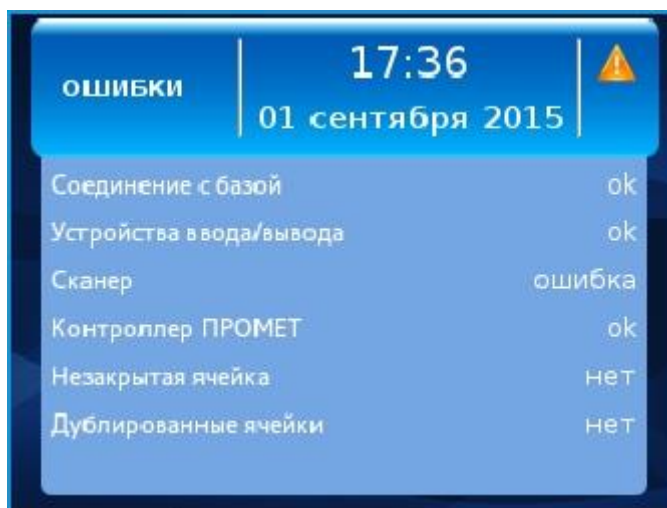


Рисунок 76. Виды ошибок при работе с ячейками

Наличие ошибки «**Контроллер ПРОМЕТ**» информирует об отсутствии связи с контроллером сейфовых ячеек. В этом случае требуется проверить настройки контроллера сейфовых ячеек и проверить, что он подключен к сети.

Наличие ошибки «**Незакрытая ячейка**» говорит о том, что сейфовая ячейка не была закрыта в отведенное время, либо произошел взлом ячейки. В этом случае необходимо проверить состояние сейфовой ячейки.

Наличие ошибки «**Дублированные ячейки**» говорит о наличии в системе ячеек с одинаковым адресом. В этом случае необходимо инициализировать терминал из ПО BioSmart Studio v5 и вновь назначить доступ сотрудникам.

12. Хранение

В помещениях для хранения терминала не должно быть паров кислот, щелочей, агрессивных газов и других вредных веществ, вызывающих коррозию.

13. Транспортирование

Транспортирование упакованных терминалов может производиться любым видом транспорта в крытых транспортных средствах.

14. Утилизация

Терминал не содержит опасных для здоровья потребителей и окружающей

среды материалов. При утилизации по окончании срока службы специальных мер по экологической безопасности не требуется.