Терминал BioSmart PV-WTC

Руководство по эксплуатации

Версия документа HW.028.M.7

Дата 01.2026

SEC.RU | Короткий путь к информации
Скачано с sec.ru

СОДЕРЖАНИЕ

1 ОПИСАНИЕ ТЕРМИНАЛА BIOSMART PV-WTC 6
1.1 Состав и внешний вид 6
1.2 Технические характеристики 7
1.3 Описание работы терминала 10
1.4 Описание платы терминала 10
1.5 Описание платы терминала BioSmart PV-WTC-EM-L 13
2 ЭКСПЛУАТАЦИОННЫЕ ОГРАНИЧЕНИЯ ТЕРМИНАЛА BIOSMART PV-WTC 16
2.1 Механические факторы 16
2.2 Климатические факторы 16
2.3 Биологические факторы 16
2.4 Электромагнитные поля и электрический ток 17
2.5 Дополнительные ограничения 17
3 МОНТАЖ BIOSMART PV-WTC 18
3.1 Меры безопасности 18
3.2 Рекомендации 18
3.3 Порядок монтажа 21
3.4 Особенности монтажа для обеспечения пылевлагозащиты 21
3.5 Монтаж и подключение терминала BioSmart PV-WTC-EM-L 22
4 ПОДКЛЮЧЕНИЕ BIOSMART PV-WTC 24
4.1 Подключение питания терминала 24
4.2 Подключение терминала к сети Ethernet 24
4.3 Подключение электромеханического замка 25
4.4 Подключение электромагнитного замка через БУР BioSmart 26
4.5 Подключение датчика прохода и кнопки управления 27
4.6 Подключение к стороннему контроллеру по Wiegand 28
4.7 Подключение к алкотестеру Динго B-02 29
5 БЫСТРЫЙ СТАРТ ТЕРМИНАЛА BIOSMART PV-WTC 30
5.1 Регистрация RFID-карт 39
5.2 Назначение сотрудникам пин-кодов 39
6 ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО ТЕРМИНАЛА 41
6.1 Обновление встроенного ПО с помощью ПО Biosmart-Studio v6 41
6.2 Обновление встроенного ПО с помощью веб-интерфейса 43
7 НАСТРОЙКИ ТЕРМИНАЛА BIOSMART PV-WTC 45

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7.1 Настройки в меню терминала BioSmart PV-WTC 45
7.2 Настройки терминала BioSmart PV-WTC в ПО Biosmart-Studio v6 52
7.2.1 Вкладка Общие 53
7.2.2 Вкладка Системные 55
7.2.3 Вкладка Диагностика 58
7.2.4 Вкладка Видеокамеры 59
7.2.5 Вкладка Пользователи 59
7.2.6 Вкладка Полномочия 60
7.3 Настройки терминала BioSmart PV-WTC в веб-интерфейсе 60
7.3.1 Доступ к веб-интерфейсу 60
7.3.2 Раздел Overview 61
7.3.3 Раздел Settings 62
7.3.4 Раздел Work Model 65
7.3.5 Структура и параметры рабочей модели 67
8 РАБОТА С ТЕРМИНАЛОМ BIOSMART PV-WTC 78
8.1 Редактирование данных сотрудника на терминале 78
8.2 Выбор и создание рабочих моделей 85
8.2.1 Предустановленные рабочие модели 85
8.2.2 Использование рабочей модели «Кн. вх/вых + код группы + ладонь/карта» 92
Описание рабочей модели 92
Порядок настройки 93
8.2.3 Создание простой рабочей модели 96
8.2.4 Создание рабочей модели с отправкой данных по интерфейсу Wiegand 99
8.2.5 Создание рабочей модели с использованием реле/кнопки 104
8.2.6 Создание рабочей модели с использованием датчика прохода 111
8.3 Настройка прав пользователей терминала 114
8.4 Применение настроек профиля 117
8.5 Работа терминала в локальном режиме 119
8.6 Работа терминала в режиме серверной идентификации 120
8.7 Работа с картами Mifare терминала PV-WTC 122
8.7.1 Работа в незащищенном режиме, чтение UID 122
8.7.2 Работа в защищенном режиме 125
8.7.3 Работа со смартфонами в качестве идентификатора 133
8.7.4 Настройка работы терминала с картами, инициализированными в стороннем ПО 138

SEC.RU | Короткий путь к информации
Скачано с sec.ru

9 РАБОТА С ДОПОЛНИТЕЛЬНЫМ ОБОРУДОВАНИЕМ 139
9.1 Работа с устройством измерения температуры BioSmart Thermoscan 139
9.1.1 Общие сведения 139
9.1.2 Настройка рабочей модели 139
9.1.3 Настройка параметров измерения температуры 142
9.1.4 Порядок работы 143
9.2 Работа с алкотестером Динго B-02 145
9.2.1 Общие сведения 145
9.2.2 Порядок работы 145
9.3 Работа с БУР BioSmart 147
9.3.1 Общие сведения 147
9.3.2 Настройка рабочей модели 148
10 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ТЕРМИНАЛА BIOSMART PV-WTC 150
11 ХРАНЕНИЕ, ТРАНСПОРТИРОВАНИЕ И УТИЛИЗАЦИЯ ТЕРМИНАЛА BIOSMART PV-WTC 154
12 ПРИЛОЖЕНИЕ 1 ПЕРЕМЕННЫЕ SNMP 155
13 ПРИЛОЖЕНИЕ 2 СПИСОК СООБЩЕНИЙ В РАЗДЕЛАХ МОНИТОРИНГ И ЖУРНАЛ В ПО BIOSMART-STUDIO V6 158

SEC.RU | Короткий путь к информации
Скачано с sec.ru

В настоящем руководстве по эксплуатации содержаться основные сведения о терминале **BioSmart PV-WTC** (далее «терминал»), порядок монтажа, подключения и настройки. Документация и программное обеспечение постоянно улучшаются, последние актуальные версии документации и ПО можно найти на сайте www.bio-smart.ru в разделе "Технический портал".

Используемые сокращения и обозначения:

ПО – программное обеспечение;

БУР BioSmart – блок управления реле;

СКУД – система контроля и управления доступом;

БП – блок питания;

ПК – персональный компьютер.



Так выделена информация, на которую следует обратить особое внимание.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1 ОПИСАНИЕ ТЕРМИНАЛА BIOSMART PV-WTC

Терминал **BioSmart PV-WTC** предназначен для работы в составе биометрической системы контроля и управления доступом BioSmart. Также терминал может работать автономно или в составе сторонней СКУД.
Терминал может использоваться для учета рабочего времени посредством идентификации пользователей по рисунку вен ладоней, RFID-картам и смартфонам, а также, в зависимости от исполнения, может применяться для организации контроля и управления доступом.

Терминал совместим с ПО Biosmart-Studio версии не ниже 5.10.5. Терминал может использоваться с более ранними версиями ПО Biosmart-Studio. В этом случае необходимо, чтобы на терминал была установлена белее ранняя версия встроенного ПО. При этом часть функций, описанных в данном руководстве, будет недоступна. Для получения информации о совместимости встроенного ПО терминала и ПО Biosmart-Studio v6 обратитесь к специалистам технической поддержки.

1.1 Состав и внешний вид

Терминал **BioSmart PV-WTC** состоит из следующих частей:

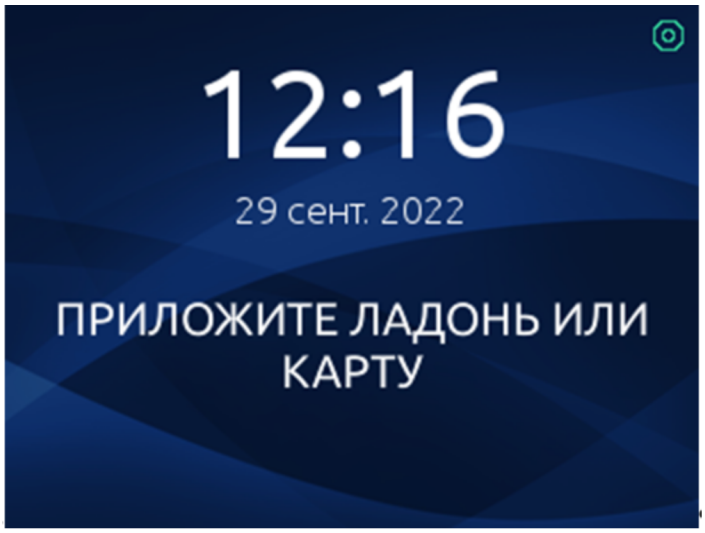
- корпус терминала;
- плата терминала;
- сканер вен ладоней;
- считыватель RFID-меток (карт);
- ЖК-дисплей;
- клавиатура.



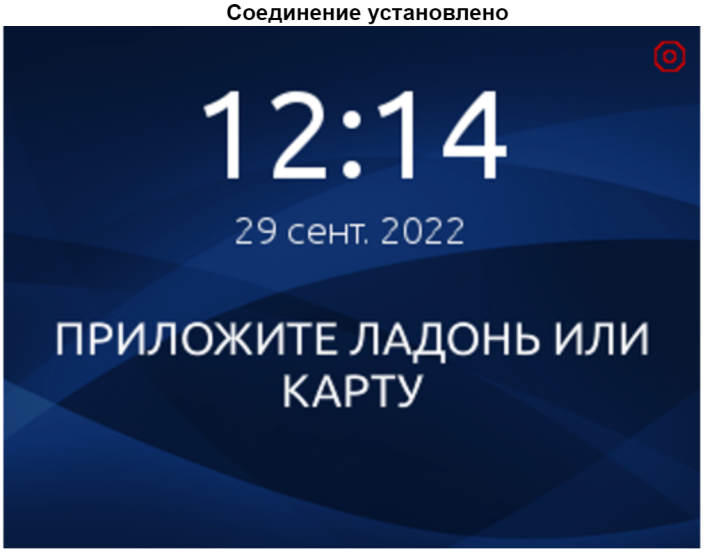
Корпус терминала состоит из передней панели и задней крышки с монтажной пластиной. Заднюю крышку можно снять, чтобы получить доступ к разъёмам на плате терминала.
На ЖК-дисплей в режиме ожидания выводится информация о текущей дате, времени, ожидаемом действии в соответствии с выбранной рабочей моделью. При входе в меню терминала на ЖК-дисплее отображаются пункты меню и варианты настроек.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

В некоторых режимах в правом верхнем углу дисплея отображается статус соединения с сервером:



Соединение установлено



Нет соединения

Клавиатура используется для входа в меню терминала и перемещения между пунктами меню, изменения настроек. В зависимости от настроек терминала клавиатура может использоваться для ввода пин-кода и выбора направления прохода сотрудника (вход/выход).

1.2 Технические характеристики

Терминалы **BioSmart PV-WTC** выпускаются в различных исполнениях в зависимости от типа встроенного RFID-считывателя и версии платы. Исполнение терминала и перечень считываемых RFID-карт указаны в паспорте на терминал.
Основные технические характеристики терминала приведены в таблице

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Параметр	Значение
Биометрический идентификатор	Рисунок вен ладони
Тип биометрического сканера	Оптический, инфракрасный
Максимальное количество шаблонов вен ладоней, при работе в режиме идентификации (1:N)	20 000
Максимальное количество шаблонов вен ладоней, при работе в режиме верификации (1:1)	300 000
Время идентификации в локальном режиме 1:1000 пользователей (1:2000 шаблонов)	Менее 2 секунд
Время идентификации в серверном режиме 1:10000 пользователей (1:20000 шаблонов)	Менее 3,5 секунд
Максимальное количество кодов RFID-меток, хранящихся на терминале	1 000 000
Максимальное количество событий, хранящихся на терминале	10 000 000
Вероятность ошибочного предоставления доступа по биометрическим данным (FAR)*	10^{-5} – 10^{-7}
Наличие встроенного считывателя RFID-меток	Да
Наличие датчика вскрытия корпуса	Да
Наличие датчика отрыва от стены	Да
Наличие дисплея и клавиатура	Да
Поддержка работы с блоком управления реле БУР BioSmart**	Да
Поддержка работы с алкотестером**	Да
Поддержка работы с устройством измерения температуры BioSmart Thermoscan H**	Да

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Параметр	Значение
Поддержка протоколов SNMP, NTP	Да
Интерфейс связи с управляющим компьютером	Ethernet (IEEE 802.3u, 100BASE-TX)
Интерфейс связи со сторонними устройствами**	Wiegand Out 26/32/64, RS-485, USB
Количество встроенных реле**	1
Электрические параметры реле	DC 12 В 1 А
Состояние контактов реле	Нормально разомкнутое
Количество дискретных входов**	1
Средства индикации	Дисплей и звуковой зуммер
Параметры электропитания	DC 12 В 1 А
Поддержка PoE	IEEE 802.3af class 3
Материал корпуса	Пластик
Габаритные размеры, мм	225 x 160 x 145
Масса нетто, г	не более 860
Масса брутто, г	1230
Температура окружающего воздуха при эксплуатации	От 0 до +50 °С
Степень защиты корпуса	IP65

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Параметр	Значение
Примечания: *значения FAR получены расчётным методом и зависят от качества биометрических шаблонов и настроек сканирования. При значении FAR = 10^{-7} вероятность ошибочного отказа в доступе (FRR) составляет 6%, при использовании базы данных, соответствующей 3000 человек. **относятся ко всем исполнениям терминала, кроме **BioSmart PV-WTC-EM-L**.	

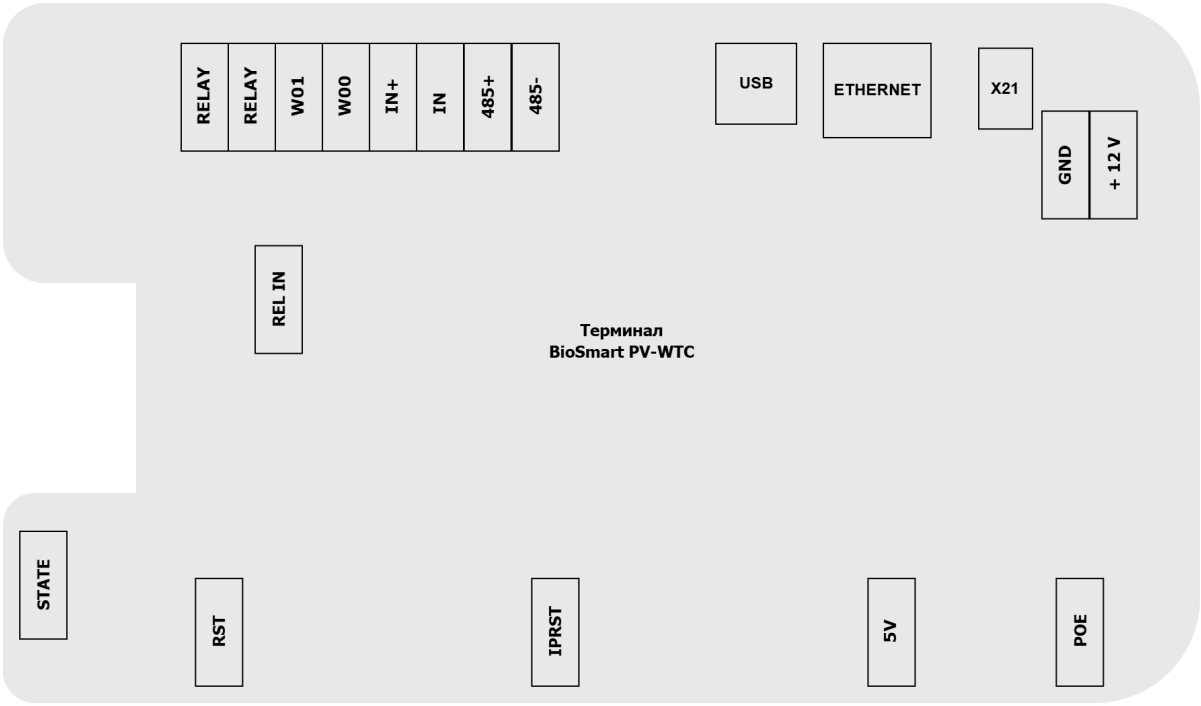
1.3 Описание работы терминала

В процессе работы терминал циклически опрашивает состояние сканера вен ладоней и RFID-считывателя. Считанные биометрические данные (или код RFID-карты) сравниваются с шаблонами вен ладоней (или кодами карт), хранящимися в базе данных. Если совпадение найдено, и доступ соответствующему сотруднику разрешен, то терминал выполняет действия, указанные в настройках терминала, например, выдает команды на исполнительные устройства или передает данные по интерфейсу Wiegand. Если совпадение не обнаружено, или доступ данному сотруднику запрещен, то выполняются другие действия в соответствии с настройками. Затем терминал возвращается к циклическому опросу состояния считывающих устройств.
Терминал поддерживает протокол SNMP (Simple Network Management Protocol) для передачи информации о своем состоянии в корпоративные средства мониторинга. Список переменных, публикуемых терминалом по протоколу SNMP, приведен в Приложении 1.

1.4 Описание платы терминала

Расположение разъёмов, перемычек и индикаторов на печатной плате терминала представлено на рисунке ниже (кроме исполнения **BioSmart PV-WTC-EM-L**). Состав и расположение элементов на плате терминала **BioSmart PV-WTC-EM-L** отличается от указанного на ниже и приведено в Описание платы терминала BioSmart PV-WTC-EM-L .

SEC.RU | Короткий путь к информации
Скачано с sec.ru



ⓘ Маркировка контактов RS-485 может отличается от приведенной на рисунке выше, при этом положение контактов остается таким же как на рисунке выше.

Перемычки

Обозначение	Назначение
IPRST	Перемычка для сброса сетевых настроек терминала до настроек установленных на предприятии-изготовителе
RST	Перемычка для перезагрузки терминала

- Для сброса сетевых настроек при включенном питании необходимо замкнуть контакты перемычки **IPRST** и дождаться, пока светодиоды **Link** и **Activity** на разъеме Ethernet погаснут. После этого перемычку необходимо разомкнуть.
- Для перезагрузки терминала необходимо при включенном питании замкнуть контакты перемычки на 1 секунду.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Светодиодные индикаторы

Название индикатора	Тип и цвет индикации	Описание
REL	зеленый	Состояние реле (индикация включается при замыкании реле)
IN	зеленый	Отображает поступление +12В на вход **IN** терминала
PoE	зеленый	Отображает наличие питания терминала по стандарту **PoE**
5V	зеленый	Отображает наличие питания микросхем +5В, что говорит об исправности источника питания терминала
STATE	зеленый	Отображает информацию о работе системы (для служебного пользования)

ⓘ Светодиоды, размещенные на разъемах Ethernet, отображают состояние физического подключения (Link, зеленый) и активности обмена по сети (Activity, красный).

Описание разъемов платы терминала приведено в таблице

Обозначение разъема	Описание	Назначение
RELAY	Выход нормально разомкнутых контактов реле (DC 12В 1А)	Подключение исполнительного устройства
RELAY		
WO1	Выход DATA1 интерфейса Wiegand	Подключение к стороннему контроллеру по интерфейсу Wiegand
WO0	Выход DATA0 интерфейса Wiegand	
IN+	Выход +12В для подачи на дискретный вход	Подключение датчика или кнопки
IN	Дискретный вход	
485-	Канал B	Подключение БУР BioSmart

SEC.RU | Короткий путь к информации
Скачано с sec.ru

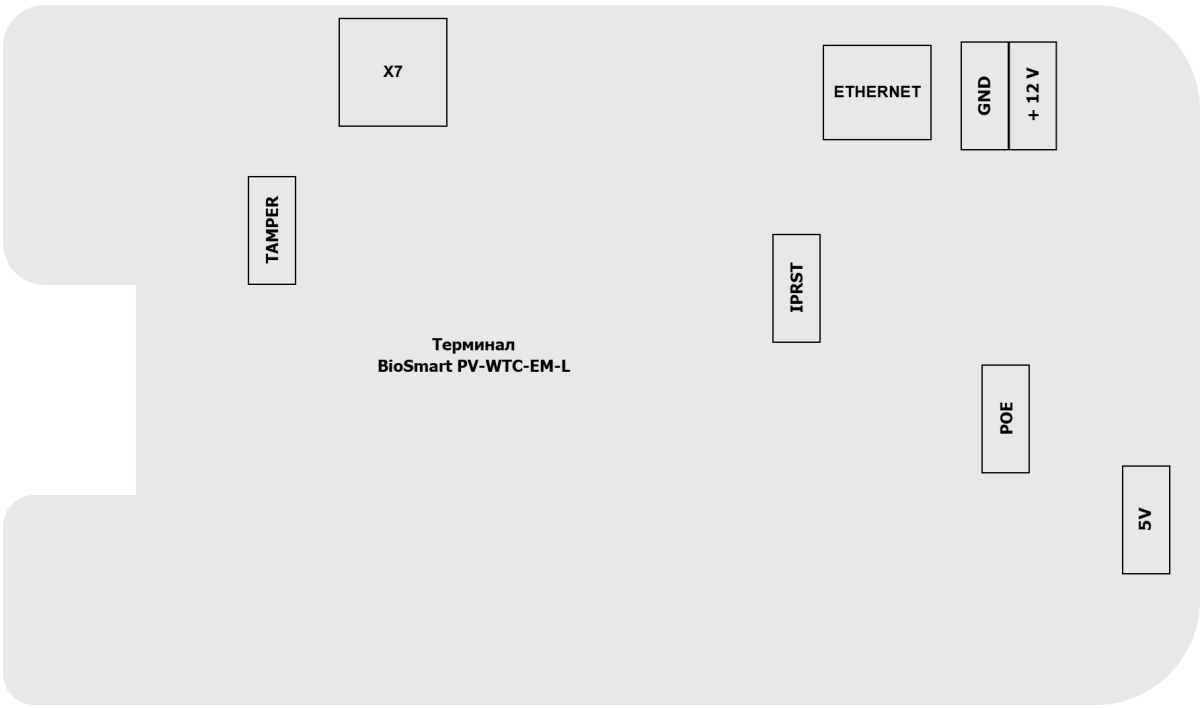
Обозначение разъема	Описание	Назначение
485+	Канал A	
USB	Разъем USB	Подключение устройства BioSmart Thermoscan или алкотестера
Ethernet	Разъем Ethernet + POE(IEEE 802.3af class 3)	Подключение к сети Ethernet или PoE-инжектору
X21	Место, зарезервированное под стандартный разъем БП (12В)	Подключение к источнику питания 12 В
GND	Питание, общий провод	Подключение к отрицательному полюсу источника питания 12 В
+12 V	Питание, +12В	Подключение к положительному полюсу источника питания 12 В

1.5 Описание платы терминала BioSmart PV-WTC-EM-L

Терминал BioSmart PV-WTC-EM-L предназначен исключительно для организации учёта рабочего времени и не поддерживает взаимодействие со сторонними устройствами. Внешний вид терминала BioSmart PV-WTC-EM-L не отличается от других исполнений, но печатная плата переработана и существенно отличается.

Расположение контактов, разъёмов, перемычек и индикаторов на печатной плате терминала BioSmart PV-WTC-EM-L показан на рисунке ниже.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Светодиодные индикаторы

Название индикатора	Тип и цвет индикации	Описание
PoE	зеленый	Отображает наличие питания терминала по стандарту PoE
5V	зеленый	Отображает наличие питания микросхем +5В, что говорит об исправности источника питания терминала

Описание разъемов платы терминала BioSmart PV-WTC-EM-L приведено в таблице

Обозначение разъема	Описание	Назначение
TAMPER	Контакты для подключения датчика отрыва корпуса от стены	Подключение к датчику отрыва корпуса от стены
X7	Разъём для карт MicroSD	Подключение карт MicroSD
Ethernet	Разъем Ethernet + POE(IEEE 802.3af class 3)	Подключение к сети Ethernet или PoE-инжектору
+12 V	Питание, +12В	Подключение к положительному полюсу источника питания 12 В
GND	Питание, общий провод	Подключение к отрицательному полюсу источника питания 12 В

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Обозначение разъема	Описание	Назначение
IPRST	Перемычка для сброса сетевых настроек терминала до настроек установленных на предприятии-изготовителе	

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2 ЭКСПЛУАТАЦИОННЫЕ ОГРАНИЧЕНИЯ ТЕРМИНАЛА BIOSMART PV-WTC

В настоящем разделе приведены требования, несоблюдение которых недопустимо по условиям безопасности и которые могут привести к выходу из строя терминала или ухудшению его технических характеристик.

2.1 Механические факторы

- Не устанавливайте терминал вблизи источников вибраций и ударных воздействий. Терминал может устанавливаться в местах с незначительным уровнем ударных воздействий, например, вблизи близко расположенных хлопающих дверей.
- Избегайте механических воздействий, которые могут привести к повреждению корпуса терминала и попаданию внутрь жидкости, пыли, насекомых, посторонних предметов.
- Не используйте абразивные или химически активные материалы для очистки наружных поверхностей терминала.
- Избегайте механических воздействий, которые могут привести к повреждению поверхности биометрического сканера (например, к появлению царапин и сколов).

2.2 Климатические факторы

- Используйте терминал при значениях температуры окружающей среды и относительной влажности воздуха, указанных в технических характеристиках.
- Не используйте терминал под прямыми солнечными лучами или в непосредственной близости от ярких источников света во избежание перегрева терминала или ухудшения качества сканирования биометрических данных (вследствие оптической помехи).
- Не используйте терминал в непосредственной близости от источников пламени.
- Поверхность биометрического сканера терминала должна быть защищена от воздействия атмосферных осадков (дождя). Дождь, попадающий на поверхность биометрического сканера, может привести к искажению светового сигнала и ухудшению качества сканирования биометрических данных.
- Терминал допускается эксплуатировать в условиях, соответствующих степени защиты корпуса IP65, при соблюдении требований по обеспечению пылевлагозащиты, обеспечении целостности корпуса. Пример допустимых воздействий на корпус с точки зрения степени защиты IP65: пыль, брызги, дождь, струи воды. Недопустимыми воздействиями являются: горячие струи воды под высоким давлением, погружение в воду.
- Не используйте терминал в средах с коррозионно-активными агентами, в условиях морского (соляного) тумана.
- Не используйте терминал в среде с высокой концентрацией статической или динамической пыли (песка). Слой пыли (песка), скапливающийся на поверхности биометрического сканера, может привести к искажению светового сигнала и ухудшению качества сканирования биометрических данных. Частицы песка могут оказывать абразивное воздействие на поверхность биометрического сканера, что также приведёт к ухудшению качества сканирования.

2.3 Биологические факторы

- Не используйте терминал в условиях воздействия плесневелых грибов, насекомых, животных.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.4 Электромагнитные поля и электрический ток

- Используйте терминал только при напряжении питания, указанном в технических характеристиках.
- Не используйте терминал вблизи источников сильных электромагнитных полей, которые могут привести к выходу терминала из строя или ухудшению работы электронных компонентов.
- При эксплуатации терминала должна обеспечиваться молниезащита линий связи и электропитания.

2.5 Дополнительные ограничения

- Не используйте терминал во взрывоопасных помещениях или иных местах, в которых возникновение разрядов статического электричества или искр может стать источником возгорания.
- Не допускается неквалифицированное вмешательство в конструкцию терминала лиц, не уполномоченных производителем.

Требования к условиям эксплуатации, приведённые в настоящем руководстве по эксплуатации, учитывают типичные факторы, влияющие на работу терминала. На объекте эксплуатации могут существовать или возникнуть в процессе эксплуатации факторы, не поддающиеся предварительному прогнозу, которые предприятие-изготовитель не могло учесть при разработке. В случае проявления подобных факторов следует согласовать допустимость эксплуатации терминала при воздействии проявившихся факторов или найти другое место для эксплуатации, где данные факторы отсутствуют или не оказывают влияния на работу терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3 МОНТАЖ BIOSMART PV-WTC

3.1 Меры безопасности

Перед началом монтажа прочитайте указанные ниже правила!

- Не производите монтаж, пусконаладочные работы терминала при грозе, ввиду опасности поражения электрическим током при грозовых разрядах от наводок на линии связи.
- Терминал должен эксплуатироваться с устройством молниезащиты.
- Не устанавливайте терминал во взрывоопасных помещениях или иных местах, в которых возникновение разрядов статического электричества или искр может стать источником возгорания.
- Все работы по монтажу и подключению терминала выполняйте только при отключенном напряжении электропитания во избежание поражения электрическим током.
- Убедитесь в отсутствии механических повреждений терминала.
- Любые удлинения кабелей производите методом пайки либо обжимки.

Не допускается производить удлинение методом скрутки!

3.2 Рекомендации

- Перед установкой терминала ознакомьтесь с эксплуатационными ограничениями.
- Терминал рекомендуется устанавливать только на вертикальной поверхности на высоте **150-170 см от пола**, исходя из соображения удобства позиционирования ладони на сканере, предъявления RFID карты, просмотра событий на ЖК экране. К терминалу должен быть обеспечен свободный и беспрепятственный доступ для удобного позиционирования руки.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Правила прикладывания ладони к сканеру терминала



Высота установки терминала и удобство прикладывания ладони оказывают существенное влияние на результат идентификации. Если сотруднику не удобно прикладывать ладонь к терминалу, приходится изгибать руку или продавливать ладонь, то рисунок вен ладони искажается и вероятность ошибки идентификации повышается.

- Рекомендуется оставлять запас длины кабелей, подключенных к терминалу, достаточный для отведения терминала от стены и доступа к перемычкам.
- Не устанавливайте терминал и не прокладывайте подключаемые к нему кабели вблизи источников электромагнитных помех.
- Пересечение сигнальных кабелей с силовыми выполняйте под прямым углом.
- Установите наконечники на все подключаемые кабели.

Для оптимальной регистрации ладоней:
1. Регистрируйте по 4 шаблона каждой ладони (4 левых и 4 правых), то есть по 8 шаблонов на каждого сотрудника.
2.Добивайтесь высокого качества шаблонов: 60-70 и более.

В таблице ниже приведены рекомендуемые максимальные длины линий связи, типы кабелей и наконечников.
Для обеспечения пылевлагозащиты необходимо выполнить указания по обеспечению пылевлагозащиты.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Терминал исполнения **BioSmart PV-WTC-EM-L** существенно ограничен в возможности подключения сторонних устройств. Перед монтажом терминала **BioSmart PV-WTC-EM-L** ознакомьтесь с описанием этого терминала и особенностями его подключения, приведенными в Монтаж и подключение терминала BioSmart PV-WTC-EM-L.

Кабельное соединение	Рекомендуемая максимальная длинна*	Тип кабеля	Тип наконечника
Сетевое устройство – терминал (по интерфейсу Ethernet)	100 м	Четыре витые пары не ниже пятой категории	8P8C
Источник питания 12 В – терминал	8 м	Кабель ШВВП сечением 0,5 мм^2	НШВИ
Источник PoE IEEE 802.3af class 3 – терминал	100 м	Четыре витые пары не ниже пятой категории	8P8C
Терминал – электрозамок	20 м	Тип и сечение кабеля зависят от мощности замка. Рекомендуется сечение не менее 2x1 мм^2	НШВИ
Терминал (дискретные входы) – внешние устройства (кнопки, датчики)	10 м	Сигнальные кабели сечением от 0,2 мм^2 (например, КСВВГ)	НШВИ
Терминал – внешние устройства (по интерфейсу Wiegand)	20 м**	Витая пара не ниже пятой категории с сечением проводов не менее 0,2 мм^2	НШВИ
Терминал – внешние устройства (по интерфейсу RS-485)	500 м	Кабель промышленного интерфейса RS-485 с сечением не менее 0,4 мм^2	НШВИ

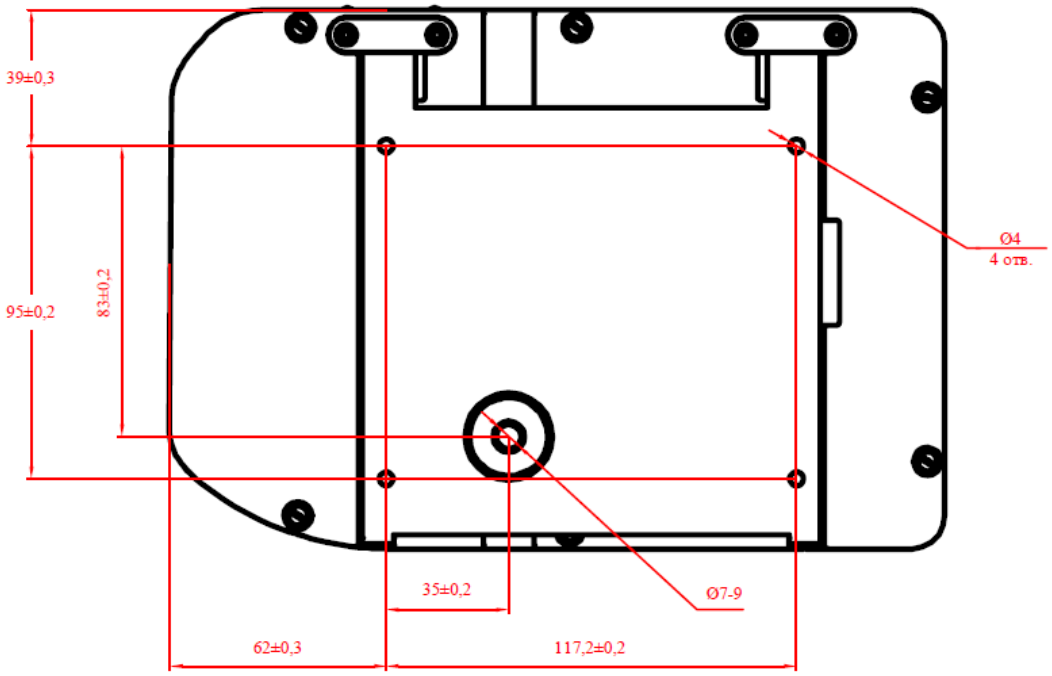
* Длина линии связи может быть увеличена или уменьшена относительно рекомендуемых значений в зависимости от условий монтажа и эксплуатации.

** Возможна реализация линии связи длиной до 100 метров при использовании витой пары FTP (F/UTP) с заземленным экраном и сечением проводов не менее 0,2 мм^2.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.3 Порядок монтажа

1. Распакуйте коробку и проверьте комплектность терминала.
2. Определите место установки терминала.
3. Выкрутите винты, расположенные в нижней части корпуса терминала и крепящие его к монтажной пластине. Снимите монтажную пластину.
4. Разметьте места крепления терминала, приложив монтажную пластину терминала к стене согласно рисунку ниже.



5. Проложите кабели и заведите их в отверстие в монтажной пластине.
6. Закрепите монтажную пластину терминала на установочной поверхности с помощью крепежа, входящего в комплект поставки или аналогичного.
7. Выкрутите винты, расположенные в задней части корпуса терминала, и снимите заднюю крышку.
8. Заведите кабели в отверстие для ввода кабелей в задней крышке терминала. Для обеспечения пылевлагозащиты терминала нужно использовать гермоввод (см. Особенности монтажа для обеспечения пылевлагозащиты).
9. Подключите терминал в соответствии со схемами, приведенными в Подключение BioSmart PV-WTC.
10. Присоедините заднюю крышку к терминалу и закрепите винтами.
11. Установите терминал на монтажную пластину и зафиксируйте его с помощью крепёжных винтов на нижнем торце пластины.
12. Снимите защитную пленку с клавиатуры и экрана.

3.4 Особенности монтажа для обеспечения пылевлагозащиты

Терминал BioSmart PV-WTC имеет степень пылевлагозащиты IP65, которая достигается за счёт использования влагозащищенного корпуса с герметизирующими элементами конструкции. Для обеспечения заявленной степени защиты при монтаже необходимо выполнение следующих правил:

- должна быть сохранена целостность корпуса терминала (трещины и сколы на корпусе могут привести к проникновению пыли и влаги);

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- электропитание терминала и подключение его к сети Ethernet должно выполняться с помощью **одного** кабеля UTP, фиксируемого посредством гермоввода (электропитание при этом должно поступать от PoE-инжектора);
- задняя крышка должна плотно прилегать к основанию корпуса терминала через уплотнительную резинку.

Терминал BioSmart PV-WTC может поставляется с гермовводом, установленным на задней крышке, или входящим в состав поставочного комплекта.
При отсутствии установленного гермоввода, его монтаж производится следующим образом:

- отсоедините заднюю крышку терминала;
- накрутите на штуцер гермоввода прижимную гайку со стороны зубчатой муфты, оставив отверстие достаточное для вставки фиксируемого кабеля;
- установите на штуцер гермоввода резиновое уплотнительное кольцо;
- вставьте штуцер гермоввода в отверстие для кабеля на задней крыше терминала так, чтобы уплотнительное кольцо оказалось плотно зажато между наружной стороной задней крышки и широкой частью штуцера;
- накрутите крепёжную гайку на резьбу штуцера, выступающую с обратной (внутренней) стороны задней крышки терминала.

Для монтажа кабеля при установленном гермовводе:

- вставьте необжатый конец кабеля в гермоввод и протяните кабель на необходимую длину, при необходимости предварительно ослабьте прижимную гайку;
- обожмите конец кабеля в соответствии с указаниями в Подключение терминала к сети Ethernet;
- плотно затяните прижимную гайку с наружной стороны задней крышки;
- вставьте разъём в порт Ethernet.

Установка задней крышки терминала выполняется следующим образом:

- приложите заднюю крышку к корпусу терминала. Убедитесь в том, что уплотнительная резинка не выпала из специальной выемки и плотно прижата выступом со стороны задней крышки;
- закрепите заднюю крышку с помощью винтов. Важно проконтролировать, чтобы в процессе затягивания винтов уплотнительная резинка не выдавилась из специальной выемки. Поэтому, затягивать винты на задней крышке следует осторожно, постепенно подкручивая каждый винт.

После выполнения вышеперечисленных указаний закончите монтаж терминала в соответствии с порядком монтажа, описанном в Порядок монтажа.

3.5 Монтаж и подключение терминала BioSmart PV-WTC-EM-L

- Монтаж терминала BioSmart PV-WTC-EM-L осуществляется так же, как и монтаж терминалов других исполнений, кроме подключения сторонних устройств. Подключение сторонних устройств не допускается конструкцией терминала BioSmart PV-WTC-EM-L.
- На плате терминала BioSmart PV-WTC-EM-L имеется разъём Ethernet для подключения к сетевому устройству. Если сетевое устройство оборудовано PoE-инжектором, то питание терминала можно осуществлять через разъём Ethernet. В противном случае, питание терминала обеспечивается через клеммы X9 от источника питания 12В.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Подключение терминала BioSmart PV-WTC-EM-L к сети Ethernet выполняется в соответствии Подключение терминала к сети Ethernet.
- Подключение терминала BioSmart PV-WTC-EM-L к источнику питания выполняется в соответствии с Подключение питания терминала.
- Настройки сетевых параметров терминала BioSmart PV-WTC-EM-L выполняется в соответствии с Настройка сетевых параметров терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

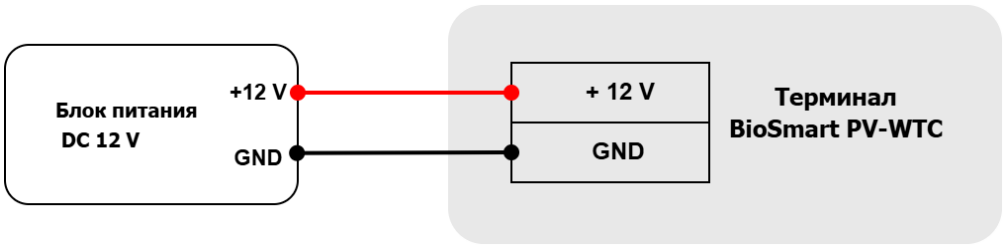
4 ПОДКЛЮЧЕНИЕ BIOSMART PV-WTC

В разделе приведены основные схемы подключения.

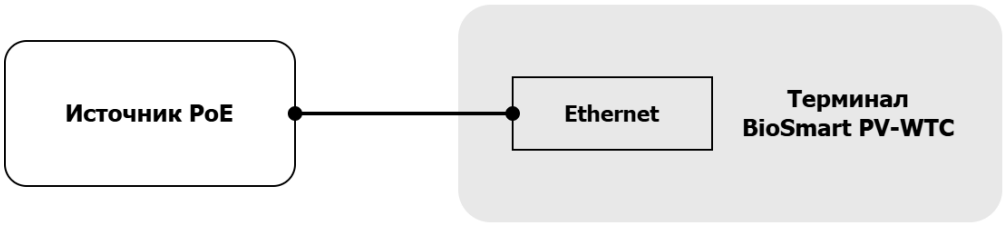
Все работы по подключению контроллера выполняйте только при отключенном напряжении электропитания во избежание поражения электрическим током!

4.1 Подключение питания терминала

Подключение терминала к источнику питания выполняется в соответствии со схемой, представленной на рисунке ниже.

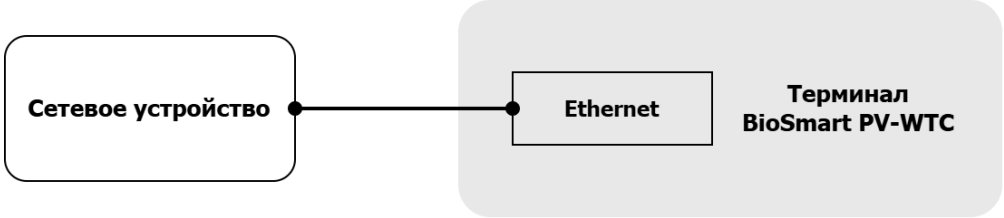


Подключение терминала к источнику PoE осуществляется через разъём Ethernet, в соответствии со схемой, приведенной ниже.



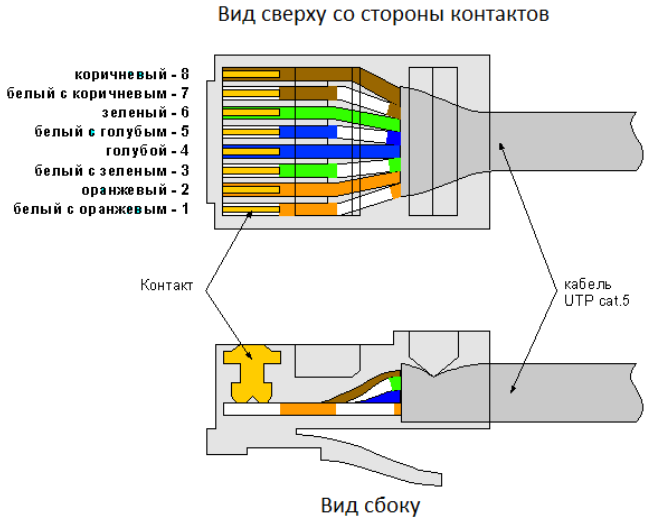
4.2 Подключение терминала к сети Ethernet

Подключение к сети Ethernet производите согласно рисунку ниже. Для обеспечения степени защиты IP65, обжимку кабеля следует производить после пропуска его через гермоввод. Если степень защиты IP65 не требуется, гермоввод можно предварительно снять. В этом случае обжим кабеля можно проводить без пропуска его через отверстие в крышке терминала.



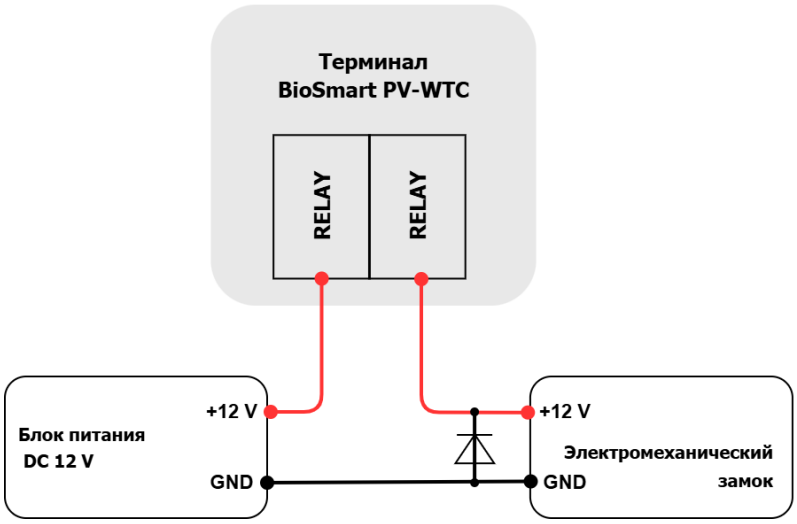
Обжимку наконечника кабеля нужно производить по стандарту TIA/EIA-568-B, согласно рисунку ниже:

SEC.RU | Короткий путь к информации
Скачано с sec.ru



4.3 Подключение электромеханического замка

Электромагнитный замок подключается к реле терминала в соответствии со схемой ниже.

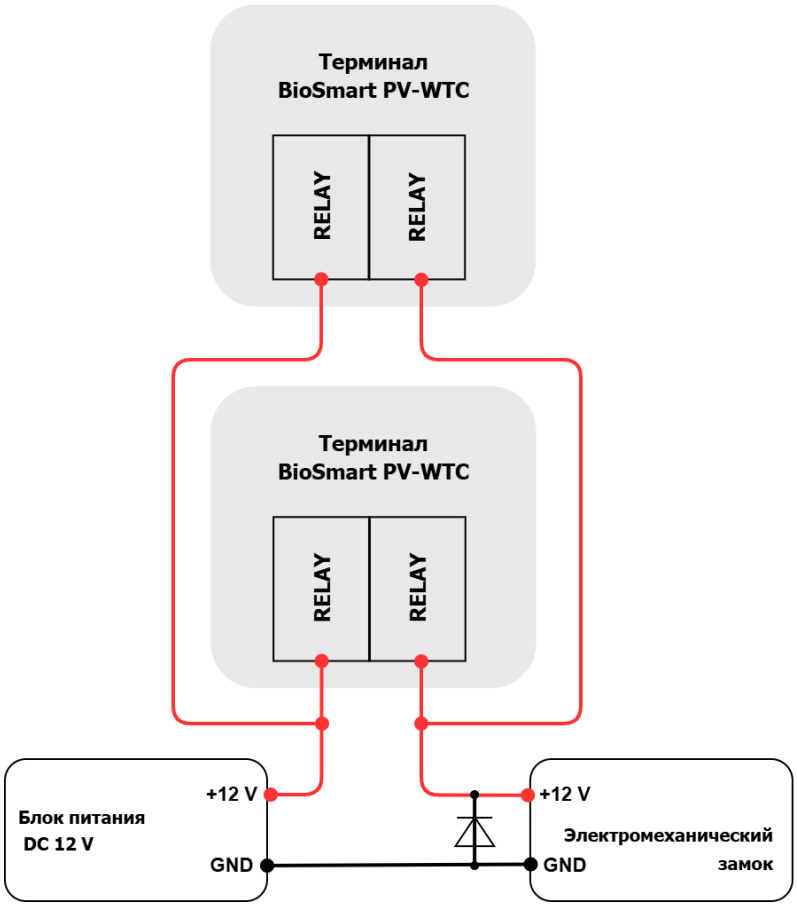


Питание электрозамков должно осуществляться от внешнего источника напряжения.
Не рекомендуется использовать один и тот же источник питания для подключения замка и терминала!

Для защиты встроенного реле от обратного тока, возникающего в цепи при срабатывании замка, необходимо установить шунтирующий диод в соответствии со схемами. Рекомендуется использовать диод типа 1N4007 (входит в комплект поставки) или аналогичный.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Для управления одним электромеханическим замком с двух терминалов подключите их в соответствии со схемой, изображенной на рисунке ниже:

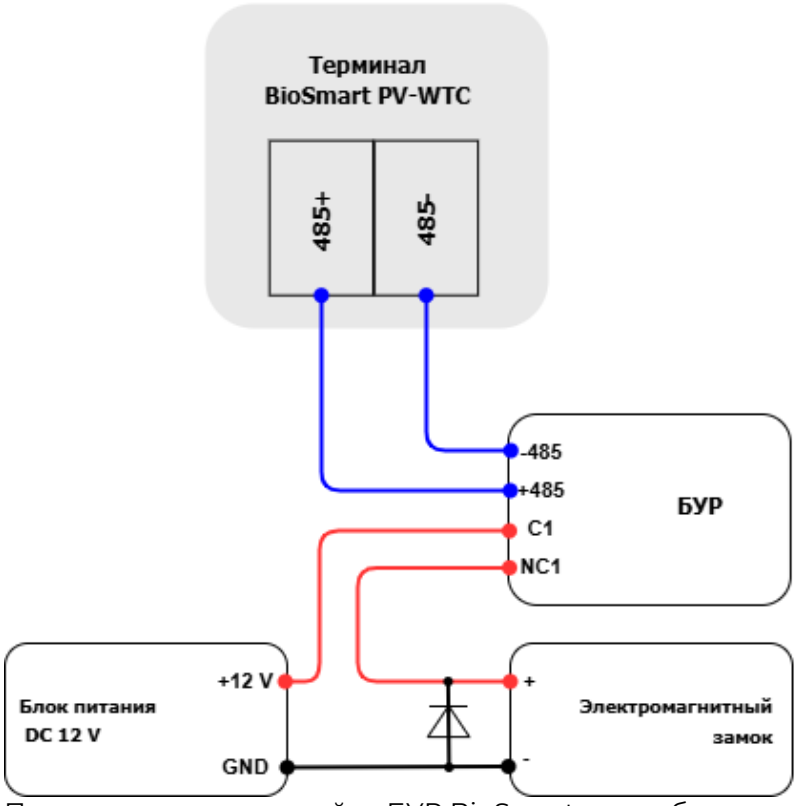


4.4 Подключение электромагнитного замка через БУР BioSmart

На терминале BioSmart PV-WTC используются нормально разомкнутые контакты реле, поэтому терминал может управлять электромагнитным замком только с помощью блока управления реле БУР BioSmart. Схема подключения приведена на рисунке ниже:

Для защиты реле БУР BioSmart от обратного тока, возникающего в цепи при срабатывании замка, требуется установить шунтирующий диод, согласно схеме, приведенной на рисунке ниже. Рекомендуется использовать диод типа 1N4007 (1A,100B) или аналогичный.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

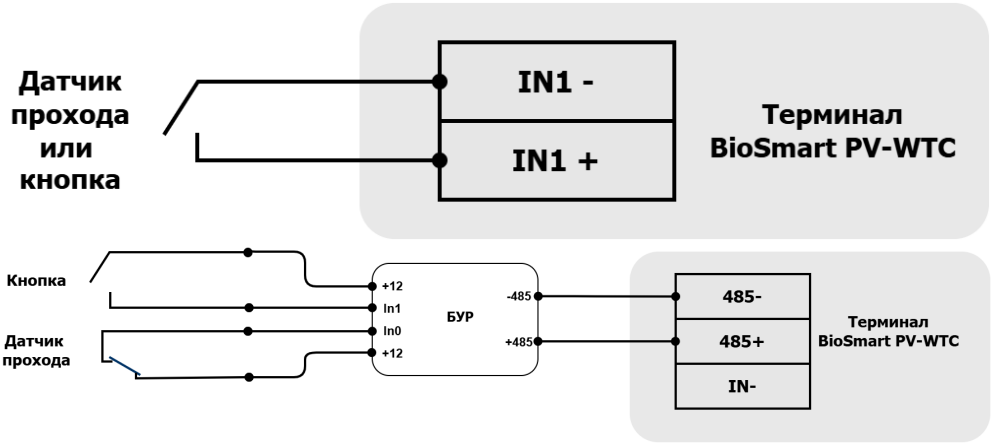


Подключение и настройка БУР BioSmart подробно описаны в Руководстве по эксплуатации БУР BioSmart. Всю необходимую информацию можно найти на сайте www.bio-smart.ru в разделе «Технический портал».

4.5 Подключение датчика прохода и кнопки управления

Датчик прохода или кнопку выхода из помещения можно подключить непосредственно к бортовому дискретному входу BioSmart PV-WTC, согласно схеме, приведенной на рисунке ниже.

Если для организации контроля и управления доступом требуется совместное применение датчика прохода и кнопки выхода из помещения, то необходимо производить подключение с использованием устройства БУР BioSmart, согласно схеме, приведенной на рисунке ниже.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

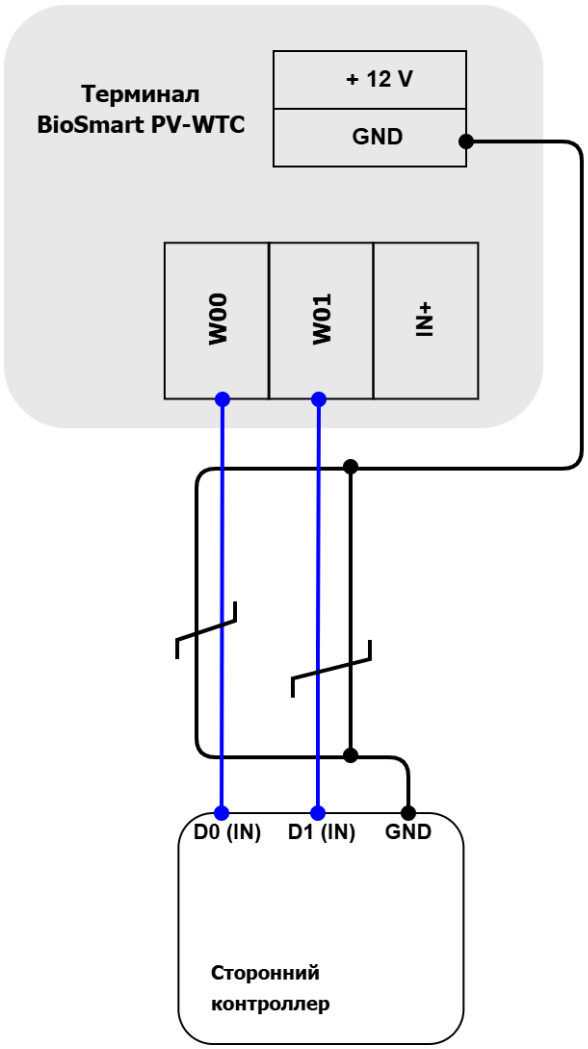
Питание электрозамков должно осуществляться от внешнего источника напряжения.

Не рекомендуется использовать один и тот же источник питания для подключения замка и терминала.

Подключение и настройка БУР BioSmart подробно описаны в Руководстве по эксплуатации БУР BioSmart. Всю необходимую информацию можно найти на сайте www.bio-smart.ru в разделе «Технический портал».

4.6 Подключение к стороннему контроллеру по Wiegand

Подключение терминала к стороннему контроллеру СКУД по интерфейсу Wiegand производится, согласно схеме, приведенной на рисунке ниже.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7 Подключение к алкотестеру Динго B-02

Подключение к алкотестеру Динго B-02 производите согласно рисунку ниже.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

5 БЫСТРЫЙ СТАРТ ТЕРМИНАЛА BIOSMART PV-WTC

В разделе описан минимальный необходимый перечень настроек, которые следует выполнить для начала работы с терминалом.

Приступать к настройке терминала следует только после монтажа (см. раздел Монтаж) и подключения (см. раздел Подключение).

Выполните настройку в следующем порядке:

1. Настройте сетевые параметры терминала

Подайте питание на терминал. Дождитесь включения экрана.

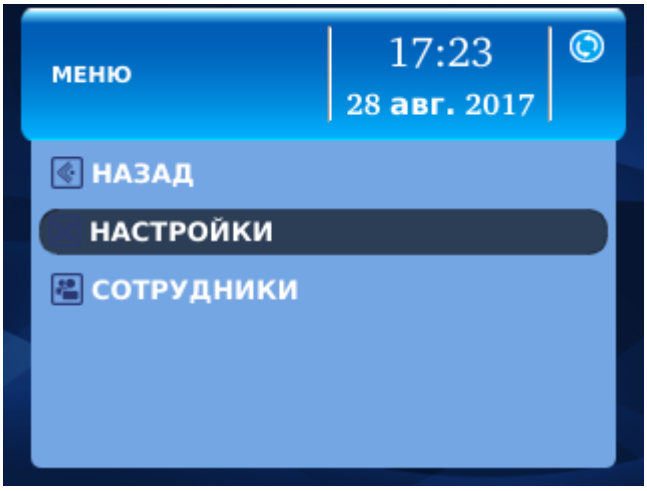
Заводские настройки пароля администратора – пустой пароль.

После первого входа в режим настроек рекомендуется установить новый пароль для исключения в дальнейшем несанкционированного доступа к настройкам терминала.

Используя навигационные клавиши, войдите в основное меню терминала и выберите **Меню**.



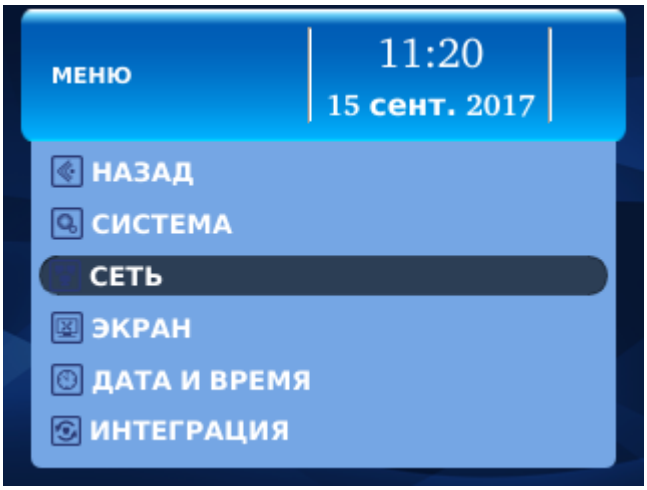
Выберите раздел **Настройки.**



SEC.RU | Короткий путь к информации
Скачано с sec.ru

С помощью навигационных клавиш выберите пункт **Сеть.**

Неправильно заданный адрес шлюза может быть причиной проблем с подключением к Biosmart-Studio v6.

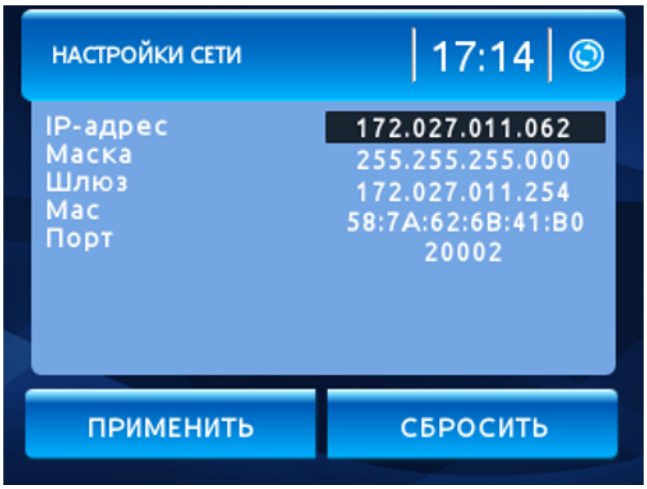


Выберите в списке раздел «**IP адрес**», нажмите .

Введите с клавиатуры требуемый IP адрес, нажмите

Таким же образом введите требуемые настройки сетевой маски и шлюза (в случае отсутствия шлюза – IP сервера Biosmart-Studio).

Перейдите на кнопку «**Применить**» и нажмите .

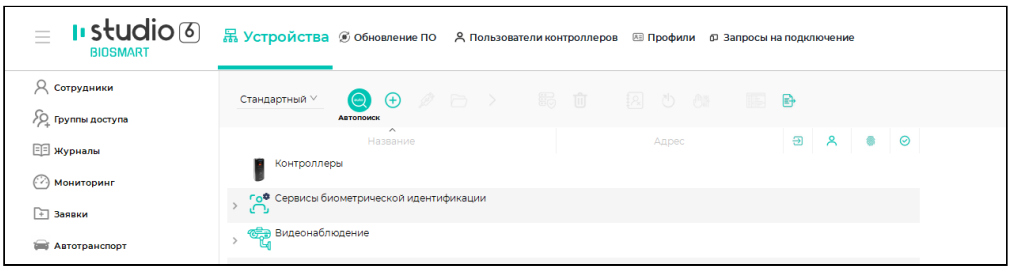


После этого новые сетевые настройки вступят в силу.

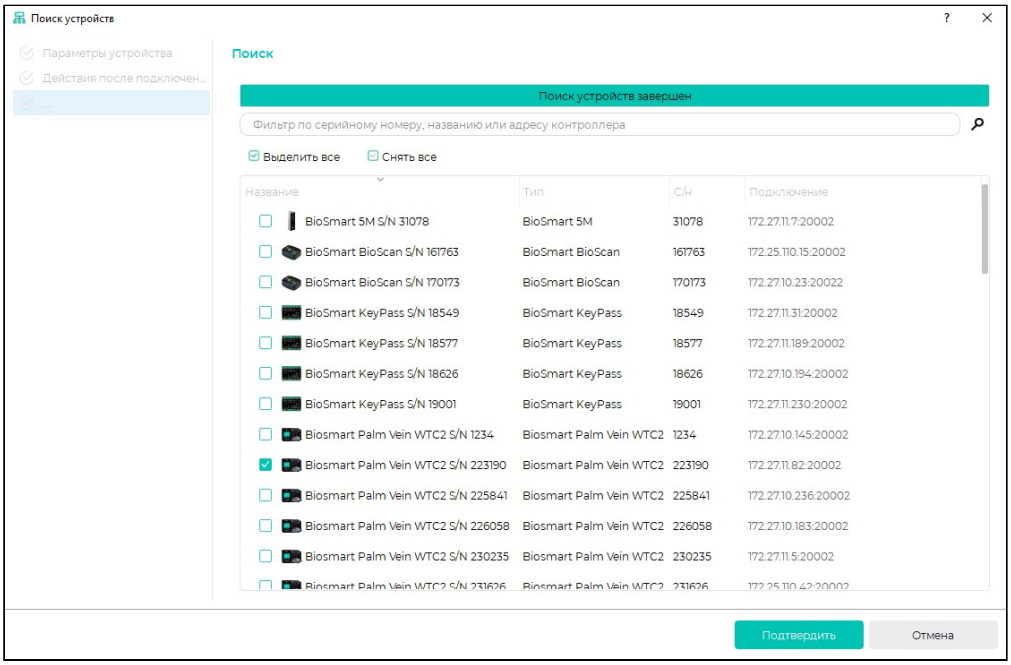
SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. Добавьте терминал в ПО Biosmart-Studio v6

В ПО Biosmart-Studio v6 в разделе **Устройства** нажмите кнопку **Автопоиск**.

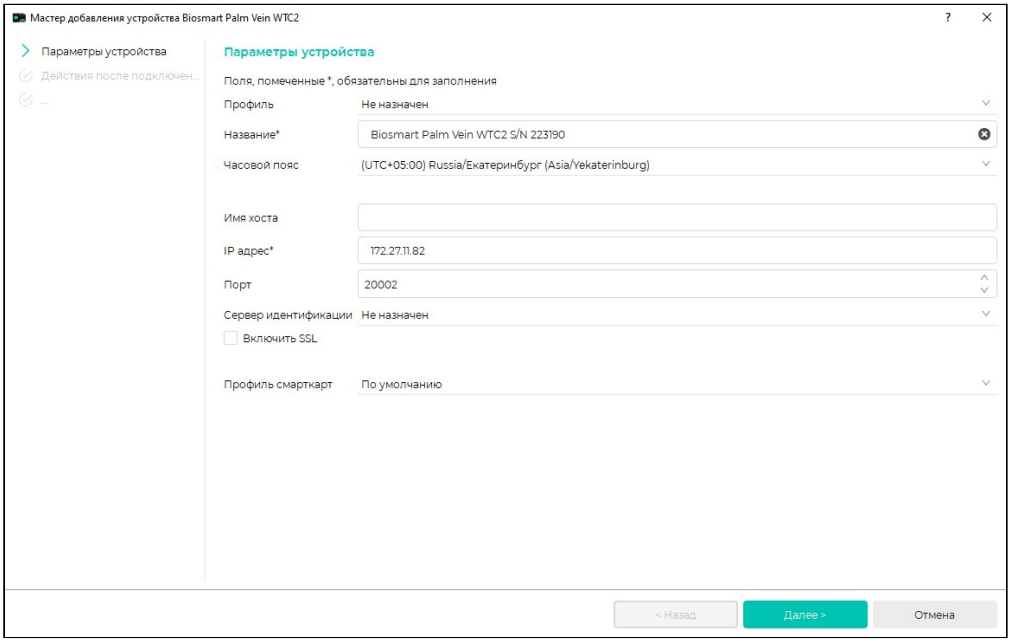


В списке устройств найдите терминал по серийному номеру, заполните чекбокс и нажмите **Подтвердить**.

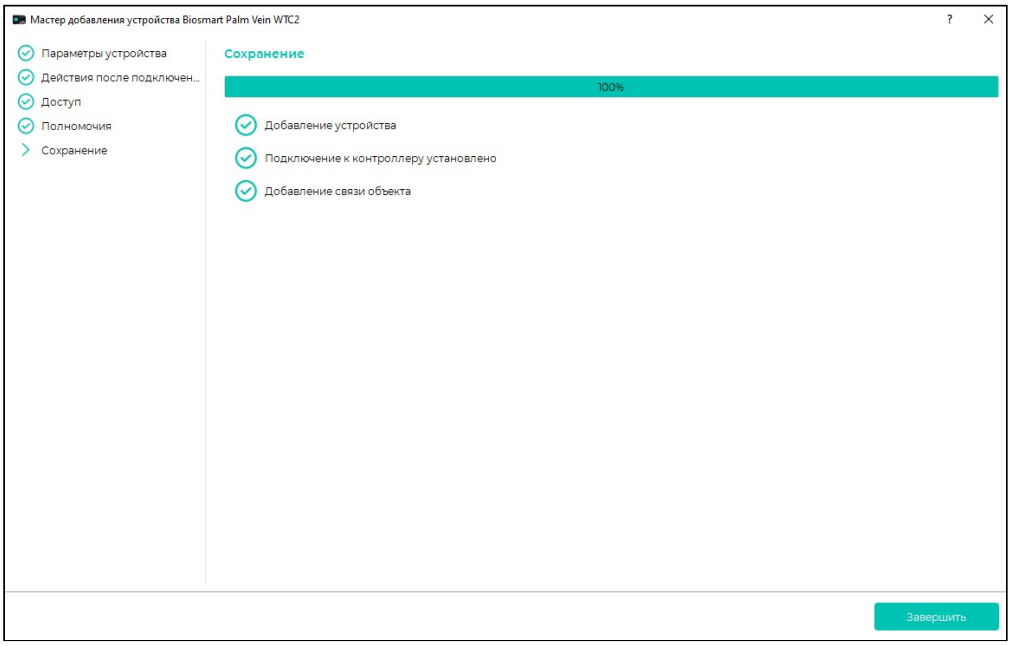


В окне **Мастер добавления устройства** нажмите **Далее**, затем **Завершить** (при необходимости изменить настройки можно будет позже).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

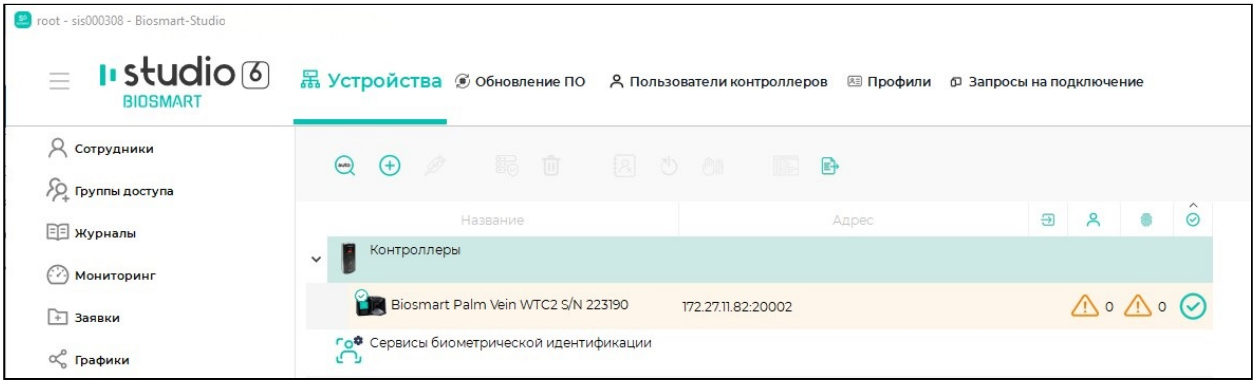


В окне **Сохранение** дождитесь добавления и подключения терминала и нажмите **Завершить**.



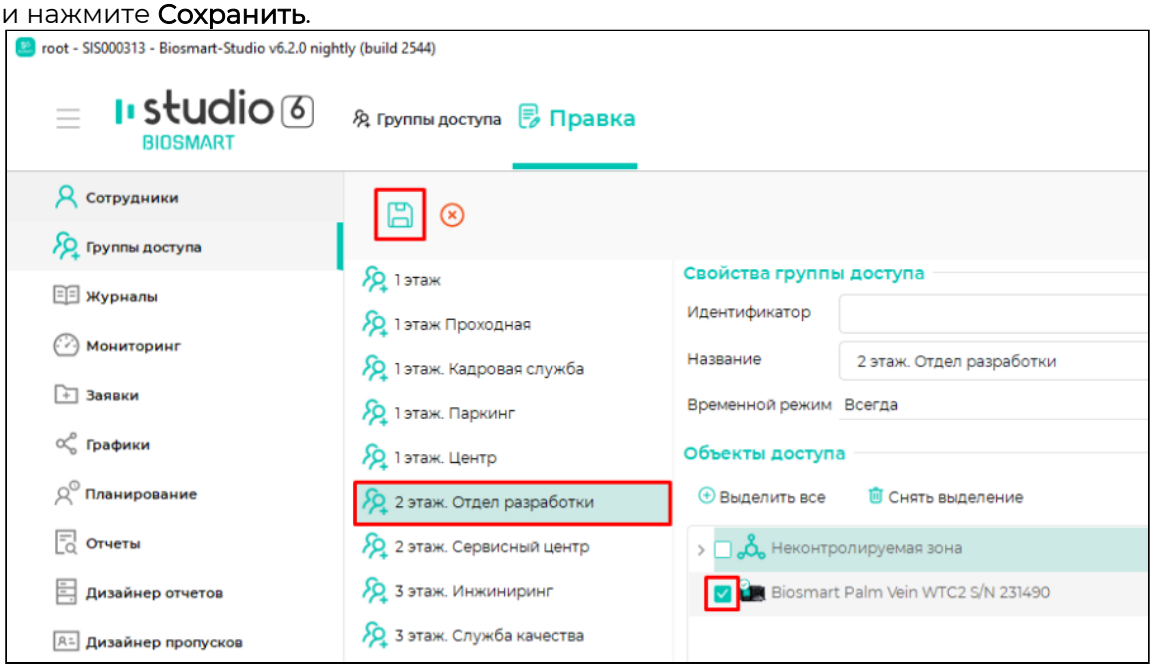
После успешного добавления терминал будет показан в списке устройств со значком **В сети** .

SEC.RU | Короткий путь к информации
Скачано с sec.ru

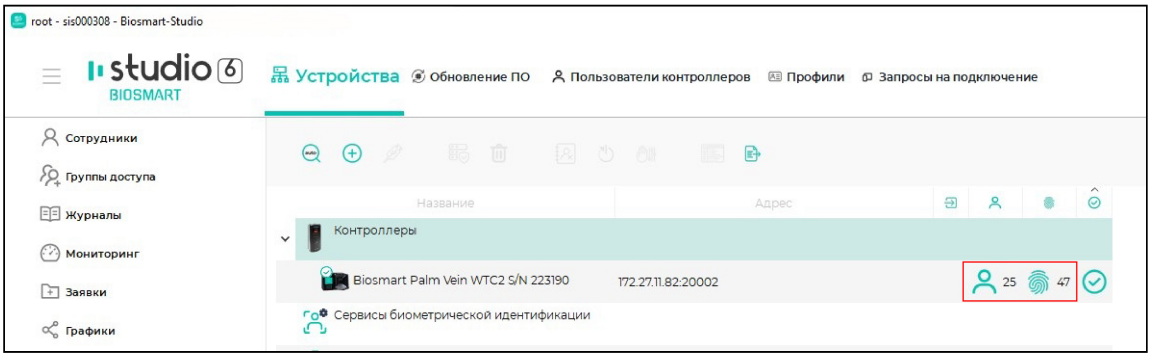


3. Загрузите на терминал список сотрудников из ПО Biosmart-Studio v6

В ПО Biosmart-Studio v6 в разделе **Группы доступа** выберите группы доступа, терминал и нажмите **Сохранить**.



После назначения группы доступа в строке с названием терминала будет показано количество сотрудников и шаблонов вен ладоней в памяти терминала.

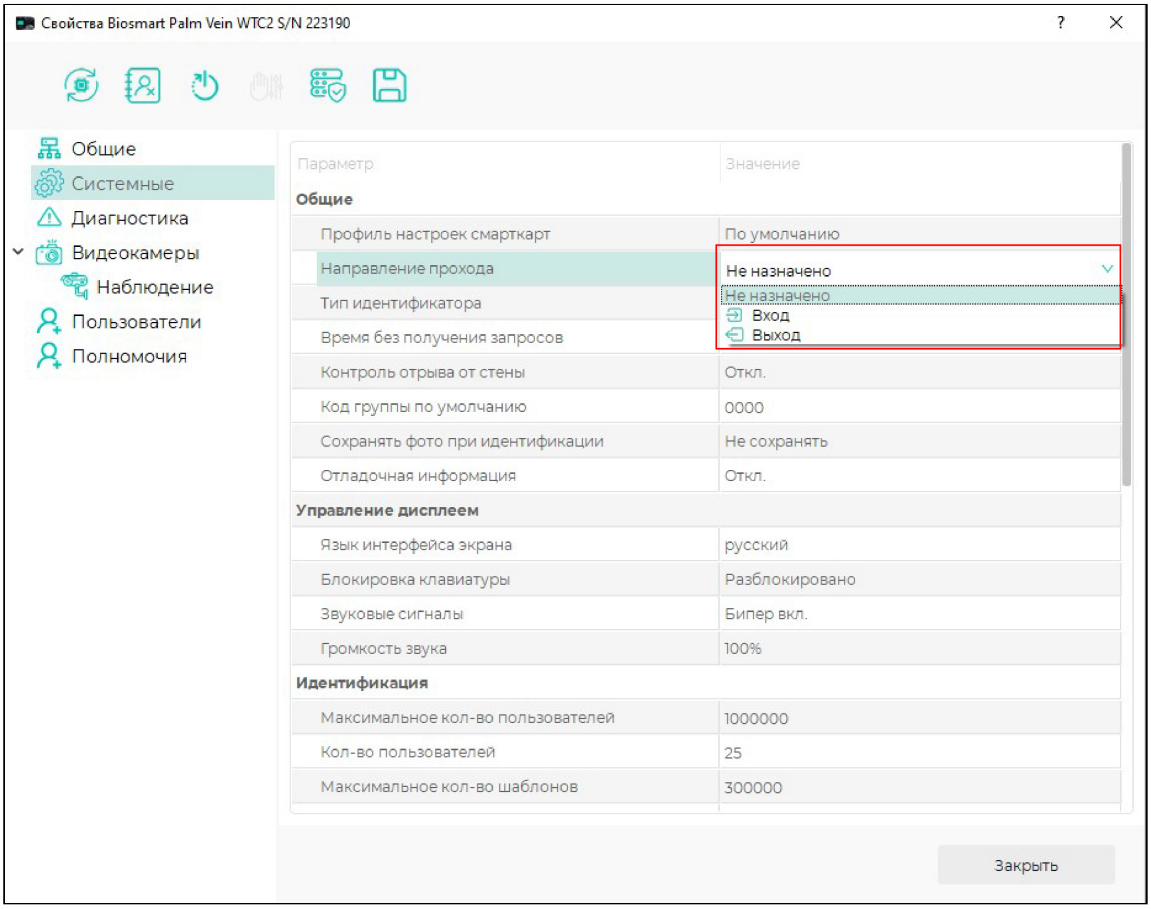


SEC.RU | Короткий путь к информации
Скачано с sec.ru

4. Выберите направление прохода

Параметр **Направление прохода** применяется при учёте рабочего времени для автоматического назначения направления движения сотрудников (вход на объект/ выход с объекта) при идентификации на терминале. В зависимости от значения параметра **Направление прохода** при успешной идентификации в ПО Biosmart-Studio v6 будет формироваться событие «**Вход сотрудника**» / «**Выход сотрудника**» или «**Идентификация сотрудника успешна**».

Для выбора направления прохода откройте в ПО Biosmart-Studio v6 окно **Свойства Biosmart Palm Vein WTC2** на вкладке **Системные**. Выберите значение параметра **Направление прохода** и нажмите **Сохранить.**

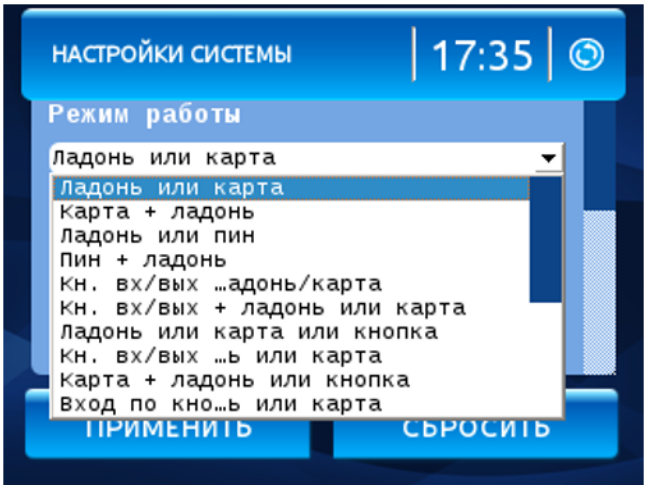


5. Выберите рабочую модель

Терминал имеет ряд предустановленных рабочих моделей, отвечающих наиболее частым сценариям использования.

В меню терминала перейдите в **Настройки** – **Система** и выберите значение параметра **Режим работы**.

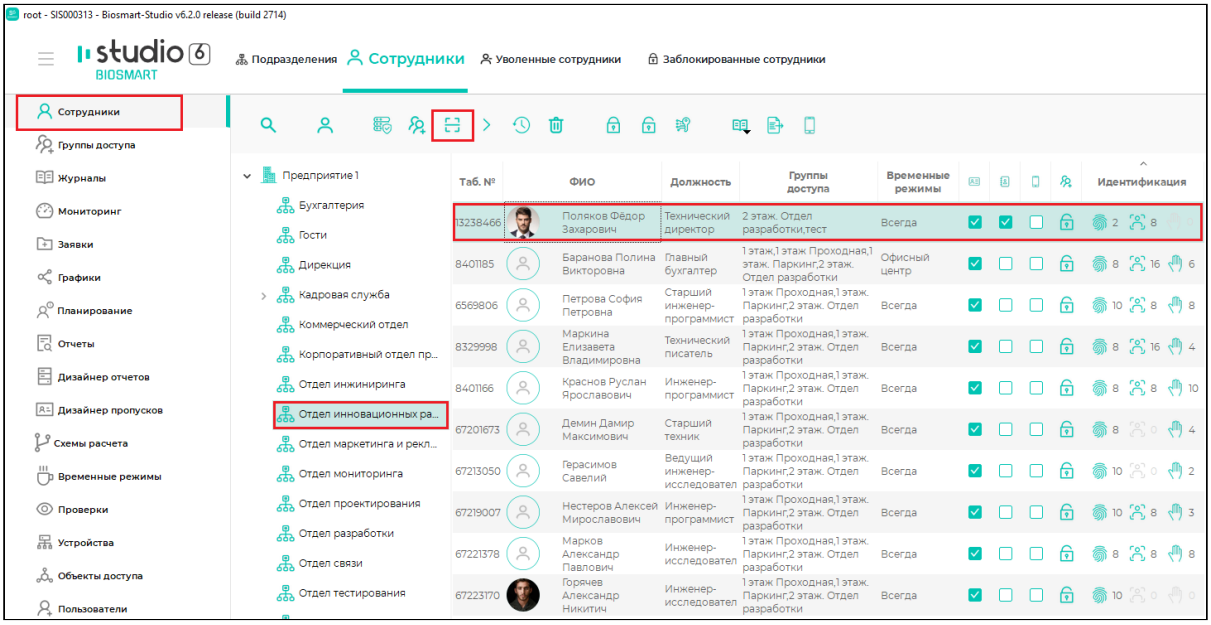
SEC.RU | Короткий путь к информации
Скачано с sec.ru



Также рабочую модель можно выбрать из предустановленных в ПО Biosmart-Studio v6 или создать свою в веб-интерфейсе терминала. Описание предустановленных рабочих моделей приведено в Предустановленные рабочие модели, описание создания рабочих моделей приведено в Создание простой рабочей модели.

6. Зарегистрируйте идентификаторы сотрудников

Для регистрации шаблонов вен ладоней сотрудников выполните следующие действия: Перейдите в раздел **Сотрудники** → выберите сотрудника → нажмите кнопку **Сканировать → Ладони.**



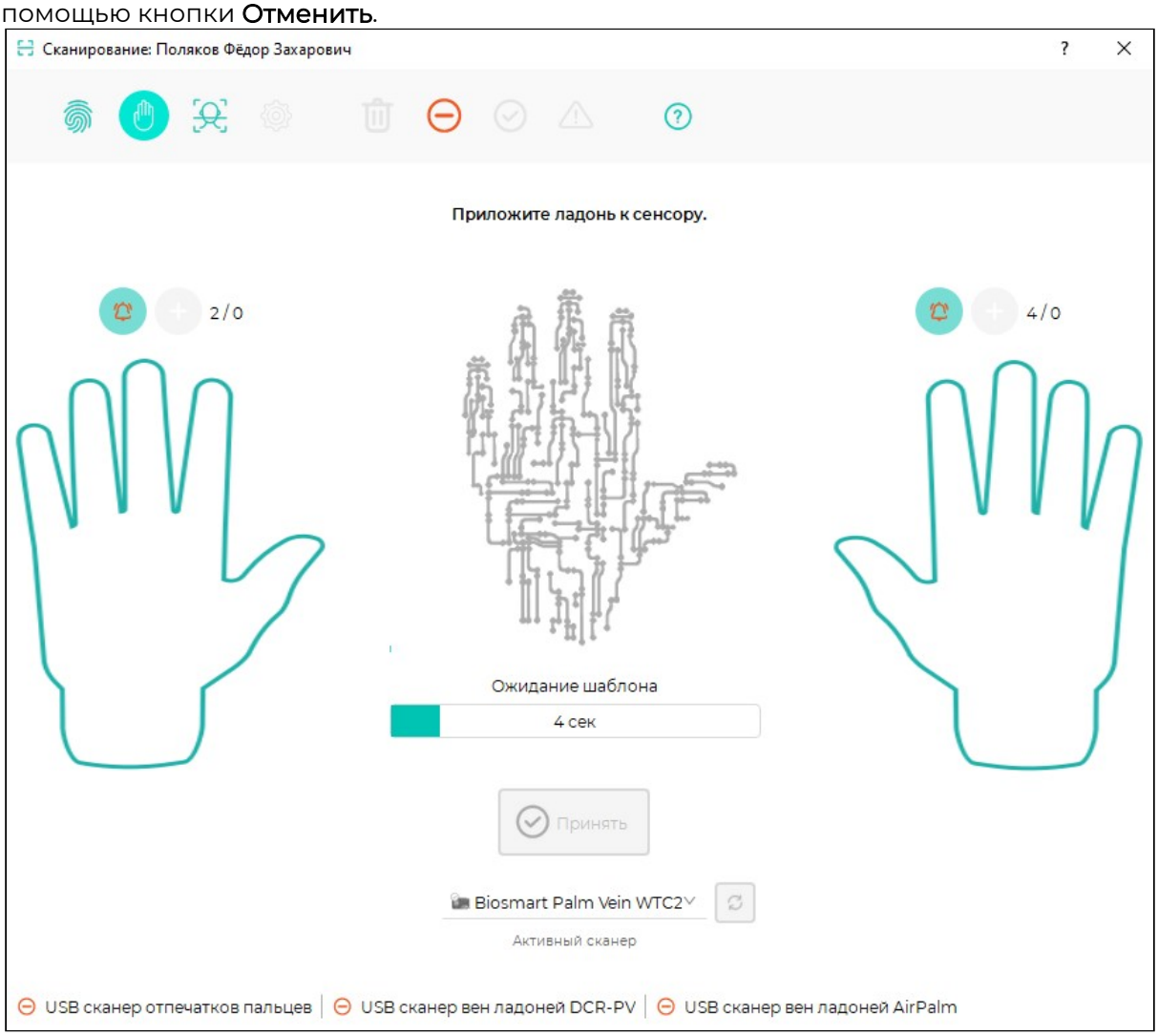
В качестве устройства, с которого будет производиться регистрация рисунка вен ладоней, из выпадающего списка выберите **BioSmart Palm Vien WTC2**.

Выберите ладонь, которая будет регистрироваться, и нажмите кнопку  над изображением этой ладони.

Появится сообщение: «**Приложите ладонь к сенсору**».
Если в течение 24 секунд ладонь не появится перед терминалом, то регистрация

SEC.RU | Короткий путь к информации
Скачано с sec.ru

шаблонов будет отменена. Прервать процесс регистрации в любой момент можно с помощью кнопки **Отменить**.



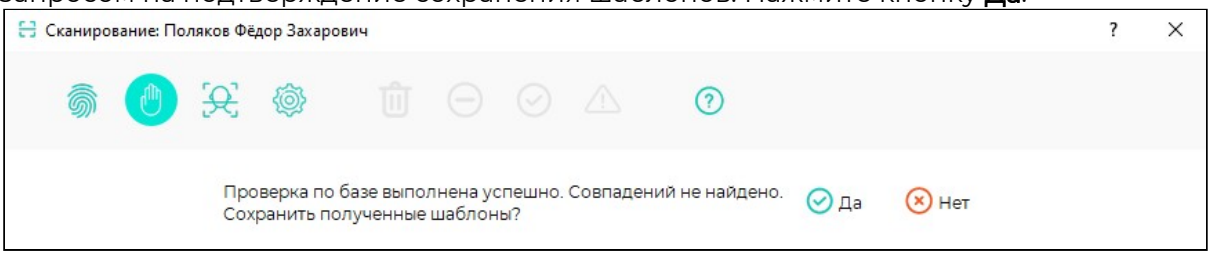
После появления на экране терминала сообщения **Приложите ладонь к сенсору** необходимо поднести ладонь к сканеру в соответствии с нижеперечисленными правилами:

- ладонь раскрыта естественным образом, большой палец отодвинут от ладони;
- центр ладони располагается над центром биометрического сканера;
- запястье лежит на нижней части держателя ладони.

Следуйте указаниям, появляющимся на дисплее терминала.
Если совпадений с шаблонами других сотрудников не найдено, появится сообщение с

SEC.RU | Короткий путь к информации
Скачано с sec.ru

запросом на подтверждение сохранения шаблонов. Нажмите кнопку **Да**.

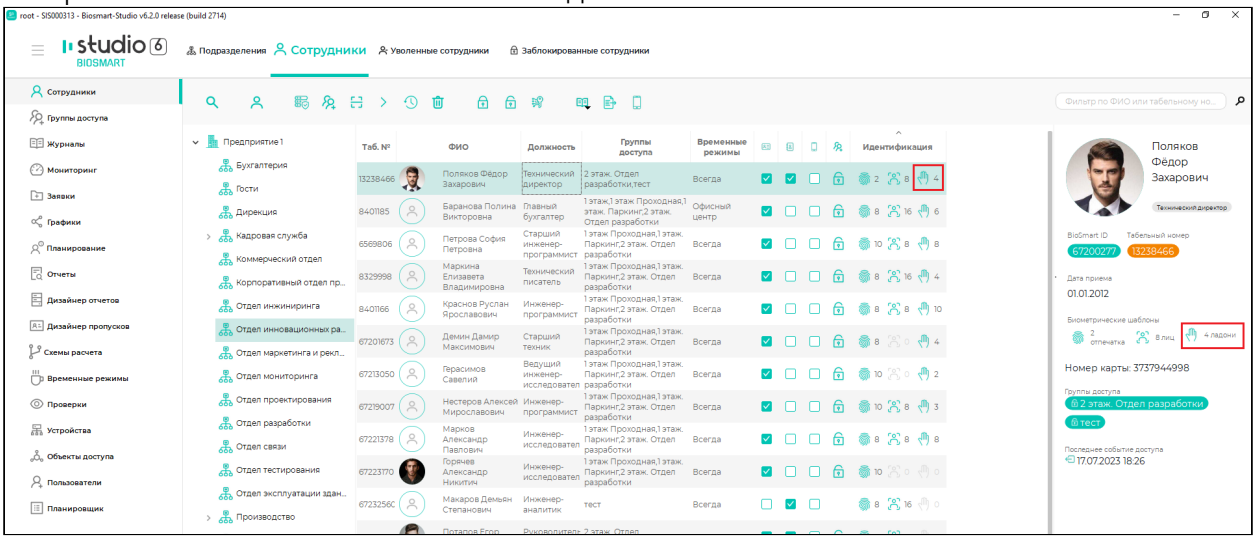


> Если совпадения обнаружены, то появится сообщение о наличии совпадений биометрических данных сотрудников, сохранение полученных шаблонов будет запрещено.

Повторяя вышеперечисленные операции, занесите в базу шаблоны вен другой ладони, или закройте окно **Сканирование**.

Существует возможность назначить одну из ладоней сотрудника «тревожной». При успешной идентификации по этой ладони, формируется специальное событие «**Проход под принуждением**». В планировщике задач можно задать реакцию системы на это событие: выслать сообщение, включить реле и т. д. Для более подробной информации обратитесь к Руководству пользователя ПО Biosmart Studio v6.
Для удаления записанных шаблонов запустите процесс удаления шаблонов, для чего нажмите кнопку **Удалить**, затем выберите ладонь, у которой будут удалены шаблоны и повторно нажмите кнопку **Удалить**.

После успешной регистрации шаблонов вен ладоней в свойствах сотрудника будет отображаться наличие шаблонов вен ладоней и их количество.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.1 Регистрация RFID-карт

Для идентификации с помощью RFID-карт необходимо назначить карты доступа сотрудникам.

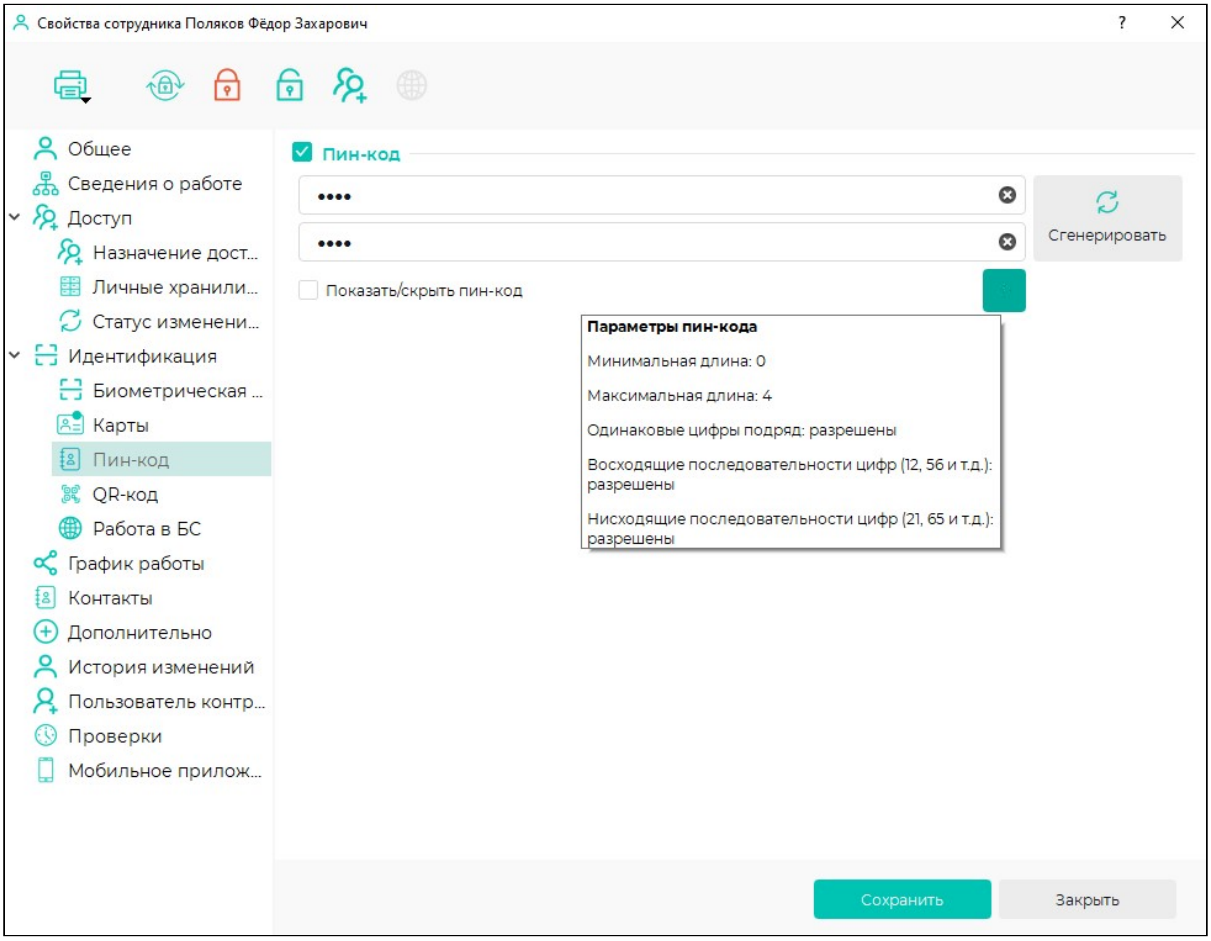
Зарегистрировать RFID-карту можно с помощью настольного считывателя RFID-карт или считывателя, подключённого к контроллеру. Порядок регистрации RFID-карт приведен в Руководстве пользователя ПО Biosmart-Studio.

- Если в качестве идентификатора будут применяться карты *Mifare Plus SL1 и SL3*, то необходимо настроить систему согласно Работа в защищенном режиме.
- Если в качестве идентификатора будут применяться *смартфоны* с установленным приложением BioSmart ID, то необходимо выполнить настройки согласно разделу Работа со смартфонами в качестве идентификатора.
- Если идентификация будет выполняться по открытому UID карты, то необходимо настроить систему согласно Работа в незащищенном режиме, чтение UID.

5.2 Назначение сотрудникам пин-кодов

В ПО Biosmart-Studio v6 в разделе **Сотрудники** откройте окно **Свойства сотрудника** и перейдите на вкладку **Идентификация – Пин-код**.
Поставьте отметку в чекбоксе **Пин-код**.
Пин-код должен удовлетворять требованиям, заданным параметром **Сложность пин-кода** в справочнике **Общие параметры** (см. Руководство пользователя ПО Biosmart-Studio v6). Просмотреть требования к пин-коду можно, нажав кнопку  .

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Опция **Показать/скрыть пин-код** показывает либо скрывает цифры пин-кода.
Пин-код можно придумать самостоятельно либо сгенерировать автоматически. Для автоматического создания пин-кода нужно при выбранной опции **Показать/скрыть пин-код** нажать кнопку **Сгенерировать**, после чего в поле для ввода пин-кода появится последовательность, сгенерированная с учётом всех требований к пин-коду.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6 ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО ТЕРМИНАЛА

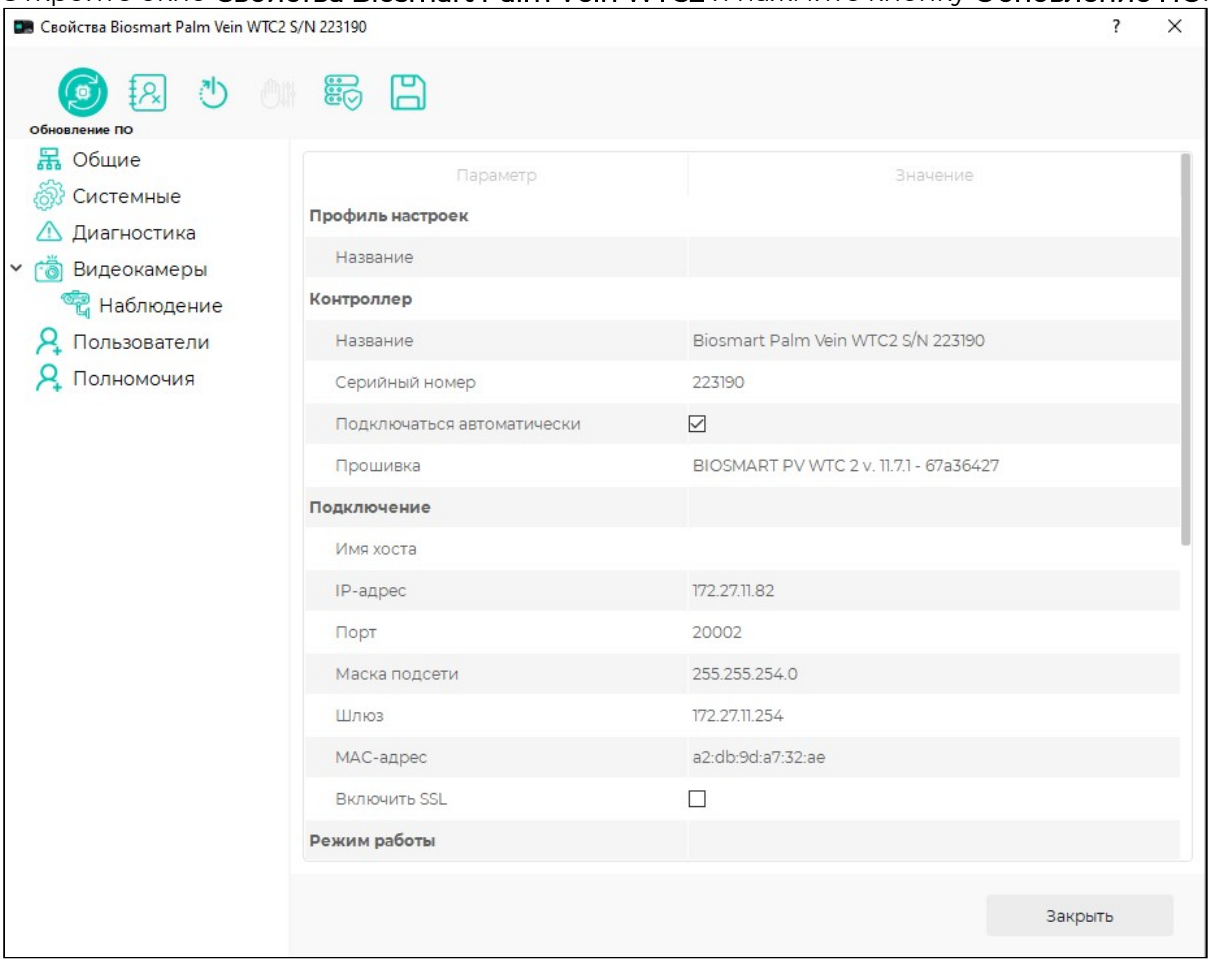
Обновить встроенное ПО терминала можно с помощью ПО Biosmart-Studio v6 или веб-интерфейса.

6.1 Обновление встроенного ПО с помощью ПО Biosmart-Studio v6

Запустить обновление из ПО Biosmart-Studio v6 можно в окне **Свойства Biosmart Palm Vein WTC2** или на вкладке **Обновление ПО** раздела **Устройства**.

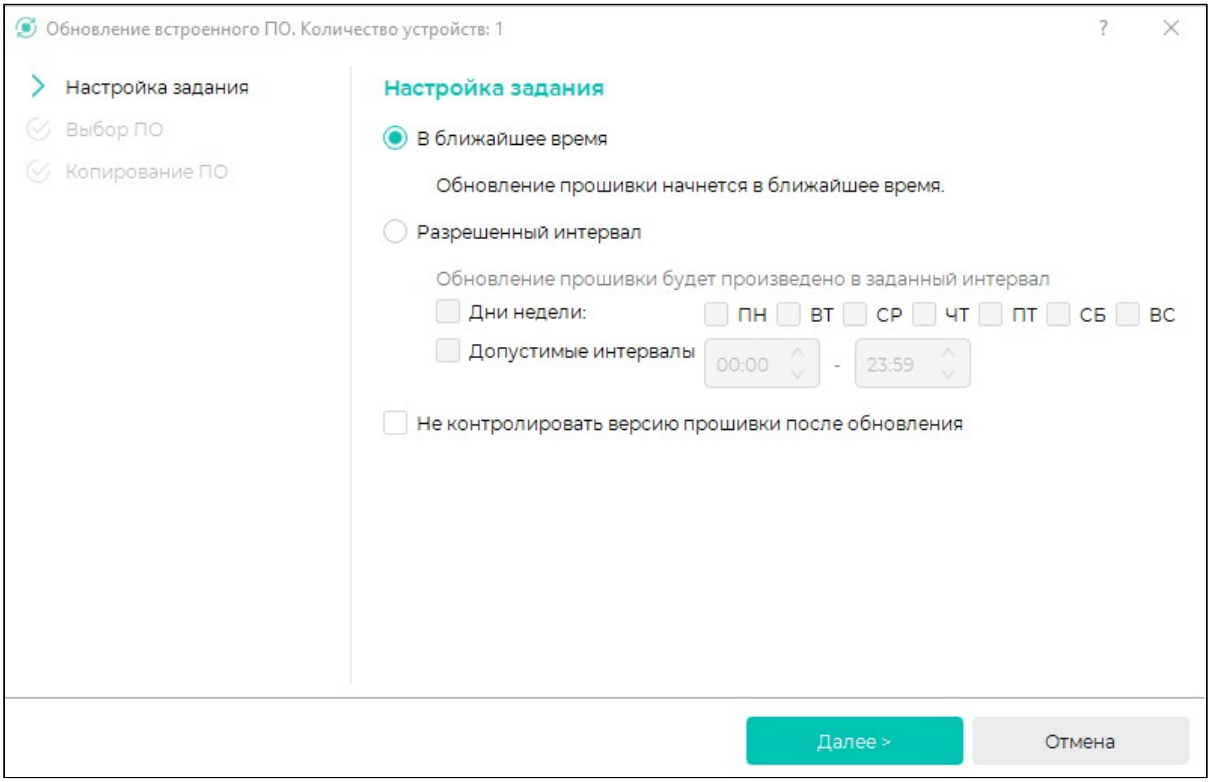
Вкладка **Обновление ПО** обычно используется для настройки обновлений сразу группы устройств. Описание интерфейса вкладки **Обновление ПО** и порядок настройки обновлений приведены в Руководстве пользователя ПО Biosmart-Studio v6.

Ниже описан порядок обновления встроенного ПО терминала, запускаемый в окне **Свойства Biosmart Palm Vein WTC2**.
Откройте окно **Свойства Biosmart Palm Vein WTC2** и нажмите кнопку **Обновление ПО**.

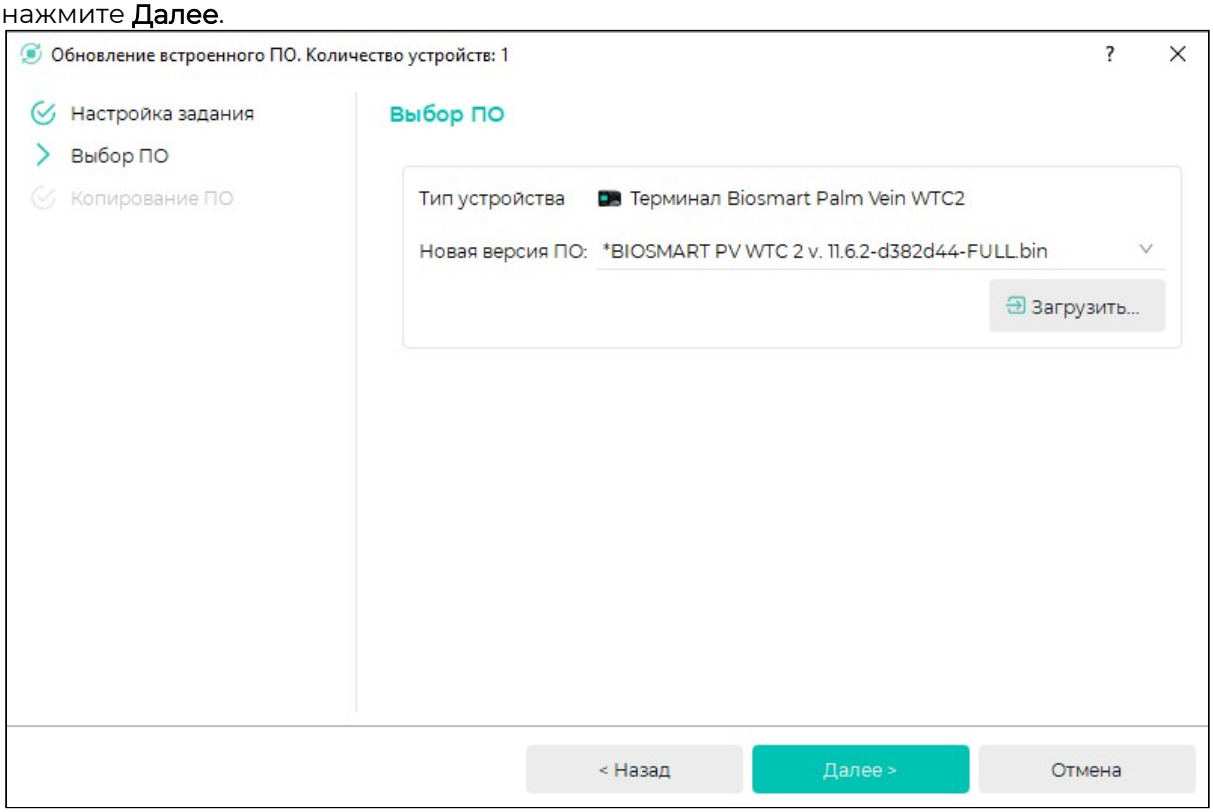


Выберите подходящие время для запуска обновления и нажмите **Далее**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



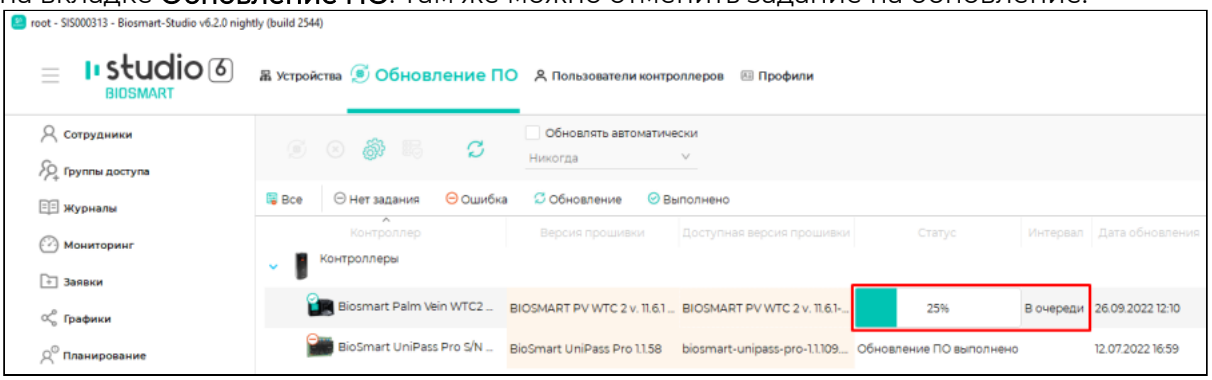
Выберите нужную версию ПО из выпадающего списка. При отсутствии нужной версии ПО в списке нажмите кнопку **Загрузить** и выберите ПО из системного каталога. Затем нажмите **Далее**.



После успешного добавления в БД задания на обновление встроенного ПО нажмите

SEC.RU | Короткий путь к информации
Скачано с sec.ru

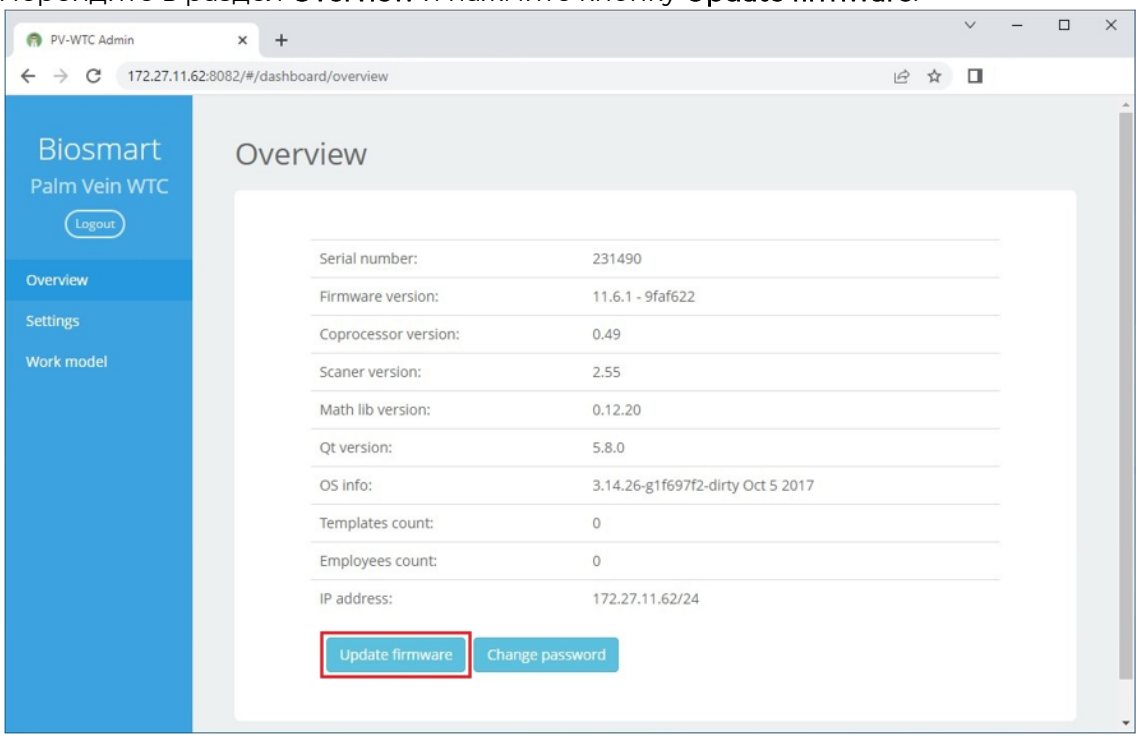
Завершить.
Процесс обновления встроенного ПО терминала можно посмотреть в разделе **Устройства** на вкладке **Обновление ПО**. Там же можно отменить задание на обновление.



6.2 Обновление встроенного ПО с помощью веб-интерфейса

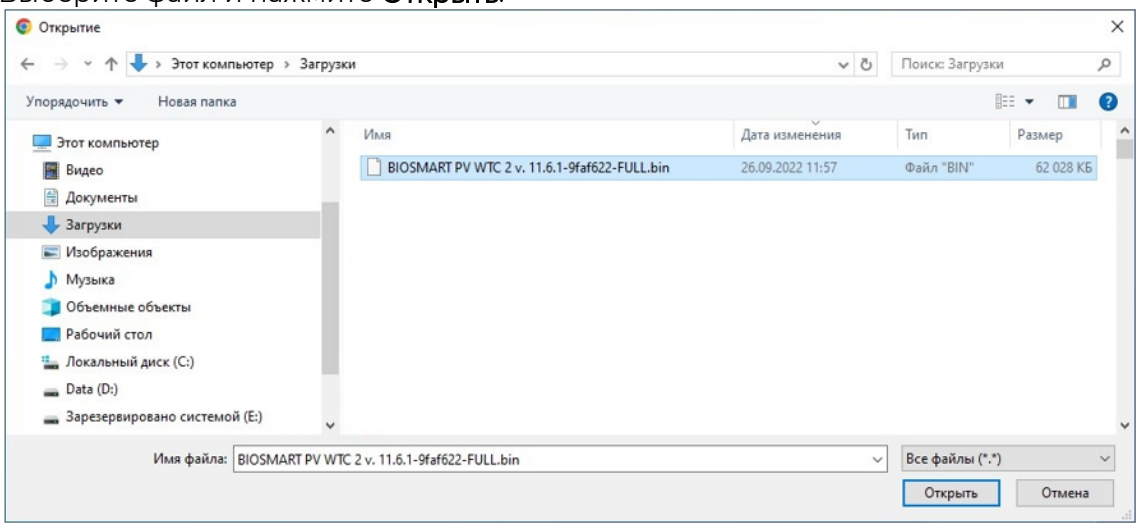
Для обновления встроенного ПО контроллера выполните следующие действия:

1. Скачайте файл встроенного ПО устройства, размещенный на сайте bio-smart.ru в разделе **Техподдержка** → **ПО** → вкладка **Firmware**.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Overview** и нажмите кнопку **Update firmware**.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

4. Выберите файл и нажмите **Открыть**.



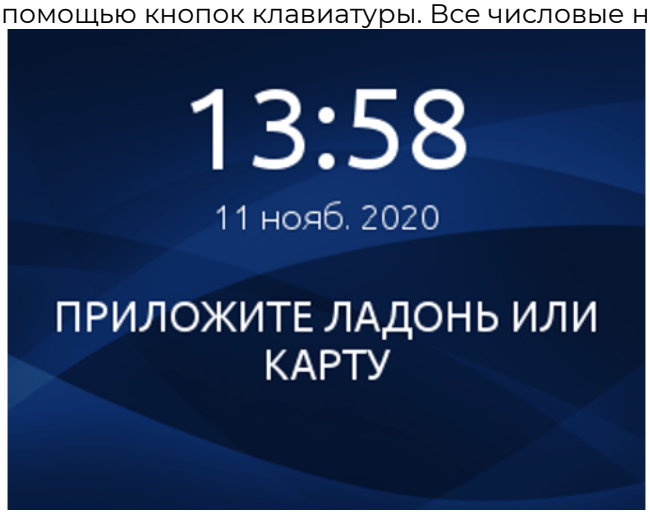
5. По окончанию установке в браузере появится уведомление **Завершить обновление**. Откройте меню браузера и завершите обновление.

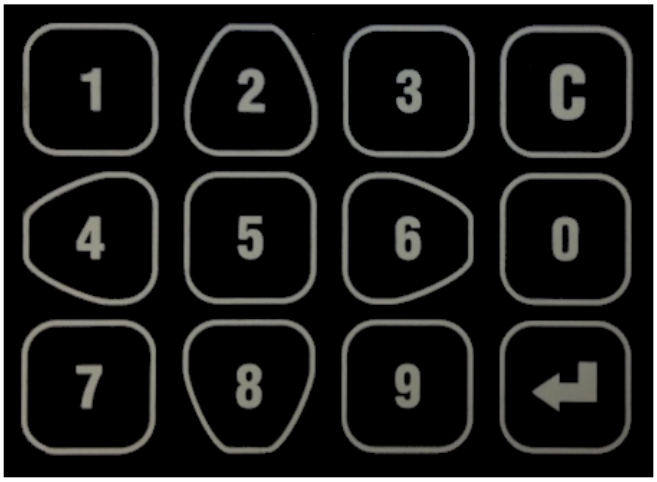
SEC.RU | Короткий путь к информации
Скачано с sec.ru

7 НАСТРОЙКИ ТЕРМИНАЛА BIOSMART PV-WTC

7.1 Настройки в меню терминала BioSmart PV-WTC

Когда терминал включен, но никаких действий с ним не производится, терминал переходит в режим ожидания. В режиме ожидания дисплей терминала имеет вид, соответствующий установленной рабочей модели. На дисплее, как правило, выводится тип действия, которое ожидается терминалом. Навигация по меню осуществляется с помощью кнопок клавиатуры. Все числовые настройки также вводятся с клавиатуры.





Ниже приведено описание кнопок клавиатуры:

	– переход вверх по списку;
	– переход вправо или переход от списка к функциональным кнопкам, в разделе меню **Сотрудники** используется для постраничной навигации вниз;

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4	– переход влево или переход от функциональных кнопок к списку, в разделе меню **Сотрудники** используется для постраничной навигации вверх;
8	– переход вниз по списку;
↵	– выполняет функции выбора (ввода) и подтверждения;
C	– возврат в предыдущий раздел меню или удаление последней введенной цифры.

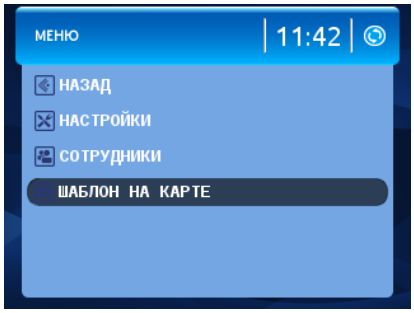
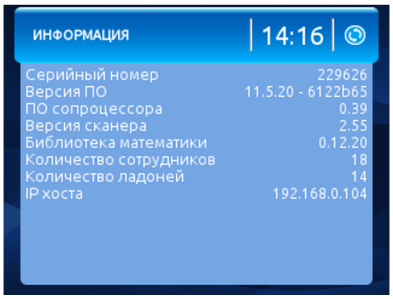
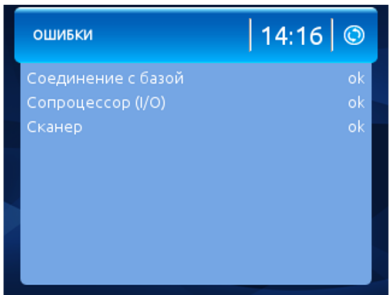
Для входа в основное меню нажмите клавишу **Ввод** ↵
Введите пароль администратора в появившемся поле.

Заводские настройки пароля администратора – пустой пароль.
После первого входа в меню рекомендуется установить новый пароль для исключения в дальнейшем несанкционированного доступа к настройкам терминала.

Вид основного меню представлен на рисунке ниже.
Перемещение между кнопками и пунктами меню осуществляется с помощью кнопок клавиатуры.



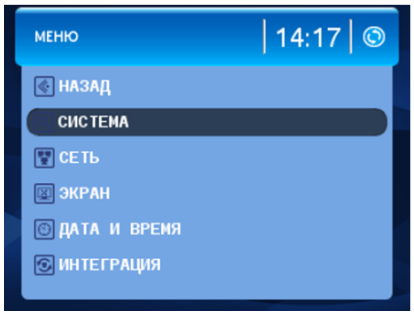
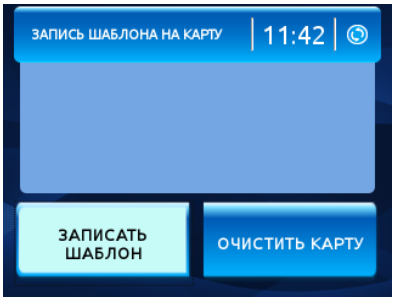
SEC.RU | Короткий путь к информации
Скачано с sec.ru

МЕНЮ	ИНФО	ОШИБКИ
Раздел **Меню** предназначен для доступа к настройкам терминала. **Меню** содержит следующие разделы: • раздел **НАСТРОЙКИ** • раздел **СОТРУДНИКИ** • раздел **ШАБЛОН НА КАРТЕ**	Раздел **Инфо** предназначен для просмотра основной информации о терминале. Раздел содержит основную информацию о терминале. IP хоста – это адрес сервера BioSmart.	Раздел **Ошибки** предназначен для просмотра ошибок, возникших на терминале. Раздел предназначен для отображения информации об ошибках в работе терминала. Если не обнаружено никаких ошибок, то напротив каждого параметра будет значение «**ok**».
		

Меню содержит следующие разделы:

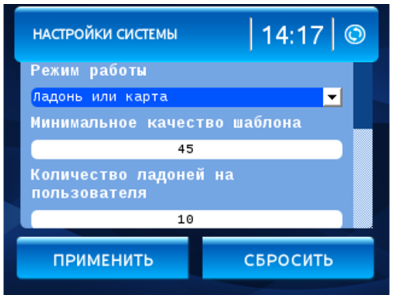
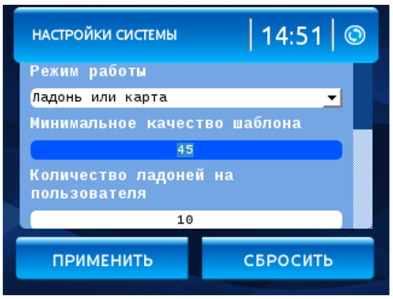
НАСТРОЙКИ	СОТРУДНИКИ	ШАБЛОН НА КАРТЕ
Раздел **НАСТРОЙКИ** включает в себя 5 подразделов: • подраздел **СИСТЕМА** • подраздел **СЕТЬ** • подраздел **ЭКРАН** • подраздел **ДАТА И ВРЕМЯ** • подраздел **ИНТЕГРАЦИЯ**	Раздел предназначен для редактирования данных о сотрудниках. Процедура редактирования данных описана в пункте Редактирование данных сотрудника на терминале.	Раздел предназначен для записи биометрических шаблонов на персональной карте сотрудника в защищенной области памяти. Шаблоны не передаются по сети и не хранятся в базе данных или в памяти контроллера. Процедура редактирования данных описана в пункте Использование рабочей модели "Шаблон на карте".

SEC.RU | Короткий путь к информации
Скачано с sec.ru

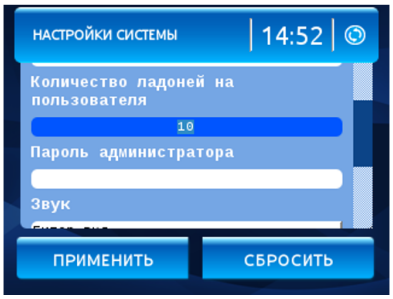
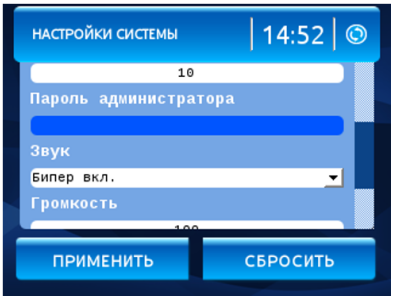
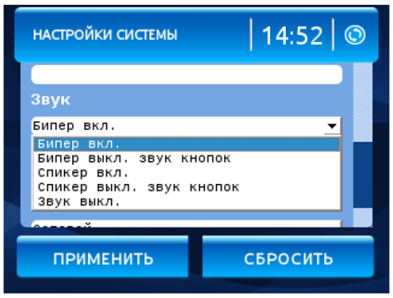
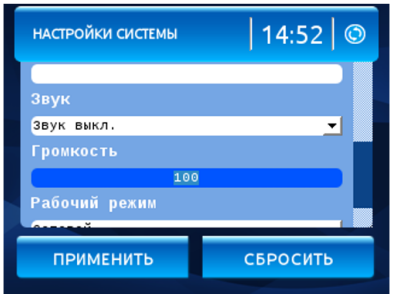
НАСТРОЙКИ	СОТРУДНИКИ	ШАБЛОН НА КАРТЕ
		

Подраздел СИСТЕМА

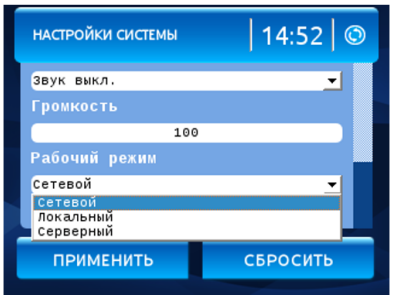
Подраздел предназначен для настройки системных параметров терминала.

Параметр	Описание
	Параметр **Режим работы** предназначен для выбора рабочей модели терминала. Описание рабочих моделей приведено в Выбор и создание рабочих моделей. В большинстве случаев использования терминала достаточно выбрать одну из предустановленных рабочих моделей. Однако, при наличии каких-либо дополнительных требований к работе терминала или при нестандартных сценариях его использования можно создать новую рабочую модель на основе предустановленных или собственную (см. пункт Создание простой рабочей модели).
	Параметр **Минимальное качество шаблона** задает численное значение, определяющее минимальное качество полученных при сканировании биометрических данных, при котором будет осуществляться поиск шаблонов сотрудника в базе. Не рекомендуется изменять данное значение.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Параметр	Описание
	Параметр **Количество ладоней на пользователя** задает количество биометрических шаблонов на одного сотрудника, хранимых в памяти терминала.
	Параметр **Пароль администратора** задает пароль для доступа пользователей в меню терминала. По умолчанию пароль пустой. Для того чтобы установить пустой пароль, введите в поле значение «**0**». ⓘ Использование значения «**0**» в качестве первого символа пароля не допускается. При установке пароля «**012345**» будет установлен пароль «**12345**».
	Параметр **Звук** позволяет выбрать и настроить работу звукового источника терминала (бипер/спикер/отключить звук).
	Параметр **Громкость** позволяет настроить громкость звукового источника терминала.
	Параметр **Нормальное состояние реле** позволяет выбрать состояние реле: **NO (нормально-разомкнутое состояние)** или **NC (нормально-замкнутое состояние)**.

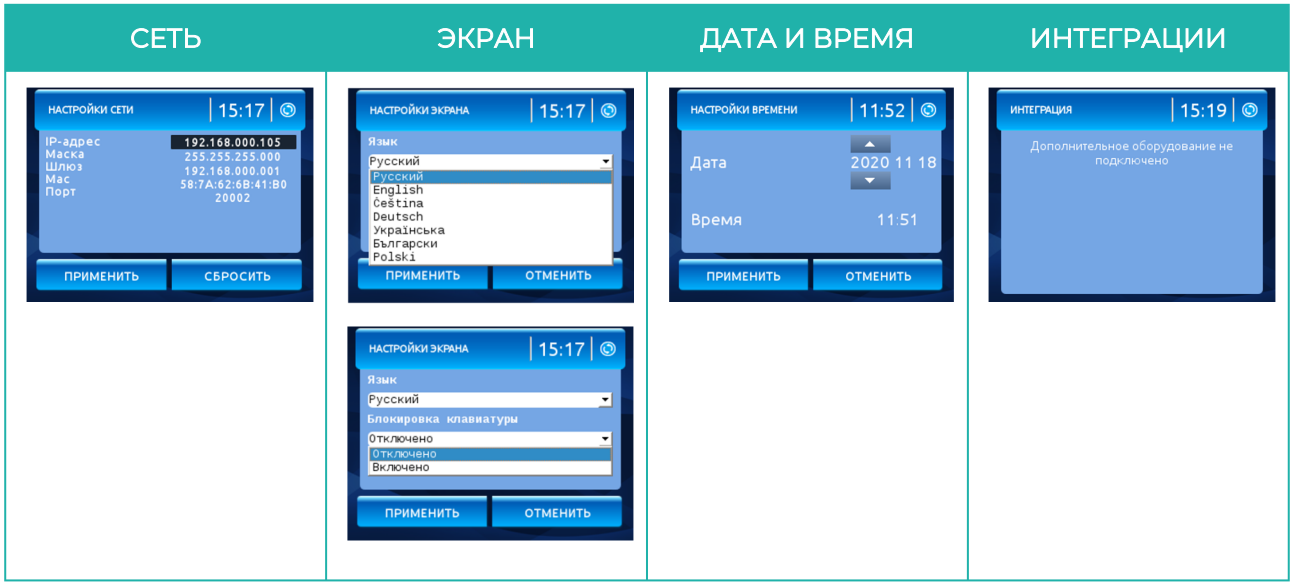
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Параметр	Описание
	Параметр **Рабочий режим** позволяет выбрать режим работы терминала. Доступны три режима: **сетевой режим**, **локальный режим** и **серверная идентификация**. В **сетевом режиме** идентификация, хранение биометрических шаблонов, кодов RFID-карт и журнала событий осуществляется на терминале с непрерывным обменом этими данными с ПО Biosmart-Studio v6. Список сотрудников, которым назначен доступ с помощью терминала, задается в ПО Biosmart-Studio v6. В **локальном режиме** регистрация данных сотрудников, идентификация, а также хранение биометрических шаблонов, кодов идентификаторов и журнала событий осуществляется на терминале. В режиме **серверной идентификации** для идентификации, хранения биометрических шаблонов, кодов RFID-карт и журнала событий используется внешний сервер биометрической идентификации (СИ BioSmart).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

СЕТЬ	ЭКРАН	ДАТА И ВРЕМЯ	ИНТЕГРАЦИИ
Подраздел предназначен для настройки сетевых параметров терминала.	В данном подразделе настраиваются следующие параметры: Параметр **Язык** устанавливает язык интерфейса дисплея (русский, английский, чешский, немецкий, украинский, болгарский или польский). Параметр **Блокировка клавиатуры** позволяет заблокировать клавиатуру терминала. Блокировка позволяет предотвратить несанкционированный вход в меню терминала и другие действия при случайном нажатии кнопок клавиатуры. При заблокированной клавиатуре последовательное нажатие кнопок **7** и **9** временно разблокирует клавиатуру.	Подраздел предназначен для настройки текущих дата и время. В сетевом режиме время синхронизируется со временем сервера BioSmart.	В подразделе отображается информация о подключенном дополнительном оборудовании.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



7.2 Настройки терминала BioSmart PV-WTC в ПО Biosmart-Studio v6

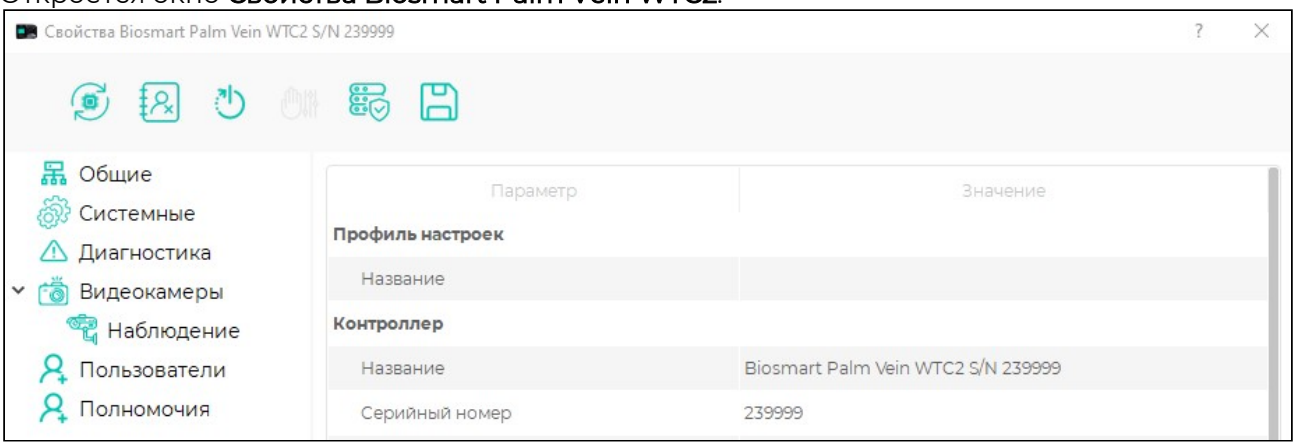
В разделе описаны настройки терминала, доступные в ПО Biosmart-Studio v6.

Общая информация о настройках

Для настройки терминала в ПО Biosmart-Studio v6 перейдите в раздел **Устройства**. Окно свойств терминала можно открыть следующими способами:

- дважды кликнуть левой кнопкой мыши на строке с терминалом
- выделить строку с терминалом и нажать кнопку **Свойства** на панели инструментов
- нажать на строку с терминалом правой кнопкой мыши и в контекстном меню выбрать пункт **Свойства**.

Откроется окно **Свойства Biosmart Palm Vein WTC2**.



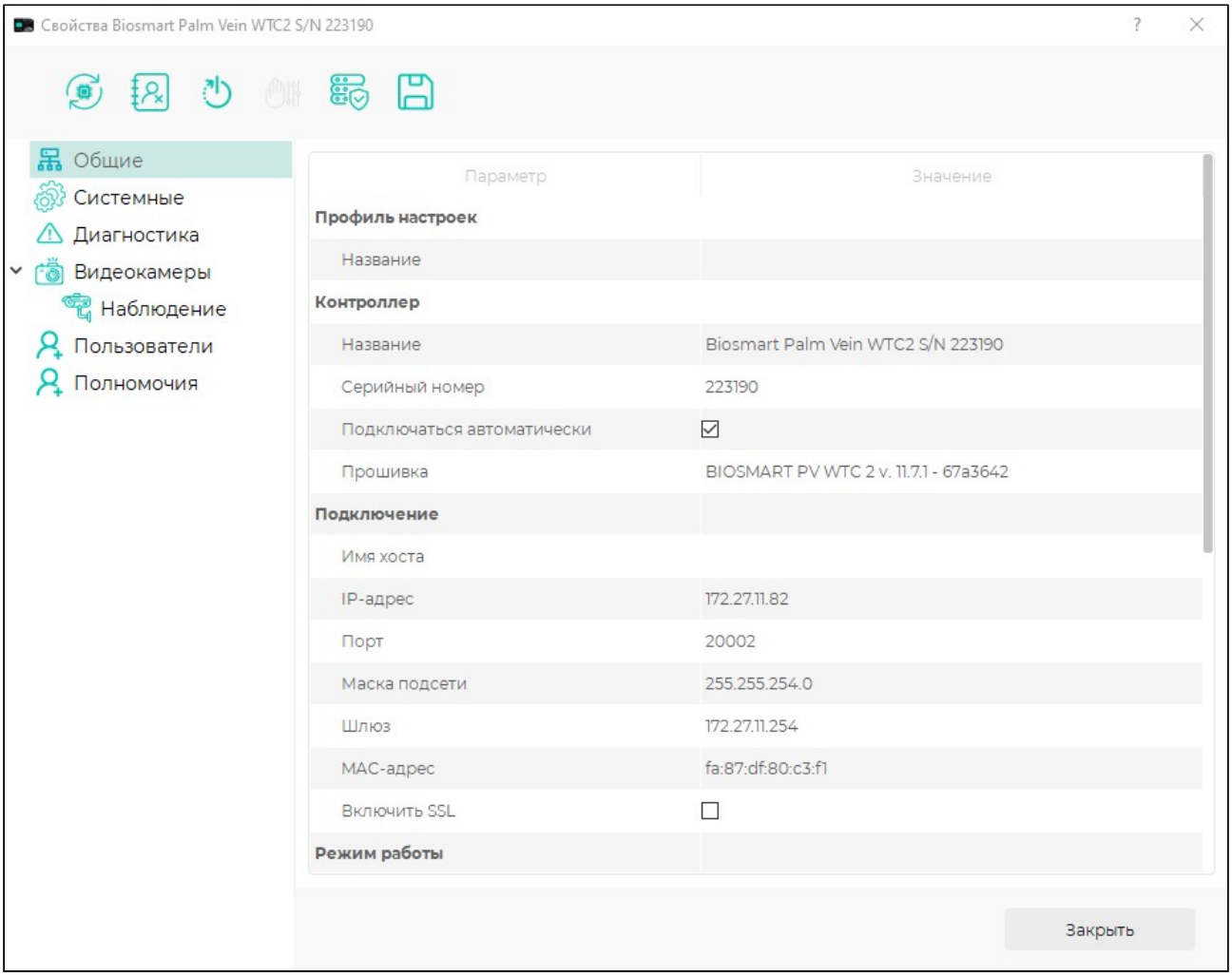
На панели управления расположены следующие кнопки:

Обновление ПО		– настройка задания на обновление встроенного ПО терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Инициализация		– инициализация терминала, в ходе которой из памяти терминала удаляются список сотрудников, их идентификаторы и события.
Сброс настроек		– сброс настроек терминала на заводские.
Калибровка сенсора		– для терминала **BioSmart PV-WTC** не используется.
Применить профиль		– применение для терминала настроек профиля.
Сохранить в профиль		– сохранение настроек терминала в профиль.

7.2.1 Вкладка Общие



Раздел **Профиль настроек**:

- **Название** – выбор профиля настроек терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Раздел **Контроллер**:

- **Название** – название терминала в ПО Biosmart-Studio v6.
- **Серийный номер** – короткий серийный номер терминала. Заполняется автоматически, не редактируется.
- **Подключаться автоматически** – флаг, при установке которого сервер BioSmart будет автоматически подключаться к терминалу в случае возобновления связи с терминалом.
- **Прошивка** – версия встроенного ПО терминала. Заполняется автоматически, не редактируется.

Раздел **Подключение**:

- **Имя хоста**, **IP-адрес**, **Порт**, **Маска подсети**, **Шлюз**, **MAC-адрес** – сетевые настройки терминала.
- **Включить SSL** – флаг, при установке которого будет включено шифрование трафика ПО Biosmart-Studio v6 – терминал.

Раздел **Режим работы**:

- **Режим работы** – режим работы терминала. Доступны три режима: **сетевой режим**, **локальный режим** и **серверная идентификация**.

В **сетевом режиме** идентификация, хранение биометрических шаблонов, кодов RFID-карт и журнала событий осуществляется на терминале с непрерывным обменом этими данными с ПО Biosmart-Studio v6. Список сотрудников, которым назначен доступ с помощью терминала, задается в ПО Biosmart-Studio v6.
В **локальном режиме** регистрация данных сотрудников, идентификация, а также хранение биометрических шаблонов, кодов идентификаторов и журнала событий осуществляется на терминале.
В режиме **серверной идентификации** для идентификации, хранения биометрических шаблонов, кодов RFID-карт и журнала событий используется внешний сервер биометрической идентификации (СИ BioSmart).

- **Сервер идентификации** – сетевой адрес внешнего сервера при работе терминала в режиме **серверная идентификация**.
- **Режим резервирования** – режим работы в **серверной идентификации**, при котором хранение биометрических шаблонов, кодов RFID-карт и журнала событий осуществляется не только на **сервере идентификации**, но и на терминале. При отсутствии соединения с **сервером идентификации** терминал будет идентифицировать сотрудников в **локальном режиме.**

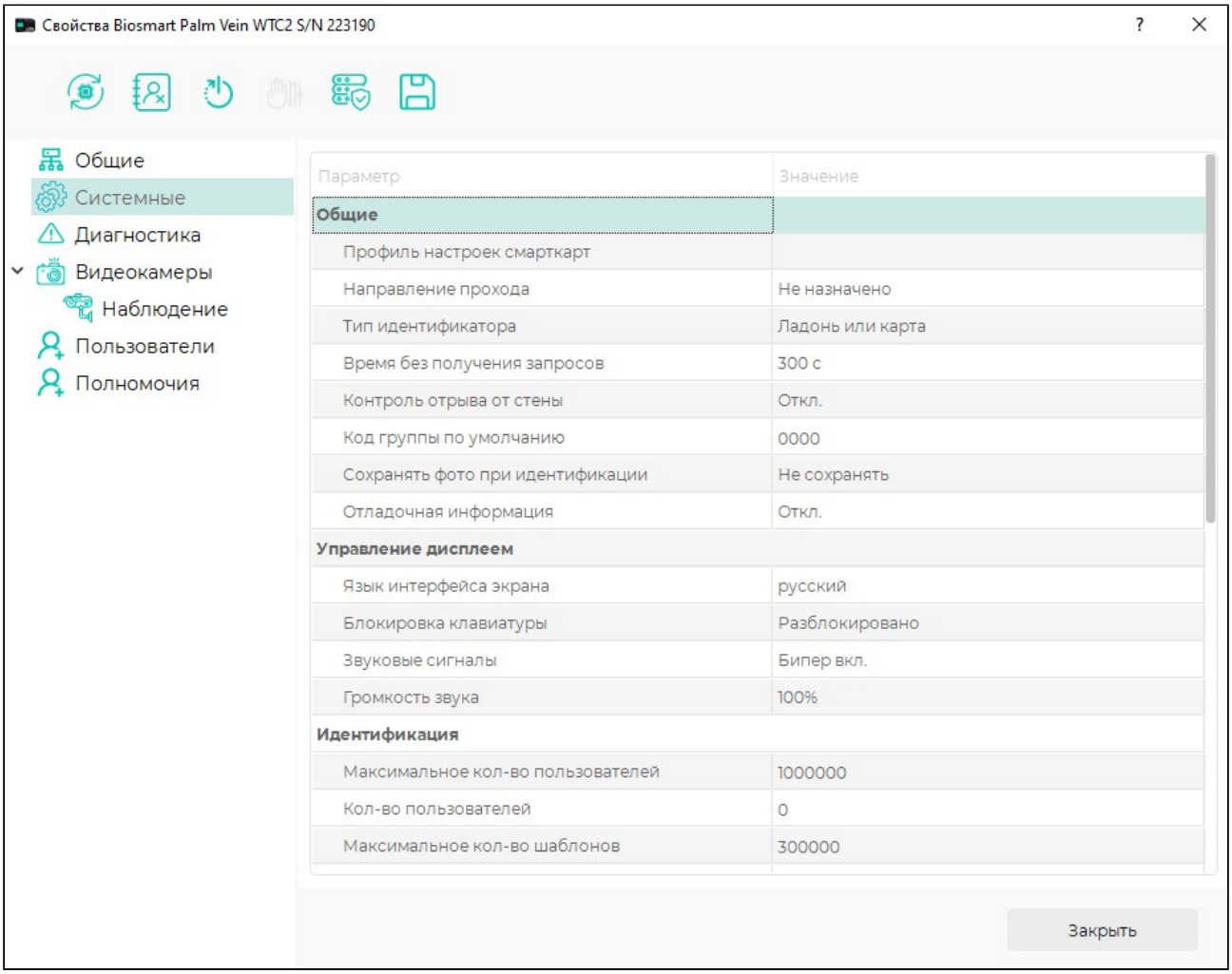
Раздел **Дополнительно**:

- **Часовой пояс** – часовой пояс, в соответствии с которым будет установлено время на терминал.
- **Сервер времени (NTP)** – поле для ввода адреса сервера времени для синхронизации внутренних часов терминала.
- **Время ожидания ответа** – интервал времени, в течение которого сервер BioSmart ожидает ответ от терминала. Если по истечении указанного интервала ответ не получен, то связь с терминалом считается разорванной.
- **Максимальный размер пакета, байт (MTU)** – максимальный размер пакета, передаваемый терминалом без фрагментации. Настройка необходима только в сетях, где есть маршрутизаторы, не поддерживающие фрагментацию пакетов.
- **Количество пользователей** – количество сотрудников, которым назначен доступ с помощью терминала.
- **Количество шаблонов** – количество биометрических шаблонов в памяти терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Кол-во журналов в памяти** – количество событий в памяти терминала, которые ещё не отправлены на сервер.

7.2.2 Вкладка Системные



Раздел **Общие**:

- **Направление прохода** – направление движения сотрудника (Вход/Выход), которое будет автоматически записано в системе учёта рабочего времени при успешной идентификации сотрудника на терминале.
- **Тип идентификатора** – выбор рабочей модели терминала. Описание предустановленных рабочих моделей приведено в пункте **Выбор и создание рабочих моделей**.
- **Время без получения запросов** – интервал времени, в течение которого терминал ожидает запрос от сервера BioSmart. Если по истечении указанного интервала запрос не был получен, соединение с сервером BioSmart будет принудительно разорвано.
- **Контроль отрыва от стены** – параметр, позволяющий включить контроль состояния датчика отрыва от стены. При прикреплении терминала к стене в ПО Biosmart-Studio будет сформировано событие «**Прикреплен к стене**», при отрыве от стены – событие «**Отрыв от стены**».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Код группы по умолчанию** – пин-код для сотрудников по умолчанию при работе терминала в режиме «Кнопка входа/выхода + код группы + ладонь/карта».
- **Режим anti-passback** – параметр для включения на терминале функции Antipassback, заключающейся в запрете повторного прохода сотрудника через терминал в одном направлении. Функция Antipassback используется только при работе терминала в режиме **серверной идентификации**.
- **Сохранять фото при идентификации** – опция, позволяющая настроить сохранение фото с камеры, интегрированной с терминалом, во время идентификации.
- **Отладочная информация** – параметр, предназначенный для включения передачи дополнительной диагностической информации в ПО Biosmart-Studio. Не рекомендуется изменять значение, заданное по умолчанию.

Раздел **Управление дисплеем**:

- **Язык интерфейса экрана** – язык интерфейса.
- **Блокировка клавиатуры** – настройка, позволяющая заблокировать клавиатуру терминала. Блокировка позволяет предотвратить несанкционированный вход в меню терминала и другие действия при случайном нажатии кнопок клавиатуры. При заблокированной клавиатуре последовательное нажатие кнопок **7** и **9** временно разблокирует клавиатуру.
- **Звуковые сигналы** – настройка звуковой индикации.
- **Громкость звука** – настройка громкости звука.

Раздел **Идентификация**:

- **Максимальное кол-во пользователей** – максимальное количество сотрудников, которым может быть назначен доступ с помощью терминала. Заполняется автоматически, не редактируется.
- **Кол-во пользователей** – количество сотрудников, которым назначен доступ с помощью терминала. Заполняется автоматически, не редактируется.
- **Максимальное кол-во шаблонов** – максимальное количество шаблонов вен ладоней в памяти терминала. Заполняется автоматически, не редактируется.
- **Кол-во шаблонов для пользователя** – количество биометрических шаблонов на одного сотрудника, хранимых в памяти терминала.
- **Минимальное качество шаблона** – численное значение, определяющее минимальное качество шаблона вен ладоней, который будет разрешено сохранить при регистрации. Не рекомендуется изменять значение, заданное по умолчанию.
- **Антифейк** – параметр для включения комплекса программно-аппаратных средств защиты от попыток идентификации по поддельным биометрическим данным. Не рекомендуется изменять значение, заданное по умолчанию.
- **Уровень строгости идентификации** – параметр, определяющий порог совпадения биометрических данных, полученных в процессе идентификации, с биометрическим шаблоном, хранящимся в базе данных. Уровень строгости идентификации и соответствующая ему вероятность ошибочного доступа (FAR) показаны в таблице:

Уровень строгости идентификации	FAR
Повышенный	10^{-8}
Высокий	10^{-7}
Средний	10^{-6}

SEC.RU | Короткий путь к информации
Скачано с sec.ru

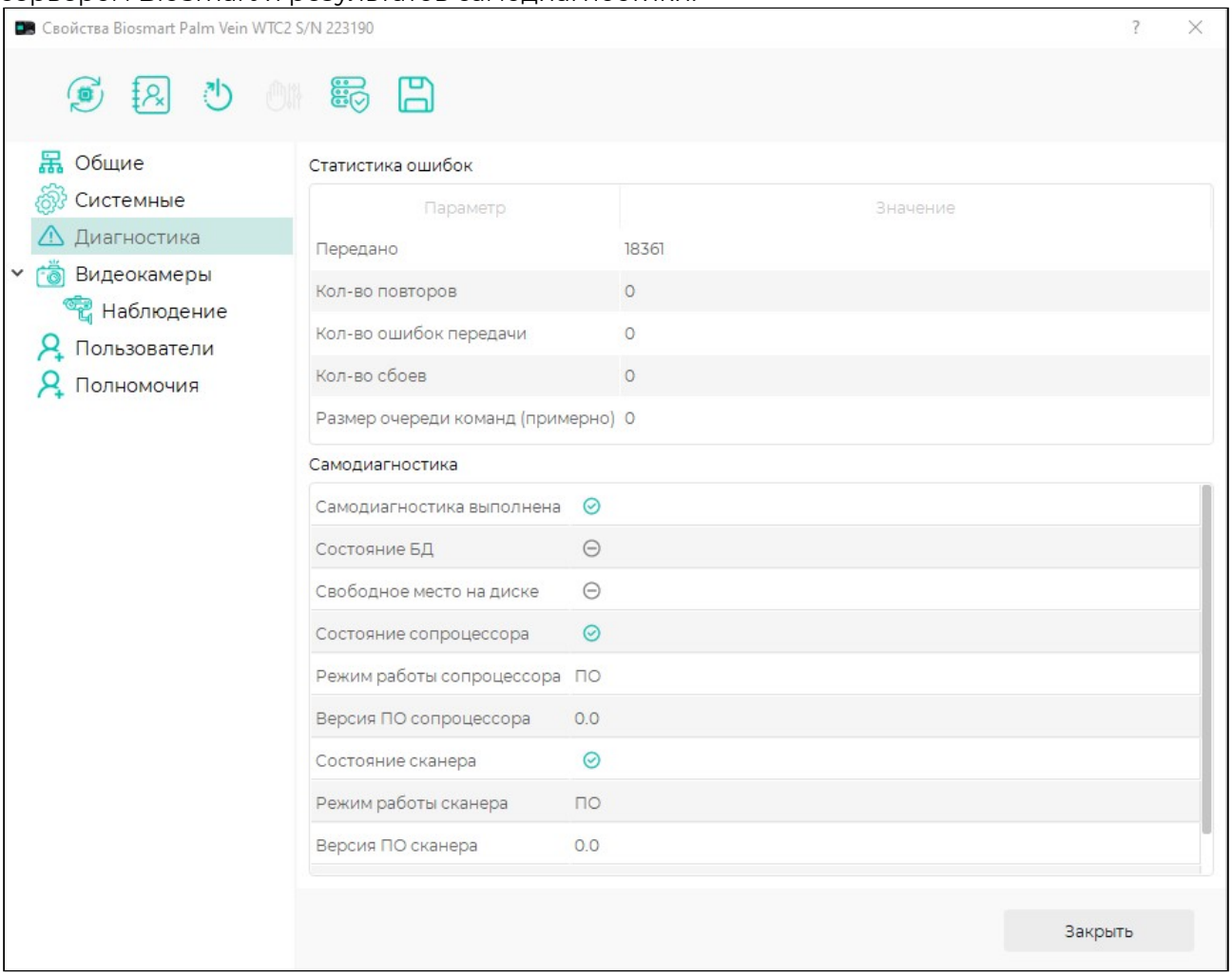
Пониженный	10^{-5}
Низкий	10^{-4}
Очень низкий	10^{-3}

- **Использовать предвыборку правой/левой ладони** – параметр, позволяющий включить определение типа ладони (правая/левая) в процессе идентификации и проведение предварительной выборки ограниченного числа шаблонов из базы данных, с которыми будет выполняться сравнение полученных биометрических данных.
- **Сохранение дополнительных шаблонов** – параметр, позволяющий настроить сохранение дополнительных шаблонов сотрудника при каждой идентификации.
- **Таймаут блокировки по антифейку** – интервал времени, на который блокируется работа терминала при попытке зарегистрировать биометрические шаблоны с помощью поддельных биометрических данных.
- **Режим работы RFID** – выбор режима работы встроенного считывателя RFID-карт.
- **Адрес ID в памяти карты (hex)** – адрес ячейки памяти карты, в которой хранится записанный пользователем код карты при работе встроенного RFID-считывателя в режиме считывания кода карты из защищенной области.
- **Длина номера карты –** длина номера RFID-карты в битах.
- **Макс. кол-во левых (правых) ладоней** – максимальное количество шаблонов вен левой (правой) ладони, которое разрешено сохранить при регистрации на терминале.
- **Мин. кол-во левых (правых) ладоней** – минимальное количество шаблонов вен левой (правой) ладони, которое разрешено сохранить при регистрации на терминале.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7.2.3 Вкладка Диагностика

Вкладка предназначена для отображения статистических данных по связи терминала с сервером BioSmart и результатов самодиагностики.



Раздел **Статистика ошибок**:

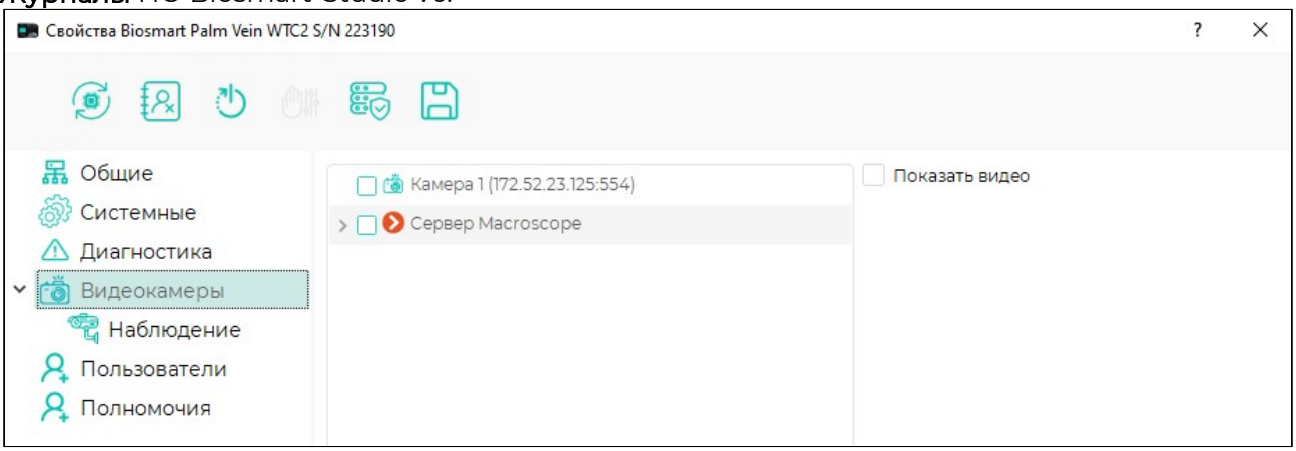
- **Передано** – число пакетов, переданных терминалом за последний час.
- **Кол-во повторов**, **Кол-во ошибок передачи** – количество повторов и ошибок за последний час.
- **Кол-во сбоев** – количество пакетов, которые терминал не смог передать на сервер BioSmart.
- **Размер очереди команд (примерно)** – количество команд, которые на данный момент поставлены в очередь сервером BioSmart для этого терминала.

Раздел **Самодиагностика** отображает результаты самодиагностики аппаратных узлов терминала. При положительном результате самодиагностики должны стоять значки ✓, в некоторых случаях могут стоять значки ⊖, означающие что значение не определено. Также в разделе есть информация о режиме работы сопроцессора и его версии ПО, версии сканера, режиме его работы и версии ПО.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

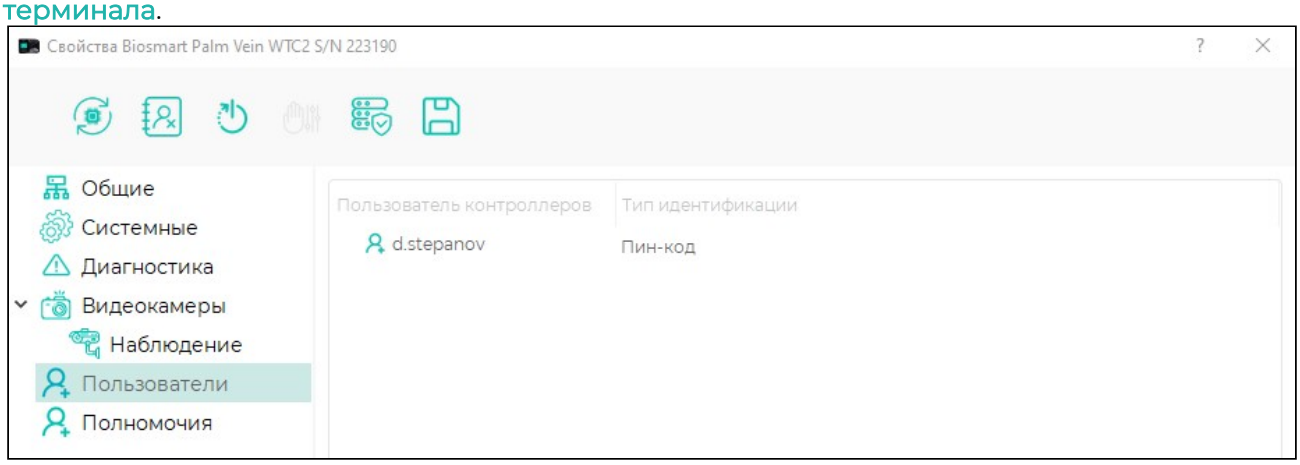
7.2.4 Вкладка Видеокамеры

На вкладке можно выбрать сервер видеонаблюдения, на котором будет храниться видео, и камеру. Видеофрагменты с выбранной камеры будут привязаны к событиям идентификации на терминале. Фрагменты видео можно просматривать в разделе **Журналы** ПО Biosmart-Studio v6.



7.2.5 Вкладка Пользователи

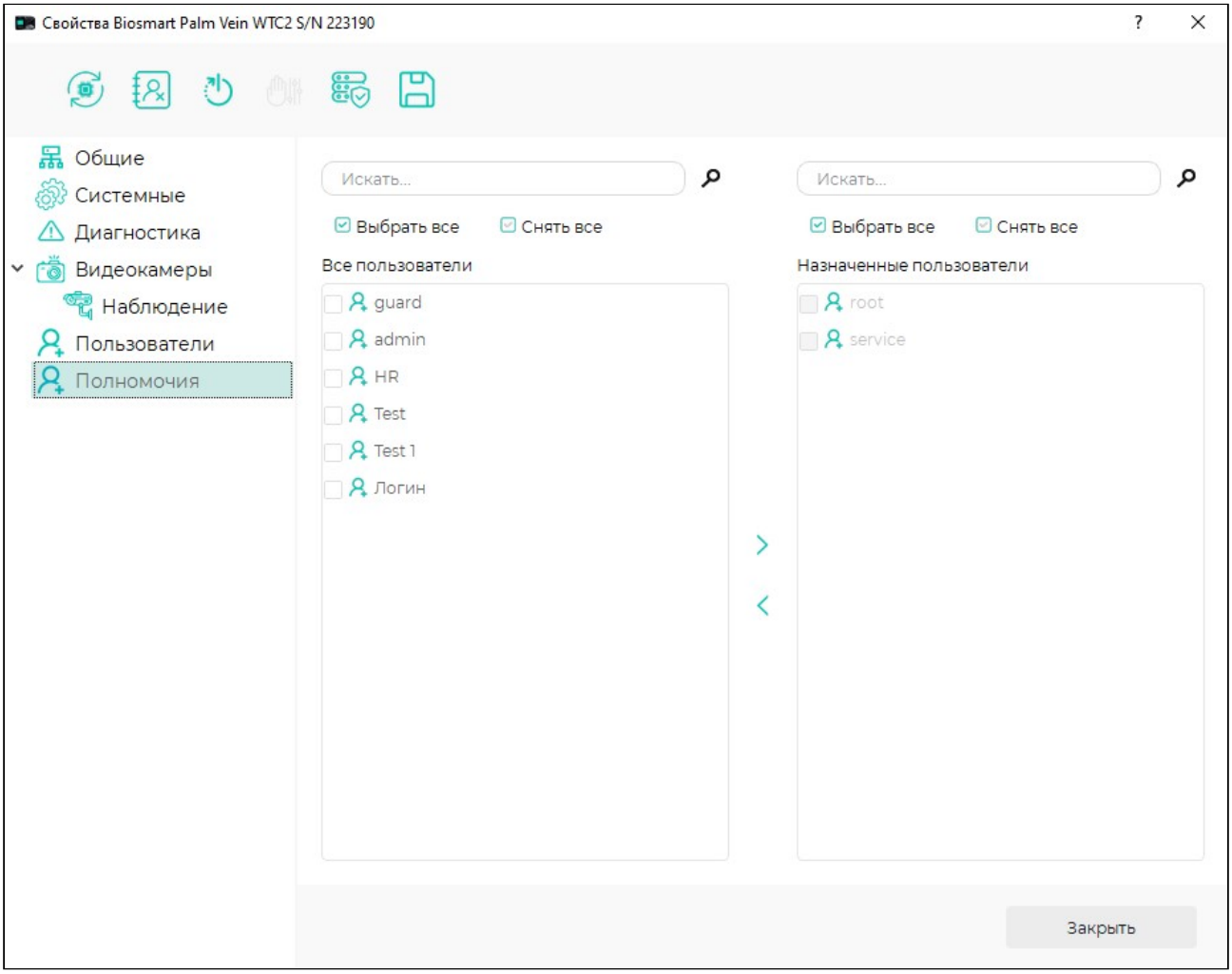
На вкладке отображаются пользователи, которым доступны настройки в меню терминала, и тип идентификации для доступа в меню.
Настройка пользователей терминала описана в пункте Настройка прав пользователей терминала.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

7.2.6 Вкладка Полномочия

На вкладке можно выбрать пользователей, которым будут доступны настройки терминала в ПО Biosmart-Studio v6.



7.3 Настройки терминала BioSmart PV-WTC в веб-интерфейсе

В разделе описаны настройки терминала, доступные в веб-интерфейсе.

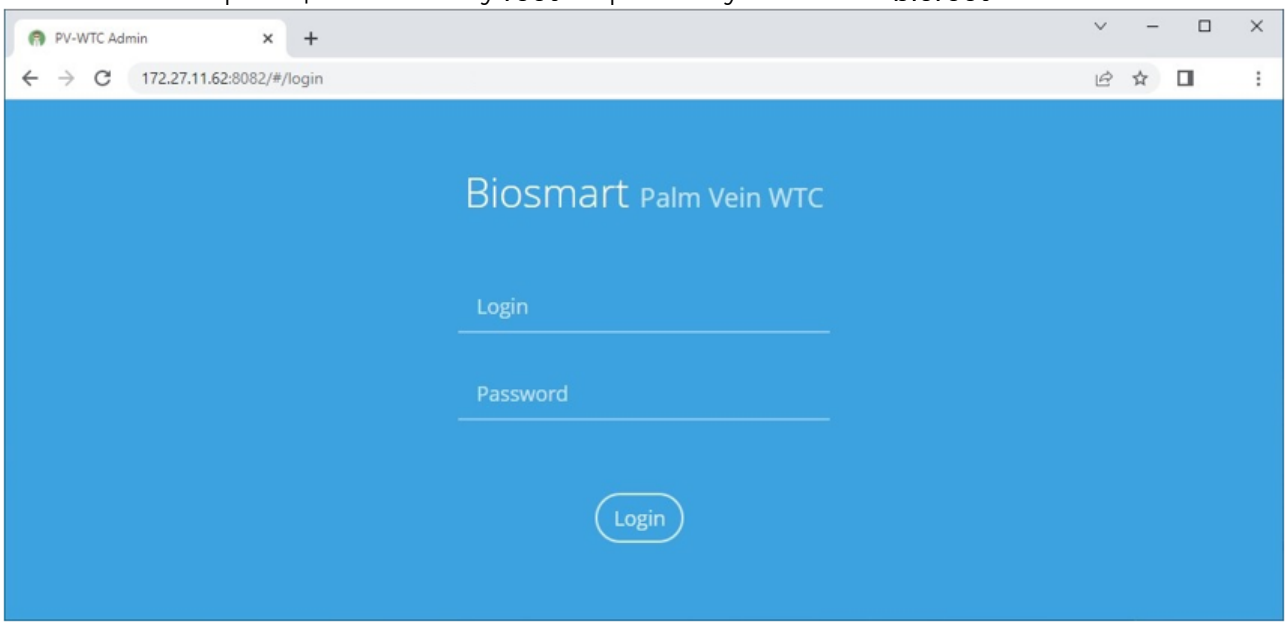
7.3.1 Доступ к веб-интерфейсу

Для доступа к веб-интерфейсу используется интернет-браузер, например, Google Chrome, Opera, Mozilla Firefox, Microsoft Edge и другие.

Убедитесь, что между компьютером и терминалом настроена маршрутизация, открыт TCP порт 8082. В интернет-браузере в строке адреса введите IP-адрес терминала в виде **IP_address:8082**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

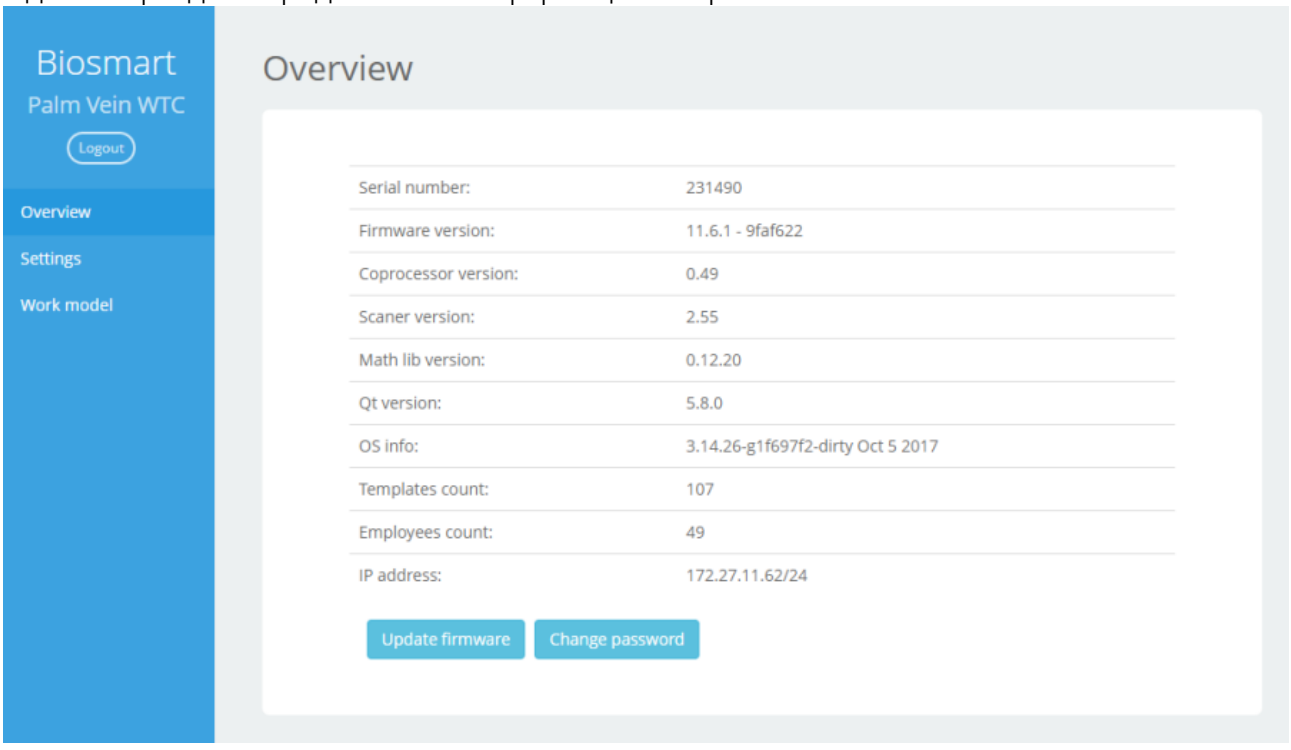
Выполните авторизацию по логину **root**. Пароль по умолчанию **bioroot**.



После успешной авторизации станут доступны разделы веб-интерфейса.

7.3.2 Раздел Overview

В данном разделе представлена информация о терминале.

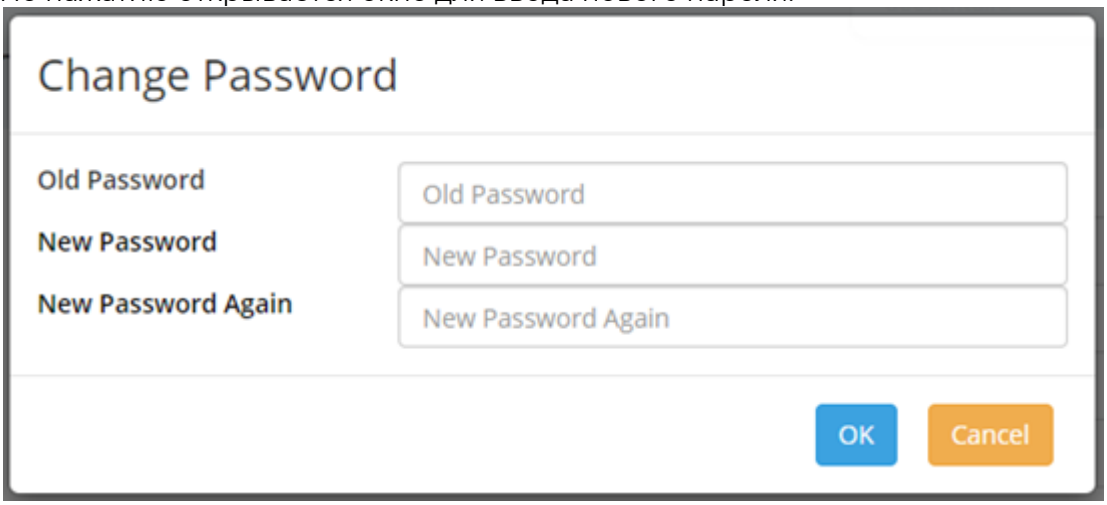


Кнопка **Update firmware**	предназначена для обновления встроенного ПО терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

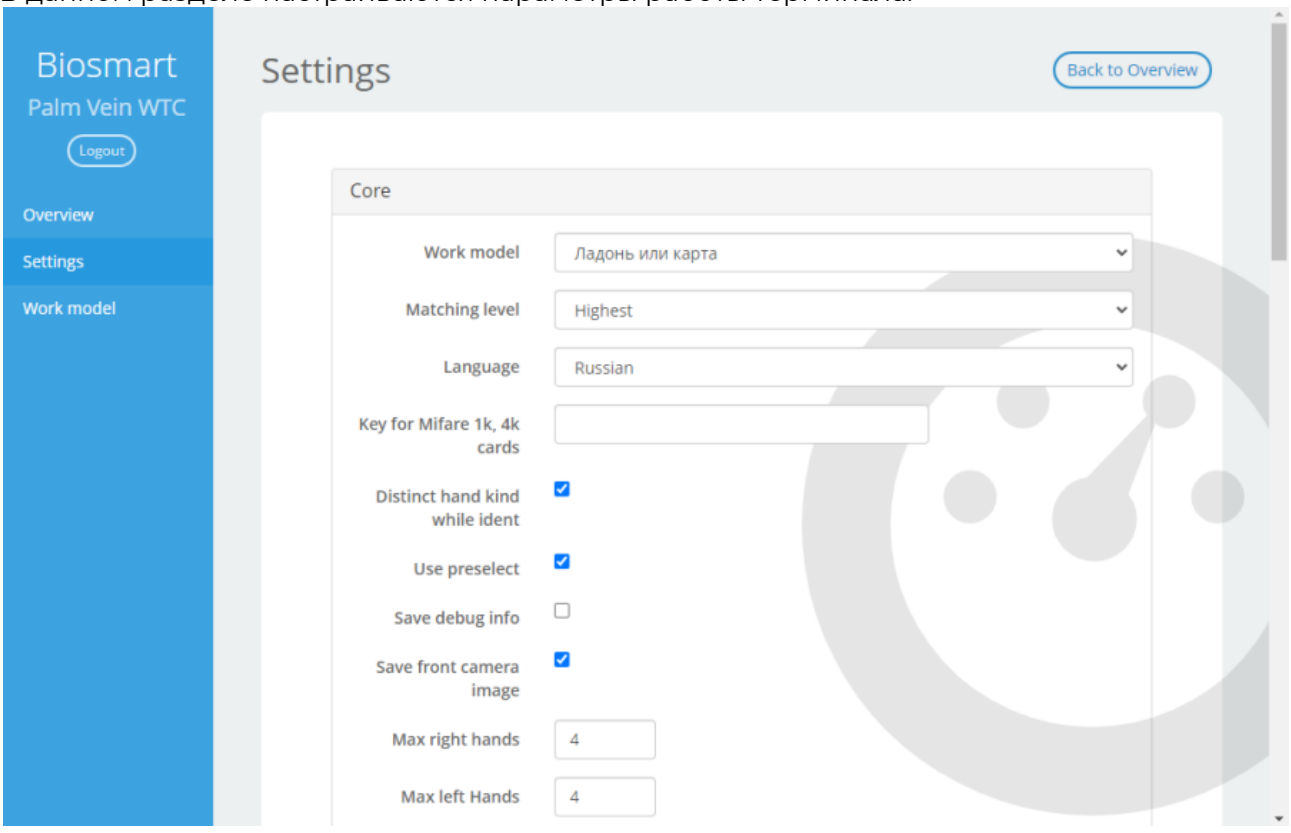
Кнопка **Change password**	предназначена для смены пароля для входа в веб-интерфейс.

По нажатию открывается окно для ввода нового пароля.



7.3.3 Раздел Settings

В данном разделе настраиваются параметры работы терминала.



Блок **Core**:

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Work model** – выбор рабочей модели терминала. Описание предустановленных рабочих моделей приведено в пункте **Настройка пользователей терминала**.
- **Matching level** – параметр, определяющий порог совпадения биометрических данных, полученных в процессе идентификации, с биометрическим шаблоном, хранящимся в базе данных. Matching level и соответствующая ему вероятность ошибочного доступа (FAR) показаны в таблице:

Matching level	FAR
Highest	10^{-8}
High	10^{-7}
Intermediate	10^{-6}
Low	10^{-5}
Very Low	10^{-4}
Lowest	10^{-3}

- **Language** – язык интерфейса дисплея.
- **Key for read template Mifare 1k, 4k cards** – ключ для считывания шаблонов карт Mifare 1k, 4k.
- **Free pass mode background color** – цвет фона в режиме "Свободный проход".
- **Blocked mode background color** – цвет фона в режиме "Блокировка прохода".
- **Key for write template Mifare 1k, 4k cards** – ключ для записи шаблонов карт Mifare 1k, 4k.
- **UID Offset address (dec, 0-4294967295)** – смещение UID для чтения идентификатора с карты.
- **The length of the data to be read from eeprom(dec, 0-4294967295)** – количество байт, которые необходимо считать при чтении идентификатора с карты.
- **RFID Offset address (dec, 0-4294967295)** – смещение шаблона карты для чтения шаблона карты, записанной не в ПО Biosmart-Studio.
- **Card Length** – длина номера RFID-карты в битах.
- **Distinct hand kind while ident** – параметр, позволяющий включить определение типа ладони (правая/левая) в процессе идентификации и проведение предварительной выборки ограниченного числа шаблонов из базы данных, с которыми будет выполнятся сравнение полученных биометрических данных. Используется для ускорения идентификации.
- **Use preselect** – параметр для включения специального алгоритма, ускоряющего поиск шаблонов в базе данных. Используется для ускорения идентификации.
- **Save debug info** – параметр для включения передачи дополнительной диагностической информации в ПО Biosmart-Studio v6. Не рекомендуется изменять значение, заданное по умолчанию.
- **Save front camera image** – в настоящее время не используется.
- **Max right (left) hands** – максимальное количество шаблонов вен правой (левой) ладони, которое разрешено сохранить при регистрации на терминале.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Min right (left) hands** – минимальное количество шаблонов вен правой (левой) ладони, которое разрешено сохранить при регистрации на терминале.
- **Minimal quality** – численное значение, определяющее минимальное качество шаблона вен ладоней, который будет разрешено сохранить при регистрации. Не рекомендуется изменять значение, заданное по умолчанию.
- **Minimal identification quality** – численное значение, определяющее минимальное качество полученных при сканировании биометрических данных, при котором будет осуществляться поиск шаблонов сотрудника в базе. Не рекомендуется изменять значение, заданное по умолчанию.
- **Studio connection warning timeout (sec)** – интервал времени без соединения с сервером BioSmart, по истечению которого на дисплее появится сообщение «**Нет связи с сервером, обратитесь в тех.поддержку**».
- **Studio connection block timeout (min)** – интервал времени без соединения с сервером BioSmart, по истечению которого терминал будет заблокирован. При восстановлении соединения работа терминала будет возобновлена.
- **Run SNMP agent** – параметр для запуска SNMP-агента.

Блок **PV WTC 2**:

- **Hello Message** – текст приветствия на дисплее при идентификации.
- **Choose hand at enroll** – параметр, позволяющий включить раздельную регистрацию шаблонов правой и левой ладони.
- **Antifraud** – параметр для включения алгоритма защиты от попыток идентификации по поддельным биометрическим данным. Не рекомендуется изменять значение, заданное по умолчанию.
- **Antifraud block timeout** – интервал времени, на который блокируется работа терминала при попытке зарегистрировать биометрические шаблоны с помощью поддельных биометрических данных.
- **Tamper signalling on start** – параметр, позволяющий включить контроль состояния датчика отрыва от стены. При прикреплении терминала к стене в ПО Biosmart-Studio v6 будет сформировано событие «**Прикреплен к стене**», при отрыве от стены событие «**Отрыв от стены**».
- **Relay inversion (on/off)** - настройка переключения реле в состояние **NO (нормально-разомкнутое состояние)** или **NC (нормально-замкнутое состояние).**

Блок **NTP**:

- **NTP enabled** – параметр для включения синхронизации времени с NTP-сервером при локальном режиме работы терминала, а также при работе со сторонними серверами биометрической идентификации.
- **NTP server** – сетевой адрес NTP-сервера.
- **Timezone** – часовой пояс.

Блок **System**:

- **Db service time [hhmm]-1 disable db service** – время запуска процедуры обслуживания базы данных терминала. В это время терминал не должен использоваться. По умолчанию установлено ночное время 2:00.
- **Max rows in table Log_image** – максимальное количество строк в таблице с данными для отладки, при превышении которого наиболее старые записи удаляются. Не рекомендуется изменять значение, заданное по умолчанию.

Блок **Temperature measurement**:

- **Calibration value, mC** – значение компенсационной поправки, добавляемой к измеренному значению температуры. Определяется эмпирически с помощью другого термометра и зависит от условий эксплуатации.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Min. threshold, mC** – минимальное значение температуры, при котором в случае успешной идентификации будет предоставлен доступ.
- **Max. threshold, mC** – максимальное значение температуры, при котором в случае успешной идентификации будет предоставлен доступ.
- **Measure time, msec** – время, в течении которого терминал ожидает прикладывания запястья сотрудника к датчику температуры.

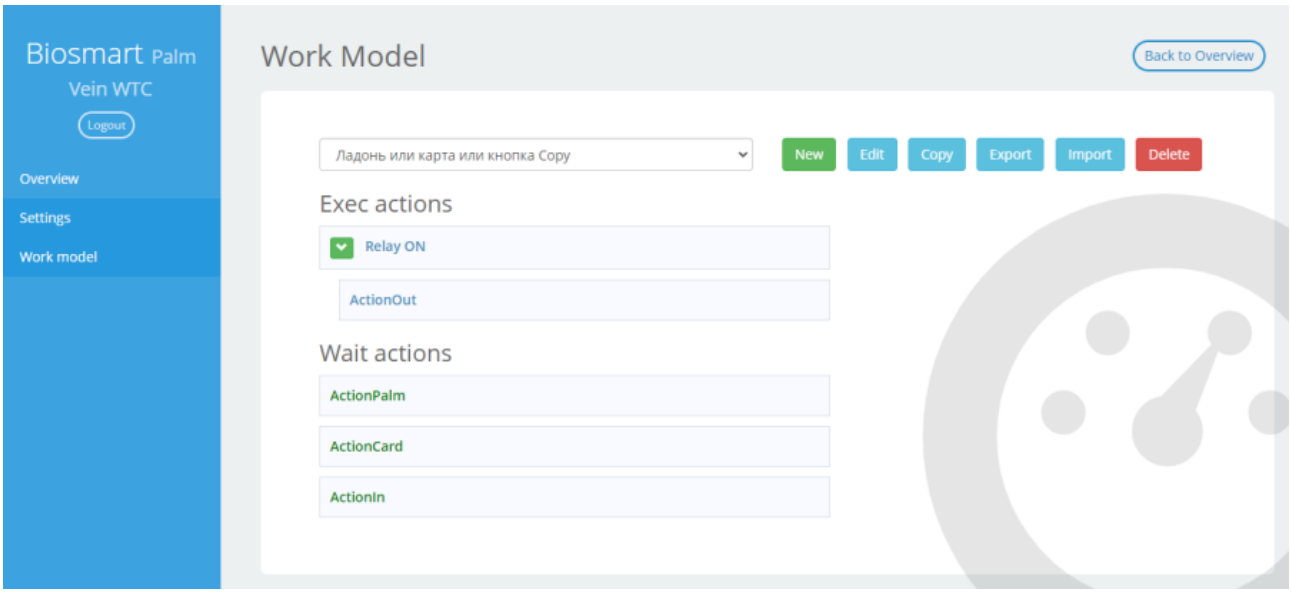
Внизу раздела **Settings** расположены следующие кнопки:

Save	Кнопка предназначена для сохранения сделанных изменений.
Cancel	Кнопка предназначена для отмены сделанных изменений. Также можно вернуться в раздел **Overview**, нажав кнопку **Back To Overview** в правой верхней части окна. Изменения при этом не сохранятся.
Reset work model	Кнопка предназначена для удаления рабочих моделей, созданных пользователем. Останутся только предустановленные рабочие модели.
Reinit DB	Кнопка предназначена инициализации терминала (удаления из памяти терминала списка сотрудников, их идентификаторов и журнала событий).
Download log files	Кнопка предназначена для скачивания LOG-файлов.

7.3.4 Раздел Work Model

В данном разделе создаются и редактируются рабочие модели.
Рабочая модель – это сценарий работы терминала, состоящий из совокупности событий (**Wait actions**) и действий (**Exec actions**). Терминал ожидает появления одного или нескольких последовательных событий (например, прикладывание ладони к сканеру, появление сигнала на дискретном входе и т.д.) и реагирует на них соответствующими действиями (срабатывание реле, отправка кода по интерфейсу Wiegand и т.д.).

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Терминал имеет ряд предустановленных рабочих моделей, отвечающих наиболее частым сценариям использования. Описание предустановленных рабочих моделей приведено в пункте Предустановленные рабочие модели.
В большинстве случаев использования терминала достаточно выбрать одну из предустановленных рабочих моделей. Однако, при наличии каких-либо дополнительных требований к работе терминала или при нестандартных сценариях его использования можно внести изменения в предустановленную рабочую модель или создать новую.

Внесение изменений в предустановленную рабочую модель выполняется путем ее копирования и редактирования сделанной копии.

Для предустановленных рабочих моделей доступны следующие опции:

New	создание новой рабочей модели;
Copy	создание копии выбранной рабочей модели, с целью ее дальнейшего редактирования;
Export	экспорт выбранной рабочей модели для сохранения на ПК;
Import	импорт рабочей модели из сохраненного файла.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Для созданных пользователем моделей доступны также опции:

Edit	редактирование рабочей модели;
Delete	удаление рабочей модели

Ниже подробно описана структура и параметры рабочей модели, примеры создания новых рабочих моделей для различных сценариев использования терминала приведены в Выбор и создание рабочих моделей.

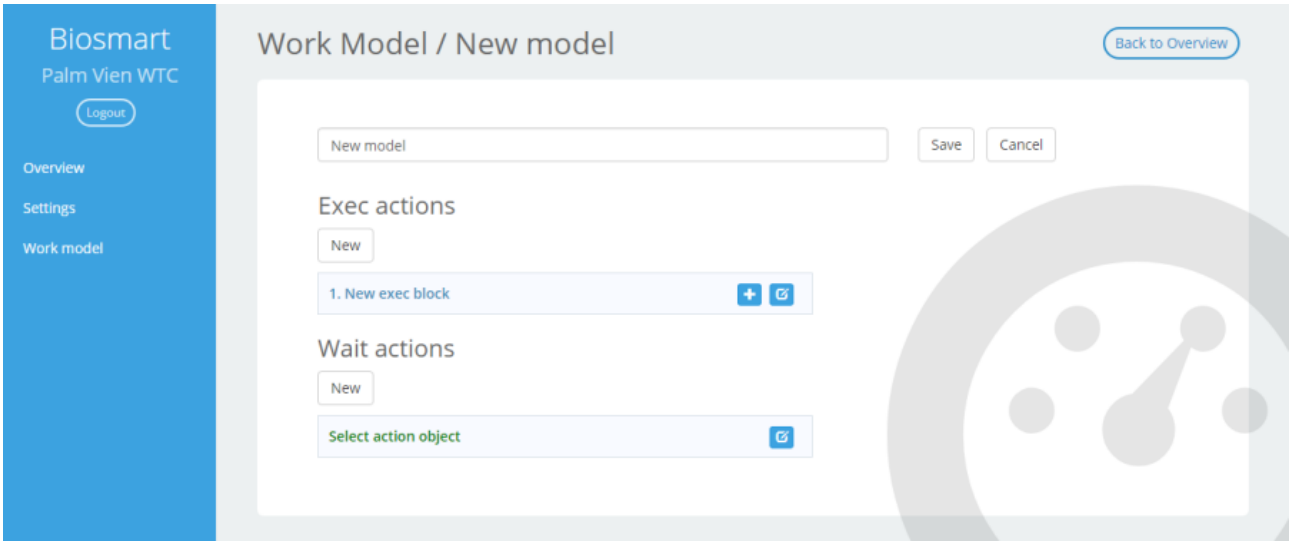
7.3.5 Структура и параметры рабочей модели

В верхней части окна создания рабочей модели находятся:

- поле с редактируемым названием рабочей модели;
- кнопка **Save** для сохранения рабочей модели;
- Кнопка **Cancel** для отмены изменений в рабочей модели.

Окно создания рабочей модели разделено на две части:

- **Exec actions** (блок действий). Каждый блок действий может содержать несколько действий, выполняющихся одновременно.
- **Wait actions** (блок событий). Каждый блок событий может содержать несколько событий, расположенных в иерархической последовательности. При появлении события, расположенного выше в списке, терминал реагирует на него соответствующими действиями блока **Exec actions** и переходит к ожиданию следующего события из текущего блока **Wait actions**.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

В блоках доступны следующие элементы управления:

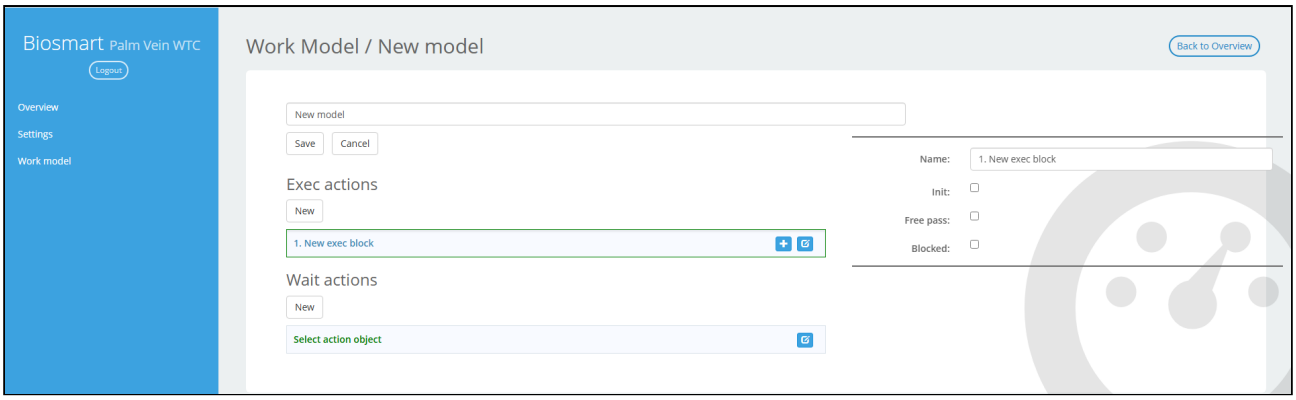
New	создать новый блок;
	развернуть или свернуть список действий/событий в блоке;
	добавить новое действие/событие в блок;
	редактировать выделенное действие/событие (по нажатию в правой части окна открывается редактор **Editor**);
	удалить выделенное действие/событие.

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.

Блок действий имеет следующие параметры:

- **Name** – Название блока
- **Init** – При включении данного пункта, выбранный блок будет выполняться безусловно, при активации данной рабочей модели.
- **Free pass** – режим "Свободный проход". В режиме **Свободный проход** реле контроллера срабатывает и удерживается в этом состоянии до выключения режима.
- **Blocked** – режим "Блокировка прохода". В режиме **Блокировка прохода** реле контроллера удерживается в состоянии **Закрыто** до выключения режима блокировки прохода.



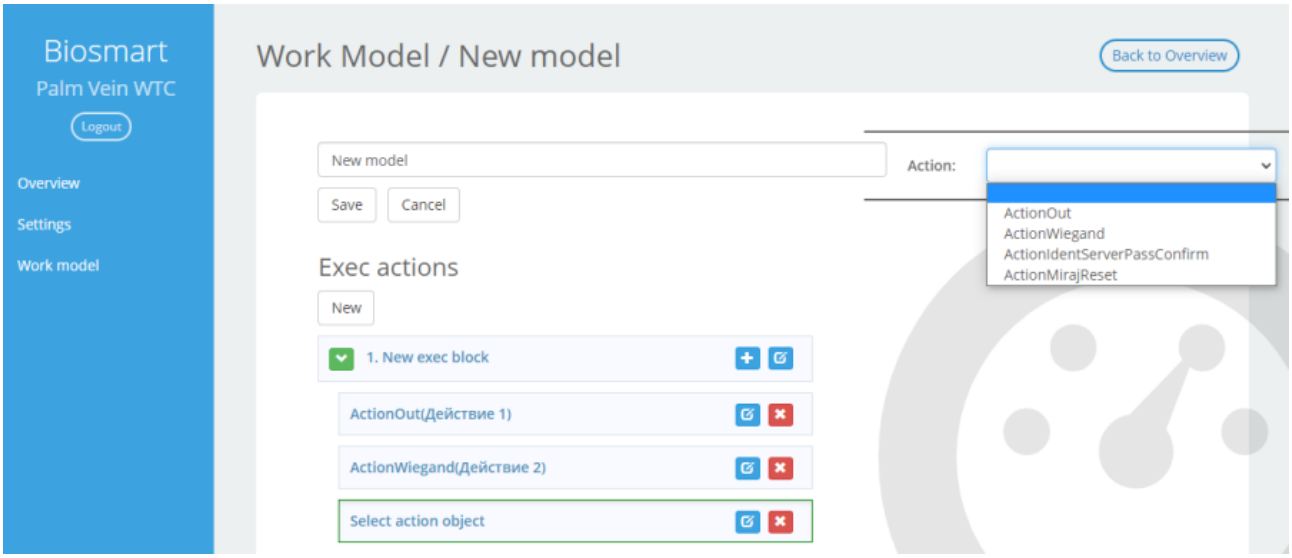
Типы возможных действий:

- **ActionOut** – управление реле
- **ActionWiegand** – передача данных по интерфейсу Wiegand
- **ActionIdentServerPassConfirm** – отправка подтверждения факта прохода на Сервер биометрической идентификации BioSmart (СИ BioSmart). Используется для

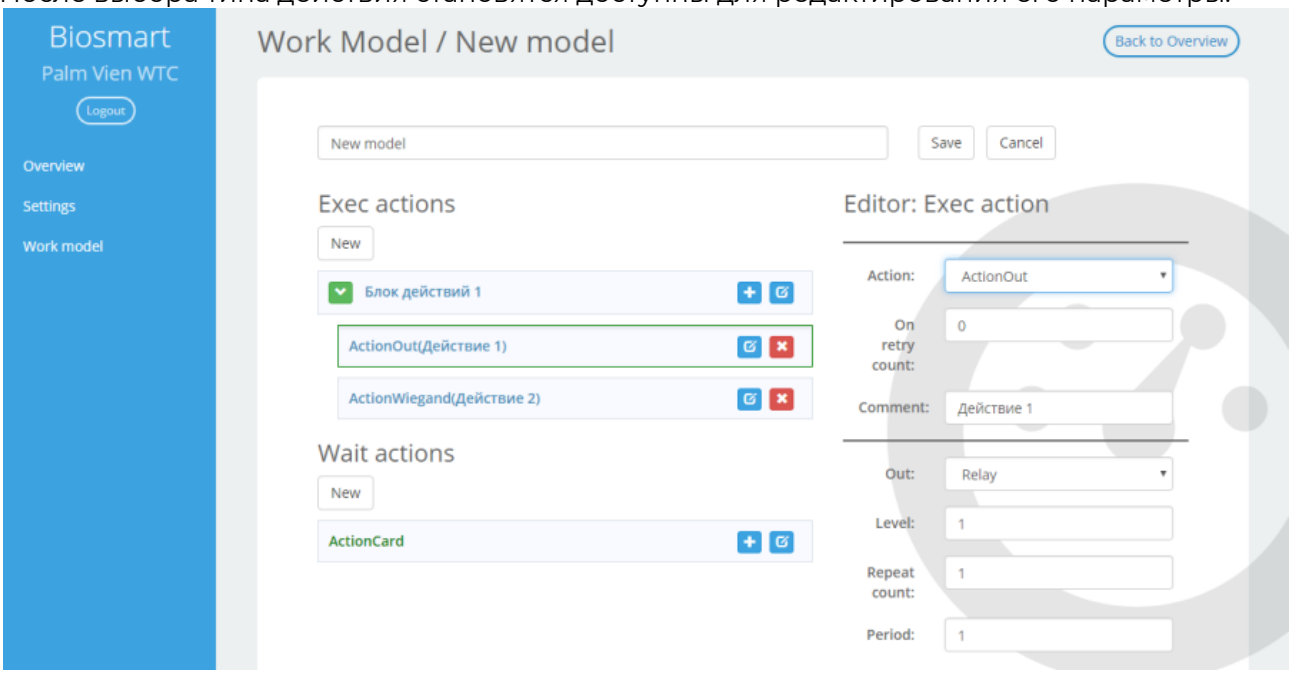
SEC.RU | Короткий путь к информации
Скачано с sec.ru

реализации функции Antipassback в рабочих моделях, где после идентификации на СИ BioSmart выполняются какие-либо проверки (например, на алкоголь).

- **ActionMirajReset** – используется при интеграции с некоторыми охранными системами.



После выбора типа действия становятся доступны для редактирования его параметры.



Для всех типов действий настраиваются общие параметры:

On retry count (Счетчик повторов)	В настоящее время не используется
Comment (Комментарий)	Текстовое описание действия. Будет отображаться рядом с названием.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Дополнительно для каждого типа действий настраиваются параметры:

ActionOut	Out	Выбор реле: **Relay** – встроенное реле терминала **Bur 1** – реле 1 блока управления реле (БУР BioSmart) **Bur 2** – реле 2 блока управления реле (БУР BioSmart)
	Level	Воздействие: **1** – срабатывание реле **0** – возврат реле в исходное состояние на время, заданное параметром **Period**
	Repeat count	Количество повторов срабатывания реле
	Period	Длительность удержания реле в сработавшем состоянии. Задается в миллисекундах.
ActionWiegand	Number	Номер wiegand-выхода (доступен «**Num 0**»)
	Type	Битность wiegand-выхода (**26 bits**, **32 bits**, **64 bits**)
	Length pulse	Ширина импульсов в микросекундах (Рекомендуемое значение – **200**)
	Length interval	Период следования импульсов в микросекундах (Рекомендуемое значение – **2000**)
	Facility Code	Часть кода RFID-карты, общая для многих карт. Используется для обозначения конкретного охраняемого объекта или здания.

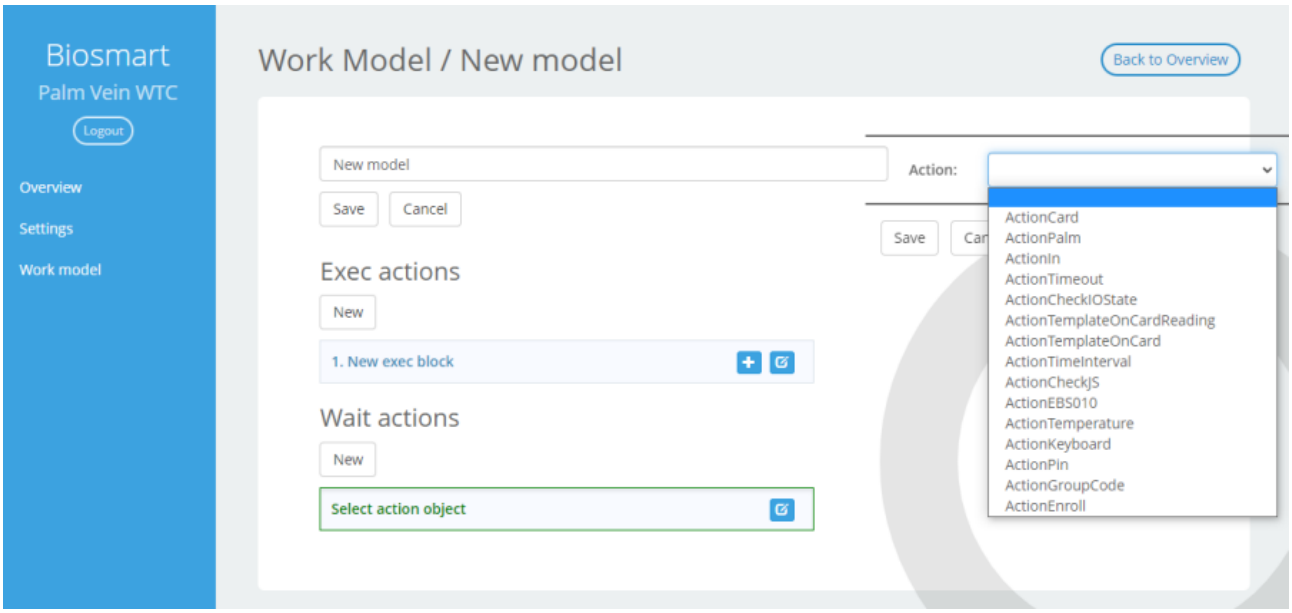
SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Role	Тип передаваемых данных: **Employee id** – код сотрудника **Employee card** – код RFID-карты сотрудника **Employee pin** – пин-код сотрудника **code** – любое число не более 4х байт
ActionIdent **ServerPassConfirm**	**Pass Direction**	Направление прохода сотрудника: **Enter** – Вход **Exit** – Выход

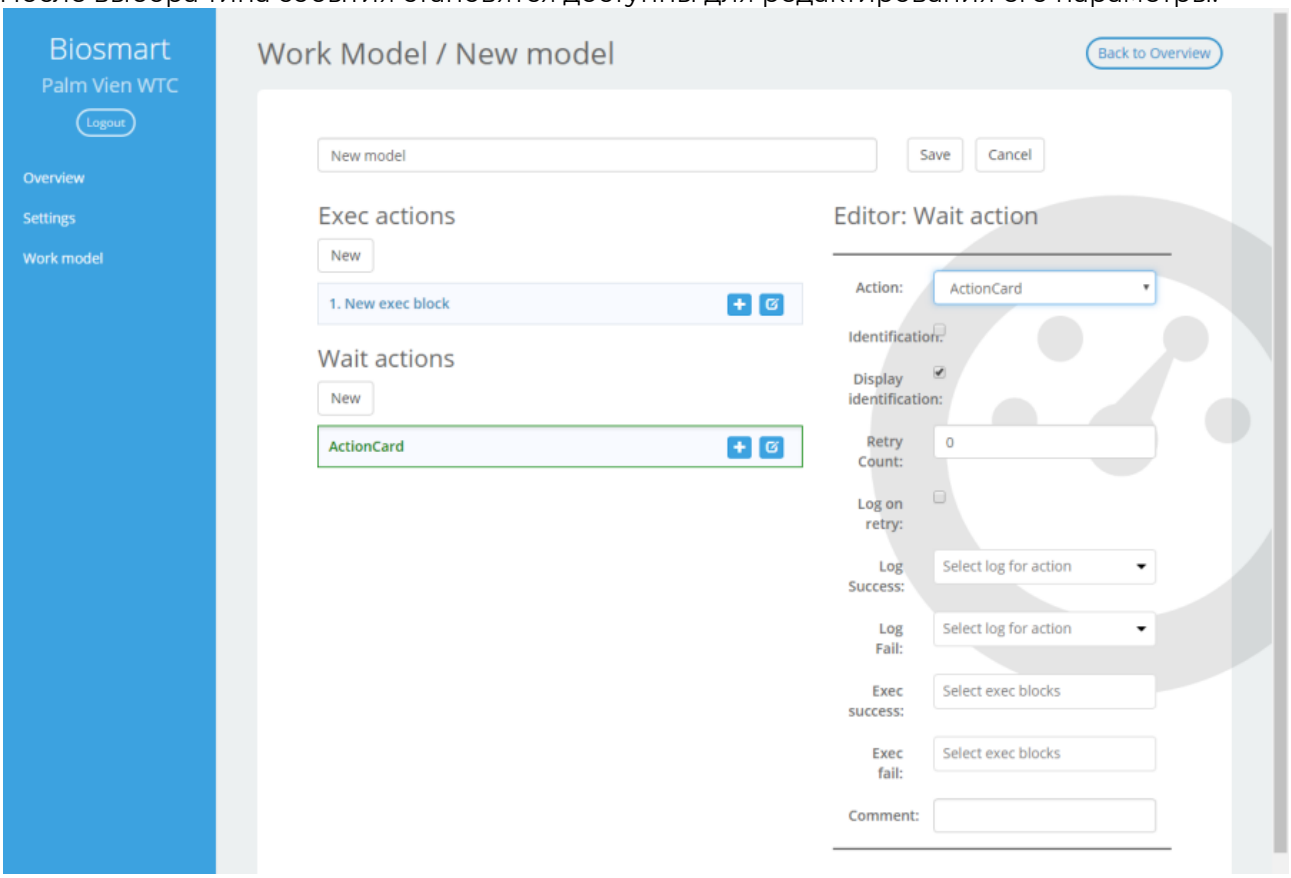
Блок событий (Wait actions)
В блоке доступны для выбора следующие типы событий:

- **ActionCard** – прикладывания RFID-карты к считывателю
- **ActionPalm** – ожидание прикладывания ладони к считывателю
- **ActionIn** – ожидание изменения состояния дискретного входа
- **ActionTimeout** – ожидание окончания временного интервала
- **ActionCheckIOState** в настоящее время не используется
- **ActionTemplateOnCardReading** – ожидание старта считывания биометрического шаблона с зашифрованной области RFID-карты
- **ActionTemplateOnCard** – ожидание считывания биометрического шаблона с зашифрованной области RFID-карты
- **ActionTimeInterval** – производится проверка, попадает ли текущее время в определенный временной интервал, например, с помощью этого компонента может быть проведена проверка не воскресенье ли сегодня, или сейчас рабочее время или нет.
- **ActionCheckJS** в настоящее время не используется.
- **ActionEBS010** – ожидание прохождения проверки на алкоголь
- **ActionTemperature** – ожидание измерения температуры с помощью устройства BioSmart Thermoscan
- **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)

SEC.RU | Короткий путь к информации
Скачано с sec.ru



После выбора типа события становятся доступны для редактирования его параметры.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Для всех типов действий настраиваются общие параметры:

Identification (Идентификация)	В настоящее время не используется
Display identification (Отображение идентификации)	Отображение на дисплее результата идентификации. По умолчанию включено.
Retry Count (Количество попыток идентификации)	Допустимое количество неуспешных попыток идентификации перед тем как будет сформировано событие неуспешной идентификации.
Log on retry (Запись лога при попытке повтора)	При каждой попытке идентификации в ПО Biosmart-Studio v6 будет генерироваться сообщение о результате идентификации. По умолчанию отключено.
Log (Запись лога при поступлении данного события)	Выбор сообщения, которое будет генерироваться в ПО Biosmart-Studio v6 при поступлении данного события. Список возможных сообщений приведен в **Приложение 3**.
Log Success\Fail (Запись лога при успешной\неуспешной идентификации)	Выбор сообщения, которое будет генерироваться в ПО Biosmart-Studio v6 при успешной\неуспешной идентификации. Список возможных сообщений приведен в **Приложение 3**.
Exec (Блоки действий на выполнение)	Выбор действия, являющегося реакцией на поступление данного события
Exec success\fail (Блоки действий на выполнение)	Выбор действия, являющегося реакцией на успешную/неуспешную идентификацию
Comment (Комментарии)	Текстовое описание события. Будет отображаться рядом с названием.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Дополнительно для каждого типа события настраиваются параметры:

ActionCard	Ident server pass direction	Направление про
	Wait pass	Опция предназна подтверждения. С
AcctionPalm	Pass verification without template	Пропускать верис биометрических ц
	Matching level	Параметр, опред биометрическим доступа (FAR) пока • **Highest** – 10^{-8} • **High** – 10^{-7} • **Intermediate** – 1 • **Low** – 10^{-5} • **Very Low** – 10^{-4} • **Lowest** – 10^{-3}
	Multiaccess	Режим одновреме **Slave** – ожидается **Master** – ладонь со **Any** – любого
	Ident server pass direction	Направление про

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Wait pass	Опция предназна подтверждения. С
	Exec on alarm palm	Выбор действия, я
ActionIn	Number	Номер дискретно **Input 0** – дискретн **Input Bur 0** – дискр **Input Bur 1** – дискр **Input Bur 2** – дискр **Input Bur 3** – дискр
	Level	Уровень сигнала: **1** – приемом сигна **0** – приемом сигна
ActionTimeout	Interval	Длительность инт
	Timer text	Сообщение, отобр
ActionTimeInterval	Mon - Sun	Выбор дней недел
ActionEBS010	Identifications for alcohol test	Параметр, задаю проверка): **0** или **1** – проверка **N > 1** – проверка на

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Selective alcohol test	Опция, при которо
	Log for skipped check	Выбор сообщения алкоголь
ActionKeyboard	Key	Кнопка, нажатие к
ActionGroupCode	Default	Если опция включ
ActionEnroll	Type	Определяет тип р **Palm** – шаблон ве **Card** – код карты **Pin** – пин-код

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8 РАБОТА С ТЕРМИНАЛОМ BIOSMART PV-WTC

8.1 Редактирование данных сотрудника на терминале

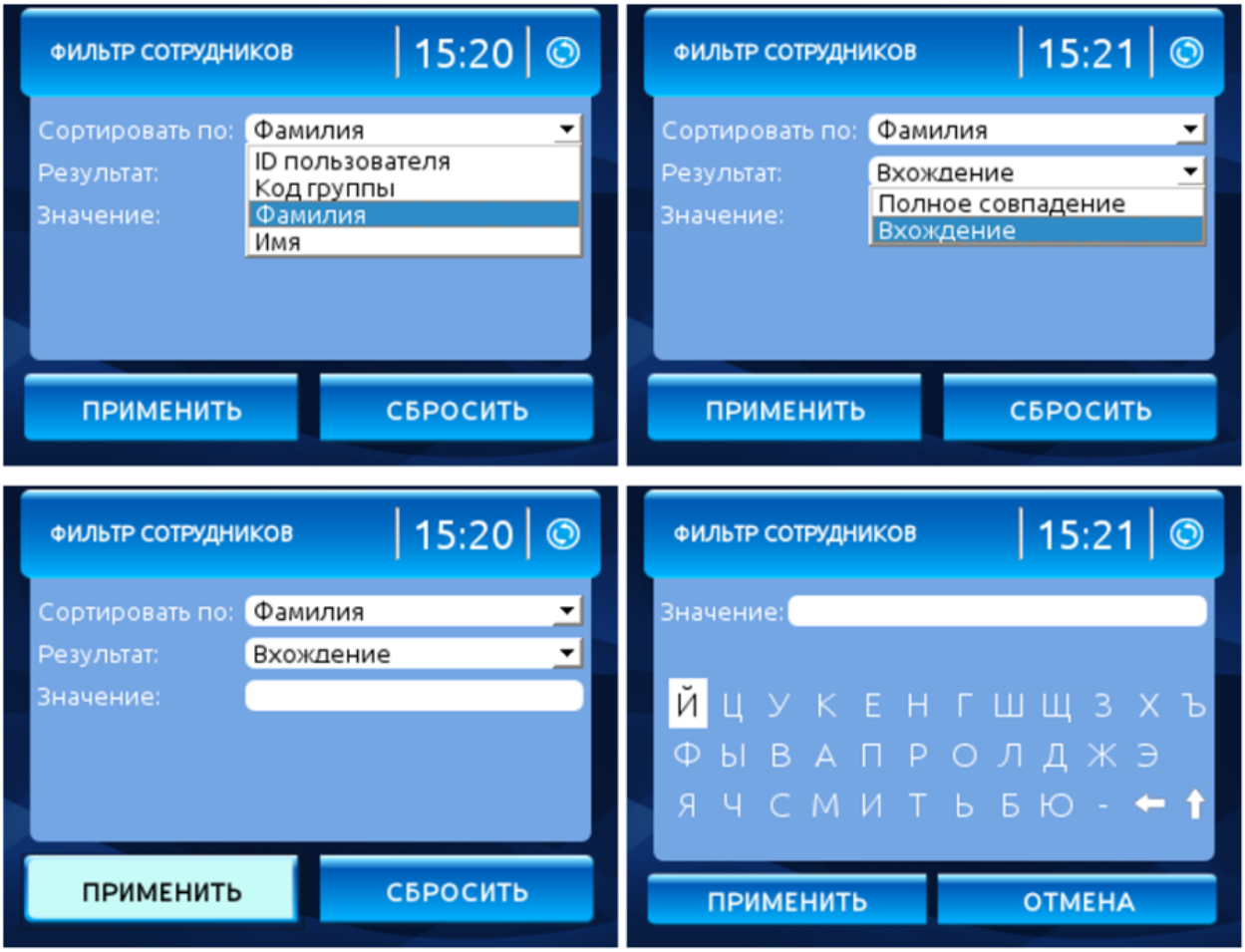
Меню терминала позволяет редактировать следующие данные сотрудника:

- **Шаблоны вен ладоней**
- **Код RFID- карты**
- **Пин-код**

Перейдите в меню терминала в раздел **Сотрудники**.
Воспользуйтесь фильтром для поиска сотрудника, данные которого нужно отредактировать.

1. Фильтр поиска сотрудников

На рисунках показаны параметры **Фильтра сотрудников**.



- **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.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

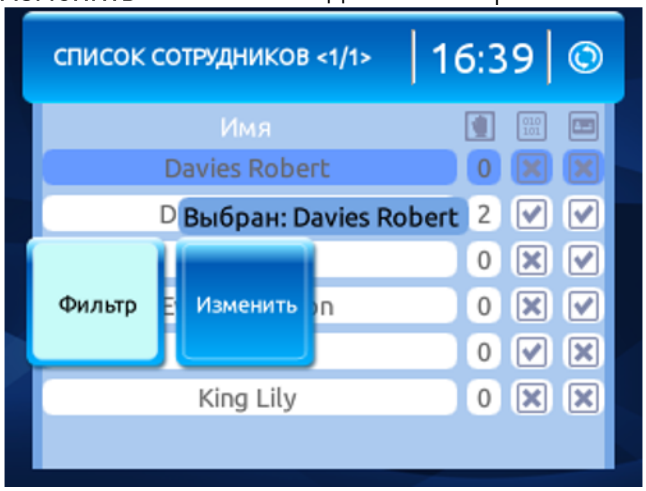
- **Значение:** – точные имя/фамилия сотрудника или фрагмент имени/фамилии.

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

После применения фильтров и нажатия клавиши **Применить** на дисплее отобразится список сотрудников.

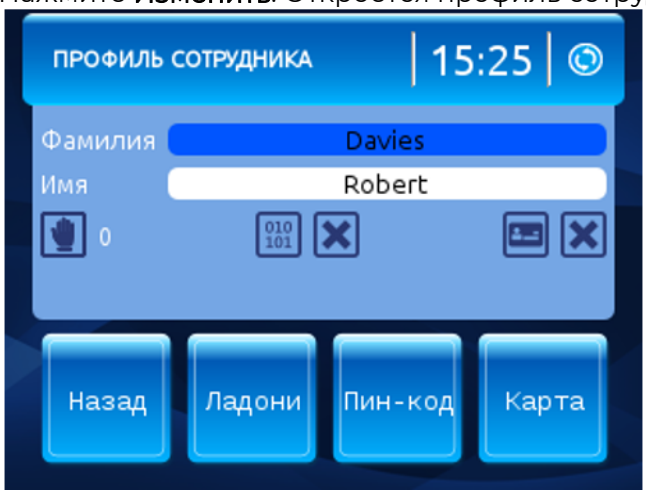


Иконки справа указывают на наличие в базе терминала шаблонов вен ладоней, кода карты и пин-кода сотрудника.
Выберите сотрудника и нажмите кнопку **5**. Откроется меню редактирования данных выбранного сотрудника. Доступны следующие пункты:
Фильтр – возврат к настройкам фильтра поиска;
Изменить – изменение данных выбранного сотрудника.



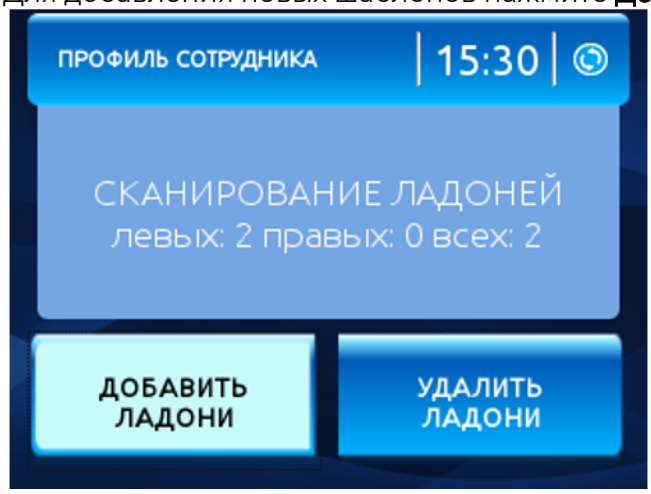
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Нажмите **Изменить**. Откроется профиль сотрудника.

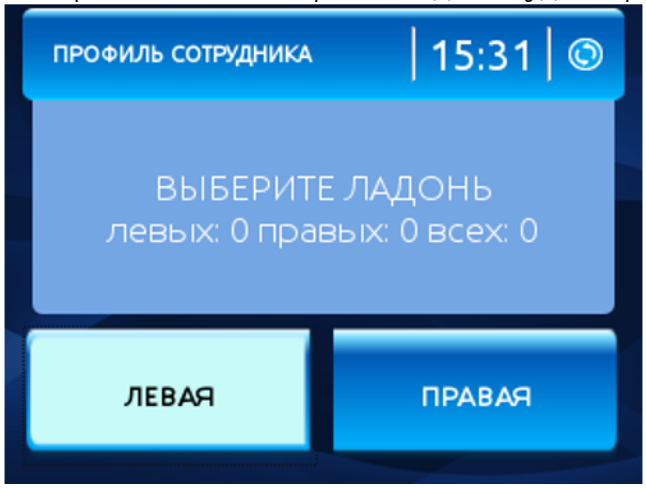


2. Добавление и удаление биометрических шаблонов вен ладоней

Для добавления/удаления шаблонов выберите **Ладони**.
Для добавления новых шаблонов нажмите **Добавить ладони**.

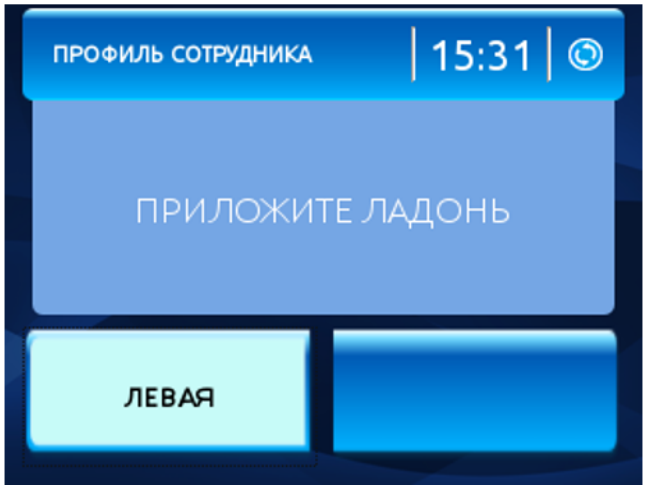


Выберите левая или правая ладонь будет зарегистрирована.

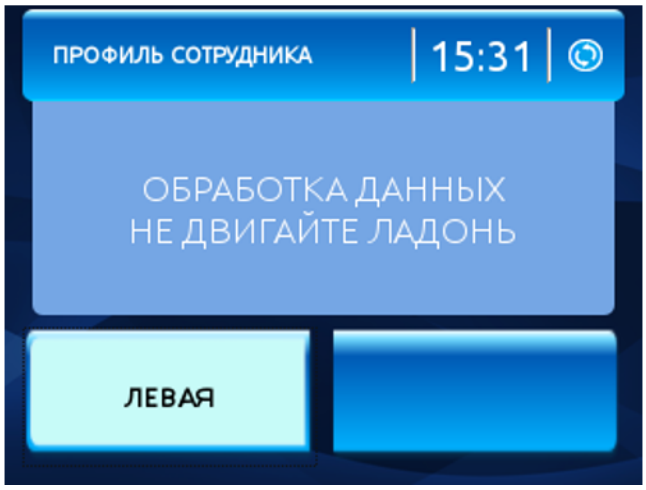


На дисплее появится надпись: «**Приложите ладонь**».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

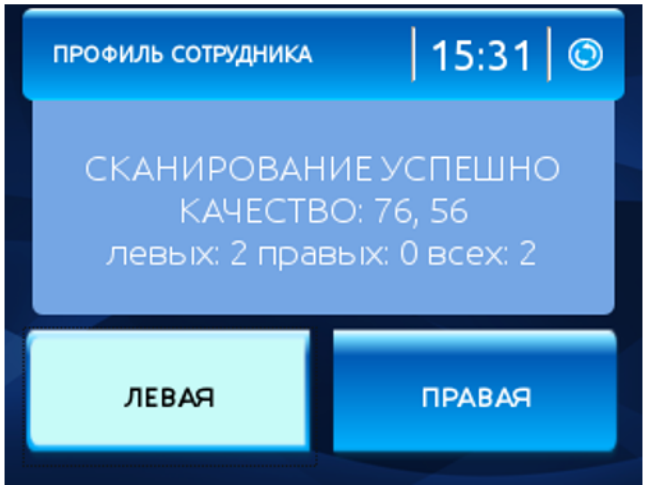


Если ладонь располагается правильно (см. Правила прикладывания ладони к сканеру терминала), то на дисплее появится надпись «**Обработка данных. Не двигайте ладонь**», а затем, через несколько секунд «**Уберите ладонь**». После этого терминал попросит ещё раз приложить ладонь для завершения процесса регистрации. Если ладонь расположена неправильно, то на дисплее появится надпись с низким значением качества шаблона, тогда нужно правильно приложить ладонь снова, чтобы создать шаблон.

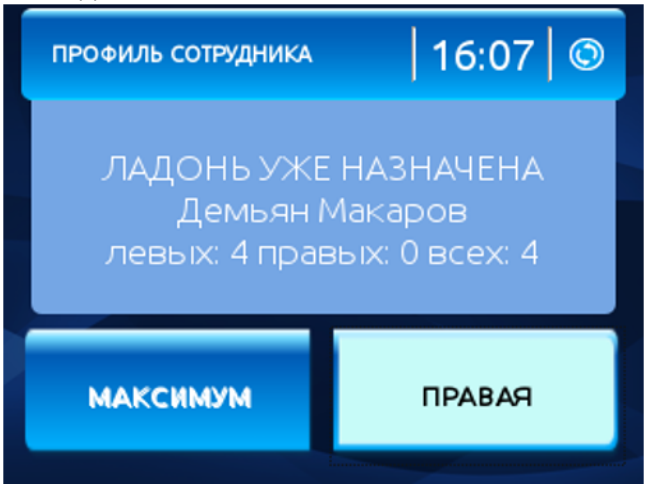


При успешной регистрации прозвучит длинный звуковой сигнал и появится надпись: «**Сканирование успешно**», также будет показано качество шаблона и общее количество шаблонов.

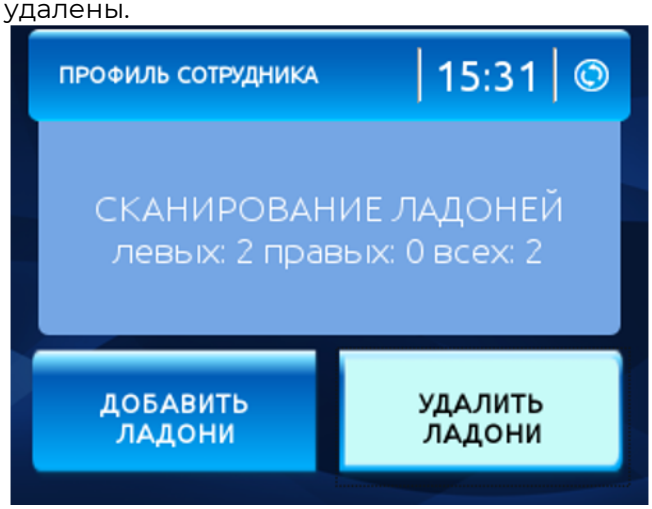
SEC.RU | Короткий путь к информации
Скачано с sec.ru



Если обнаружено совпадение с уже имеющимися шаблонами, то появится надпись: «**Ладонь уже назначена**» с указанием имени сотрудника, с которым обнаружено совпадение.



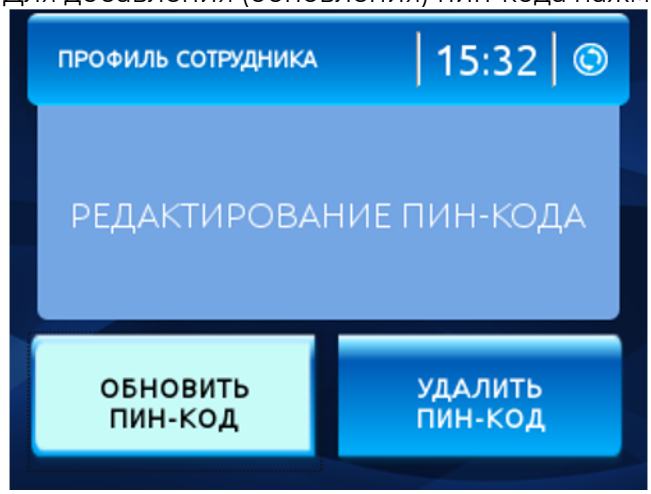
Для удаления шаблонов выберите **Удалить ладони**. В результате все шаблоны будут удалены.



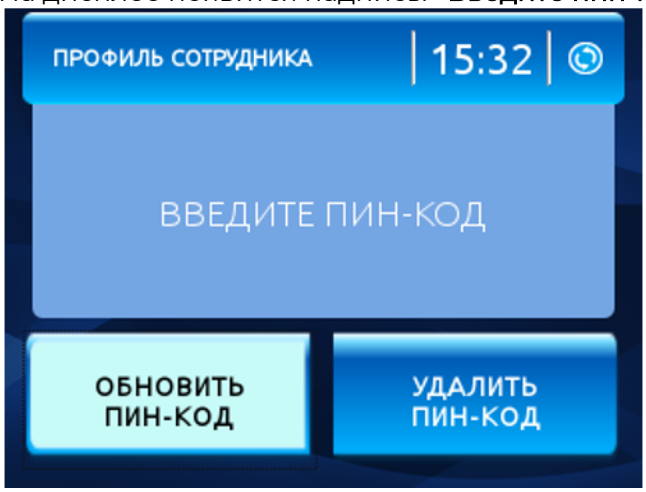
SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. Добавление и удаление пин-кода

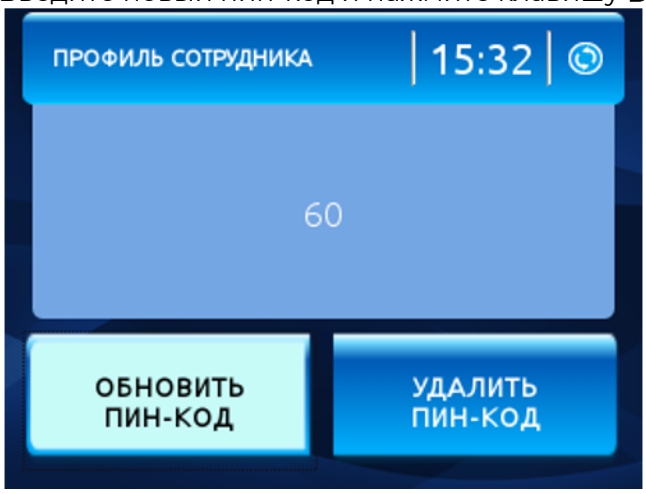
Для добавления/удаления пин-кода выберите **Пин-код**.
Для добавления (обновления) пин-кода нажмите **Обновить пин-код**.



На дисплее появится надпись: «**Введите пин-код**».

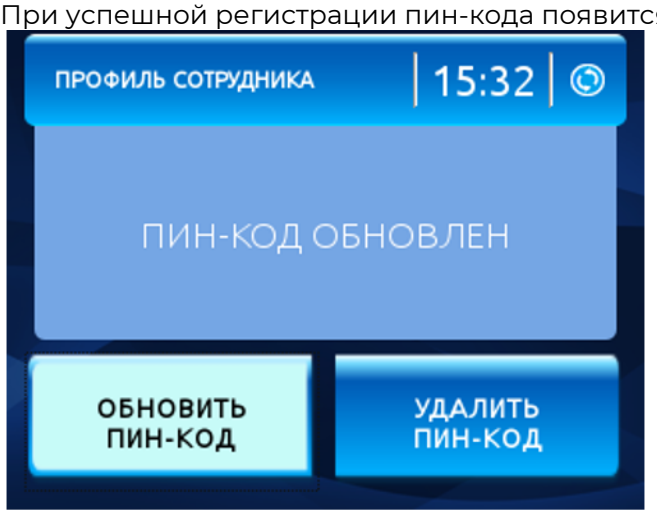


Введите новый пин-код и нажмите клавишу **Ввод**  .



SEC.RU | Короткий путь к информации
Скачано с sec.ru

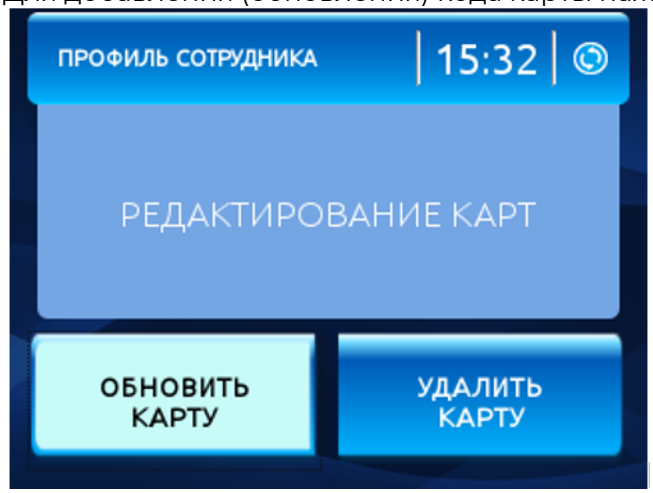
При успешной регистрации пин-кода появится надпись: «**Пин-код обновлен**».



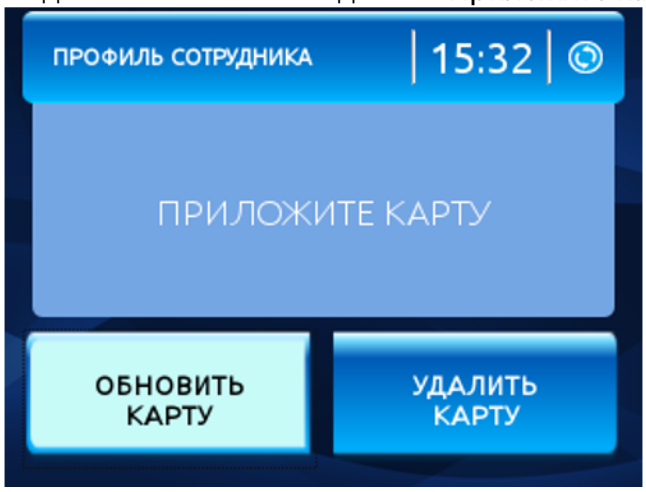
Для удаления пин-кода выберите **Удалить пин-код**. В результате пин-код будет удален.

4. Добавление и удаление кода карты

Для добавления/удаления кода карты выберите **Карта**.
Для добавления (обновления) кода карты нажмите **Обновить карту**.

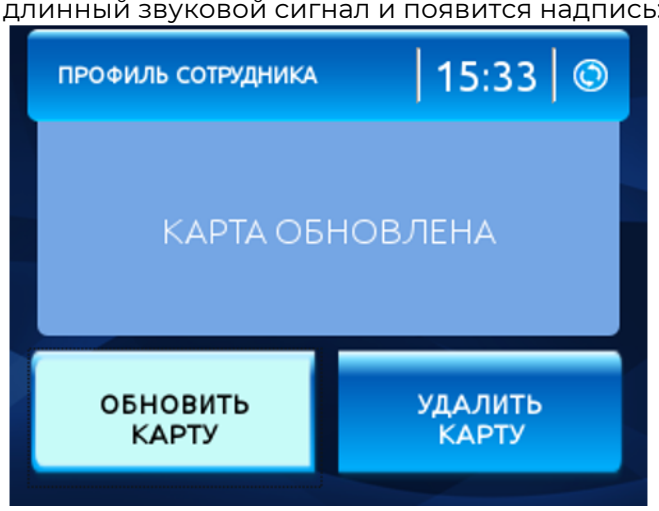


На дисплее появится надпись: «**Приложите карту**».

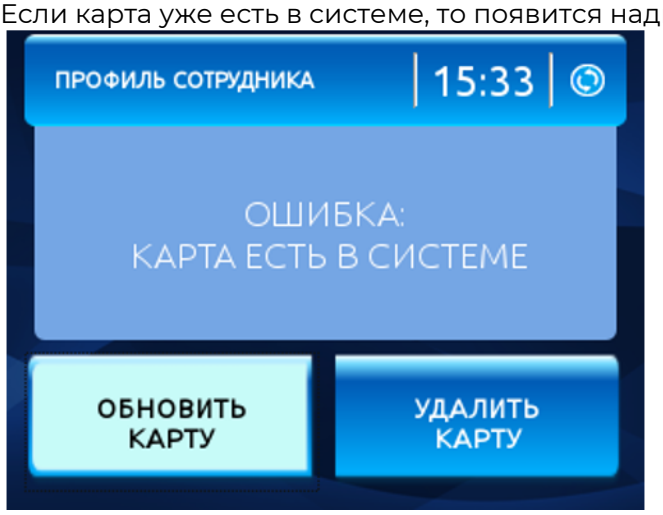


SEC.RU | Короткий путь к информации
Скачано с sec.ru

Приложите карту к терминалу. При успешной регистрации кода карты прозвучит длинный звуковой сигнал и появится надпись: «**Карта обновлена**».



Если карта уже есть в системе, то появится надпись: «**Ошибка. Карта есть в системе**».



Для удаления кода карты выберите **Удалить карту**. В результате код карты будет удален.

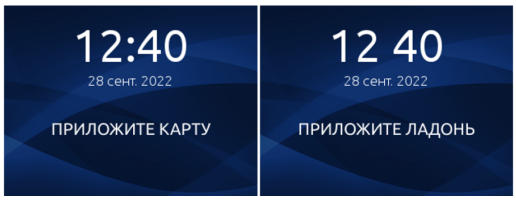
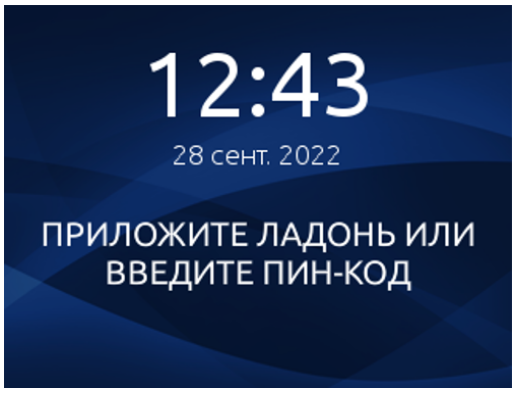
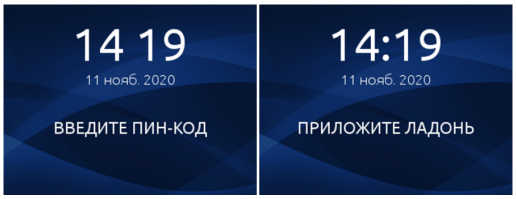
8.2 Выбор и создание рабочих моделей

8.2.1 Предустановленные рабочие модели

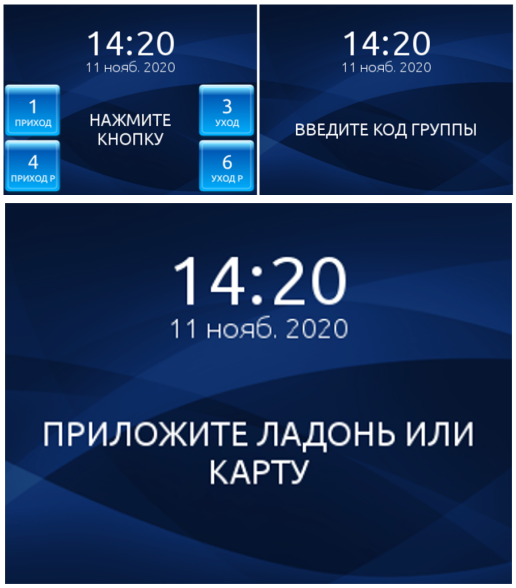
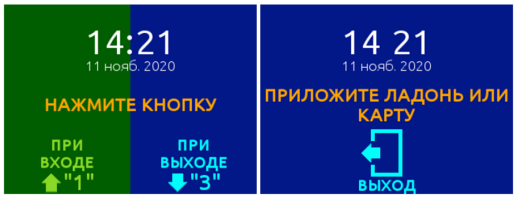
Терминал имеет ряд предустановленных рабочих моделей, отвечающих наиболее частым сценариям использования.

Описание предустановленных рабочих моделей приведено ниже:

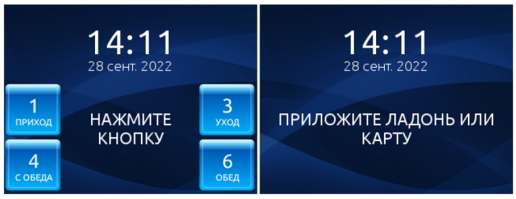
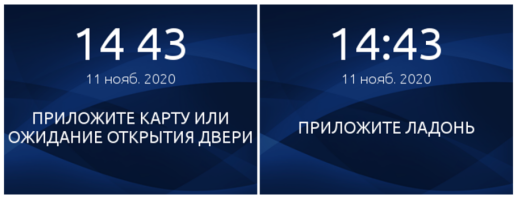
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим работы	Описание	
Ладонь или карта	Терминал ожидает прикладывания ладони или карты. При успешной идентификации будет формироваться событие «**Идентификация сотрудника успешна**».	
Карта + ладонь	Терминал ожидает прикладывания карты. После успешной идентификации по карте ожидается прикладывание ладони. При успешной идентификации по ладони будет формироваться событие «**Идентификация сотрудника успешна**».	
Ладонь или пин-код	Терминал ожидает прикладывания ладони или ввода пин-кода. При успешной идентификации будет формироваться событие «**Идентификация сотрудника успешна**».	
Пин-код + ладонь	Терминал ожидает ввода пин-кода. После успешной идентификации по пин-коду ожидается прикладывание ладони. При успешной идентификации по ладони будет формироваться событие «**Идентификация сотрудника успешна**».	

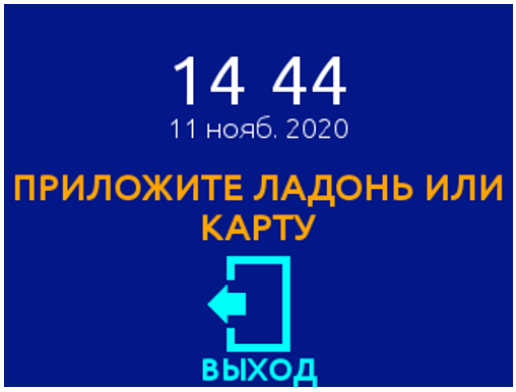
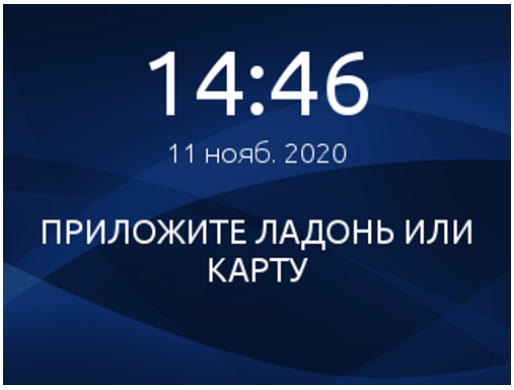
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим работы	Описание	
Кн. вх/вых + код группы + ладонь или карта	Терминал ожидает нажатия соответствующей кнопки на клавиатуре. В случае нажатия кнопок 1 или 3 требуется ввод кода группы, затем идентификация по ладони или карте. В случае нажатия кнопок 4 или 6 ввод кода группы не требуется (он берется из настроек терминала), требуется идентификация по ладони или карте. При успешной идентификации будет формироваться событие «**Вход сотрудника**» или «**Выход сотрудника**». Данная рабочая модель используется в случае большой базы данных и позволяет проводить предварительную выборку ограниченного списка сотрудников из базы данных для проведения идентификация. Подробное описание данной рабочей модели и необходимые настройки для ее использования приведены в Использование рабочей модели «Кн. вх/вых + код группы + ладонь/карта»	
Кн. вх/вых + ладонь или карта	Терминал ожидает нажатия соответствующей кнопки на клавиатуре. Затем требуется идентификация по ладони или карте. При успешной идентификации будет формироваться событие «**Вход сотрудника**» или «**Выход сотрудника**.	
Ладонь или карта или кнопка	Терминал ожидает прикладывания ладони/карты или нажатия кнопки (замыкания контактов IN и IN+). При успешной идентификации по ладони или карте будет формироваться событие «**Идентификация сотрудника успешна**», а в случае нажатия кнопки будет формироваться событие «**Открытие по кнопке**». Формирование событий сопровождается срабатыванием встроенного реле.	

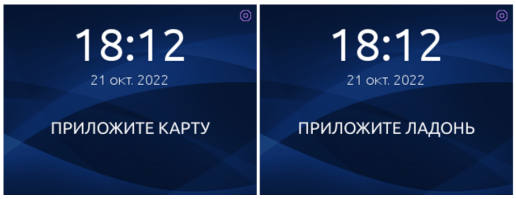
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим работы	Описание	
Кн. вх/вых + обед + ладонь или карта	Терминал ожидает нажатия соответствующей кнопки на клавиатуре. Доступны варианты «**Приход**», «**Уход**», «**С обеда**», «**Обед**». Затем требуется идентификация по ладони или карте. При успешной идентификации будут формироваться события «**Вход сотрудника/Выход сотрудника**» и «**Выход на обед/Вход с обеда**».	
Карта + ладонь или кнопка	Терминал ожидает прикладывания карты или нажатия кнопки (замыкания контактов IN и IN+). После успешной идентификации по карте, требуется идентификация по ладони. При успешной идентификации по ладони будет формироваться событие «**Идентификация сотрудника успешна**», а в случае нажатия кнопки будет формироваться событие «**Открытие по кнопке**». Формирование событий сопровождается срабатыванием встроенного реле.	
Вход по кнопкам + ладонь или карта	Терминал ожидает прикладывания ладони или карты. При успешной идентификации будет формироваться событие «**Вход сотрудника**». Нажимать кнопки не требуется. Подразумевается, что терминал работает только в направлении «Вход».	

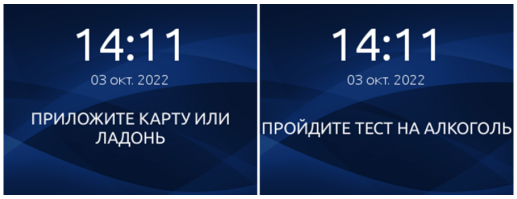
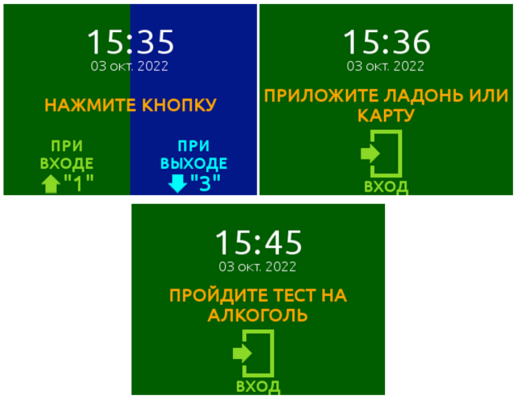
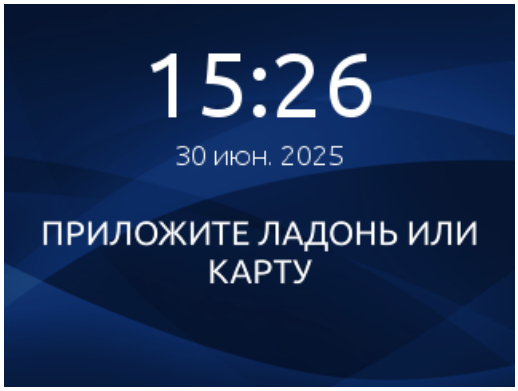
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим работы	Описание	
Выход по кнопкам + ладонь или карта	Терминал ожидает прикладывания ладони или карты. При успешной идентификации будет формироваться событие «**Вход сотрудника**». Нажимать кнопки не требуется. Подразумевается, что терминал работает только в направлении «Выход»	
Помещение для хранения ценностей	В настоящее время не используется.	
Карта или Пин + Ладонь	Терминал ожидает прикладывания карты или ввода пин-кода. После успешной идентификации по карте или пин-коду ожидается прикладывание ладони. При успешной идентификации по ладони будет формироваться событие «**Идентификация сотрудника успешна**».	
Ладонь или Карта + Действие	Терминал ожидает прикладывания ладони или карты. При успешной идентификации будет формироваться событие «**Идентификация сотрудника успешна**», срабатывать встроенное реле и передаваться код карты по интерфейсу Wiegand.	

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим работы	Описание	
Шаблон на карте	Терминал ожидает считывания биометрического шаблона с защищенной области памяти карты, приложенной к RFID-считывателю. После считывания шаблона терминал ожидает прикладывания ладони. Если биометрические данные ладони соответствуют шаблону с карты, будет формироваться событие «**Идентификация сотрудника успешна**». Рабочая модель «Шаблон на карте» используется в случаях, когда необходимо исключить хранение биометрических шаблонов в базе данных и их передачу по сети. Рабочая модель «Шаблон на карте» поддерживается терминалами BioSmart PV-WTC-MF и применяется с картами Mifare Classic 4K, Mifare Plus SL1 4K, Mifare Plus SL3 4K, Mifare Desfire EV1 4K/ 8K. Подробную информацию можно найти в Описание работы СКУД BioSmart в режиме "Шаблон на карте".	
Ладонь или карта Алко	В настоящее время не используется.	
Кн. вх/ вых + ладонь или карта + Алко	В настоящее время не используется.	

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Режим работы	Описание	
Ладонь или карта + алкотестер USB	Терминал ожидает прикладывания ладони или карты. При успешной идентификации формируется событие «**Идентификация сотрудника успешна**» и происходит проверка на алкоголь с помощью алкотестера. При успешном прохождении проверки будет формироваться событие «**Тест на алкоголь пройден успешно**», срабатывать встроенное реле и передаваться код карты по интерфейсу Wiegand.	
Кн. вх/вых + ладонь или карта + алкотестер USB	Терминал ожидает нажатия соответствующей кнопки на клавиатуре. Затем требуется идентификация по ладони или карте. При успешной идентификации будет формироваться событие «**Вход сотрудника**» или «**Выход сотрудника**» и происходит проверка на алкоголь с помощью алкотестера. При успешном прохождении проверки будет формироваться событие «**Тест на алкоголь пройден успешно**», срабатывать встроенное реле и передаваться код карты по интерфейсу Wiegand.	
Ладонь или Карта + ладонь	Терминал ожидает прикладывания карты или ладони. После успешной идентификации по ладони формируется событие «**Идентификация сотрудника успешна**», срабатывает встроенное реле и передается код карты по интерфейсу Wiegand. После успешной идентификации по карте ожидается прикладывание ладони. При успешной идентификации по ладони формируется событие «**Идентификация сотрудника успешна**», срабатывает встроенное реле и передается код карты по интерфейсу Wiegand.	

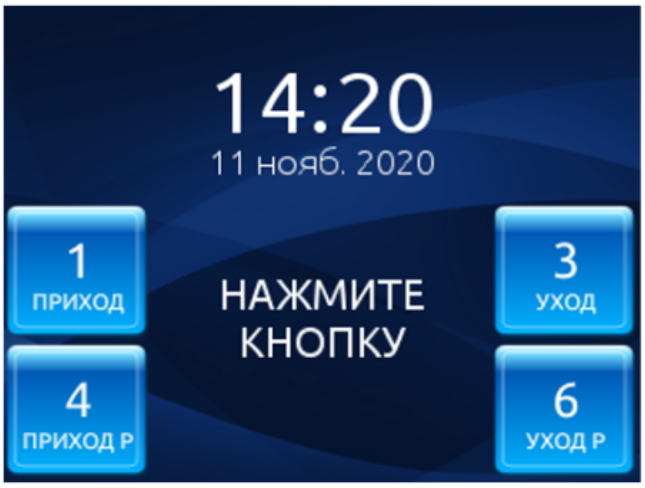
SEC.RU | Короткий путь к информации
Скачано с sec.ru

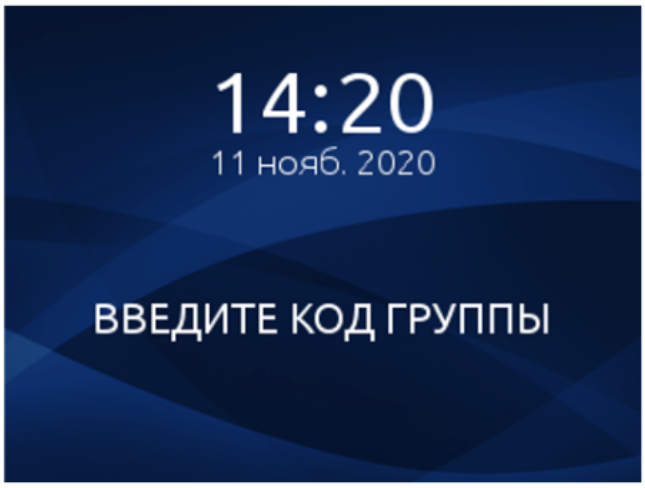
8.2.2 Использование рабочей модели «Кн. вх/вых + код группы + ладонь/карта»

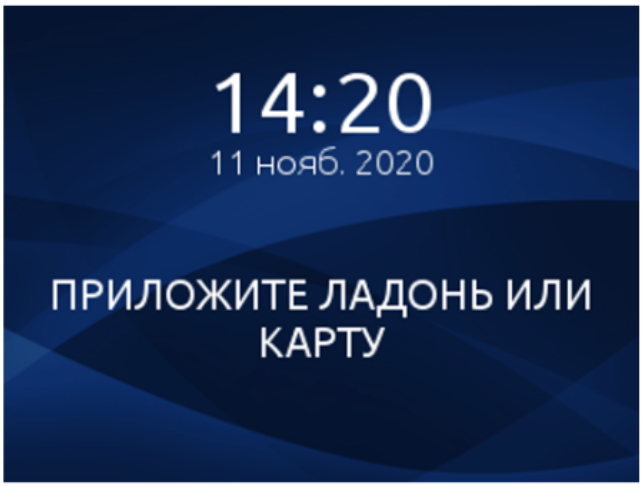
Описание рабочей модели

Рабочая модель **Кн. вх/вых + код группы + ладонь/карта** используется для ускорения идентификации в случае большой базы данных, например, базы данных персонала крупной сети магазинов. Сеть магазинов как правило имеет несколько филиалов. В каждом филиале свой штат сотрудников, но иногда сотрудники одного филиала выходят на работу в другой, например, на замену или в командировку.
В рабочей модели **Кн. вх/вых + код группы + ладонь/карта** идентификация каждого сотрудника проводится не по всей базе сети магазинов, а только по списку сотрудников того филиала, в котором числится идентифицируемый сотрудник. Это реализовано за счет присвоения каждому филиалу кода группы, а каждому сотруднику пин-кода, равного коду группы филиала, в котором он числится.
При идентификации на терминале сотрудник вводит свой пин-код, и таким образом ограничивает базу данных для идентификации только своим филиалом.
Если сотрудник вышел на работу в другой филиал, то он нажимает на терминале кнопку **1** (**ПРИХОД**) или **3** (**УХОД**), **вводит номер филиала, в котором числится** (свой пин-код), и идентифицируется по ладони или карте.
Если сотрудник вышел на работу в свой филиал, то нажимает на терминале кнопку **4** (**ПРИХОД Р**) или **6** (**УХОД Р**) и идентифицируется по ладони или карте. Вводить номер филиала (пин-код) в этом случае не требуется, он берется из настроек терминала. В настройках каждого терминала устанавливается код группы по умолчанию, равный коду группы филиала, в котором терминал установлен.

SEC.RU | Короткий путь к информации
Скачано с sec.ru





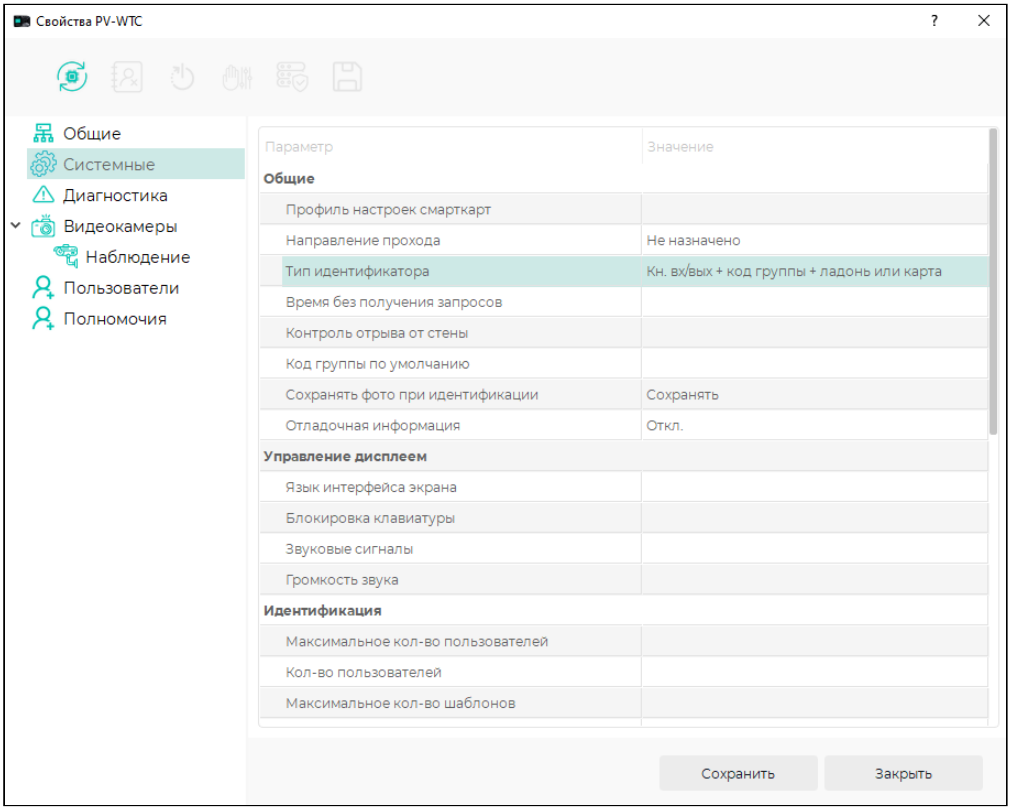


В пределах одного филиала могут быть сотрудники-**совместители**.
Если сотрудник является **совместителем**, после нажатия кнопки **4** (**ПРИХОД Р**) / **6** (**УХОД Р**) и идентификации по ладони/карте на дисплее появится список должностей. С помощью кнопок перемещения **2** (**Вверх**) / **8** (**Вниз**) нужно выбирать необходимую должность и нажать **Enter**.
Во всех вышеописанных случаях при успешной идентификации в ПО Biosmart-Studio будет формироваться событие «**Вход сотрудника**» или «**Выход сотрудника**».

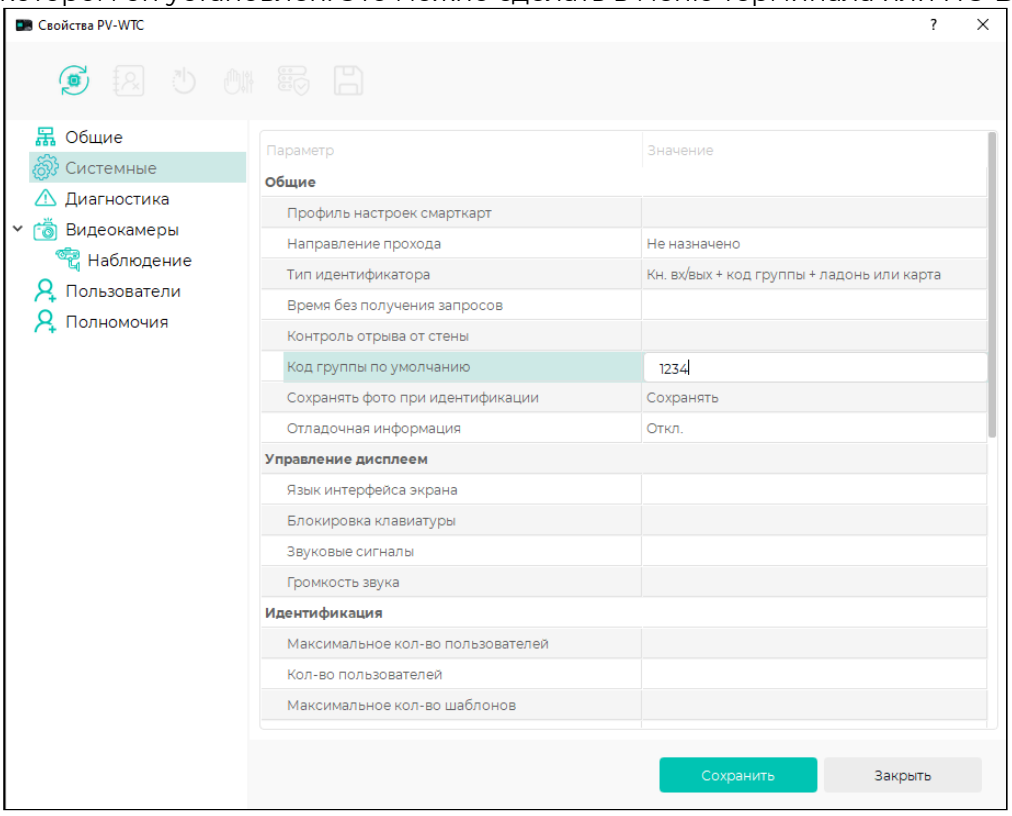
Порядок настройки

Установите на терминале рабочую модель **Кн. вх/вых + код группы + ладонь/карта**. Это можно сделать в меню терминала, в WEB-интерфейсе или ПО Biosmart-Studio v6.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

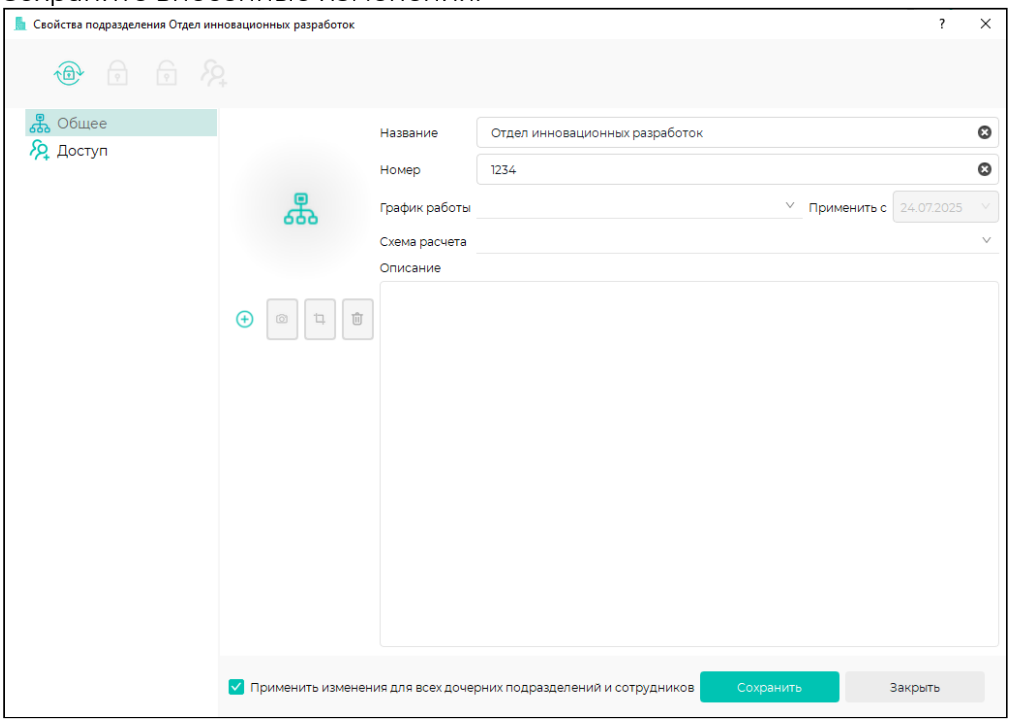


Назначьте каждому терминалу **Код группы по умолчанию**, равный коду группы филиала, в котором он установлен. Это можно сделать в меню терминала или ПО Biosmart-Studio.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

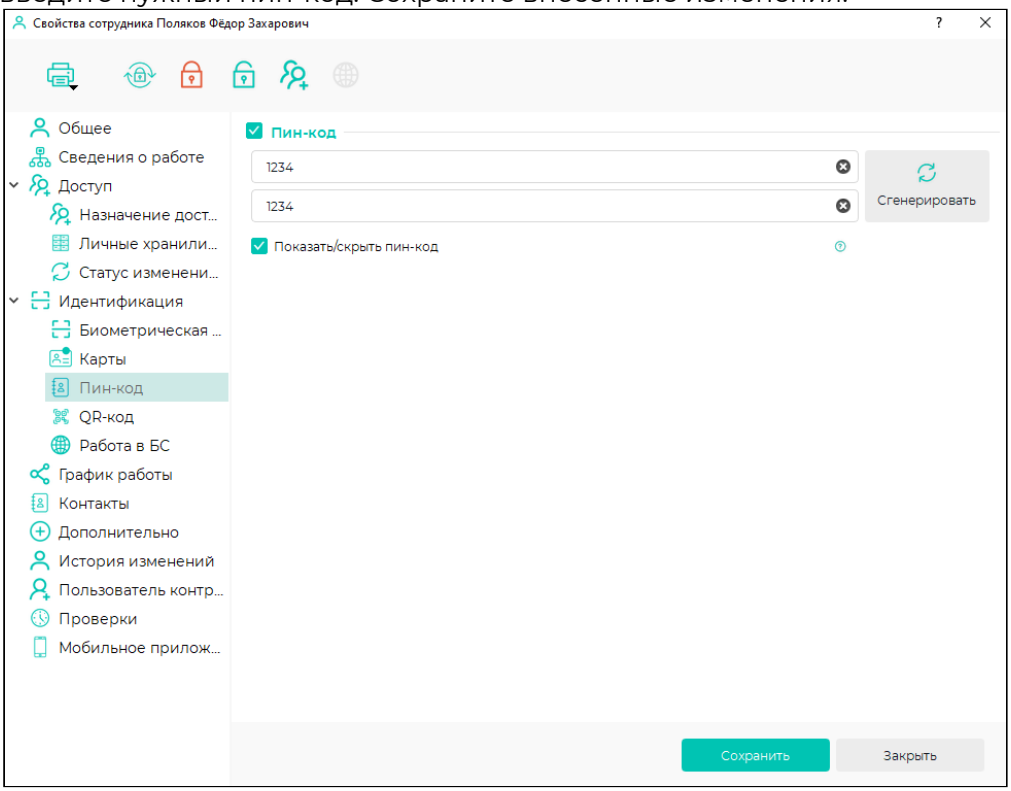
Назначьте код группы каждому филиалу (подразделению). Для этого откройте окно **Свойства подразделения** на вкладке **Общее** и в поле **Номер** введите нужный код группы. Сохраните внесенные изменения.



Назначьте каждому сотруднику пин-код, равный коду группы филиала, в котором он числится. Для этого откройте окно **Свойства сотрудника**, перейдите на вкладку **Пин-код** и

SEC.RU | Короткий путь к информации
Скачано с sec.ru

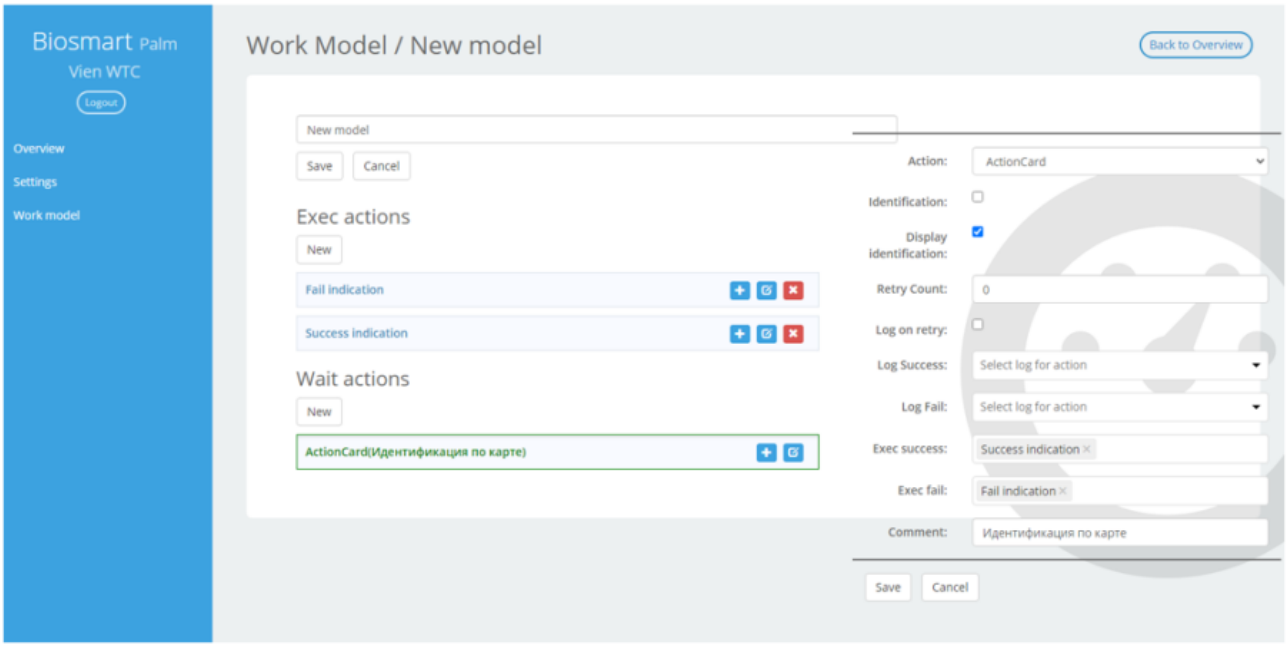
введите нужный пин-код. Сохраните внесенные изменения.



8.2.3 Создание простой рабочей модели

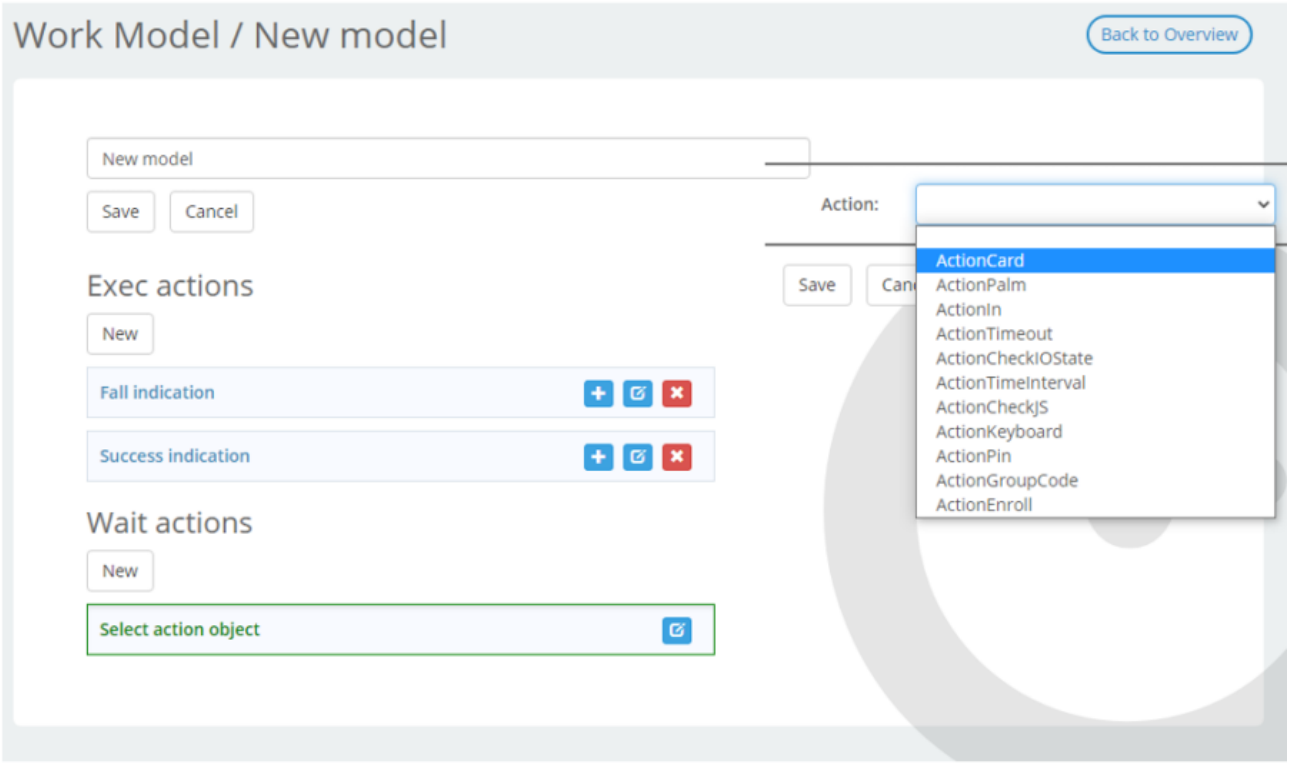
В пункте приведен пример создания простой рабочей модели: идентификация сотрудника по карте.
Терминал ожидает прикладывания карты, после чего происходит проверка наличия данной карты в памяти. В случае успеха вызывается блок действий **Success indication**, в противоположном случае **Fail indication**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



1. Создайте событие, которого будет ожидать терминал, в данном случае это будет приложение карты к считывателю. Для этого:

- В блоке **Wait actions** нажмите кнопку **Редактировать** - 
- В правой части окна выберите событие **ActionCard**.



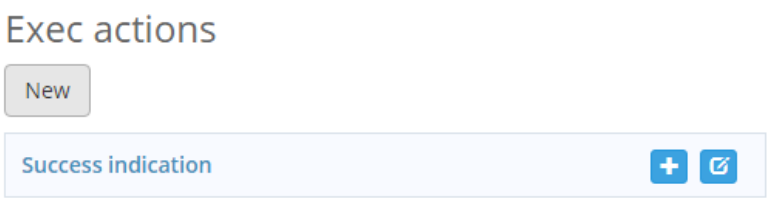
SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. Создайте блоки действий, выполняемых при успешной либо неудачной идентификации.

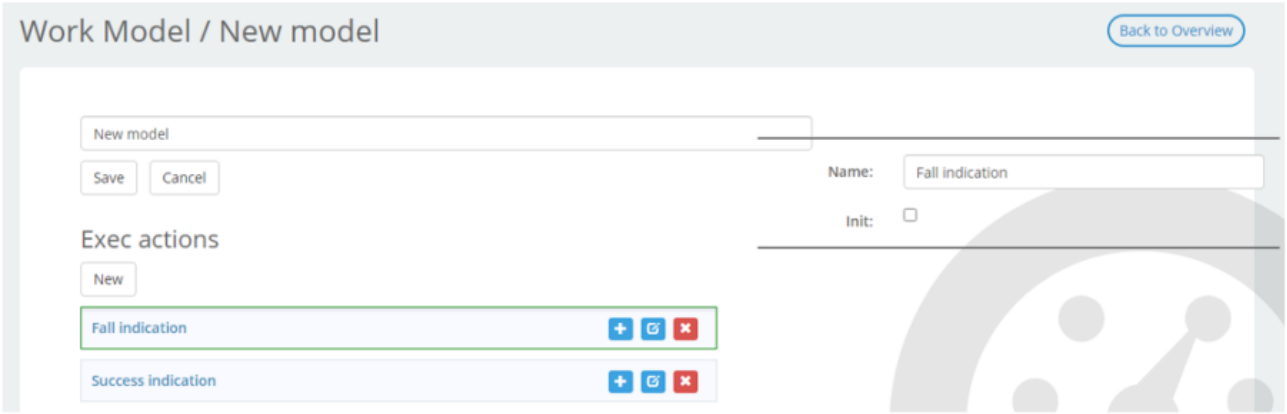
- В блоке **Exec actions** нажмите кнопку **Редактировать**
- В правой части окна введите название выбранного действия. В данном примере это будет блок действий при успешной идентификации (**Success indication**)



- Добавьте также блок действий, выполняющихся при неудачной идентификации. Нажмите кнопку **New** в блоке **Exec action**



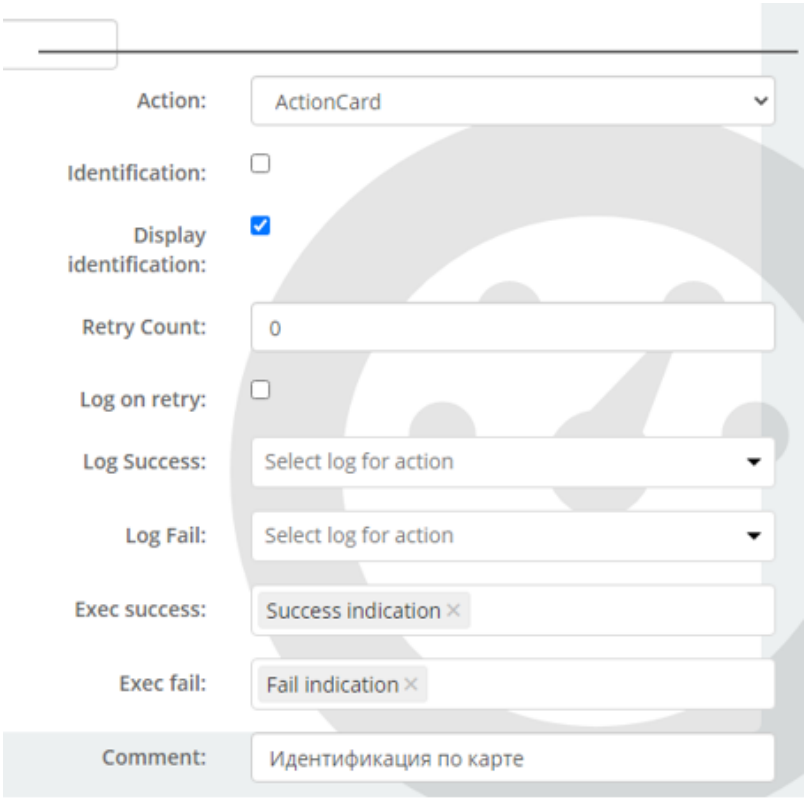
- Отредактируйте название созданного блока аналогично первому блоку.



3. Свяжите блок события и блоки действий.

- В блоке **Wait actions** нажмите кнопку **Редактировать**
- В правой части окна в поле **Exec success** выберите из выпадающего списка пункт **Success indication**. Аналогично в поле **Exec fail** выберите пункт **Fail indication**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



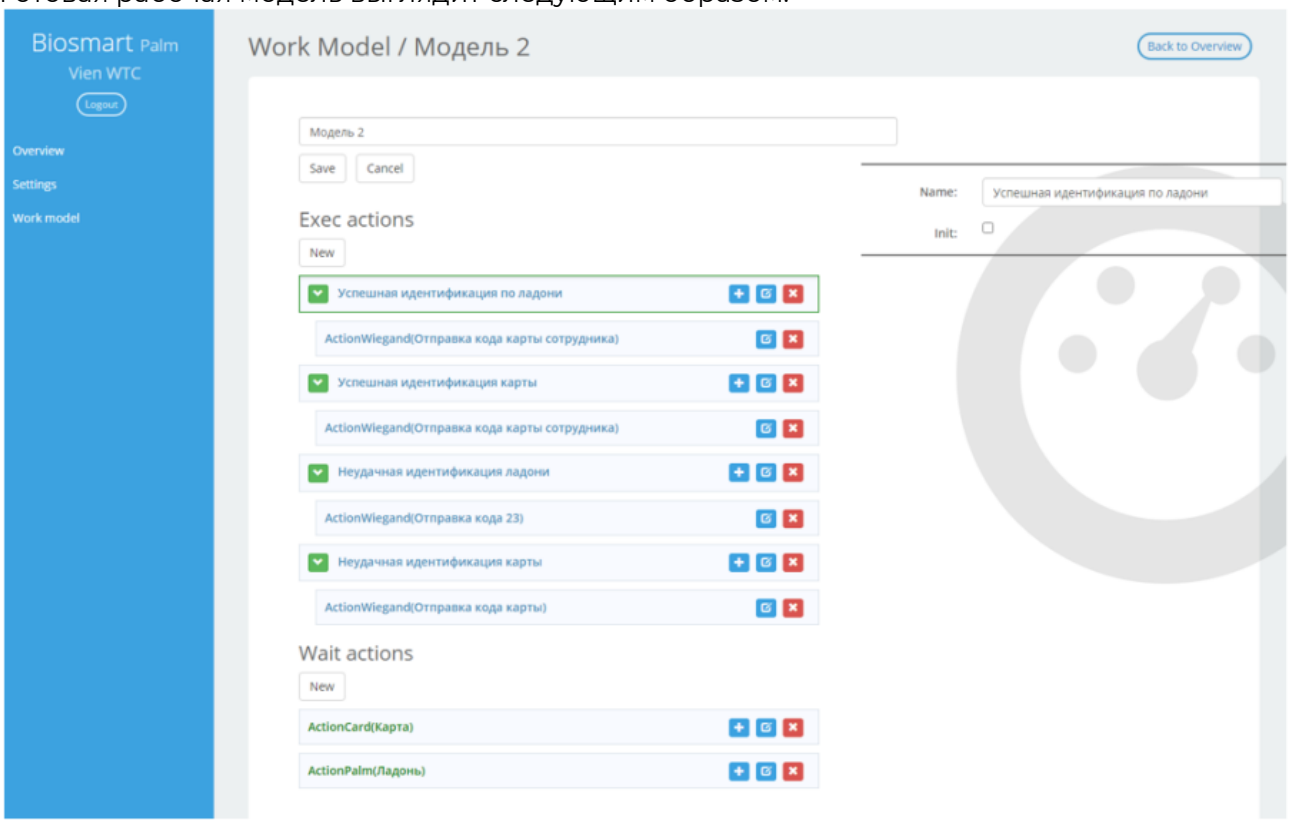
8.2.4 Создание рабочей модели с отправкой данных по интерфейсу Wiegand

В данном пункте описано создание более сложной рабочей модели.
В начальный момент времени терминал ожидает приложенной ладони или карты.

- При успешной идентификации по ладони отправляет код карты по интерфейсу **wiegand**
- При успешной идентификации по карте отправляет код карты по интерфейсу **wiegand**
- При неудачной идентификации по ладони отправляет код «**23**» по интерфейсу **wiegand**
- При неудачной идентификации по карте отправляет код карты по интерфейсу **wiegand**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Готовая рабочая модель выглядит следующим образом:

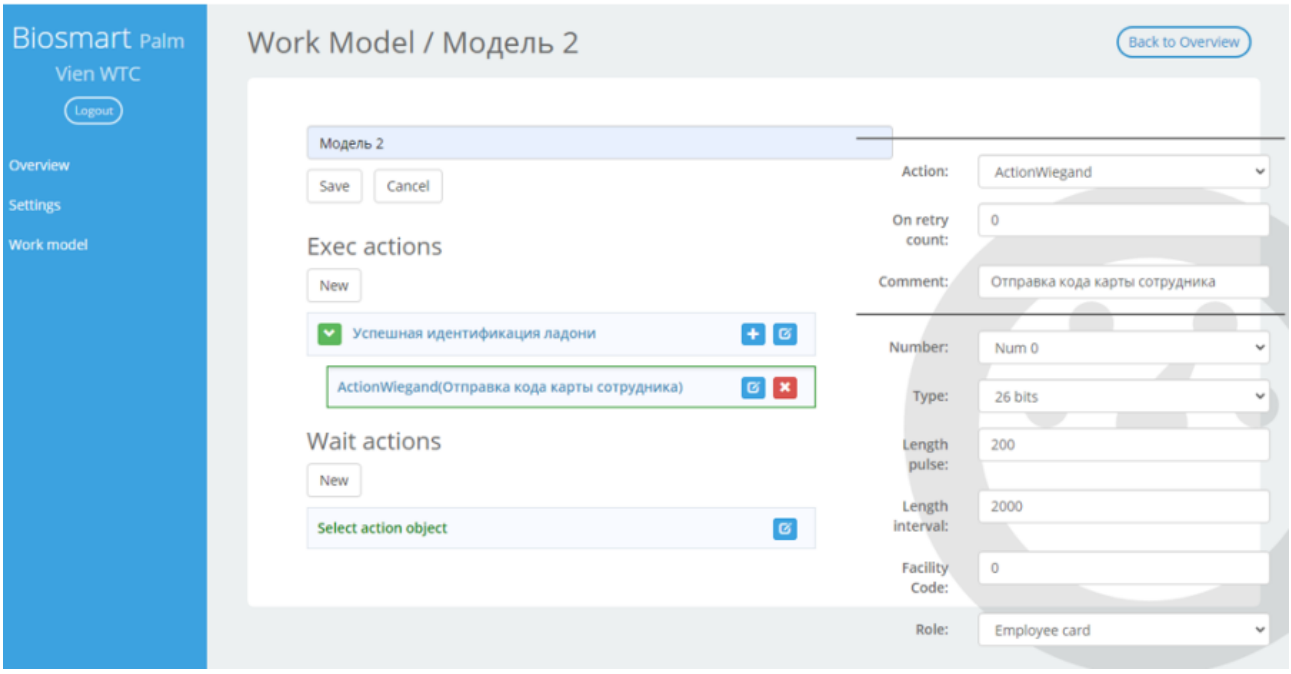


Создайте первый блок действий – **Успешная идентификация ладони**. Он используется при успешной идентификации по ладони. Итогом его выполнения станет отправка кода карты сотрудника на wiegand-выход.

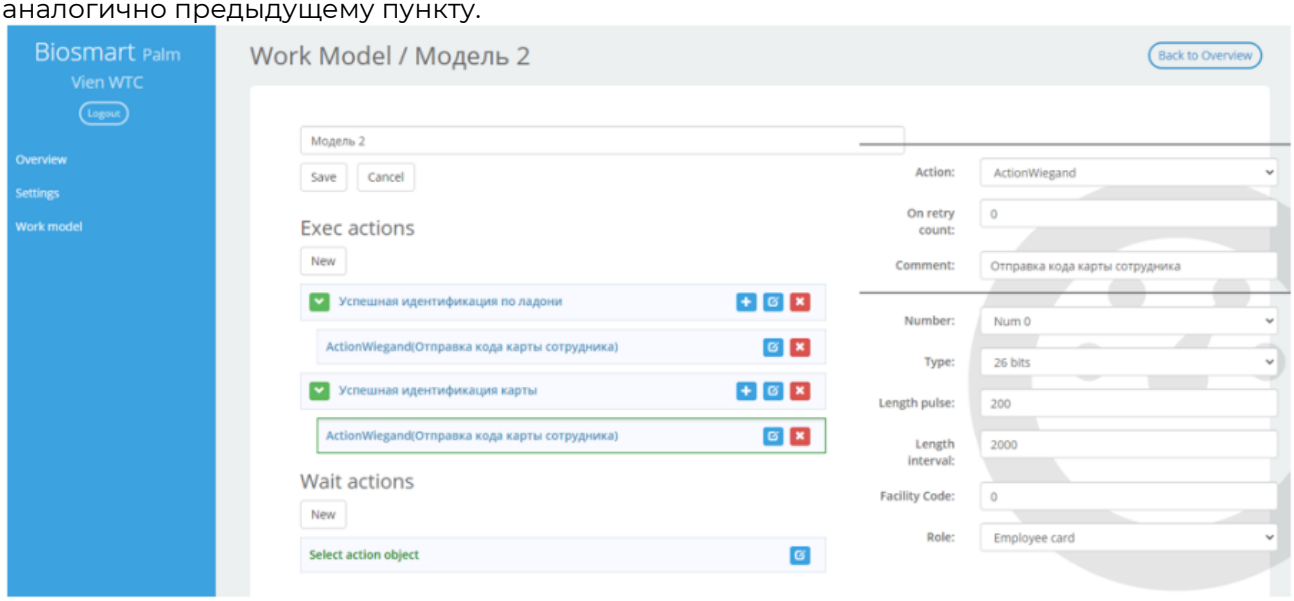
Добавьте действие **ActionWiegand** (**Отправка кода карты сотрудника**) со следующими параметрами:

Number (номер wiegand-выхода): **Num 0**
Type (битность wiegand-выхода): **26 bits**
Length pulse (ширина импульсов в микросекундах): **200** (рекомендуемое значение)
Length interval (период следования импульсов в микросекундах): **2000** (рекомендуемое значение)
Role (тип передаваемых данных): **Employee card**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

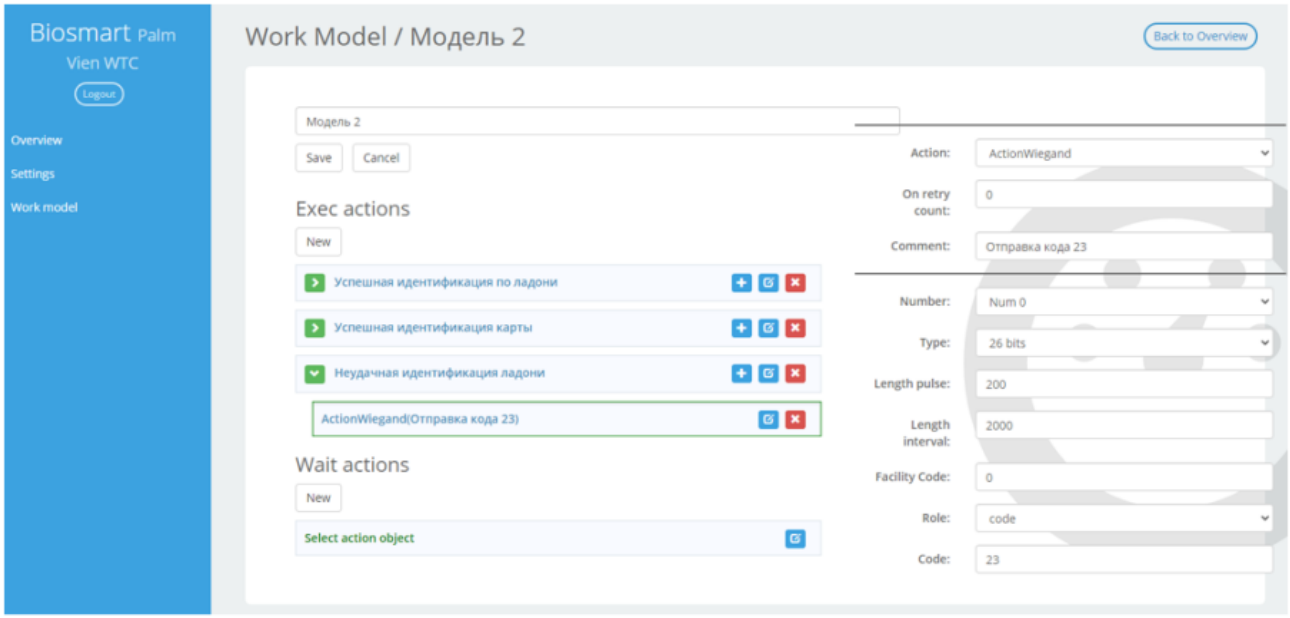


Создайте следующий блок действий – **Успешная идентификация карты**. Он используется при успешной идентификации по карте. Итогом его выполнения станет отправка кода карты сотрудника на wiegand-выход.
Добавьте действие **ActionWiegand** (**Отправка кода карты сотрудника**). Параметры зададим аналогично предыдущему пункту.

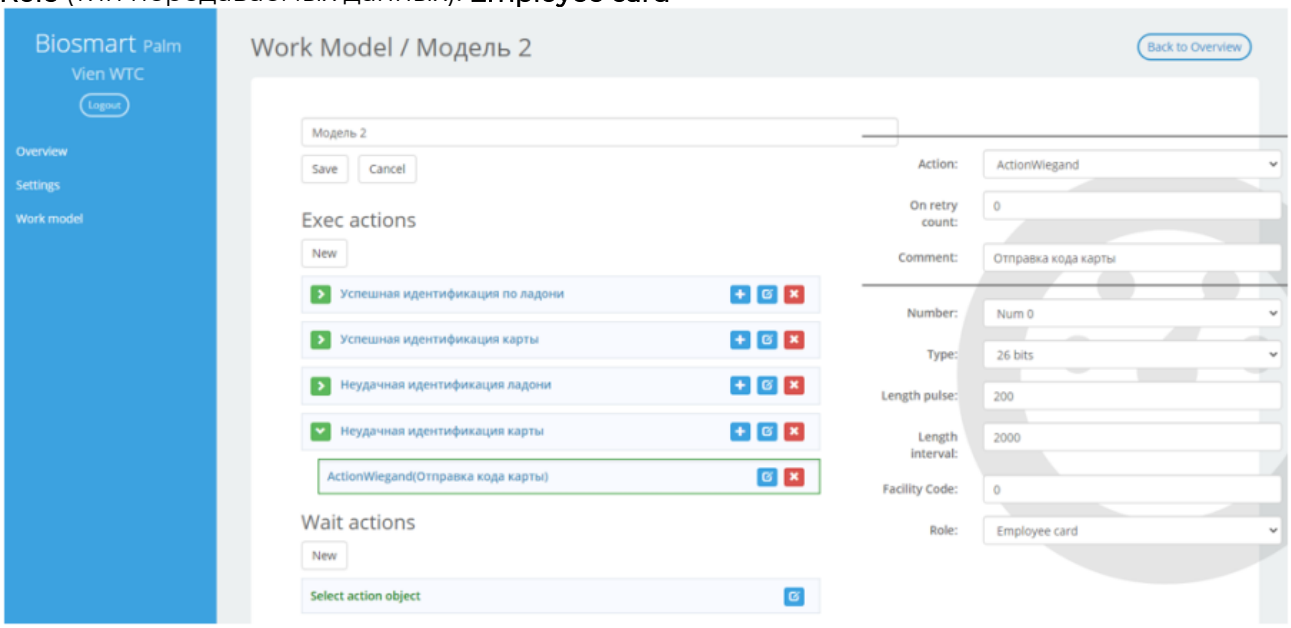


Создайте третий блок действий – **Неудачная идентификация ладони**. Он используется, если ладонь не была идентифицирована. Итогом его выполнения станет отправка кода «**23**» на wiegand-выход.
Добавьте действие **ActionWiegand** (**Отправка кода 23**) со следующими параметрами:
Role (тип передаваемых данных): **code**
Code (передаваемый код): **23**

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Создайте последний блок действий – **Неудачная идентификация карты**. Он используется, если код карты не найден в базе данных. Итогом его выполнения станет отправка кода приложенной карты на wiegand-выход.
Добавьте действие **ActionWiegand** (**Отправка кода карты**) с параметром:
Role (тип передаваемых данных): **Employee card**

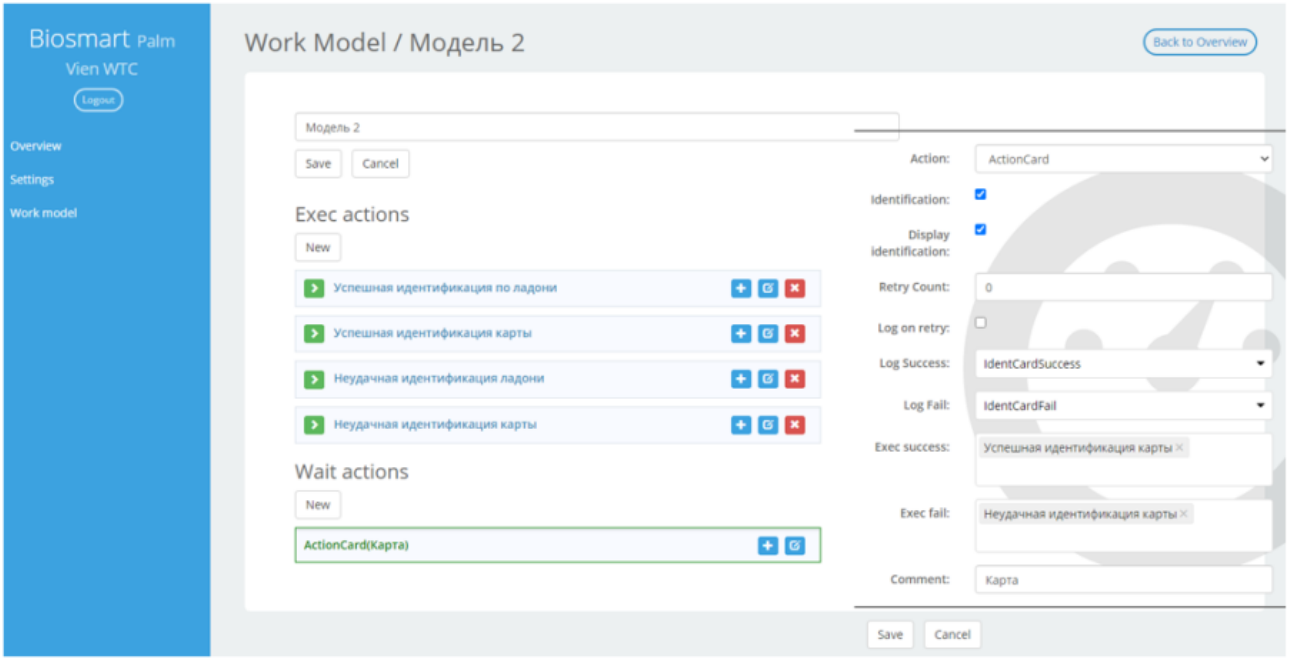


Теперь определите события, которые будут вызывать описанные выше действия. Для этого создайте событие **Карта** (**ActionCard**). Оно будет отвечать приложению карты.
Установите следующие параметры данного события:

- Производить идентификацию и отображать результат на дисплее (установите галочки в **Identification** и **Display Identification**);
- Генерировать сообщения в ПО Biosmart-Studio v6 при успешной и неудачной идентификации по карте (укажите в полях **Log success** и **Log fail** логи **IdentCardSuccess** и **IdentCardFail** соответственно);

SEC.RU | Короткий путь к информации
Скачано с sec.ru

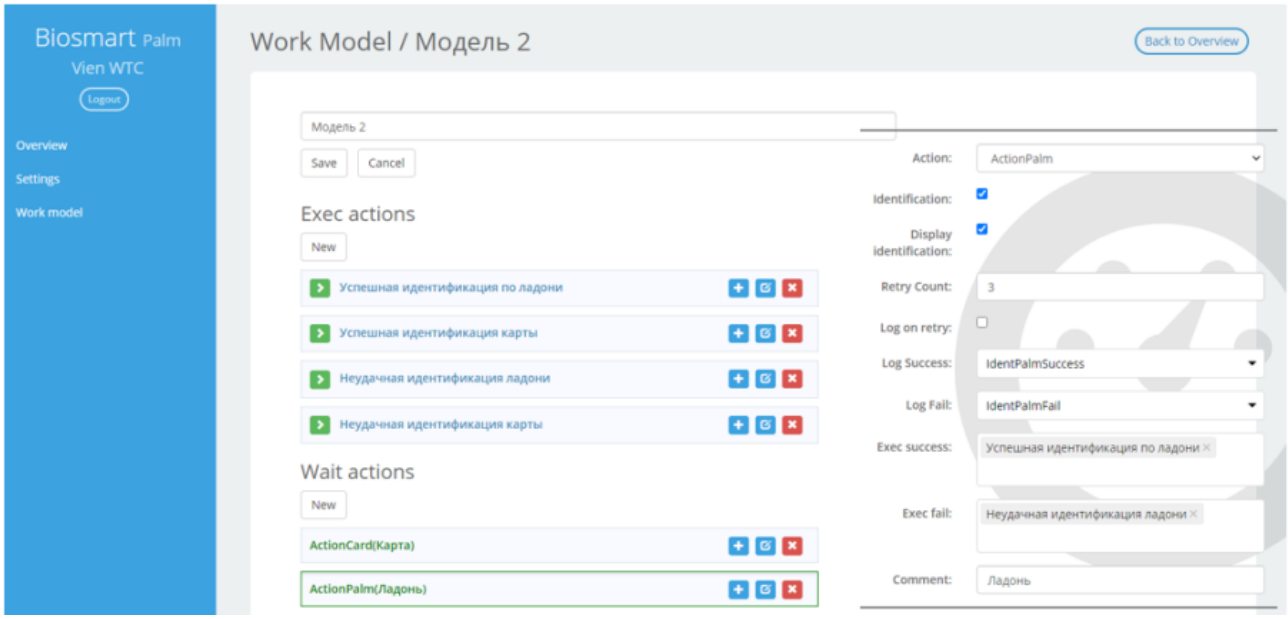
- В случае успешной идентификации отправлять код карты на wiegand-выход(укажите блок действий **Успешная идентификация карты** в поле **Exec success**);
- В случае неудачной идентификации отправлять код карты на wiegand-выход (укажите блок действий **Неудачная идентификация карты** в поле **Exec fail**).



Создайте событие **Ладонь** (**ActionPalm**), которое будет отвечать приложенной ладони. Параметры события определим следующим образом:

- Производить идентификацию и отображать результат на дисплее (установите галочки в **Identification** и **Display Identification**);
- Установите три попытки идентификации (**Retry Count:3**);
- Генерировать сообщения в ПО Biosmart-Studio при успешной и неудачной идентификации по ладони (укажите в полях **Log success** и **Log fail** логи **IdentCardSuccess** и **IdentCardFail** соответственно);
- В случае неудачной идентификации отправлять код **23** на wiegand-выход (укажите блок действий **Неудачная идентификация ладони** в поле **Exec fail**);
- В случае успешной идентификации отправить код карты на wiegand-выход (укажите блок действий **Успешная идентификация ладони** в поле **Exec Success**)

SEC.RU | Короткий путь к информации
Скачано с sec.ru



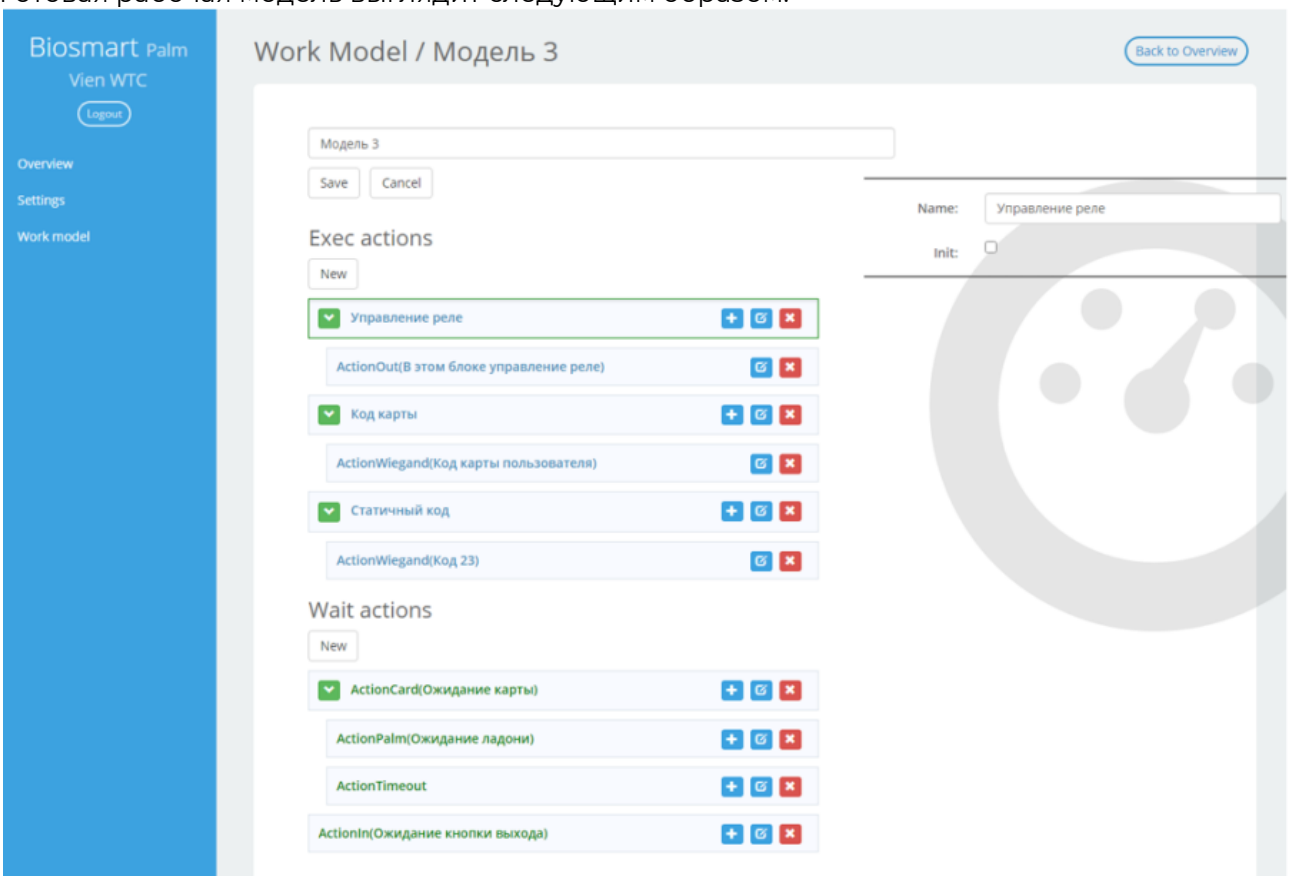
8.2.5 Создание рабочей модели с использованием реле/кнопки

В данном пункте будет описано создание рабочей модели с использованием реле и кнопки.
В начальный момент времени терминал ожидает прикладывания карты или нажатия кнопки.

- При нажатии кнопки срабатывает встроенное реле на 7 секунд
- При успешной идентификации по карте ожидается идентификация по ладони в течение 10 секунд
- При успешной идентификации по ладони срабатывает встроенное реле на 7 секунд
- При неуспешной идентификации по ладони отправляется код ранее приложенной карты по интерфейсу **wiegand**
- При неуспешной идентификации по карте отправляется код «**23**» по интерфейсу **wiegand**

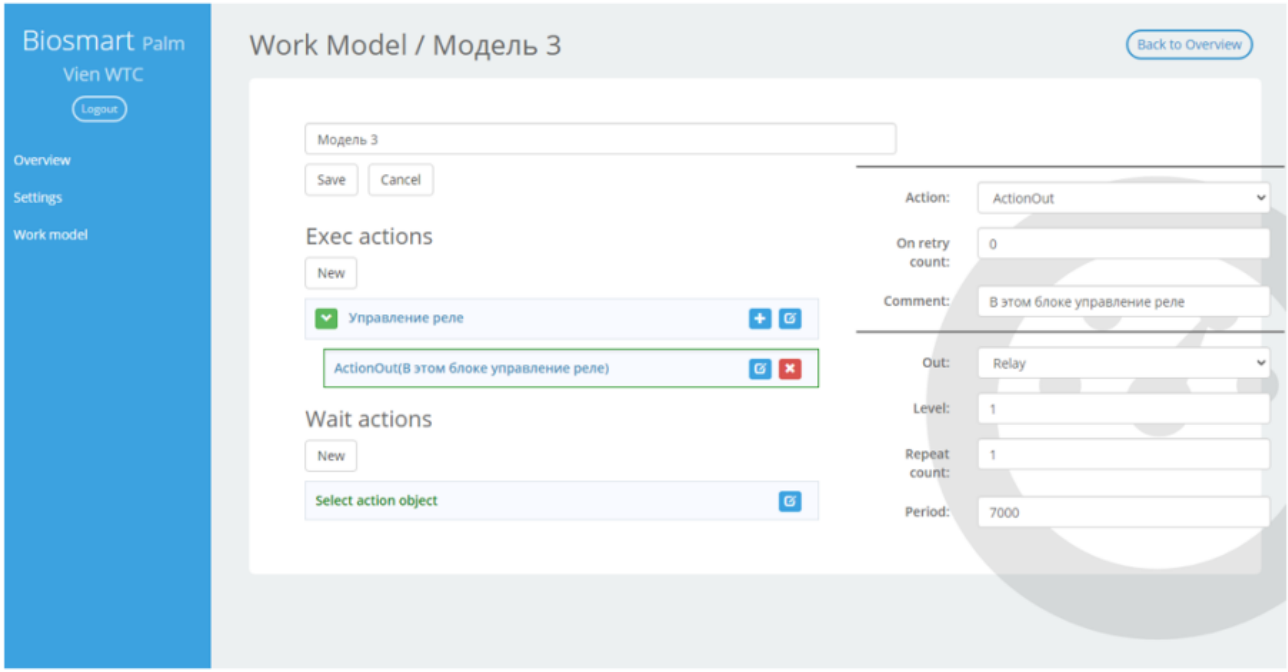
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Готовая рабочая модель выглядит следующим образом:



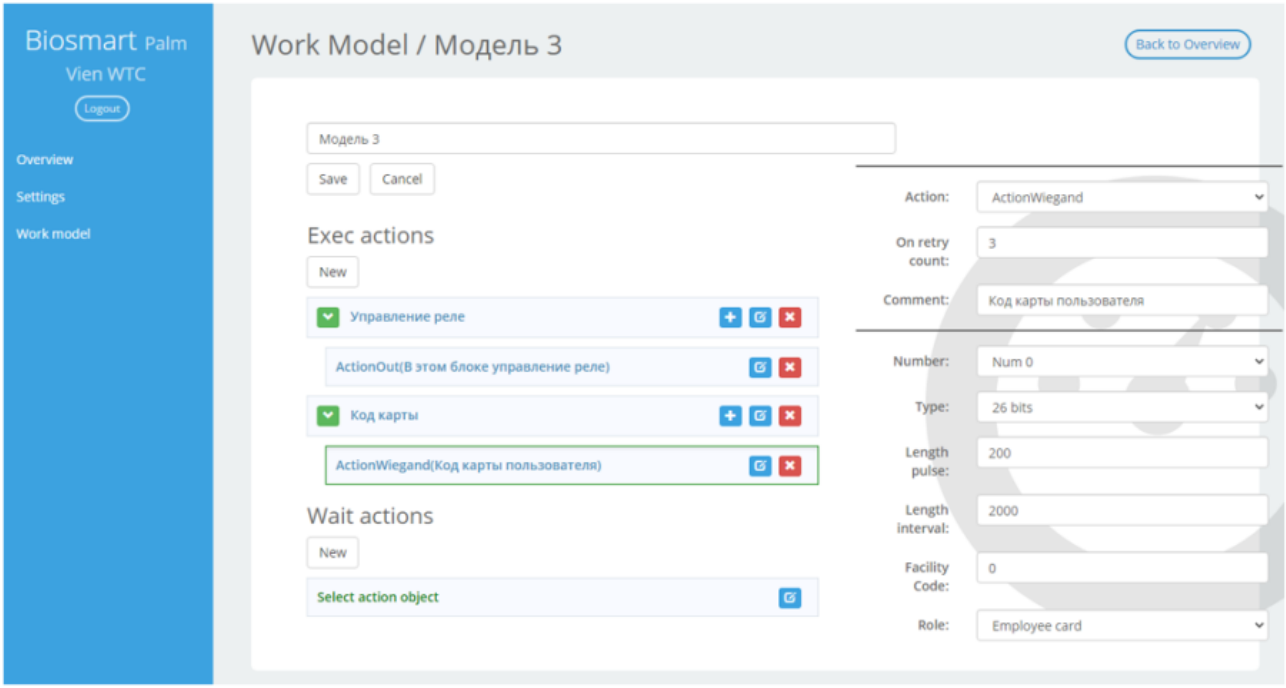
Потребуются три различных блока действий: блок для срабатывания реле и блоки для отправки разных кодов на wiegand-выход.
Создайте первый блок действий - **Управление реле**. Он используется при нажатии на кнопку и при успешной идентификации по ладони.
Добавьте в блок действие **ActionOut** (**Управление выходом**) с параметрами:
Out (выбор реле или дискретного выхода): **Relay**;
Repeat count (количество повторов срабатывания реле): **1**
Period (длительность в миллисекундах удержания реле в сработавшем состоянии): **7000**

SEC.RU | Короткий путь к информации
Скачано с sec.ru



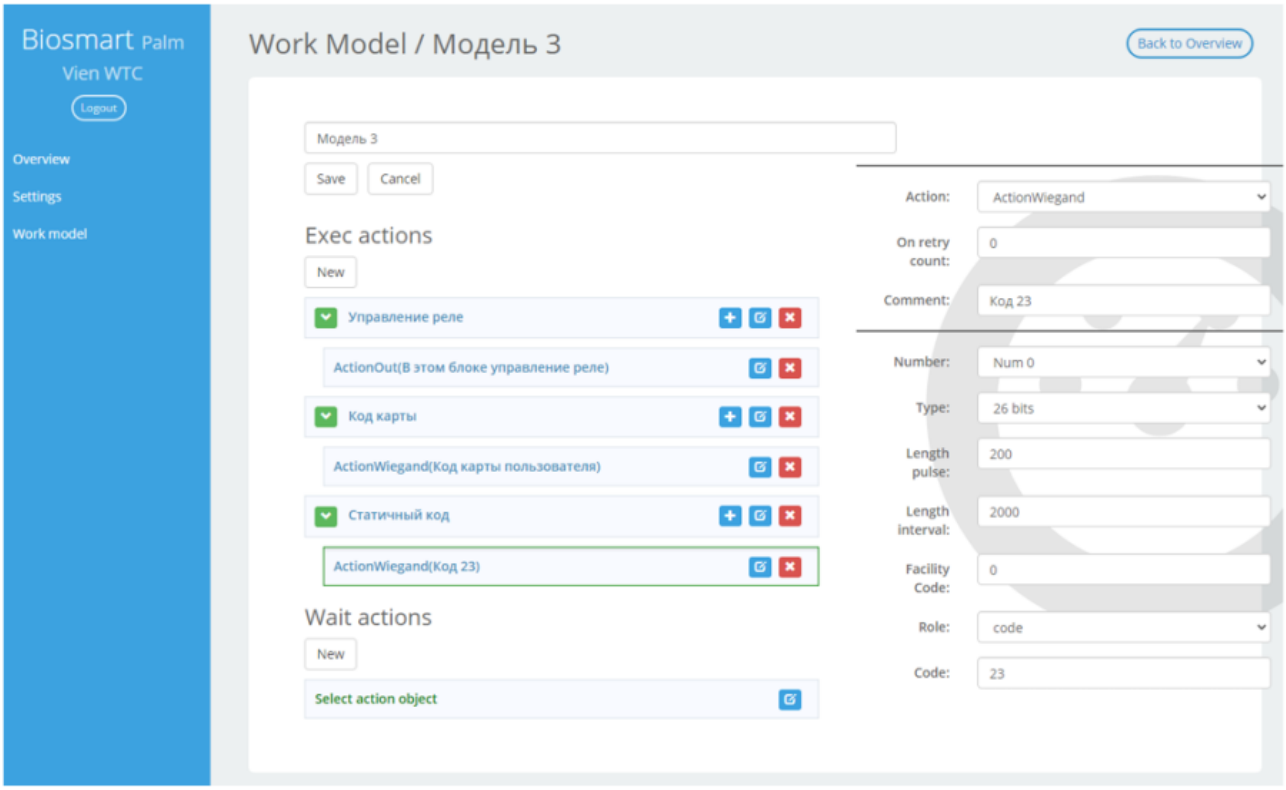
Создайте следующий блок действий – **Код карты**. Он используется при неуспешной идентификации по ладони.
Добавьте действие **ActionWiegand** (**Код карты пользователя**) со следующими параметрами:
Number (номер wiegand-выхода): **Num 0**
Type (битность wiegand-выхода): **26 bits**
Length pulse (ширина импульсов в микросекундах): **200** (рекомендуемое значение)
Length interval (период следования импульсов в микросекундах): **2000** (рекомендуемое значение)
Role (тип передаваемых данных): **Employee card**
Устанавливаем три попытки идентификации (**On retry count: 3**), то есть после третьей неудачной попытки идентификации по ладони на wiegand-выход будет отправлен код карты.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Последний необходимый блок действий – **Статичный код**. Он отвечает за отправку кода «**23**» на wiegand-выход.
Добавьте действие **ActionWiegand** (**Код 23**) со следующими параметрами:
Number (номер wiegand-выхода): **Num 0**
Type (битность wiegand-выхода): **26 bits**
Length pulse (ширина импульсов в микросекундах): **200** (рекомендуемое значение)
Length interval (период следования импульсов в микросекундах): **2000** (рекомендуемое значение)
Role (тип передаваемых данных): **code**
Code (передаваемый код): **23**

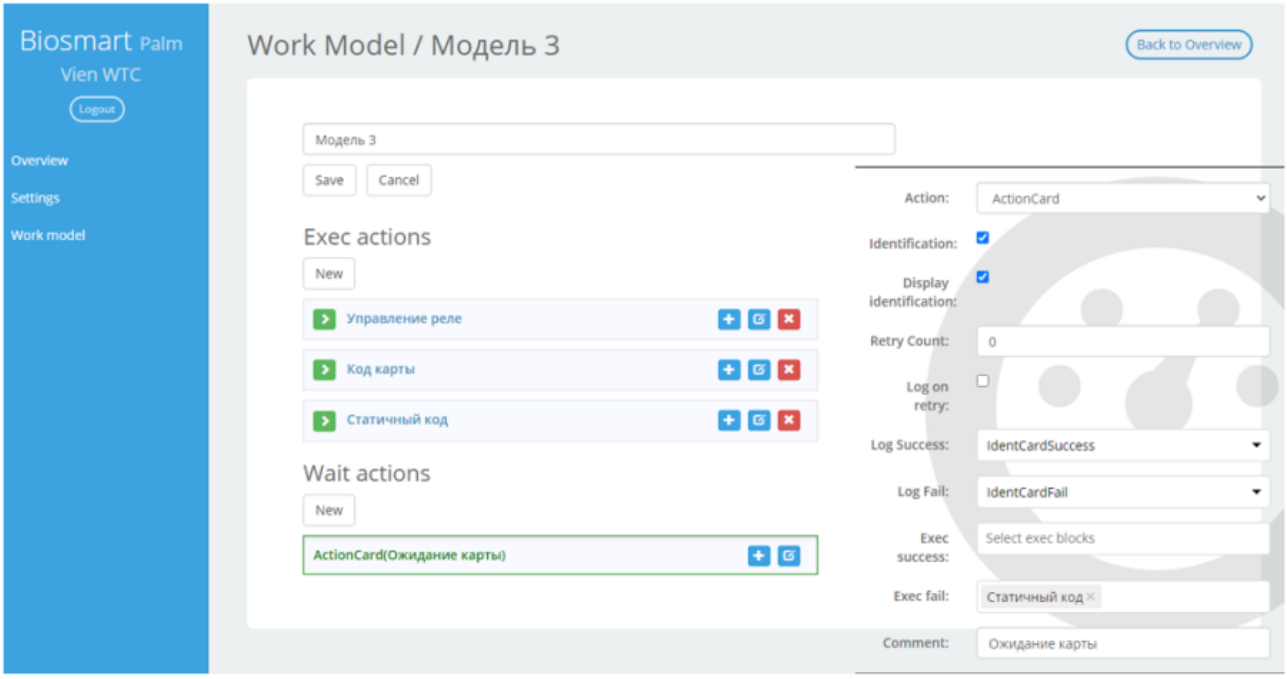
SEC.RU | Короткий путь к информации
Скачано с sec.ru



Теперь определите события, которые будут вызывать описанные выше действия. Для этого создайте событие **ActionCard** (**Ожидание карты**).
Установите следующие параметры данного события:

- Производить идентификацию и отображать результат на дисплее (установите галочки в **Identification** и **Display Identification**);
- Генерировать сообщения в ПО Biosmart-Studio v6 при успешной и неуспешной идентификации по карте (укажите в полях **Log success** и **Log fail** логи **IdentCardSuccess** и **IdentCardFail** соответственно);
- В случае неуспешной идентификации отправлять код «**23**» на wiegand-выход (укажите блок действий **Статичный код** в поле **Exec fail**).

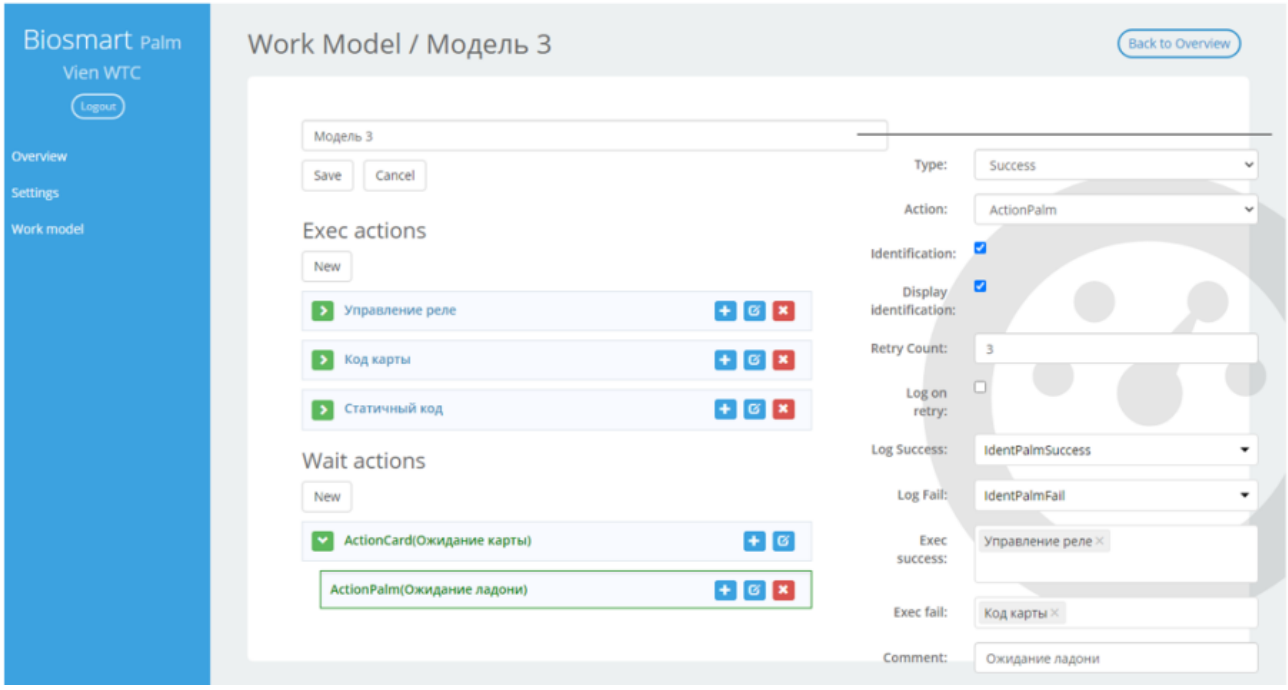
SEC.RU | Короткий путь к информации
Скачано с sec.ru



Далее добавьте событие идентификации по ладони **ActionPalm** (**Ожидание ладони**). Обратите внимание, что это событие должно располагаться ниже по иерархии, так как ожидается после события **ActionCard** (**Ожидание карты**).
Установите следующие параметры данного события:

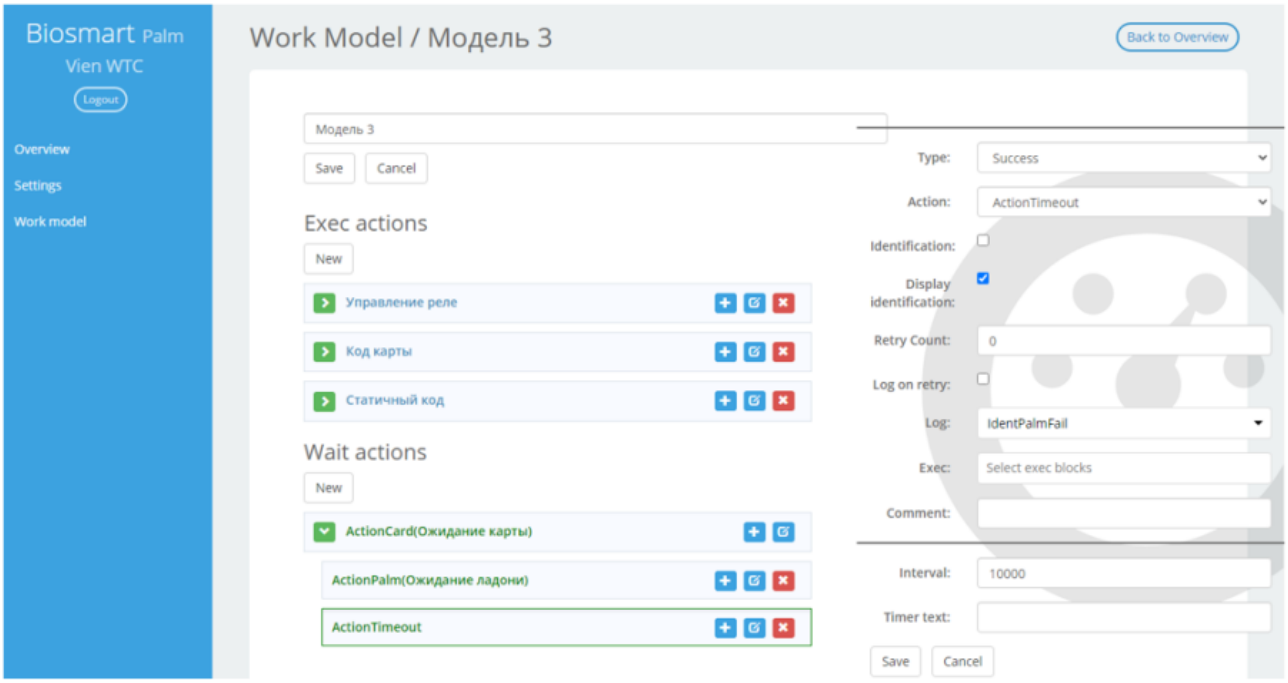
- Производить идентификацию и отображать результат на дисплее (установите галочки в **Identification** и **Display Identification**);
- Установить три попытки идентификации по ладони (**Retry count**: **3**).
- Генерировать сообщения в ПО Biosmart-Studio v6 при успешной и неуспешной идентификации по ладони (укажите в полях **Log success** и **Log fail** логи **IdentPalmSuccess** и **IdentPalmFail** соответственно);
- Срабатывание встроенного реле в случае успешной идентификации (укажите блок действий **Управление реле** в поле **Exec Success**);
- Отправка кода карты на wiegand-выход в случае неуспешной идентификации по ладони (укажите блок действий **Код карты** в поле **Exec Fail**).

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Для того, чтобы ограничить время, в течение которого терминал ожидает прикладывания ладони (чтобы терминал вернулся к ожиданию карты), создайте событие **ActionTimeout** с параметрами:

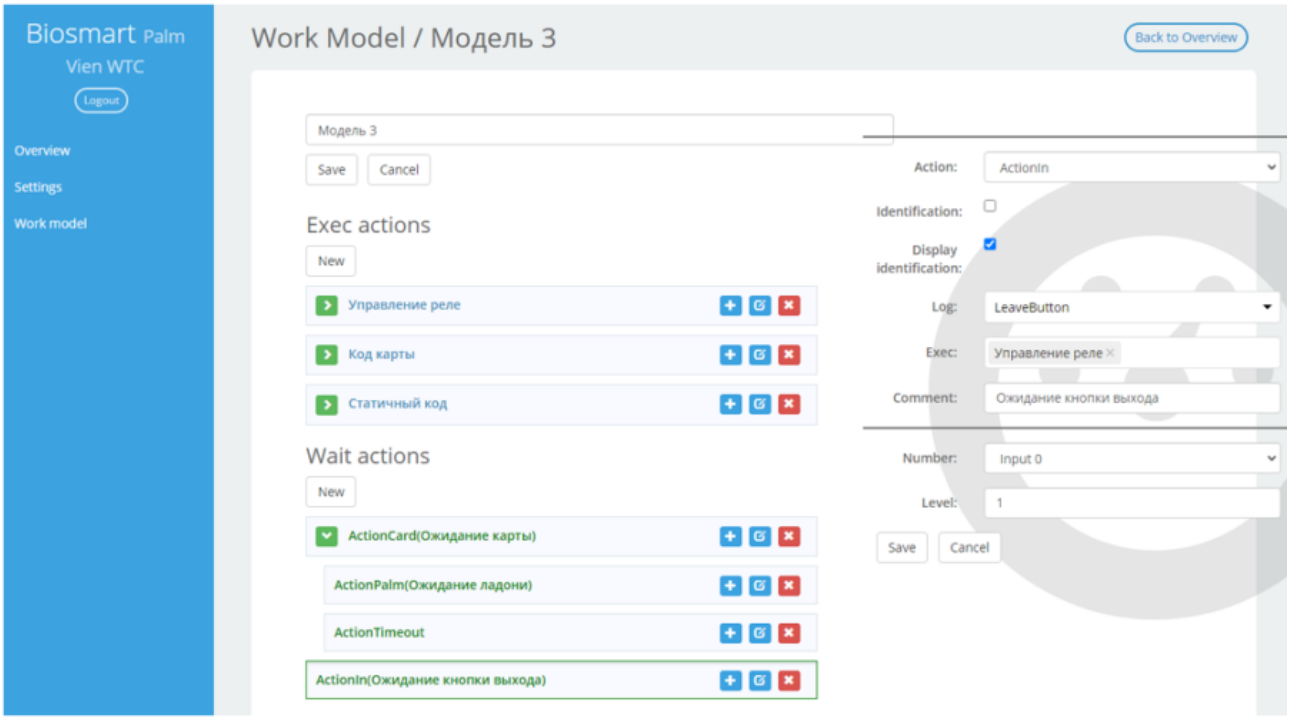
- Интервал времени на идентификацию по ладони **Interval: 10000** (10 секунд);
- Генерировать сообщения в ПО Biosmart-Studio v6 по истечении заданного интервала (укажите в поле **Log** лог **IdentPalmFail**).



Создайте последнее событие **ActionIn** (**Ожидание кнопки выхода**) с параметрами:

SEC.RU | Короткий путь к информации
Скачано с sec.ru

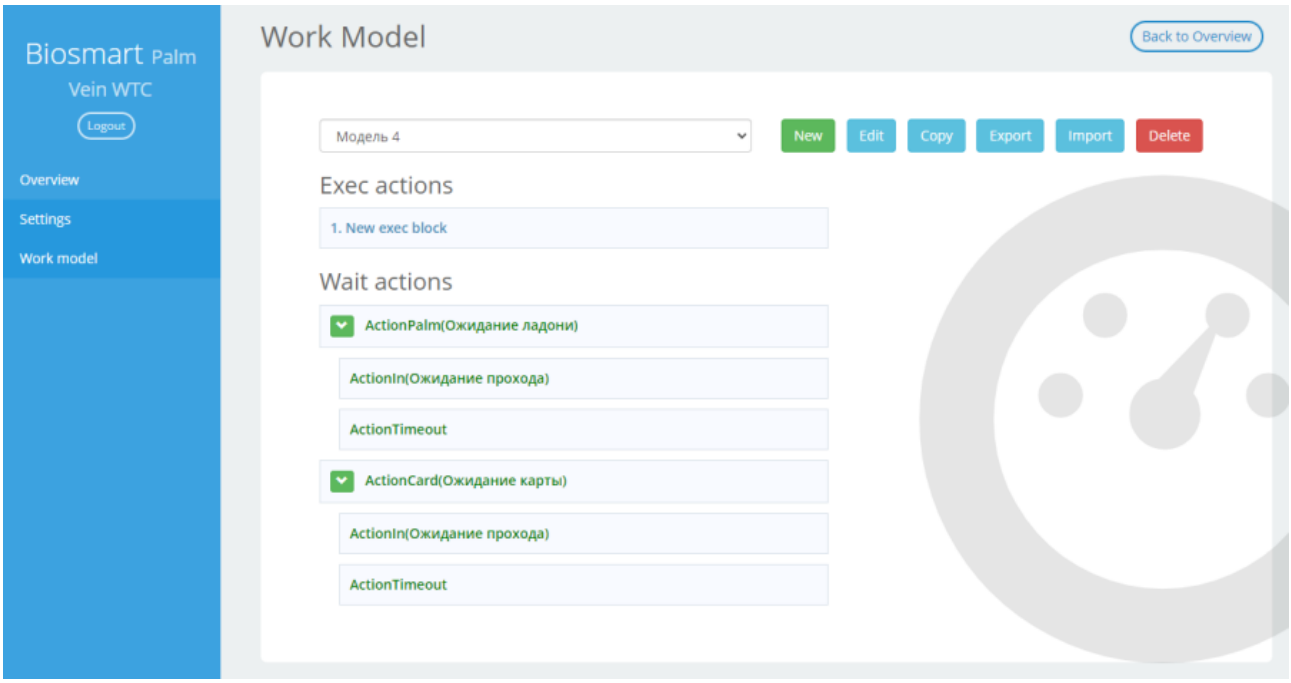
- Номер дискретного входа, к которому подключена кнопка (**Number: Input 0**) и уровень сигнала (**Level: 1**);
- Генерировать сообщения в ПО Biosmart-Studio v6 по нажатию кнопки (укажите в поле **Log** лог **LeaveButton**);
- Срабатывание встроенного реле по нажатию кнопки (укажите блок действий **Управление реле** в поле **Exec**).



8.2.6 Создание рабочей модели с использованием датчика прохода

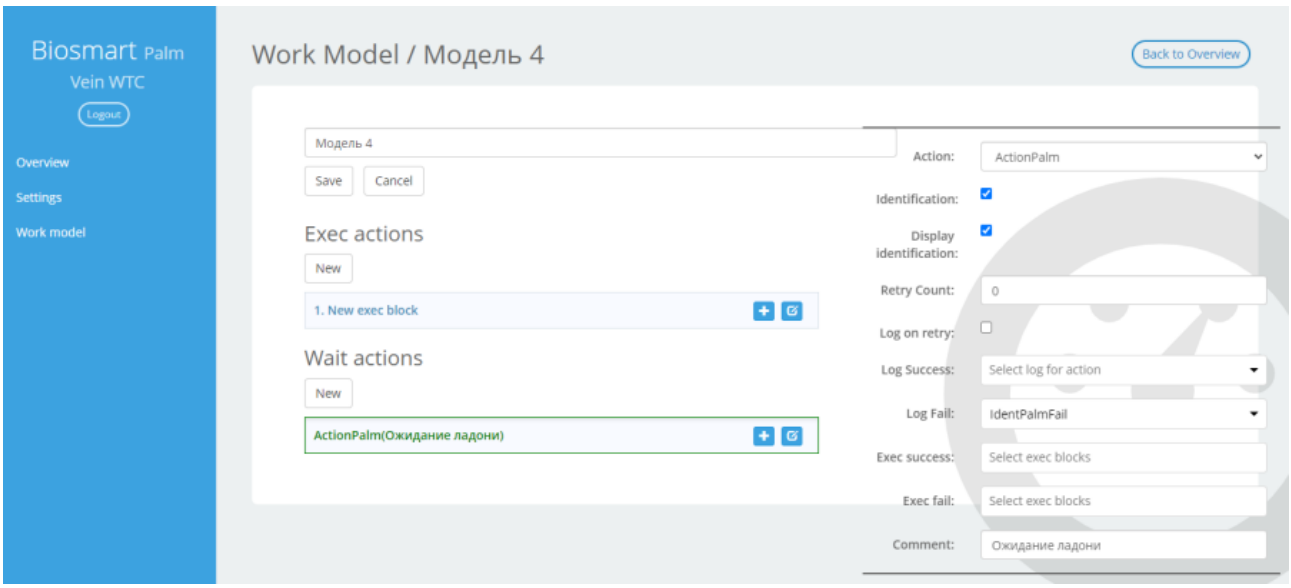
В данном пункте будет описано создание рабочей модели с использованием датчика прохода.
Терминал ожидает прикладывания ладони или карты.
При успешной идентификации по ладони или карте ожидается срабатывание датчика прохода или истечение временного интервала 4 секунды.
Если сотрудник идентифицировался и прошел в течение указанного интервала времени, то в ПО Biosmart-Studio v6 будет сформировано событие «**Идентификация сотрудника успешна**».
Если сотрудник идентифицировался, но не прошел в течение указанного интервала времени, то в ПО Biosmart-Studio v6 будет сформировано событие «**Идентификация успешна. Проход не выполнен**», которое не будет учтено в системе учёта рабочего времени.
Готовая рабочая модель выглядит следующим образом:

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Создайте событие идентификации по ладони **ActionPalm** (**Ожидание ладони**).
Установите следующие параметры данного события:

- Производить идентификацию и отображать результат на дисплее (установите галочки в **Identification** и **Display Identification**);
- Генерировать сообщение в ПО Biosmart-Studio v6 при неуспешной идентификации по ладони (укажите в поле **Log fail** лог **IdentPalmFail**);

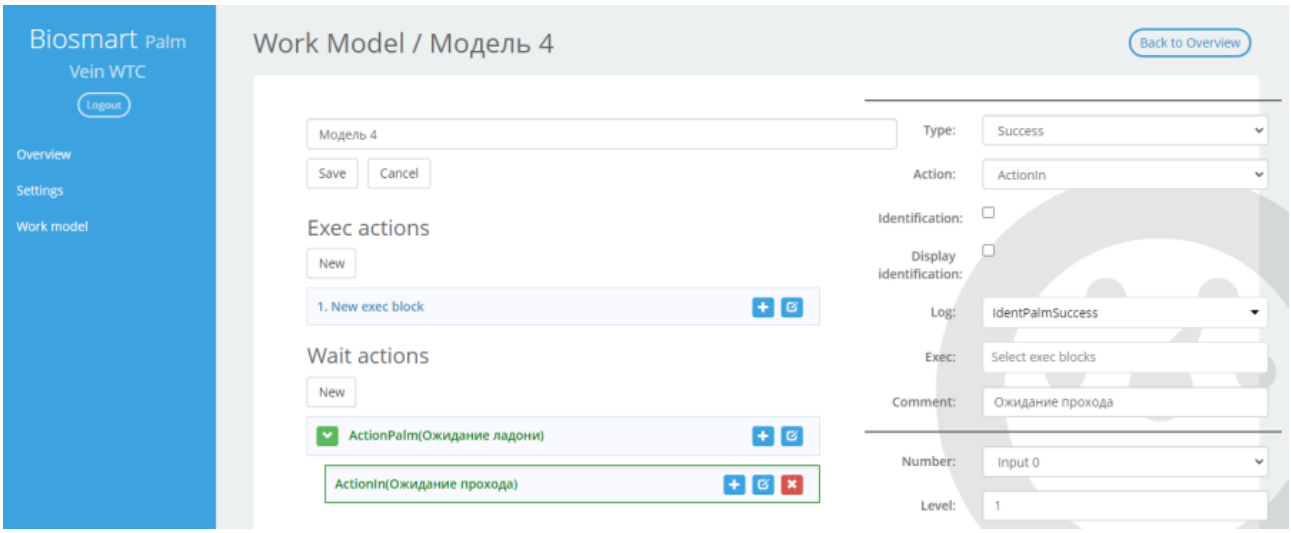


Создайте следующее событие **ActionIn** (**Ожидание прохода**). Обратите внимание, что это событие должно располагаться ниже по иерархии, так как ожидается после события **ActionPalm** (**Ожидание ладони**).
Установите следующие параметры данного события:

- Номер дискретного входа, к которому подключен датчик прохода (**Number: Input 0**) и уровень сигнала (**Level: 1**);

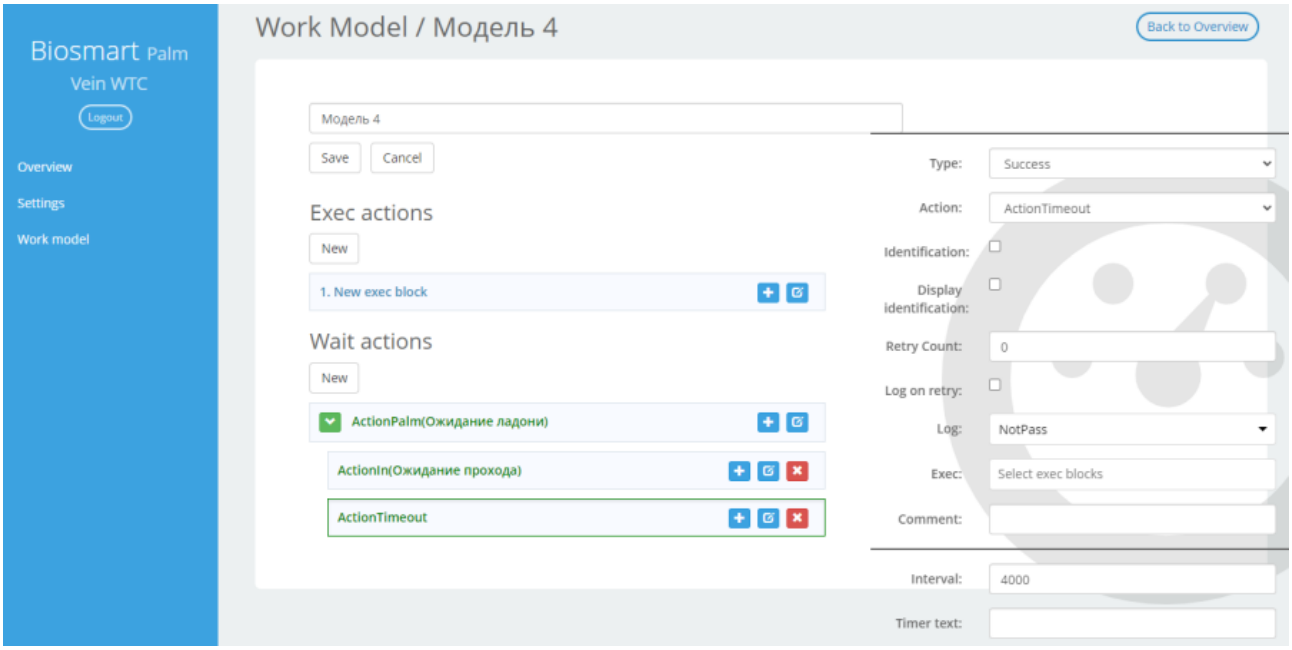
SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Генерировать сообщение в ПО Biosmart-Studio v6 по срабатыванию датчика прохода (укажите в поле **Log** лог **IdentPalmSuccess**);



Для того, чтобы ограничить время, в течение которого терминал ожидает срабатывания датчика прохода (чтобы терминал вернулся к ожиданию ладони), создайте событие **ActionTimeout**. Обратите внимание, что это событие расположено на одном уровне с событием **ActionIn** (**Ожидание прохода**), так как они ожидаются одновременно.
Установите следующие параметры данного события:

- Интервал времени **Interval: 4000** (4 секунды);
- Генерировать сообщение в ПО Biosmart-Studio v6 по истечении заданного интервала (укажите в поле **Log** лог **NotPass**).

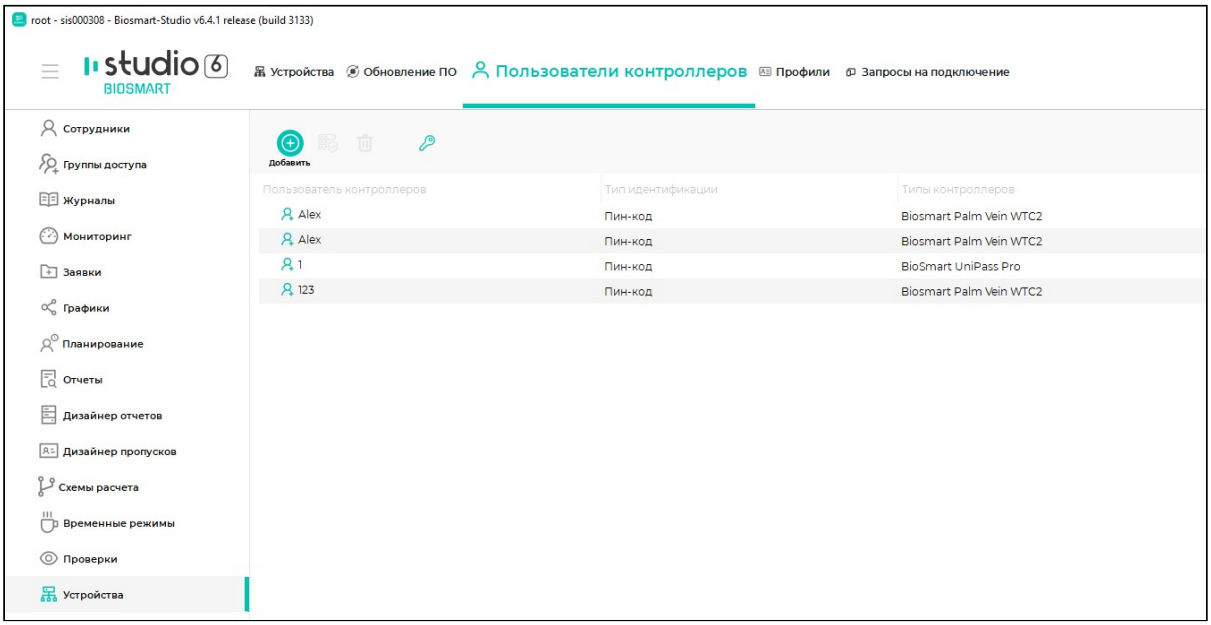


Аналогичным образом создайте событие идентификации по карте **ActionCard** (**Ожидание карты**) с последующим ожиданием срабатывания датчика прохода **ActionIn** (**Ожидание прохода**) или истечения интервала времени **ActionTimeout**.

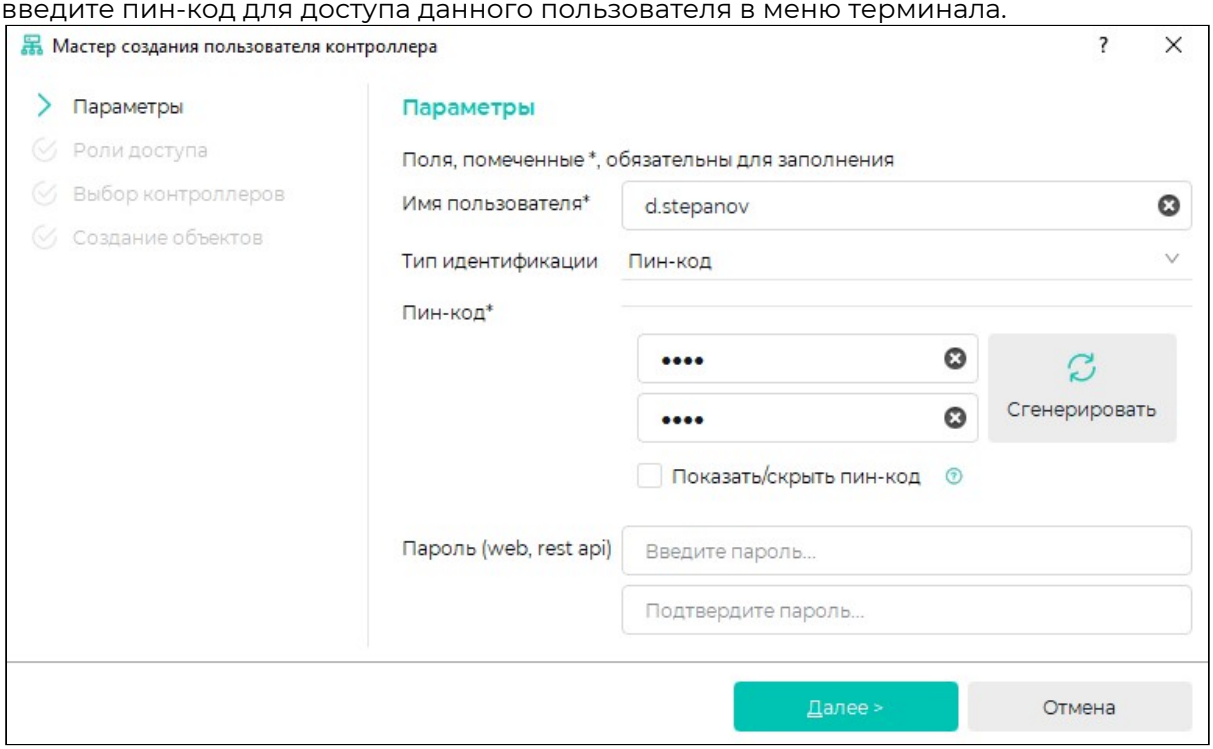
SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.3 Настройка прав пользователей терминала

Для того чтобы ограничить для отдельных пользователей набор настроек, доступный в меню терминала, перейдите в раздел **Устройства** на вкладку **Пользователи контроллерами** и нажмите кнопку **Добавить**.



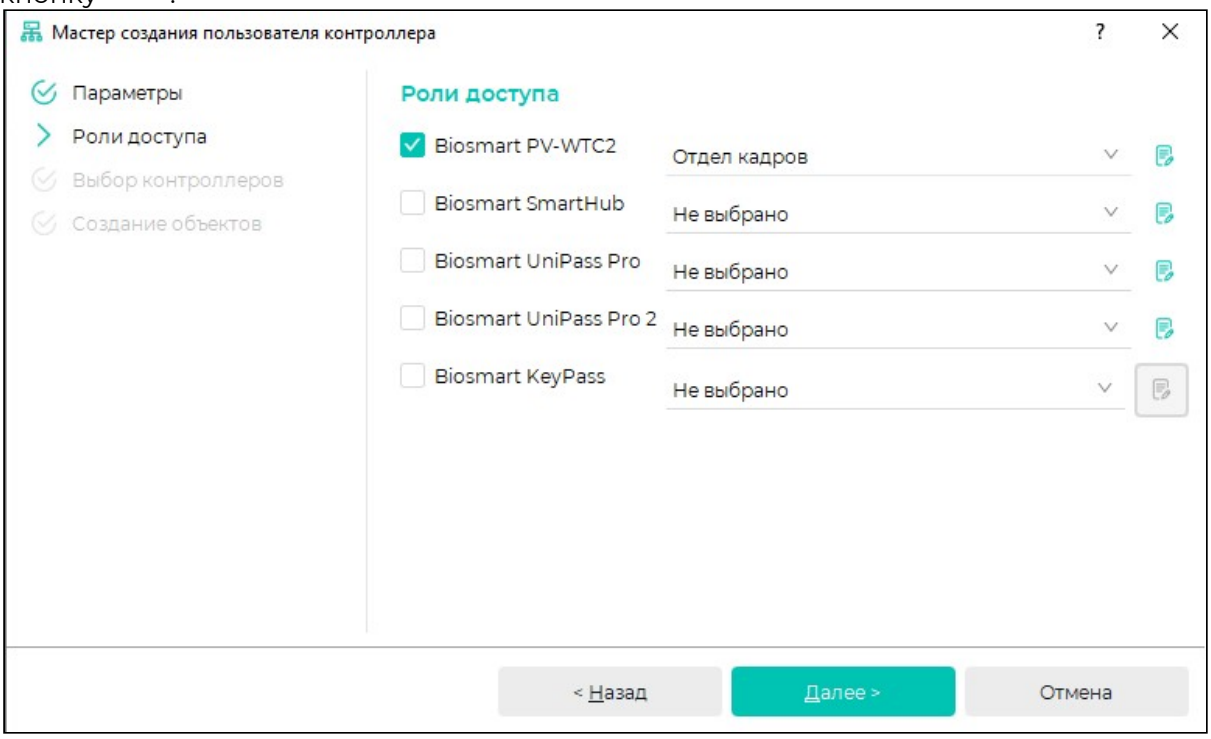
В открывшемся окне введите **Имя пользователя**, выберите **Тип идентификации**: **Пин-код** и введите пин-код для доступа данного пользователя в меню терминала.



Пин-код должен удовлетворять требованиям, заданным параметром **Сложность пин-кода** в справочнике **Общие параметры** (см. Руководство пользователя ПО Biosmart-Studio v6).

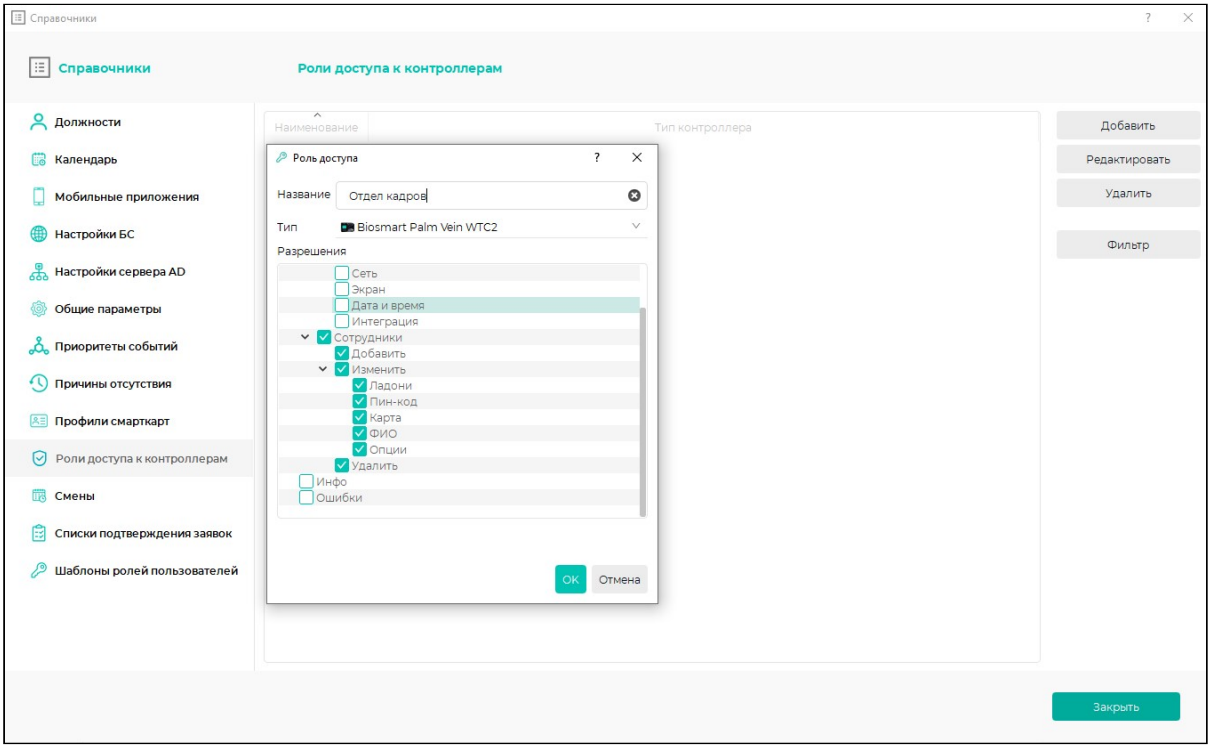
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Просмотреть требования к пин-коду можно, нажав кнопку .
Опция **Показать/скрыть пин-код** показывает либо скрывает цифры пин-кода.
Пин-код можно придумать самостоятельно либо сгенерировать автоматически. Для автоматического создания пин-кода нужно при выбранной опции **Показать/скрыть пин-код** нажать кнопку **Сгенерировать**, после чего в поле для ввода пин-кода появится последовательность, сгенерированная с учётом всех требований к пин-коду.
После ввода пин-кода нажмите **Далее**.
Поставьте отметку в чек-боксе Biosmart PV-WTC2 и выберите из выпадающего списка роль доступа. Если роли доступа не были созданы ранее, это можно сделать сейчас, нажав на кнопку .

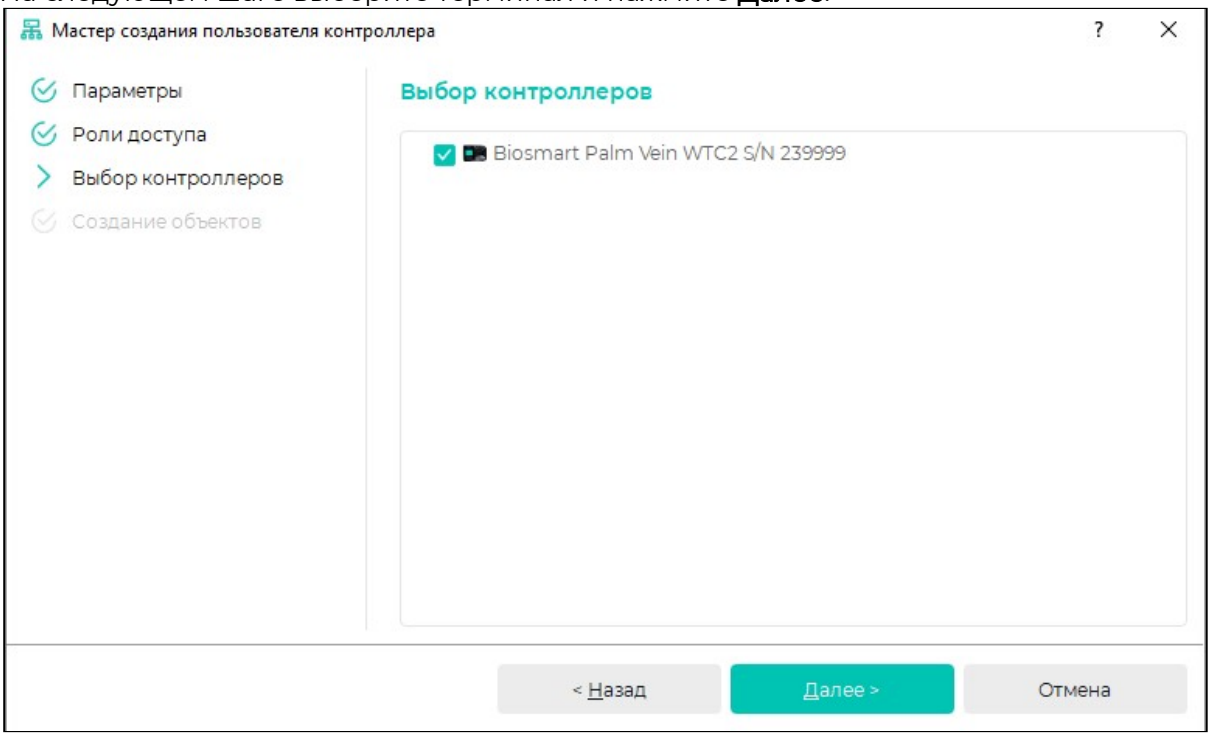


Откроется справочник **Роли доступа к контроллерам**.
Нажмите **Добавить**, введите **Название** роли доступа, выберите **Тип контроллера** Biosmart Palm Vein WTC2, укажите набор доступных настроек и нажмите **OK**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

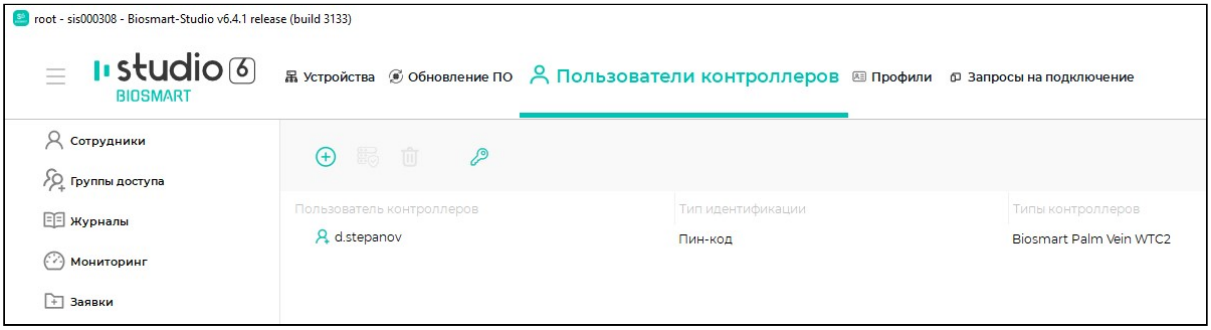


После выбора роли доступа нажмите **Далее**.
На следующем шаге выберите терминал и нажмите **Далее**.



Дождитесь добавления пользователя и нажмите **Завершить**.
В списке пользователей контроллеров появится добавленный пользователь.

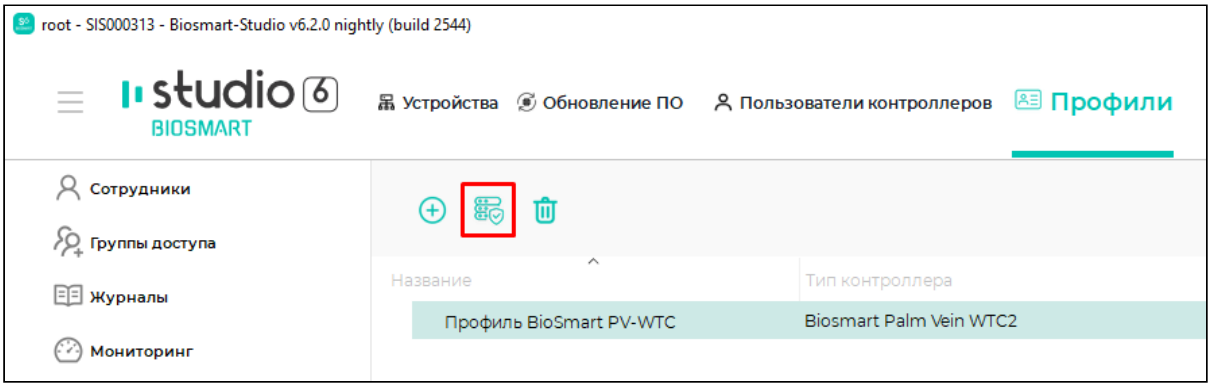
SEC.RU | Короткий путь к информации
Скачано с sec.ru



Примечание: в случае если пользователь терминала является сотрудником, использующим терминал для идентификации, можно настроить дополнительную верификацию введенного пин-кода с помощью ладони. В этом случае настройка выполняется в карточке сотрудника в разделе Пользователь контроллеров (см. Руководство пользователя ПО Biosmart-Studio v6).

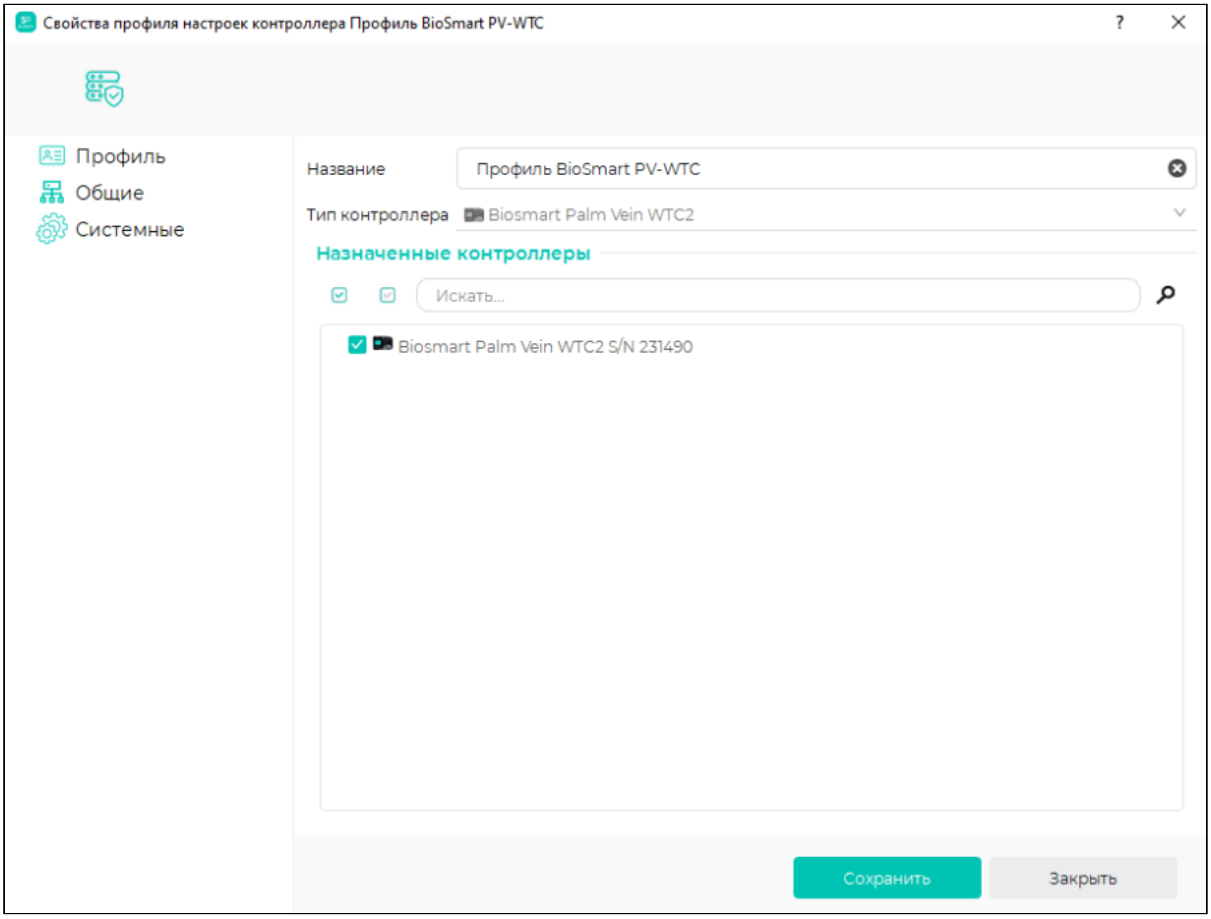
8.4 Применение настроек профиля

Использование профилей настроек позволяет применить одинаковые настройки для группы однотипных устройств без необходимости выполнения одних и тех же настроек на каждом устройстве по отдельности.
Профили настроек создаются в разделе **Устройства** на вкладке **Профили** (см. Руководство пользователя ПО Biosmart-Studio v6).
Применить профиль настроек можно на вкладке **Профили**, отметив перечень терминалов в свойствах профиля или в окне **Свойства** для каждого терминала в отдельности.
Для применения профиля на вкладке **Профили** выберите нужный профиль и нажмите **Свойства**.



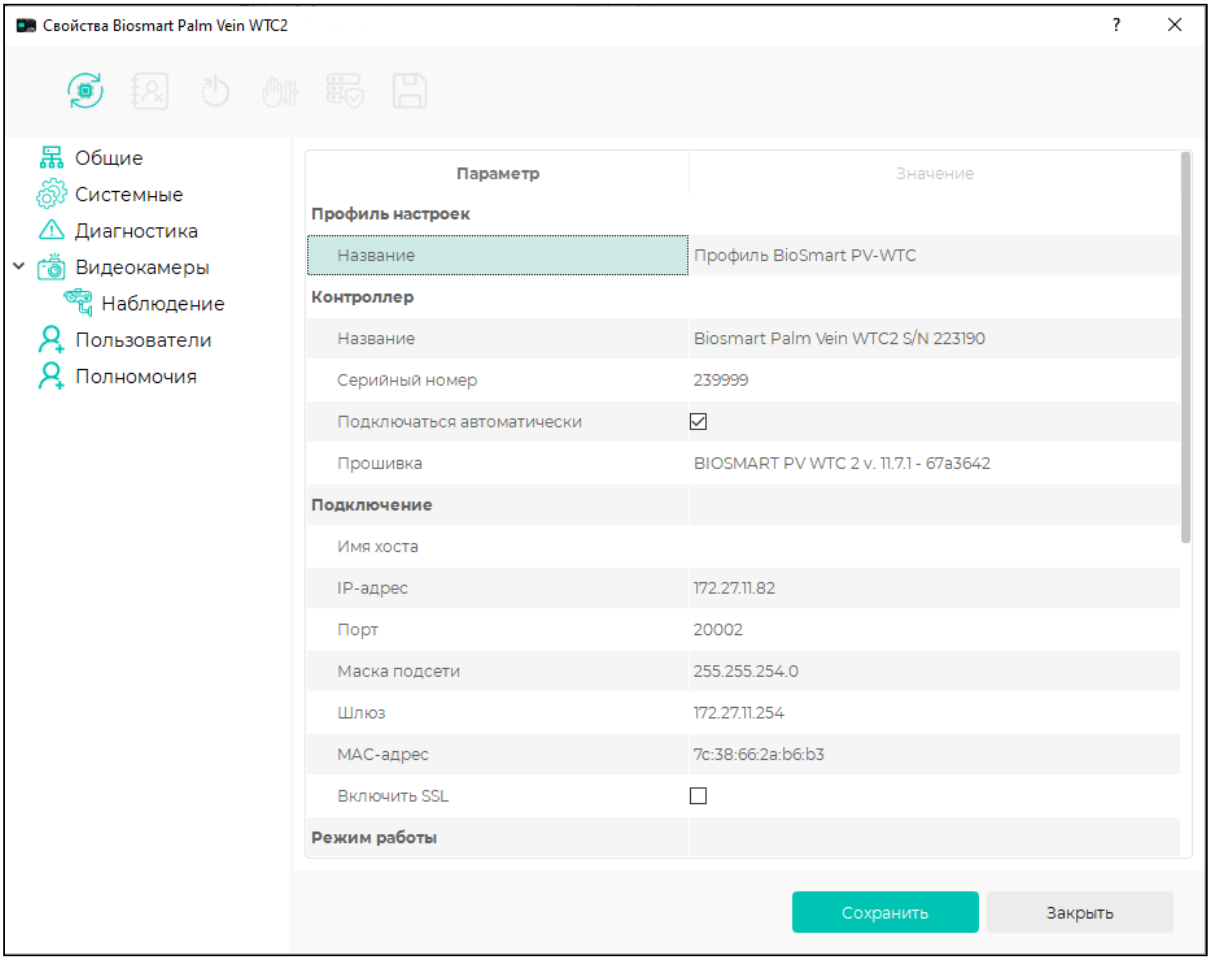
В свойствах профиля отметьте терминалы, к которым должен примениться данный профиль настроек, и нажмите **Сохранить**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Настройки профиля будут применены на всех отмеченных терминалах.
Для применения профиля в окне **Свойства** перейдите на вкладку **Общие** в раздел **Профиль настроек**, выберите из списка название профиля. Нажмите **Сохранить**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



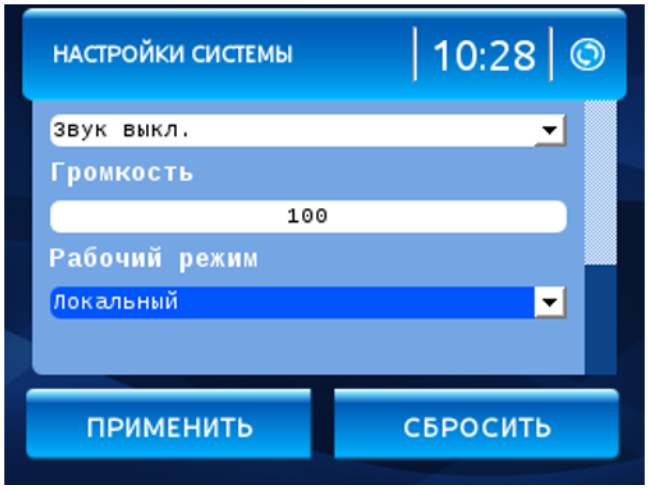
Настройки профиля будут применены к данному терминалу.
После применения профиля настроек у терминалов будут установлены значения параметров в соответствии с настройками профиля. Изменение настроек терминала, заданных профилем, будет запрещено. Настройки, которые заданы применённым профилем, не доступны для изменения в окне **Свойства** терминала.

8.5 Работа терминала в локальном режиме

В локальном режиме регистрация данных сотрудников, идентификация, а также хранение биометрических шаблонов, кодов идентификаторов и журнала событий осуществляется на терминале. Локальный режим работы не требует наличия ПО Biosmart-Studio v6 и применяется только для управления доступом.
Для настройки работы терминала в локальном режиме выполните следующие действия:

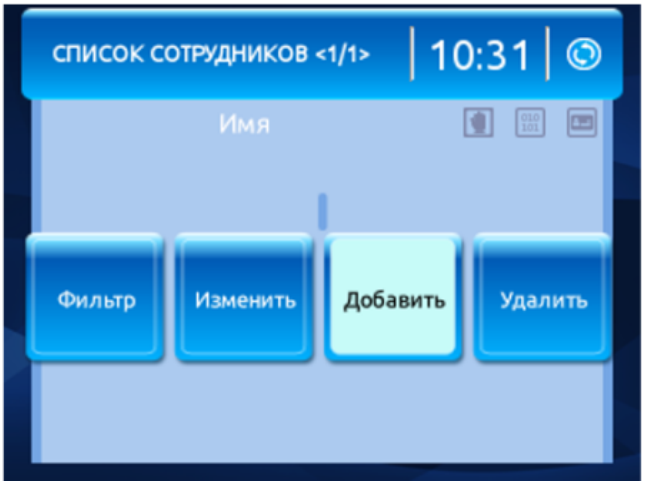
1. В меню терминала перейдите в **Настройки** – **Система** и для параметра **Рабочий режим** установите значение **Локальный**.

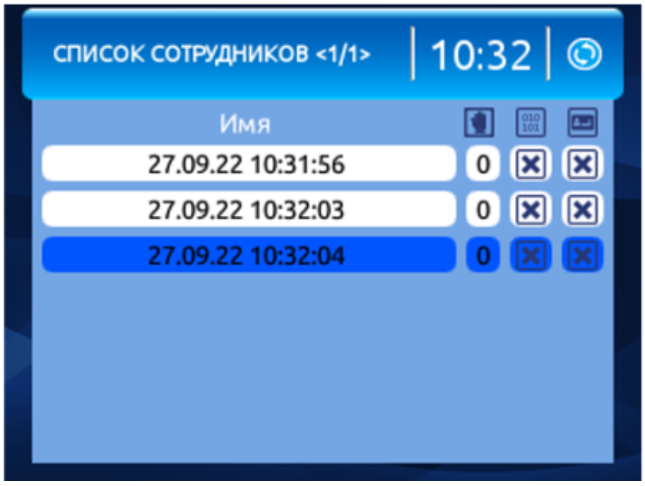
SEC.RU | Короткий путь к информации
Скачано с sec.ru



2. Выберите рабочую модель (в меню или в WEB-интерфейсе терминала).

3. Добавьте на терминал сотрудников. Для этого в меню терминала перейдите в раздел **Сотрудники**. В списке сотрудников нажмите кнопку **5**, затем кнопку **Добавить**. Каждое нажатие на кнопку **Добавить** добавляет в список одного сотрудника с фамилией и именем, равным текущим дате и времени. Добавьте необходимое количество сотрудников, затем отредактируйте их фамилии и имена. При необходимости удалить сотрудника из памяти терминала воспользуйтесь кнопкой **Удалить**.





4. В зависимости от выбранной рабочей модели зарегистрируйте необходимые идентификаторы сотрудников: шаблоны вен ладоней, RFID-карты, пин-коды. Регистрация идентификаторов с терминала описана в пункте Редактирование данных сотрудника на терминале.

5. Настройте работу терминала с подключенными устройствами (см. раздел Работа с дополнительным оборудованием).

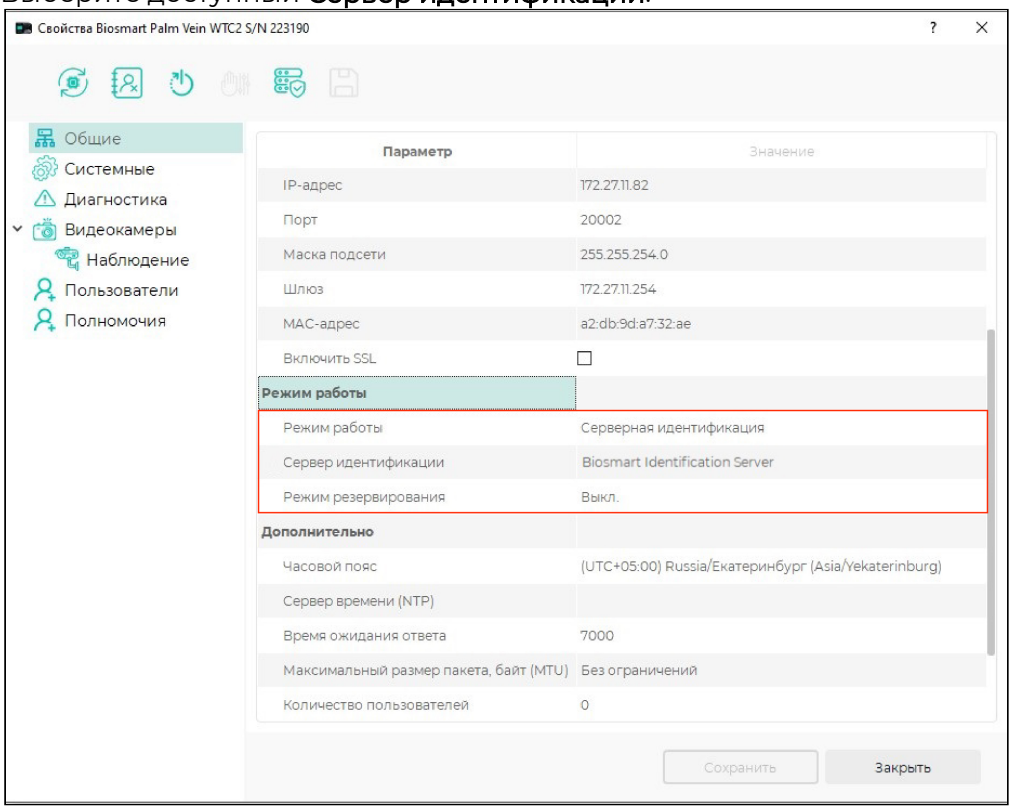
8.6 Работа терминала в режиме серверной идентификации

В режиме серверной идентификации для идентификации, хранения биометрических шаблонов, кодов идентификаторов и журнала событий используется внешний сервер биометрической идентификации (СИ BioSmart).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Для настройки работы терминала в режиме серверной идентификации выполните следующие действия:

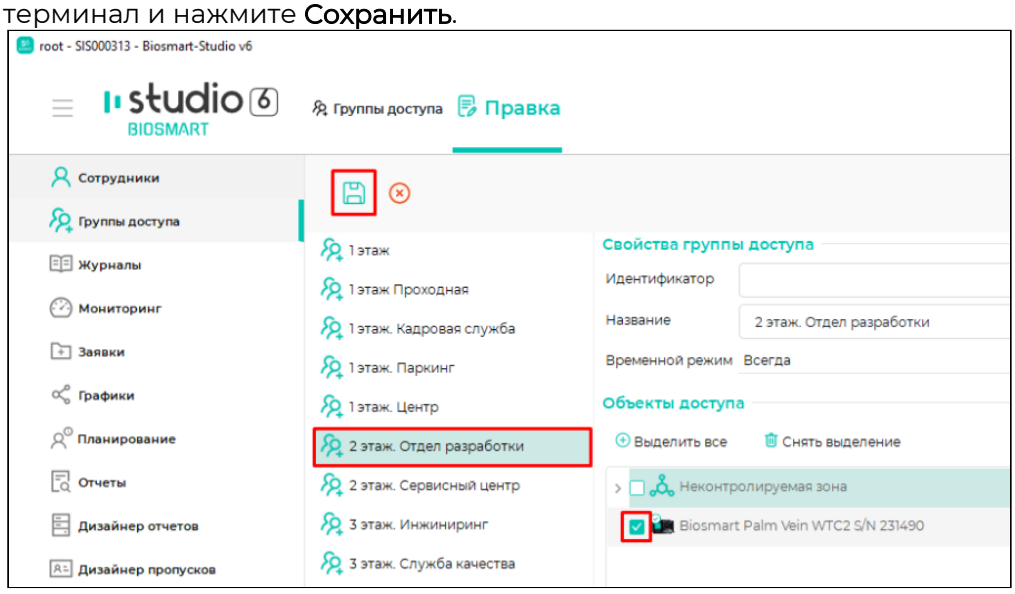
1. Настройте сетевые параметры терминала в меню **Настройки** – **Сеть**.
2. Добавьте терминал в ПО Biosmart-Studio v6.
3. Выберите рабочую модель (в меню терминала, в WEB-интерфейсе или ПО Biosmart-Studio v6).
4. В ПО Biosmart-Studio v6 перейдите в окно **Свойства Biosmart Palm Vein WTC2** и для параметра **Режим работы** установите значение **Серверная идентификация**. Выберите доступный **Сервер идентификации**.



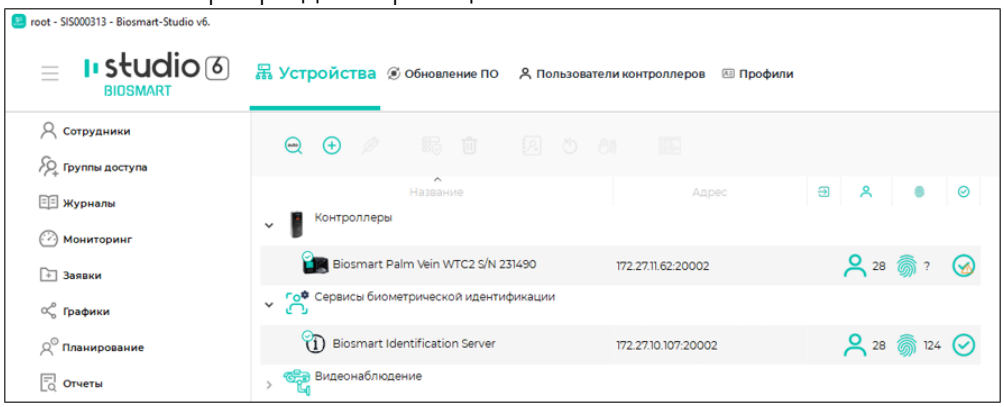
5. Загрузите на терминал из ПО Biosmart-Studio v6 список сотрудников с зарегистрированными идентификаторами (шаблонами вен ладоней, RFID-картами, пин-кодами). Для этого в разделе **Группы доступа** выберите группы доступа,

SEC.RU | Короткий путь к информации
Скачано с sec.ru

терминал и нажмите **Сохранить**.



6. Данные сотрудников, имеющих эту группу доступа, будут автоматически переданы на внешний сервер идентификации.



7. Настройте работу терминала с подключенными устройствами (см. раздел Работа с дополнительным оборудованием).

8.7 Работа с картами Mifare терминала PV-WTC

- Работа в незащищенном режиме, чтение UID
- Работа в защищенном режиме
- Работа со смартфонами в качестве идентификатора
- Настройка работы терминала с картами, инициализированными в стороннем ПО

8.7.1 Работа в незащищенном режиме, чтение UID

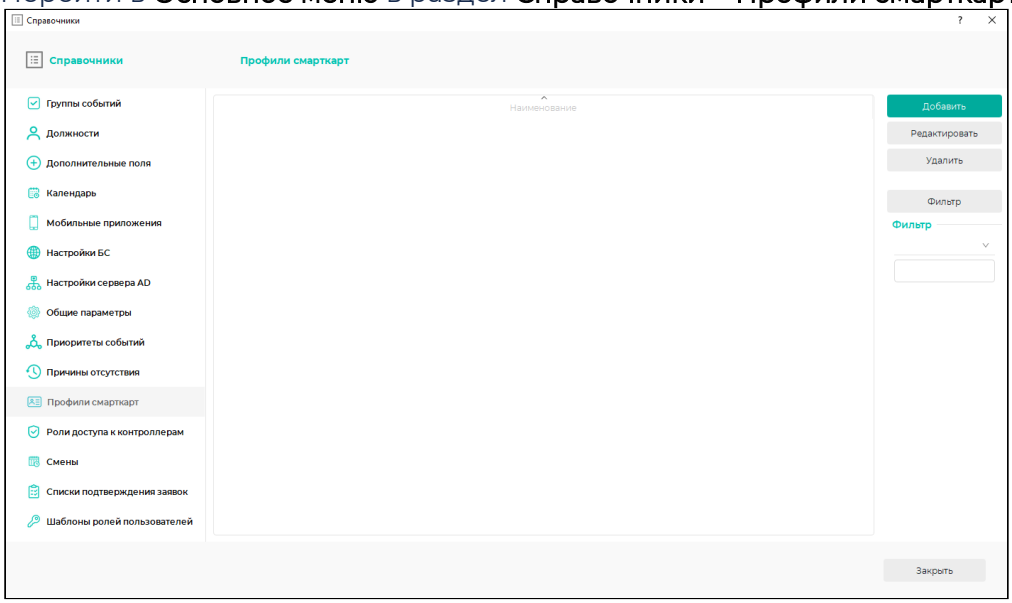
Для карт Mifare поддерживается функция считывания их открытого уникального идентификатора – UID.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Чтобы работать в незащищенном режиме, необходимо перед назначением карт доступа выполнить следующие действия:

1. Создать профиль смарткарт в ПО Biosmart-Studio v6

- Перейти в **Основное меню** в раздел **Справочники** → **Профили смарткарт**.



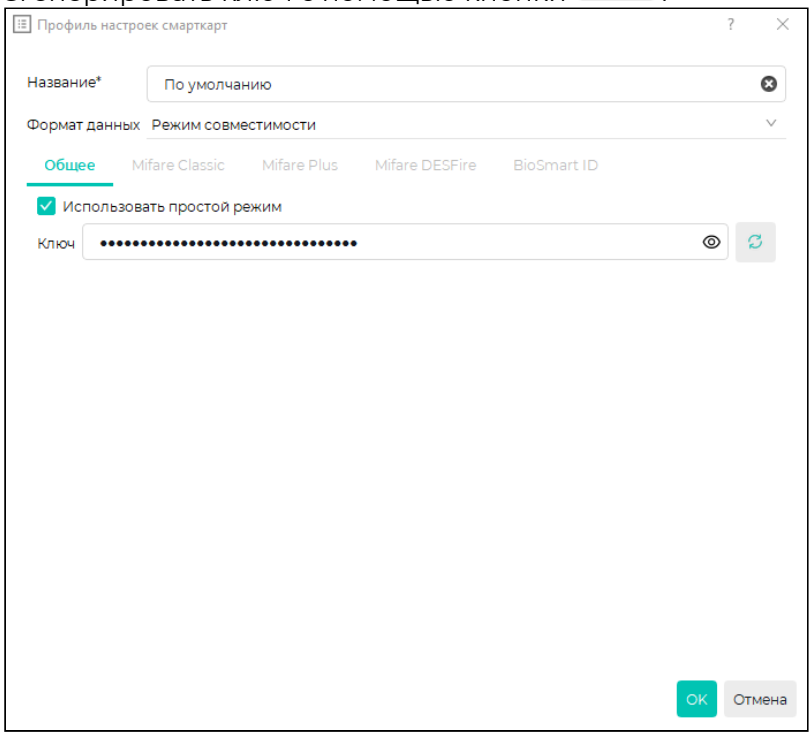
- Нажать кнопку **Добавить**, чтобы создать новый профиль смарткарт.
- В поле **Формат данных** установить одно из значений приведённых в таблице ниже.

Значение	Описание
Biosmart-Studio v6	Настройка определяет количество информации (8 байт), которое может быть записано в защищенную область карты. Можно записать следующие идентификаторы: • биометрический шаблон лица; • биометрический шаблон вен ладони; • UID карты.
Режим совместимости	Настройка определяет количество информации (4 байта), которое может быть записано в защищенную область карты. Можно записать следующие идентификаторы: • биометрический шаблон отпечатка пальца; • UID карты.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Выбрать вкладку **Общие.** Поставить отметку **Использовать простой режим**.

Сгенерировать ключ с помощью кнопки  .

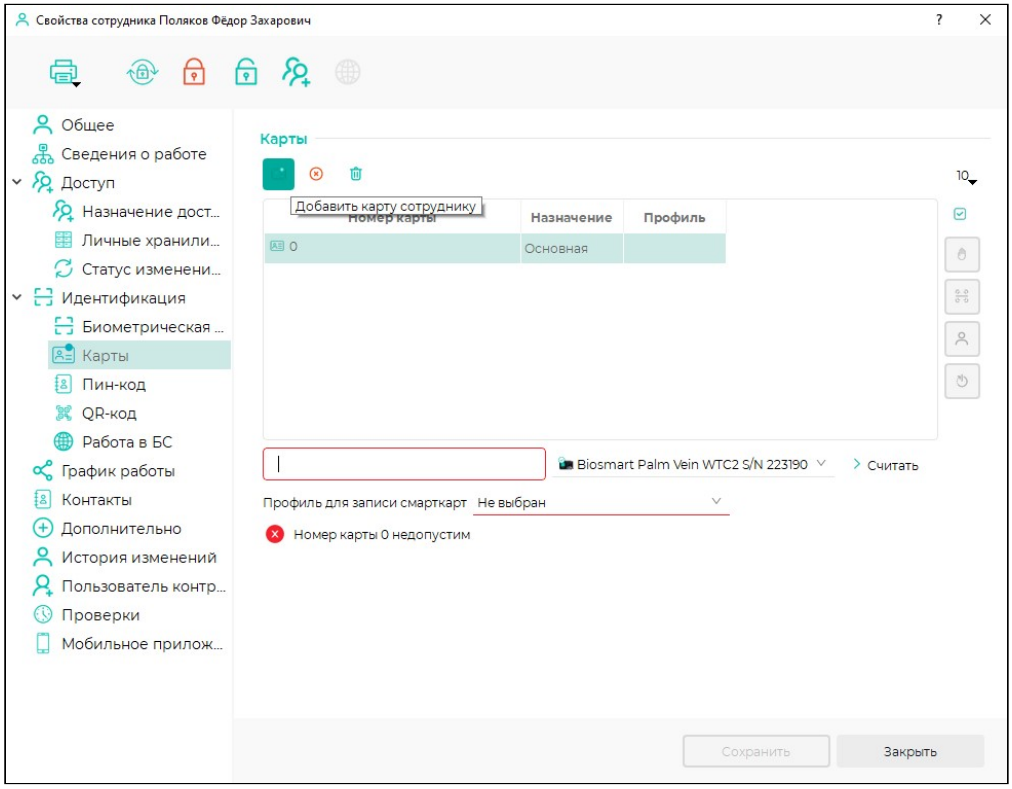


- Сохранить изменения, нажав кнопку **OK**.

2. Добавить идентификаторы карт в Biosmart-Studio v6

- В ПО Biosmart-Studio v6 в разделе **Сотрудники** откройте окно **Свойства сотрудника** и перейдите на вкладку **Идентификация – Карты**.
- В выпадающей строке выберите устройство (**BioSmart Palm Vein WTC2**) с помощью которого будет считан код карты и созданный профиль для записи смарткарт. После выбора устройства и профиля для записи смарткарт будет разблокирована кнопка **Считать**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Тип считывателя терминала должен быть совместим с типом RFID-карты, иначе код карты не будет считан. Совместимость форматов карт и исполнений терминала приведена в паспорте на терминал.

- Чтобы считать код карты, нажмите кнопку **Считать**. В поле ввода кода карты появится считанный код карты. Нажмите **Сохранить**.

> Для работы с RFID-картами в незащищенном режиме используйте предустановленную рабочую модель с передачей номера карты в формате Wiegand или настройте рабочую модель в веб-интерфейсе по инструкции Создание рабочей модели с отправкой данных по интерфейсу Wiegand.

8.7.2 Работа в защищенном режиме

Терминалом поддерживается защищённый режим работы для карт Mifare Plus SL1 и SL3.

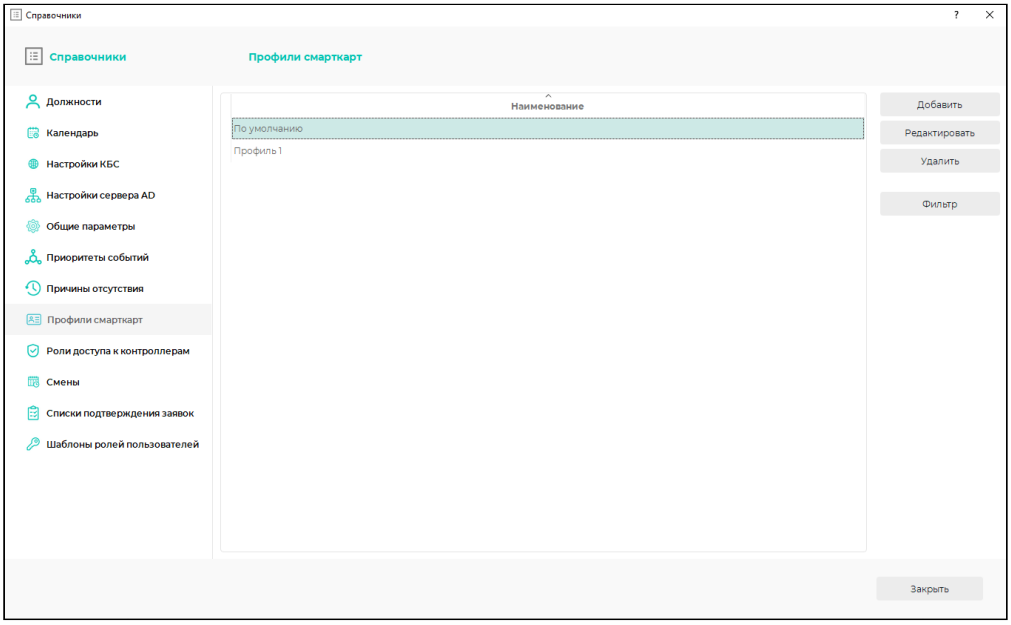
Для работы с картами Mifare Plus в защищенном режиме необходимо выполнить следующие действия:

1. Создать профиль смарткарт в ПО Biosmart-Studio v6

Для создания профиля смарткарт выполните вход в ПО Biosmart-Studio v6.

- Перейдите в **Основное меню** в раздел **Справочники** → **Профили смарткарт**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

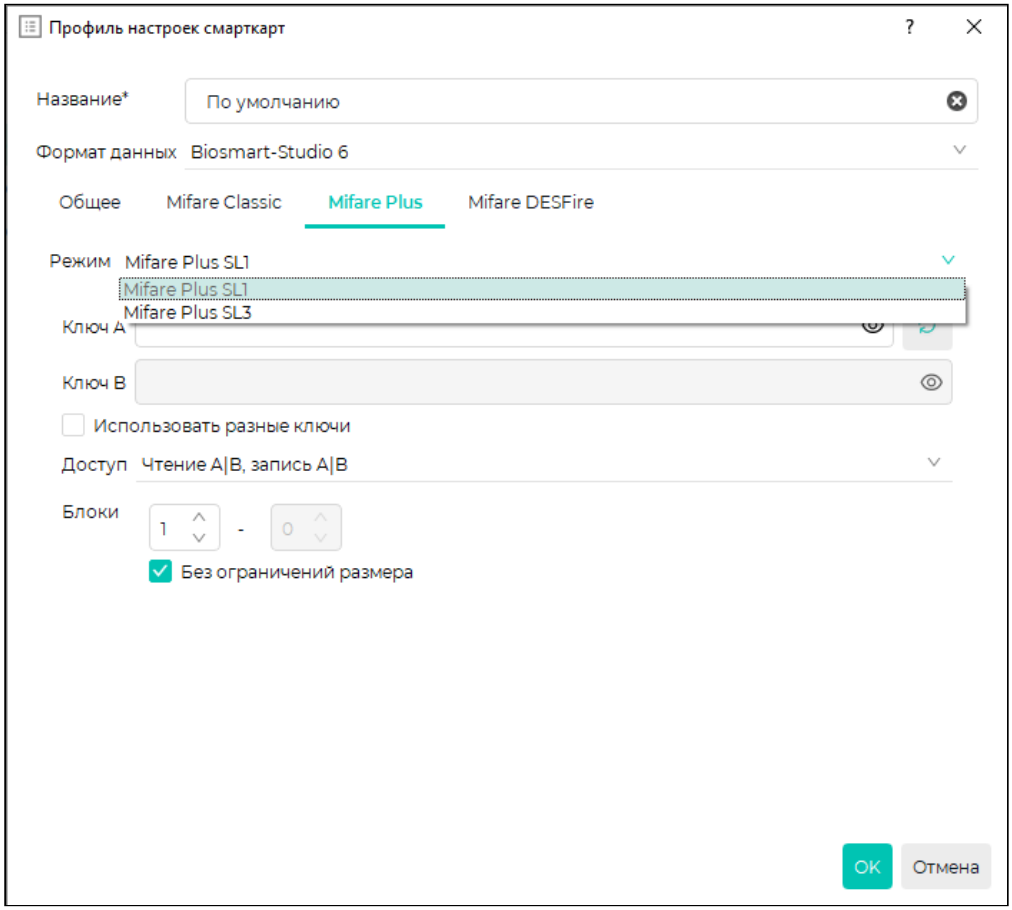


- Нажмите кнопку **Добавить**, чтобы создать новый профиль смарткарт.
- В поле **Формат данных** установите одно из значений приведённых в таблице ниже.

Значение	Описание
Biosmart-Studio v6	Настройка определяет количество информации (8 байт), которое может быть записано в защищенную область карты. Можно записать следующие идентификаторы: • биометрический шаблон лица; • биометрический шаблон вен ладони; • UID карты.
Режим совместимости	Настройка определяет количество информации (4 байта), которое может быть записано в защищенную область карты. Можно записать следующие идентификаторы: • биометрический шаблон отпечатка пальца; • UID карты.

- Выберите вкладку **Mifare Plus.** На вкладке задаются параметры для доступа к защищенной области памяти карт типа Mifare Plus и их перевода в режимы SL1 или SL3.
  В поле **Режим** из выпадающего списка выберите **Mifare Plus SL1** или **Mifare Plus SL3** в зависимости от используемого режима безопасности.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



- Заполните следующие поля в зависимости от используемого режима безопасности:

Описание параметров для режима безопасности SL1

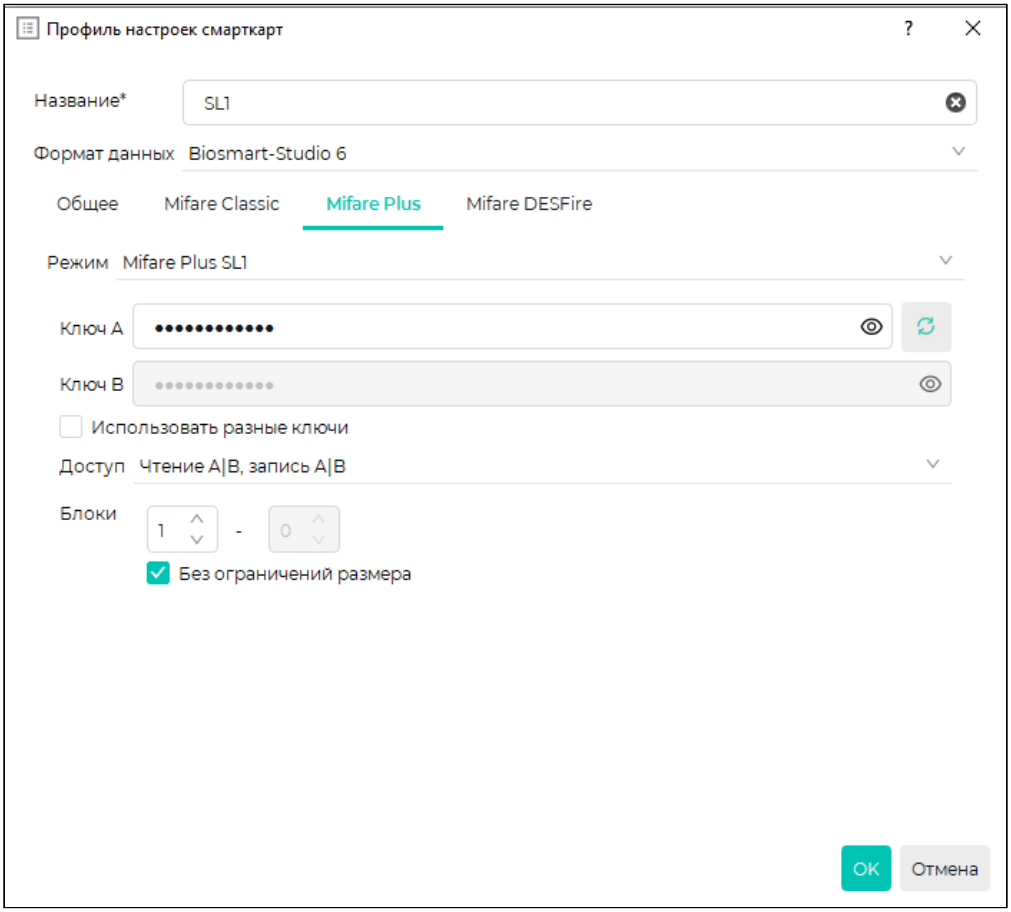
Название поля	Описание
Ключ A	Поле для указания ключей, которые используются для доступа к указанному блоку памяти карты. Ключ состоит из 12 шестнадцатеричных символов.
Ключ B	
Использовать разные ключи	Отметка в чек-боксе позволяет использовать различные ключи (ключ A и ключ B) для чтения и записи информации в память карты. В настоящее время данная функция недоступна. Для чтения и записи информации могут использоваться только одинаковые ключи A и B.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Название поля	Описание
Доступ	• Чтение AIB, запись AIB - для чтения и записи информации в память карты может использоваться ключ A или ключ B; • Чтение AIB, запись B - для чтения информации может использоваться ключ A или ключ B, для записи только ключ B; • Чтение B, запись B - для чтения и записи информации может использоваться только ключ B.
Блоки	В настоящее время данная функция недоступна. • В первом переключателе с помощью стрелок указывается номер блока памяти, в котором будут хранится биометрические шаблоны или UID сотрудника. Номер блока указывается в шестнадцатеричном формате. Указываемый блок не должен быть нулевым блоком нулевого сектора. • Во втором переключателе с помощью стрелок указывается максимальная длинна идентификатора, который может быть записан в выбранный блок памяти. Переключатель активен, если в чек-боксе **Без ограничений размера** не проставлена отметка. В таком случае, длина идентификатора, записываемого на карту, ограничивается ("обрезается") в соответствии с выбранным значением. Если в чек-боксе проставлена отметка, то в память карты будет записываться идентификатор без ограничений по длине. Например, в случае, если в память карты был записан идентификатор длинной 4 байта, а считыватель подключается по Wiegand-26, то считанный номер карты будет "обрезаться".

Ниже приведен пример настроек профиля смарткарт, используемого для перевода карты в режим SL1.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Описание параметров для режима безопасности SL3

Название поля	Описание
Мастер ключ	Поле для указания универсального ключа карты. Ключи задаются в шестнадцатеричном формате и должны состоять из 16 байт (32 символа)
Ключ конфигурации Ключ SL3 Ключ SL1 AES	Поле для указания ключей, используемых при переключения карты на более высокий уровень безопасности. Ключи задаются в шестнадцатеричном формате и должны состоять из 16 байт (32 символа)
Ключ A Ключ B	Поле для указания ключа, который используется для доступа к указанному блоку памяти карты. Ключи задаются в шестнадцатеричном формате и должны состоять из 16 байт (32 символа).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

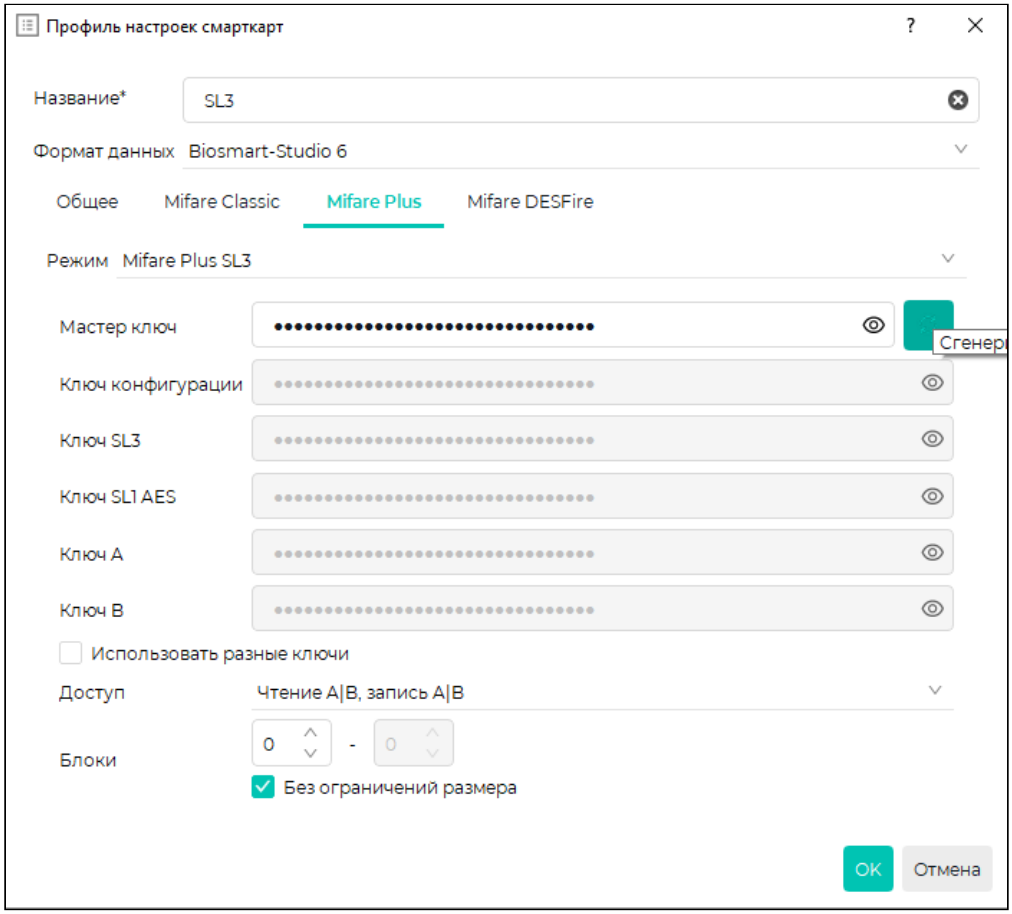
Название поля	Описание
Использовать разные ключи	Отметка в чек-боксе позволяет использовать различные ключи.  В настоящее время данная функция недоступна.
Доступ	• Чтение AIB, запись AIB - для чтения и записи информации в память карты может использоваться ключ A или ключ B; • Чтение AIB, запись B - для чтения информации может использоваться ключ A или ключ B, для записи только ключ B; • Чтение B, запись B - для чтения и записи информации может использоваться только ключ B.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Название поля	Описание
Блоки	В настоящее время данная функция недоступна. • В первом поле с помощью стрелок указывается номер блока памяти, в котором будут хранится биометрические шаблоны или UID сотрудника. Номер блока указывается в шестнадцатеричном формате. Указываемый блок не должен быть нулевым блоком нулевого сектора. • Во втором поле с помощью стрелок указывается максимальная длинна идентификатора, который может быть записан в выбранный блок памяти. Поле активно, если в чек-боксе **Без ограничений размера** не проставлена отметка. В таком случае, длина идентификатора, записываемого на карту, ограничивается ("обрезается") в соответствии с выбранным значением. Если в чек-боксе проставлена отметка, то в память карты будет записываться идентификатор без ограничений по длине. Например, в случае, если в память карты был записан идентификатор длинной 4 байта, а считыватель подключается по Wiegand-26, то считанный номер карты будет "обрезается".

Ниже приведен пример настроек профиля смарткарт, используемого для перевода карты в режим SL3.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



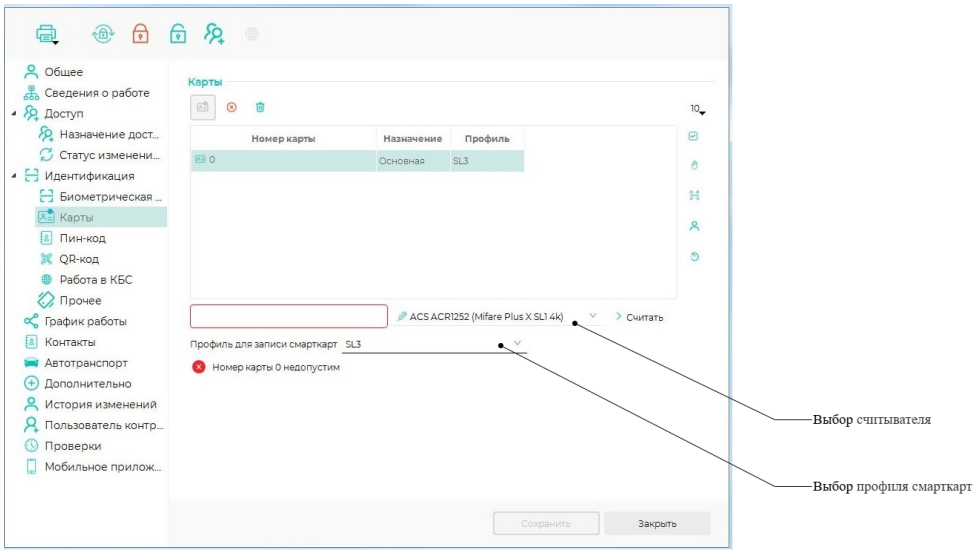
- Сохраните изменения в профиле смарткарт, нажав кнопку **OK**.

2. Перевести карту в один из режимов SL1 или SL3. Записать идентификатор сотрудника в защищенную паролем область памяти карты

Для перевода карты в режим SL1 или SL3 выполните следующие действия:

- Подключите к ПК считыватель, с помощью которого будет производится занесение карт в базу данных ПО Biosmart-Studio v6.
  Для перевода карт Mifare Plus в режим SL1 или SL3 должен использоваться USB-считыватель ACR1252U.
- Перейдите в раздел **Сотрудники** → выберите **Предприятие** → выберите сотрудника в списке → нажмите кнопку **Свойства** на панели инструментов.
- Перейдите в раздел **Карты** → нажмите кнопку **Добавить новую карту сотруднику** → выберите считыватель ACR1252U.
- В поле **Профиль для записи смарткарт** из выпадающего списка выберите профиль, созданный ранее, в который необходимо перевести карту.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



- Нажмите кнопку **Считать**.
- Поднесите карту к считывателю и нажмите кнопку **Записать шаблоны сотрудника/ Записать UID сотрудника на карту/Сканировать биометрическую информацию сотрудника и записать ее на карту,** следуйте дальнейшим указаниям.
  После этого смарткарта будет переведена в выбранный режим безопасности, в память карты будет записан идентификатор сотрудника и ключ доступа к защищенной области.

Перевод осуществляется последовательно от низшего уровня к высшему. Выполнить перевод с более высокого уровня на более низкий невозможно.

3. Настроить терминал на работу с картами Mifare Plus в режимах безопасности SL1 или SL3

Чтобы настроить терминал PV-WTC на чтение информации из защищенной области памяти карты необходимо выполнить следующие действия:

1. Открыть веб-интерфейс терминала PV-WTC.
2. В блоке **Core** заполнить следующие поля:

Параметр	Значение
Key for read template Mifare 1k, 4k cards	Указать ключ, используемый для считывания данных с защищенной области памяти карты.
Key for write template Mifare 1k, 4k cards	Указать ключ, используемый для считывания записи шаблонов с защищенной области памяти карты.

3. Нажать на кнопку **Save** и сохранить выбранные настройки.

8.7.3 Работа со смартфонами в качестве идентификатора

Терминал **BioSmart PV-WTC** позволяет использовать смартфоны (с установленным приложением BioSmart ID) в качестве идентификатора.

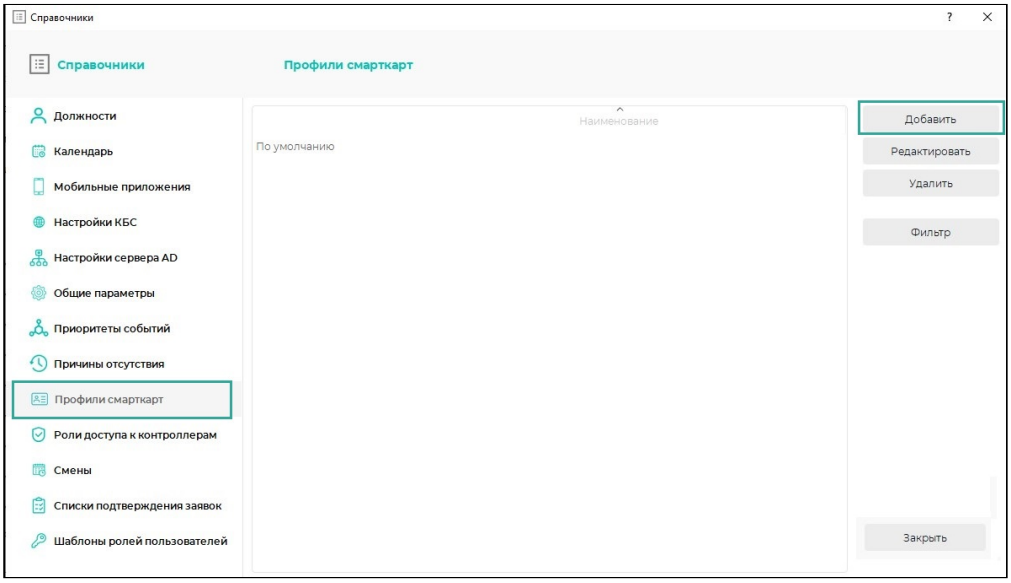
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Общие требования к смартфонам приведены в руководстве пользователя BioSmart ID в разделе **Общие сведения о приложении BioSmart ID.**

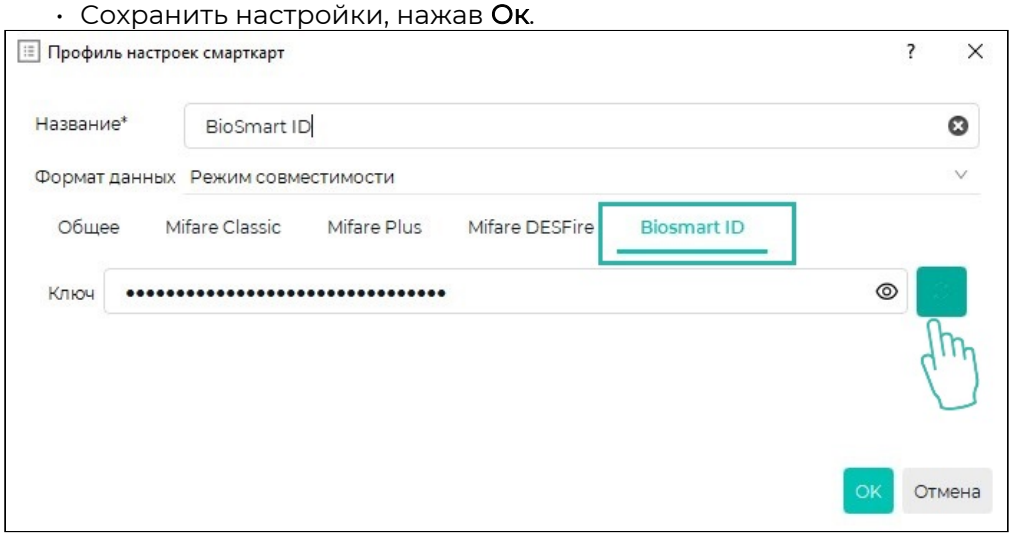
Для работы терминала и ПО на работу со смартфонами необходимо выполнить следующие действия:

1. Создать профиль смарткарт в ПО Biosmart-Studio v6

- Перейти в раздел **Основное меню** → **Справочники** → **Профили смарткарт**.
- Для создания нового профиля смарткарт нажать **Добавить.**



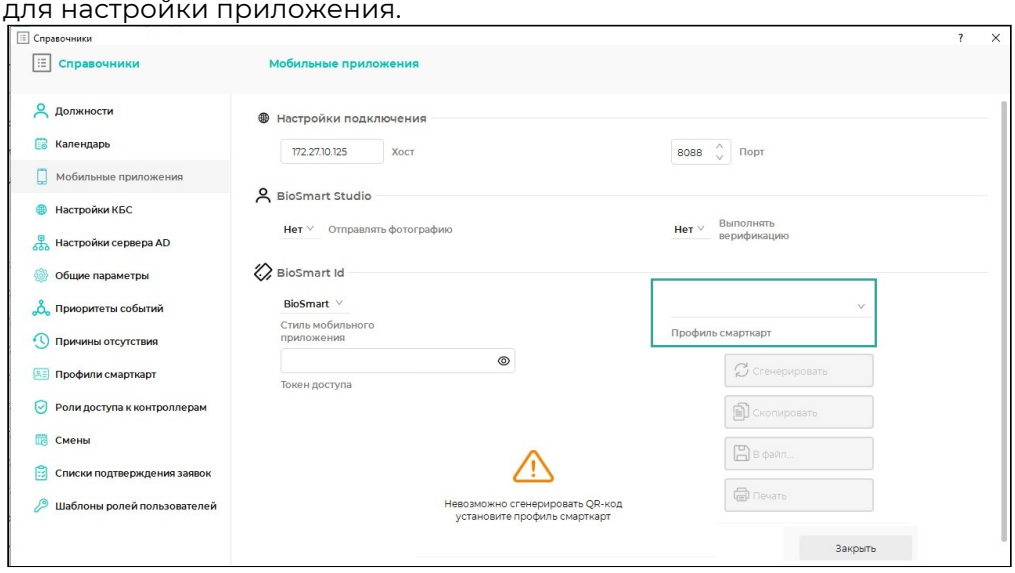
- Заполнить настройки профиля смарткарт:
  - **Название** – название профиля.
  - Во вкладке **BioSmart ID** нажать **Сгенерировать ключи**.
  - Сохранить настройки, нажав **Ок**.



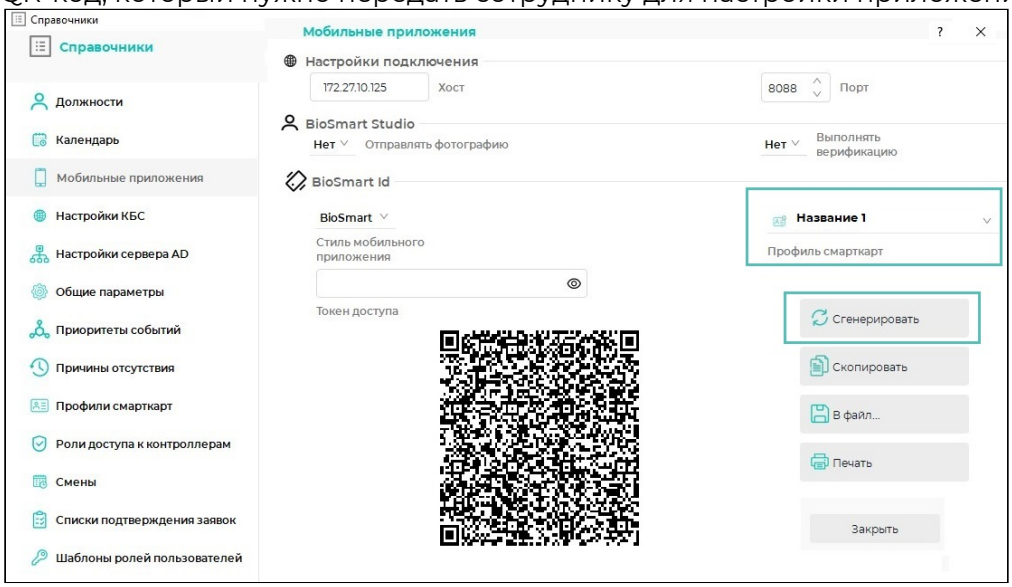
- Перейти в раздел **Основное меню** → **Справочники** → **Мобильные приложения**.
- В блоке **BioSmart ID** в поле **Профиль смарткарт** из выпадающего списка выбрать название профиля смарткарт.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Выбор профиля смарткарт необходим для генерации QR-кода с номером ключа для настройки приложения.



- После заполнения поля **Профиль смарткар**т нажать **Сгенерировать**. Отобразится QR-код, который нужно передать сотруднику для настройки приложения.



2. Создать виртуальную карту в мобильном приложении BioSmart ID

Чтобы использовать смартфон в качестве идентификатора сотруднику необходимо выполнить следующие действия:

- Скачать мобильное приложение **BioSmart ID** из онлайн-магазина Google Play или App Store. После первого запуска приложения необходимо предоставить разрешение для использования Bluetooth;
- Открыть мобильное приложение и нажать **Сгенерировать карту.**
- Ввести название в поле **Название карты.**
- Поле **Хеш-код** не редактируется.
- Нажать **Добавить новую карту.**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Нажать кнопку  в правом нижнем углу экрана и выбрать формат, в котором будет скопирован номер карты.
  Настройки должны соответствовать следующим требованиям:
  - Система счисления в приложении должна соответствовать системе счисления, выбранной в ПО Biosmart-Srudio v6.
  - Разрядность кода карты должна соответствовать битности интерфейса Wiegand используемого считывателя BioSmart.

- Нажать кнопку  и выбрать **Копировать номер**.
- Передать номер карты администратору СКУД для назначение ее сотруднику в ПО Biosmart-Studio v6.
- Если в конфигурации считывателя был задан **Ключ шифрования**, то в **BioSmart ID** необходимо нажать кнопку  → нажать **Сканировать настройки** → отсканировать QR-код, выданный администратором СКУД.

3. Настроить терминал на работу с картами Mifare Plus в режимах безопасности SL1 или SL3

Чтобы настроить терминал PV-WTC на чтение информации из защищенной области памяти карты необходимо выполнить следующие действия:

1. Открыть веб-интерфейс терминала PV-WTC.
2. В блоке **Core** заполнить следующие поля:

Параметр	Значение
Key for read template Mifare 1k, 4k cards	Указать ключ, используемый для считывания данных с защищенной области памяти карты.
Key for write template Mifare 1k, 4k cards	Указать ключ, используемый для считывания записи шаблонов с защищенной области памяти карты.

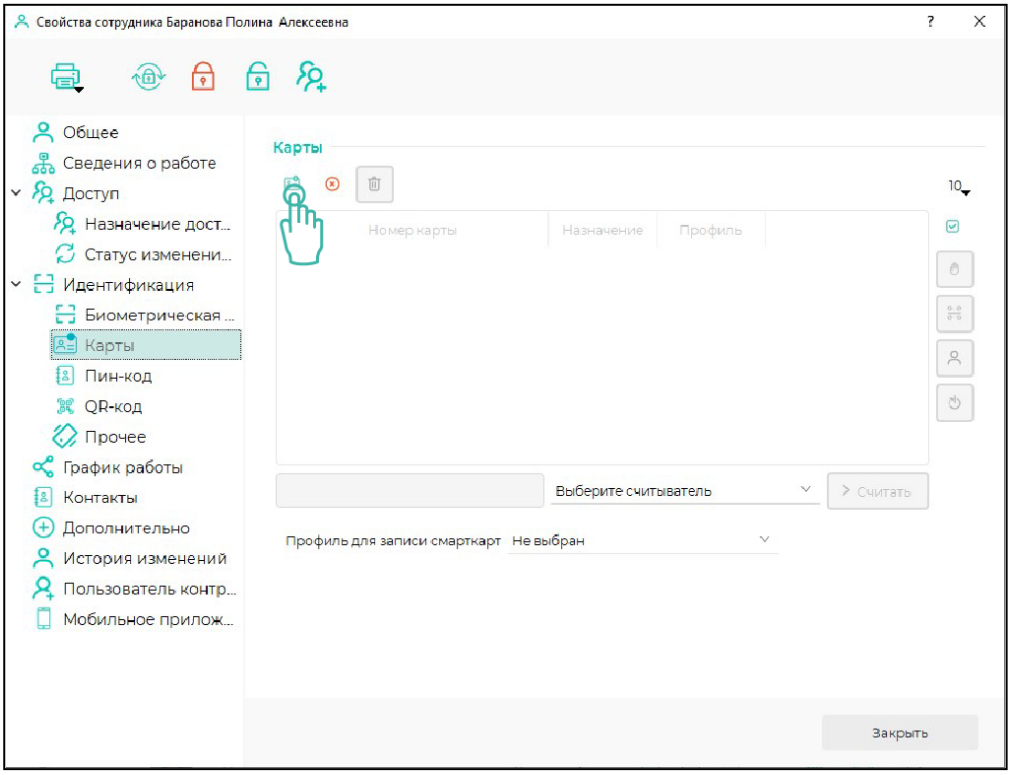
3. Нажать на кнопку **Save** и сохранить выбранные настройки.

4. Добавить мобильные идентификаторы в Biosmart-Studio v6

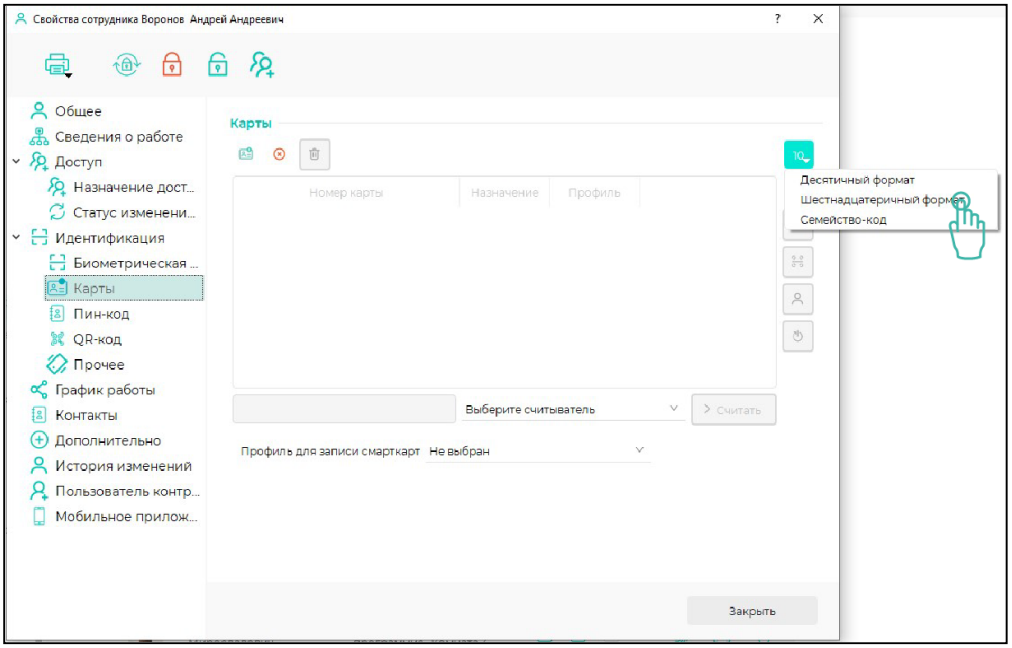
Для назначения сотруднику карты выберите сотрудника, откройте окно **Свойства сотрудника** и перейдите на вкладку **Карты**.

- Нажмите кнопку **Добавить карту сотруднику.**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

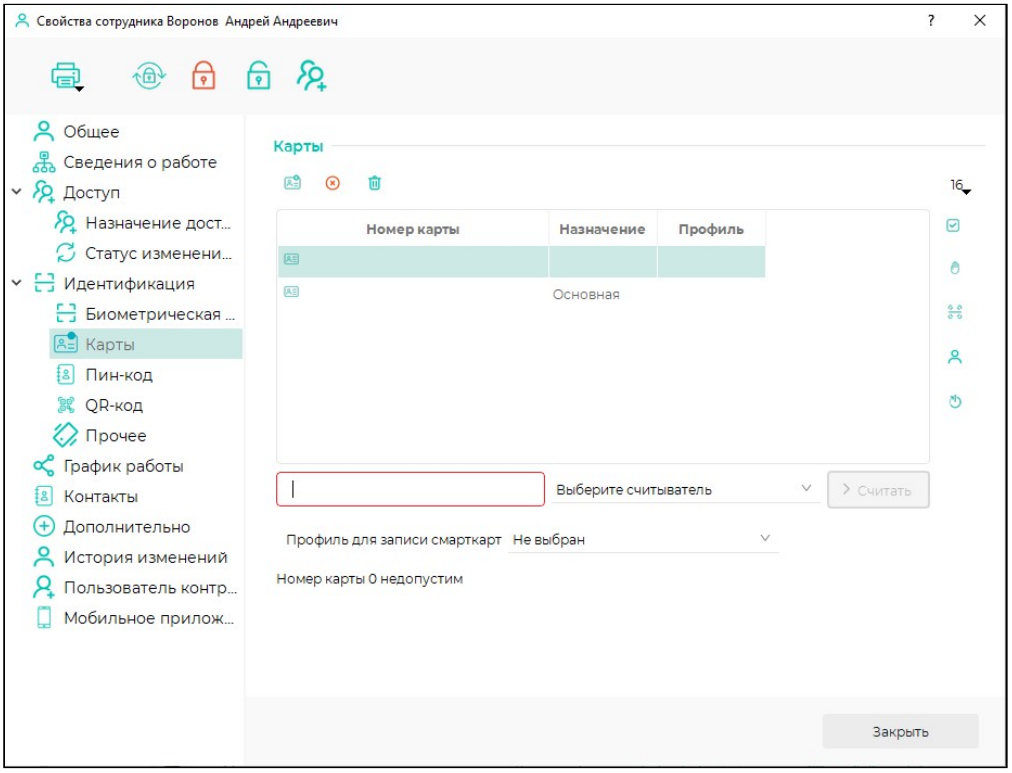


- Выберите формат отображения кода карты **Шестнадцатеричный формат/ Десятичный формат.**



- Укажите код карты.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



По завершению регистрации карты нажмите кнопку **Сохранить**, затем **Закрыть**.

8.7.4 Настройка работы терминала с картами, инициализированными в стороннем ПО

Чтобы настроить терминал на чтение идентификатора сотрудника из защищенной области карты **Mifare Plus SL3**, инициализированной с помощью стороннего ПО, необходимо выполнить следующие действия:

1. Открыть веб-интерфейс терминала PV-WTC.
2. В блоке **Core** заполнить следующие поля:

Параметр	Значение
Key for read template Mifare 1k, 4k cards	Указать ключ, используемый для считывания данных с защищенной области памяти карты.
Key for write template Mifare 1k, 4k cards	Указать ключ, используемый для считывания записи шаблонов с защищенной области памяти карты.
RFID Offset address (dec, 0-4294967295)	Указать смещение шаблона карты для чтения шаблона карты.

3. Нажать на кнопку **Save** и сохранить выбранные настройки.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

9 РАБОТА С ДОПОЛНИТЕЛЬНЫМ ОБОРУДОВАНИЕМ

9.1 Работа с устройством измерения температуры BioSmart Thermoscan

В данном разделе описан порядок настройки терминала BioSmart PV-WTC для работы с устройством BioSmart Thermoscan H, а также порядок действий сотрудников при выполнении идентификации с термометрией.

9.1.1 Общие сведения

Устройство BioSmart Thermoscan H предназначено для бесконтактного измерения температуры тела человека в районе запястья. Использование BioSmart Thermoscan H совместно с терминалом BioSmart PV-WTC позволяет автоматизировать процесс измерения температуры при проведении идентификации сотрудника.

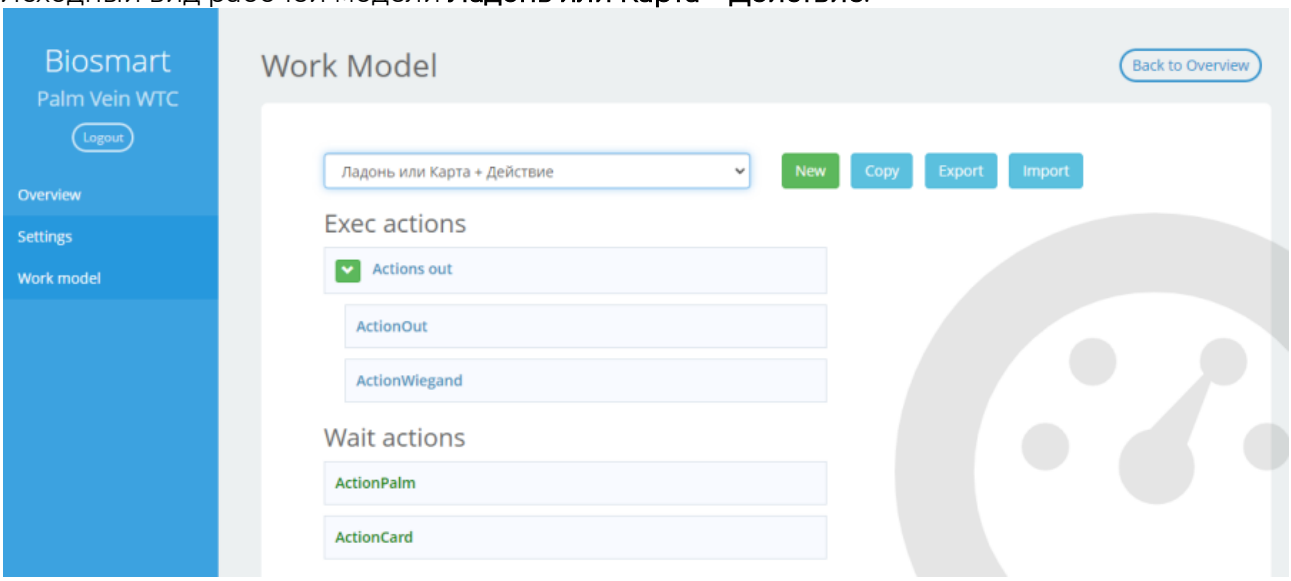
Работа терминала с устройством BioSmart Thermoscan поддерживается, начиная с версии 11.6.0 встроенного ПО терминала и версии 5.10.3 ПО Biosmart-Studio.

Устройство BioSmart Thermoscan подключается к разъему USB на плате терминала **при выключенном питании терминала**.

Настройка работы с устройством BioSmart Thermoscan H выполняется путем внесения изменений в существующую рабочую модель или путем создания новой рабочей модели в веб-интерфейсе терминала. Затем необходимо настроить параметры измерения температуры в меню терминала или в веб-интерфейсе.

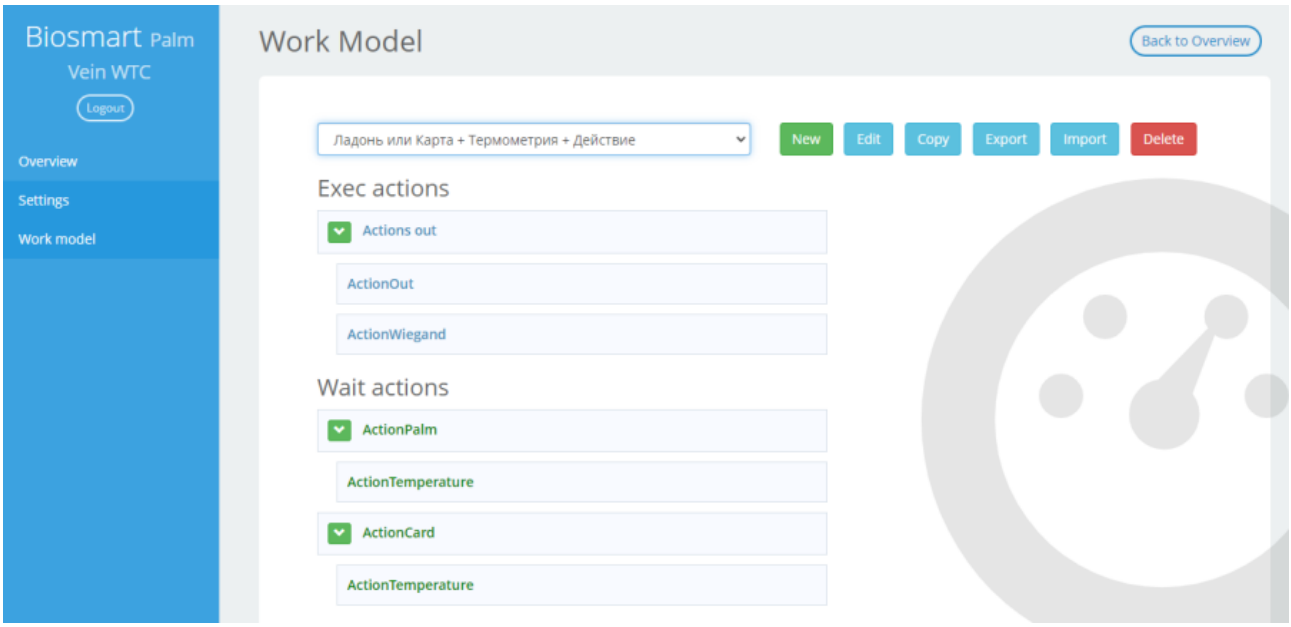
9.1.2 Настройка рабочей модели

Откройте веб-интерфейс терминала и перейдите в раздел **Work model**.
Для примера рассмотрим внесение изменений в предустановленную рабочую модель **Ладонь или Карта + Действие**.
Исходный вид рабочей модели **Ладонь или Карта + Действие**:

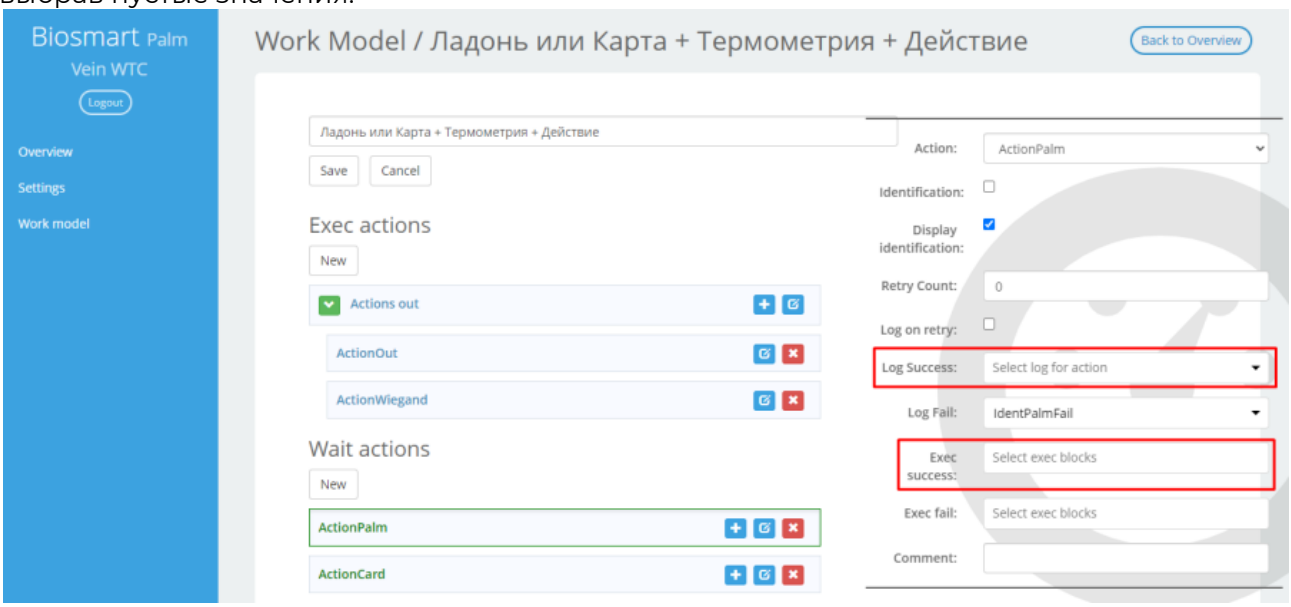


Отредактированная рабочая модель **Ладонь или Карта + Действие**:

SEC.RU | Короткий путь к информации
Скачано с sec.ru



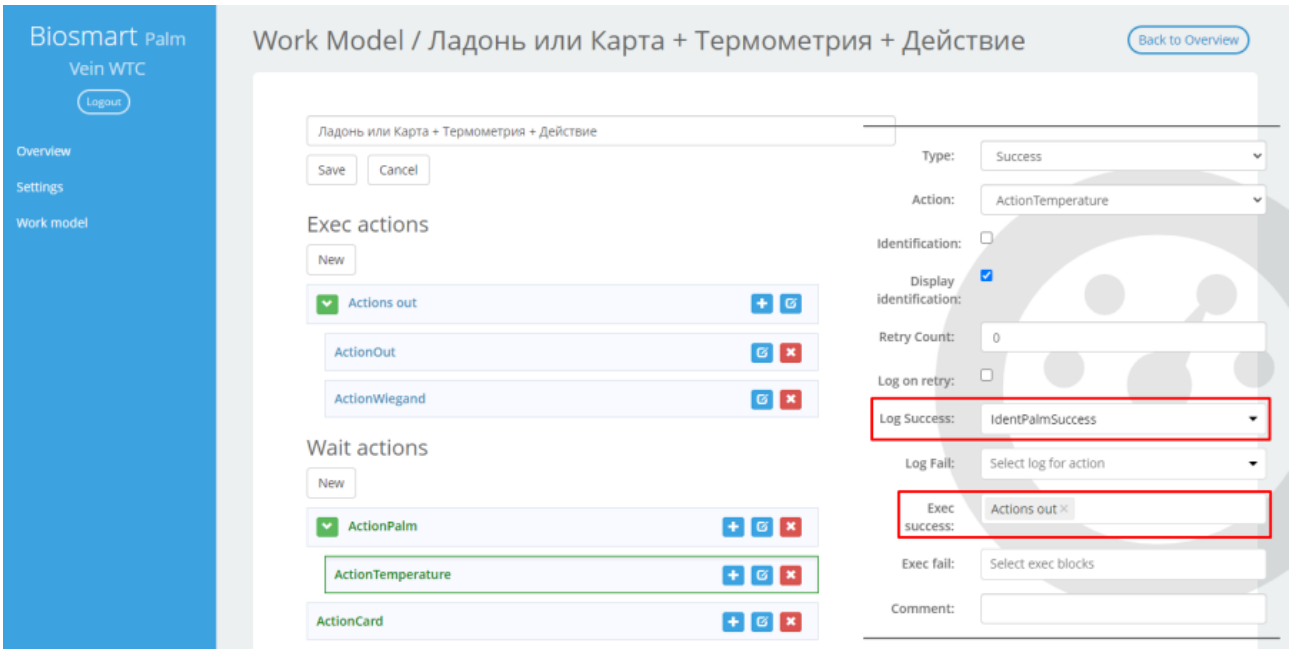
Создадим копию выбранной рабочей модели. После создания копии станет доступно редактирование параметров.
При желании можно изменить название новой рабочей модели.
У события **ActionPalm** (Ожидание ладони) очистим поля **Log Success** и **Exec Success**, выбрав пустые значения.



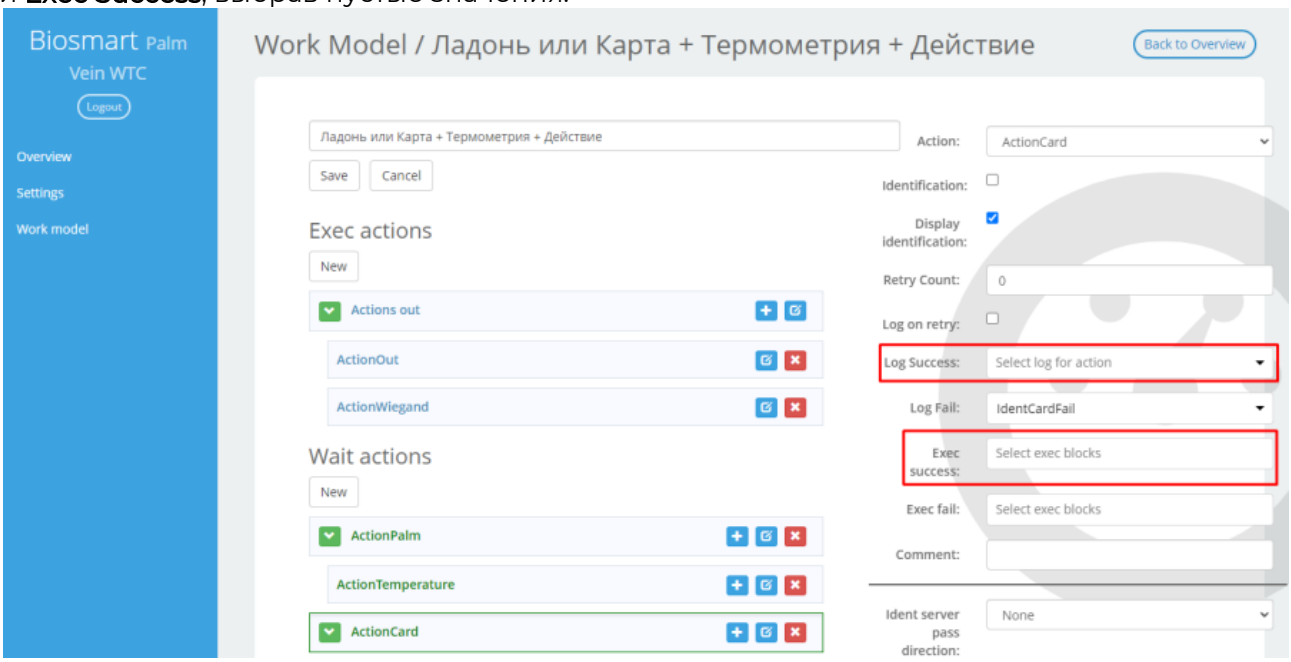
Добавим действие **ActionTemperature** со следующими параметрами:

- Генерировать сообщения в ПО Biosmart-Studio v6 по результатам измерения температуры (укажем в поле **Log Success** лог **IdentPalmSuccess**);
- Выполнять блок действий, если результат измерения температуры не выходит за пороговые значения (укажем необходимый блок действий в поле **Exec Success**). Пороговые значения настраиваются в меню терминала (см. пункт Настройка параметров измерения температуры) или в веб-интерфейсе (см. пункт Настройки терминала BioSmart PV-WTC в веб-интерфейсе).

SEC.RU | Короткий путь к информации
Скачано с sec.ru



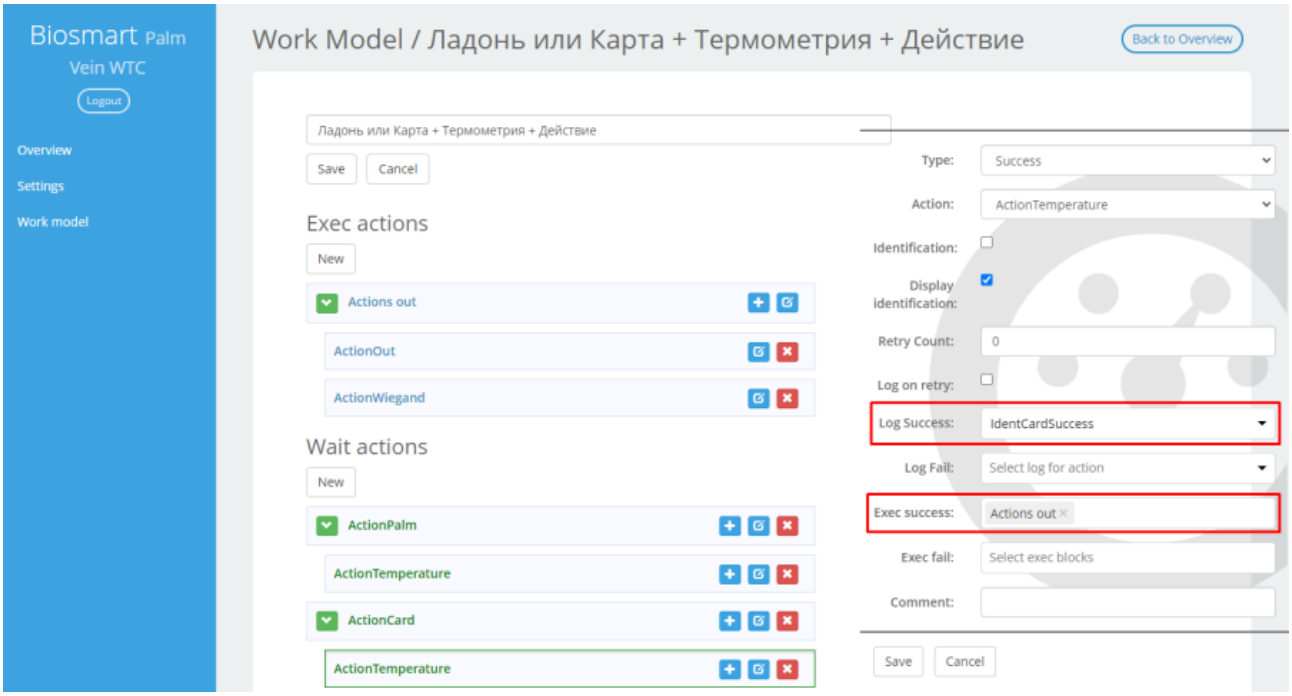
Аналогичным образом у события **ActionCard** (Ожидание карты) очистим поля **Log Success** и **Exec Success**, выбрав пустые значения.



Добавим действие **ActionTemperature** со следующими параметрами:

- Генерировать сообщения в ПО Biosmart-Studio v6 по результатам измерения температуры (укажем в поле **Log Success** лог **IdentCardSuccess**);
- Выполнять блок действий, если результат измерения температуры не выходит за пороговые значения (укажем необходимый блок действий в поле **Exec Success**). Пороговые значения настраиваются в меню терминала (см. пункт Настройка параметров измерения температуры) или в веб-интерфейсе (см. пункт Настройки терминала BioSmart PV-WTC в веб-интерфейсе).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

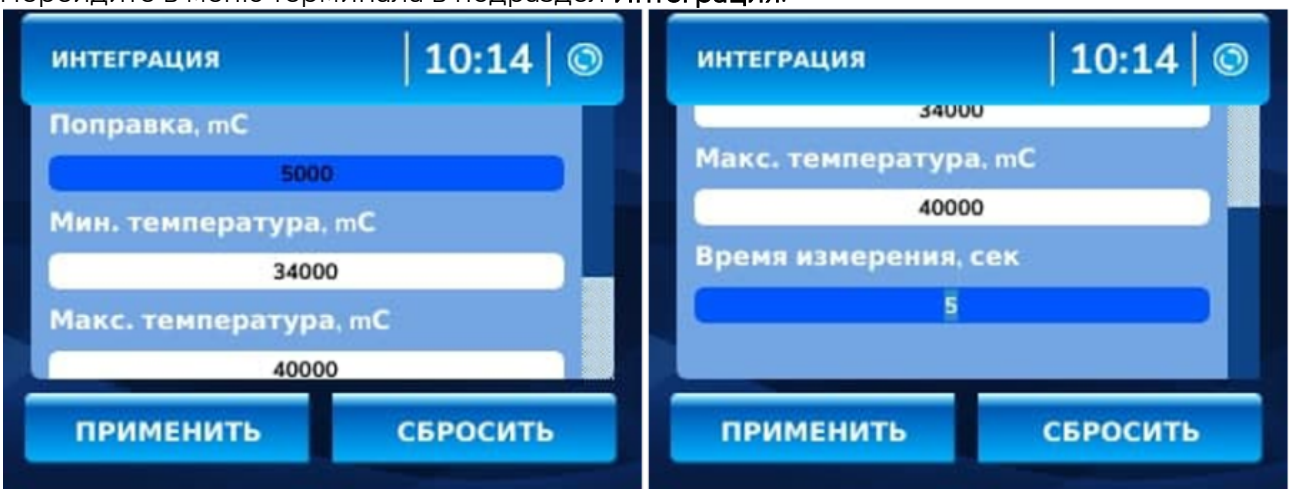


Сохраним внесенные изменения нажатием кнопки **Save**.

9.1.3 Настройка параметров измерения температуры

Параметры измерения температуры можно настроить в меню терминала или в веб-интерфейсе. Настройки в веб-интерфейсе описаны в пункте Настройки терминала BioSmart PV-WTC в веб-интерфейсе. В данном пункте будут описаны настройки в меню терминала.

Перейдите в меню терминала в подраздел **Интеграция**.



Доступные настройки:

- **Поправка, mC** - значение компенсационной поправки в 1/1000 °C, добавляемой к измеренному значению температуры. Определяется экспериментально с помощью другого термометра и зависит от условий эксплуатации поправочное значение, применяемое к результату измерения. Например, для того чтобы выводимое на

SEC.RU | Короткий путь к информации
Скачано с sec.ru

дисплей значение температуры было выше измеренного на 4,5 °C, нужно указать значение поправки равное 4500.

- **Мин. температура, mC** - минимальное значение температуры в 1/1000 °C, ниже которого идентификация будет считаться неуспешной. Если результат измерения температуры с учётом поправки оказался ниже минимального значения, то на дисплей терминала будет выводиться сообщение «**Температура слишком низкая**». Например, для того чтобы задать минимальное значение равное 35 °C, значение параметра нужно указать 35000.
- **Макс. температура, mC** - максимальное значение температуры в 1/1000 °C, выше которого идентификация будет считаться неуспешной. Если результат измерения температуры с учётом поправки оказался выше максимального значения, то на дисплей терминала будет выводиться сообщение «**Температура слишком высокая**». Например, для того, чтобы задать максимальное значение температуры равное 37 °C, значение параметра нужно указать 37000.
- **Время измерения, сек** - время в секундах, в течении которого терминал ожидает прикладывания запястья сотрудника к датчику температуры.

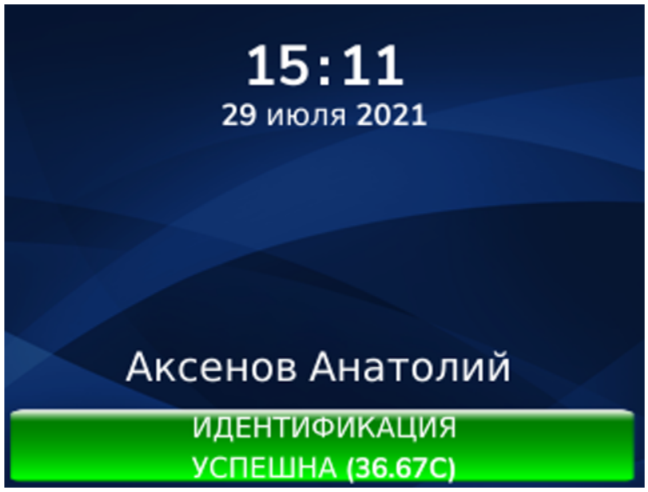
9.1.4 Порядок работы

В режиме ожидания на дисплее терминала выводится ожидаемое действие в соответствии с выбранной рабочей моделью, например, «**Приложите ладонь**». Сотрудник подходит к терминалу и прикладывает ладонь к сканеру. Терминал проводит идентификацию сотрудника по венам ладони.
Если идентификация успешна, терминал отображает сообщение «**Поднесите руку к сенсору температуры**». При этом на дисплее отображается полоска прогресса, показывающая оставшееся до конца измерения время, и максимальное значение температуры, полученное в ходе текущего измерения. По окончании времени измерения это значение будет считаться результатом измерения.

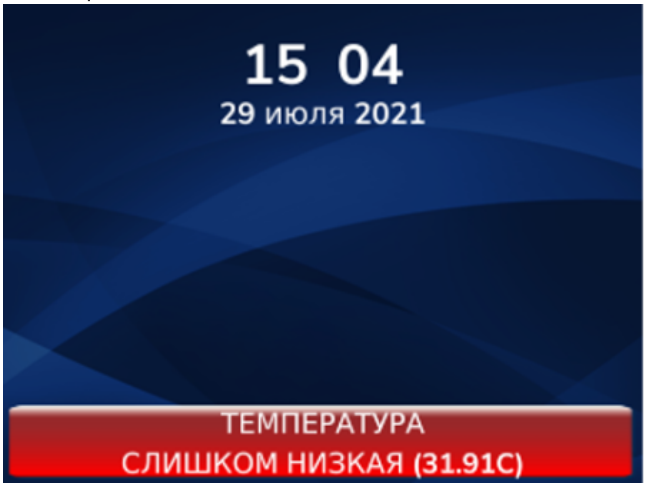


По окончании времени измерения терминал сравнивает результат измерения с заданными в настройках максимальным и минимальным пороговыми значениями. В случае, если результат не выходит за пороговые значения, на дисплее терминала появится сообщение «**Идентификация успешна**».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

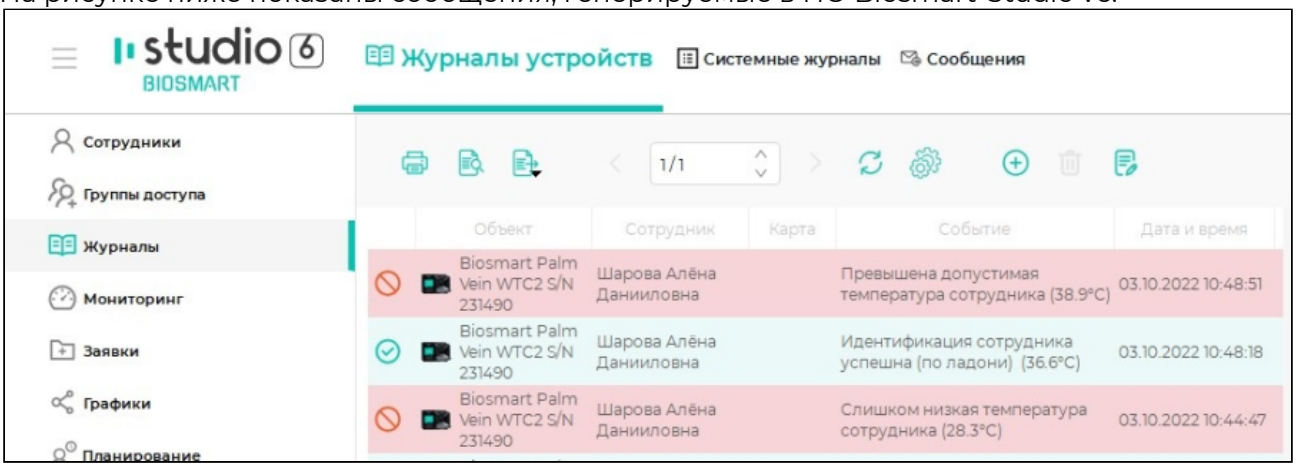


В случае, если результат выходит за пороговые значения – на дисплее отображается сообщение о слишком высокой или слишком низкой температуре.





На рисунке ниже показаны сообщения, генерируемые в ПО Biosmart-Studio v6.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

9.2 Работа с алкотестером Динго B-02

9.2.1 Общие сведения

Алкотестер Динго B-02 предназначен для контроля трезвости персонала методом экспресс анализа выдыхаемого воздуха на содержание паров алкоголя. Использование Динго B-02 совместно с терминалом BioSmart PV-WTC позволяет автоматизировать процесс проверки на алкоголь при проведении идентификации сотрудника.

Работа терминала с алкотестером Динго B-02 поддерживается, начиная с версии 11.6.0 встроенного ПО терминала.

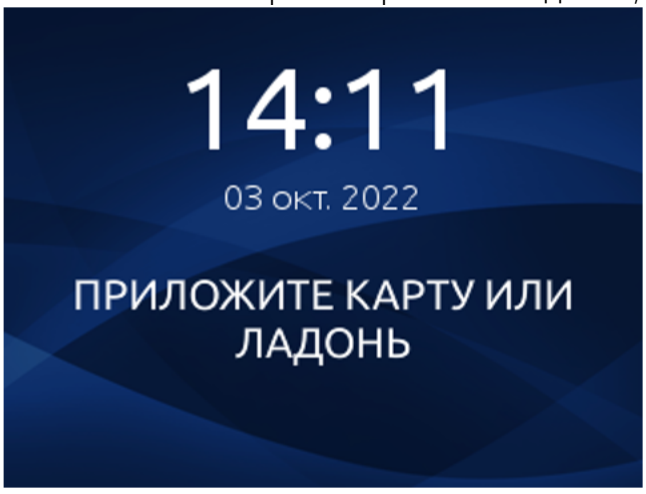
Порядок подключения алкотестера Динго B-02 описан в разделе Подключение к алкотестеру Динго B-02.

Перед началом работы проверьте, что на алкотестере Динго B-02 (на плате, при вскрытии корпуса) переключатель находится в положении PC mode.

Для работы с алкотестером установите на терминале рабочую модель **Ладонь или карта + алкотестер USB** или **Кн. вх/вых + ладонь или карта + алкотестер USB**. Это можно сделать в меню терминала, в веб-интерфейсе или ПО Biosmart-Studio v6. Описание рабочих моделей приведено в пункте Предустановленные рабочие модели.

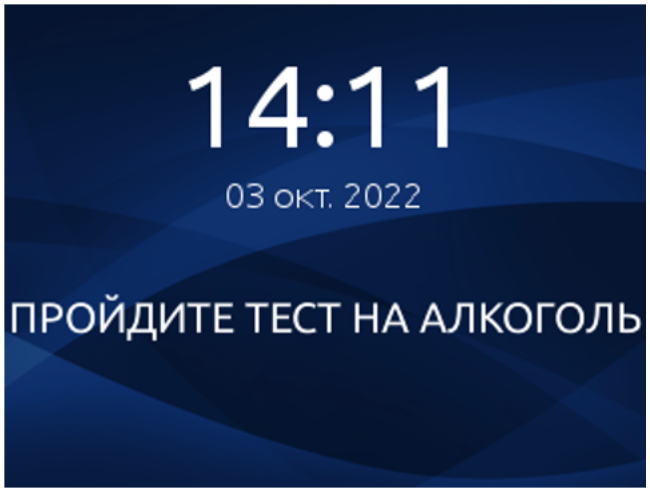
9.2.2 Порядок работы

В режиме ожидания на дисплее терминала выводится ожидаемое действие в соответствии с выбранной рабочей моделью, например, «**Приложите карту или ладонь**».

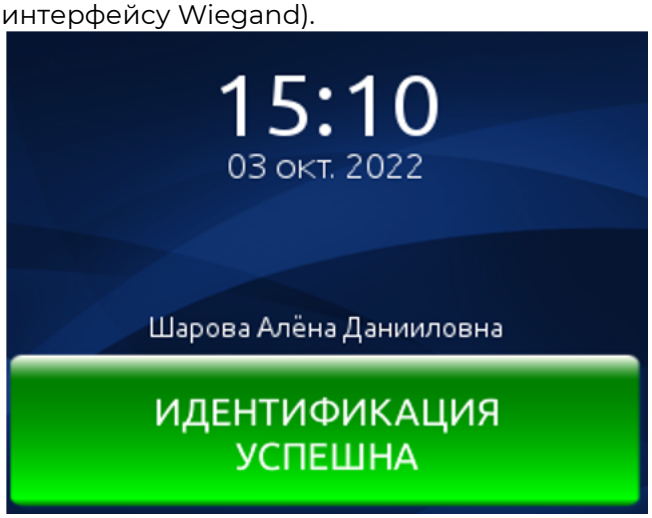


Сотрудник подходит к терминалу и прикладывает ладонь к сканеру. Терминал проводит идентификацию сотрудника по венам ладони.
Если идентификация успешна, терминал отображает сообщение «**Пройдите тест на алкоголь**» и посылает команду запуска на алкотестер.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

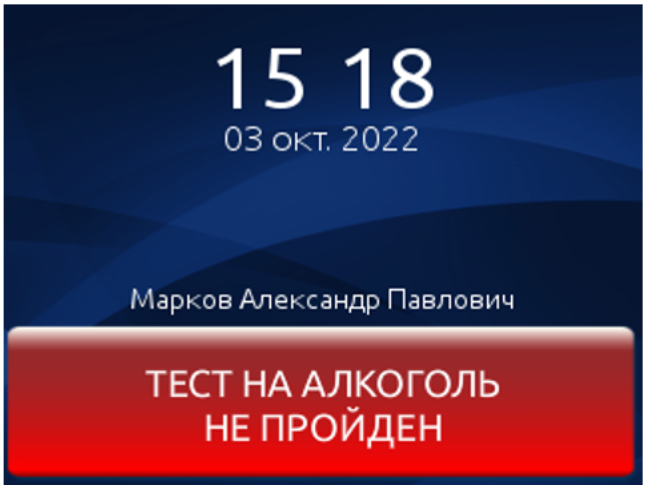


Алкотестер издает короткий звуковой сигнал. Индикатор **СОСТОЯНИЕ** на передней панели алкотестера начинает мигать красным, что означает прогрев и подготовку к тестированию. Через несколько секунд алкотестер издаст два коротких звуковых сигнала и индикатор **СОСТОЯНИЕ** изменит цвет на зелёный, указывая на то, что алкотестер готов к тестированию.
Сотрудник выдыхает в отверстие для приёма анализируемого воздуха.
Индикатор **СОСТОЯНИЕ** загорается оранжевым, что означает проведение анализа.
Если результат анализа не превышает пороговое значение, индикатор **В НОРМЕ** загорится зелёным, на дисплее терминала появится сообщение «**Идентификация успешна**» и будут выполнены действия согласно установленной рабочей модели (сработает встроенное реле терминала, код карты сотрудника будет передан по интерфейсу Wiegand).

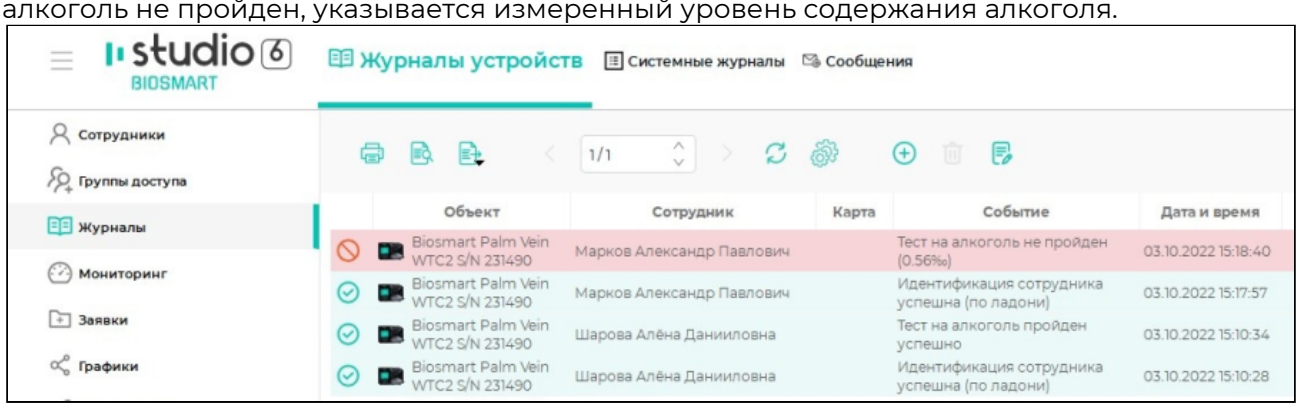


Если результат анализа превысил пороговое значение, индикатор **АЛКОГОЛЬ** загорится красным и на дисплее терминала появится сообщение «**Тест на алкоголь не пройден**».

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Пороговое значение устанавливается на алкотестере (см. документацию на алкотестер Динго B-02) и может находится в диапазоне от 0,10‰ до 0,90‰ (промилле). По умолчанию установлено 0,2‰.
В ПО Biosmart-Studio v6 генерируются соответствующие сообщения. В случае если тест на алкоголь не пройден, указывается измеренный уровень содержания алкоголя.



По зафиксированным событиям в ПО Biosmart-Studio v6 можно сформировать отчет «**Журнал проверки на алкоголь**» (см. Руководство пользователя ПО Biosmart-Studio v6).

9.3 Работа с БУР BioSmart

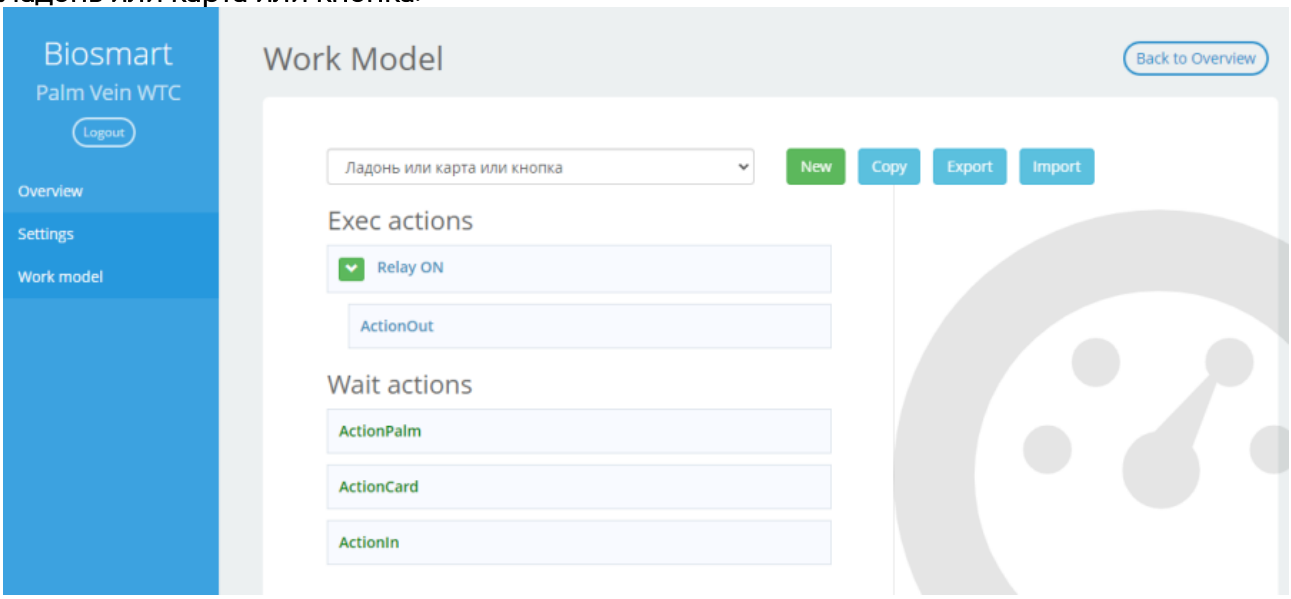
9.3.1 Общие сведения

Блок управления реле БУР BioSmart предназначен для дистанционного включения исполнительных устройств (электромагнитные замки, турникеты и т.д.) и приема данных с внешних датчиков (датчик прохода, сигнальная кнопка и т.д.).
Обмен данными между БУР BioSmart и терминалом производится по интерфейсу RS-485, тем самым обеспечивается надежная защита объектов от несанкционированного доступа путем замыкания управляющих проводов.
Порядок подключения БУР BioSmart описан в разделе Подключение электромагнитного замка через БУР BioSmart.
Настройка работы с БУР BioSmart выполняется путем внесения изменений в существующую рабочую модель или путем создания новой рабочей модели в WEB-интерфейсе терминала.

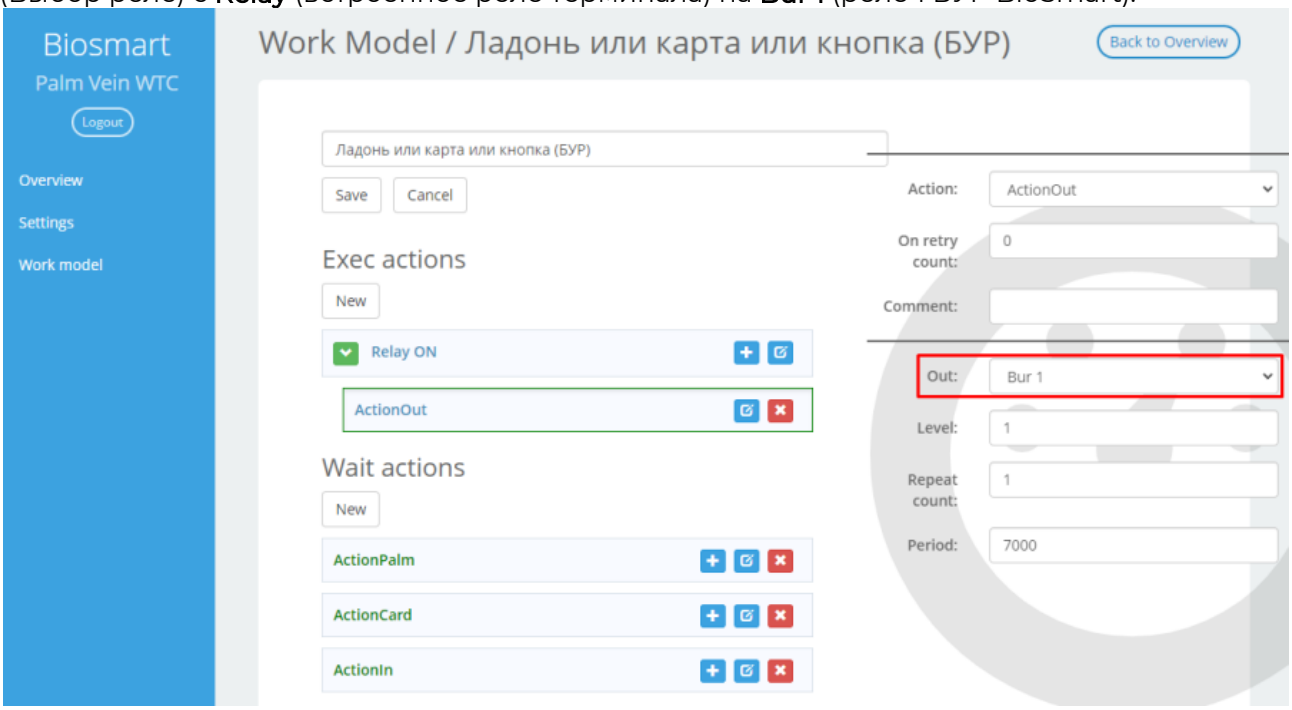
SEC.RU | Короткий путь к информации
Скачано с sec.ru

9.3.2 Настройка рабочей модели

Откройте WEB-интерфейс терминала и перейдите в раздел **Work model**.
Для примера рассмотрим внесение изменений в предустановленную рабочую модель **Ладонь или карта или кнопка**.

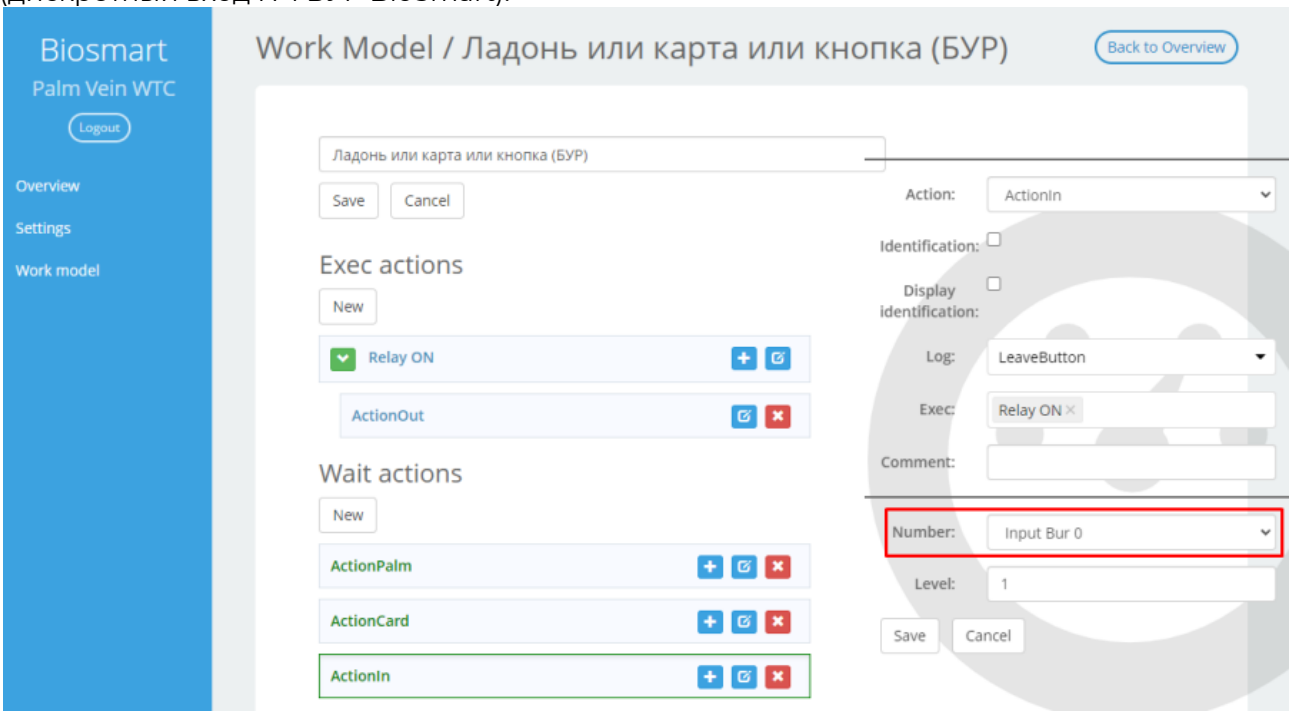


Предположим, что в ней необходимо заменить срабатывание встроенного реле терминала на срабатывание реле БУР BioSmart и прием сигнала с дискетного входа терминала на прием сигнала с дискретного входа БУР BioSmart.
Создадим копию выбранной рабочей модели. После создания копии станет доступно редактирование параметров.
При желании можно изменить название новой рабочей модели.
В блоке **Exec actions** у действия **ActionOut** (Управление реле) изменим параметр **Out** (Выбор реле) с **Relay** (встроенное реле терминала) на **Bur 1** (реле 1 БУР BioSmart).



SEC.RU | Короткий путь к информации
Скачано с sec.ru

В блоке **Wait actions** у события **ActionIn** (Ожидание нажатия кнопки) изменим параметр **Number** (Номер дискретного входа) с **Input 0** (дискретный вход терминала) на **Input Bur 0** (дискретный вход №1 БУР BioSmart).



Сохраним внесенные изменения нажатием кнопки **Save**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ ТЕРМИНАЛА BIOSMART PV-WTC

В данном разделе приведены виды технического обслуживания терминала, соответствующий им перечень операций, а также меры безопасности.
При хранении и эксплуатации терминала требуется проведение периодического технического обслуживания, включающего в себя проверку внешнего вида, удаление грязи и пыли, проверку работоспособности. Операции, перечисленные в настоящем разделе, имеют своей целью поддержание терминала в работоспособном состоянии и обеспечение условий для длительной безотказной работы.
В разделе указана рекомендуемая периодичность технического обслуживания. Заказчик должен самостоятельно определять частоту проведения технического обслуживания в зависимости от условий эксплуатации терминала. Например, если терминал эксплуатируется в запыленном помещении, то операцию по удаления грязи и пыли с поверхностей терминала следует проводить чаще, чем это указано в настоящем разделе.

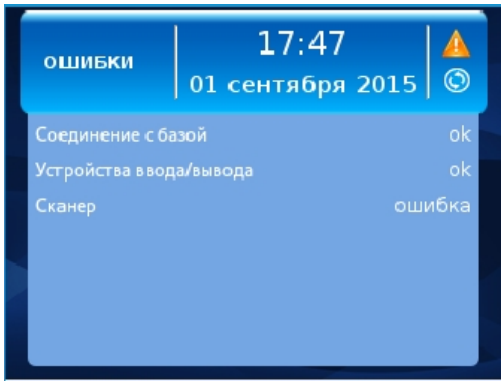
При проведении технического обслуживания нужно учитывать, что терминал находится под напряжением.

Не производите техническое обслуживание во взрывоопасных помещениях или иных местах, в которых возникновение разрядов статического электричества может стать источником возгорания.

В таблице ниже приведены операции технического обслуживания при эксплуатации.

Название операции	Описание	Периодичность
Внешний осмотр, удаление грязи и пыли с наружных поверхностей	• Проверьте целостность корпуса, отсутствие повреждений, через которые внутрь корпуса может попасть жидкость, пыль, насекомые. • Проверьте отсутствие повреждений (царапин, сколов) биометрического сканера. • Протрите наружную поверхность терминала сухой мягкой тканью. Для дезинфекции можно использовать ткань, смоченную в 70% изопропиловом спирте, при условии, что спирт не будет попадать на разъёмы и внутрь корпуса. • Аккуратно удалите пыль и грязь с поверхности биометрического сканера.	Раз в месяц

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Название операции	Описание	Периодичность
Проверка наличия ошибок	• Проверьте наличие значка ошибки  в работе терминала. При отсутствии значка проверку можно прекратить • В меню терминала выберите раздел «Ошибки»  	Раз в месяц

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Название операции	Описание	Периодичность
Проверка работоспособности	• Проверьте работу RFID-считывателя, для этого приложите к считывателю RFID-карту совместимого формата и убедитесь, что код считан правильно. • Проверьте работу биометрического сканера, для этого выполните попытку идентификации по биометрии и убедитесь в том, что сотрудник идентифицирован правильно. • Если изделие управляет исполнительным устройством (например, электрозамком, турникетом), то инициировать выдачу команды управления на исполнительное устройство (нажать кнопку, выполнить идентификацию.	Раз в год

При хранении терминала в пользовательской упаковке выполнение операций по техническому обслуживанию в течение назначенного срока хранения не требуется. При хранении терминала не в пользовательской упаковке следует выполнять операции, перечисленные в таблице ниже.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Название операции	Описание	Периодичность
Осмотр изделия, удаление пыли.	• Вскройте упаковку (при наличии). • Проверьте целостность корпуса, отсутствие повреждений, через которые внутрь корпуса может попасть жидкость, пыль, насекомые. Убедитесь в отсутствии пыли, грязи, следов жидкостей или насекомых на наружных поверхностях терминала. • При обнаружении пыли удалите её с помощью сухой мягкой ткани или пылесоса с узким соплом. • Если при осмотре терминала выявлена сильная запыленность, то следует принять меры для выяснения причин запылённости. Возможно, понадобится сменить место хранения терминала, обеспечить дополнительную герметизацию упаковки. • Если при осмотре терминала выявлено наличие грязи, следов жидкости или насекомых, то следует по возможности удалить грязь и следы насекомых и принять меры для защиты от дальнейшего попадания грязи, жидкости и насекомых внутрь упаковки. • Если при осмотре терминала обнаружены следы конденсации влаги, то следует принять меры для выяснения причин образования конденсата. Возможно, потребуется изменение условий хранения и замена силикагеля. • Поместите терминал в упаковку (при наличии).	Раз в год

SEC.RU | Короткий путь к информации
Скачано с sec.ru

11 ХРАНЕНИЕ, ТРАНСПОРТИРОВАНИЕ И УТИЛИЗАЦИЯ ТЕРМИНАЛА BIOSMART PV-WTC

Хранение и транспортирование терминала осуществляются в следующих условиях окружающей среды:

- Температура окружающего воздуха от минус 40 до плюс 50 °С
- Относительная влажность воздуха (без конденсации) до 80%

Транспортировка упакованного терминала может осуществляться любым видом транспорта, кроме морского транспорта, в крытых транспортных средствах.
Для всех видов транспортирования упакованные терминалы должны быть закреплены таким образом, чтобы исключить их перемещение и соударение.
Не храните и не транспортируйте терминал при следующих условиях:

- в непосредственной близости от источников тепла и открытого огня;
- при воздействии атмосферных осадков, в средах с коррозионно-активными агентами, в условиях морского (соленого) тумана;
- в условиях воздействия биологических факторов, таких как, плесневелые грибы, насекомые, животные.

После пребывания терминала в условиях низкой температуры или повышенной влажности его необходимо достать из упаковки и выдержать в сухом помещении при температуре (20±5) °С не менее 30 минут перед включением.

Терминал не должен утилизироваться вместе с бытовыми отходами. По окончанию эксплуатации обратитесь в сертифицированный пункт сбора.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

12 ПРИЛОЖЕНИЕ 1 ПЕРЕМЕННЫЕ SNMP

В настройках мониторинга по SNMP необходимо установить следующие настройки:

- Adress - IP терминала PV-WTC;
- Port (161) - Оставить без изменений;
- Version (1) - Оставить без изменений;
- Community - «publick» заменить на «snmpall».

В таблице приведен список переменных, публикуемых терминалом BioSmart PV-WTC по протоколу SNMP.

№	Имя переменной	OID	Тип данных	Описание
1	pvwtc2Mode	.1.3.6.1.4.1.99992.1.1.0	INTEGER	Режим работы терминала. 0 - сетевой1 - локальный2 - серверный
2	pvwtc2WorkModel	.1.3.6.1.4.1.99992.1.2.0	INTEGER	Рабочая модель. Базовые значения:0 - "Ладонь или карта"1 - "Карта + ладонь"2 - "Ладонь или пин"3 - "Пин + ладонь"4 - "Кн. вх/вых + код группы + ладонь/карта" 5 - "Кн. вх/вых + ладонь или карта"6 - "Ладонь или карта или кнопка"7 - "Кн. вх/вых + обед + ладонь или карта"8 - "Карта + ладонь или кнопка"9 - "Вход по кнопкам + ладонь или карта"10 - "Выход по кнопкам + ладонь или карта"11 - "Помещение для хранения ценностей"
3	pvwtc2Language	.1.3.6.1.4.1.99992.1.3.0	INTEGER	Язык интерфейса. Базовые значения: 0 - русский1 - английский
4	pvwtc2IpAddress	.1.3.6.1.4.1.99992.1.4.0	IpAddress	IP-адрес терминала.
5	pvwtc2Port	.1.3.6.1.4.1.99992.1.5.0	INTEGER	TCP-порт, по которому происходит соединение с BioSmart Studio. Значение по умолчанию: 20002

SEC.RU | Короткий путь к информации
Скачано с sec.ru

№	Имя переменной	OID	Тип данных	Описание
6	pvwtc2IpMask	.1.3.6.1.4.1.99992.1.6.0	IpAddress	Маска подсети IP.
7	pvwtc2IpGate	.1.3.6.1.4.1.99992.1.7.0	IpAddress	Адрес IP-шлюза.
8	pvwtc2MACAddr	.1.3.6.1.4.1.99992.1.8.0	DisplayString	MAC-адрес сетевого интерфейса терминала.
9	pvwtc2Timezone	.1.3.6.1.4.1.99992.1.9.0	DisplayString	Код часового пояса, установленного на терминале.
10	pvwtc2IsAlive	.1.3.6.1.4.1.99992.1.10.0	INTEGER	Индикация работы сервиса BioSmart. 0 - сервис не работает1 - сервис работает
11	pvwtc2StudioConnected	.1.3.6.1.4.1.99992.1.11.0	INTEGER	Индикация наличия соединения с BioSmart Studio.0 - подключения нет1 - подключение есть
12	pvwtc2KeypadLock	.1.3.6.1.4.1.99992.1.12.0	INTEGER	Индикация блокировки клавиатуры терминала.0 - блокировки нет.1 - блокировка есть.
13	pvwtc2PVSHwVer	.1.3.6.1.4.1.99992.1.13.0	INTEGER	Версия сканера вен.
14	pvwtc2SwVer	.1.3.6.1.4.1.99992.1.14.0	DisplayString	Версия прошивки терминала.
15	pvwtc2PVSSwVer	.1.3.6.1.4.1.99992.1.15.0	DisplayString	Версия прошивки сканера вен.
16	pvwtc2CopSwVer	.1.3.6.1.4.1.99992.1.16.0	DisplayString	Версия прошивки сопроцессора (если сопроцессор есть в терминале).
17	pvwtc2SerialNum	.1.3.6.1.4.1.99992.1.17.0	DisplayString	Серийный номер терминала.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

№	Имя переменной	OID	Тип данных	Описание
18	pvwtc2HwErrors	.1.3.6.1.4.1.99992.1.18.0	INTEGER	Наличие аппаратных ошибок. 0 - аппаратных ошибок не зарегистрировано.1 - есть аппаратные ошибки.
19	pvwtc2EmployeeCnt	.1.3.6.1.4.1.99992.1.19.0	Integer32	Количество сотрудников в памяти терминала.
20	pvwtc2TemplateCnt	.1.3.6.1.4.1.99992.1.20.0	Integer32	Количество шаблонов в памяти терминала.
21	pvwtc2SuccessIdentCnt	.1.3.6.1.4.1.99992.1.21.0	Integer32	Количество событий удачной идентификации за последние сутки.
22	pvwtc2FailIdentCnt	.1.3.6.1.4.1.99992.1.22.0	Integer32	Количество событий неудачной идентификации за последние сутки.
23	pvwtc2LeftTemplCnt	.1.3.6.1.4.1.99992.1.23.0	Integer32	Количество шаблонов левой руки в памяти терминала.
24	pvwtc2RightTemplCnt	.1.3.6.1.4.1.99992.1.24.0	Integer32	Количество шаблонов правой руки в памяти терминала.
25	pvwtc2IdentSrvConnected	.1.3.6.1.4.1.99992.1.25.0	INTEGER	Индикация соединения с сервером идентификации (только в серверном режиме).0 - нет соединения.1 - есть соединение.
26	pvwtc2LogCnt	.1.3.6.1.4.1.99992.1.26.0	Integer32	Количество событий в памяти терминала.
27	pvwtc2RoleCnt	.1.3.6.1.4.1.99992.1.27.0	Integer32	Количество ролей на терминале
28	pvwtc2AdminCnt	.1.3.6.1.4.1.99992.1.28.0	Integer32	Количество админов на терминале

SEC.RU | Короткий путь к информации
Скачано с sec.ru

13 ПРИЛОЖЕНИЕ 2 СПИСОК СООБЩЕНИЙ В РАЗДЕЛАХ МОНИТОРИНГ И ЖУРНАЛ В ПО BIOSMART-STUDIO V6

В зависимости от указанного лога, каждое событие в рабочей модели может быть отражено соответствующим сообщением в разделах **Мониторинг** и **Журнал** ПО Biosmart-Studio v6.

AlcoTestSuccess	Тест на алкоголь пройден успешно
AlcoTestFailed	Тест на алкоголь не пройден
AlcoTestHwError	Ошибка проверки на алкоголь
IdentPalmEnter	Вход сотрудника
IdentPalmLeave	Выход сотрудника
IdentPalmSuccess	Идентификация сотрудника успешна (по ладони)
IdentPalmFail	Идентификация сотрудника неудачна (по ладони)
IdentPalmDinnerLeave	Выход на обед
IdentPalmDinnerEnter	Вход с обеда
IdentCardEnter	Вход сотрудника (по карте)
IdentCardLeave	Выход сотрудника (по карте)
IdentCardSuccess	Идентификация сотрудника успешна (по карте)
IdentCardFail	Идентификация сотрудника неудачна (по карте)
IdentCardDinnerLeave	Выход на обед (по карте)
IdentCardDinnerEnter	Вход с обеда (по карте)
IdentPinEnter	Вход сотрудника (по пин-коду)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

IdentPinLeave	Выход сотрудника (по пин-коду)
IdentPinSuccess	Идентификация сотрудника успешна (по коду)
IdentPinFail	Идентификация сотрудника неудачна (по коду)
IdentPinDinnerLeave	Выход на обед (по пин-коду)
IdentPinDinnerEnter	Вход с обеда (по пин-коду)
IdentBlockStudio	Отказ идентификации - сотрудник заблокирован
IdentBlockAntiPassBack	Отказ доступа (anti-passback)
IdentBlockHoliday	Отказ идентификации - сотрудник заблокирован праздником
IdentBlockShedule	Отказ идентификации - сотрудник заблокирован временным режимом
IdentTimeout	Превышено время операции
IdentUnknownError	Неизвестная ошибка идентификации
DeviceInitialization	Инициализация контроллера
DeviceRestart	Перезапуск системы
LogSaveError	Ошибка сохранения журнала событий
EmployeeAddOK	Добавление сотрудника успешно
EmployeeAddError	Добавление сотрудника неудачно
EmployeeUpdateError	Изменение доступа у сотрудника неудачно
EmployeeUpdateOK	Изменение доступа у сотрудника успешно
EmployeeDeleteOk	Удаление сотрудника успешно

SEC.RU | Короткий путь к информации
Скачано с sec.ru

EmployeeDeleteError	Удаление сотрудника неудачно
EmployeeBlockOK	Блокировка сотрудника успешна
EmployeeBlockError	Блокировка сотрудника неудачна
EmployeeUnblockOK	Разблокировка сотрудника успешна
EmployeeUnblockError	Разблокировка сотрудника неудачна
HardwareUnknownError	Неизвестная ошибка оборудования
HardwareErrorScaner	Ошибка сканера
HardwareErrorCoproc	Ошибка процессора
LeaveButton	Открытие по кнопке (N1)
NotPass	Идентификация успешна. Проход не выполнен.
TryCrackByPalm	Ошибка чтения ладони
DoorOpened	Дверь открыта
DoorOpenedWhenBlocked	Дверь открыта без разблокирования
DoorOpenedWhenGuard	Дверь открыта без снятия с охраны
DoorClose	Дверь закрыта
DoorNotClosedInTime	Дверь не была закрыта
GuardOn	Постановка помещения на охрану (инициатор BioSmart)
GuardOff	Снятие помещения с охраны (инициатор BioSmart)
DoorOpenedUnexpectedly	Внештатное открытие двери

SEC.RU | Короткий путь к информации
Скачано с sec.ru

GuardOpenedUnexpectedly	Внештатное снятие с охраны
SendWiegandA	Отправлен код по первому разделу охраны
SendWiegandB	Отправлен код по второму разделу охраны
NotApprovedInTime	Не было подтверждающего действия
GuardOffTomerComplete	Завершено ожидание снятия с охраны
DuressPass	Проход под принуждением
WrongMultiAccessType	Идентификация сотрудника из неразрешённой группы
LeaveBottonWhenOnGuard	Нажатие кнопки разблокировки при охране
ShadowTemplate	Добавлен теневой шаблон
AdminAccessGranted	Доступ к меню контроллера разрешён
AdminAccessRejected	Доступ к меню контроллера запрещён
AdminUserAdded	Добавлен пользователь контроллера
RoleAdded	Добавлена роль пользователь контроллера
AdminUserAddErr	Ошибка добавления пользователя контроллера
RoleAddErr	Ошибка добавления роли пользователя контроллера
ServerIdentSuccess	Идентификация сотрудника успешна
ServerIdentFail	Идентификация сотрудника неудачна
MobieEmployeeEnter	Вход мобильного сотрудника
MobileEmployeeExit	Выход мобильного сотрудника

SEC.RU | Короткий путь к информации
Скачано с sec.ru

MobileEmployeeSuccess	Идентификация мобильного сотрудника
TamperDeviceOpened	Вскрыт корпус
TamperOffTheWall	Отрыв от стены
TamperDeviceClosed	Закрыт корпус
TamperOnTheWall	Прикреплён к стене
FirmwareUpdateStart	Обновление ПО контроллера началось
FirmwareUpdateSuccess	Обновление ПО контроллера успешно завершено
Scannet FirmwareUpdateSuccess	Обновление ПО сканера успешно завершено
Coprocessor FirmwareUpdateSuccess	Обновление ПО сопроцессора успешно завершено
MigrationFails	Ошибка обновления структуры БД контроллера
TestStartFails	Ошибка запуска ПО контроллера
VersionTestFails	Недопустимая версия ПО контроллера
ServerIdentIsNotResponding	Сервер не отвечает
ServerIdentIsConnected	Соединение с сервером идентификации установлено
ServerIdentIsCommectionLost	Соединение с сервером идентификации потеряно
ServiceDbFinished	Произведено обслуживание БД контроллера
TemperatureTooHigh	Превышена допустимая температура сотрудника
TemperatureTooLow	Слишком низкая температура сотрудника

SEC.RU | Короткий путь к информации
Скачано с sec.ru

TemperatureHwFail	Ошибка работы с датчиком температуры

SEC.RU | Короткий путь к информации
Скачано с sec.ru