Терминал BioSmart Quasar 7

Руководство по эксплуатации

Версия документа HW.063.M.7
Дата 06.2026

СОДЕРЖАНИЕ

В настоящем руководстве по эксплуатации содержатся основные сведения о терминале BioSmart Quasar 7, порядок монтажа, подключения и настройки.

Так выделена информация, на которую следует обратить особое внимание.

1 ОПИСАНИЕ ТЕРМИНАЛА BIOSMART QUASAR 7

1.1 Общие сведения

Терминал **BioSmart Quasar 7** предназначен для организации контроля и управления доступом, а также учёта рабочего времени посредством идентификации пользователей по:

- лицу (*соответствует требованиям 572-ФЗ*);
- RFID-картам;
- смартфону с NFC;
- рисунку вен ладони (опционально может быть встроен сканер рисунка вен ладони).

> Терминал соответствует требованиям федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных».

Терминал выпускаются в следующих исполнениях:

- BioSmart Quasar 7-MFR;
- BioSmart Quasar 7 PV-MFR;
- BioSmart Quasar 7-MFR-T;
- BioSmart Quasar 7 PV-MFR-T.

Терминал **BioSmart Quasar 7-MFR, BioSmart Quasar 7-MFR-T** идентифицирует по лицу, RFID-картам и/или смартфону. **BioSmart Quasar 7 PV-MFR,BioSmart Quasar 7 PV-MFR-T** идентифицирует по лицу и венам ладони, RFID-картам и/или смартфону.

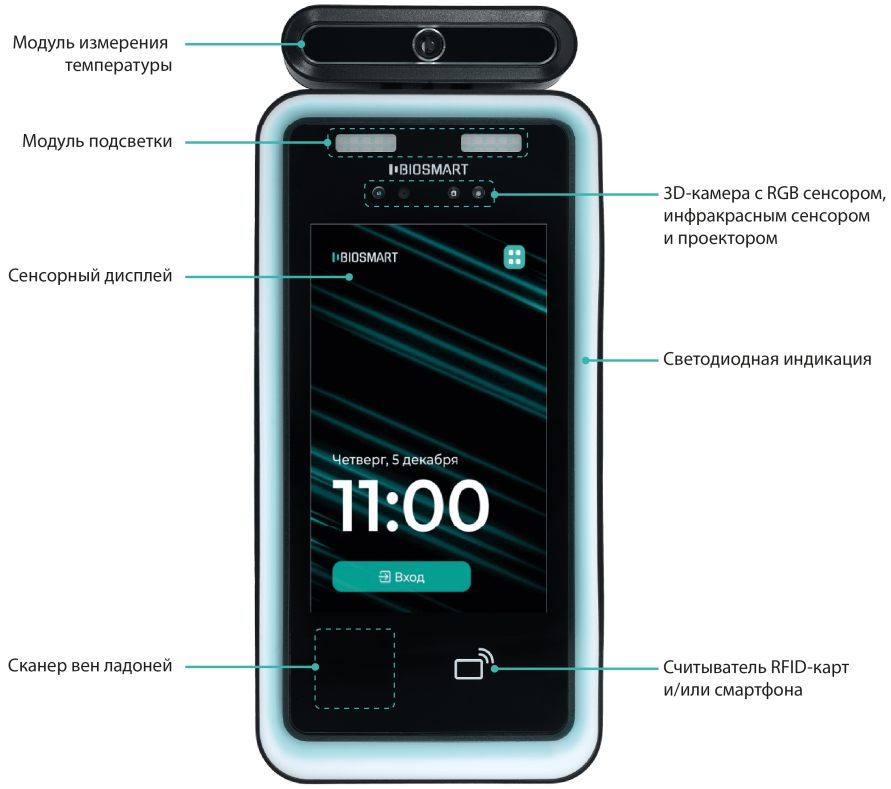
Исполнения **BioSmart Quasar 7-MFR-T**, **BioSmart Quasar 7 PV-MFR-T** выпускаются со встроенным бесконтактным датчиком для измерения температуры лица.

1.2 Состав и внешний вид

В зависимости от исполнения состав терминала может отличаться. Терминал BioSmart Quasar 7 состоит из следующих основных модулей:

- плата терминала;
- 3D-камера с RGB сенсором, инфракрасным сенсором и проектором;
- модуль подсветки;
- светодиодная индикация;
- считыватель RFID-карт и смартфона;
- сканер вен ладоней (только для BioSmart Quasar 7 PV-MFR, BioSmart Quasar 7 PV-MFR-T);
- дисплей;
- динамик;
- пластиковый корпус с радиатором охлаждения;
- датчик измерения температуры лица (только для BioSmart Quasar 7 PV-MFR-T, BioSmart Quasar 7-MFR-T).

На изображении ниже указаны основные элементы для исполнения **BioSmart Quasar 7 PV-MFR-T.**



1.3 Формат поддерживаемых карт

Терминал поддерживает работу с идентификаторами, приведёнными в таблице ниже.

Идентификатор	BioSmart Quasar 7
EM-Marine	✓
MIFARE Classic	✓
MIFARE ID	✓
MIFARE Ultralight	✓
MIFARE Ultralight C	✓
MIFARE Ultralight EV1	✓
MIFARE Plus SE	✓
MIFARE Plus X	✓
MIFARE Plus EV1	✓

Идентификатор	BioSmart Quasar 7
MIFARE DESFire EV1	✓
MIFARE Plus SL1	✓
MIFARE Plus SL3	✓
Смартфоны	
По технологии NFC*	✓
* Для идентификации используется смартфон с установленным приложением BioSmart ID по протоколу NFC.	

1.4 Технические характеристики

Параметр	Значение			
	BioSmart Quasar 7-MFR	BioSmart Quasar 7 PV-MFR	BioSmart Quasar 7-MFR-T	BioSmart Quasar 7 PV-MFR-T
Биометрический идентификатор	Лицо	Лицо, рисунок вен ладони	Лицо	Лицо, рисунок вен ладони
Наличие встроенного датчика температуры	Нет		Да	
Точность измерения температуры	-		± 0,5 °C	
Наличие встроенного считывателя RFID-карт	Да			
Наличие датчика вскрытия задней крышки	Да			
Наличие защиты от попыток фальсификации биометрических данных лица (антиспуфинг)	Да			
Максимальное количество пользователей при работе в режиме идентификации (1:N)	25 000			

Параметр	Значение
Максимальное количество пользователей при работе в режиме верификации (1:1)	100 000
Максимальное количество шаблонов лица	1 000 000
Максимальное количество событий, хранимых на терминале	100 000
Вероятность ошибочного предоставления доступа по биометрическим данным, FAR*	10^{-6} – 10^{-8}
Модуль камер	3D-камера с RGB сенсором 5 Mpx, Ir сенсором 1 Mpx и с инфракрасным проектором
Процессор	Rockchip RK3399
GPU	Mali-T864 GPU
Память	4GB RAM, 16GB Flash
Интерфейс взаимодействия с управляющим компьютером	Ethernet (100BASE-TX / 10BASE-Te IEEE 802.3), Wi-Fi IEEE 802.11
Интерфейс связи со сторонними устройствами	USB 2.0, RS-485, Wiegand (двунаправленный)
Поддерживаемые форматы Wiegand	Wiegand-26/32/34/37/40/42/48/64
Количество интерфейсов Wiegand (направление In/Out задаётся программно)	1
Количество дискретных входов	2
Максимальное напряжение, подаваемое на дискретный вход, В	12
Количество встроенных реле	1
Электрические параметры реле	DC 30 В 2 А

Параметр	Значение	
Состояние контактов реле	Нормально разомкнутые и нормально замкнутые	
Дисплей	Сенсорный ёмкостный, 7”	
Наличие адаптивной подсветки	Да	
Встроенный полифонический динамик	Да	
Параметры электропитания	DC 12 В 2 А	
Поддержка PoE	IEEE 802.3at class 4, потребляемая мощность 25 Вт	
Материал корпуса	Пластик, металл	
Габаритные размеры, мм	280 x 140 x 40	318 x 140 x 40
Масса нетто, кг	1,5	1,8
Температура воздуха при эксплуатации	От -10 °C до +50 °C	От +15 °C до +35 °C
Степень защиты корпуса	IP54	IP20

* Значение FAR получено расчётным методом. Зависит от настроек терминала, условий идентификации и качества шаблонов биометрических данных.

Вероятность ошибочного отказа в доступе (FRR) при идентификации по лицу не более 1,1% (при FAR = $5*10^{-8}$). Результаты соответствуют базе данных LFW (лица в разных ракурсах, 13233 изображений, 5749 человек).

Вероятность ошибочного отказа в доступе (FRR) при идентификации по венам ладони не более 1,3% (при FAR = 10^{-8}). Результаты соответствуют базе данных 10 000 человек.

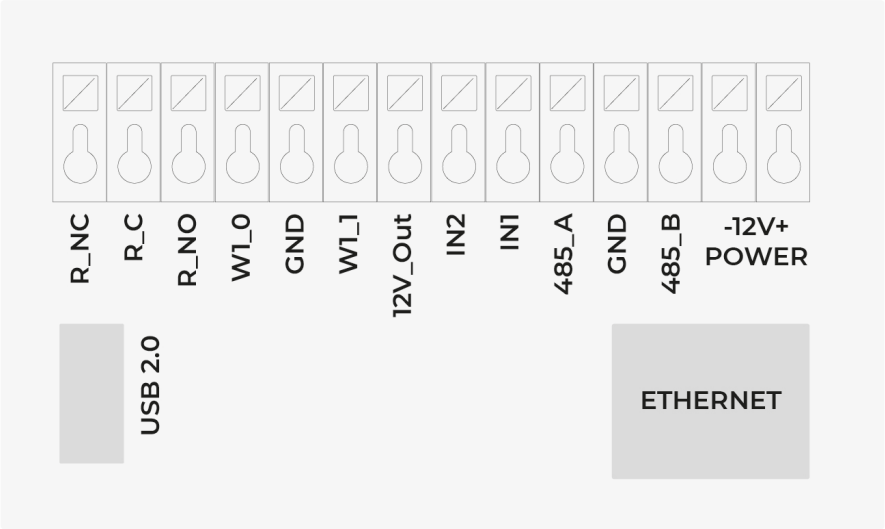
1.5 Описание работы терминала

Терминал **BioSmart Quasar 7** по умолчанию работает в энергосберегающем режиме, активируясь только при обнаружении лица в зоне действия 3D-камеры. Далее запускается последовательная проверка найденного лица: проверяется качество изображения лица, а по 3D-облаку точек проверяется объёмность объекта. При успешном прохождении проверок терминал создает биометрический шаблон. Считанные биометрические данные сравниваются с биометрическими шаблонами лиц, хранящимися в базе данных терминала.
Если совпадение найдено, то адаптивная светодиодная подсветка по периметру корпуса загорается зеленым цветом, тем самым даёт сигнал об успешной идентификации и предоставляет доступ сотруднику. В случае несовпадения шаблонов – светодиодный индикатор загорится красным светом и доступ сотруднику будет запрещён. Параллельно подсветке встроенный полифонический динамик воспроизводит аудио-уведомление в

соответствии с результатом идентификации. Далее информация об успешной/неуспешной идентификации отправляется на сервер Biosmart и выводится на дисплей терминала.
Данный принцип работы применяется в тех случаях, когда терминал не используется для работы с ЕБС, КБС и Региональным сегментом. Порядок подключения и настройки работы с биометрическими системами приведён в инструкции Интеграция BioSmart с биометрическими системами.

1.6 Описание платы терминала

Разъёмы, используемые для подключения, расположены на задней стороне терминала под съёмной пластиковой крышкой. Описание разъемов приведено в таблице ниже.



Обозначение контакта	Описание	Назначение
USB 2.0	Разъем USB	Подключение сторонних устройств.
Ethernet	Разъем Ethernet	Подключение к сети Ethernet, подключение источника PoE IEEE 802.3at class 4 (25 Вт).
R_NC	Нормально замкнутый контакт	Подключение исполнительного устройства.
R_C	Общий контакт	
R_NO	Нормально разомкнутый контакт	
W1_0	Вход Wiegand DATA0	Подключение к стороннему устройству по интерфейсу Wiegand. Направление (IN/OUT) задается программно.
GND	Wiegand общий	
W1_1	Вход Wiegand DATA1	

Обозначение контакта	Описание	Назначение
12V_Out	Напряжение 12 В (не более 100 мА)	Электропитание стороннего маломощного устройства или подключение кнопки, датчика.
IN1	Дискретный вход. Напряжение, подаваемое на дискретный вход от 5 до 12 В. Логическая «1» при напряжении более 4 В. Логический «0» при напряжении менее 1 В.	Подключение кнопки/датчика прохода.
IN2		
485_A	Канал А	Подключение к стороннему контроллеру по интерфейсу RS-485 (OSDP).
GND	RS-485 общий	
485_B	Канал В	
+12V	Питание DC 12 В 2 А	Подключение к положительному полюсу источника питания 12 В.
-12V	Питание, общий провод	Подключение к отрицательному полюсу источника питания 12 В.

2 ЭКСПЛУАТАЦИОННЫЕ ОГРАНИЧЕНИЯ ТЕРМИНАЛА

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

2.1 Механические факторы

- Не устанавливайте устройство вблизи источников вибраций и ударных воздействий. Устройство может устанавливаться в местах с незначительным уровнем ударных воздействий, например, рядом с часто захлопывающимся дверями.
- Избегайте механических воздействий, которые могут привести к повреждению корпуса устройства и попаданию внутрь жидкости, пыли, посторонних предметов.
- Не используйте абразивные или химически активные материалы для очистки наружных поверхностей устройства.
- Избегайте механических воздействий, которые могут привести к повреждению стекла на лицевой панели устройства.

2.2 Климатические факторы

- Терминалы **BioSmart Quasar 7-MFR**, **BioSmart Quasar 7 PV-MFR** допускается эксплуатировать в условиях, соответствующих степени защиты корпуса IP54 и температуре окружающего воздуха от – 10°С до+ 50°С.
- Терминалы **BioSmart Quasar 7-MFR-T**, **BioSmart Quasar 7 PV-MFR-T** допускается эксплуатировать в условиях, соответствующих степени защиты корпуса IP20 и температуре окружающего воздуха от + 15°С до+ 35°С.
- **Не используйте терминал под прямыми солнечными лучами или в непосредственной близости от ярких источников света во избежание перегрева или ухудшения качества сканирования биометрических данных (вследствие оптической помехи).**
- Задняя стенка терминала выполнена из металла и служит для отвода тепла. Не закрывайте ее и оставляйте зазор для свободной циркуляции воздуха, чтобы не допустить перегрева.
- Не используйте устройство в непосредственной близости от источников пламени.
- Не рекомендуется эксплуатировать терминалы при наличии механических повреждений.

2.3 Биологические факторы

- Не используйте устройство в условиях воздействия плесени, насекомых, животных.

2.4 Электромагнитные поля и электрический ток

- Используйте устройство только при напряжении питания, указанном в технических характеристиках.
- Не используйте устройство вблизи источников сильных электромагнитных полей, которые могут привести к выходу из строя или ухудшению работы электронных компонентов.

2.5 Дополнительные ограничения

- При эксплуатации изделия должна обеспечиваться молниезащита линий связи и электропитания.

- Не используйте устройство во взрывоопасных помещениях или иных местах, в которых возникновение разрядов статического электричества или искр может стать источником возгорания.
- Не допускается вмешательство в конструкцию неквалифицированных и не уполномоченных производителем лиц.
- Для минимизации погрешности измерения температуры при использовании терминалов **BioSmart Quasar 7-MFR-T, BioSmart Quasar 7 PV-MFR-T** исключите воздействие на считыватель потоков холодного воздуха (например, из улицы или кондиционера) или потоков горячего воздуха, а также влияние разного рода обогревателей и горячих приборов.

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

3 МОНТАЖ ТЕРМИНАЛА

Меры безопасности

Перед началом монтажа прочитайте правила ниже:

- не производите монтаж, пусконаладочные работы терминала при грозе, ввиду опасности поражения электрическим током от наводок на линии связи во время грозовых разрядов;
- 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;
- любое удлинение кабелей производите методом пайки либо обжима.

Не допускается производить удлинение кабелей методом скрутки!

3.1 Рекомендации по выбору кабелей

- 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.

В таблице приведены рекомендуемые максимальные длины линий связи и типы кабелей.

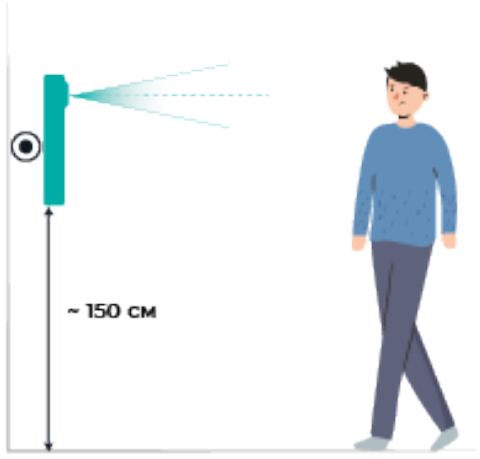
Кабельное соединение	Рекомендуемая максимальная длина*	Тип кабеля	Тип наконечника
Сетевое устройство – терминал (по интерфейсу Ethernet)	100 м	Четыре витые пары не ниже пятой категории	8P8C
Источник питания – терминал	8 м	Кабель ШВВП сечением 1 мм^2	НШВИ
Источник PoE IEEE 802.3at class 4 – терминал	100 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

Кабельное соединение	Рекомендуемая максимальная длина*	Тип кабеля	Тип наконечника
Терминал (дискретные входы) – внешние устройства (кнопки, датчики)	10 м	Сигнальные кабели сечением от 0,2 мм^2 (например, КСВВГ)	НШВИ
Терминал (дискретные выходы) – внешние устройства (нагрузка)	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.			

3.2 Рекомендации по установке и порядок монтажа терминала

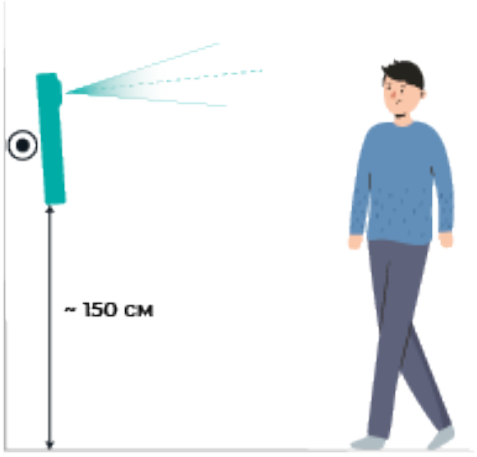
3.2.1 Рекомендации по установке

1. Для наилучшего качества идентификации устанавливайте терминал на высоте **150 см** от пола до нижней части терминала.

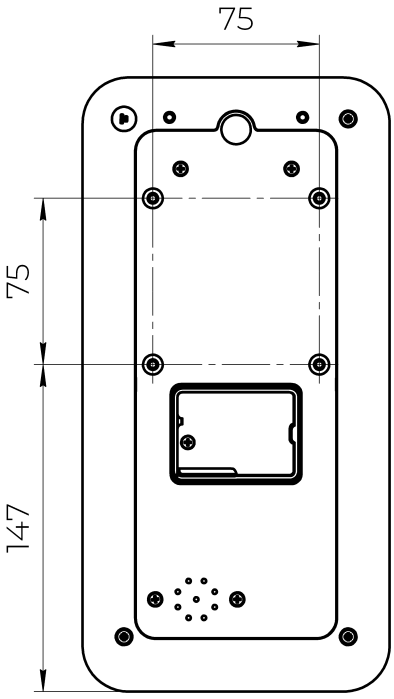


2. Исполнения со сканером вен (BioSmart Quasar 7 PV-MFR, BioSmart Quasar 7 PV-MFR-T) устанавливайте под наклоном, чтобы ладонь можно было прикладывать

параллельно сканеру.



3. Используйте наклонно-поворотные кронштейны для регулировки положения терминала в процессе эксплуатации для обеспечения наибольшего удобства и качества идентификации.
4. Для крепления терминала используйте кронштейны стандарта VESA **75 x 75 мм**. Расположение монтажных отверстий на терминале показано на рисунке ниже.

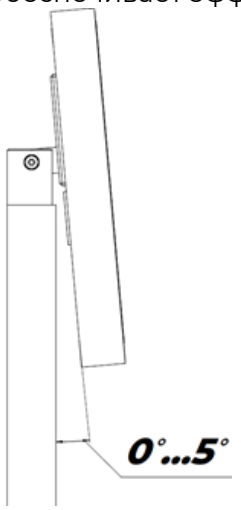


3.2.2 Правила монтажа на улице

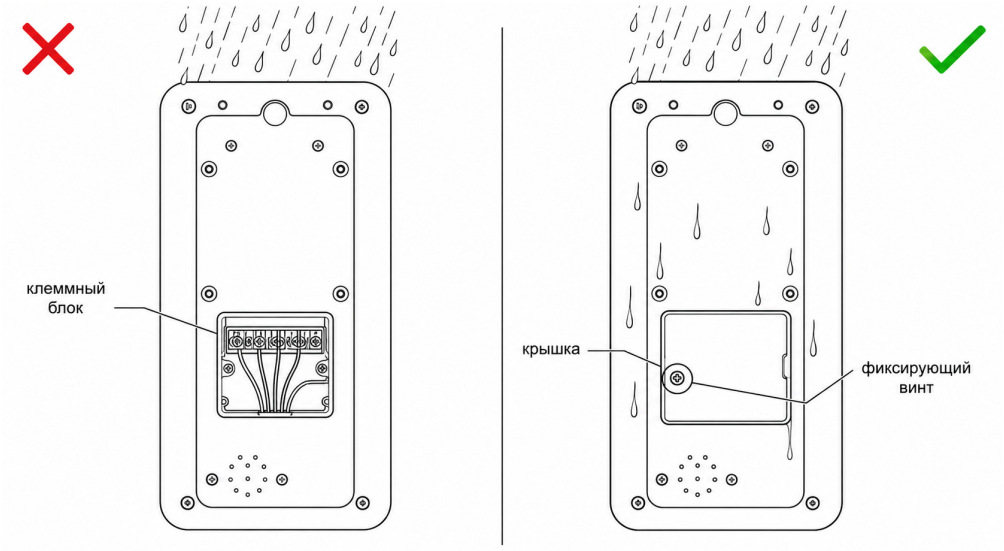
Если терминал устанавливается на улице или в других местах, где требуется защита от пыли и влаги, необходимо соблюдать следующие правила монтажа:

1. **Наклон корпуса терминала.**
   Устройство должно быть установлено вертикально или с положительным углом наклона относительно вертикальной плоскости. Такая ориентация предотвращает попадание и скопление осадков на контактных группах (клеммном блоке), а также

обеспечивает эффективный сток воды с рабочей поверхности.



2. **Герметизация клеммного блока**.
   После завершения монтажа крышка клеммного блока должна быть установлена на место и зафиксирована винтом, входящим в комплект поставки. Невыполнение требования ведёт к риску попадания влаги и пыли внутрь устройства.



3. **Защита кабеля Ethernet**.
   Перед началом монтажа убедитесь в целостности внешней оболочки всех кабелей, подключаемых к терминалу. Повреждённая изоляция кабеля недопустима.
   Место подключения обратного конца кабелей (Ethernet розетка, разъемы стороннего оборудования) должно располагаться в сухом, защищённом от воды месте. Это необходимо попадания влаги в терминал из-за капиллярного эффекта (затягивания влаги внутрь кабеля и затем внутрь терминала).
   В процессе эксплуатации регулярно контролируйте состояние внешней оболочки кабеля и при обнаружении повреждений изоляцию восстановите или замените кабель.
4. **Дополнительная защита от осадков**.
   По возможности размещайте терминал под козырьком, навесом или другим

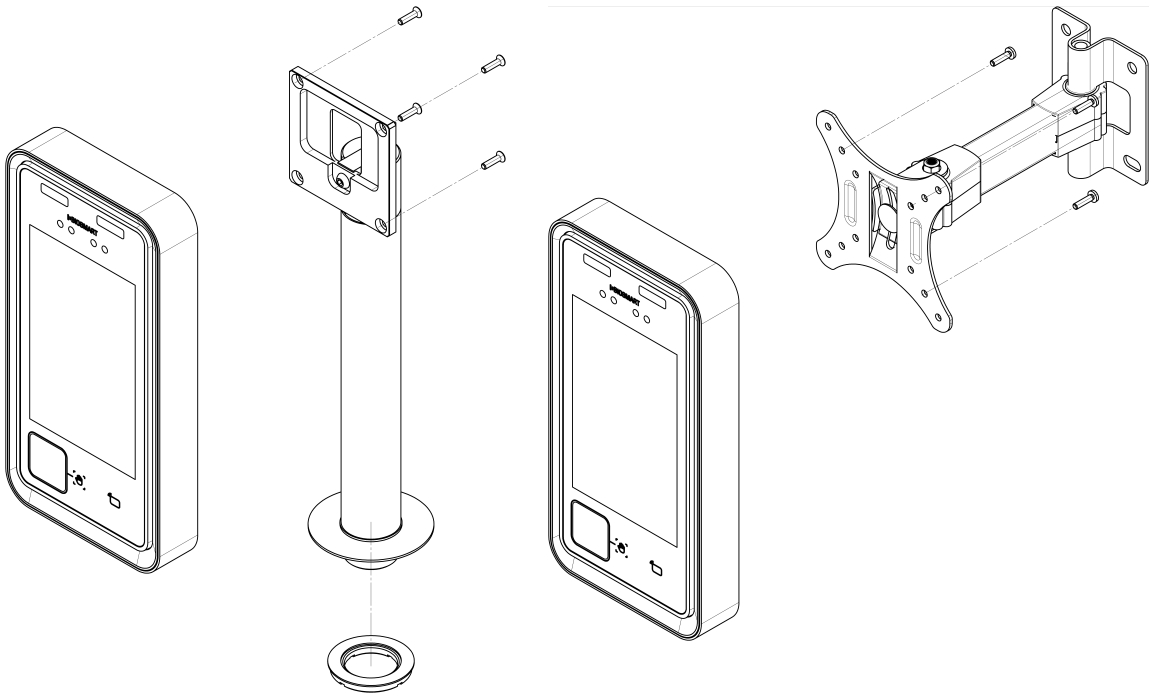
укрытием. Это снижает риск попадания влаги даже при сильном дожде или снегопаде.

3.2.3 Порядок монтажа

Монтаж терминала должен осуществляться при отключенном напряжении электропитания!

Выполните монтаж терминала на кронштейн:

1. Распакуйте коробку и проверьте комплектность терминала.
2. Выберите место для установки согласно разделам Эксплуатационные ограничения, Рекомендациями по установке и Правила монтажа улице.
3. Подведите кабели к месту установки терминала.
4. Закрепите терминал на кронштейне VESA 75×75 мм. Схема установки на кронштейн показана на схемах ниже.



5. Снимите пластиковую крышку, закрывающую разъемы терминала. Подключите кабели к терминалу согласно разделу Подключение терминала и верните крышку на место.

> При установке устройства на улице обязательно учитывайте требования, указанные в разделе Правила монтажа на улице.

6. После завершения монтажа снимите защитную плёнку с дисплея.

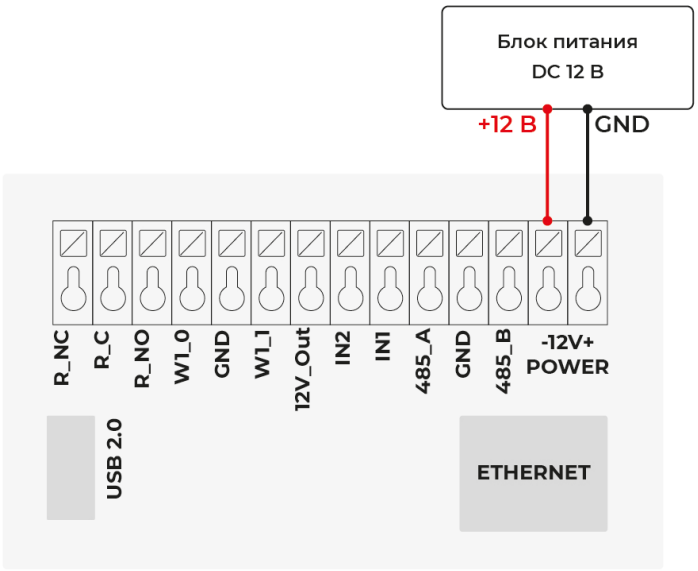
4 ПОДКЛЮЧЕНИЕ ТЕРМИНАЛА

4.1 Подключение питания

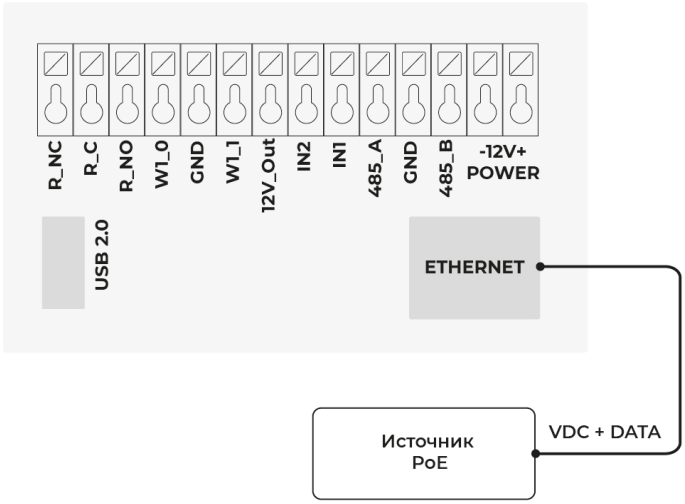
Электропитание терминала может осуществляться двумя способами:

- от источника питания с параметрами DC 12 В 2 А. Рекомендуется использовать источник питания с заземлением;
- от источника PoE IEEE 802.3at class 4 (25 Вт). Для подключения рекомендуется использовать кабель FTP не ниже пятой категории.

Подключение терминала к источнику питания 12 В осуществляется через разъем **"-12V+ POWER"**.

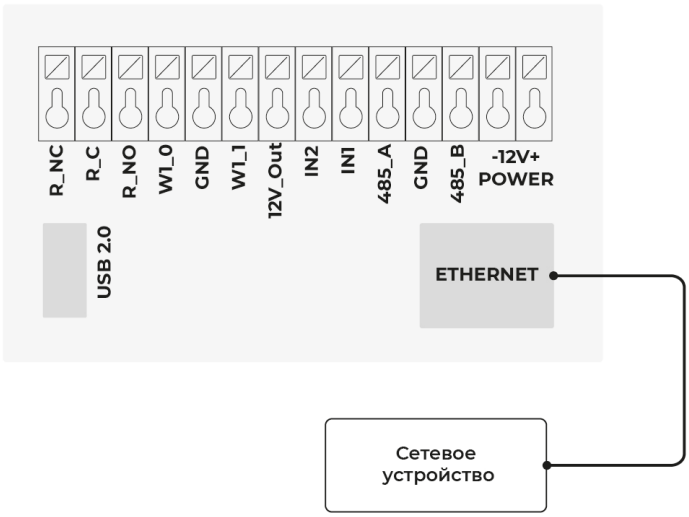


Подключение терминала к источнику PoE осуществляется через разъём **Ethernet**.



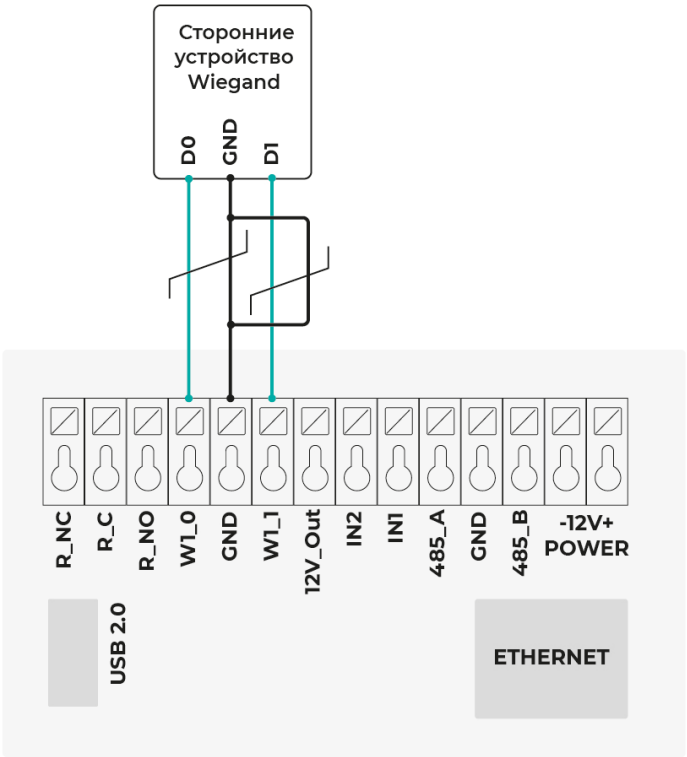
4.2 Подключение к сети Ethernet

Подключение терминала к сети Ethernet выполняется в соответствии со схемой ниже. Для подключения рекомендуется использовать кабель FTP не ниже пятой категории.



4.3 Подключение к терминалу устройств по Wiegand

Для подключения терминала к стороннему устройству по интерфейсу Wiegand используются разъемы **W1_0**, **W1_1**, **GND**.



Для повышения помехозащищенности рекомендуется выполнить попарное скручивание линий данных **Data0** и **Data1** с линией **GND**.

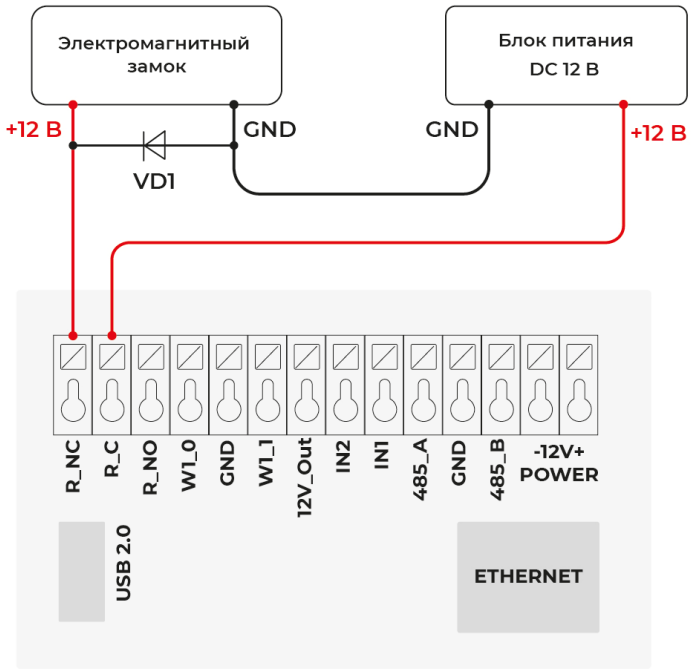
4.4 Подключение электрозамков

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

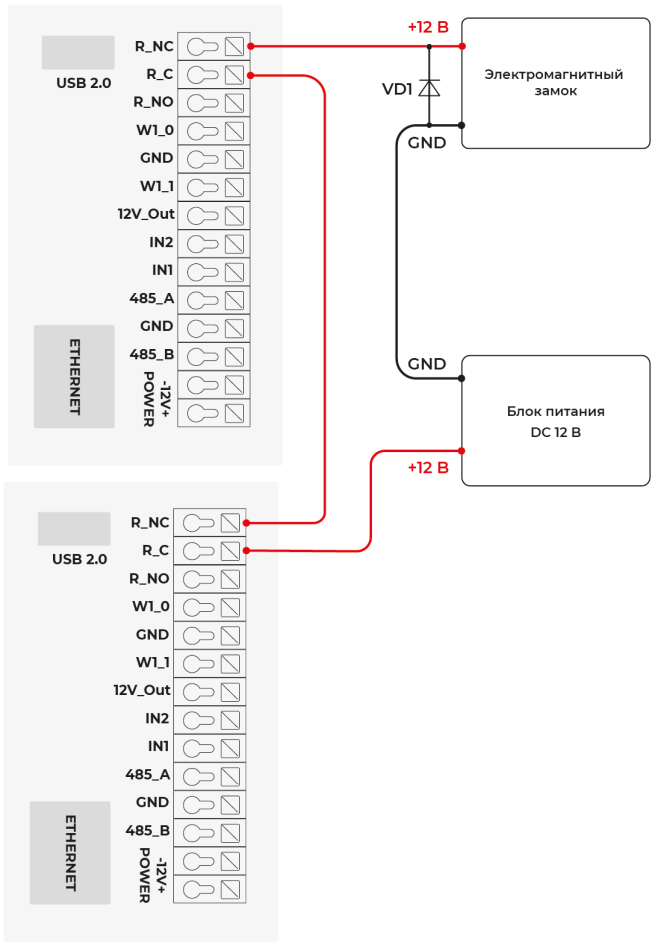
Для защиты встроенного реле от обратного тока, возникающего в цепи при срабатывании замка, необходимо установить шунтирующий диод VD1 в соответствии со схемами. Рекомендуется использовать диод типа 1N4007 (входит в комплект поставки) или аналогичный.

Подключение электромагнитного замка

Электромагнитный замок подключается к разъемам **R_C** и **R_NC** в соответствии со схемой ниже.

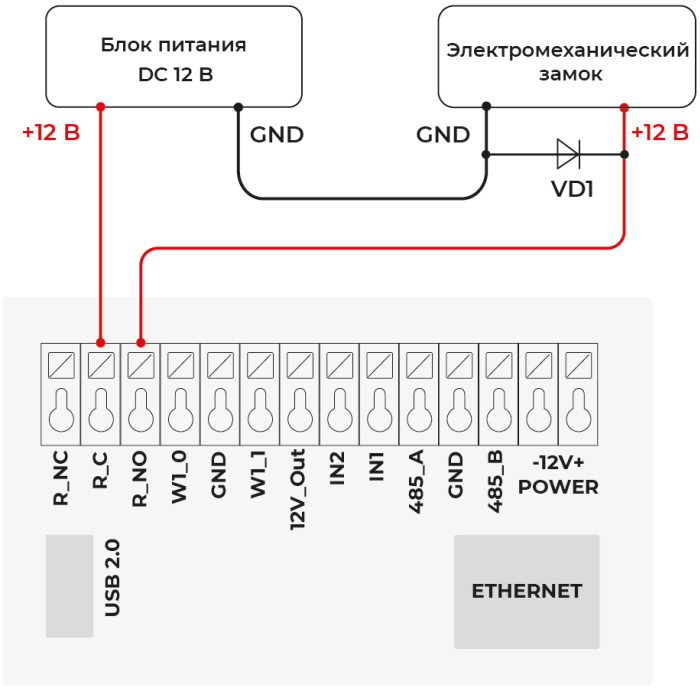


Подключение двух терминалов к одному электромагнитному замку осуществляется в соответствии со схемой ниже.

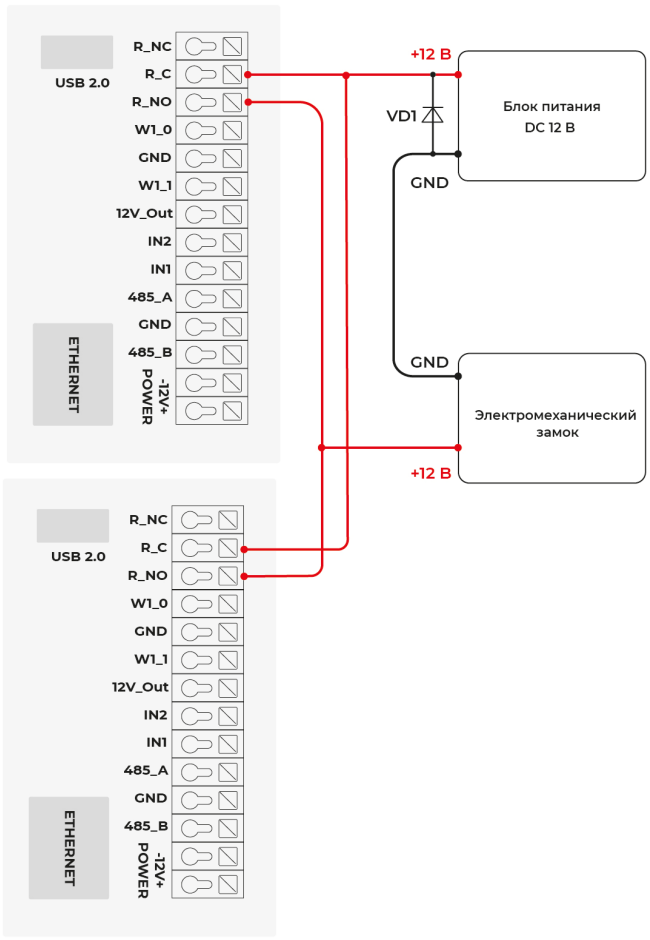


Подключение электромеханического замка

Электромеханический замок подключается к разъемам R_NO и R_C в соответствии со схемой ниже.

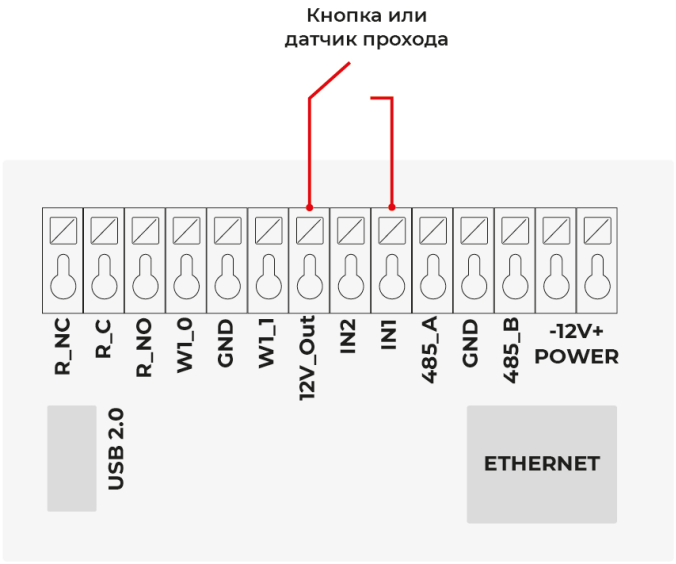


Подключение двух терминалов к одному электромеханическому замку осуществляется в соответствии со схемой ниже.



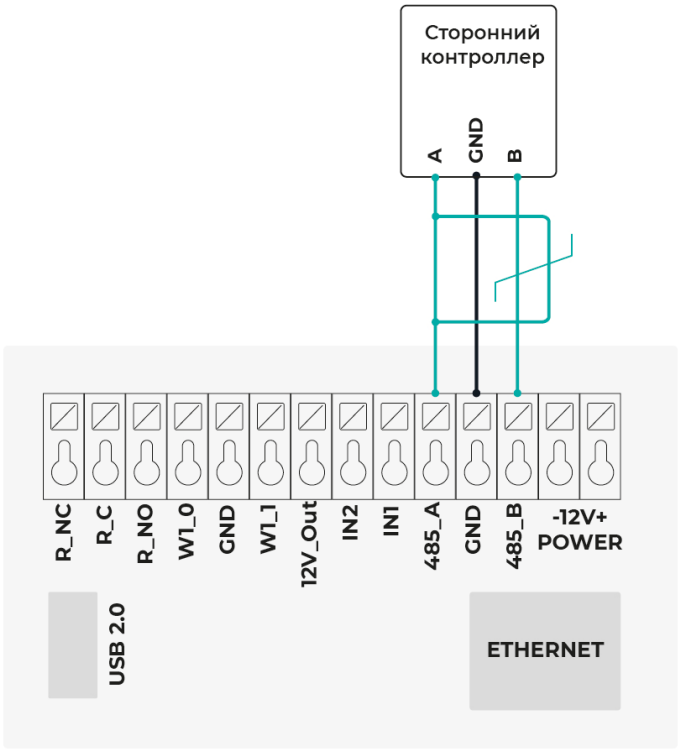
4.5 Подключение кнопок и датчиков

В терминале предусмотрена возможность опроса состояния кнопок и датчиков прохода. Кнопки и датчики прохода подключаются к разъемам **12V_Out** и **IN1** (**IN2**) в соответствии со схемой ниже.



4.6 Подключение терминала по интерфейсу RS-485

Терминал может работать с контролерами по интерфейсу RS-485 (OSDP) в режиме считывателя. Подключение осуществляется к разъемам A, B и GND в соответствии со схемой ниже.



5 БЫСТРЫЙ СТАРТ BIOSMART QUASAR 7

В разделе описан минимально необходимый перечень настроек, которые следует выполнить для начала работы с терминалом. Приступать к настройке терминала следует после его монтажа (см. раздел Монтаж) и подключения (см. раздел Подключение).

> ⓘ ПО BioSmart Quasar 7 версии **3.2.82** работает с ПО Biosmart-Studio версии не ниже **6.4.5**.

Выполните настройку в следующем порядке:

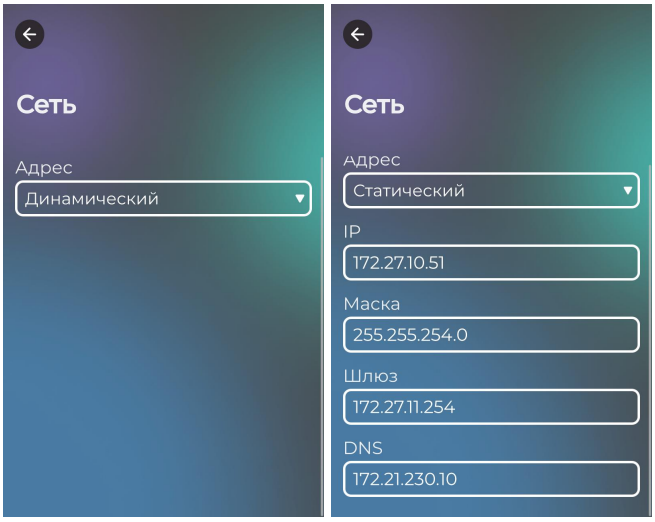
1. Настройте сетевые параметры терминала

На предприятии-изготовителе терминалу BioSmart назначается IP-адрес **172.25.110.71**.

Для начала работы с терминалом, установите сетевые настройки терминала в соответствии с настройками используемой сети.

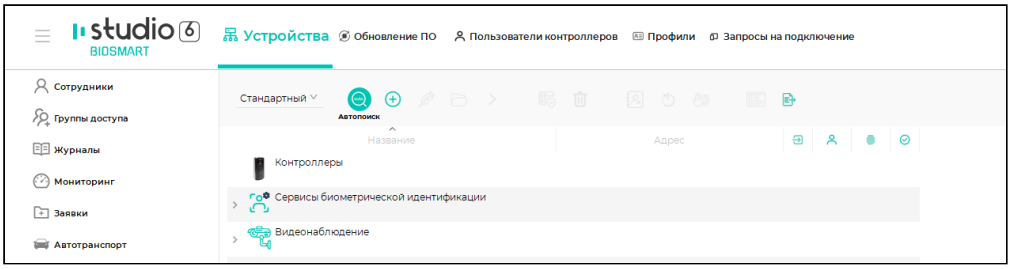
Для этого войдите в меню терминала, пароль по умолчанию **bioroot**.

Перейдите в раздел **Настройки** → **Сеть**. В поле **Адрес** выберете **Статический адрес**, укажите IP-адрес и остальные сетевые параметры.

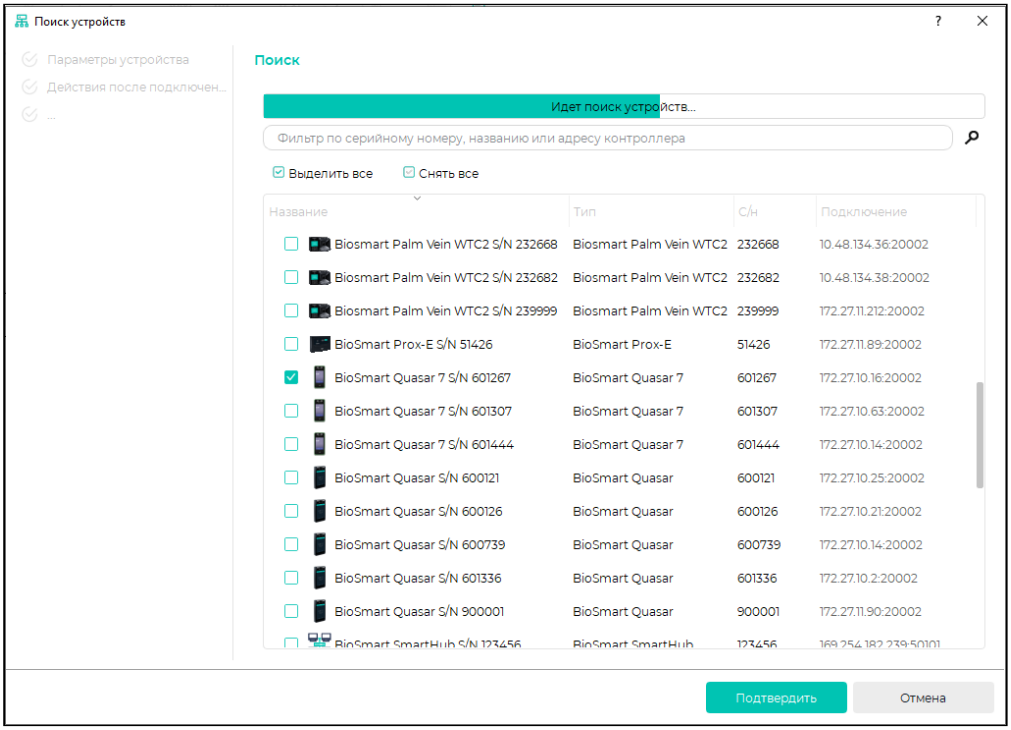


2. Добавьте терминал в ПО Biosmart-Studio v6

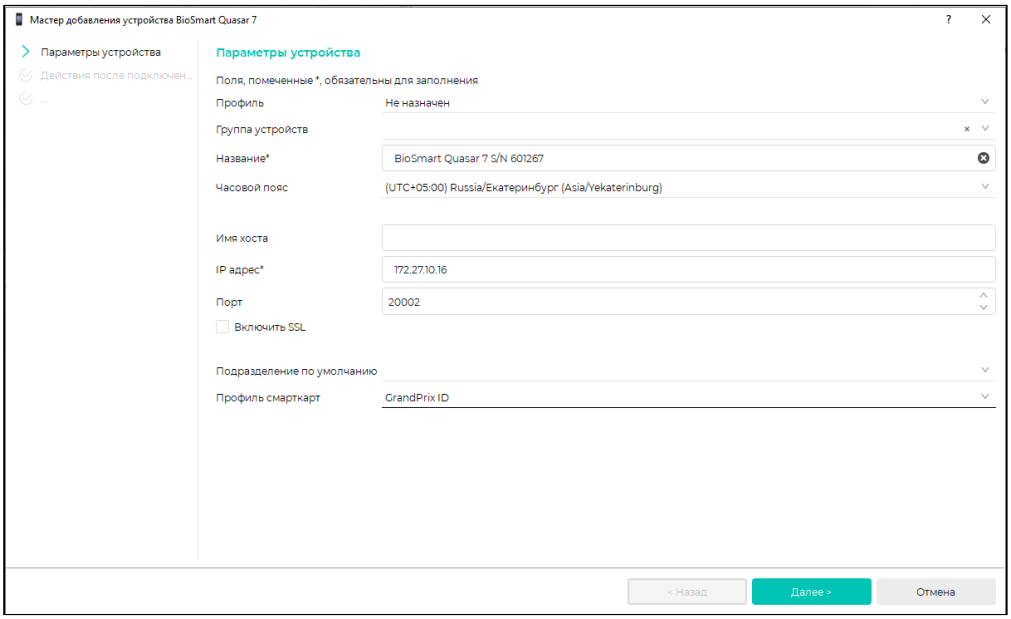
В ПО Biosmart-Studio v6 в разделе **Устройства** нажмите кнопку **Автопоиск**.



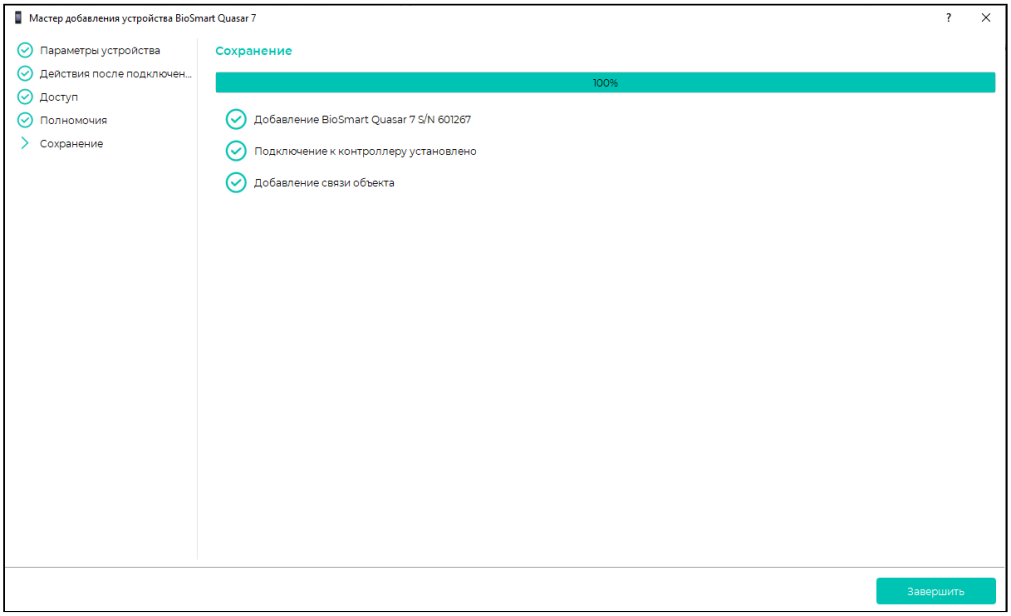
В списке устройств найдите терминал по серийному номеру, поставьте флаг в чекбоксе и нажмите **Подтвердить**.



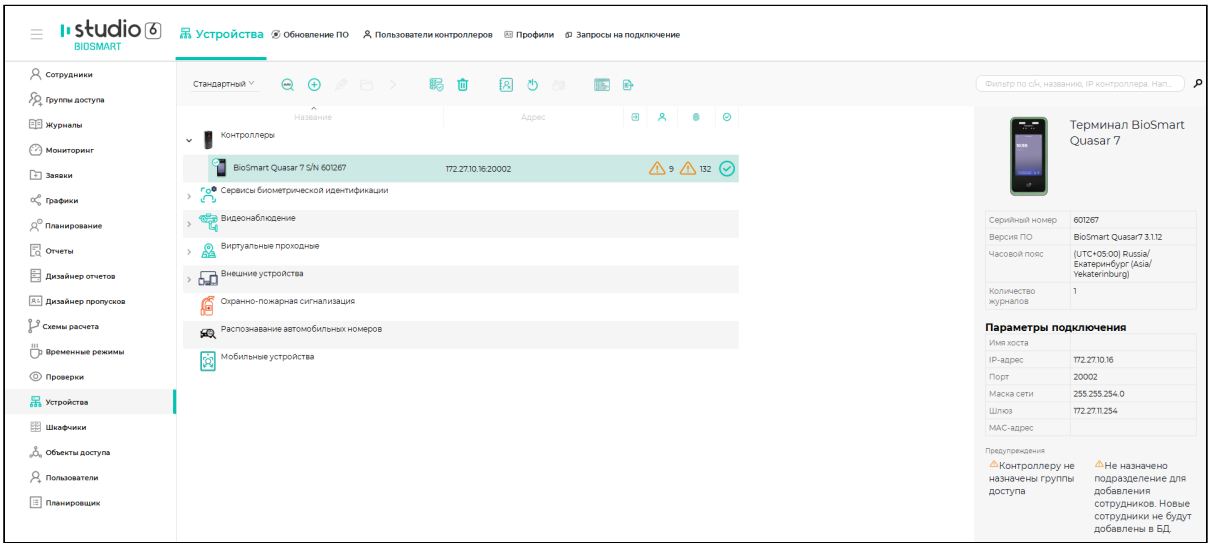
В окне **Мастер добавления устройства** нажмите **Далее**, затем **Завершить** (при необходимости изменить настройки можно будет позже).



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

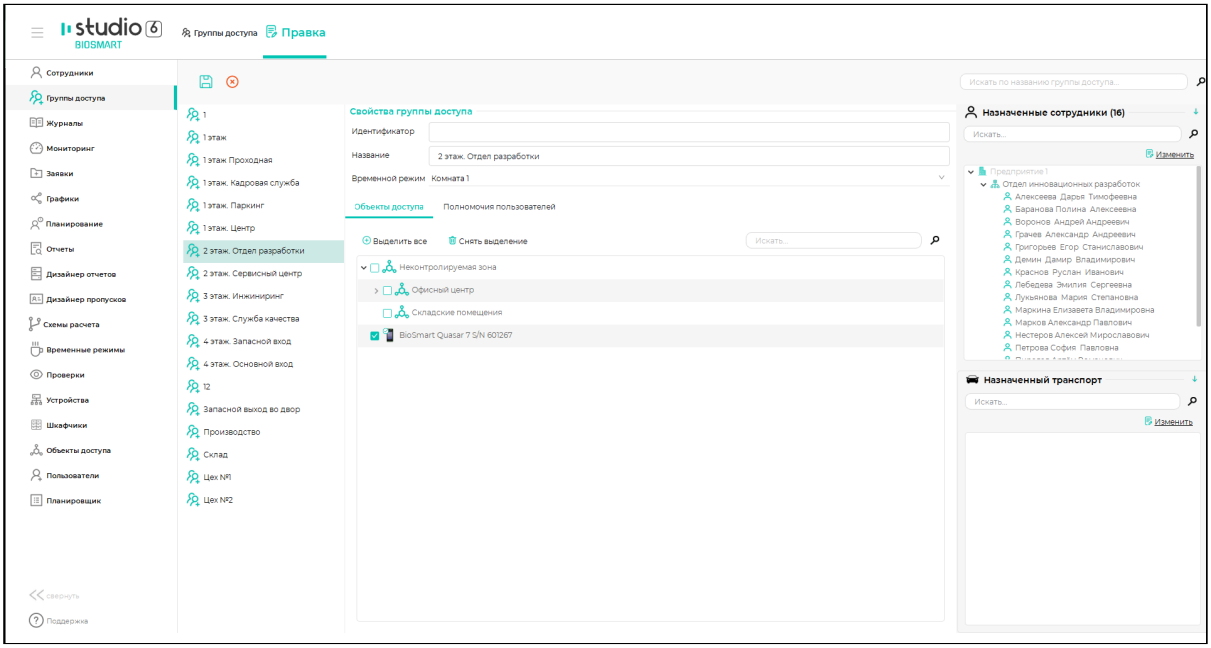


После успешного добавления терминал появится в списке устройств.



3. Загрузите на терминал список сотрудников

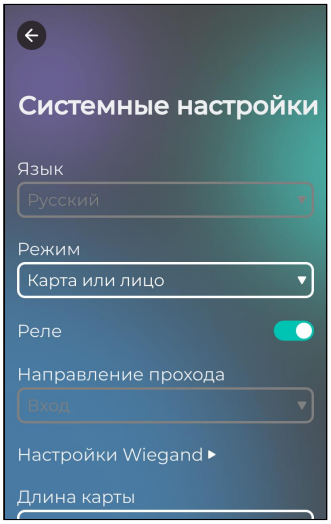
В ПО Biosmart-Studio v6 в разделе **Группы доступа** → выберите группу доступа → отметьте терминал и нажмите кнопку **Сохранить**.



В разделе **Устройства** отобразится количество сотрудников, которым предоставлен доступ с помощью терминала, и количество биометрических шаблонов в памяти.

4. Выберите режим работы

В меню терминала перейдите в раздел **Настройки** → **Системные настройки** и выберите рабочую модель в выпадающем списке поля **Режим**.



Также рабочую модель можно выбрать в ПО Biosmart-Studio v6 или веб-интерфейсе терминала. Описание рабочих моделей приведено в разделе Выбор режима работы и модальности.

5. Выберите направление прохода

Параметр **Направление прохода** применяется при учете 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 перейдите в раздел **Устройства** ПО Biosmart-Studio v6. Откройте окно **Свойства BioSmart Quasar 7** → перейдите на вкладку **Системные**. В поле **Направление прохода** выберите из списка направление прохода сотрудника. Нажмите кнопку **Сохранить** → **Закрыть.**

6. Зарегистрируйте идентификаторы сотрудников

Терминал **BioSmart Quasar 7** поддерживает несколько методов идентификации пользователей:

- по лицу (*соответствует требованиям 572-ФЗ*);
- по RFID-картам и смартфону;
- по рисунку вен ладони (опционально может быть встроен сканер рисунка вен ладони).

Выполните регистрацию идентификаторов соответствующих выбранному режиму работы. Порядок регистрации шаблонов приведён в разделе Регистрация идентификаторов сотрудников.

6 НАСТРОЙКИ ТЕРМИНАЛА BIOSMART QUASAR 7

6.1 Настройки меню BioSmart Quasar 7

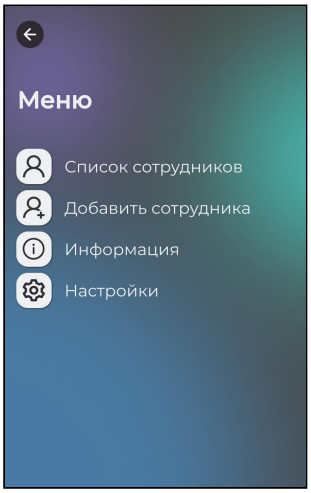
В разделе приведена информация о настройках в меню терминала **BioSmart Quasar 7.**

6.1.1 Доступ к меню терминала

Для входа в меню нажмите кнопку в правом верхнем углу → введите пин-код.

> По умолчанию установлен пин-код: **bioroot**.

Откроется окно **Меню**, из которого можно перейти в интересующий раздел.



Основное меню состоит из следующих разделов:

- Список сотрудников
- Добавить сотрудника
- Информация
- Настройки

6.1.2 Раздел Список сотрудников

Раздел предназначен для управления базой данных сотрудников, а именно:

- просмотра списка сотрудников;
- редактирования данных сотрудников;
- регистрации идентификаторов.

6.1.3 Раздел Добавить сотрудника

Раздел предназначен для быстрой регистрации новых сотрудников, а именно:

- добавления нового сотрудника на терминал;
- регистрации идентификаторов.

6.1.4 Раздел Информация

Раздел предназначен для просмотра основных сведений о терминале и сведений об ошибках.

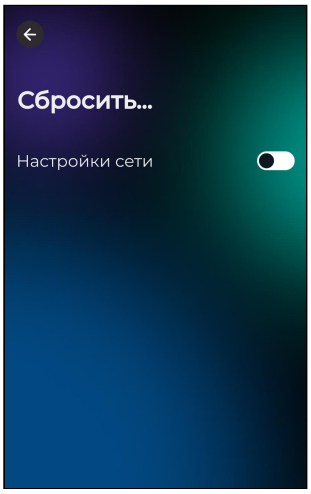
Описание основных сведений приведено в таблице ниже.

Поле	Описание
Устройство	Название устройства.
Серийный номер	Короткий серийный номер терминала.
Версия прошивки	Версия встроенного ПО терминала.
Тип считывателя карт	Тип используемого RFID-считывателя. В зависимости от типа терминал может считывать разные типы карт.
Версия алгоритмов по лицам	Версия ПО для распознавания лиц.
Версия алгоритмов по венам ладони	Версия ПО для распознавания ладоней.
Количество сотрудников	Число пользователей на терминале.
Количество шаблонов лиц	Общее количество шаблонов лиц на терминале.
Тип подключения	Способ подключения к сети, например, проводной (LAN).
IP	IP-адрес терминала.
Маска	Диапазон IP-адресов в локальной сети.
Шлюз	Адрес маршрутизатора для выхода в другие сети.
DNS	Адрес сервера, преобразующего доменные имена в IP-адреса.
MAC	Физический адрес сетевого интерфейса терминала.
IP хоста	IP-адрес серверной части ПО Biosmart-Studio v6.

В нижней части экрана находится кнопка **Сведения об ошибках**. Нажмите её для просмотра списка ошибок.

6.1.5 Раздел Настройки

Содержание раздела и назначение подразделов приведено в таблице ниже.

Подраздел	Описание
Система	Подраздел предназначен для изменения следующих настроек: • выбора режима работы и модальности терминала; • включения/отключения реле терминала; • включение/отключение идентификации по QR-коду; • изменения настроек Wiegand; • изменения длины карты; • выбора формата считываемой карты; • изменения параметров индикации.
Сеть	Для изменения сетевых параметров (см. раздел Настройки сетевых параметров).
Сброс	Для сброса сетевых параметров до заводских включите опцию **Настройки сети**. Следуйте инструкциям на экране (см. раздел Сброс параметров терминала на заводские). 
Перезапуск	Для выполнения перезагрузки терминала или приложения (см. раздел Перезапуск).

6.2 Настройки BioSmart Quasar 7 в веб-интерфейсе

В разделе приведена информация о настройках терминала в веб-интерфейсе.

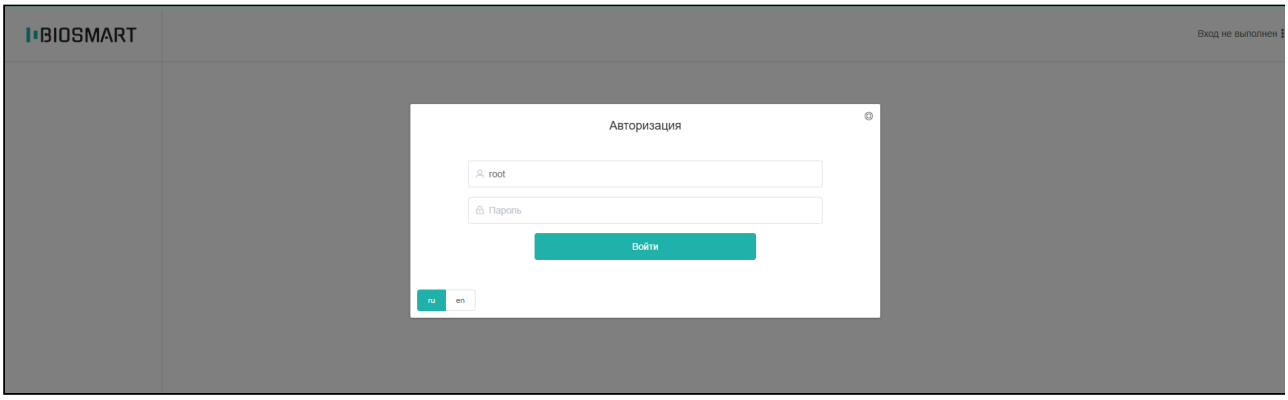
ⓘ Разделы веб-интерфейса, не описанные здесь, не используются.

6.2.1 Доступ к веб-интерфейсу

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

В адресной строке браузера введите IP-адрес терминала в виде https://IP_address.

По умолчанию на терминале установлен IP-адрес **172.25.110.71**, таким образом, если IP-адрес не изменялся, в строку браузера введите **https://172.25.110.71**. На экране отобразится окно авторизации приведенное ниже.



В поля **Login** и **Password** введите логин и пароль.

✓ По умолчанию установлены:

- Логин: **root**
- Пароль: **bioroot**

Основное меню веб-интерфейса состоит из следующих разделов:

- Устройство
- Параметры
- Система
- Хранилище
- Журнал работы
- Обновление прошивки
- СКЗИ

ⓘ Разделы, не описанные здесь, не используются.

6.2.2 Раздел Устройство

Раздел предназначен для просмотра общей информации об устройстве и содержит следующие вкладки:

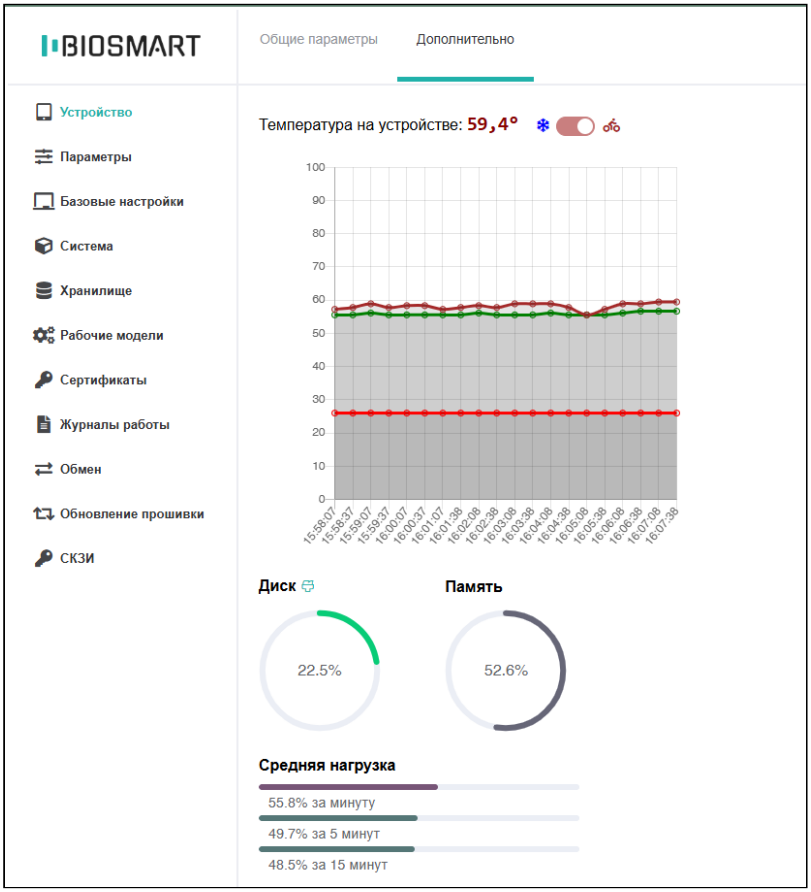
Общие параметры

На вкладке приведены основные сведения о терминале. Описание параметров указано в таблице ниже.

Параметр	Описание
Устройство	Название устройства.
Серийный номер	Короткий серийный номер терминала.
Версия прошивки	Версия встроенного ПО терминала.
IP	IP-адрес терминала.
Маска	Диапазон IP-адресов в локальной сети.
Шлюз	Адрес маршрутизатора для выхода в другие сети.
DNS	Адрес сервера, преобразующего доменные имена в IP-адреса.
Текущее время на устройстве	Дата и время на терминале.

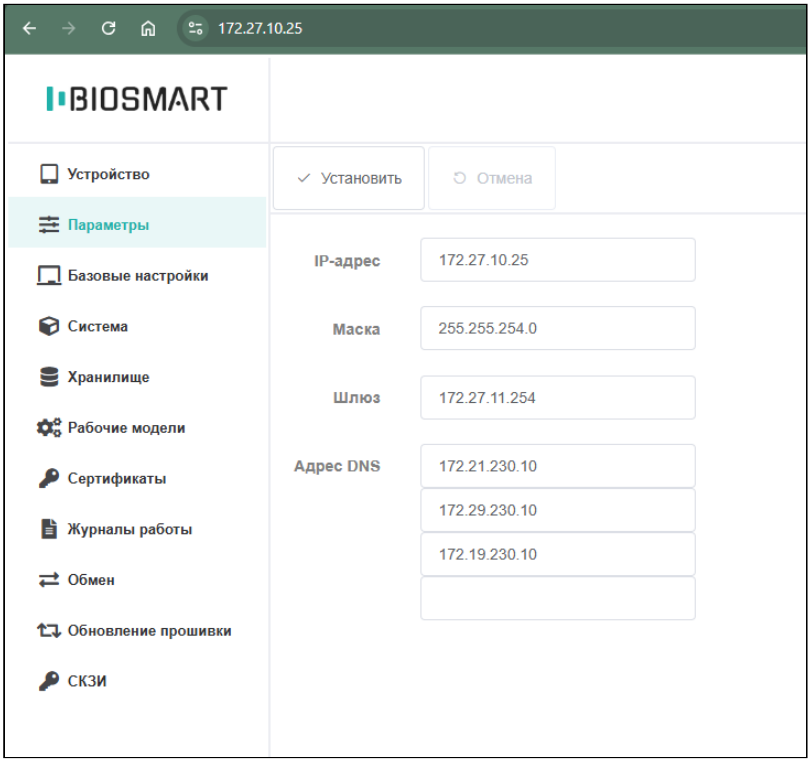
Дополнительно

На вкладке отображается информация о состоянии памяти, температуре устройства и другое.



6.2.3 Раздел Параметры

Раздел предназначен для изменения сетевых параметров терминала. При необходимости измените сетевые настройки согласно инструкции в разделе Настройка сетевых параметров терминала.

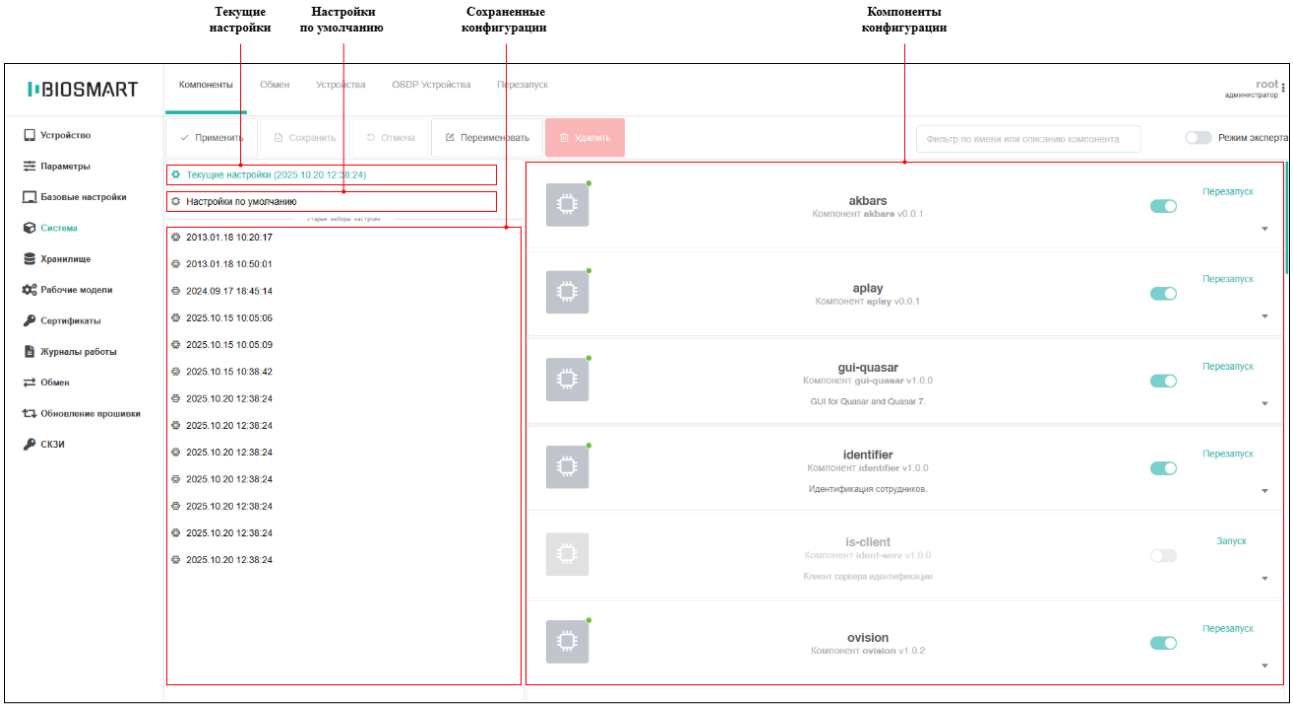


6.2.4 Раздел Система

Раздел предназначен для управления настройками терминала, подключёнными устройствами и содержит следующие вкладки:

Компоненты

Вкладка содержит конфигурации терминала (текущую, принятую по умолчанию и сохраненные), а также список компонентов и их настройки. Описание компонентов конфигурации и порядок работы приведены в разделе Настройка конфигурации терминала.



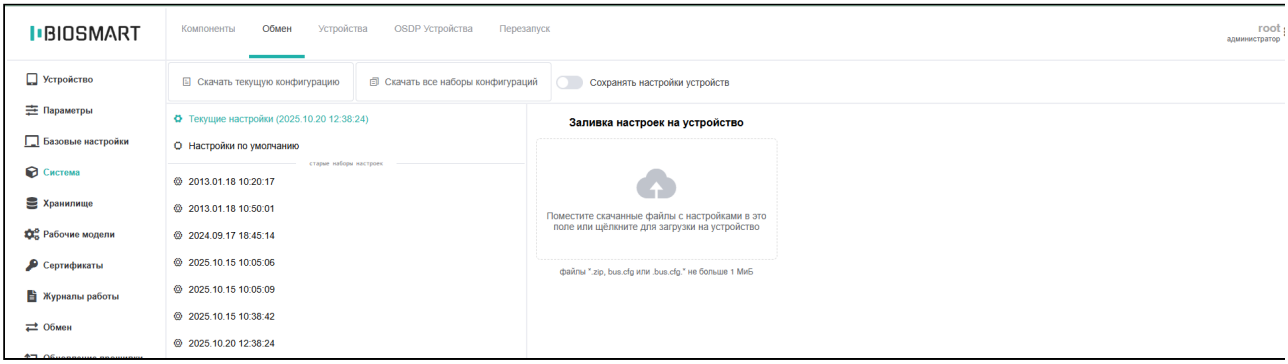
Описание кнопок на панели сверху приведено в таблице ниже.

Кнопка	Описание
Применить	– применение изменений и загрузка конфигурации на устройство.
Сохранить	– сохранение изменений, внесенных в конфигурацию.
Отмена	– отмена изменений, внесенных в конфигурацию.
Переименовать	– изменение наименования конфигурации.
Удалить	– удаление конфигурации.

Обмен

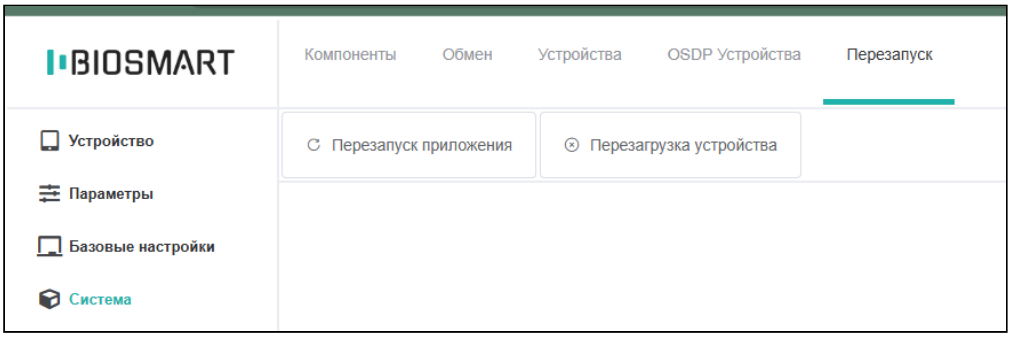
Вкладка позволяет управлять конфигурацией терминала: экспортировать текущую и импортировать её для настройки других терминалов. Достаточно настроить один терминал, экспортировать его конфигурацию и использовать этот файл для быстрой настройки остальных.

Для выполнения экспорта или импорта, следуйте инструкции в разделе Управление конфигурацией терминала.



Перезапуск

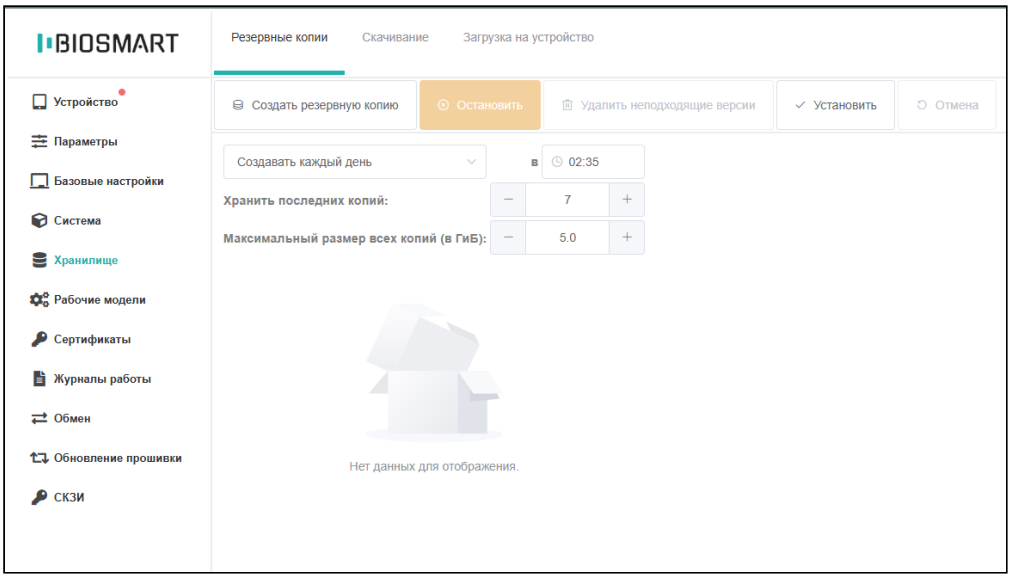
Вкладка используется для перезапуска терминала (см. раздел Перезапуск).



6.2.5 Раздел Хранилище

Раздел предназначен для управления базой данных терминала. С его помощью можно выполнять следующие операции:

- настраивать правила резервного копирования базы данных (далее - БД) терминала;
- экспортировать БД полностью или частично;
- импортировать БД на терминал.



6.2.6 Раздел Журналы работы

Раздел предназначен для скачивания и очистки журналов работы, экспорта и импорта файлов настроек журналов, и просмотра сообщений о работе приложения. Он содержит следующие вкладки:

Скачивание

На вкладке доступны кнопки для скачивания журналов, описание приведено в таблице ниже.

Кнопка	Описание
Скачать выбранные журналы	Для скачивания определенных журналов. Выберите журналы для скачивания, включив опции: • Скачивать журналы приложения; • ...в том числе журналы после ротации; • Скачивать журналы обновления; • Скачивать системные журналы; • Скачивать все прочие журналы.
Скачать все журналы	Для скачивания всех журналов.
Остановить	Для отмены скачивание журналов.

Очистка

На вкладке доступны кнопки для удаления журналов, описание приведено в таблице ниже.

Кнопка	Описание
Удалить выбранные журналы	Для удаления определенных журналов. Выберите журналы для удаления, включив опции: • Очищать журналы приложения; • Очищать журналы приложения после ротации; • Очищать журналы обновления; • Очищать системные журналы; • Очищать все прочие журналы.
Удалить все журналы	Для удаления всех журналов.

Сообщения

Вкладка **Сообщения** предназначена для просмотра журнала событий приложения.

6.2.7 Раздел Обновление прошивки

Раздел предназначен для обновления встроенного ПО терминала. При необходимости обновите встроенное ПО в соответствии с инструкцией в разделе Обновление встроенного ПО терминала.

6.2.8 Раздел СКЗИ

Раздел предназначен для настройки защищённого подключения между терминалом и сторонней системой. В нём доступны следующие вкладки:

- **VipNet Client** предназначена для просмотра информации о сети VipNet и статуса подключения, а также для загрузки и установки ключа доступа;
- **VipNet OSSL** предназначена для активации протокола TLS использующего российские криптографические алгоритмы;
- **КриптоПро CSP** предназначена для просмотра информации о лицензии, её активации, добавления и удаления корневых и клиентских сертификатов, а также для указания целевого адреса подключения;
- **КБС Крипт** предназначена для включения сервиса, выбора сертификата подписи, просмотра информации о статусе подключения и лицензии, а также для установки ключа лицензии. Используется для КБС OVISION.

Подробное описание вкладок и порядок настройки СКЗИ приведено в разделе Настройка СКЗИ.

6.3 Настройки BioSmart Quasar 7 в ПО Biosmart-Studio v6

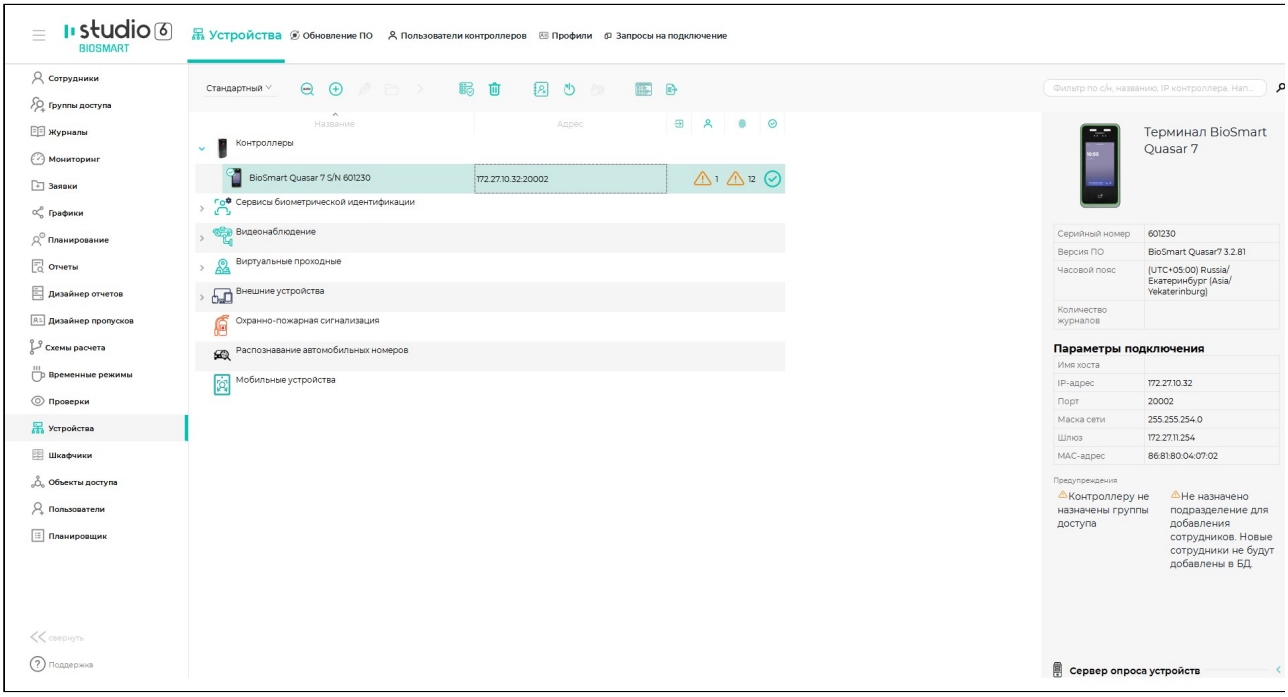
В разделе приведена информация о настройках терминала в ПО Biosmart-Studio v6.

> ⓘ Встроенное ПО BioSmart Quasar 7 версии **3.2.82** работает с ПО Biosmart-Studio версии не ниже **6.4.5.**

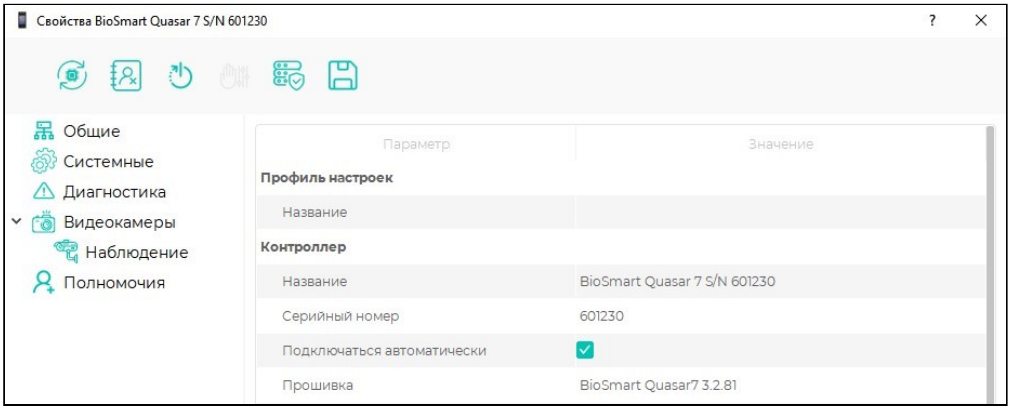
6.3.1 Общая информация о настройках

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 терминал и нажать кнопку **Свойства** на панели инструментов;
- нажать на терминал правой кнопкой мыши и в контекстном меню выбрать пункт **Свойства.**



Откроется окно **Свойства BioSmart Quasar 7.**

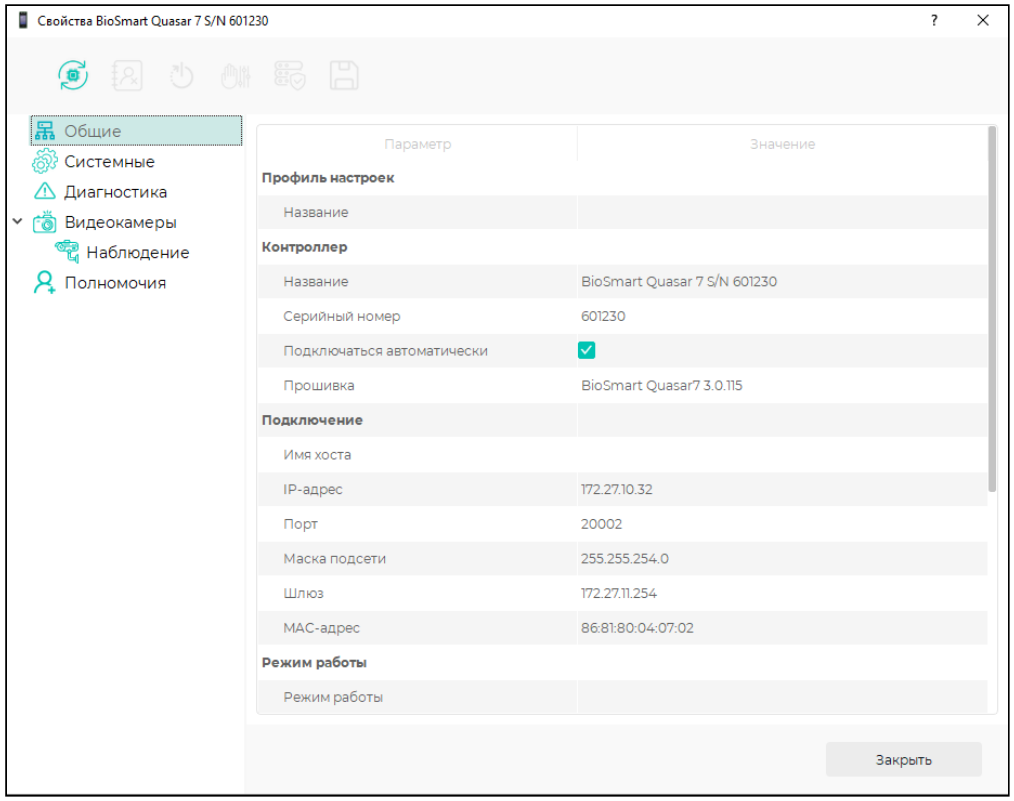


На панели управления расположены следующие кнопки:

Обновление ПО		– настройка задания на обновление встроенного ПО терминала
Инициализация		– инициализация терминала, в ходе которой из памяти удаляются список сотрудников, их идентификаторы и события
Сброс настроек		– сброс настроек терминала на заводские
Калибровка сенсора		– для терминала не используется

Применить профиль		– применение для терминала настроек профиля
Сохранить в профиль		– сохранение настроек терминала в профиль

6.3.2 Вкладка Общие



Описание полей приведено в таблице ниже.

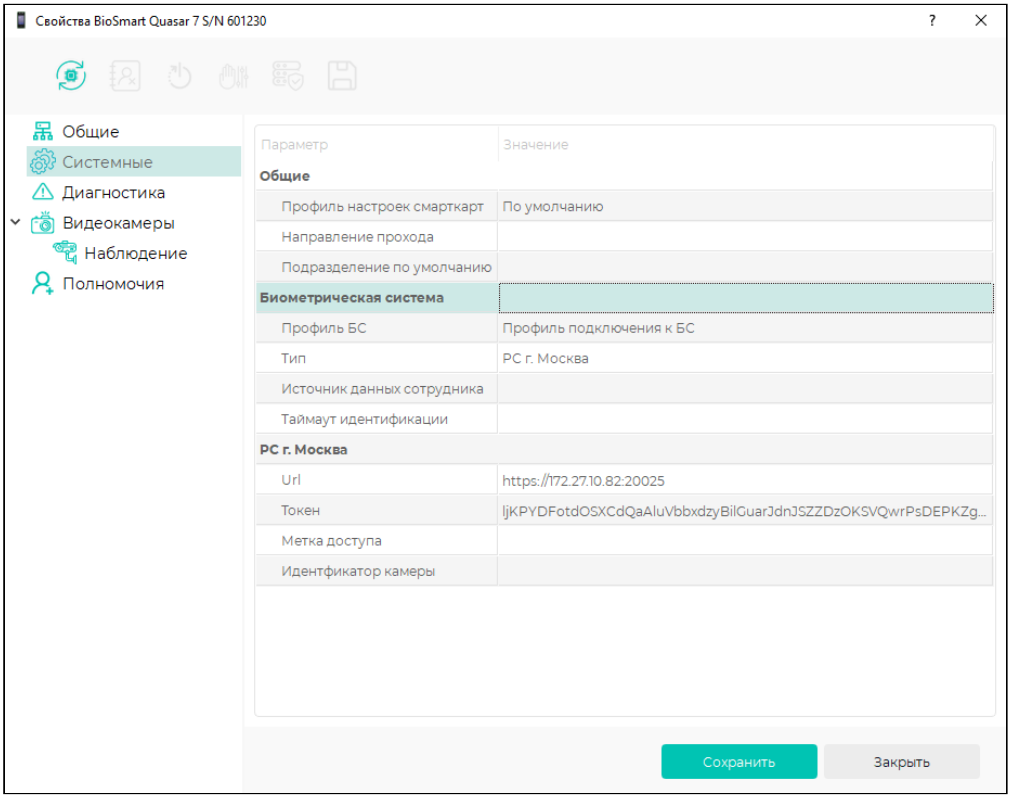
Поле	Описание
Профиль настроек	
Название	Выбор профиля настроек. Это позволяет применить одинаковые настройки для группы однотипных устройств.
Контроллер	
Название	Название устройства в ПО Biosmart-Studio v6.
Серийный номер	Короткий серийный номер устройства. Заполняется автоматически, не редактируется.

Поле	Описание
Подключаться автоматически	При заполненном чекбоксе серверная часть ПО Biosmart-Studio v6 будет автоматически подключаться к устройству в случае возобновления связи.
Прошивка	Версия встроенного ПО устройства. Заполняется автоматически, не редактируется.
Подключение	
Имя хоста	Сетевые настройки контроллера
IP-адрес	
Порт	
Маска подсети	
Шлюз	
MAC-адрес	
Режим работы	
Режим работы	Режим работы устройства. Доступные значения: **автономный режим** и **серверная идентификация**. В **режиме серверной идентификации** для идентификации, хранения кодов RFID-карт используется внешний сервер. В **автономном режиме** идентификация, хранение кодов RFID-карт и журнала событий осуществляется на устройстве с непрерывным обменом этими данными с ПО Biosmart-Studio v6. Список сотрудников, которым назначен доступ с помощью устройства, задается в ПО Biosmart-Studio v6. ⚠ Режим серверной идентификации поддерживается начиная с версии 3.2.81 встроенного ПО устройства.
Сервер идентификации	Сетевой адрес внешнего сервера идентификации при работе устройства в режиме **Серверная идентификация**
Дополнительно	
Часовой пояс	Часовой пояс, в соответствии с которым будет установлено время на устройстве

Поле	Описание
Время ожидания ответа	Интервал времени, в течение которого сервер BioSmart ожидает ответ от устройства. Если по истечении указанного интервала ответ не получен, то связь с устройством считается разорванной
Максимальный размер пакета, байт (MTU)	Не используется. Максимальный размер пакета, передаваемый устройством без фрагментации. Настройка необходима только в сетях, где есть маршрутизаторы, не поддерживающие фрагментацию пакетов
Количество пользователей	Количество сотрудников, которым назначен доступ с помощью устройства
Количество шаблонов	Количество биометрических шаблонов в памяти устройства
Кол-во журналов в памяти	Количество событий в памяти устройства, которые ещё не отправлены на сервер

6.3.3 Вкладка Системные

Вкладка **Системные** предназначена для настройки параметров работы устройства.



Описание полей приведено в таблице ниже.

Поле	Описание
Общие	
Профиль настроек смарткарт	Профиль настроек смарткарт для терминала (см. раздел Профили смарткарт Руководства пользователя ПО Biosmart-Studio v6). Он позволяет применить параметры защиты карт.
Направление прохода	Направление движения сотрудника (Вход/Выход), которое автоматически запишется в ПО Biosmart-Studio v6 при успешной идентификации на терминале (см. раздел Выбор направления прохода).
Подразделение по умолчанию	Подразделение, в которое добавляются новые сотрудники после регистрации на терминале.
Биометрическая система	
Профиль БС	Профиль биометрической системы для терминала.
Тип	Тип биометрической системы определяется автоматически по профилю БС.
Источник данных сотрудника	Основная система, являющаяся источником данных по сотрудникам для терминала. Доступные значения: • Установите значение *Biosmart-Studio*, если данные о сотрудниках будут загружаться из БД ПО Biosmart-Studio v6; • Установите значение *Биометрическая система*, если данные о сотрудниках будут загружаться из БД биометрической системы. ⚠ Значение **Биометрическая система** недоступно для КБС Pridex.
Таймаут идентификации	Максимальное время, выделенное на идентификацию.
КБС Pridex	
Url	Параметры заполнятся автоматически при выборе соответствующего профиля БС.
Токен	
КБС Face2	

Поле	Описание
Url	Укажите **Url**, предоставленный БС.
Токен	
КБС OVISION	
Url	Укажите **Url**, предоставленный БС.

6.3.4 Вкладка Диагностика

Вкладка **Диагностика** предназначена для отображения статистических данных по связи устройства с серверной частью ПО Biosmart-Studio v6 и результатов самодиагностики. Описание полей приведено в таблице ниже.

Поле	Описание
Передано	Число пакетов, переданных контроллером за последний час.
Кол-во повторов, Кол-во ошибок передачи	Количество повторов и ошибок за последний час.
Кол-во сбоев	Количество пакетов, которые контроллер не смог передать на серверную частью ПО Biosmart-Studio v6.
Размер очереди команд (примерно)	Количество команд, которые на данный момент поставлены в очередь серверной частью ПО Biosmart-Studio v6 для этого контроллера.

6.3.5 Вкладка Видеокамеры

ⓘ В настоящее время вкладка не используется.

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

6.3.6 Вкладка Полномочия

ⓘ В настоящее время вкладка не используется.

Вкладка **Полномочия** предназначена для выбора пользователей, которым будут доступны настройки терминала в ПО Biosmart-Studio v6.

7 РАБОТА С ТЕРМИНАЛОМ BIOSMART QUASAR 7

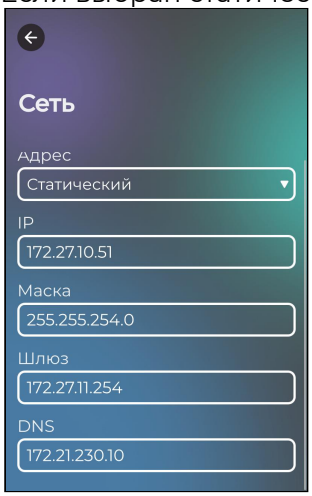
7.1 Настройка сетевых параметров терминала

> ⓘ При первичной настройке обязательно измените IP-адрес терминала через меню устройства. Замените заводской адрес 172.25.110.71 на статический адрес, соответствующий параметрам вашей локальной сети.

Сетевые параметры можно изменить через:

Меню терминала

1. Для входа в меню нажмите кнопку в правом верхнем углу → введите пин-код.
2. Выберите **Настройки** → **Сеть**.
3. В открывшемся окне выберите тип получения IP-адреса из выпадающего списка:
   - **Динамический адрес:** Адрес будет получен автоматически от сервера вашей сети.
   - **Статический адрес:** Позволяет задать параметры вручную.
4. Если выбран статический адрес, введите параметры вручную.

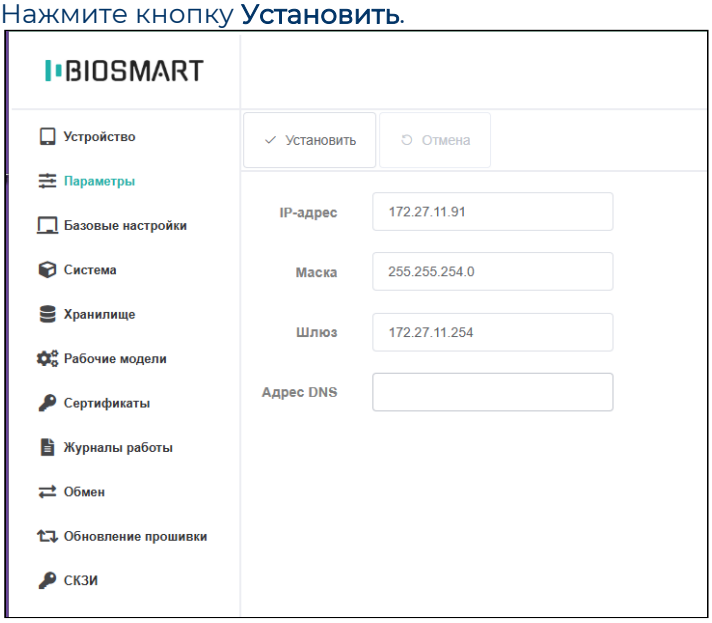


5. Нажмите **Сохранить**.

Веб-интерфейс

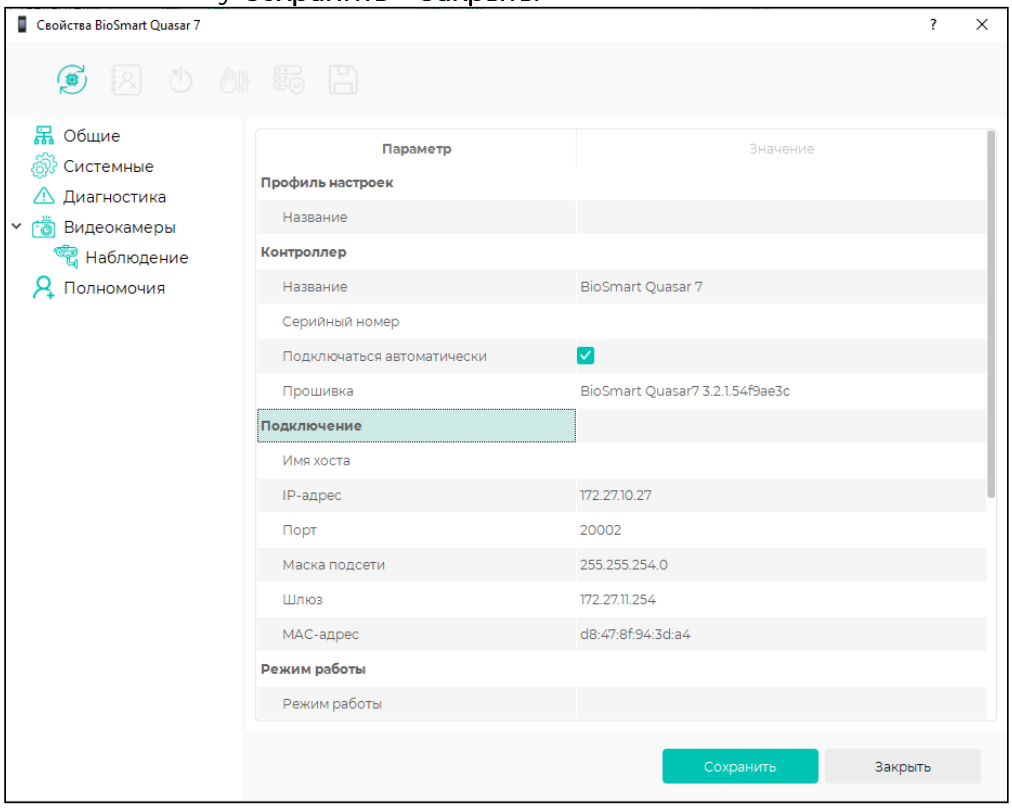
1. Откройте браузер и введите в адресной строке текущий IP-адрес терминала.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Параметры**.
4. Измените параметры сети.

5. Нажмите кнопку **Установить**.



ПО Biosmart-Studio v6

1. Выполните вход в ПО Biosmart-Studio v6.
2. Перейдите в раздел **Устройства** → откройте окно **Свойства BioSmart Quasar 7.**
3. Измените параметры сети.
4. Нажмите кнопку **Сохранить → Закрыть.**



7.2 Изменение настроек терминала

7.2.1 Выбор режима работы и модальности

Режим работы

Согласно требованиям федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных» идентификация по биометрическим данным (лицо, голос) может производиться только в единой биометрической системе (**ЕБС**), в том числе в ее региональных сегментах, и коммерческих биометрических системах (**КБС**).

- **ЕБС** — это государственная информационная система, обеспечивающая сбор биометрических персональных данных, их хранение и использование для аутентификации и идентификации пользователей.
- **КБС** — это аккредитованная информационная система, выполняющая биометрическую аутентификацию. Особый статус ее компании-владельца позволяет правомерно осуществлять обработку биометрических персональных данных в собственной инфраструктуре без прямого взаимодействия с **ЕБС**.
- **Региональный сегмент ЕБС** — это часть Единой Биометрической Системы, которая собирает, хранит и обрабатывает биометрические данные пользователей для нужд конкретного региона. С 1 сентября 2024 года на территории города Москвы действует Региональный сегмент ЕБС (ПП № 1151 от 26.08.2024 г.).

ПО Biosmart-Studio v6 совместно с терминалом **BioSmart Quasar 7** позволяет организовать работу СКУД в соответствии с федеральным законом №572-ФЗ от 29.12.2022г.

> ⓘ Для работы ПО Biosmart-Studio v6 с *ЕБС*, *КБС* или *Региональным сегментом г.Москвы* необходимо наличие соответствующей лицензии:
>
> - «Интеграция с ЕБС»
> - «Интеграция с КБС»
> - «Интеграция с РС г.Москва»

Для терминала реализованы следующие модели работы в соответствии с федеральным законом от 29 декабря 2022 г. № 572-ФЗ:

Векторная модель

Для идентификации сотрудников используются математические шаблоны, созданные на основе фотографий. Эти шаблоны отправляются в КБС, где их сравнивают с шаблонами, ранее выгруженными из ЕБС.

Порядок идентификации сотрудника по **векторной модели** выглядит следующим образом:

1. При попытке идентификации терминал отправляет изображение лица сотрудника в КБС.
2. На основе полученного изображения в КБС формируется математический шаблон, который сравнивается с шаблонами, загруженными из ЕБС.

3. При успешном совпадении КБС передает идентификатор сотрудника на терминал BioSmart Quasar 7.
4. Терминал отправляет запрос в ПО Biosmart-Studio v6, где выполняется поиск по полученному идентификатору. Если идентификатор найден, на терминале отобразится сообщение об успешной идентификации.
5. После успешной идентификации терминал передает информацию о событии в журнал ПО Biosmart-Studio v6.

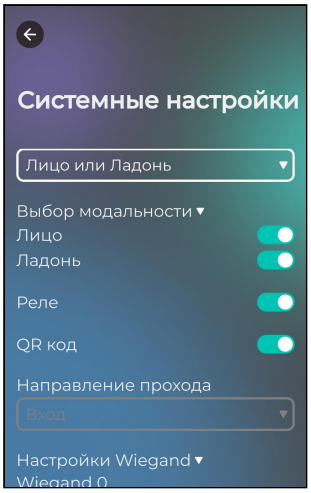
Транзакционная модель

Идентификация осуществляется напрямую через ЕБС.

Порядок идентификации сотрудника по **транзакционной модели** выглядит следующим образом:

1. При попытке идентификации терминал отправляет изображение лица сотрудника в ЕБС. Выполняется идентификация.
2. Персональный идентификатор сотрудника, полученный из ЕБС, отправляется на ТИБ-сервер.
3. После успешного сопоставления, информация возвращается в терминал BioSmart Quasar 7.
4. После получения всех необходимых идентификаторов и сопоставлений, терминал принимает решение о разрешении или запрете на вход/выход.

В меню терминала нажмите **Настройки** → **Система**. Выберите режим работы из выпадающего списка в поле **Режим** и нажмите **Сохранить.**



Терминал поддерживает работу в следующих режимах:

Карта или лицо

В данном режиме для доступа требуется идентификация по одному из факторов: **карте** или **лицу.** Терминал перейдет к обработке того фактора, который будет обнаружен первым.

Идентификация по лицу выполняется по транзакционной или векторной модели. По карте локально на терминале.

После успешной идентификации по одному из факторов терминал выполняет действия, заданные в настройках (например, включает реле).

Карта и лицо

В данном режиме для доступа требуется двухфакторная идентификация (верификация):

1. **Идентификация по карте**. Терминал находится в ожидании прикладывания карты к встроенному RFID-считывателю. После успешной идентификации терминал переходит к следующему этапу.
2. **Идентификация по лицу.** Идентификация выполняется по транзакционной или векторной модели. После успешной идентификации по второму фактору терминал выполняет действия, заданные в настройках (например, включает реле).

Лицо или ладонь

В данном режиме для доступа требуется идентификация по одному из биометрических факторов: **лицу** или **ладони**. Терминал перейдет к обработке того фактора, который будет обнаружен первым, либо запустит идентификацию при нажатии кнопки на экране (см. раздел Выбор модальности).

Идентификация по лицу выполняется по транзакционной или векторной модели. По ладони локально на терминале.

После успешной идентификации по одному из факторов терминал выполняет действия, заданные в настройках (например, включает реле).

Лицо и ладонь

В данном режиме для доступа требуется двухфакторная идентификация (верификация):

1. **Идентификация по лицу.** Идентификация выполняется по транзакционной или векторной модели. После успешной идентификации терминал переходит к следующему этапу.
2. **Идентификация по ладони**. После успешной идентификации по лицу терминал запрашивает подтверждение личности по второму биометрическому идентификатору – ладони. После успешной идентификации по второму фактору терминал выполняет действия, заданные в настройках (например, включает реле).

Карта и ладонь

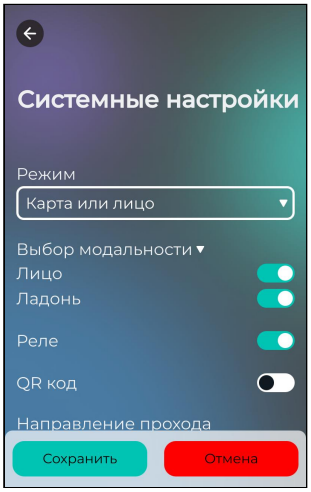
В данном режиме для доступа требуется двухфакторная идентификация (верификация):

1. **Идентификация по карте**. Терминал находится в ожидании прикладывания карты к встроенному RFID-считывателю. После успешной идентификации терминал переходит к следующему этапу.
2. **Идентификация по ладони**. Терминал запрашивает подтверждение личности по биометрическим данным ладони. После успешной идентификации по второму фактору терминал выполняет действия, заданные в настройках (например, включает реле).

Режим верификации позволяет работать с большим количеством биометрических шаблонов и сотрудников, сокращает время идентификации. Работая в режиме **Карта и ладонь,** терминал не противоречит требованиям федерального закона от 29 декабря 2022 г. № 572-ФЗ и не требует подключения к ЕБС, КБС или Региональному сегменту г. Москвы.

Выбор модальности

В меню терминала нажмите **Настройки** → **Система** → разверните список **Выбор модальности.** Нажмите **Сохранить.**



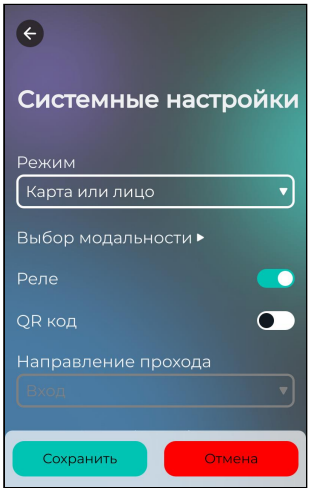
Если опции **Лицо** и **Ладонь** включены, то в режиме **Лицо и Ладонь** на экране терминала появятся соответствующие кнопки. Нажатие на одну из них запустит процесс идентификации по выбранному биометрическому фактору.

7.2.2 Настройка работы реле терминала

Активировать работу реле терминала можно через:

Меню терминала

В меню терминала нажмите **Настройки** → **Система**. Включите или отключите опцию **Реле** в зависимости от требуемого состояния.



Нажмите **Сохранить.**

Веб-интерфейс

1. Откройте браузер и введите в адресной строке текущий IP-адрес терминала.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Система** → вкладка **Компоненты**.
4. Найдите компонент рабочей модели (например, work-model-card-orface) и раскройте его.
5. В поле **Реле** установите значение **включено** или **отключено** в зависимости от требуемого состояния.
6. В поле **Таймаут реле, мс** укажите длительность удержания реле в активированном состоянии.
7. Нажмите **Применить**.
8. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

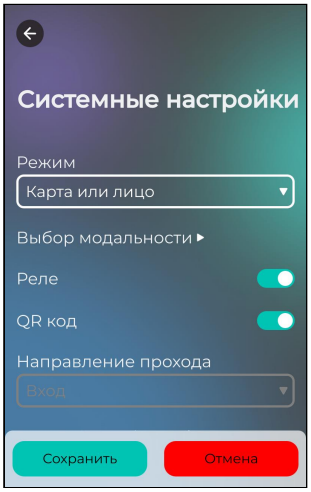
7.2.3 Настройка идентификации по QR-кодам

На устройстве предусмотрена возможность идентификации сотрудников по QR-кодам с экрана телефона или распечатанным на бумаге. При этом QR-коды должны быть заранее сгенерированы в ПО Biosmart-Studio v6 на основе данных сотрудников (см. раздел Вкладка Идентификация Руководства пользователя ПО Biosmart-Studio v6).

Идентификация по QR-коду возможна только при работе в режиме **Карта или Лицо** (см. раздел Выбор режима и модальности). Управлять работой QR-кода можно через:

Меню терминала

В меню терминала нажмите **Настройки** → **Система.** Включите или отключите опцию **QR код** в зависимости от требуемого состояния.



Нажмите **Сохранить.**

Веб-интерфейс

1. Откройте браузер и введите в адресной строке текущий IP-адрес терминала.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Система** → вкладка **Компоненты**.
4. Найдите компонент рабочей модели (например, work-model-card-orface) и раскройте его.
5. В поле **Qr code enable** установите значение **включено** или **отключено** в зависимости от требуемого состояния.
6. Нажмите **Применить**.
7. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

7.2.4 Выбор направление прохода

Для автоматической регистрации направления движения сотрудника (вход на объект или выход с объекта) при успешной идентификации на терминале используется параметр **Направление прохода**. Направление задается для каждого терминала, и именно это значение автоматически записывается в ПО Biosmart-Studio v6 при срабатывании.

Направление прохода можно установить через:

Меню терминала

В настоящий момент функция не поддерживается.

В меню терминала нажмите **Настройки** → **Система**. В поле **Направление прохода** выберите из списка направление прохода сотрудника.

Нажмите **Сохранить.**

Веб-интерфейс

1. Выполните вход в веб-интерфейс.

2. Перейдите в раздел **Система** → вкладка **Компоненты**.
3. Найдите компонент рабочей модели (например, work-model-card-orface) и раскройте его.
4. В поле **Направление прохода** выберите из списка направление прохода сотрудника.
5. Нажмите **Применить**.
6. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

ПО Biosmart-Studio v6

1. Выполните вход в ПО Biosmart-Studio v6.
2. Перейдите в раздел **Устройства** → откройте окно **Свойства BioSmart Quasar 7.**
3. Перейдите на вкладку **Системные**.
4. В поле **Направление прохода** выберите из списка направление прохода сотрудника.
5. Нажмите кнопку **Сохранить → Закрыть.**

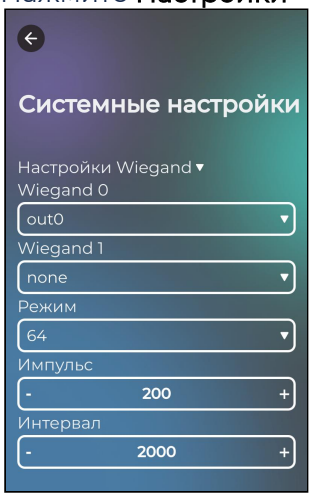
7.2.5 Настройка работы по интерфейсу Wiegand

Терминал можно настроить на прием или передачу данных по интерфейсу Wiegand для интеграции терминала в стороннюю СКУД.

Получение информации от внешних устройств

Для настройки выполните следующие действия:

1. Войдите в меню терминала.
2. Нажмите **Настройки** → **Система**.



3. В поле **Wiegand 0** установите **in** для для приёма информации от внешних устройств.
4. В выпадающем меню поля **Режим** выберите битность интерфейса Wiegand.

> ⓘ В зависимости от выбранной битности и объема данных, номер карты может быть обрезан. Убедитесь, что битность соответствует формату ваших карт.

5. В поле **Ширина импульса** укажите ширину передаваемых импульсов. Рекомендуемое значение 200 мкс.

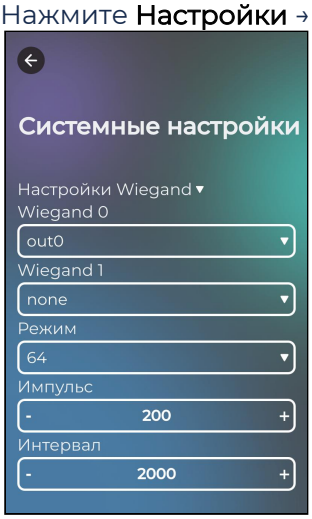
6. В поле **Время между посылками** установите период следования импульсов. Рекомендуемое значение 2000 мкс.
7. Нажмите **Сохранить**.

Передача информации на внешние устройства

Настройка Wiegand в меню терминала

Для передачи на внешнее устройство успешного результата идентификации выполните следующие настройки:

1. Войдите в меню терминала.
2. Нажмите **Настройки** → **Система**.



3. В поле **Wiegand 0** установите значение **out**. Это активирует передачу данных с терминала на внешние устройства (например, контроллер СКУД).
4. В выпадающем меню поля **Режим** выберите битность интерфейса Wiegand.

> Битность должна соответствовать формату ваших карт. Если битность выбрана неправильно, номер карты будет обрезан или передан некорректно.

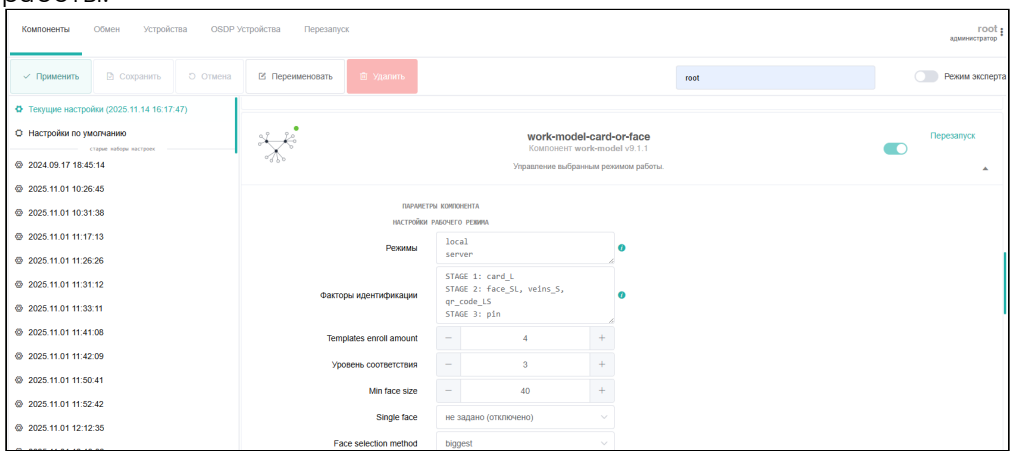
5. В поле **Ширина импульса** укажите ширину передаваемых импульсов. Рекомендуемое значение 200 мкс.
6. В поле **Время между посылками** установите период следования импульсов. Рекомендуемое значение 2000 мкс.
7. Нажмите **Сохранить**.

Настройка отправки кода при неудачной идентификации

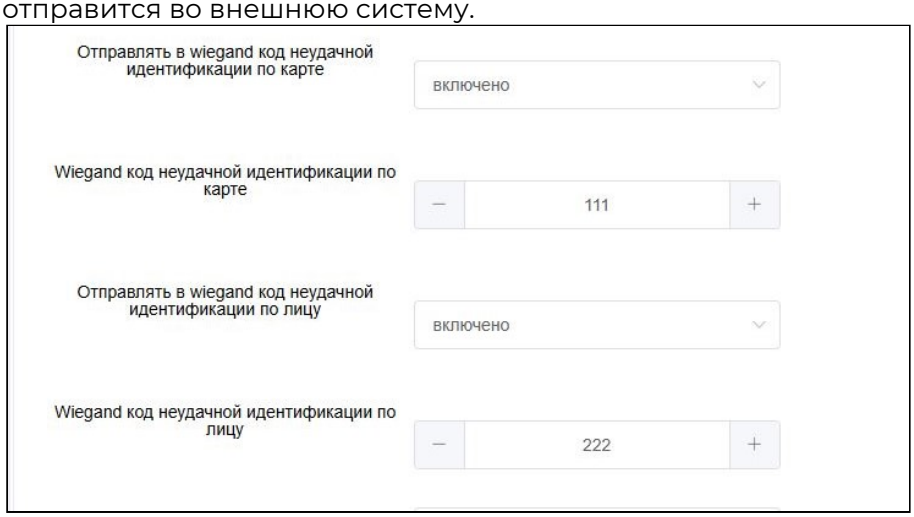
При неуспешной идентификации на внешнее устройство передается код, указанный в настройках веб-интерфейса терминала. Для настройки отправки кода выполните следующие действия:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Система** → вкладка **Компоненты**.
3. В списке выберите конфигурацию, в которую вносятся изменения. Например, **Текущие настройки.** Раскройте компонент, управляющий режимом

работы.



4. Найдите параметр **Отправлять в wiegand код неудачной идентификации по карте** и в выпадающем меню выберите **включено**.
5. В поле **Wiegand код неудачной идентификации по карте** укажите значение, которое отправится во внешнюю систему.



6. **Для других методов идентификации:** Если в терминале активны режимы распознавания по лицу или по венам ладони, установите значения в аналогичных полях.

> Для идентификации по лицу:
>
> - Отправлять в wiegand код неудачной идентификации по лицу
> - Wiegand код неудачной идентификации по лицу
>
> Для идентификации по венам ладони:
>
> - Отправлять в wiegand код неудачной идентификации по венам ладони
> - Wiegand код неудачной идентификации по венам ладони

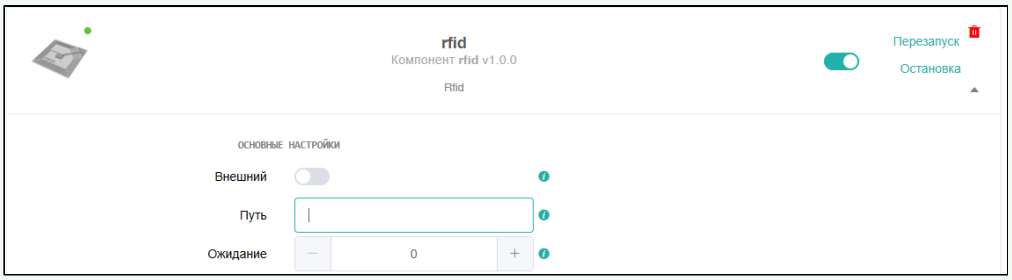
7.2.6 Настройки RFID-карт

Для корректной работы с RFID-картами необходимо согласовать параметры терминала с используемыми картами. Для этого выполните следующие настройки:

1. В поле **Длина карты** укажите длину идентификатора карты в байтах, которую должен считать терминал.
   Например, для карт Mifare Classic 1K длиной 4 байта в поле выберите значение 32.
2. В поле **Формат карты** выберите из выпадающего списка алгоритм обработки данных с карты:

Поле	Описание
UID	– чтение открытого идентификатора карты.
RAW	– чтение данных непосредственно из памяти карты, игнорируя служебные области. Используется для карт инициализированных в стороннем ПО.
UserID	– чтение пользовательских данных из памяти карты с учетом служебной информации. Основной режим для карт, инициализированных непосредственно в Biosmart-Studio.

Если в поле формат карты выбрано значение **RAW**, то войдите в веб-интерфейс терминала. Перейдите в раздел **Система** → вкладка **Компоненты**. В списке выберите конфигурацию (например, **Текущие настройки**). Включите опцию **Режим эксперта** и раскройте компонент **rfid**.



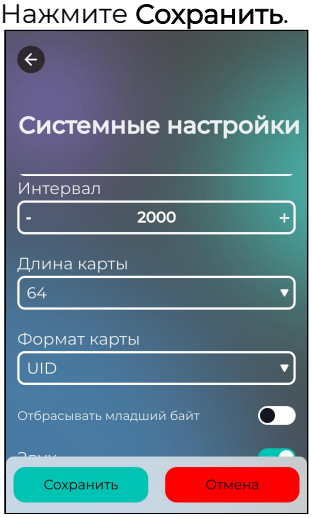
Заполните следующие поля:

- **Auth code** – ключ доступа к защищенной области памяти карты;
- **Card offset** – адрес смещения.

Примените изменения и загрузить конфигурацию на устройство. Для этого нажмите **Применить**. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

3. Включите опцию **Отбрасывать младший байт**, чтобы игнорировать последний байт при чтении идентификатора карты. Используется для совместимости со сторонними системами или картами, где контрольный байт не является частью уникального идентификатора.

4. Нажмите **Сохранить**.



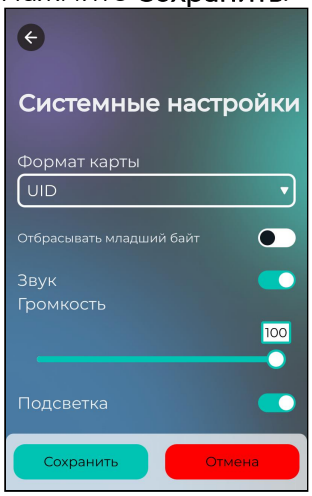
7.2.7 Настройка звука и подсветки

> По умолчанию звук и подсветка включены, а уровень громкости установлен на 65%.

Настройки звука и подсветки можно выполнить через:

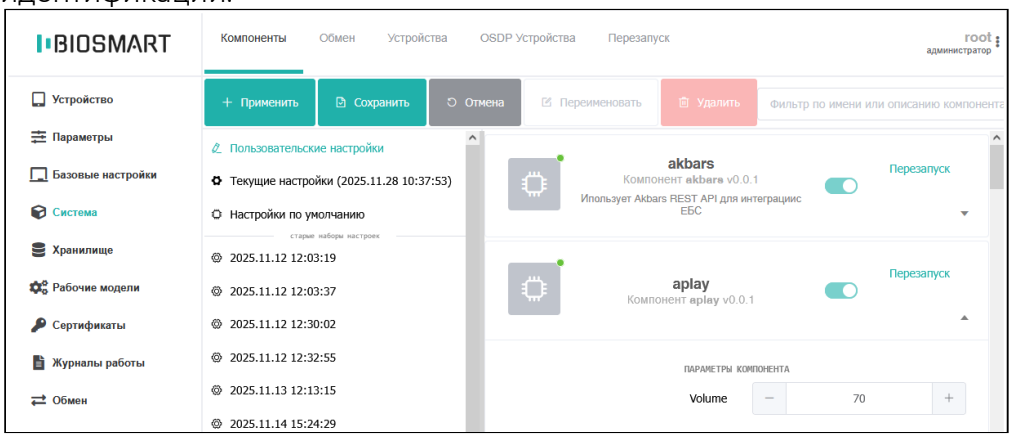
Меню терминала

1. Перейдите в раздел **Настройки → Система**.
2. В открывшемся меню настройте параметры:
   - **Звук:** Включите опцию, чтобы активировать звуковое сопровождение при идентификации.
   - **Громкость:** Отрегулируйте уровень громкости с помощью ползунка.
   - **Подсветка:** Включите опцию для активации светодиодной подсветки по периметру корпуса терминала.
3. Нажмите **Сохранить**.

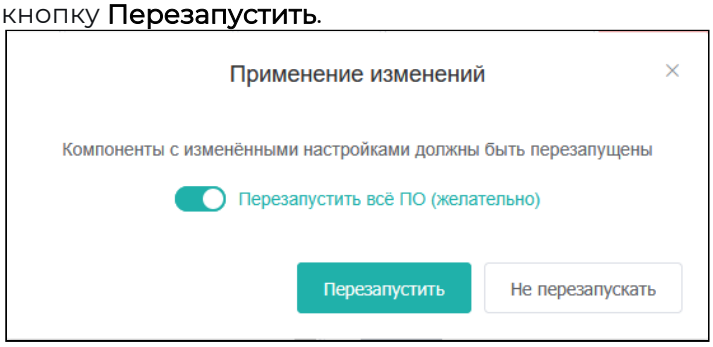


Веб-интерфейс

1. Откройте браузер и введите в адресной строке текущий IP-адрес терминала.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Система** → вкладка **Компоненты**.
4. Найдите компонент **aplay** и раскройте его.
5. В поле **Volume** отрегулируйте уровень громкости звукового сигнала при идентификации.



6. Нажмите **Применить**.
7. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.



7.2.8 Настройка датчика прохода

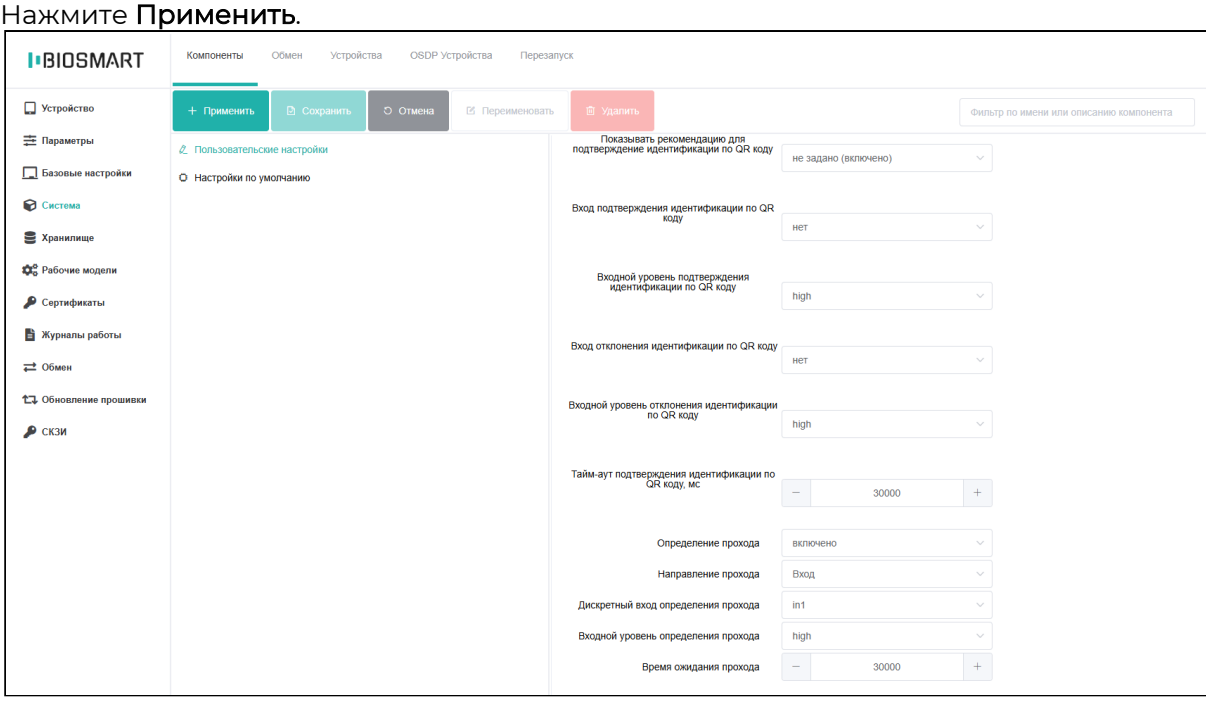
Для контроля прохода сотрудника (вход на объект или выход с объекта) после успешной идентификации может использоваться датчик прохода, подключенный к одному из дискретных входов терминала.

Появление сигнала на дискретном входе расценивается как срабатывание датчика прохода и позволяет контролировать, прошел ли сотрудник через преграждающее устройство (дверь, турникет и др.) после успешной идентификации. Если сотрудник идентифицировался, но не прошел в течение заданного интервала времени, то в ПО Biosmart-Studio v6 будет отправлено событие **Идентификация успешна. Проход не выполнен**, которое не будет учитываться в системе учета рабочего времени.

Для настройки датчика прохода выполните следующие действия:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Система** → вкладка **Компоненты**.

3. Найдите компонент рабочей модели (например, work-model-card-or-face) и раскройте его.
4. Включите параметр **Определение прохода**. После идентификации сотрудника терминал будет ожидать сигнала от датчика прохода.
5. В поле **Направление прохода** выберите значение **Вход** или **Выход**.
6. В поле **Дискретный вход определения прохода** выберите дискретный вход терминала, к которому подключен датчик прохода.
7. В поле **Входной уровень определения прохода** выберите уровень срабатывания дискретного входа.
   Допустимые значения:
   - **high** – приемом сигнала считается появление напряжения на дискретном входе;
   - **low** – приемом сигнала считается пропадание напряжения на дискретном входе.
8. В поле **Время ожидания прохода, мс** укажите время, в течение которого терминал будет ожидать сигнал от датчика прохода.
9. Нажмите **Применить**.



10. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

7.3 Настройка компонентов конфигурации

7.3.1 Описание компонентов конфигурации

Конфигурация терминала состоит из компонентов, каждый из которых отвечает за определенные функции.

> Поля, не описанные здесь, не используются.

Назначение и описание полей компонентов приведено ниже:

akbars

Компонент предназначен для настройки подключения терминала к КБС **Face2**.

Поле	Описание
Token	Данные, предоставляемые КБС.
Server address	
Proxy address	
Scope	
Kbscrypt api key	
Compamy prefix	
Password	
Client id	
Client secret	
Username	
Auth address	

> Описание функциональных возможностей и порядок настройки взаимодействия с *ЕБС*, *КБС* и *региональным сегментом г. Москвы* приведено в инструкции по настройке взаимодействия с биометрическими системами.

aplay

Компонент предназначен для регулировки уровня громкости звукового сигнала при идентификации. По умолчанию установлено значение 65%. Отредактируйте уровень громкости согласно разделу Настройка звука и подсветки.

gui-quasar

Компонент предназначен для изменения оформления и языка в меню терминала.

Поле	Описание
Dark mode	В настоящий момент функция не поддерживается.

Поле	Описание
Main color	Главный цвет в меню терминала. Указывается в формате HEX.
Accent color	Акцентный цвет в меню терминала. Указывается в формате HEX.
Language	Выбор языка на терминале: Русский или Английский.

identifier

Компонент предназначен для выбора параметров идентификации сотрудников.

Поле	Описание
Длина номера карты	Длина идентификатора карты в байтах, которую должен считать терминал. *Например, для карт Mifare Classic 1K длиной 4 байта в поле выберите значение 32.* Доступные значения: 24, 32, 35, 40, 48, 58, 64.
Employee source	Выбор источника данных о сотруднике при идентификации. Для выбора доступны следующие значения: • **studio** – источником данных является ПО Biosmart-Studio v6; • **external** – источником данных является сторонняя система.

ovision

Компонент предназначен для настройки подключения терминала к КБС **OVISION.**

В поле **Server address** автоматически проставится адрес сервера КБС **OVISION** после выполнения настроек в ПО Biosmart-Studio v6.

> Описание функциональных возможностей и порядок настройки взаимодействия с *ЕБС*, *КБС* и *региональным сегментом г. Москвы* приведено в инструкции по настройке взаимодействия с биометрическими системами.

recfaces

Компонент отвечает за работу терминала с КБС **Pridex.**

Поле	Описание
Token	Уникальный идентификатор.
Server address	Путь до сервера КБС в формате http://172.27.10.93.

> Описание функциональных возможностей и порядок настройки взаимодействия с *ЕБС*, *КБС* и *региональным сегментом г. Москвы* приведено в инструкции по настройке взаимодействия с биометрическими системами.

regional

Компонент предназначен для настройки подключения терминала к региональному сегменту г. Москва.

Поле	Описание
Reply timeout	Максимальное время, выделенное на идентификацию. Если по истечении этого времени не будет получен ответ от регионального сегмента, на терминале отобразится сообщение о неуспешной идентификации. Рекомендуемое значение: 10 000 мс.
Camera number	Идентификатор камеры, полученный от РС г. Москвы.
Access mark	Согласованная с КБС метка доступа.
Token	Токен авторизации, полученный от РС г. Москвы.
Address	Адрес для получения основных данных (доступы и профили) от РС г. Москвы.

> Описание функциональных возможностей и порядок настройки взаимодействия с *ЕБС*, *КБС* и *региональным сегментом г. Москвы* приведено в инструкции по настройке взаимодействия с биометрическими системами.

ubs

Компонент предназначен для настройки подключения терминала к ЕБС.

Поле	Описание
Proxy address	Укажите учетные данные, полученные от ЕБС.
Auth token	
Studio token	Токен доступа для обмена информацией между терминалом BioSmart Quasar 7 и ПО Biosmart-Studio v6.
Bestshot url	Укажите учетные данные, полученные от ЕБС.
Stidio address	IP-адрес ПК, на котором установлена серверная часть ПО Biosmart-Studio v6.

Поле	Описание
Tib address	Укажите учетные данные, полученные от ЕБС.

wiegand

Компонент предназначен для изменения настроек интерфейса Wiegand.

Поле	Описание
Type	Битность интерфейса Wiegand. Допустимые значения: 26, 32, 34, 37, 40, 42, 48, 50, 56, 58, 64.
Импульс	Ширина передаваемых импульсов. Рекомендуемое значение 200 мкс.
Интервал	Период следования импульсов. Рекомендуемое значение 2000 мкс.
Fixed direction	Фиксация направления движения сотрудника и передача в стороннюю систему. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Dev 0	Направление передачи данных по интерфейсу Wiegand. Для выбора доступны следующие значения: • **in0** – приём информации от внешних устройств; • **out0** – передача информации от внешних устройств; • **none** – настройка отключена.
Dev 1	Не используется.

work model card or face

Компонент предназначен для управления выбранным режимом работы терминала.

> ⓘ Не рекомендуется изменять параметры режима работы, которые не описаны в таблице ниже.

Поле	Описание
Реле	Включение реле. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено. Включите реле в соответствии с инструкцией в разделе Настройка работы реле.
Таймаут реле, мс	Длительность удержания реле в активированном состоянии.
Тип Wiegand	Битность интерфейса Wiegand. Допустимые значения: 26, 32, 34, 37, 40, 42, 48, 50, 56, 58, 64. Настройте терминал в соответствии с инструкцией в разделе Настройка работы по интерфейсу Wiegand.
Отправлять в wiegand код неудачной идентификации по карте	Включите параметр, чтобы передавать код по интерфейсу Wiegand при неуспешной идентификации по карте. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Wiegand код неудачной идентификации по карте	Код, передаваемый по интерфейсу Wiegand при неудачной идентификации по карте.
Отправлять в wiegand код неудачной идентификации по лицу	Включите параметр, чтобы передавать код по интерфейсу Wiegand при неуспешной идентификации по лицу. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Wiegand код неудачной идентификации по лицу	Код, передаваемый по интерфейсу Wiegand при неудачной идентификации по лицу.

Поле	Описание
Отправлять в wiegand код неудачной идентификации по венам ладони	Включите параметр, чтобы передавать код по интерфейсу Wiegand при неуспешной идентификации по венам ладони. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Wiegand код неудачной идентификации по венам ладони	Код, передаваемый по интерфейсу Wiegand при неудачной идентификации по венам ладони.
Qr code enable	Идентификация сотрудников по QR-кодам. Включите идентификацию по QR-коду согласно инструкции в разделе Настройка идентификации по QR-кодам.
User selects a face modality User selects a palm modality	Выбор модальности. При включении параметров на экране терминала появятся кнопки. Нажатие на одну из них запустит процесс идентификации по выбранному биометрическому фактору. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено. Выберите модальность в соответствии с инструкцией в разделе Выбор режима работы и модальности.
Подтверждение идентификации по карте	Включение или отключение режима ожидания внешнего подтверждения идентификации по карте. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Показывать рекомендацию для подтверждения идентификации по карте	Вывод подсказки пользователю. Если параметр включен, то после идентификации в меню терминала отобразится сообщение «Ожидаем подтверждение идентификации». Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.

Поле	Описание
Вход подтверждения идентификации по карте	Номер дискретного входа терминала, на который сторонний контроллер подаёт сигнал об успешной идентификации и разрешении доступа. В этот момент адаптивная подсветка по периметру корпуса загорается зеленым цветом и включается звуковой сигнал. Допустимые значения: In1 или In2.
Входной уровень подтверждения идентификации по карте	Уровень срабатывания дискретного входа. Допустимые значения: • high – приемом сигнала считается появление напряжения на дискретном входе; • low – приемом сигнала считается пропадание напряжения на дискретном входе.
Вход отклонения идентификации по карте	Номер дискретного входа терминала, на который сторонний контроллер подаёт сигнал о неуспешной идентификации и запрете доступа. В этот момент адаптивная подсветка по периметру корпуса загорается красным цветом и включается звуковой сигнал. Допустимые значения: In1 или In2.
Входной уровень отклонения идентификации по карте	Уровень срабатывания дискретного входа. Допустимые значения: • high – приемом сигнала считается появление напряжения на дискретном входе; • low – приемом сигнала считается пропадание напряжения на дискретном входе.
Тайм-аут подтверждения идентификации по карте, мс	Максимальное время ожидания сигнала от контроллера после успешной идентификации. Задается в миллисекундах.
Подтверждение идентификации по лицу	Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.

Поле	Описание
Показывать рекомендацию для подтверждения идентификации по лицу	Вывод подсказки пользователю. Если параметр включен, то после идентификации в меню терминала отобразится сообщение «Ожидаем подтверждение идентификации». Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Вход подтверждения идентификации по лицу	Номер дискретного входа терминала, на который сторонний контроллер подаёт сигнал об успешной идентификации и разрешении доступа. В этот момент адаптивная подсветка по периметру корпуса загорается зеленым цветом и включается звуковой сигнал. Допустимые значения: **In1** или **In2**.
Входной уровень подтверждения идентификации по лицу	Уровень срабатывания дискретного входа. Допустимые значения: • **high** – приемом сигнала считается появление напряжения на дискретном входе; • **low** – приемом сигнала считается пропадание напряжения на дискретном входе.
Вход отклонения идентификации по лицу	Номер дискретного входа терминала, на который сторонний контроллер подаёт сигнал о неуспешной идентификации и запрете доступа. В этот момент адаптивная подсветка по периметру корпуса загорается красным цветом и включается звуковой сигнал. Допустимые значения: **In1** или **In2**.
Входной уровень отклонения идентификации по лицу	Уровень срабатывания дискретного входа. Допустимые значения: • **high** – приемом сигнала считается появление напряжения на дискретном входе; • **low** – приемом сигнала считается пропадание напряжения на дискретном входе.
Тайм-аут подтверждения идентификации по лицу, мс	Максимальное время ожидания сигнала от контроллера после успешной идентификации. Задается в миллисекундах.

Поле	Описание
Подтверждение идентификации по ладони	Включает или отключает запрос биометрического подтверждения после успешного считывания карты. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Показывать рекомендацию для подтверждения идентификации по ладони	Вывод подсказки пользователю. Если параметр включен, то после идентификации в меню терминала отобразится сообщение «Ожидаем подтверждение идентификации». Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Вход подтверждения идентификации по ладони	Задает номер дискретного входа терминала, на который сторонний контроллер подает сигнал об успешной идентификации и разрешении доступа. В этот момент адаптивная подсветка по периметру корпуса загорается зеленым цветом и включается звуковой сигнал. Допустимые значения: **In1** или **In2**.
Входной уровень подтверждения идентификации по ладони	Уровень срабатывания дискретного входа. Допустимые значения: • **high** – приемом сигнала считается появление напряжения на дискретном входе; • **low** – приемом сигнала считается пропадание напряжения на дискретном входе.
Вход отклонения идентификации по ладони	Номер дискретного входа терминала, на который сторонний контроллер подаёт сигнал о неуспешной идентификации и запрете доступа. В этот момент адаптивная подсветка по периметру корпуса загорается красным цветом и включается звуковой сигнал. Допустимые значения: **In1** или **In2**.
Входной уровень отклонения идентификации по ладони	Уровень срабатывания дискретного входа. Допустимые значения: • **high** – приемом сигнала считается появление напряжения на дискретном входе; • **low** – приемом сигнала считается пропадание напряжения на дискретном входе.

Поле	Описание
Тайм-аут подтверждения идентификации по ладони, мс	Максимальное время ожидания сигнала от контроллера после успешной идентификации. Задается в миллисекундах.
Определение прохода	Включает или отключает прием сигналов на дискретных входах терминала. Параметр используется для настройки работы датчика прохода. Выполните настройку согласно инструкции в разделе Настройка датчика прохода. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Направление прохода	Автоматическая регистрация направления движения сотрудника (вход на объект или выход с объекта) при успешной идентификации на терминале. Допустимые значения: вход или выход. Установите направление прохода одним из способов в соответствии с инструкцией в разделе Выбор направления прохода.
Дискретный вход определения прохода	Дискретный вход устройства, к которому подключен датчик прохода. Сигнал означает, что сотрудник прошёл через преграждающее устройство. Допустимые значения: **in1** или **in2**.
Входной уровень определения прохода	Уровень срабатывания дискретного входа. Допустимые значения: • **high** – приемом сигнала считается появление напряжения на дискретном входе; • **low** – приемом сигнала считается пропадание напряжения на дискретном входе.
Время ожидания прохода	Время, в течении которого терминал будет ожидать сигнал от датчика прохода.

Поле	Описание
Измерение температуры	Включение/отключение измерения температуры сотрудника с помощью **BioSmart Quasar 7 MFR-T, BioSmart Quasar 7 PV-MFR-T.** Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Количество попыток измерения температуры	Количество выполняемых измерений температуры. После завершения измерений вычисляется среднее значение и записывается в журнал событий.
Разрешать проход при низкой температуре	Параметр определяет предоставлять или нет доступ сотрудникам, у которых измеренное значение температуры окажется ниже *минимально допустимого значения*. Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Разрешать проход при высокой температуре	Параметр определяет предоставлять или нет доступ сотрудникам, у которых измеренное значение температуры окажется выше *максимального допустимого значения*. Если переключатель **Разрешить проход при высокой температуре** включен, то при превышении заданного максимального допустимого значения температуры тела доступ будет разрешен, в ПО Biosmart-Studio v6 будет зафиксировано событие **Превышение температуры, доступ разрешен.** Для выбора доступны следующие значения: • не задано (отключено); • включено; • отключено.
Время измерения температуры, мс	Время, в течении которого терминал будет проводить измерение температуры. Задается в миллисекундах.
Минимально допустимая температура, °C	Минимально допустимая температура сотрудника.
Максимально допустимая температура, °C	Максимально допустимая температура сотрудника.

7.3.2 Настройка внешнего подтверждения доступа

В разделе приведен порядок настройки взаимодействия терминала со сторонним контроллером доступа (например, Elsys).

В этом режиме терминал выполняет идентификацию или верификацию (по карте, лицу или ладони) и отправляет номер карты пользователя на контроллер по интерфейсу Wiegand. Окончательное решение о доступе принимается контроллером на основе своих баз данных и правил, а результат передаётся обратно на терминал через дискретные входы.

Такая модель работы позволяет добавить идентификацию по биометрическим данным в систему, где ранее идентификация выполнялась только по RFID-картам без замены всей инфраструктуры.

Для настройки внешнего подтверждения выполните следующие настройки:

1. Установите настройки в меню терминала

Откройте в меню терминала **Настройки** → **Система**. В поле **Режим** выберите значение в зависимости от условий работы:

- для двухфакторной идентификации – **Карта и ладонь**;
- для идентификации по одному фактору – **Лицо или ладонь**.

Для режима **Лицо или ладонь** разверните список **Выбор модальности** и проверьте, что опция **Лицо** включена, опция **Ладонь** выключена.

Раскройте настройки Wiegand. В поле **Wiegand 0** установите значение **out**. Это активирует передачу данных с терминала на внешние устройства (например, контроллер СКУД).

В выпадающем меню поля **Режим** выберите битность интерфейса Wiegand.

> Битность должна соответствовать формату ваших карт. Если битность выбрана неправильно, номер карты будет обрезан или передан некорректно.

Включите опцию **Отбрасывать младший байт**, чтобы игнорировать последний байт при чтении идентификатора карты.

Нажмите **Сохранить**.

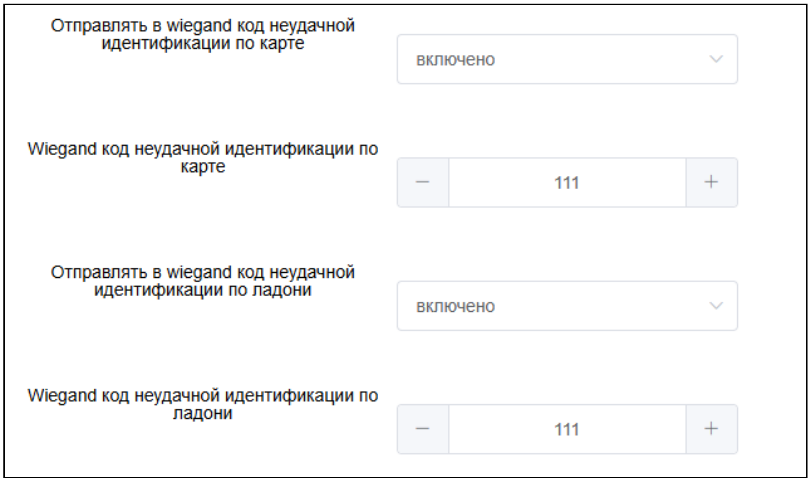
2. Настройте отправку кода по интерфейсу Wiegand при неудачной идентификации

Выполните вход в веб-интерфейс терминала. Перейдите в раздел **Система** → вкладка **Компоненты**.

В списке выберите конфигурацию (например, **Текущие настройки**). Раскройте компонент, управляющий режимом работы.

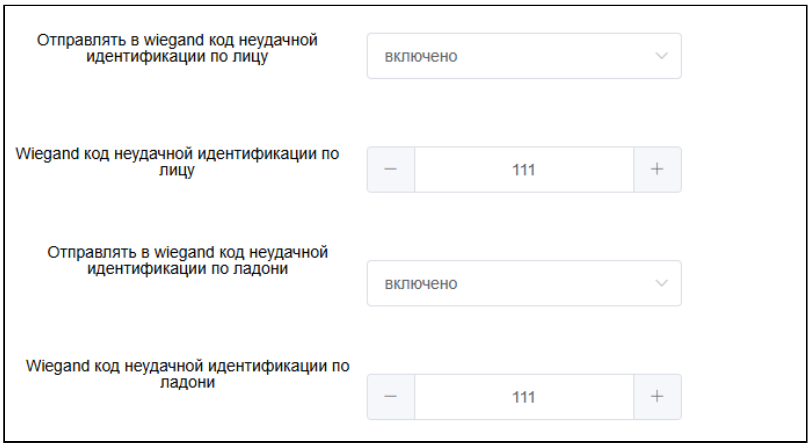
Включите передачу кода о неуспешной идентификации на сторонний контроллер.

Для режима **Карта и ладонь** установите значения в полях согласно изображению ниже.



При неуспешной идентификации по первому или второму фактору терминал отправит на контроллер код 111. Доступ сотруднику предоставлен не будет.

Для режима **Лицо или ладонь** установите значения в полях согласно изображению ниже.



При неуспешной идентификации по одному из факторов терминал отправит на контроллер код 111. Доступ сотруднику предоставлен не будет.

Подробное описание параметров приведено в разделе Описание компонентов конфигурации.

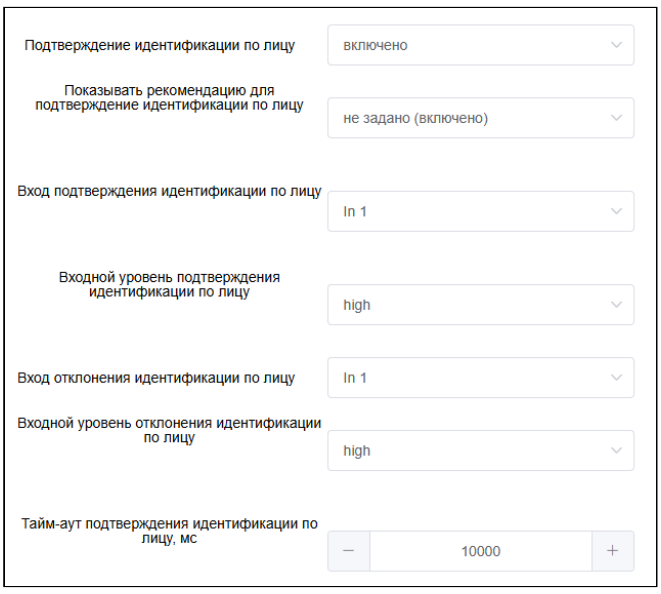
3. Настройка дискретных входов терминала

Настройте дискретные входы для приёма сигналов от контроллера. Если в течение заданного времени на них не поступит сигнал, терминал отобразит сообщение **Идентификация не подтверждена,** светодиодная подсветка по периметру корпуса загорится красным цветом и сработает звуковой сигнал.

Для режима **Карта и ладонь** установите значения в полях согласно изображению ниже.

Если сотруднику разрешен доступ, то контроллер отправит сигнал на дискретный вход In1 и светодиодная подсветка по периметру корпуса загорится зеленным цветом и сработает звуковой сигнал. Если подать сигнал на In2, то получим сообщение **Идентификация не подтверждена** с красной рамкой и звуковым сигналом.

Для режима **Лицо или ладонь** установите значения в следующих полях:



Если сотруднику по одному из идентификаторов разрешен доступ, то контроллер отправит сигнал на дискретный вход In1 и светодиодная подсветка по периметру корпуса загорится зеленным цветом и сработает звуковой сигнал. Если подать сигнал на In2, то получим сообщение **Идентификация не подтверждена** с красной рамкой и звуковым сигналом

Нажмите **Применить**. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

4. Настройте сторонний контроллер

Сторонний контроллер настройте на прием данных по интерфейсу Wiegand согласно рекомендациям в соответствующих руководствах.

7.4 Работа с данными о сотрудниках

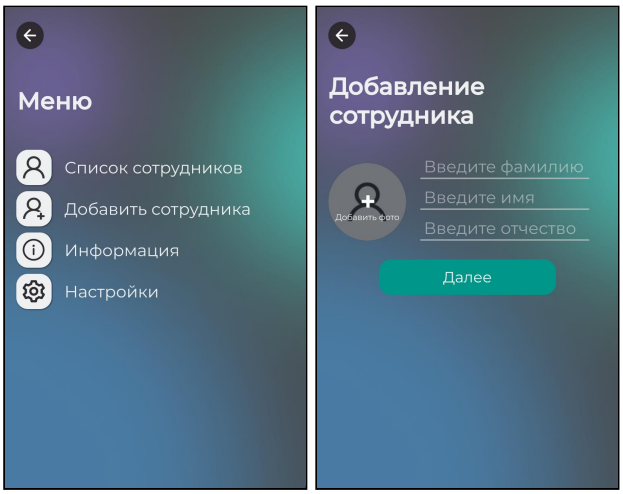
7.4.1 Добавление сотрудников

Добавить сотрудников на терминал можно следующими способами: через меню терминала или с использованием ПО Biosmart-Studio v6.

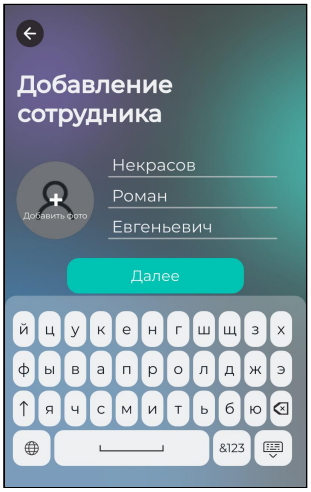
> Для работы с большой базой данных предпочтительно добавлять сотрудников через ПО Biosmart-Studio v6.

Добавление сотрудника через меню терминала

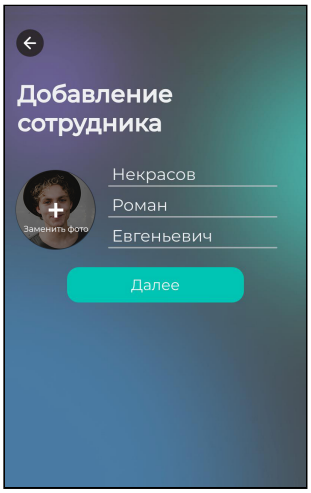
Для создания нового сотрудника войдите в меню терминала и нажмите **Добавить сотрудника**.



Укажите **Фамилию**, **Имя** и **Отчество**.

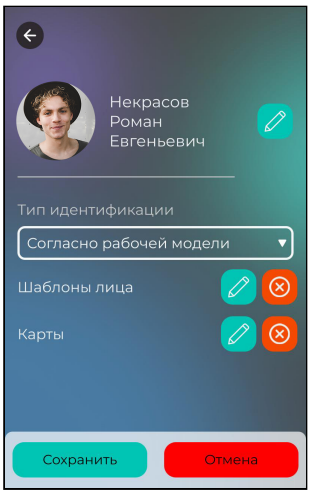


При необходимости добавьте фотографию сотрудника. Для этого нажмите **Добавить фото**, затем **Сделать фото**.



Нажмите **Далее**.

Откроется карточка сотрудника со следующими кнопками:



Кнопка	Описание
	– редактирование ФИО, добавление/редактирование фотографии сотрудника
	– добавление биометрических шаблонов, номера RFID-карты
	– удаление биометрических шаблонов, номера RFID-карты

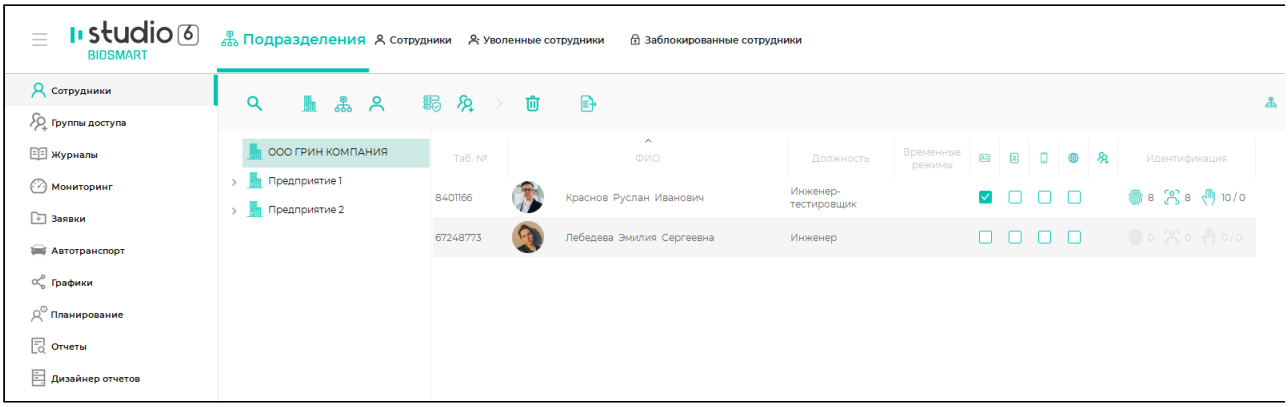
Зарегистрировать идентификаторы сотрудника можно позже согласно разделу Регистрации идентификаторов сотрудников.

Нажмите кнопку **Сохранить**.

Сотрудник будет добавлен в список сотрудников на терминале и автоматически передан в ПО Biosmart-Studio v6, где он будет сохранён в подразделении по умолчанию. После добавления сотрудника зайдите в ПО Biosmart-Studio v6 и измените/дополните сведения о сотруднике, переместите в подразделение, в котором он будет числиться в дальнейшем.

Добавление сотрудников с помощью ПО Biosmart-Studio v6

Откройте ПО Biosmart-Studio v6, перейдите в раздел **Сотрудники** → выберите предприятие/подразделение из списка или создайте новое (см. раздел Добавление предприятия и подразделения Руководства пользователя ПО Biosmart-Studio v6).



Нажмите кнопку **Добавить сотрудника** на панели инструментов. Заполните карточку сотрудника (см. раздел Добавление сотрудника Руководства пользователя ПО Biosmart-Studio v6).

Для передачи данных сотрудника на терминал:

1. В разделе **Группы доступа** выберите группу, в блоке **Назначенные сотрудники** нажмите **Изменить** и добавьте нужного сотрудника.
2. Затем для этой же группы в списке объектов доступа отметьте терминал и нажмите **Сохранить**.

7.4.2 Регистрации идентификаторов сотрудников

Терминал **BioSmart Quasar 7** поддерживает идентификацию сотрудников с использованием следующих идентификаторов:

- лицо (*соответствует требованиям 572-ФЗ*);
- RFID-карты и смартфон;
- рисунок вен ладони.

> ⓘ Идентификации по рисунку вен ладони возможна на терминалах BioSmart Quasar 7 PV-MFR, BioSmart Quasar 7 PV-MFR-T.

Заказчик может самостоятельно выбрать предпочтительный способ идентификации. В следующих разделах описаны правила и порядок регистрации, идентификации, изменения и удаления идентификаторов.

Регистрация шаблонов лиц

> ✅ Процедура регистрации лица зависит от обязанности вашей организации передавать данные в Единую биометрическую систему (ЕБС).
>
> Перед началом регистрации определите, к какой категории относится ваша организация. Это влияет на порядок действий, получаемые согласия и функционал терминала.

Регистрация данных с передачей в ЕБС

Согласно требованиям федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных» идентификация по биометрическим данным (лицо, голос) может производиться только в единой биометрической системе (**ЕБС**), в том числе в ее региональных сегментах, и коммерческих биометрических системах (**КБС**).

- **ЕБС** — это государственная информационная система, обеспечивающая сбор биометрических персональных данных, их хранение и использование для аутентификации и идентификации пользователей.
- **КБС** — это аккредитованная информационная система, выполняющая биометрическую аутентификацию. Особый статус ее компании-владельца позволяет правомерно осуществлять обработку биометрических персональных данных в собственной инфраструктуре без прямого взаимодействия с **ЕБС**.
- **Региональный сегмент ЕБС** — это часть Единой Биометрической Системы, которая собирает, хранит и обрабатывает биометрические данные пользователей для нужд конкретного региона. С 1 сентября 2024 года на территории города Москвы действует Региональный сегмент ЕБС (ПП № 1151 от 26.08.2024 г.).

ПО Biosmart-Studio v6 совместно с терминалом **BioSmart Quasar 7** позволяет организовать работу СКУД в соответствии с федеральным законом №572-ФЗ от 29.12.2022г.

ⓘ Для работы ПО Biosmart-Studio v6 с *ЕБС*, *КБС* или *Региональным сегментом г.Москвы* необходимо наличие соответствующей лицензии:

- «Интеграция с ЕБС»
- «Интеграция с КБС»
- «Интеграция с РС г.Москва»

✅ При регистрации сотрудника в ПО Biosmart-Studio v6 система сгенерирует индивидуальную ссылку, QR-код для предоставления сотрудником согласия на обработку персональных данных через портал «Госуслуги».

Сотруднику необходимо:

1. Отсканировать полученный QR-код или перейти по полученной на почту ссылке.
2. Дать своё согласие.

Способы сдачи биометрических данных

Способ 1. Дистанционно, через приложение Госуслуги Биометрия

1. Скачайте официальное приложение:
   - App Store (для iOS);
   - Google Play (для Android).
2. Пройдите сканирование биометрических данных в приложении.

Способ 2. Очно, в отделении банка

1. Обратитесь в отделение банка (адреса отделений банков расположены на сайте ebs.ru).
2. Пройдите процедуру сдачи биометрических данных в отделении.

Порядок работы с биометрическими системами описан в инструкции Интеграция BioSmart с биометрическими системами.

Регистрация данных для внутреннего использования

В разделе описан порядок регистрации биометрических шаблонов лиц, если организация **не обязана** передавать биометрические данные в ЕБС.

Зарегистрировать шаблоны можно разными способами:

- на терминале;
- с помощью ПО Biosmart-Studio v6.

Лучшее качество шаблонов достигается при регистрации на терминале или с помощью терминала по команде от ПО Biosmart-Studio v6.

Допускается регистрация с помощью веб-камеры или по фотографии, но качество шаблонов может оказаться недостаточным для стабильно успешной идентификации

некоторых сотрудников. В таком случае придётся повторить регистрацию одним из других способов.

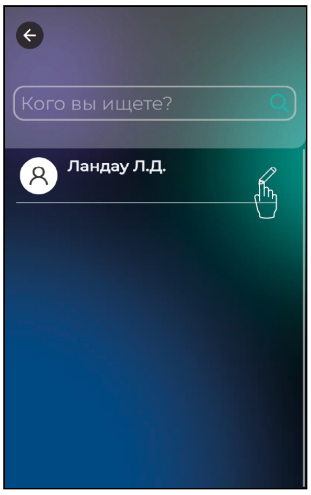
Правила регистрации биометрических шаблонов лиц на терминале

Для обеспечения высокого качества биометрического шаблона, при регистрации соблюдайте следующие условия:

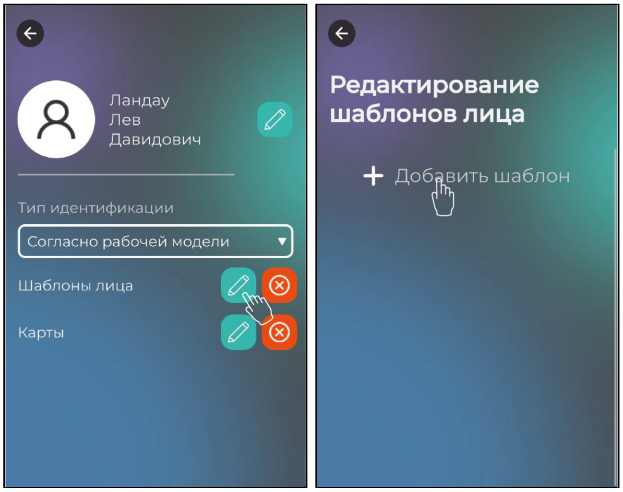
1. Рекомендуемый уровень освещенности в зоне регистрации — от 100 до 150 люкс. Избегайте резких теней на лице и прямых лучей света, направленных в камеру.
2. Расстояние между терминалом и сотрудником около 80 – 100 см. В кадр должно попасть лицо и верхняя часть плеч, расположенные по центру экрана.
3. Голову следует держать прямо, без наклонов и поворотов. Взгляд должен быть направлен на объектив камеры в верхней части терминала.
4. Выражение лица нейтральное.
5. Лицо сотрудника не должны закрывать волосы, головные уборы, солнцезащитные очки и иные аксессуаров.

Регистрация шаблонов лица на терминале

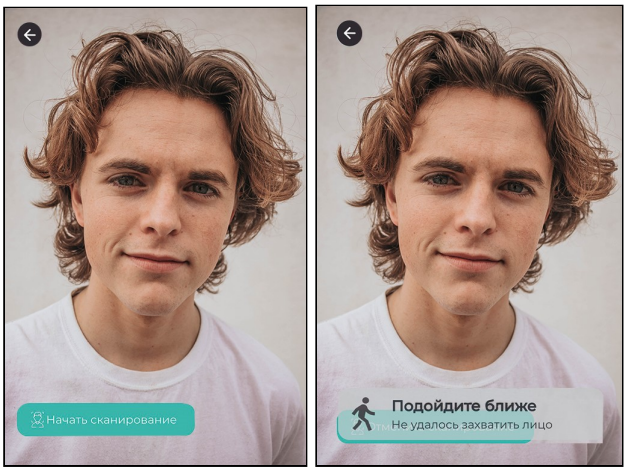
Войдите в меню терминала → нажмите **Список сотрудников** → выберите сотрудника в списке.



В строке **Шаблоны лица** нажмите кнопку редактирования, затем **Добавить шаблон**.

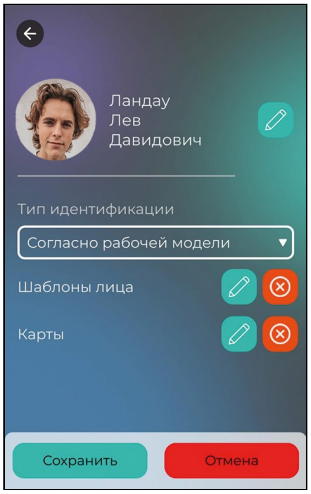


Встаньте перед камерой согласно правилам выше, нажмите **Начать сканирование**. При необходимости во время сканирования будут появляться подсказки.



Чтобы завершить сканирование, нажмите **Закончить**. За одно сканирование создаётся 4 биометрических шаблона. Для добавления новых нажмите **Добавить ещё**.

Чтобы сохранить изменения нажмите **Сохранить**.

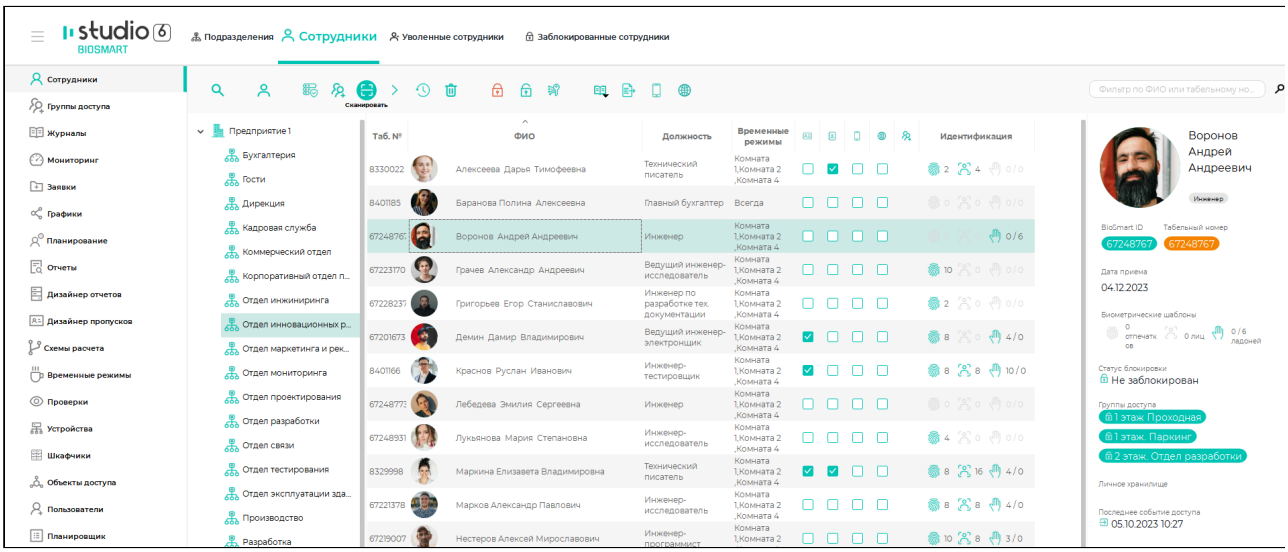


Регистрация с помощью ПО Biosmart-Studio v6

Зарегистрировать шаблоны можно разными способами:

- на терминале по команде от ПО Biosmart-Studio v6 (способ доступен только для версии встроенного ПО 2.4);
- из файла (см. раздел Сканирование лица Руководства пользователя Biosmart-Studio v6);
- на веб-камере (см. раздел Сканирование лица Руководства пользователя Biosmart-Studio v6).

Выполните вход в ПО Biosmart-Studio v6 → откройте раздел **Сотрудники** → выберите сотрудника → нажмите кнопку **Сканировать.**



В окне **Сканирование** перейдите на вкладку **Лица** → выберите устройство **BioSmart Quasar 7** → нажмите кнопку **Добавить.** После этого на терминале откроется окно сканирования. Дальнейший процесс аналогичен процедуре, описанной в разделе Регистрация шаблонов лица на терминале.

Регистрация шаблонов ладоней

Исполнения терминала **BioSmart Quasar 7 PV-MFR**, **BioSmart Quasar 7 PV-MFR-T** поддерживают идентификацию сотрудников по венам ладони. В разделе описан порядок регистрации биометрических шаблонов ладоней.

Зарегистрировать шаблоны можно разными способами:

- на терминале;
- с помощью терминала по команде ПО Biosmart-Studio v6;
- с помощью настольного считывателя BioSmart AirPalm (см. раздел Сканирование вен ладоней ПО Biosmart-Studio v6).

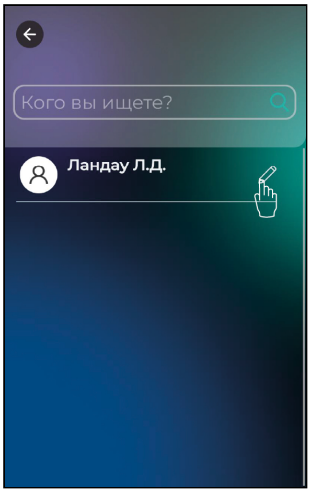
Правила регистрации биометрических шаблонов ладоней на терминале

Для обеспечения высокого качества биометрического шаблона, при регистрации соблюдайте следующие условия:

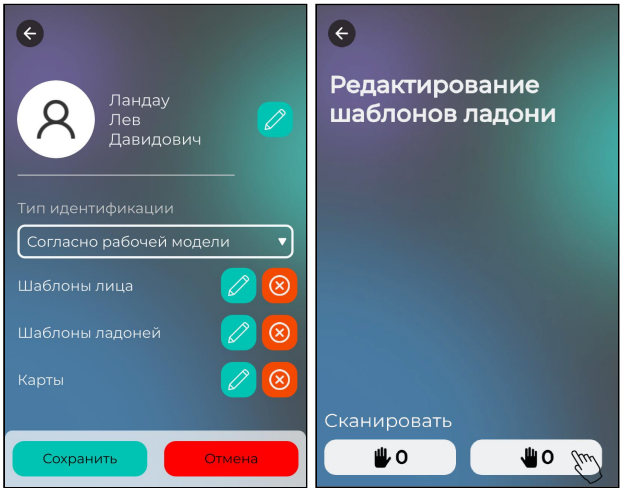
1. Расстояние ладони до сканера 50-80 мм.
2. Чистая и сухая ладонь.
3. Рука должна быть расслабленной, ладонь плоской и открытой, пальцы естественно разведены.
4. Центр ладони должен быть совмещен с целевой маркировкой на сканере (на корпусе нарисован белый квадратный контур).

Регистрация шаблонов ладоней на терминале

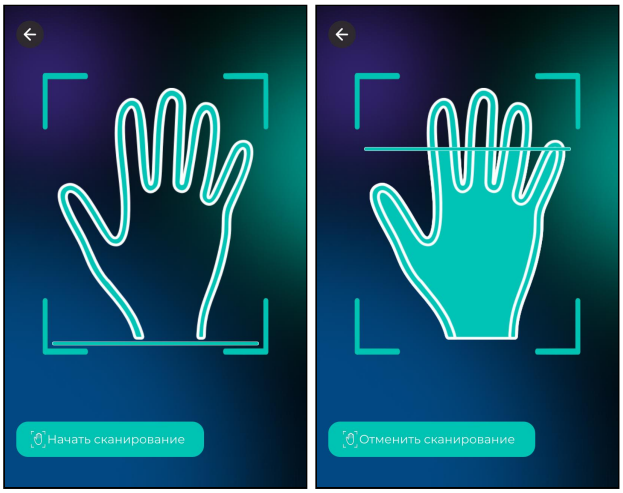
Войдите в меню терминала → нажмите **Список сотрудников** → выберите сотрудника в списке.



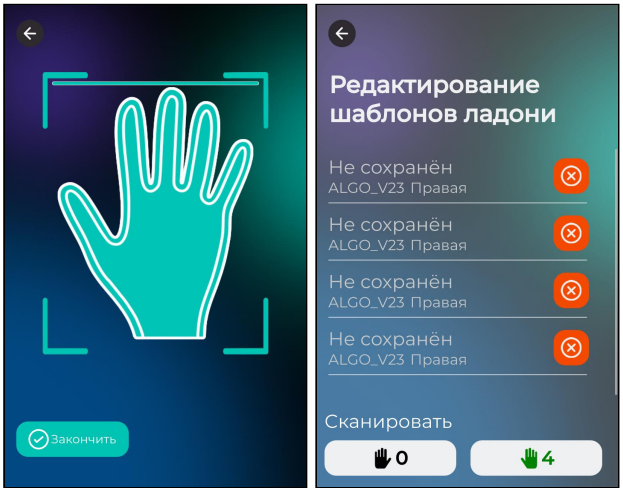
В строке **Шаблоны ладоней** нажмите кнопку **Редактировать** и выберите ладонь для регистрации.



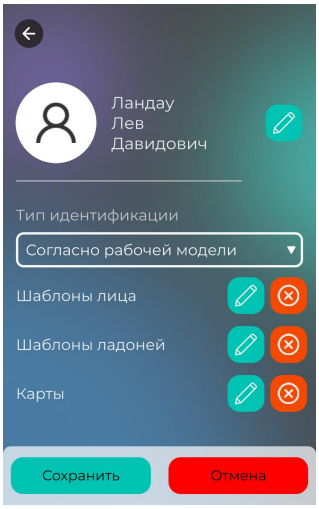
Нажмите **Начать сканирование** и поднесите ладонь к сканеру. При необходимости во время сканирования будут появляться подсказки.



После завершения сканирования нажмите **Закончить**. За одно сканирование создаётся 4 биометрических шаблона. Для добавления новых нажмите на изображение правой или левой ладони внизу экрана.

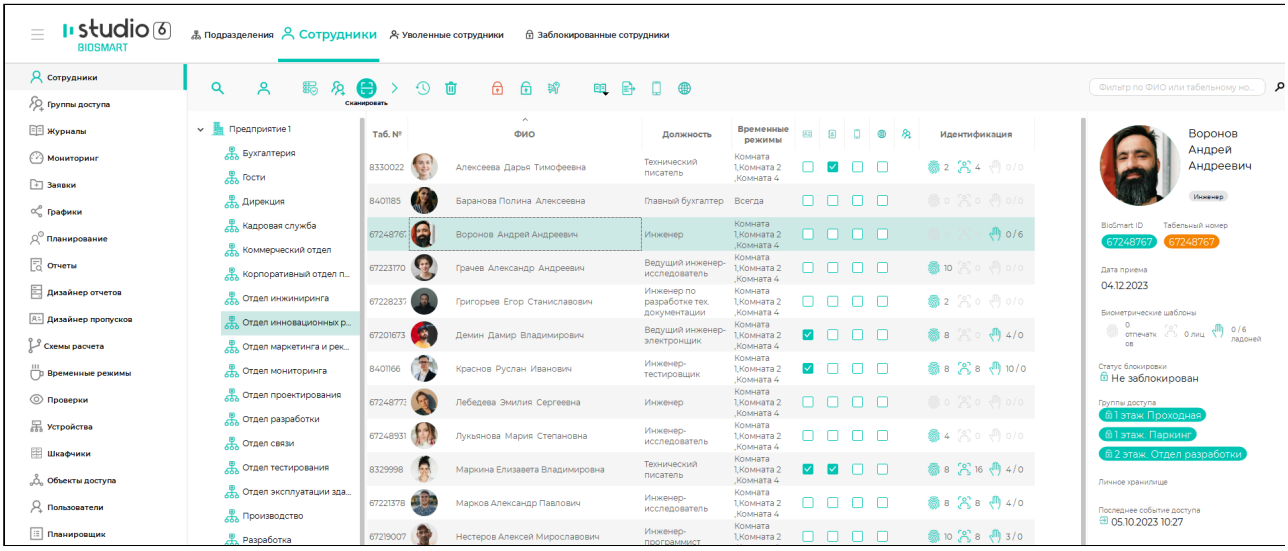


Вернитесь в карточку сотрудника и сохраните изменения нажав **Сохранить**.



Регистрация с помощью ПО Biosmart-Studio v6

Выполните вход в ПО Biosmart-Studio v6 → откройте раздел **Сотрудники** → выберите сотрудника → нажмите кнопку **Сканировать.**



В окне **Сканирование** перейдите на вкладку **Ладони** → выберите устройство **BioSmart Quasar 7** → нажмите кнопку **Добавить.** После этого на терминале откроется окно сканирования. Дальнейший процесс аналогичен процедуре, описанной в разделе Регистрация шаблонов ладоней на терминале.

Работа с RFID-картами

Зарегистрировать RFID-карту можно разными способами:

- с помощью настольного считывателя ACR1252U;
- на терминале.

Если для идентификации будут использоваться карты в защищенных режимах (например, Mifare Plus SL1 и SL3), рекомендуется регистрировать идентификаторы в системе с помощью настольного считывателя ACR1252U (см. раздел Регистрация RFID-карты с помощью настольного считывателя).

Регистрация RFID-карты с помощью настольного считывателя

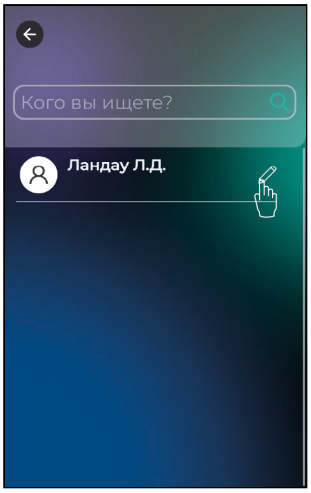
Для перевода карты в защищенный режим и регистрации идентификатора сотрудника в системе, выполните следующие действия:

1. Создайте профиль смарткарт (см. раздел Профили смарткарт Руководства пользователя ПО Biosmart-Studio v6).
2. Откройте раздел **Сотрудники** → выберите сотрудника → нажмите кнопку **Свойства** на панели инструментов → перейдите на вкладку **Карты**.
3. Нажмите кнопку **Добавить карту сотруднику**.
4. Убедитесь, что настольный считыватель ACR1252U подключён к ПК, и выберите его в выпадающем списке.
5. В поле **Профиль для записи смарткарт** выберите ранее созданный профиль.
6. Нажмите кнопку **Считать**.
7. Поднесите карту к считывателю и нажмите кнопку **Записать UID сотрудника на карту**. Следуйте дальнейшим указаниям системы.
8. Карта переведена в выбранный режим безопасности и назначена сотруднику. В память карты записан UID сотрудника и ключ доступа к защищенной области.

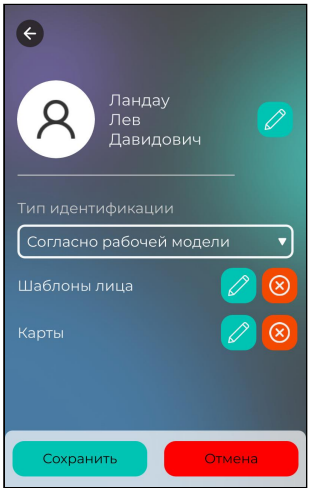
Регистрация RFID-карты на терминале

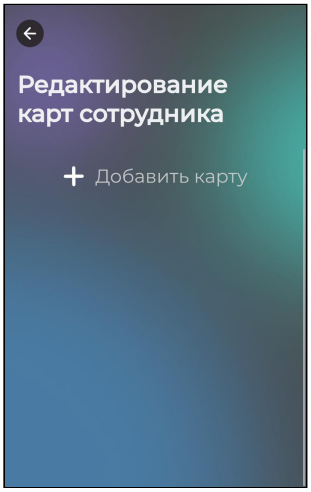
> Перед использованием карт в защищенных режимах в качестве идентификаторов убедитесь, что они были предварительно инициализированы.

Войдите в меню терминала → нажмите **Список сотрудников** → выберите сотрудника в списке.

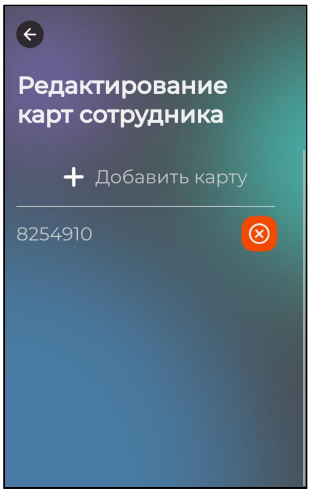


В строке **Карты** нажмите кнопку **Редактировать**, затем **Добавить карту**. Следуйте подсказкам на экране.





После завершения сканирования карта отобразится в списке карт сотрудника. Вернитесь в карточку сотрудника и сохраните изменения нажав **Сохранить**.



Правила идентификации сотрудников

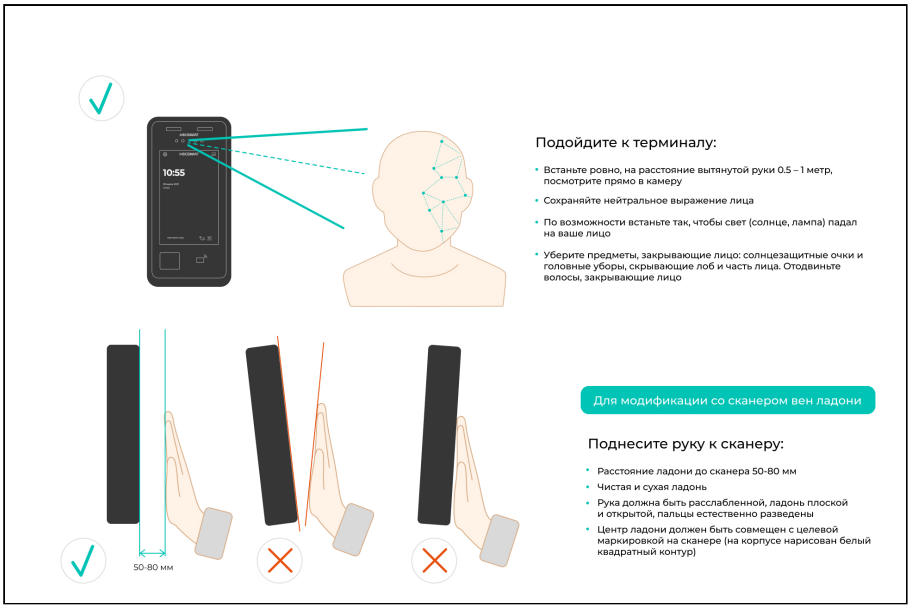
Идентификация по лицу

Рекомендации для идентификации по лицу

Для обеспечения качественной идентификации соблюдайте следующие условия:

1. Минимально допустимый уровень освещенности в зоне идентификации — 50 люкс.
2. Встаньте прямо на расстоянии 0,5 – 1 метра от терминала и смотрите в объектив камеры или на экран терминала.
3. Не наклоняйте голову сильно вниз, вверх или в сторону. Сохраняйте нейтральное выражение лица.
4. Проверьте, что лицо не закрыто волосами, головными уборами, солнцезащитными очками и иными аксессуарами.

Если идентификация не удалась с первой попытки, сделайте шаг назад, вернитесь на исходную позицию и повторите процедуру. Следуйте инструкциям на экране.

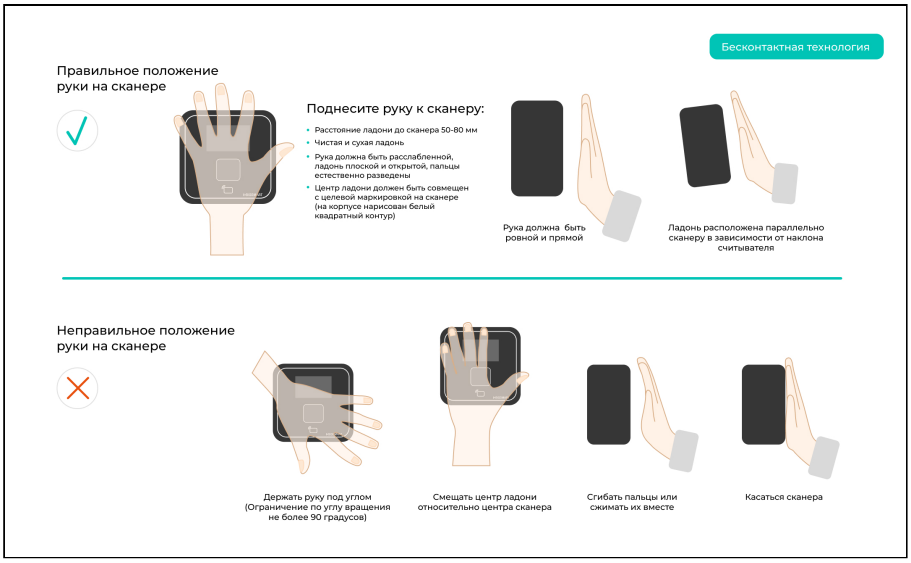


Идентификация по рисунку вен ладони

Рекомендации для идентификации по венам ладони

Для обеспечения высокого качества биометрического шаблона, при регистрации соблюдайте следующие условия:

1. Расстояние ладони до сканера 50-80 мм.
2. Чистая и сухая ладонь.
3. Рука должна быть расслабленной, ладонь плоской и открытой, пальцы естественно разведены.
4. Центр ладони должен быть совмещен с целевой маркировкой на сканере (на корпусе нарисован белый квадратный контур).

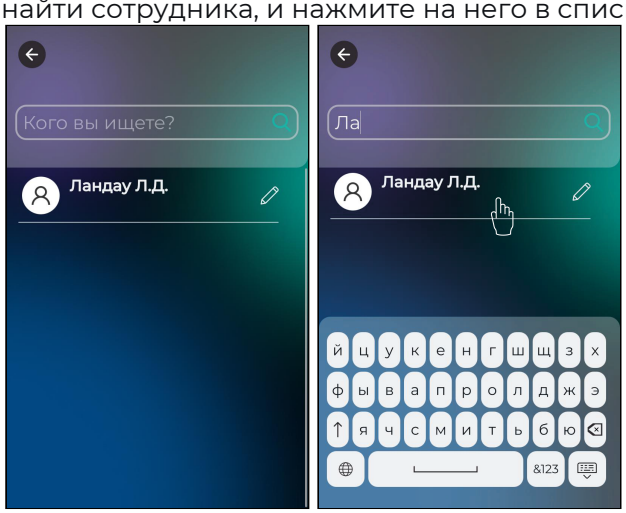


7.4.3 Удаление идентификаторов сотрудников

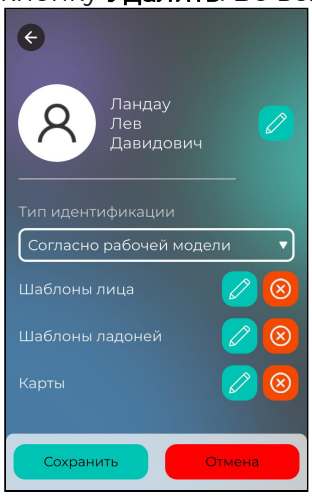
Для удаления идентификаторов сотрудника через меню терминала выполните следующие действия:

1. Войдите в меню терминала.

2. Перейдите в раздел **Список сотрудников**. Воспользуйтесь поисковой строкой, чтобы найти сотрудника, и нажмите на него в списке.

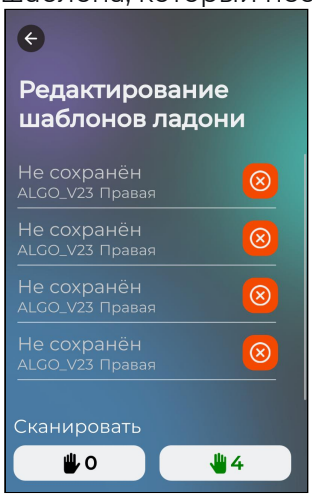


3. Для удаления **всех** биометрических шаблонов/номеров карт назначенных сотруднику в строке **Шаблоны лица/Шаблоны ладоней/Карты** нажмите кнопку **Удалить**. Во всплывающем окне подтвердите удаление.



4. Для удаления каждого биометрического шаблона/карты отдельно в строке **Шаблоны лица/Шаблоны ладоней/Карты** нажмите кнопку **Редактировать.**

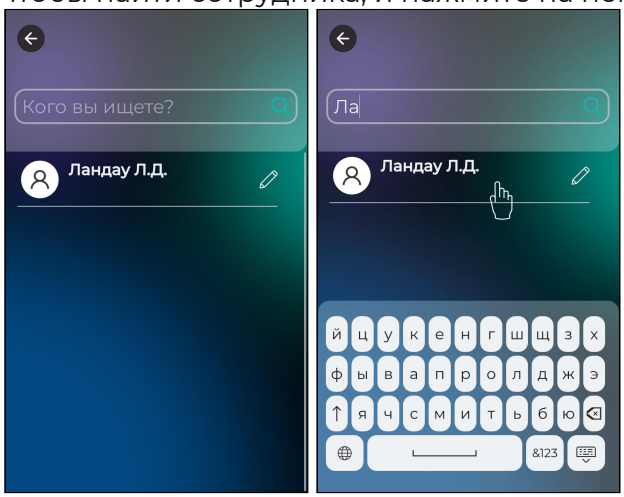
5. Откроется перечень всех шаблонов. Нажмите кнопку **Удалить** напротив каждого шаблона, который необходимо удалить.



7.4.4 Редактирование данных о сотрудниках

Для изменения данных о сотруднике через меню терминала выполните следующие действия:

1. Выполните вход в меню терминала.
2. Перейдите в раздел **Список сотрудников**. Воспользуйтесь поисковой строкой, чтобы найти сотрудника, и нажмите на него в списке.



3. Отредактируйте данные сотрудника с помощью кнопок.

Кнопка	Описание
	– редактирование ФИО, добавление/редактирование фотографии сотрудника.

Кнопка	Описание
———	– добавление биометрических шаблонов, номера RFID-карты (см. раздел Регистрации идентификаторов сотрудников).
	– удаление биометрических шаблонов, номера RFID-карты (см. раздел Удаление идентификаторов сотрудников).

7.5 Управление конфигурацией терминала

Веб-интерфейс терминала позволяет сэкономить время при работе с большим количеством устройств. Настройте конфигурацию на одном терминале, скачайте файл и используйте его для быстрой настройки остальных.

Включите опцию **Сохранять настройки устройств**, чтобы при каждом изменении конфигурации текущие настройки сохранялись.

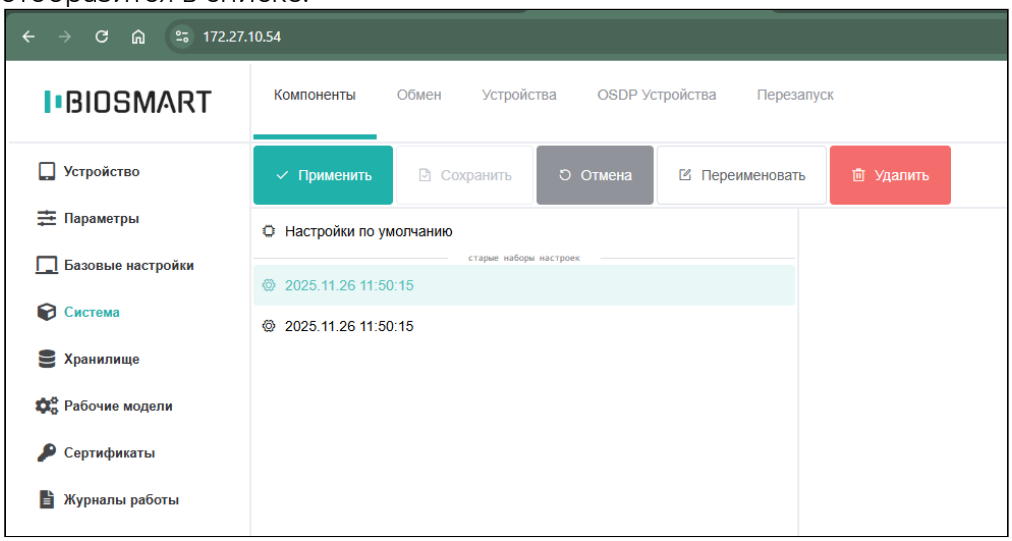
7.5.1 Экспорт конфигурации терминала

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Система** → вкладка **Обмен**.
3. Чтобы скачать одну конфигурацию, выберите ее из списка и нажмите кнопку **Скачать текущую конфигурацию**.
4. Чтобы скачать все конфигурации, нажмите **Скачать все наборы конфигураций**.
5. Заархивированные файлы конфигураций появятся в папке загрузок вашего ПК.

7.5.2 Импорт конфигурации на терминал

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Система** → вкладка **Обмен**.
3. Переместите файл конфигурации в область **Заливка настроек на устройство** или нажмите на нее, чтобы воспользоваться диалоговым окном для выбора файла.

4. После завершения загрузки перейдите на вкладку **Компоненты.** Конфигурация отобразится в списке.



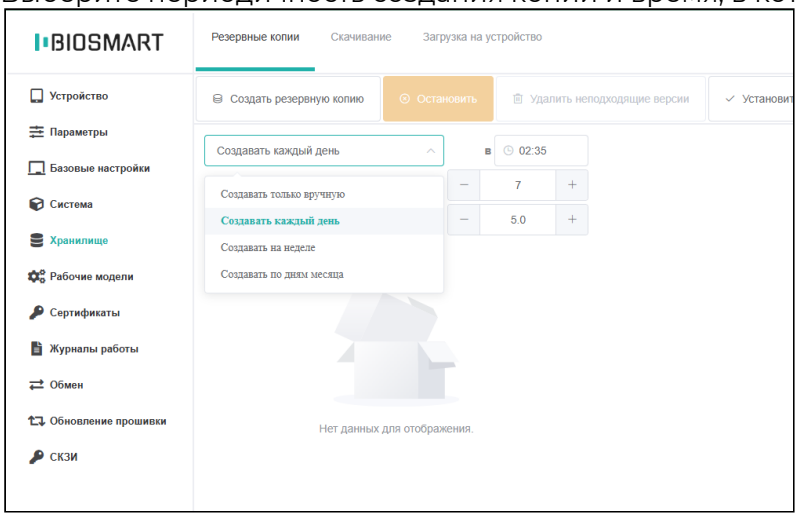
5. Нажмите кнопку **Применить**.

7.6 Управление базой данных терминала

Раздел предназначен для настройки правил резервного копирования, экспорта и импорта базы данных терминала.

7.6.1 Настройка правил резервного копирования

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Хранилище** → вкладка **Резервные копии**.
3. Выберите периодичность создания копий и время, в которое они будут сохраняться.



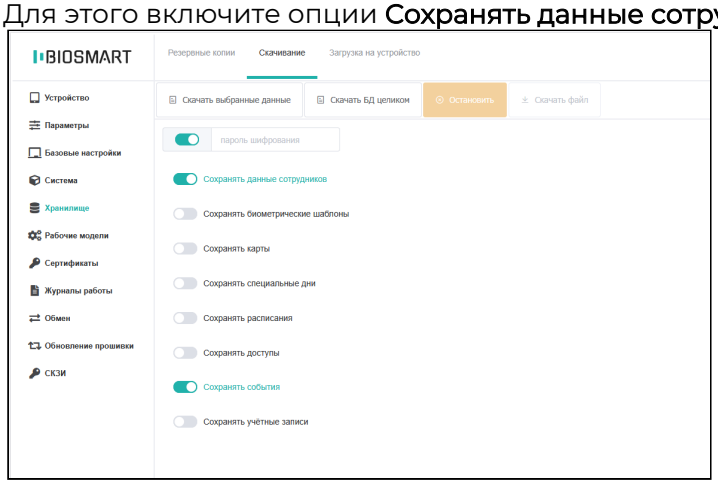
4. В поле **Хранить последних копий** укажите какое количество резервных копий будет сохраняться.

5. В поле **Максимальный размер всех копий (в ГиБ)** задайте максимальный суммарный размер для всех копий.
6. Для сохранения изменений нажмите **Установить**.

> Для создания резервной копии вручную нажмите кнопку **Создать резервную копию** на панели инструментов.

7.6.2 Экспорт базы данных терминала

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Хранилище** → вкладка **Скачивание**.
3. Выберите данные, которые будут сохраняться. Например, события и данные сотрудников.
   Для этого включите опции **Сохранять данные сотрудников** и **Сохранять события**.



4. Скачайте выбранные данные, нажав кнопку **Скачать выбранные данные**.

> Для скачивания базы данных целиком нажмите кнопку **Скачать БД целиком**.

7.6.3 Импорт базы данных терминала

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **Хранилище** → вкладка **Загрузка на устройство**.
3. Перетащите файл с базой данных в выделенную область с текстом «Поместите скаченные файлы БД в это поле...» или кликните на эту область, чтобы открыть стандартный диалог выбора файла в вашей операционной системе, и найдите нужный файл.

7.7 Настройка СКЗИ

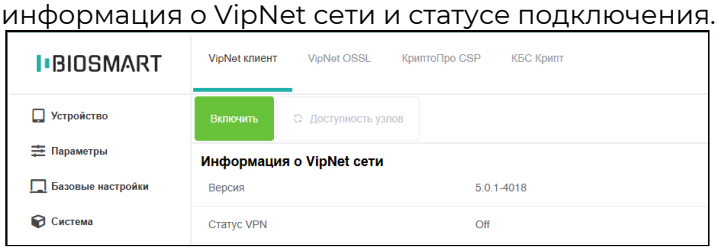
7.7.1 Настройка VipNet клиента и VipNet OSSL

Вкладки **VipNet клиент** и **VipNet OSSL** предназначены для настройки средств криптографической защиты информации.

Настройка подключения VipNet клиента

Для настройки подключения к VipNet сети выполните следующие настройки:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **СКЗИ** → вкладка **VipNet клиент**. На вкладке отображается информация о VipNet сети и статусе подключения.



3. Установите ключ одним из способов:
Способ 1. Загрузка ключа из файла
- нажмите кнопку **Загрузить ключ** и выберите файл с ключом;
- дождитесь завершения загрузки. При успешном завершении отобразится статус **Ключ загружен**.

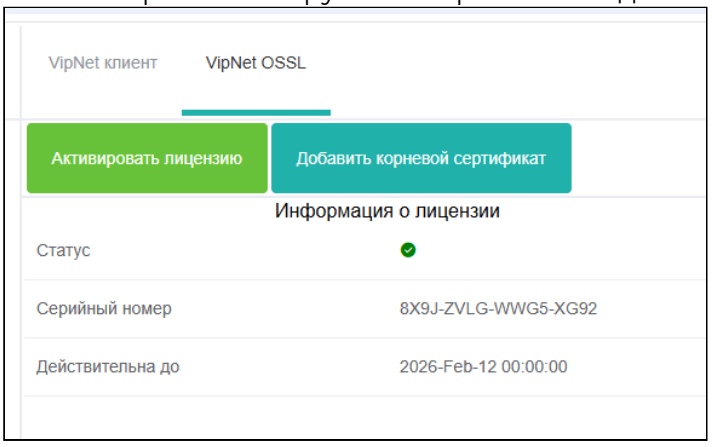
> Для загрузки нового ключа, необходимо сначала удалить текущий. Для этого нажмите кнопку **Сброс**

Способ 2. Ручной ввод ключа
- задайте пароль в поле **Пароль ключа;**
- нажмите кнопку **Установить ключ.**

Активация VipNet OSSL

Для активации VipNet OSSL выполните следующие настройки:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **СКЗИ** → вкладка **VipNet OSSL**.
3. Нажмите кнопку **Активировать лицензию** и выберите файл лицензии.
4. После завершения загрузки отобразятся сведения о лицензии.



5. Нажмите кнопку **Добавить корневой сертификат** и выберите файл. Дождитесь завершения загрузки.

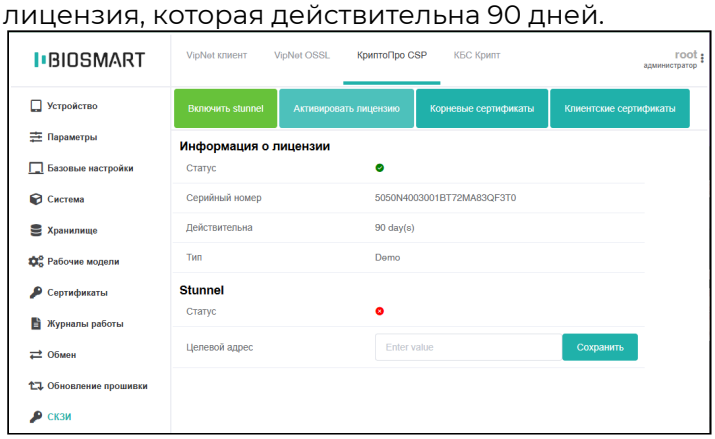
7.7.2 Настройка КриптоПро CSP

Вкладка **КриптоПро CSP** предназначена для настройки средств криптографической защиты информации.

Активация лицензии

Для активации лицензии КриптоПро CSP выполните следующие настройки:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **СКЗИ** → вкладка **КриптоПро CSP**. По умолчанию встроена demo-лицензия, которая действительна 90 дней.

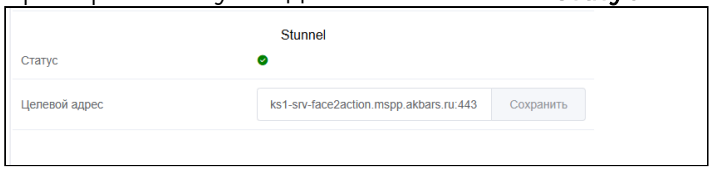


3. Для активации новой лицензии нажмите кнопку **Активировать лицензию**.
4. В открывшемся окне введите номер лицензии, затем нажмите кнопку **Confirm**.

Включение протокола TLS

Для включения протокола TLS выполните следующие настройки:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **СКЗИ** → вкладка **КриптоПро CSP**.
3. Введите адрес сервера в поле **Целевой адрес** и нажмите **Сохранить**.
4. Нажмите кнопку **Включить Stunnel**.
5. Проверьте статус подключения в поле **Статус**.

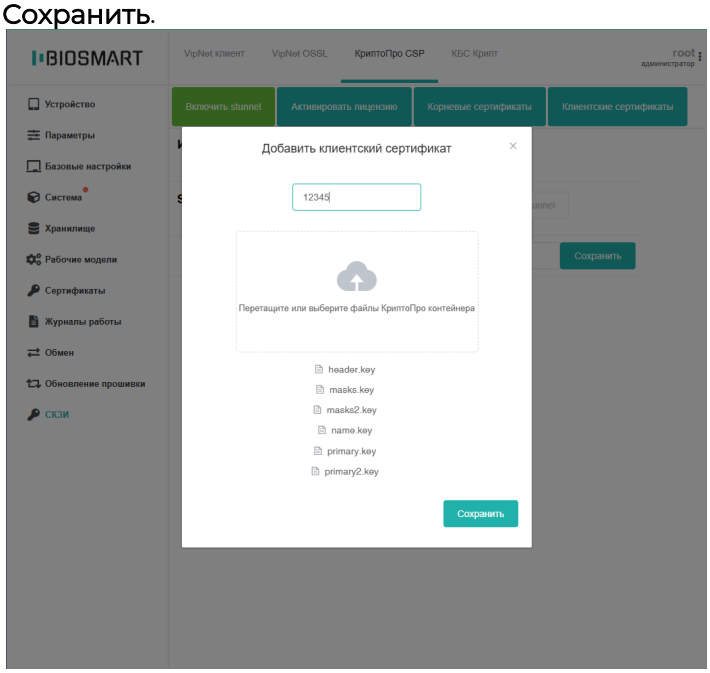


Управление корневыми и клиентскими сертификатами

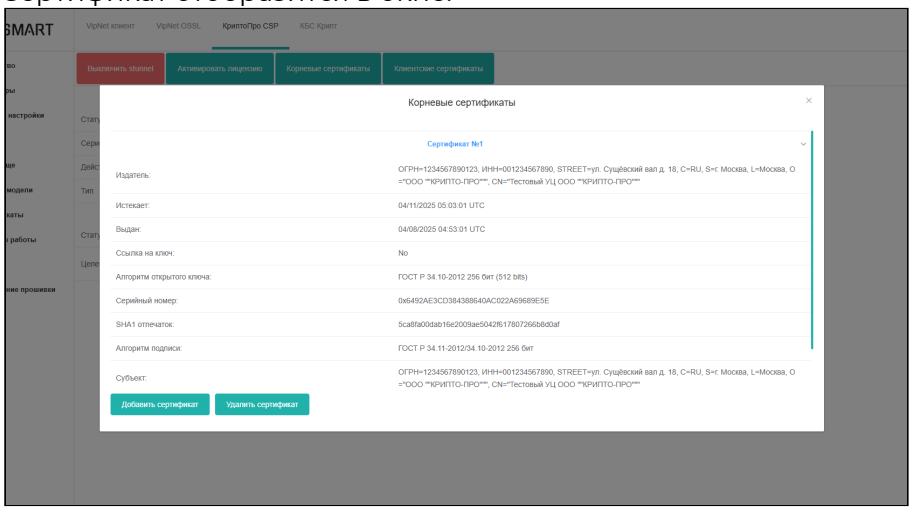
Для управления сертификатами выполните следующие действия:

1. Выполните вход в веб-интерфейс.
2. Перейдите в раздел **СКЗИ** → вкладка **КриптоПро CSP**.

3. Для управления корневыми сертификатами нажмите кнопку **Корневые сертификаты**, а для управления клиентскими — **Клиентские сертификаты**.
4. Для добавления сертификата в открывшемся окне нажмите кнопку **Добавить сертификат**.
5. Перетащите или выберите файлы сертификата, укажите пароль и нажмите **Сохранить**.



6. Сертификат отобразится в окне.



7. Если необходимо загрузить новый сертификат, сперва удалите старый. Для этого нажмите кнопку **Удалить сертификат**.

7.8 Перезапуск

Выполнить перезапуск можно через:

Меню терминала

1. В меню терминала выберите **Настройки** → **Перезапуск**.
2. Перетяните один из слайдеров:
   - **Приложение** — для перезапуска программной части терминала.
   - **Устройство** — для полной перезагрузки устройства (аппаратный сброс).

Веб-интерфейс

1. Откройте браузер и введите в адресной строке IP-адрес терминала.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Система** → вкладка **Перезапуск.**
4. Нажмите одну из кнопок:
   - **Перезапуск приложения** — для перезапуска программной части терминала.
   - **Перезагрузка устройства** — для полной перезагрузки устройства (аппаратная перезагрузка).

7.9 Обновление встроенного ПО терминала

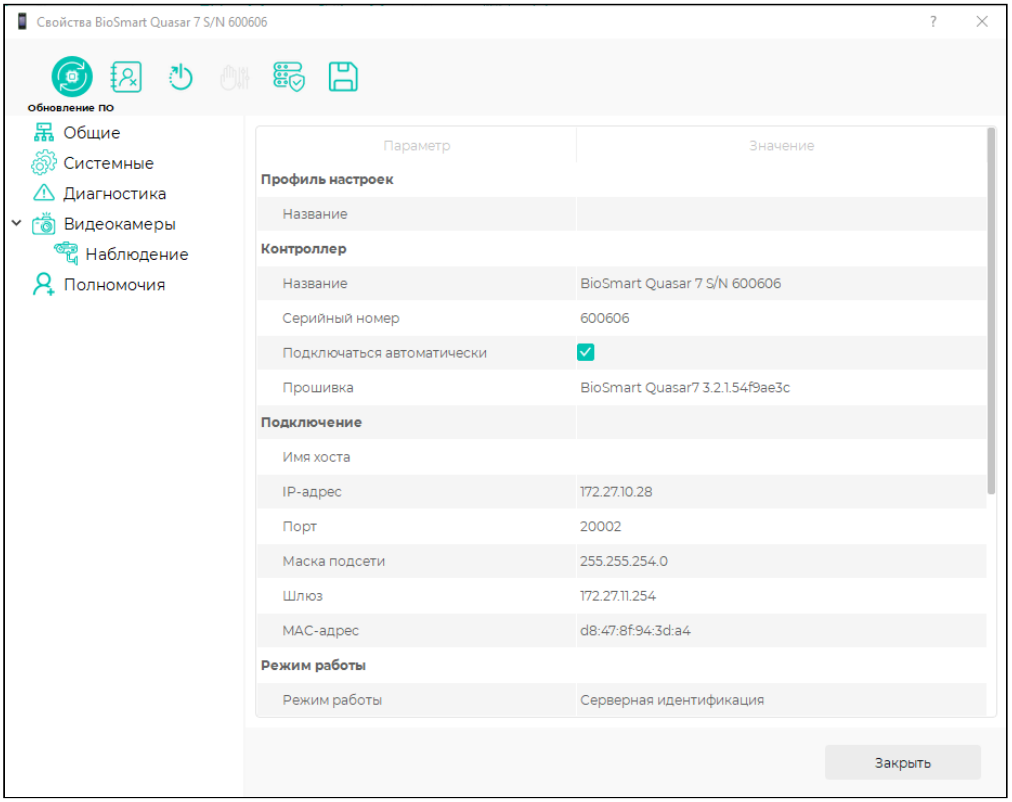
Обновить встроенное ПО терминала можно с помощью веб-интерфейса или в ПО Biosmart-Studio v6.

7.9.1 Обновление встроенного ПО контроллера в ПО Biosmart-Studio v6

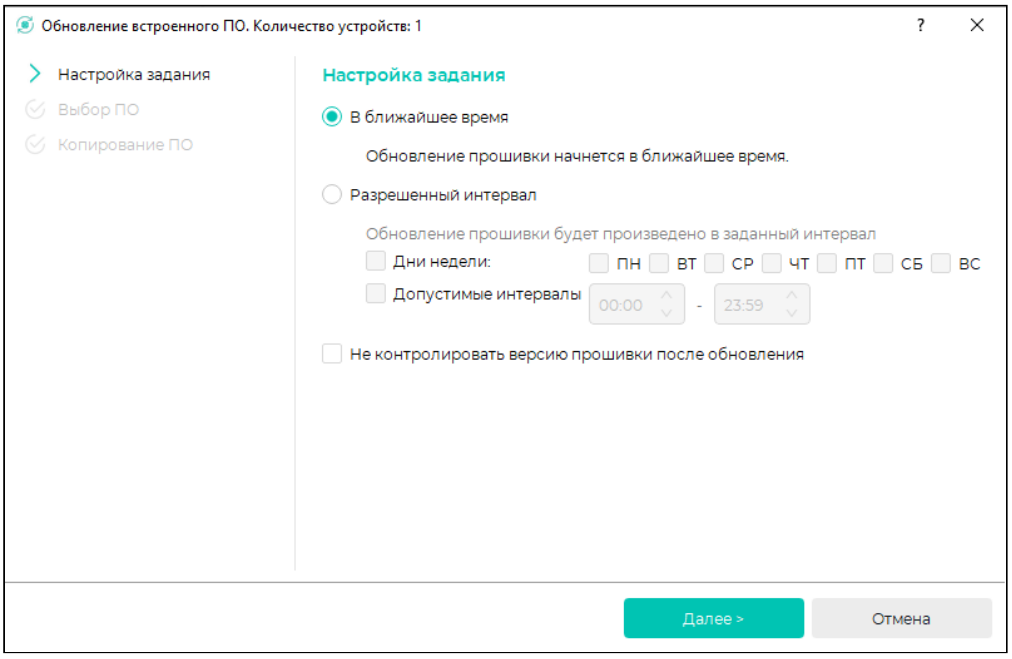
Запустить обновление из ПО Biosmart-Studio v6 можно в окне **Свойства BioSmart Quasar 7** или на вкладке **Обновление ПО** раздела **Устройства**.

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 контроллера, запускаемый в окне **Свойства BioSmart Quasar 7**.

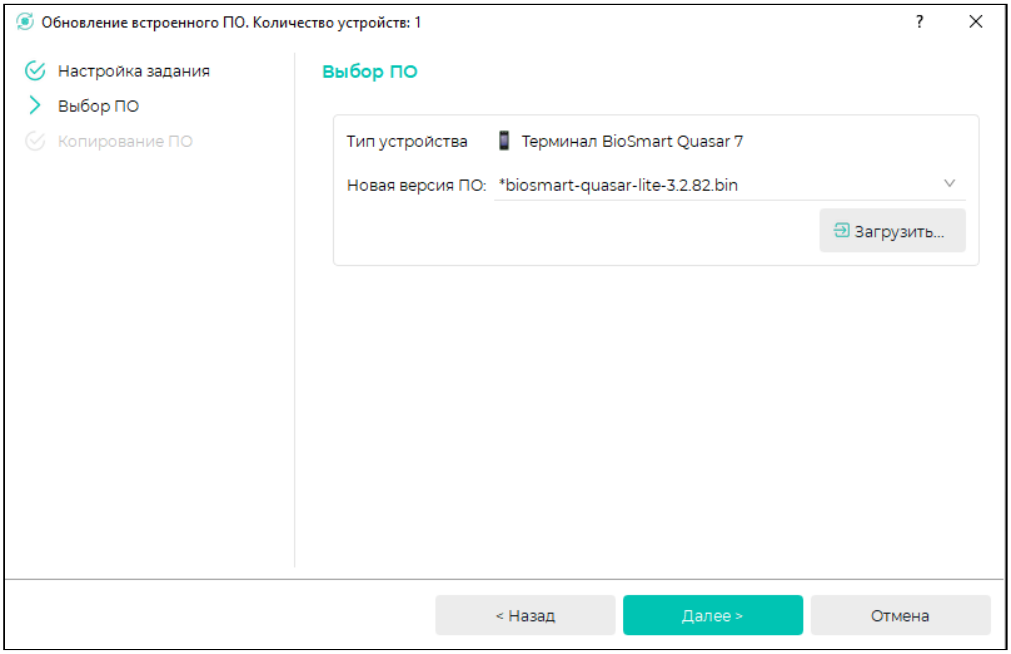
Откройте окно **Свойства BioSmart Quasar 7** и нажмите кнопку **Обновление ПО**.



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



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 **Завершить.**

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

7.9.2 Обновление встроенного ПО терминала в веб-интерфейсе

Для обновления встроенного ПО терминала 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 **Обновление прошивки.**
4. Перетащите файл в выделенную область с текстом "Переместить файл прошивки в эту область..." или кликните на эту область, чтобы открыть стандартный диалог выбора файла в вашей операционной системе, и найдите нужный файл.
5. После завершения загрузки нажмите **Запустить обновления**.

> Чтобы отменить загрузку, наведите курсор на индикатор выполнения и нажмите на значок (X).

7.10 Сброс параметров терминала на заводские

7.10.1 Сброс сетевых параметров терминала

Для сброса сетевых параметров терминала перейдите в меню терминала нажмите **Настройки** → **Сброс**. Включите опцию **Настройки сети**. Следуйте инструкциям на

экране.

7.10.2 Сброс параметров терминала к заводским

Для сброса параметров терминала на настройки по умолчанию выполните следующие действия:

1. Откройте браузер и введите в адресной строке текущий IP-адрес терминала.
2. Выполните вход в веб-интерфейс.
3. Перейдите в раздел **Система** → вкладка **Компоненты**.
4. Выберите в списке конфигураций **Настройки по умолчанию**.
5. Нажмите **Применить**.
6. В открывшемся диалоговом окне подтвердите применение изменений, нажав кнопку **Перезапустить**.

7.10.3 Сброс параметров терминала к заводским в ПО Biosmart-Studio v6

Выполнить сброс параметров можно из ПО Biosmart-Studio v6.

Чтобы сбросить настройки перейдите в раздел **Устройство** ПО Biosmart-Studio v6 → выберите терминал в списке устройств → нажмите на панели инструментов кнопку **Сброс параметров**.

8 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ BIOSMART QUASAR 7

В данном разделе приведены виды технического обслуживания изделия, соответствующий им перечень операций, а также меры безопасности и периодичность.

При хранении изделия и использовании его по назначению требуется проведение периодического технического обслуживания. Техническое обслуживание включает в себя проверку внешнего вида, удаление грязи и пыли, проверку работоспособности. Операции, перечисленные в настоящем разделе, имеют своей целью поддержание изделия в работоспособном состоянии и обеспечение условий для длительной безотказной работы.

В разделе указана рекомендуемая периодичность технического обслуживания. Заказчик должен самостоятельно оценивать необходимость более частого проведения технического обслуживания в зависимости от условий эксплуатации изделия. Например, если изделие эксплуатируется в запыленном помещении, то операцию по удаления грязи и пыли с поверхностей изделия следует проводить чаще, чем это указано в настоящем разделе.

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

Техническое обслуживание при эксплуатации

Название операции	Описание	Периодичность
Внешний осмотр, удаление пыли и грязи с наружных поверхностей	• проверьте целостность корпуса, отсутствие повреждений дисплея и модуля камер; • проверьте состояние проводов, подключенных к терминалу. Убедитесь в отсутствии обрывов и видимых повреждений изоляции; • аккуратно удалите пиль и грязь с поверхности терминала с помощью сухой мягкой ткани или пылесоса с узким соплом. Для дезинфекции можно использовать ткань, смоченную в 70% изопропиловом спирте, при условии, что спирт не будет попадать внутрь корпуса.	Раз в месяц
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 лицу и убедитесь в том, что сотрудник идентифицирован правильно; • если терминал управляет исполнительным устройством (например, электрозамком, турникетом), то инициировать выдачу команды управления на исполнительное устройство (нажать кнопку, выполнить идентификацию).	Раз в год

Техническое обслуживание при хранении

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.

Название операции	Описание	Периодичность
Осмотр изделия, удаление пыли	• вскройте упаковку (при наличии); • проверьте целостность корпуса, отсутствие повреждений дисплея и модуля камер; • при обнаружении пыли или грязи на наружных поверхностях, удалите её с помощью сухой мягкой ткани или пылесоса с узким соплом; • поместите терминал в упаковку (при наличии).	Раз в год или чаще в зависимости от условий хранения

9 ХРАНЕНИЕ, ТРАНСПОРТИРОВАНИЕ И УТИЛИЗАЦИЯ QUASAR 7

Хранение и транспортировка устройства 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 устройства может осуществляться любым видом транспорта, кроме морского транспорта, в крытых транспортных средствах.

Для всех видов транспортировки упакованные устройства должны быть закреплены таким образом, чтобы исключить перемещение и соударение.

Не храните и не транспортируйте устройство:

- 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 плесень, насекомые, животные.

После пребывания устройства 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. После окончания эксплуатации терминала обратитесь в сертифицированный пункт сбора.