

Интеграция устройств BioSmart с ПК Бастион-3

Инструкция по настройке

СОДЕРЖАНИЕ

1	ПОДКЛЮЧЕНИЕ И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА ОБОРУДОВАНИЯ BIOSMART.	4
2	УСТАНОВКА И НАСТРОЙКА ПРОГРАММНЫХ ПРОДУКТОВ.....	9
3	ДОБАВЛЕНИЕ И НАСТРОЙКА ДРАЙВЕРОВ УСТРОЙСТВ.....	20
4	НАСТРОЙКА ПЛАНОВ, ДОСТУПА И ДОБАВЛЕНИЕ СОТРУДНИКОВ.....	26
4.1	Создание уровней доступа	26
4.2	Добавление сотрудника.....	27
4.2.1	Создание карточки сотрудника	27
4.2.2	Регистрация биометрических шаблонов вен ладони.....	30
5	МОНИТОРИНГ СОБЫТИЙ В ПК «БАСТИОН-3»	31

В настоящем документе описан порядок настройки устройств BioSmart для работы с программным комплексом «Бастион-3» (далее – ПК «Бастион-3») и контроллером Elsys-MB.

ПК «Бастион-3» и контроллер Elsys-MB можно использовать со следующими устройствами:

- терминалом [BioSmart Quasar 7](#);
- контроллером [BioSmart UniPass Pro 2](#), считывателем [BioSmart PalmJet 2](#).

Программно-аппаратные требования к ПК «Бастион-3» необходимо уточнять в документации производителя, расположенной на сайте twinpro.ru.

Порядок подключения и настройки устройств BioSmart описан в следующих разделах.

С информацией о работе ПК «Бастион-3» с устройствами BioSmart также можно ознакомиться в [Бастион-3 - BioSmart. Руководстве администратора](#).

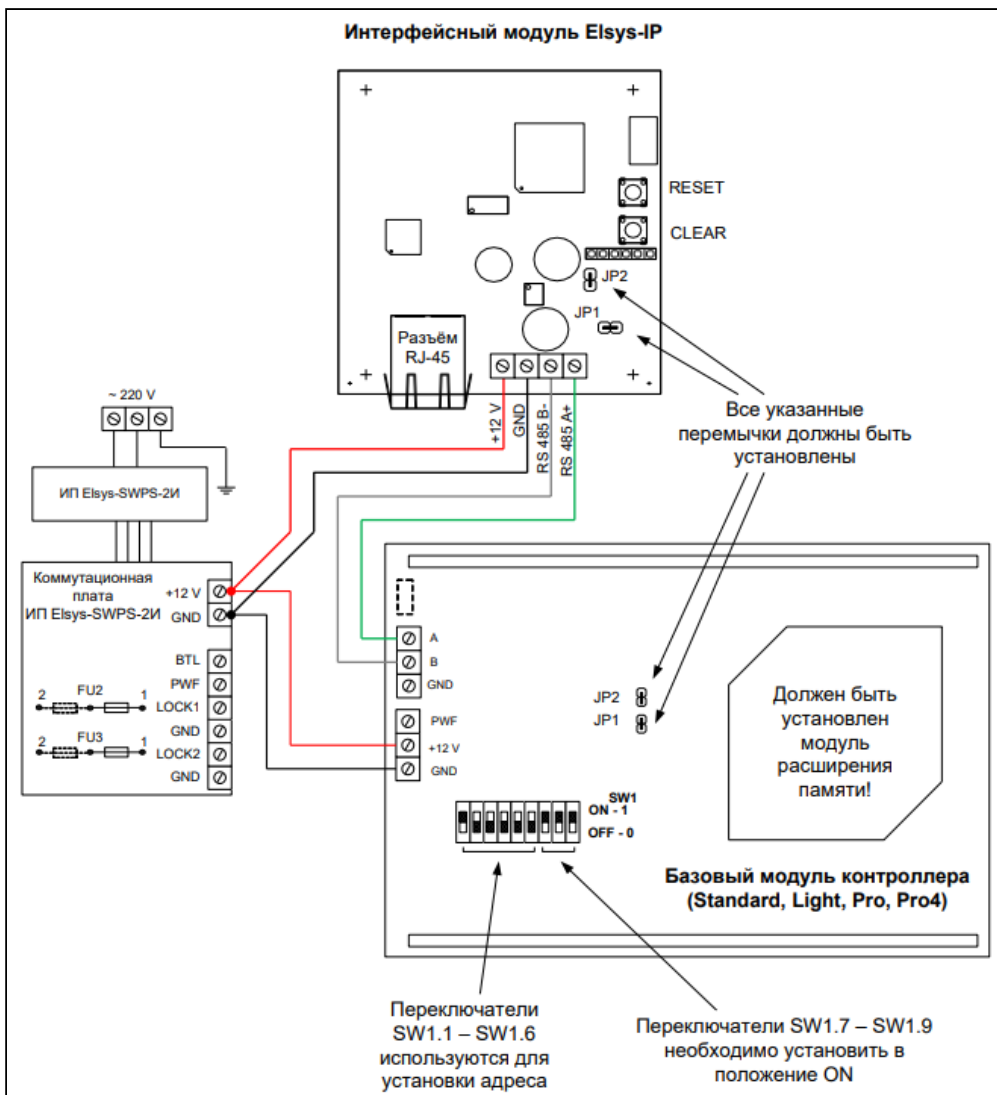
1 ПОДКЛЮЧЕНИЕ И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА ОБОРУДОВАНИЯ BIOSMART

В разделе описан порядок подключения оборудования BioSmart к контроллеру Elsys-MB и его первоначальной настройки.

Выполните подключение и настройку в следующем порядке:

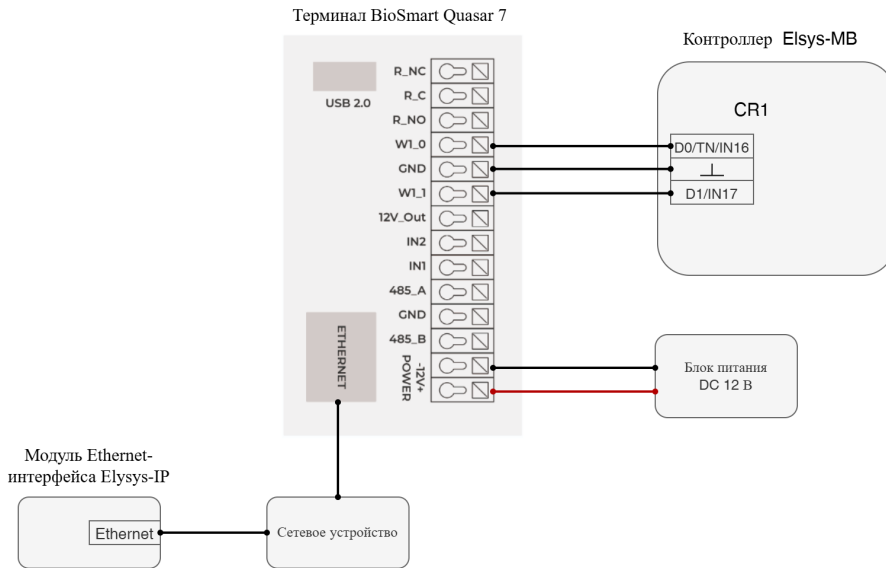
1. Подключите модуль Ethernet-интерфейса Elsys-IP к контроллеру Elsys-MB

К контроллеру **Elsys-MB** подключите модуль Ethernet-интерфейса **Elsys-IP** в соответствии со схемой, приведённой ниже. Более подробно с описанием модуля Ethernet-интерфейса, контроллером Elsys-MB можно ознакомиться в технической документации, расположенной на сайте производителя twinpro.ru.

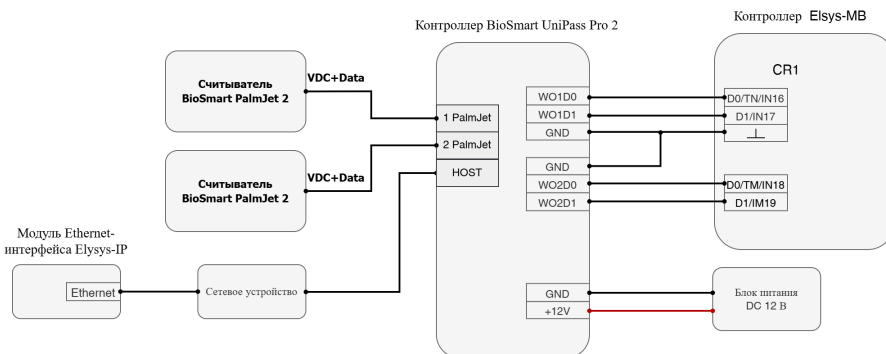


2. Подключите устройства BioSmart к контроллеру Elsys-MB

Выполните подключение терминала **BioSmart Quasar 7** к контроллеру **Elsys-MB** в соответствии со схемой ниже.



Выполните подключение контроллера **BioSmart UniPass Pro 2** к контроллеру **Elsys-MB** в соответствии со схемой ниже.



3. Настройте контроллер BioSmart UniPass Pro 2 и считыватели BioSmart PalmJet 2

Настройте сетевые параметры контроллера.

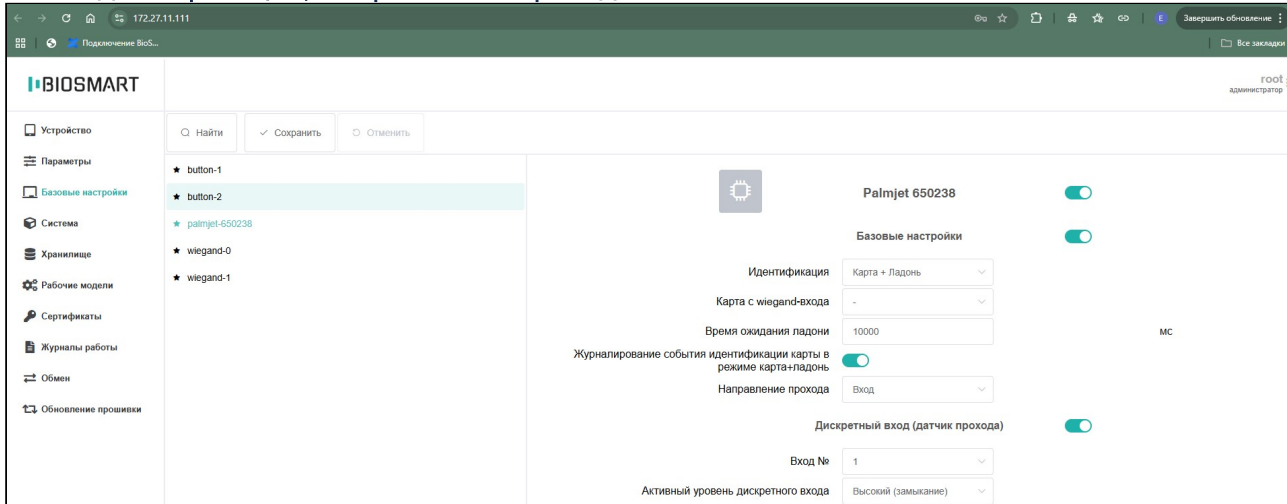
Для смены IP-адрес контроллера, выполните следующие действия:

1. Скачайте приложение **IP CHANGER Utility**, размещенное на сайте bio-smart.ru в разделе **Техподдержка** → **ПО** → вкладка **Драйверы**.
2. Распакуйте файл **ipchanger.zip** в любой каталог и перейдите в него.
3. Откройте папку **ipchanger** → запустите приложение **ipchanger.exe**.
4. В открывшемся окне нажмите кнопку **Search** → в списке выберите контроллер → нажмите кнопку **Change IP**.
5. Укажите сетевые настройки контроллера в соответствии с настройками используемой сети → нажмите кнопку **OK**.
6. Контроллер готов для дальнейшей настройки.

Перейдите в веб-интерфейс контроллера. Для этого в адресную строку браузера введите IP-адрес контроллера в виде **https://IP_address**. В поля **Login** и **Password** введите **admin**, **bioroot** (по умолчанию).

В разделе **Базовые настройки** нажмите кнопку **Найти**. Считыватели, подключенные к контроллеру, отобразятся в списке. Для корректной работы необходимо настроить каждый из считывателей. Выберите считыватель и заполните

поля Идентификация, Направление прохода.



Настройте передачу данных по Wiegand. Для этого включите переключатели **Wiegand при успешной идентификации**, **Wiegand при неуспешной идентификации**.

Задайте значения в полях, описанных в таблице.

Поле	Описание
Wiegand	Номер линии связи (Wiegand output port 0 или Wiegand output port 1), к которой подключен настраиваемый считыватель.
Режим	Битность интерфейса Wiegand.
Тип	Тип данных передаваемых по Wiegand в случае успешной идентификации.
Код	Код, передаваемый по Wiegand, в случае неуспешной идентификации.

Wiegand при успешной идентификации

Wiegand №

Режим

Тип

Wiegand при неуспешной идентификации

Wiegand №

Режим

Код

Сохраните изменения нажав кнопку **Сохранить**. Повторите настройку для второго считывателя.

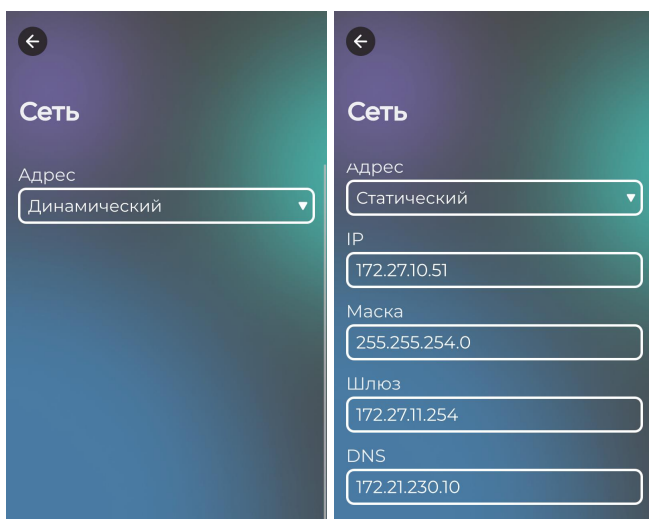
4. Настройте терминал BioSmart Quasar 7

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

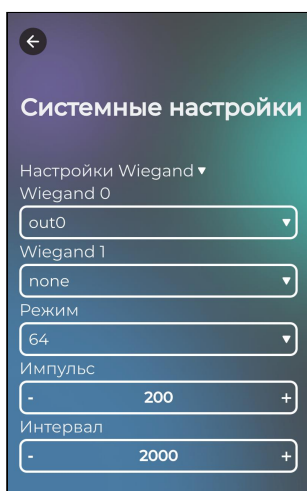
Для начала работы с терминалом, установите сетевые настройки терминала в соответствии с настройками используемой сети.

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

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



Откройте **Настройки** → **Система**. Выберите режим работы из выпадающего списка в поле **Режим**. Описание режимов приведено в [Руководстве по эксплуатации терминала BioSmart Quasar 7](#).



В поле **Wiegand 0** установите значение **out** для активации передачи данных с терминала на внешние устройства.

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

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

Нажмите **Сохранить**.

Откройте веб-интерфейс терминала. Для этого в адресную строку браузера введите IP-адрес терминала в виде https://IP_address. В поля **Login** и **Password** введите **root**, **biroot** (по умолчанию).

Перейдите в раздел **Система** → вкладка **Компоненты**. Выберите конфигурацию, в которую вносятся изменения. Раскройте компонент, управляющий режимом работы.

Найдите параметр **Отправлять в wiegand код неудачной идентификации по карте** и в выпадающем меню выберите **включено**.

В поле **Wiegand код неудачной идентификации по карте** укажите значение, которое отправится во внешнюю систему.

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

i 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


Нажмите кнопку **Применить**.

2 УСТАНОВКА И НАСТРОЙКА ПРОГРАММНЫХ ПРОДУКТОВ

Для работы интеграции необходимо установить следующие программные продукты:

- СУБД PostgreSQL 11.11;
- ПК «Бастион-3»;
- драйверы Guardant;
- сервер интеграции (программный сервис Elsys-SDK II);
- конфигуратор контроллеров СКУД и ОС Elsys.

Программное обеспечение можно скачать с сайта производителя twinpro.ru.

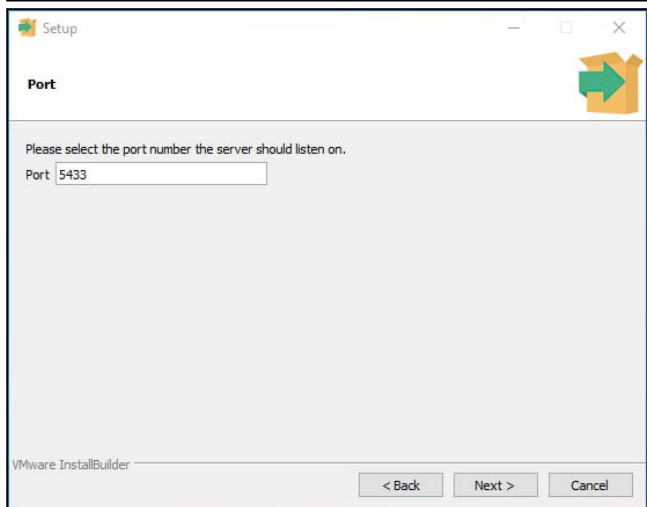
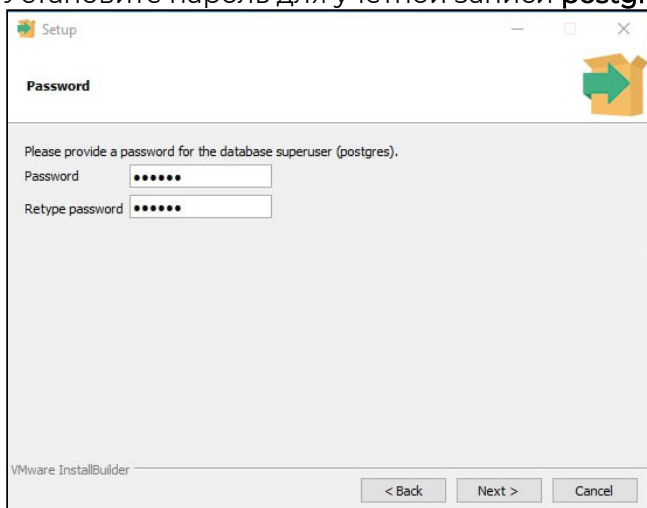
 Для использования ПК «Бастион-3» необходимо приобрести лицензию.

Для настройки программного обеспечения выполните следующие шаги:

1. Установите и настройте СУБД PostgreSQL 11.11

Для установки и настройки PostgreSQL выполните следующие действия:

1. Запустите установочный файл **postgresql-11.11-1-windows-x64.exe**, следуйте инструкциям программы установки.
2. Установите пароль для учетной записи **postgres**, выберите свободный порт.



3. Проверьте и настройте параметры сервера PostgreSQL. Для этого откройте конфигурационные файлы **postgresql.conf** и **pg_hba.conf**, расположенные по умолчанию в папке: **C:\Program Files\PostgreSQL\XX\data** в Windows, и **/etc/postgresql/XX/main** в Linux (XX – версия СУБД), (см. п.3.1.4 [Руководства администратора ПК «Бастион-3»](#)).
4. Проверьте временную зону в файле **postgresql.conf**. Параметр **timezone** должен соответствовать часовому поясу, установленному на хосте. Просмотрите список поддерживаемых в СУБД PostgreSQL временных зон с помощью запроса:

```
select * from pg_timezone_names
```

5. В файле **postgresql.conf** установите следующие параметры:

```
# - Connection Settings -
max_connections = 500          # (change requires restart)

# - Memory -
shared_buffers = 256MB        # min 128kB
temp_buffers = 32MB           # min 800kB
work_mem = 64MB               # min 64kB
maintenance_work_mem = 128MB # min 1MB

# - Background Writer -
bgwriter_delay = 20ms         # 10-10000ms between rounds
bgwriter_lru_maxpages = 400   # 0-1000 max buffers written/round
bgwriter_lru_multiplier = 4.0

# AUTOVACUUM PARAMETERS
autovacuum = on
autovacuum_max_workers = 6    # max number of autovacuum subprocesses
autovacuum_naptime = 20s      # time between autovacuum runs
autovacuum_vacuum_cost_limit = 400 # default vacuum cost limit for
```

6. В файле **pg_hba.conf** установите следующие параметры:

```
# Allow replication connections from localhost, by a user with the
# replication privilege.
host    replication    all             127.0.0.1/32    md5
host    replication    all             ::1/128         md5
host    all all         0.0.0.0/0      127.0.0.1/32   md5
```

7. После изменения конфигурации перезапустите сервер СУБД.

2. Установите драйверы Guardant

Для установки драйверов выполните следующие действия:

1. Загрузите актуальную версию драйверов с [сайта производителя](#).
2. Для установки через deb-пакет можно использовать команду:

```
sudo dpkg i grdcontrol*.deb
```

3. Для установки через rpm-пакет можно использовать команду:

```
sudo yum install grdcontrol-*.rpm
```

4. В ОС Windows на сервере системы для работы с ключами Guardant необходимо дополнительно установить драйверы Guardant. Актуальную версию можно скачать [тут](#).

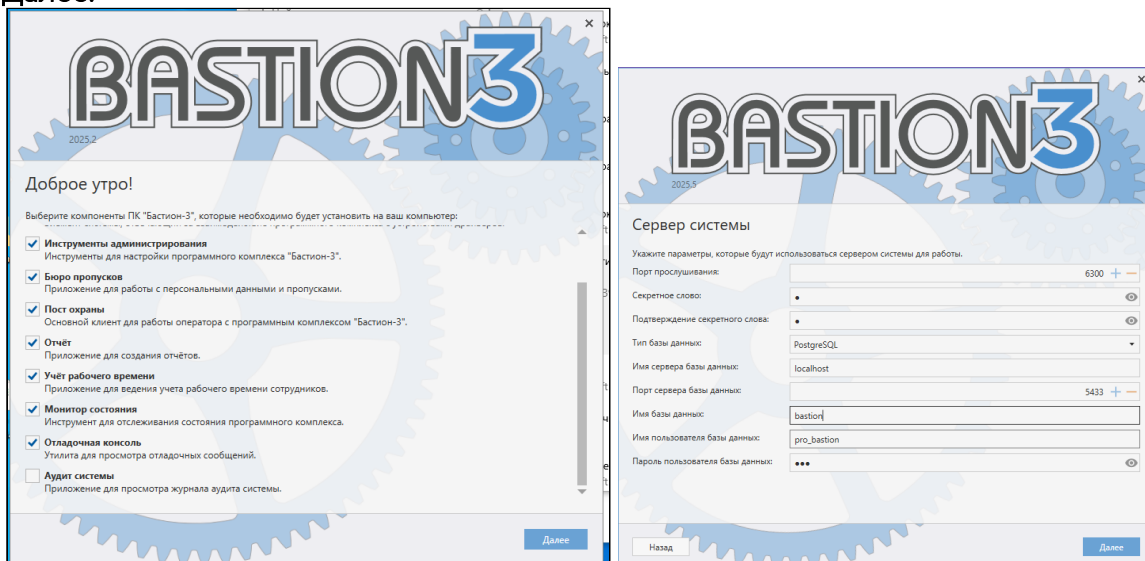
3. Установите ПК «Бастион-3»

Для установки ПК «Бастион-3» выполните следующие действия:

1. Скачайте дистрибутив ПК «Бастион-3» с сайта производителя [twinpro.ru](#).
2. Запустите программу установки ПК «Бастион-3» с правами администратора ОС. Следуйте инструкциям программы установки.

i Рекомендуется выполнять установку на том компьютере, с которого будет разворачиваться схема базы данных ПК «Бастион-3». До развёртывания схемы работа системы будет невозможна.

3. Выберите все компоненты программы, кроме компонента **Аудит системы**. Нажмите **Далее**.



4. Введите параметры для подключения к СУБД PostgreSQL согласно таблице.

Поле	Описание
Пользователь PostgreSQL	– имя пользователя PostgreSQL для подключения к БД ПК «Бастион-3».
Пароль пользователя PostgreSQL	– пароль пользователя для подключения к базе данных всеми модулями ПК «Бастион-3».

Поле	Описание
Имя базы данных PostgreSQL	– название БД ПК «Бастион-3» на сервере PostgreSQL.
Адреса сервера PostgreSQL	– IP-адрес или DNS-имя сервера PostgreSQL.
Порт сервера PostgreSQL	– порт, используемый для подключений к серверу PostgreSQL (5432 по умолчанию).



Запомните имя и пароль для БД ПК «Бастион-3» для дальнейшей настройки.

5. Введите настройки сервера системы согласно таблице.

Поле	Описание
Адрес сервера	– IP-адрес или DNS-имя компьютера, на котором будет работать сервер системы.
Порт сервера	– порт, на котором будет работать сервис сервера систем.
Код подключения	– кодовое слово, используемое для подключения к серверу системы. Необходимо вводить одинаковый код подключения на всех компьютерах системы.

6. После ввода всех параметров будет произведена установка системы.

 В некоторых случаях необходимо выполнить дополнительные действия для безошибочной работы системы:

- В дистрибутиве ПК «Бастион-3» перейдите в папку: `\ExtModules\BioSmartSDK\BioSmartSDK_2025.03.24_windows` и распакуйте файл **BioSmartSdkSetup.msi**. Переместите его в папку **Bastion3** (по расположена в `C:\Program Files (x86)\ES-Prom\Bastion3`).
- Перейдите в раздел **Приложения и возможности** (для ОС Windows) и нажмите кнопку **Исправить**, после чего дождитесь окончания процесса.

Более подробно с описанием установки можно ознакомиться в [Руководстве администратора ПК «Бастион-3»](#).

4. Настройте подключение к БД

1. Откройте приложение **Управление схемами баз данных**.

2. Выполните вход в программу. Для этого введите пароль → нажмите **Подключится**.

3. В открывшемся окне нажмите кнопку **Создать базу данных**, введите параметры базы данных, после нажмите кнопку **Создать**.

4. База данных будет добавлена в список. Приложение **Управление схемами баз данных** можно закрыть.

Имя базы данных	Владелец	Дата/вр.	Версия	Всего объектов	Активные подключения
bastion	pro_bastion	23.01.20	3.25.5	1337	0

5. Установите сервер интеграции СКУД и ОС Elsys и конфигуратор контроллеров СКУД и ОС Elsys

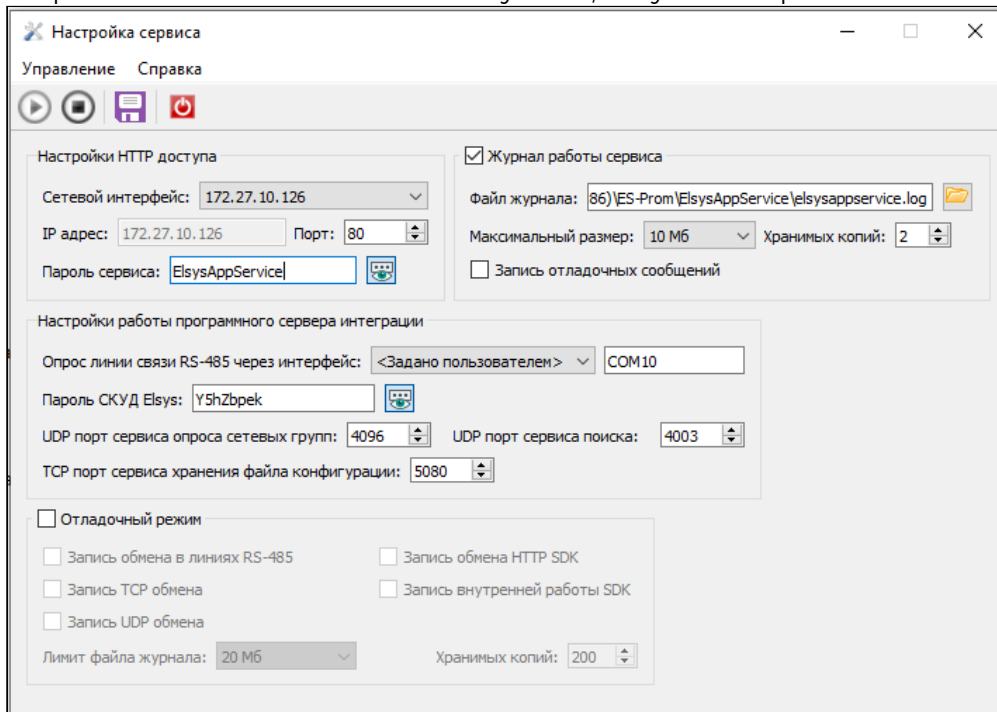
1. Скачайте **конфигуратор контроллеров СКУД Elsys**, который функционирует под управлением сервера интеграции, с сайта производителя twinpro.ru.
2. В скачанном дистрибутиве откройте папки **elsys_service_setup** и **elsys_config_setup**.
3. Выберите файл установки для операционной системы, на которую будут установлены сервер и конфигуратор.
4. Запустите установочные файлы.

Более подробно с процессом установки можно ознакомиться в **Руководстве пользователя конфигулятора СКУД Elsys** и **Руководстве администратора ElsysAppService**. Данная документация входит в состав установочных файлов, скачанных с сайта производителя.

6. Настройте сервер интеграции СКУД и ОС Elsys

1. Откройте приложение **Настройка сервиса**. При первом входе будет предложено создать новый файл с настройками по умолчанию, необходимо нажать кнопку **OK**.
2. Введите пароль доступа к сервису. По умолчанию – **ElsysAppService**.
3. Настройте параметры сетевого доступа. В поле **Сетевой интерфейс** выберите **<Задано пользователем>** и укажите корректный адрес IPv4 в расположенном ниже поле ввода.
4. В поле **Пароль сервиса** задается пароль, используемый для работы с программным сервисом SDK. Пароль необходимо запомнить, потребуется для дальнейшей настройки.
5. В поле **Пароль СКУД Elsys** указать пароль установленный для контроллера Elsys-MB. Пароль должен быть установлен одинаковым во всех контроллерах системы и в управляющем ПО – только в этом случае управляющее ПО и контроллер будут взаимодействовать между собой.

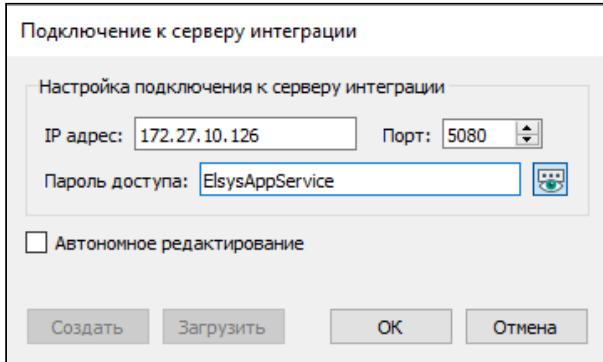
6. Сохраните изменения нажав кнопку , запустите сервис нажав кнопку .



Подробнее с настройками программного сервиса можно ознакомиться в **Руководстве администратора**, которое загружается с сайта производителя совместно с установочным файлом.

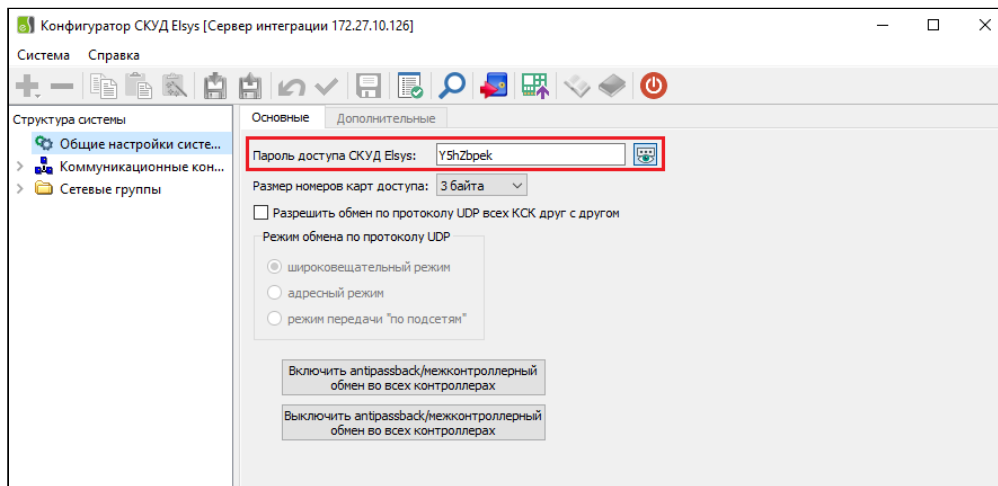
7. Настройте конфигуратор контроллеров СКУД и ОС Elsys

Откройте приложение **Конфигуратор СКУД Elsys**. При запуске укажите корректные параметры подключения к серверу: адрес хоста сервера интеграции в формате IPv4, номер порта сервиса и пароль доступа сервера интеграции (по умолчанию – **ElsysAppService**).

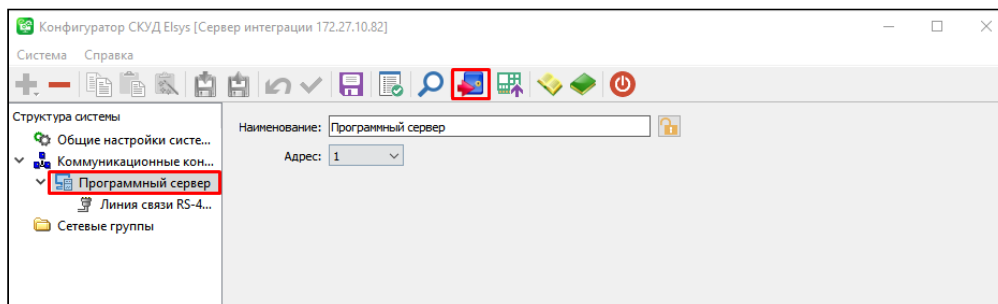


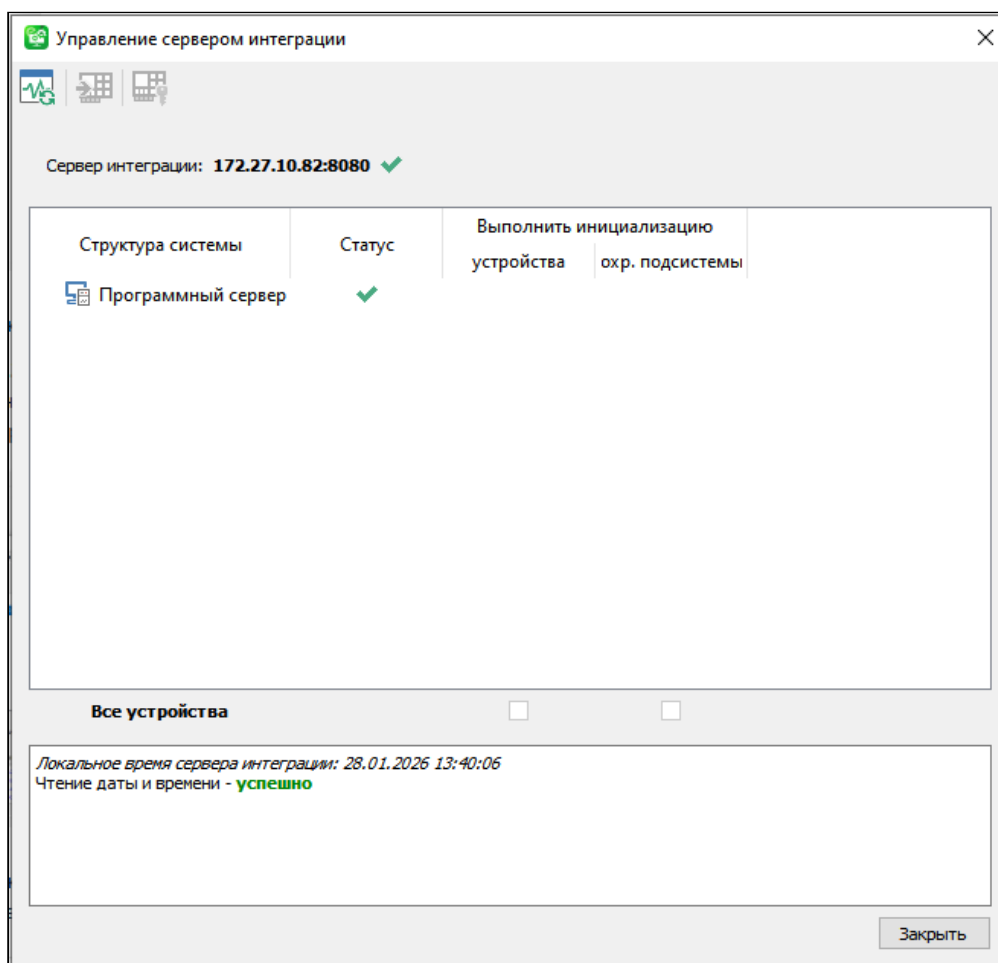
В открывшемся окне проверьте следующие параметры:

- **Пароль доступа СКУД Elsys** совпадает с паролем, указанным в настройках сервера.



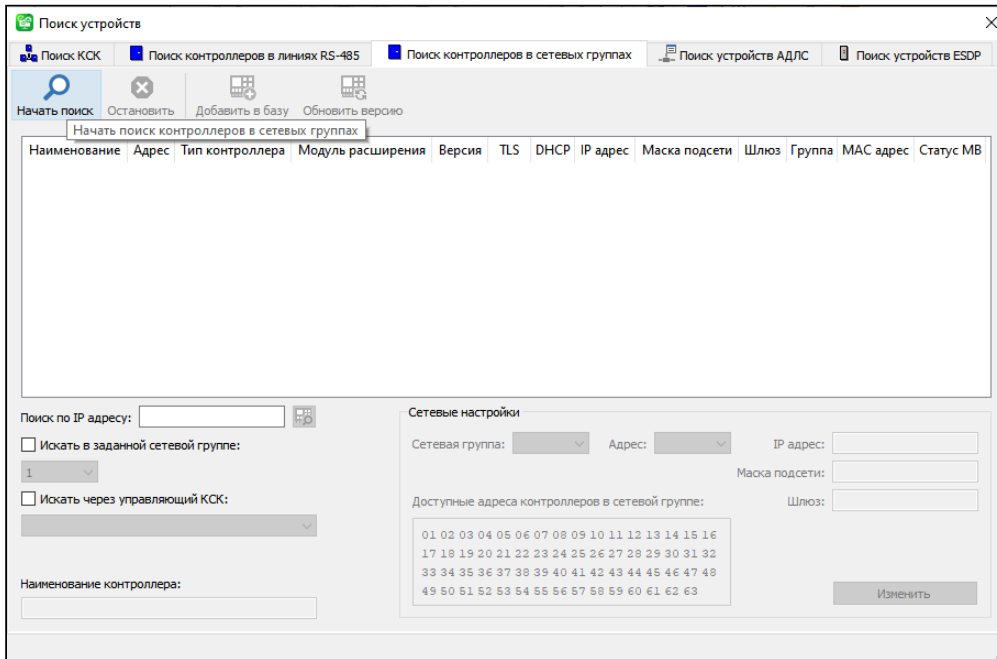
- Инициализация программного сервиса Elsys-SDK II проходит успешно. Для проверки нажмите кнопку **Отображение формы управления сервером интеграции**.





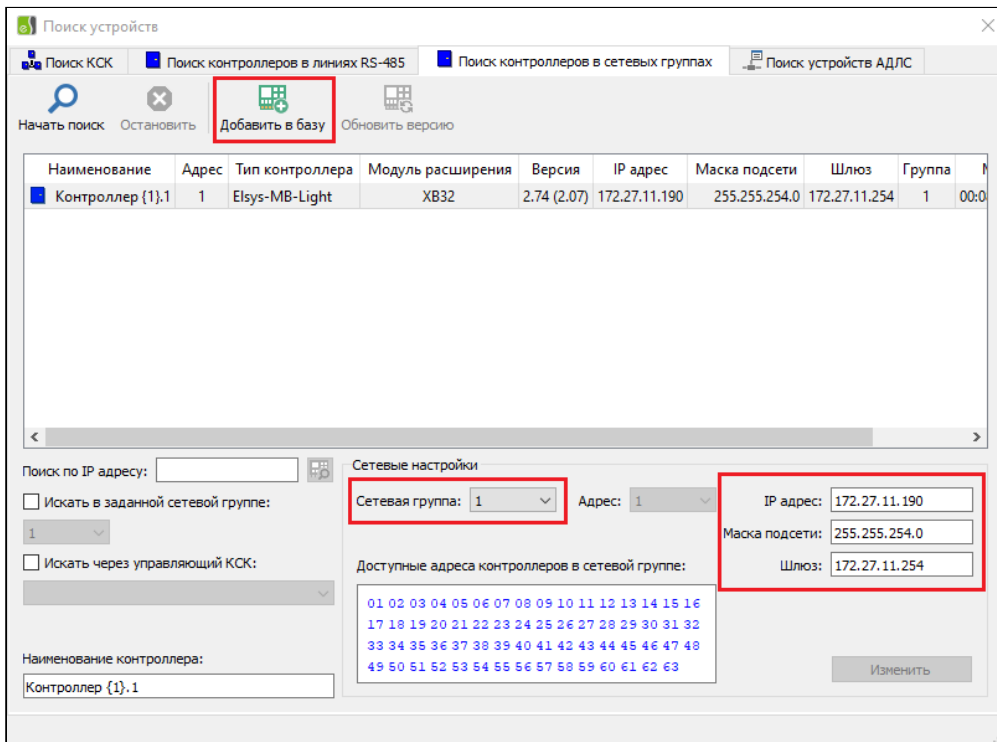
После инициализации добавьте необходимые контроллеры.

Для этого нажмите кнопку **Поиск КСК, контроллеров и устройств**. В открывшемся окне перейдите во вкладку **Поиск контроллеров в сетевых группах** → нажмите кнопку **Начать поиск**.

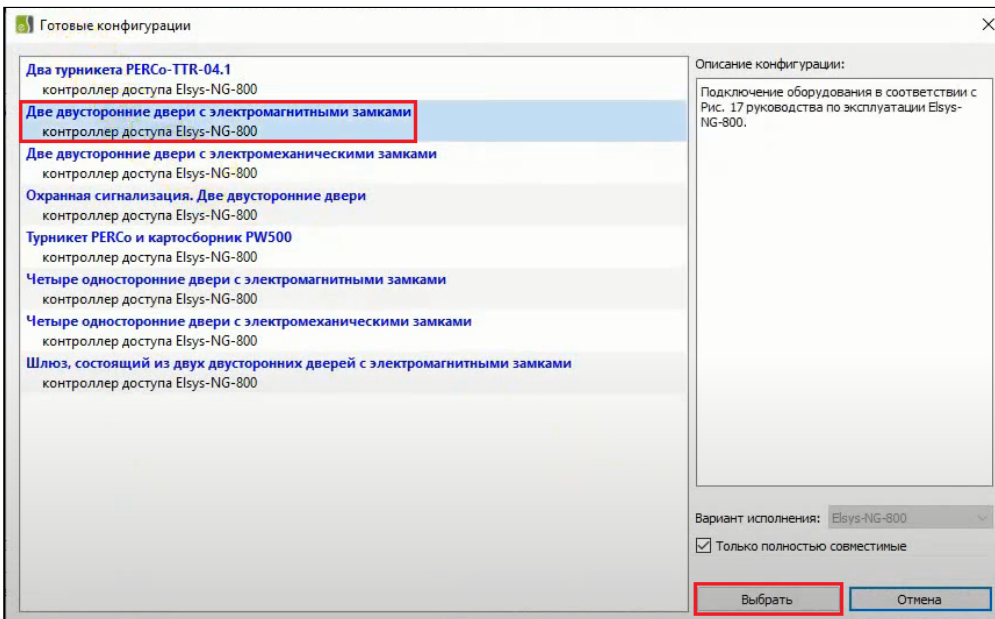


В списке устройств должен отобразиться контроллер. Контроллеры при первом подключении имеют IP адрес 192.168.127.254 и номер сетевой группы равный нулю, их запрещено добавлять в конфигурацию системы.

Для добавления контроллера в систему, присвойте сетевую группу 1 и измените сетевые настройки. Нажмите кнопку **Изменить**, после чего настройки будут записаны в контроллер. Добавьте контроллер в конфигурацию системы с помощью кнопки **Добавить в базу**.



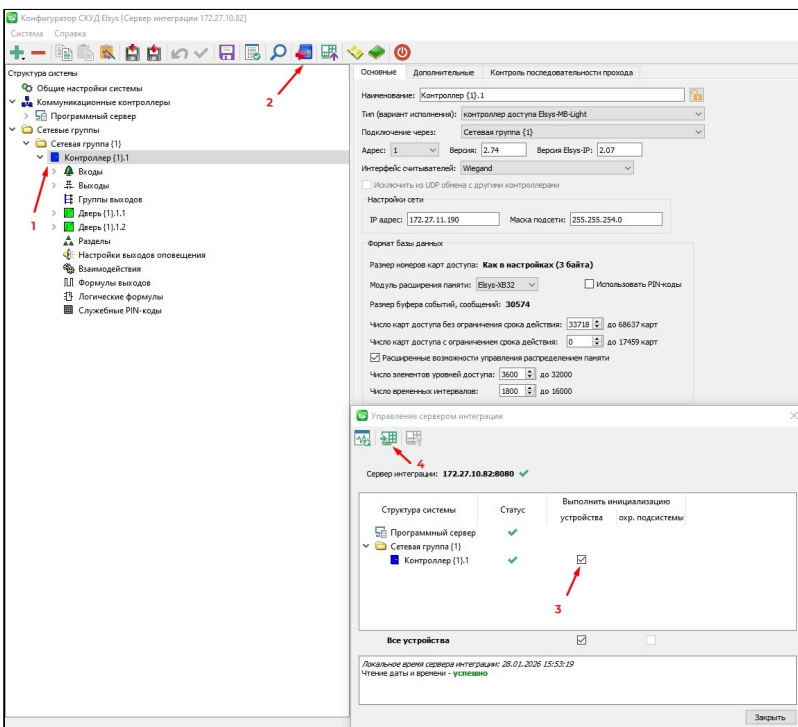
Если для контроллера существуют готовые конфигурации, то выберите готовую конфигурацию и нажмите кнопку **Выбрать**.




Добавленный контроллер необходимо инициализировать, после чего настройка программного обеспечения будет завершена.

Для инициализации выберите контроллер в дереве устройств (1) → нажмите кнопку **Отображение формы управления сервером интеграции** (2).

В окне **Управление сервером интеграции** в строке с контроллером заполните чекбокс (3), нажмите кнопку (4).



Настройки завершены, сохраните конфигурацию нажав кнопку . Приложение **Конфигуратор СКУД Elsys** можно закрыть.

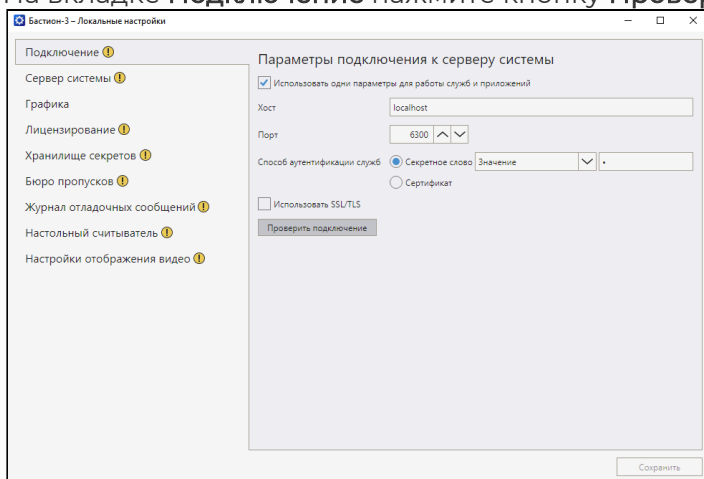
Подробнее с настройками программного сервиса можно ознакомиться в Руководстве администратора, которое загружается с сайта производителя совместно с установочным файлом.

3 ДОБАВЛЕНИЕ И НАСТРОЙКА ДРАЙВЕРОВ УСТРОЙСТВ

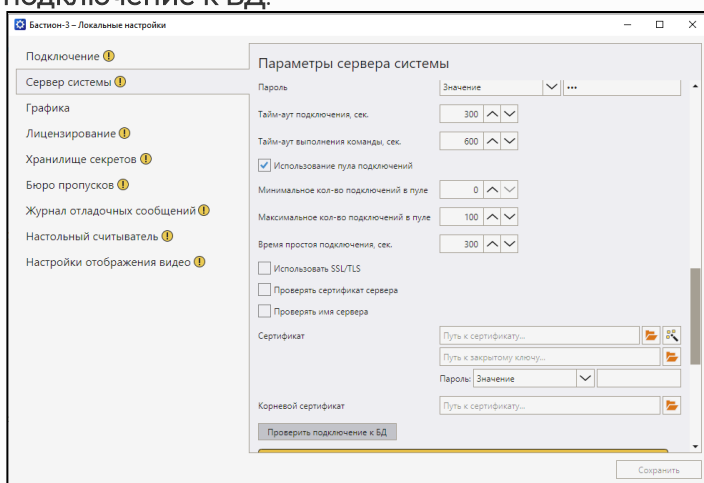
i Перед использованием ПК «Бастион-3» убедитесь, что лицензия активирована и все службы запущены.

Для проверки выполните следующие действия:

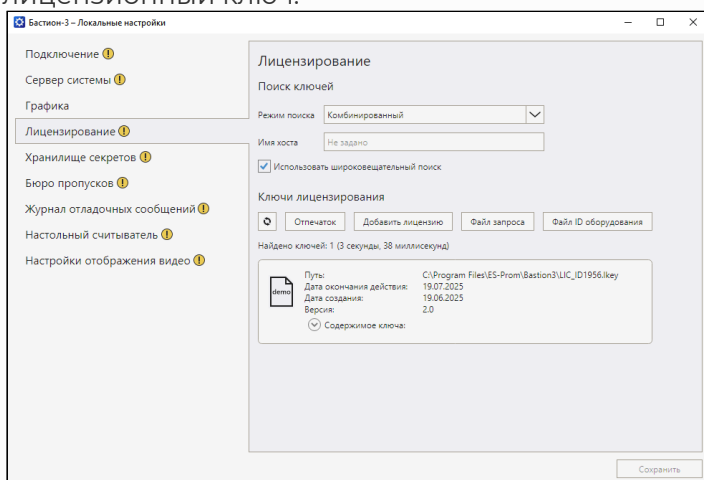
1. Запустите приложение **Локальные настройки**.
2. На вкладке **Подключение** нажмите кнопку **Проверить подключение**.



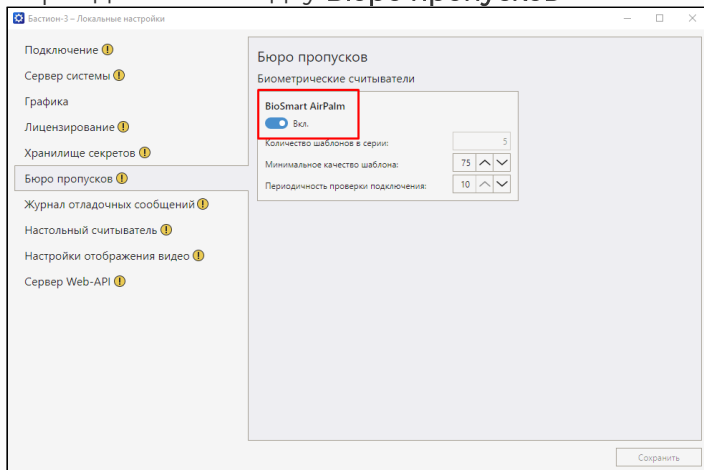
3. Перейдите на вкладку **Сервер системы** и нажмите кнопку **Проверить подключение к БД**.



4. Перейдите на вкладку **Лицензирование** и проверьте, что отображается лицензионный ключ.



5. Перейдите на вкладку **Бюро пропусков** и включите опцию **Вкл.**

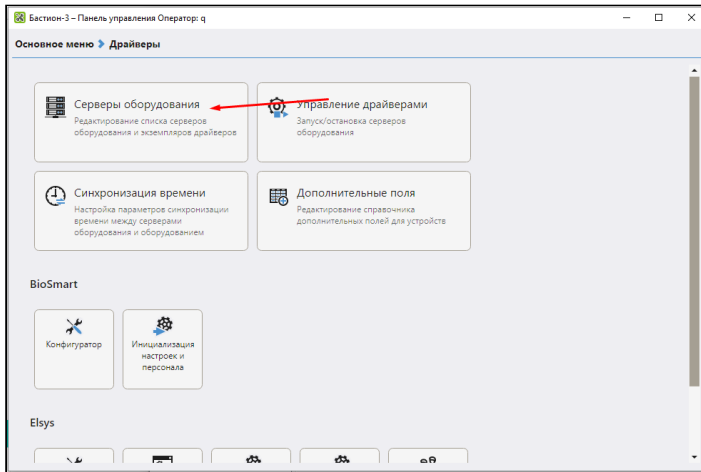
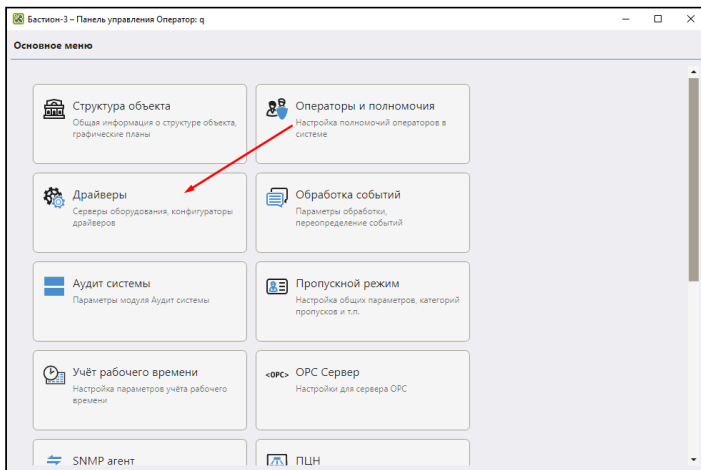


Для добавления и настройки драйверов выполните следующие шаги:

1. Добавьте драйверы

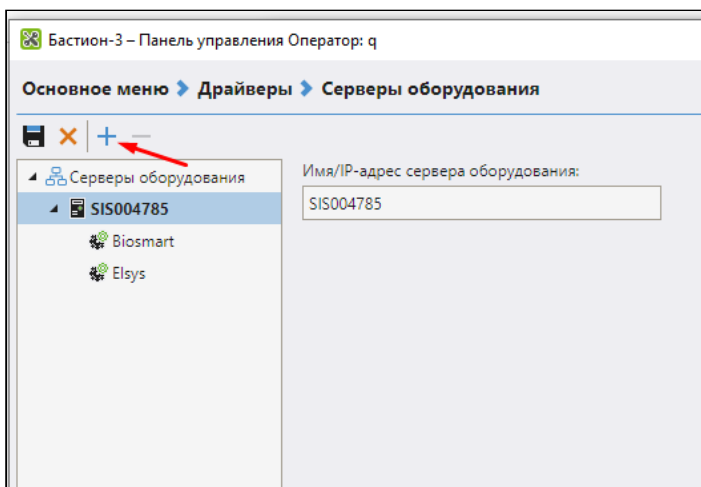
Откройте приложение **Панель управления** → введите пароль.

В основном меню выберите подраздел **Драйверы** → **Серверы оборудования**.



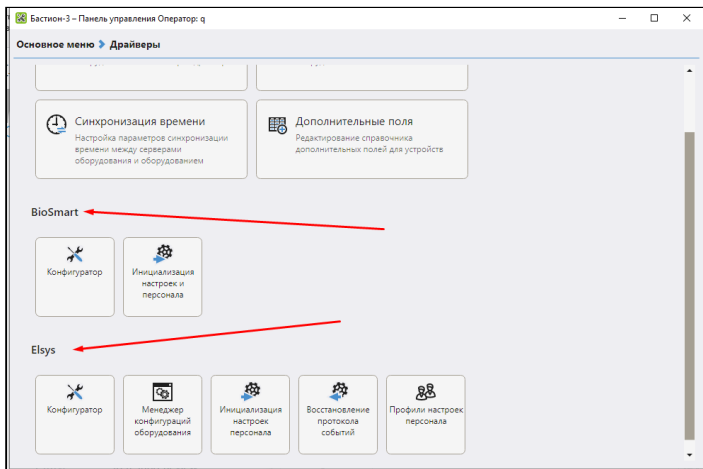
В открывшемся окне в дереве состава выберите сервер оборудования и нажмите кнопку **Добавить драйвер**.

Выберите тип драйвера из выпадающего списка, пропишите имя в поле выше. Для работы интеграции необходимо добавить драйвера **Бастион-3 - BioSmart**, **Бастион-3 - Elsys v2**.



Сохраните изменения нажав кнопку **Сохранить**. Перезапустите ПК «Бастион-3» и программный сервис Elsys-SDK II.

После перезапуска ПК «Бастион-3» перейдите на вкладку **Драйверы** и проверьте, что драйверы отобразились.



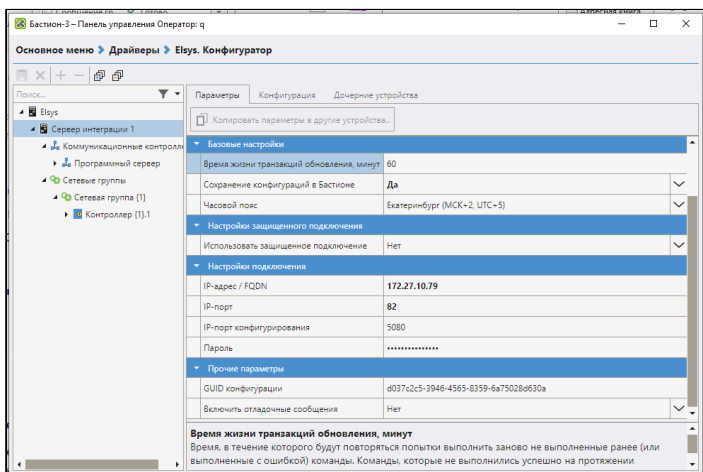
2. Настройте драйвер Elsys

В окне **Драйверы** нажмите кнопку **Конфигуратор** для драйвера Elsys.

В открывшемся окне укажите параметры сервера интеграции (IP-адрес, пароль), после внесения изменений нажмите кнопку **Сохранить**.

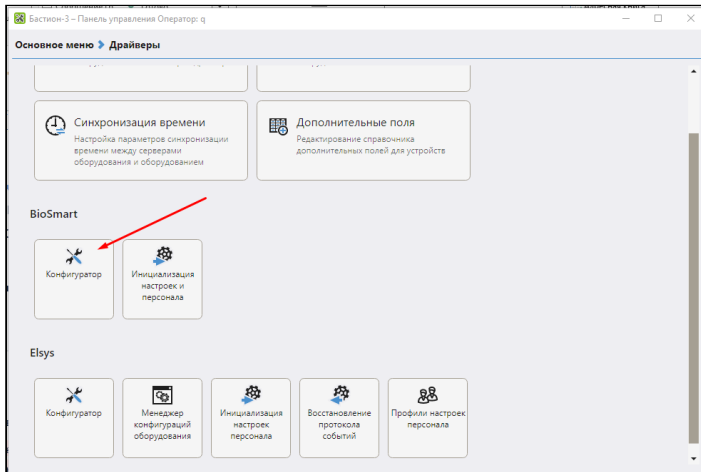
Для обновления конфигурации драйвера закройте окно **Elsys. Конфигуратор**, затем откройте. Дайте согласие на изменение конфигурации, затем на изменение названия устройства.

Убедитесь, что в дереве состава отображился контроллер.

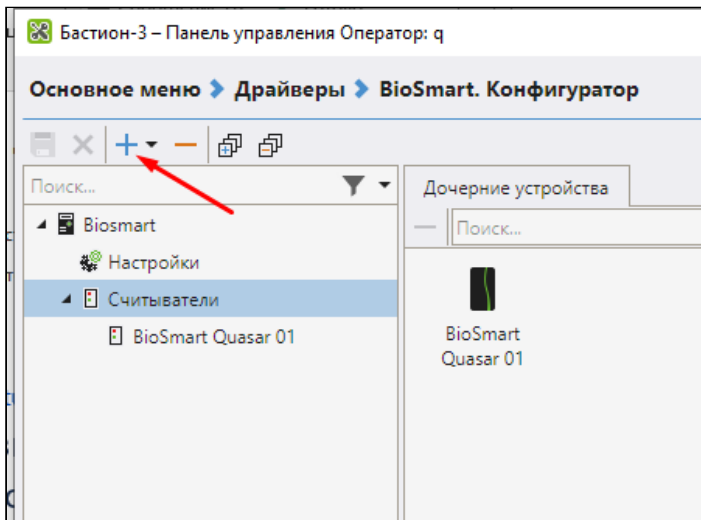


3. Настройте драйвер BioSmart

В окне **Драйверы** нажмите кнопку **Конфигуратор** для драйвера BioSmart.



В открывшемся окне в дереве состава выберите строку **Считыватели** → нажмите кнопку **Добавить**.



Из выпадающего списка выберите контроллер BioSmart UniPass Pro 2 или терминал BioSmart BioSmart Quasar 7. Далее настройка будет показана на примере терминала BioSmart Quasar 7.

Выберите добавленное устройство в дереве состава и заполните поля согласно изображению ниже.

Общие параметры	
Адрес	1
Использовать считыватель	Активен
Название	BioSmart Quasar7PV 01
Тип считывателя	BioSmart Quasar7PV
Часовой пояс	Екатеринбург (МСК+2, UTC+5)
Подключение	
IP адрес	172.27.10.5
Порт ТСР/IP	20002
Идентификация	
Длина кода карты	3 байта
Режим верификации	Карта и ладонь

Сохраните изменения нажав кнопку **Сохранить**.

i Для контроллера BioSmart UniPass Pro 2, считывателей BioSmart PalmJet 2 заполните следующие поля:

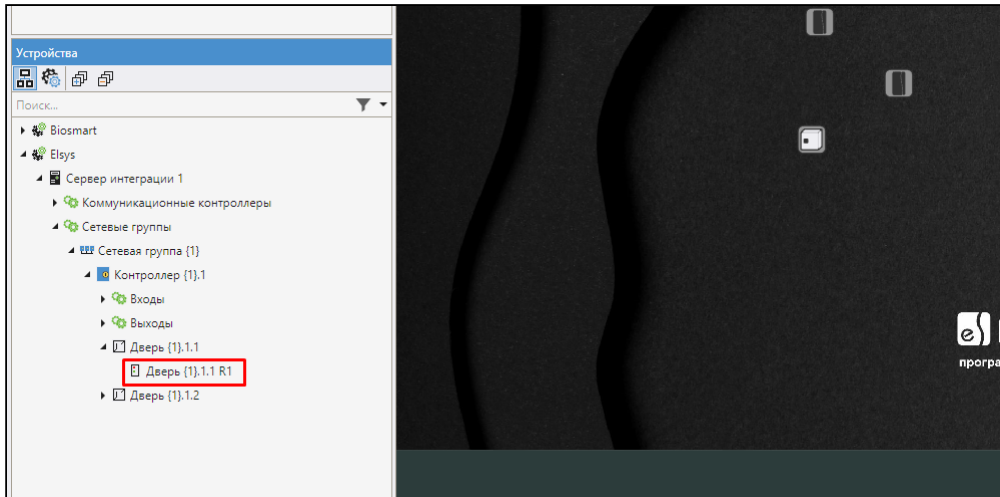
- **IP-адрес** укажите адрес контроллера;
- **Использовать два считывателя** выберите **Да** или **Нет**;
- **Серийный номер PalmJet 2** укажите последние 6 цифр серийного номера считывателя.

4 НАСТРОЙКА ПЛАНОВ, ДОСТУПА И ДОБАВЛЕНИЕ СОТРУДНИКОВ

Настройка планов

Для управления устройствами и просмотра текущего статуса устройств в системе необходимо настроить графические планы.

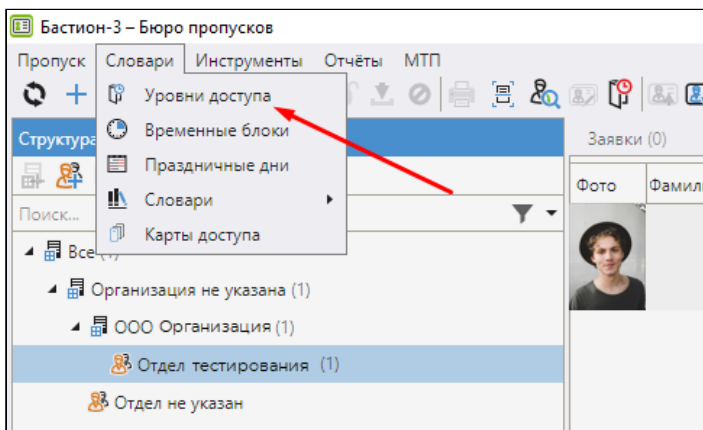
В приложение **Панель управления** выберите подраздел **Структура объекта** → **Графические планы**. В открывшемся окне раскройте дерево устройств → в списке выделите дверь, к которой подключено устройство → перенесите его на план.



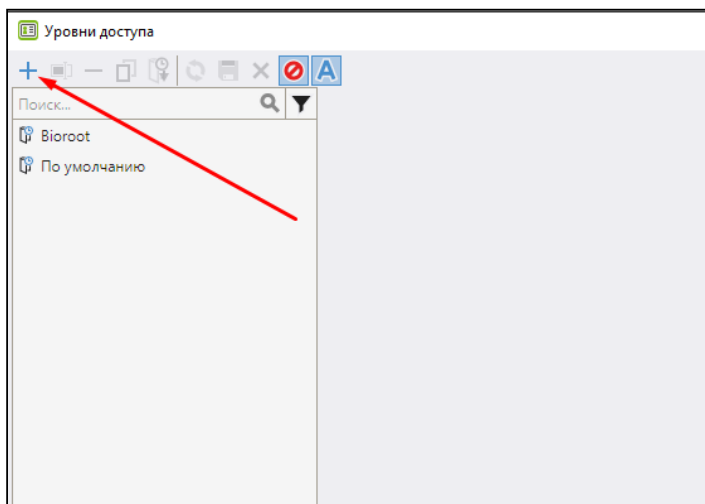
4.1 Создание уровней доступа

Для определения правил доступа сотрудника в помещения необходимо создать и настроить уровень доступа.

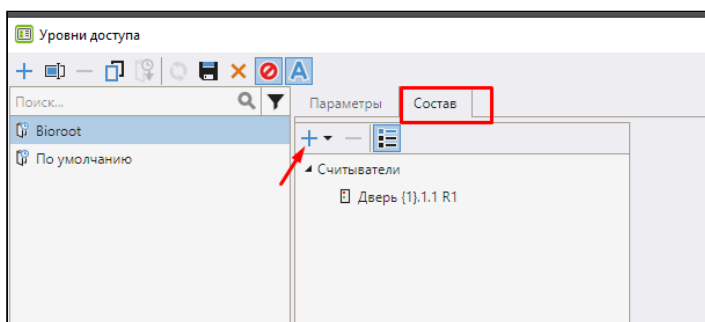
Откройте приложение **Бюро пропусков**. Нажмите **Словари** → **Уровни доступа**.



В открывшемся окне создайте уровень доступа с помощью кнопки **Создать уровень доступа**.



Задайте имя уровню доступа и нажмите кнопку **Enter** на клавиатуре.

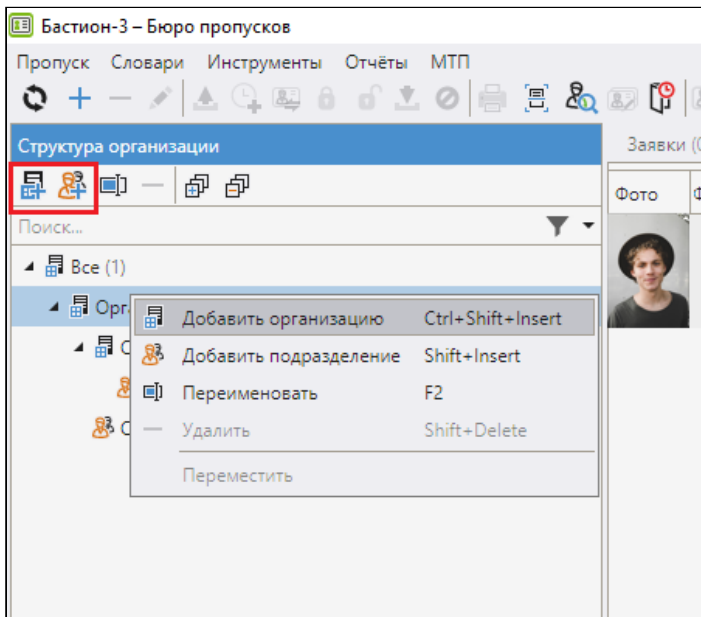


С порядком настройки уровня доступа (временных режимов, праздничных дней, доступных территорий и другого) можно ознакомиться в [Бастион-3 - Бюро пропусков. Руководство оператора](#).

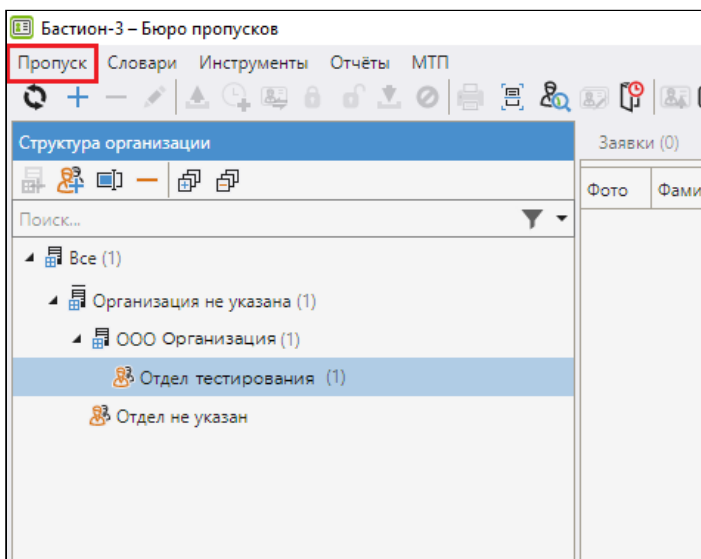
4.2 Добавление сотрудника

4.2.1 Создание карточки сотрудника

Для добавления сотрудника необходимо предварительно создать организацию и подразделение. Нажмите соответствующие кнопки на панели инструментов или вызовите контекстное меню правой кнопкой мыши.



Далее выберите подразделение в дереве состава → нажмите кнопку **Пропуск** → **Новая заявка**.



Заполните карточку сотрудника. На вкладке **Персона** обязательными для заполнения являются поля **Фамилия (1)**, **Должность (2)**, поля **Табельный номер** и **Корпоративный код** заполняются автоматически.

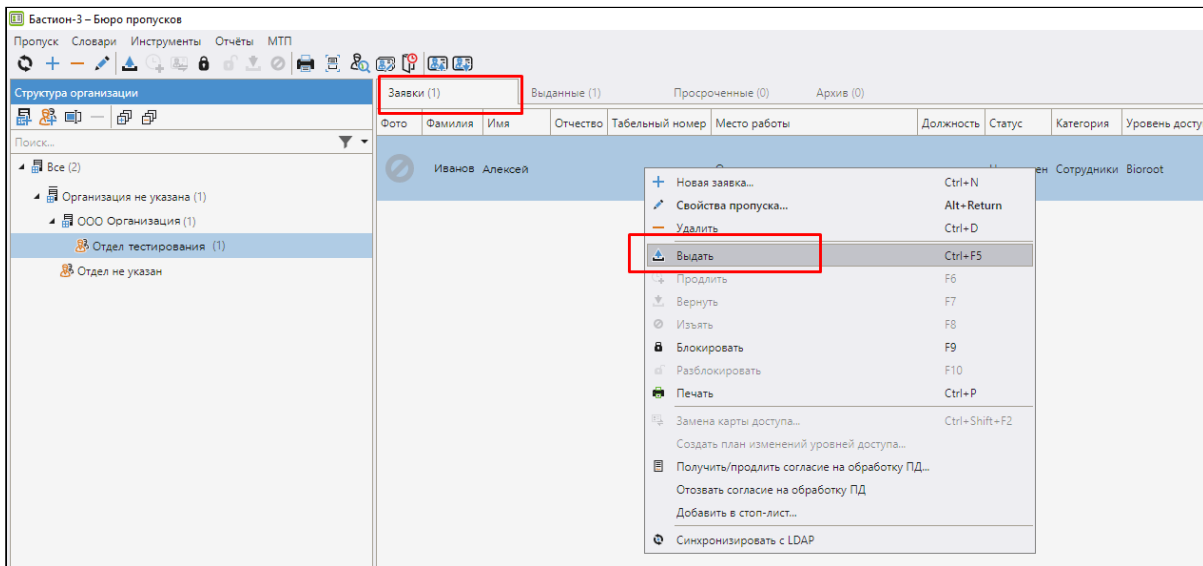
i Если для идентификации используется терминал BioSmart Quasar 7, то необходимо загрузить фотографию из файла (3) или получить с помощью цифрового устройства (4).

На вкладке **Пропуск** в поле **Категория** проверьте, что установлено корректное значение **Сотрудники**.

На вкладке **Уровень доступа** в поле **Уровень доступа** из выпадающего списка выберите группу доступа созданную ранее (см. раздел Настройка уровней доступа).

Затем нажмите кнопку **ОК**.

Перейдите на вкладку **Заявки**, выберите в списке новую заявку, нажмите на ней правой кнопкой мыши и в контекстном меню выберите пункт **Выдать**.



В открывшемся окне добавьте RFID-карту сотруднику вручную или с помощью настольного считывателя и нажмите **ОК**.

После этого заявка отобразится во вкладке **Выданные**.

i Если для идентификации используется терминал BioSmart Quasar 7 и в карточку сотрудника добавлена фотография, то редактирование данных сотрудника завершено.

4.2.2 Регистрация биометрических шаблонов вен ладони

Для регистрации биометрических шаблонов вен ладони рекомендуется использовать настольный считыватель BioSmart AirPalm.

Перед регистрацией шаблонов установите драйвер, который можно скачать с сайта bio-smart.ru в разделе **Техподдержка** → **ПО** → вкладка **Драйверы**, и подключите считыватель к ПК.

В карточке сотрудника перейдите на вкладку **Биометрия**, выберите биометрический считыватель BioSmart AirPalm и нажмите кнопку **Добавить**.

Следуйте инструкциям на экране и зарегистрируйте биометрический шаблон. После сканирования нажмите кнопку **ОК**. Карточку сотрудника можно закрыть.

5 МОНИТОРИНГ СОБЫТИЙ В ПК «БАСТИОН-3»

Откройте приложение **Панель управления**. Из основного меню перейдите на вкладку **Драйверы** и нажмите **Инициализация настроек персонала**.

Запустите приложение **Пост охраны**. В главном окне отобразится ранее созданный план объекта с устройствами, а также список событий, связанных с ними.

