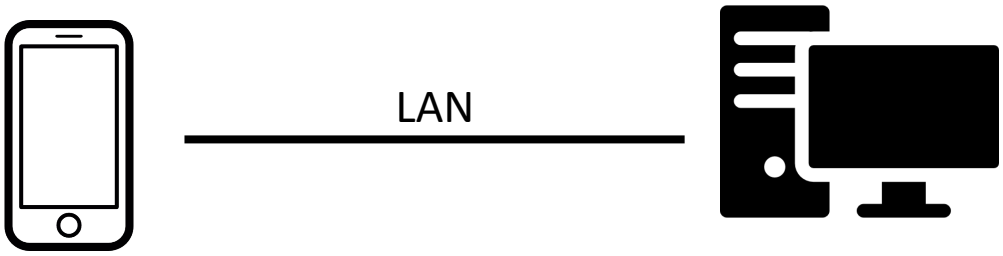
Добавление устройств ZKTeco в ПО

Пошаговая инструкция по добавлению устройств СКД и УРВ в программное обеспечение BioTA и BioCVSecurity (BioAccess IVS)

09.2023 г.

Оглавление

1. Подключение терминала к серверу



1.1 Выбор режима

Терминалы последних версий, могут работать в двух режимах – это СКУД и УРВ.

В зависимости от выбранного режима его можно добавить в то или иное ПО (BioTA или BioCVSecurity\BioAccess).

1.2 Переключение режима работы терминала

Если терминал на данный момент находится в неподходящем режиме его можно переключить.

Для этого мы заходим в **меню** терминала -> **Система** -> **Режим работы**. И выбираем нужный.

(Если в терминале отсутствует данная опция, обратитесь в службу технической поддержки. Специалисты смогут подключиться и выполнить эту процедуру удаленно)

1.3 Узнаем IP-адрес сервера

В нашем случае, сервером выступает компьютер с установленным ПО ZKTeco.

В дальнейшем, нам будет нужен его IP-адрес. О том, как его узнать можно прочесть в интернете.

1.4 Порты

Кроме IP нам нужно будет знать порт связи с программой.

Порты могут отличаться в зависимости от ПО, которое вы планируете использовать.

Указать нужный порт можно в процессе установки программы, либо в процессе работы.

Где посмотреть порт?

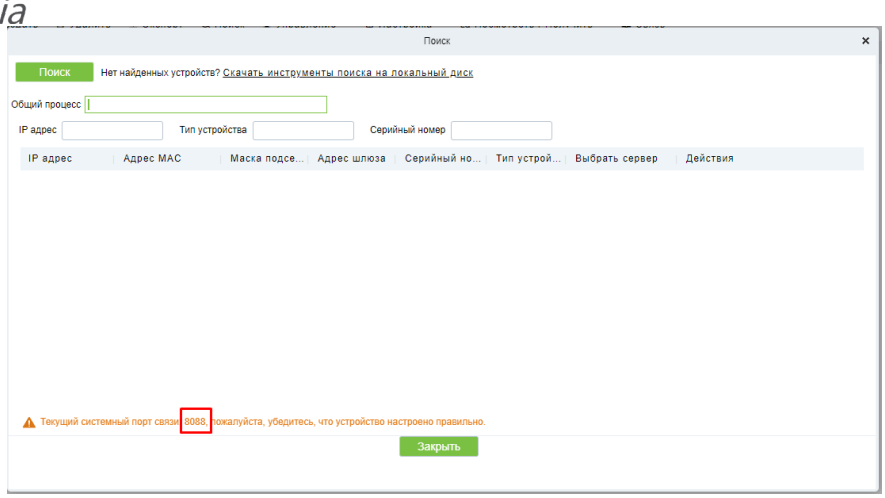
- BioTA 8.0

В консоли сервера. Консоль находится в трее и запускается вместе с ОС. Если по какой-то причине консоль не была запущена ее можно найти и открыть в фалах программы.

- BioCVSecurity & BioAccess

В модуле **Доступ** необходимо зайти в раздел **Устройства** и открыть поиск.

Программа сама подскажет необходимый порт подключения.



Порты связи по умолчанию:

Для BioCVSecurity & BioAccess: 8088

Для BioTA: 80

1.5 HTTPS

Это расширение протокола HTTP, который отвечает за передачу гипертекстовой разметки.

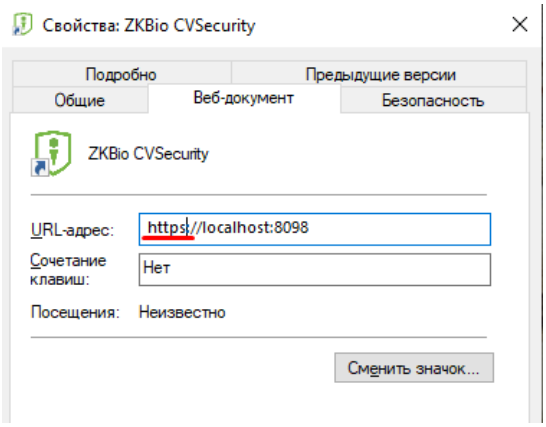
Как и порты программы, опция https может быть включена при установке программы. Инженеры не рекомендуют использовать ее, если предполагается, что устройства будут работать, исключительно, в пределах локальной сети.

Где посмотреть https?

Самый простой способ проверить используется ли сейчас шифрование – в свойствах ярлыка программы.

Для этого находим ярлык с программой на рабочем столе и нажимаем ПКМ, выбираем Свойства и проверяем.

Так же, можно проворить https можно в консоли программы.

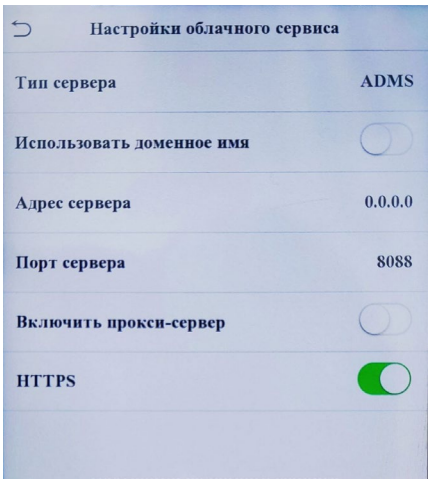


1.6 Настройки облачного сервиса

Теперь нам необходимо прописать полученные параметры.

Для этого мы открываем **меню** в терминале -> **Связь** -> **Настройки облачного сервиса**.
Тут мы указываем то, что узнали выше.

Все остальные параметры можно оставить по умолчанию.



(Https необходимо включить или выключить в зависимости от того, включен ли он в программе)

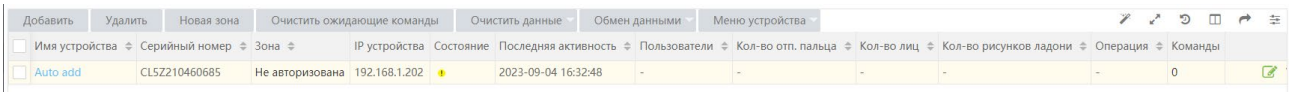
1.7.1 Поиск и добавление в BioTA 8.0

Теперь мы закончим настройку на стороне сервера. Заходим в программу.

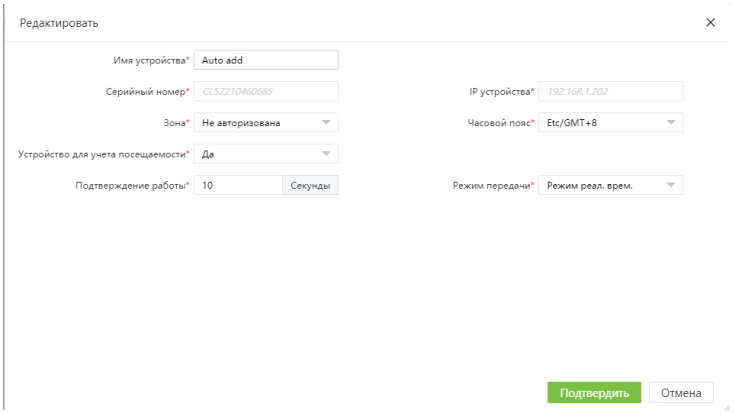
ZKBio TA 8.0

После логирования в ПО мы переходим в модуль **Устройства**.

Если все было сделано верно, то мы сразу увидим терминал в списке устройств.



Далее нажимаем на имя устройства и заполняем форму.

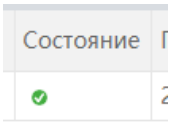


Обратите внимание, что зона должна быть отличная от зоны по умолчанию!

Первая зона не участвует в обмене данных. Необходимо создать другую, не объявляя первую зону родительской.

Подтверждаем применение параметров.

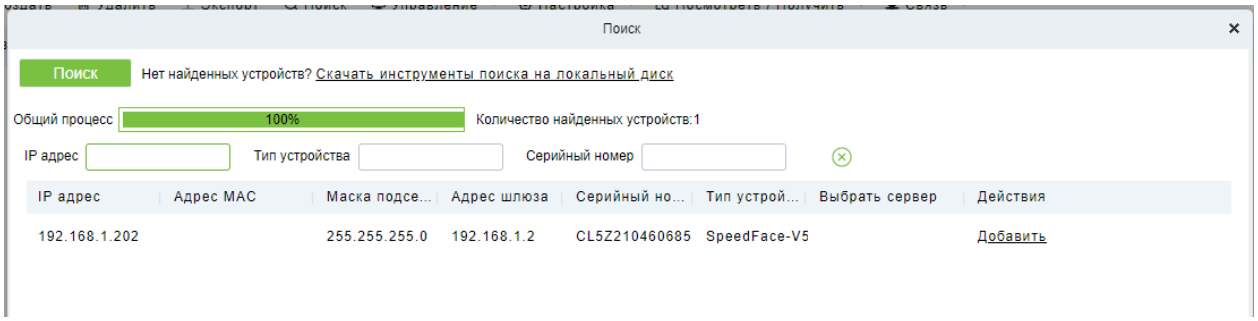
Если все сделано верно, то статус Состояние будет «зеленой галочкой».



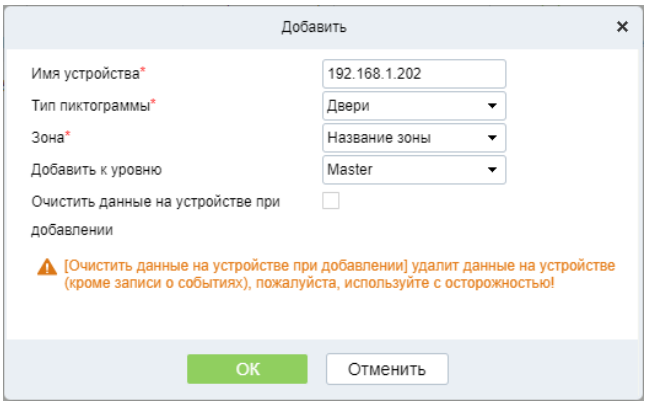
1.7.1 Поиск и добавление в BioCVSecurity

Чтобы завершить настройку в ПО для контроля доступа заходим в модуль **Доступ**, раздел **Устройства** и нажимаем «поиск».

Программа просканирует сеть и найдет устройство.



Нажимаем «**Добавить**» и заполняем форму.



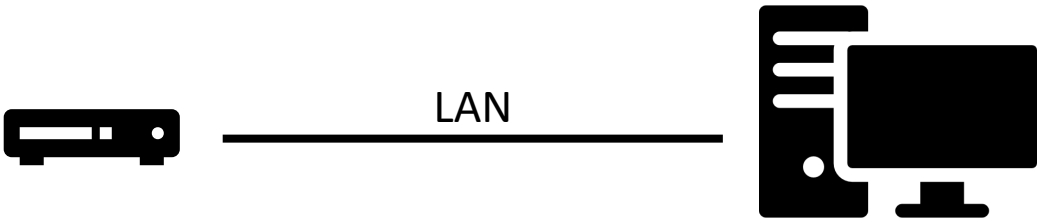
Нажимаем «Ок», получаем уведомление об авторизации устройства.

Далее обновляем страницу и устройство появится в списке и будет готов к использованию.

В BioCVSecurity есть возможность добавлять терминалы в режиме УРВ в модуль **Посещаемость** напрямую.

Шаги по добавлению идентичны добавлению в модуль **Доступа.** Кроме того, что искать их нужно в модуле **Посещаемость -> Управление устройствами -> Устройства посещаемости. И терминал должен находится в режиме УРВ.**

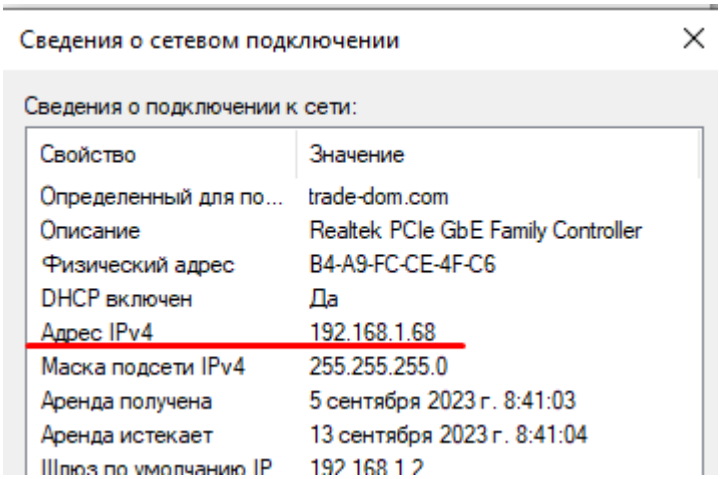
2. Подключение контроллера к серверу



2.1 Одна подсеть

Устройства и сервер должны находится в одной подсети. По умолчанию у контроллеров установлен IP-адрес **192.168.1.201**. Необходимо добавить компьютеру адрес той же подсети. В дальнейшем IP-адрес можно будет поменять.

(Как поменять или добавить IP-адрес можно прочесть тут)



Внимание!

1. Контроллеры могут быть добавлены только в ПО СКУД (BioCVSecurity, BioAccess)

В BioTA контроллеры добавить не получится!

2. Популярные контроллеры серии C3, C5 являются Pull-устройствами. Чтобы добавить их в систему, следует убедится в том, что лицензия имеет соответствующую опцию. Проверить это можно в информации о системе. Если данная опция отсутствует – обратитесь к менеджерам.

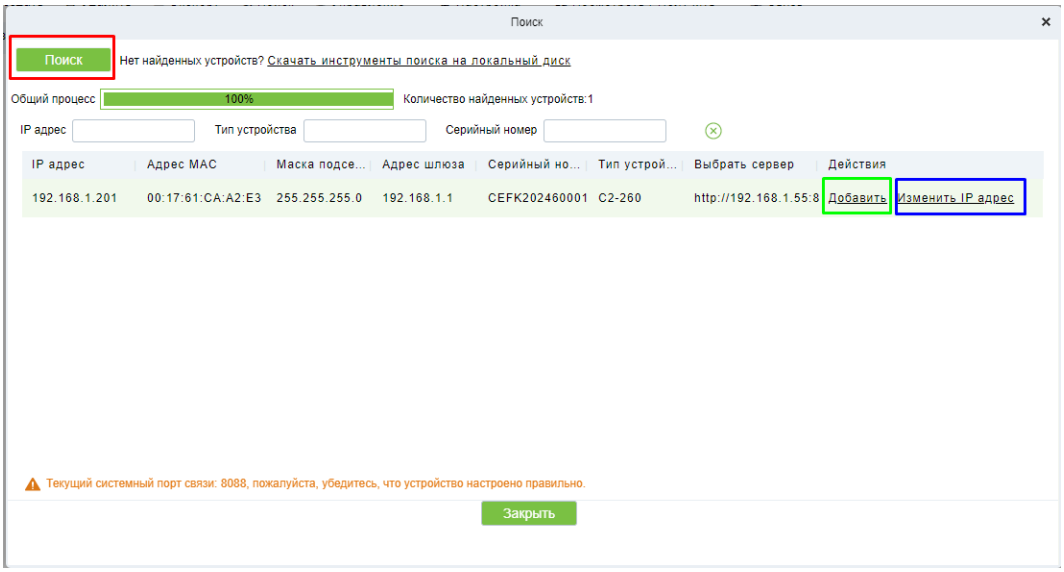
3. Так же, следует учесть, что все контроллеры занимают точки прохода соответствующее количеству поддерживаемых ими дверей.

К примеру, С2-260 работает с двумя дверьми, а значит после добавления будет резервировать сразу 2 точки прохода. Вне зависимости от того, используется ли эта дверь.

2.2 Поиск контроллера в ПО

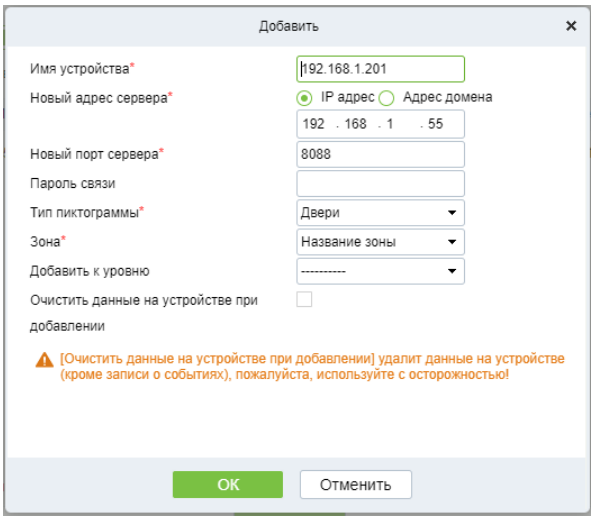
Заходим в программу, переходим в модуль Доступ, раздел Устройства и нажимаем «**поиск**».

После сканирования сети программа должна обнаружить устройство. Можно будет сразу изменить IP-адрес или добавить контроллер в систему.



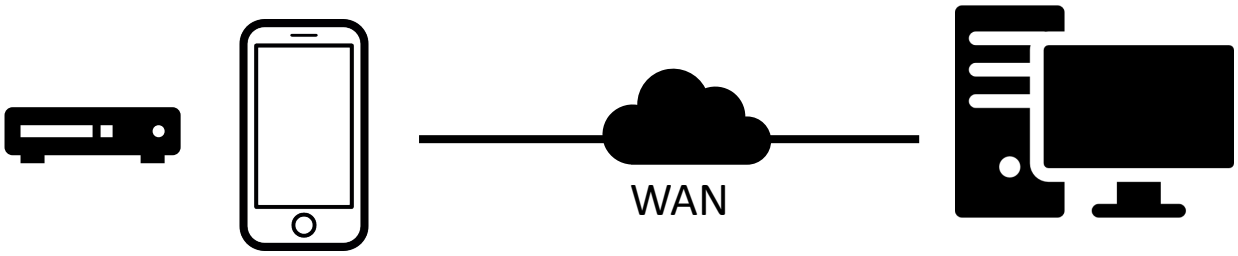
На финальном этапе подключения необходимо заполнить форму. Внимательно заполните все поля. Адрес сервера – это адрес ПК с установленной программой. Пароль связи заполнять не обязательно. Остальные поля можно оставить по умолчанию.

Нажимаем «Ок» и система предупредит нас о том, что контроллер будет доступен после перезагрузки. Ждем некоторое время и обновляем страниц чтобы убедиться в том, что устройство появилось в программе.


Добавить
Имя устройства*
192.168.1.201
Новый адрес сервера*
IP адрес
Адрес домена
192 . 168 . 1 . 55
Новый порт сервера*
8088
Пароль связи
Тип пиктограммы*
Двери
Зона*
Название зоны
Добавить к уровню

Очистить данные на устройстве при добавлении
[Очистить данные на устройстве при добавлении] удалит данные на устройстве (кроме записи о событиях), пожалуйста, используйте с осторожностью!
OK
Отменить

3. Подключение устройств через WAN



Метод подключения устройств через интернет, в сущности, ничем не отличается от подключения устройств в локальной сети.

Способ 1. Использовать VPN-туннель.

Это шифрованный канал передачи данных, который позволяет связывать объекты через Интернет в локальную сеть. Он повсеместно используется в крупных и средних организациях, где необходима общая сеть между филиалами.

В этом случае, алгоритм подключения устройств не будет отличаться от описанного выше. Однако, необходимо убедиться, что порты необходимые для работы ПО открыты и сегменты сети связаны между собой.

Способ 2. С использованием внешнего IP-адреса.

Для этого потребуется получить у вашего провайдера внешний («белый») IP-адрес, который и будет использоваться в качестве адреса сервера.

Если внешний адрес уже есть, необходимо убедиться, что порты связи ПО открыты (см. пн. 1.4) для внешнего использования, а также настроить «проброс» на маршрутизаторе.

Для терминалов нам необходимо указать в качестве адреса сервера, в настройках облачного сервиса (см. пн.1.6) внешний IP.

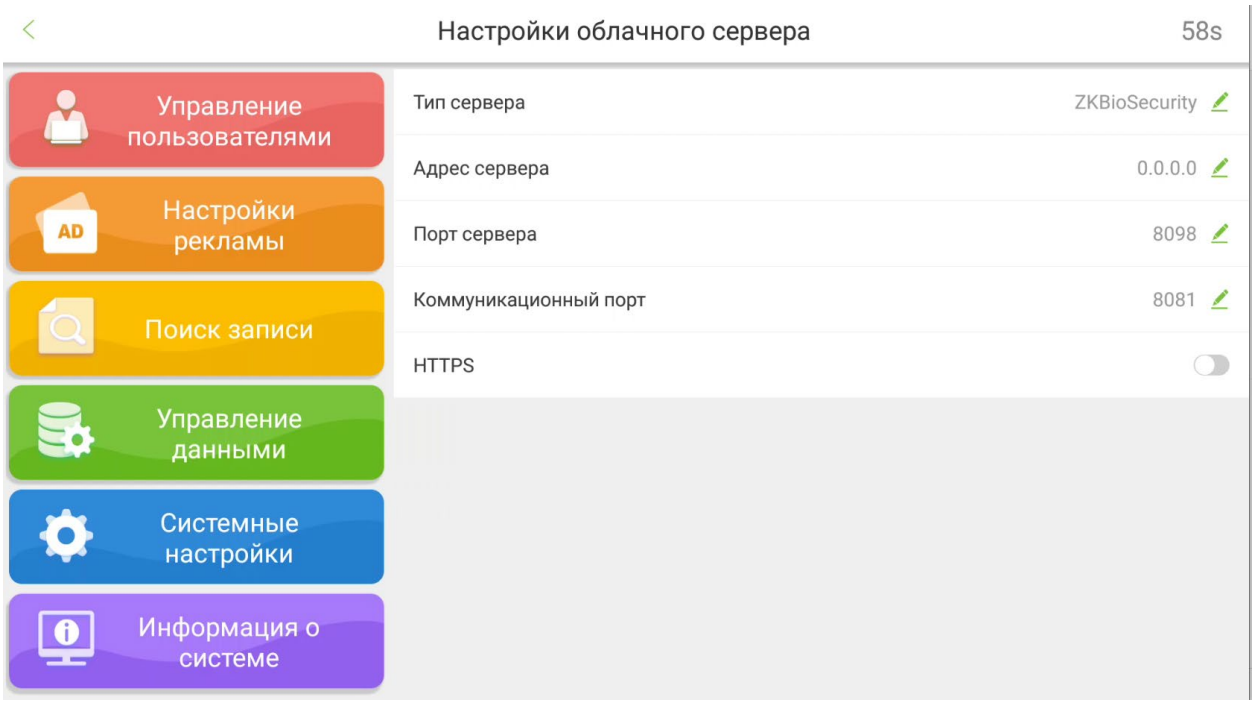
Для контроллеров адрес сервера мы сможем задать в веб-интерфейсе устройства.

(Для такого подключения рекомендуется использовать контроллеры серии InBio).

4. Подключение специализированных устройств (FaceKiosk)

Подключение FaceKiosk на стороне устройства происходит так же, как и в обычном терминале. Т.е. по средствам настройки облачного сервиса. (см пн 1.1-1.6)

В устройстве заходим в **меню -> Системные настройки -> Настройки связи -> Настройки облачного сервиса.**



Тип сервера – это режим работы устройства. (см. пн 1.1)

Адрес сервера – это IP сервера с установленным ПО

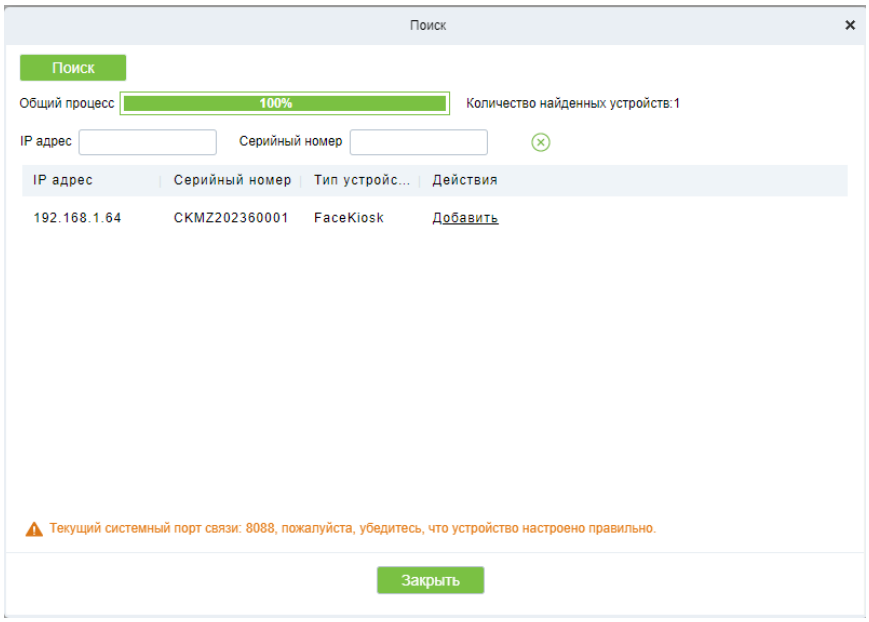
Порт сервера – это порт по которому мы получаем доступ к веб-интерфейсу (по молчанию 8098)

Порт коммуникации – это порт для обмена данными между устройством и сервером (по молчанию 8088)

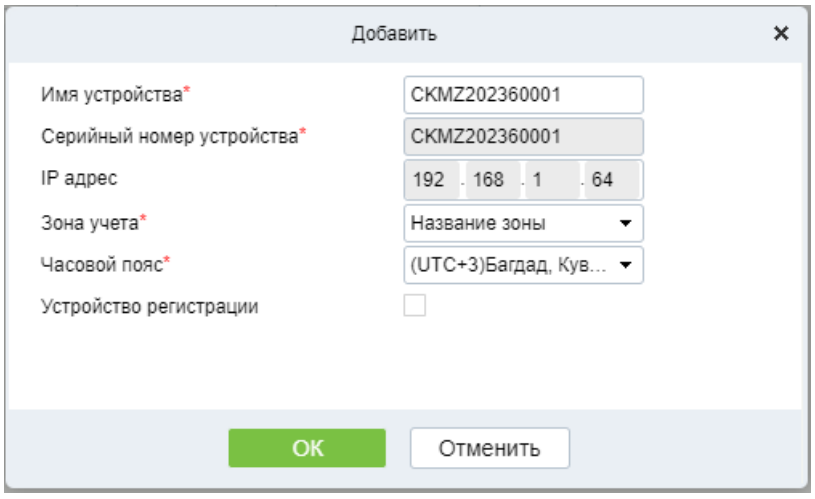
HTTPS – это шифрование. Его использование опционально. Проверка этого параметра описана в пн 1.5.

Подключение FaceKiosk на стороне сервера. Заходим в ПО и переходим в модуль **FaceKiosk**, раздел **Устройства** и нажимаем «Поиск».

Если все сделано верно, программа просканирует сеть и найдет устройство.



Нажимаем «**Добавить»**, выставляем необходимые параметры в открывшейся форме и жмем **Ок**.



5. Возможные проблемы при подключении

- Защита ОС и сети

Частой проблемой при подключении и обменом данными между устройством и сервером может являться безопасность ОС или сети.

Если вы следовали всем пунктам, но устройство так и не нашлось в программе, следует:

1. проверить политики безопасности;
2. проверить доступность портов;
3. проверить файрволы и антивирусное ПО.

- Разные подсети

Стоит отметить, что инженеры рекомендуют использовать отдельную подсеть для работы устройств и сервера. Несмотря на то, что устройство и сервер могут «видеть» друг друга в разных сегментах сети, это может мешать обнаружить устройство в программе и обмену данными между ними.

- Человеческий фактор

Пожалуй, самой частой проблемой является ошибки в настройках. Пожалуйста, проверьте описанные выше инструкции. Особое внимание обратите на состояние настроек HTTPS (пн. 1.5).

- Ограничения лицензии

Количество подключаемых устройств ограничено лицензией. Чтобы узнать, сколько устройств вы можете добавить в тот или иной модуль, нужно проверить раздел «информация о системе».

Так же, система сама предупредит вас о том, если вы попытаетесь добавить устройств больше установленного максимума.

Если возникла такая ситуация, пожалуйста, обратитесь к менеджерам за расширенной лицензией.

6. Использование добавленных устройств в других модулях

Иногда, возникает необходимость задействовать уже добавленные терминалы в других модулях.

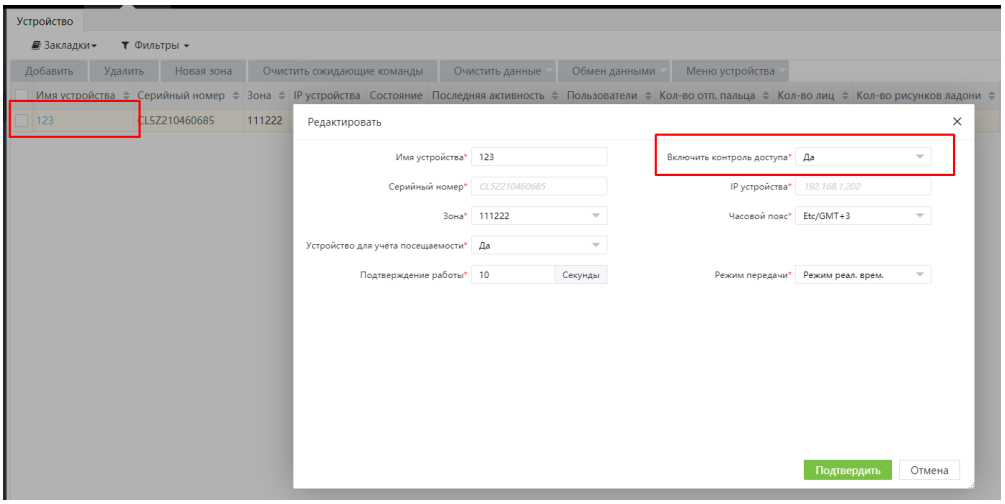
Например, для получения информации о проходах, через устройства доступа или расширить настройки СКУД в программе BioTA.

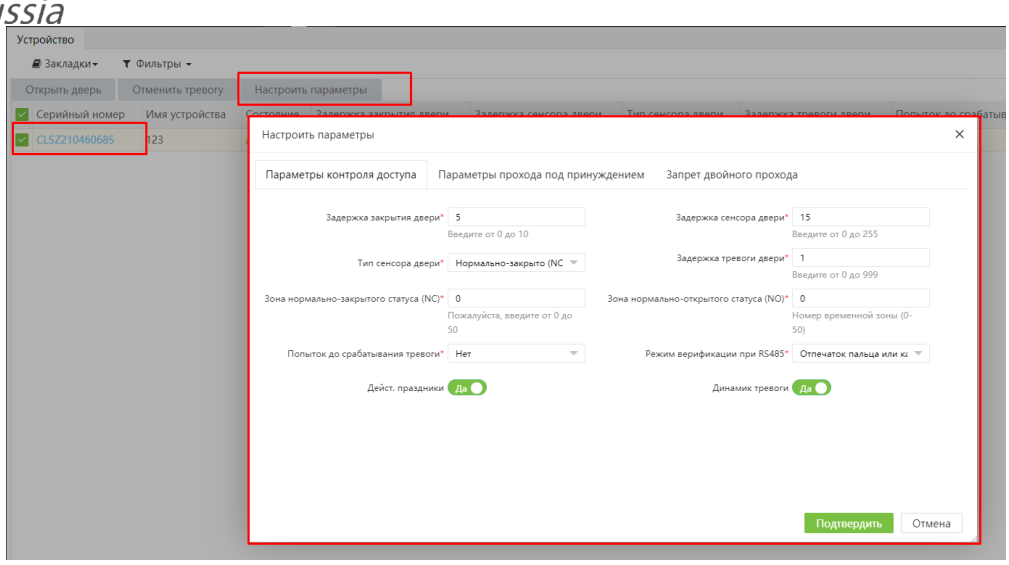
6.1 СКУД в BioTA

Гибкость настроек СКУД в BioTA ограничена доступом в помещение лиц, находящихся в пределах одной зоны с терминалом.

Логику настроек можно сделать более гибкой, если терминал будет «проброшен» в модуль **Доступ**.

Чтобы это сделать потребуется зайти в список уже добавленных устройств, зайти в параметры нужного терминала и указать «Да» в графе «Включить контроль доступа». Теперь можем найти терминал в модуле Доступ и настроить правила доступа.





Примечание:

1. Пункт «Включить контроль доступа» можно будет активировать только в добавленное устройство.

При первом добавлении в программу этот пункт меню не отображаться.

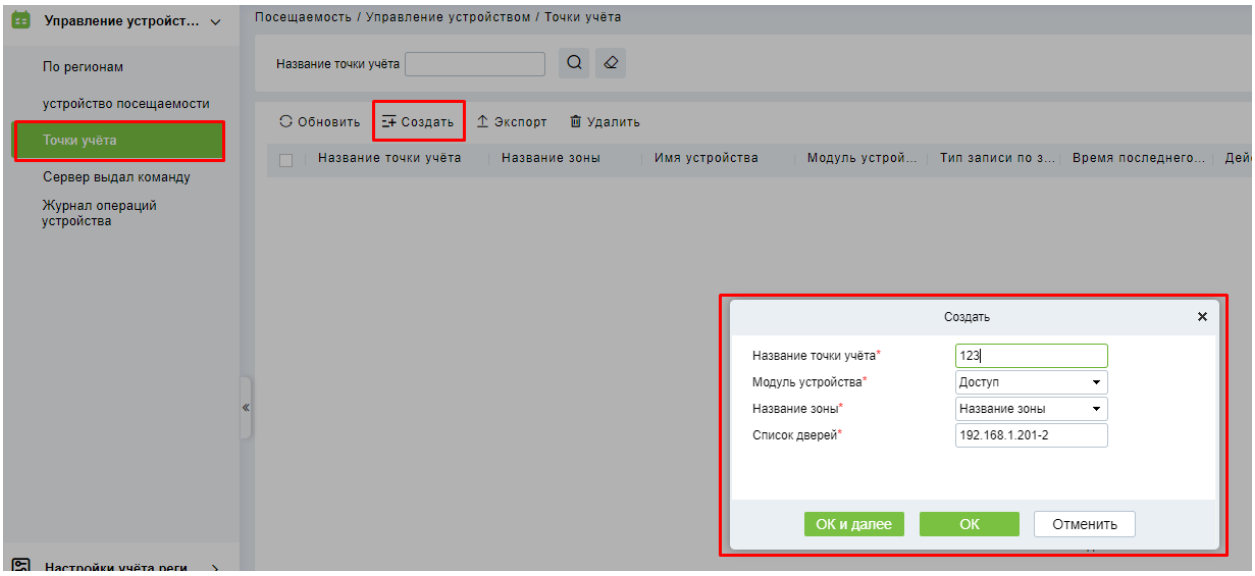
2. Не все устройства могут быть добавлены в модуль Доступ. Уточните это при покупке.

3. Если захотите удалить терминал из программы, предварительно его нужно удалить из модуля Доступа. В противном случае, программа выдаст ошибку.

6.2 УРВ в BioCVSecurity

Для сбора данных о событиях и формирования на их основе отчетов необходимо использовать модуль **Посещаемость**. Добавить в него устройства можно напрямую (см пн. 1.7.b), либо использовать уже добавленные ранее устройства в модуле **Доступ**.

Чтобы произвести настройку переходим в **модуль Посещаемость -> Точки учета** и нажимаем **«Создать».**



В открывшейся форме заполняем поля:

Модуль устройства – это список модулей из которого мы будет получать данные с устройств (в нашем примере «Доступ»)

Список дверей. Нажав на пустое поле, открывается меню, где перемещением из левой колонки в правую мы создаем привязку точки прохода к точке учета.

Нажимаем «Ок» и настройка завершена!

Примечание:

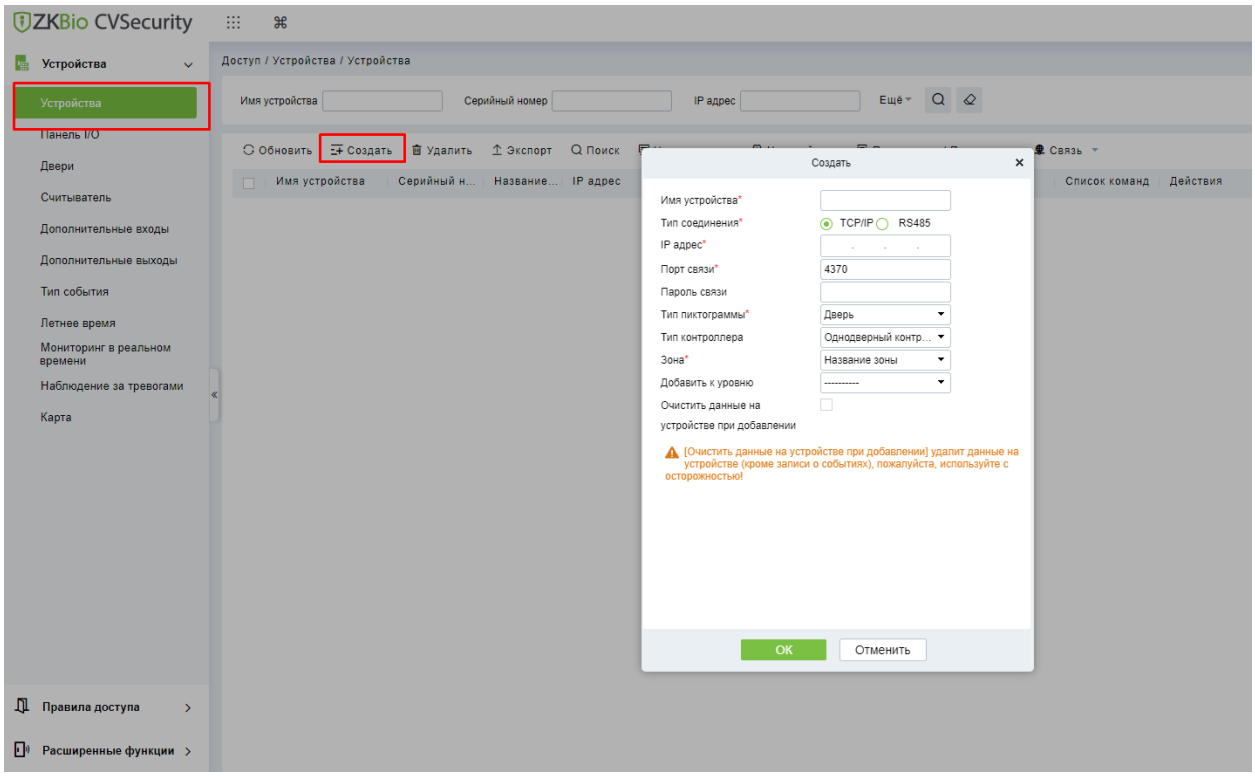
1. Если захотите удалить устройство из программы, предварительно его нужно удалить из модуля Посещаемость. В противном случае, программа выдаст ошибку.
2. К одной точке учета можно привязать только одну точку доступа.
3. Количество точек учета так же может быть ограничено лицензией, обратите на это внимание при проектировании.

7. Добавление Pull-терминалов в ПО СКД.

В последнее время, все чаще возникает необходимость миграции оборудования с более старого ПО на новое.

К примеру, терминал F-16 может быть добавлен в ПО СКУД по IP адресу.

Для этого заходим в программу -> модуль **Доступ** –> **Устройства** и в панели инструментов нажимаем «**Создать**».



Перед нами откроется форма, в которой нам необходимо заполнить:

1. Имя устройства;
2. Тип соединения (обычно TCP\IP);
3. IP адрес терминала;
4. Порт связи (обычно остается по умолчанию. Если не подходит смотрите в настройках связи в терминале или сбросьте устройство к заводским настройкам);
5. Пароль связи (можно оставить пустым).

И остальные настройки по необходимости.
Нажимаем ОК. И терминал появится в общем списке используемых устройств.

Примечания:

1. Данный способ подключение распространяется на ограниченный список pull-устройств. Во всех иных случаях, корректное подключение описано в пн. 1 данного руководства. (о совместимости устройств и ПО проконсультируйтесь со специалистом технической поддержки)
2. Программа должна поддерживать формат Pull-устройств в лицензии. Проверить это можно в информации о системе.
   Например: