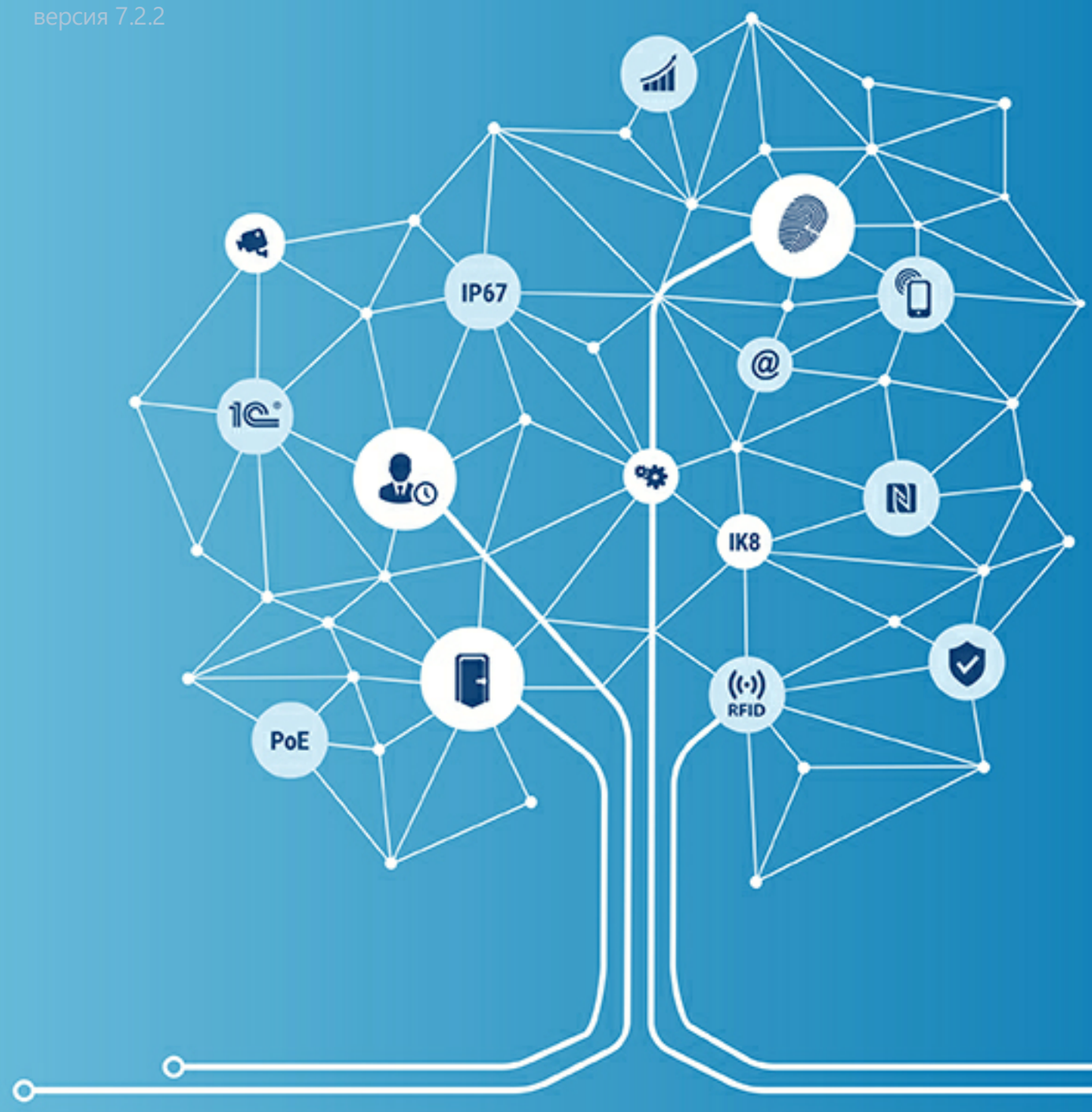
Подсистема
Управление доступом

Руководство пользователя

версия 7.2.2



Соглашения, используемые в книге

В этой книге используются следующие соглашения о шрифтах:

- *курсив* — используется при ведении новых терминов и указаний текстовых значений переменных,
- **полужирное начертание** — используется для выделения названий элементов окон,
- ***полужирный курсив*** — используется для выделения названий окон,
- «кавычки» — используются для выделения названий приложений и пунктов меню.

Оглавление

1

Подсистема Управление доступом

Подсистема Управление доступом задает права доступа на объект: в какие помещения может проходить сотрудник и в какое время. С помощью подсистемы, например, можно разрешить доступ менеджерам только в их отдел и запретить доступ в серверную, разрешить вход в офис ночью только охране и так далее.

Особенности подсистемы:
- назначает права доступа сотрудникам и гостям предприятия.
- настраивает права доступа различных подсистем в одном интерфейсе. Если у вас установлены разные контроллеры, например, Suprema и Apollo, настройка прав для них не будет различаться.
- показывает ошибки и неточности прав доступа. Например, подсистема предупредит, если на карте установлено альтернативное время прохода, но контроллер не разрешает его использовать.
- поддерживает все функции оборудования: всё, что умеют делать контроллеры, можно настроить в APACS Bio.

В текущей версии подсистема поддерживает следующее оборудование:
- контроллеры СКД Suprema,
- контроллеры СКД Suprema 2.

Основные объекты подсистемы Управление доступом

Доступ настраивается с помощью следующих объектов: *Владелец карты*, *Идентификатор*, *Уровень доступа*, *Группа доступа*.

- *Владелец карты* — объект, содержащий информацию о сотруднике.
- *Идентификатор* — объект, который ассоциируется с картой, брелоком или ключом на руках сотрудника.
- *Биоданные* — объект системы, который хранит данные об отпечатке или скане лица сотрудника.
- *Уровень доступа* — объект, определяющий территорию, куда может проходить сотрудник и время, в которое он может это делать.
- *Группа доступа* — объект, включающий в себя один или несколько уровней доступа контроллеров. Группа доступа назначается сотруднику или идентификатору.

Эти объекты позволяют гибко назначать права доступа владельцам карт/идентификаторам в рамках контролируемой территории.

1.1 Принципы настройки доступа

Для доступа на предприятие сотруднику выдается карта или заводятся в базе отпечатки пальца/лица. Также определяются зоны доступа сотрудника: помещения, ограниченные считывателями, куда он может проходить, например, столовая и склад.

Чтобы сотрудник мог проходить по считывателям, системе необходимо знать две вещи: считыватели, доступные сотруднику и время, в которое он может проходить по этим считывателям.

Считыватели берутся из зоны доступа сотрудника. Время прохода указывается в объекте ***Временная зона***. Затем временная зона вместе со считывателями указываются в объекте ***Уровень доступа***.

Уровень доступа указывается в объекте ***Группа доступа***. В свою очередь ***Группа доступа*** назначается сотруднику и наделяет его правами доступа.

Смотри также: пример настройки доступа

1.2 Пример настройки доступа

Пример настройки доступа для четырех контроллеров Suprema BioEntry W2.

Рассмотрим настройку прав доступа на следующем примере:

- предприятие состоит из двух помещений: офиса и кабинета директора, который находится внутри офиса.
- каждая дверь, в офис и в кабинет директора, имеет по два считывателя: один на вход и один на выход.

Схема предприятия

Необходимо настроить права доступа с условиями:

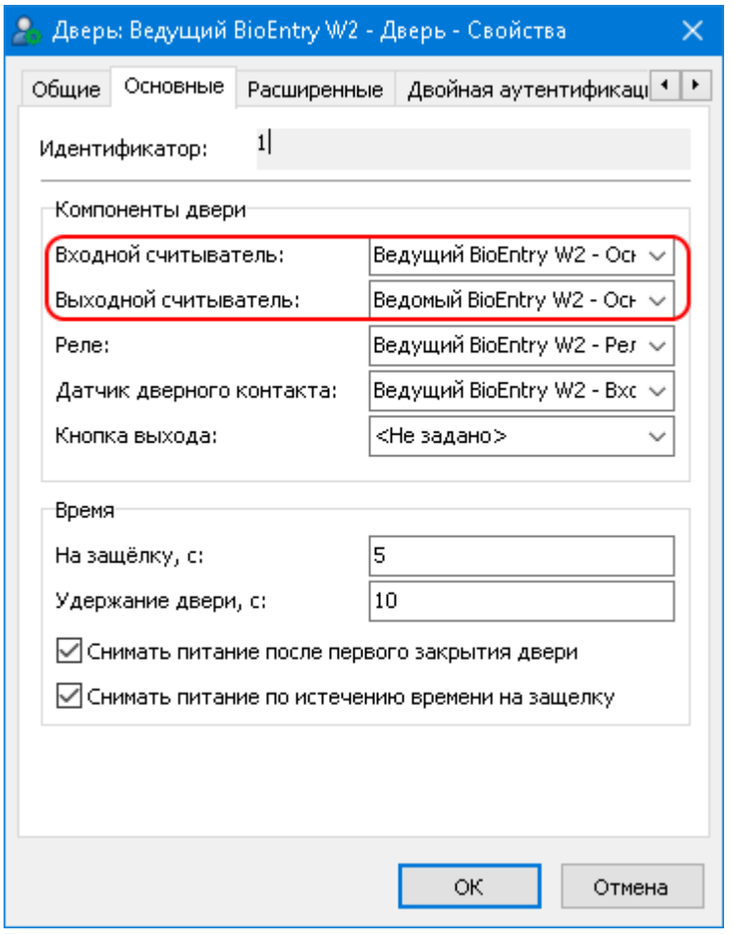
- сотрудники предприятия могут входить в офис с понедельника по пятницу с 9:00 до 18:00,
- директор может входить в офис и свой кабинет с понедельника по пятницу с 9:00 до 18:00,
- уборщица может входить в офис и кабинет директора с понедельника по пятницу с 7:00 до 9:00.

Конфигурирование контроллера

Добавьте в дерево оборудования четыре контроллера BioEntry W2.

1. В контекстном меню объекта *Сервер оборудования* выберите пункт «Поиск и добавление оборудования / Suprema 2». Откроется окно Поиск и добавление оборудования Suprema 2 с найденными контроллерами. При необходимости поменяйте настройки и нажмите **Далее.**
   Выберите один контроллер BioEntry W2 и нажмите кнопку **Добавить**. В дерево оборудования добавится драйвер СКД Suprema 2 с контроллером BioEntry W2.
2. Подключите к добавленному контроллеру еще один контроллер BioEntry W2 в ведомом режиме по линии RS-485.
3. Добавьте ведомый контроллер к существующему в дереве оборудования: выберите пункт контекстного меню контроллера BioEntry W2 «Найти и добавить ведомые устройства». В открывшемся окне выберите ведомый контроллер и нажмите **Добавить**.
4. В объекте *Дверь*, основного контроллера, на вкладке «Основные» укажите ведомый контроллер в качестве одного из считывателей.

По аналогии добавьте вторую пару контроллеров.



Объект *Дверь* с ведущим и ведомым контроллерами в качестве считывателей

Определение зон доступа

Зона доступа — это помещение или несколько помещений, ограниченных считывателями, в которые могут проходить сотрудники.

Предприятие имеет следующие зоны доступа:

- офис — для доступа сотрудников, директора и уборщицы,
- офис + кабинет директора — для доступа директора и уборщицы.

Определение времени работы сотрудников

Далее необходимо определить дни и время, в которые сотрудники могут проходить на предприятие. Такая совокупность дней и времени называется временная зона, далее ВЗ.

На предприятии можно выделить две временные зоны:

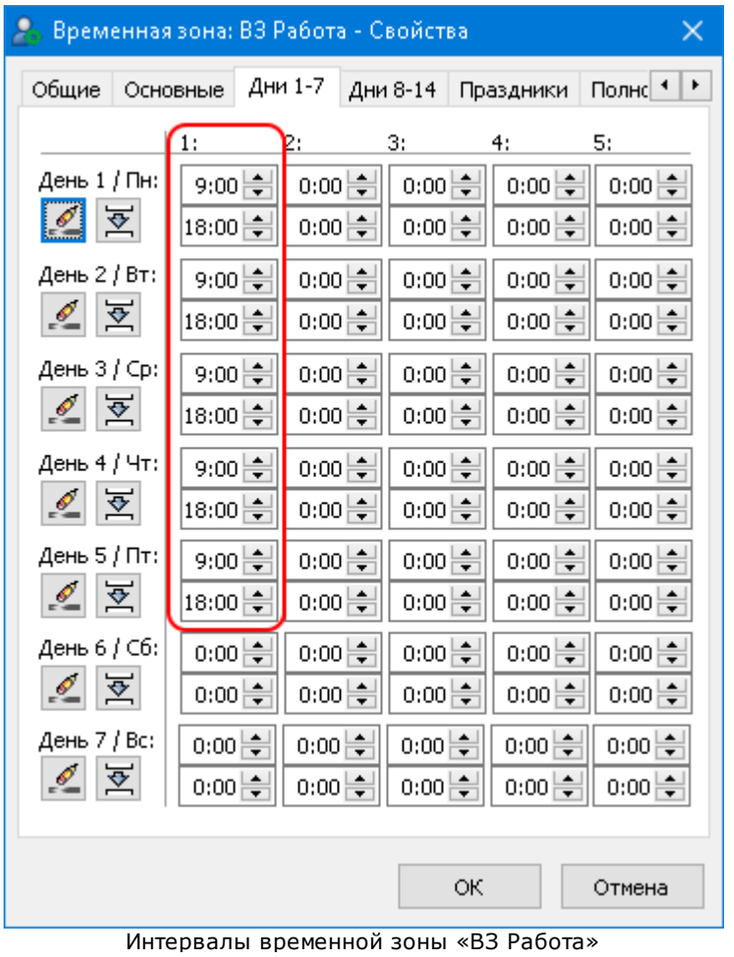
- «ВЗ Работа» — для сотрудников и директора. С временем доступа с 9:00 до 18:00 по будням.
- «ВЗ Уборка» — для уборщицы. С временем с 7:00 до 9:00 по будням.

▾ Создайте Временные зоны:

1. Добавьте к ведущему контроллеру BioEntry W2 объект типа *Временная зона СКД Suprema 2*.
2. На вкладке **«Дни 1–7»** с понедельника по пятницу укажите интервалы с 9:00 до 18:00.
3. На вкладке **«Общие»** задайте имя «ВЗ Работа». Нажмите кнопку **ОК**.
4. Добавьте вторую временную зону.

5. На вкладке **«Дни 1–7»** с понедельника по пятницу укажите интервалы с 7:00 до 9:00.
6. На вкладке **«Общие»** задайте имя «ВЗ Уборка». Нажмите кнопку **ОК**.

По аналогии добавьте временные зоны ко второму ведущему контроллеру.



Интервалы временной зоны «ВЗ Работа»

Создание Уровней доступа

Уровень доступа объединяет в себе считыватели зон доступа и временные зоны, указывающие, когда можно проходить по этим считывателям.

На контроллере, ведущем офис, можно выделить следующие уровни доступа:

- «УД Офис» — для сотрудников офиса и для директора, включает в себя считыватели двери в офис и временную зону «ВЗ Работа»,
- «УД Офис (Уборка)» — для уборщицы, включает в себя считыватели двери в офис и временную зону «ВЗ Уборка».

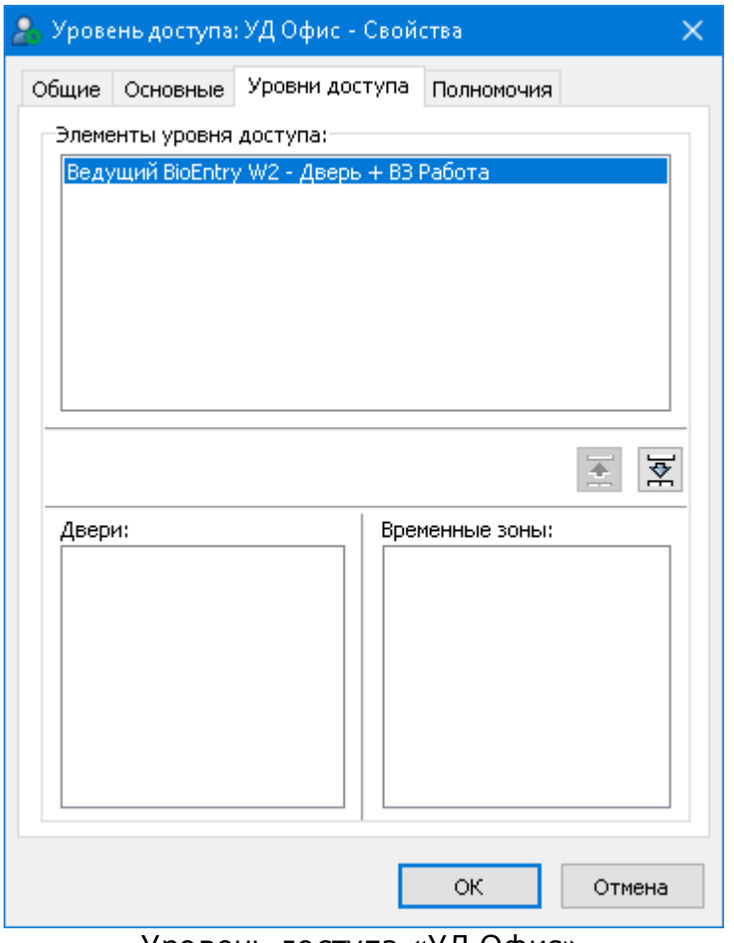
На контроллере, ведущем в кабинет директора, можно выделить следующие уровни доступа:

- «УД Кабинет» — для директора, включает в себя считыватели двери в кабинет и временную зону «ВЗ Работа»,
- «УД Кабинет (Уборка)» — для уборщицы, включает в себя считыватели двери в кабинет и временную зону «ВЗ Уборка».

- Создайте Уровни доступа, и укажите в них считыватели и временные зоны:
  1. Добавьте к ведущему контроллеру BioEntry W2, находящемуся на входе в офис, объект типа *Уровень доступа СКД Suprema 2*.
  2. На вкладке **«Уровни доступа»** выберите созданную дверь и временную зону «ВЗ Работа» и нажмите кнопку **Добавить пару**.
  3. На вкладке **«Общие»** задайте имя «УД Офис» и нажмите **ОК**.

Аналогично создайте:

- на этом же контроллере — «УД Офис (Уборка)», но вместо «ВЗ Работа» укажите временную зону «ВЗ Уборка»,
- на контроллере, ведущем в кабинет директора — «УД Кабинет» с временной зоной «ВЗ Работа» и «УД Кабинет (Уборка)» с временной зоной «ВЗ Уборка».



Уровень доступа «УД Офис»

Создание списков уровней доступа

Все уровни доступа необходимо добавить в одноименные Списки уровней доступа, так как именно списки уровней доступа указываются в дальнейшем в группе доступа.

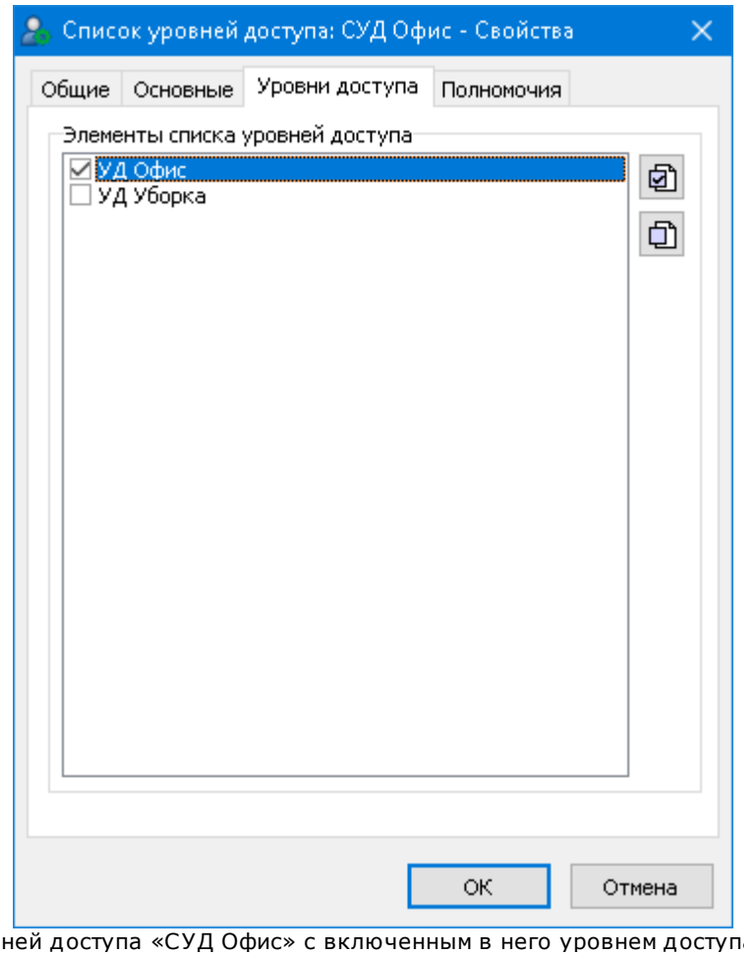
- Создайте Списки уровней доступа, и укажите в них уровни доступа:
  1. Добавьте к ведущему контроллеру, ведущему в офис, объект типа Список уровней доступа СКД Suprema 2. На вкладке

«Уровни доступа» выберите «УД Офис».

2. На вкладке **«Общие»** задайте имя «СУД Офис» и нажмите **ОК**.

Аналогично создайте:

- на этом же контроллере — «СУД Офис (Уборка)», куда включите «УД Офис (Уборка)».
- на контроллере, ведущем в кабинет — «СУД Кабинет», куда включите «УД Кабинет», и «СУД Кабинет (Уборка)», куда включите «УД Кабинет (Уборка)».



Список уровней доступа «СУД Офис» с включенным в него уровнем доступа «УД Офис»

Создание Групп доступа

На предприятии можно выделить три группы доступа:

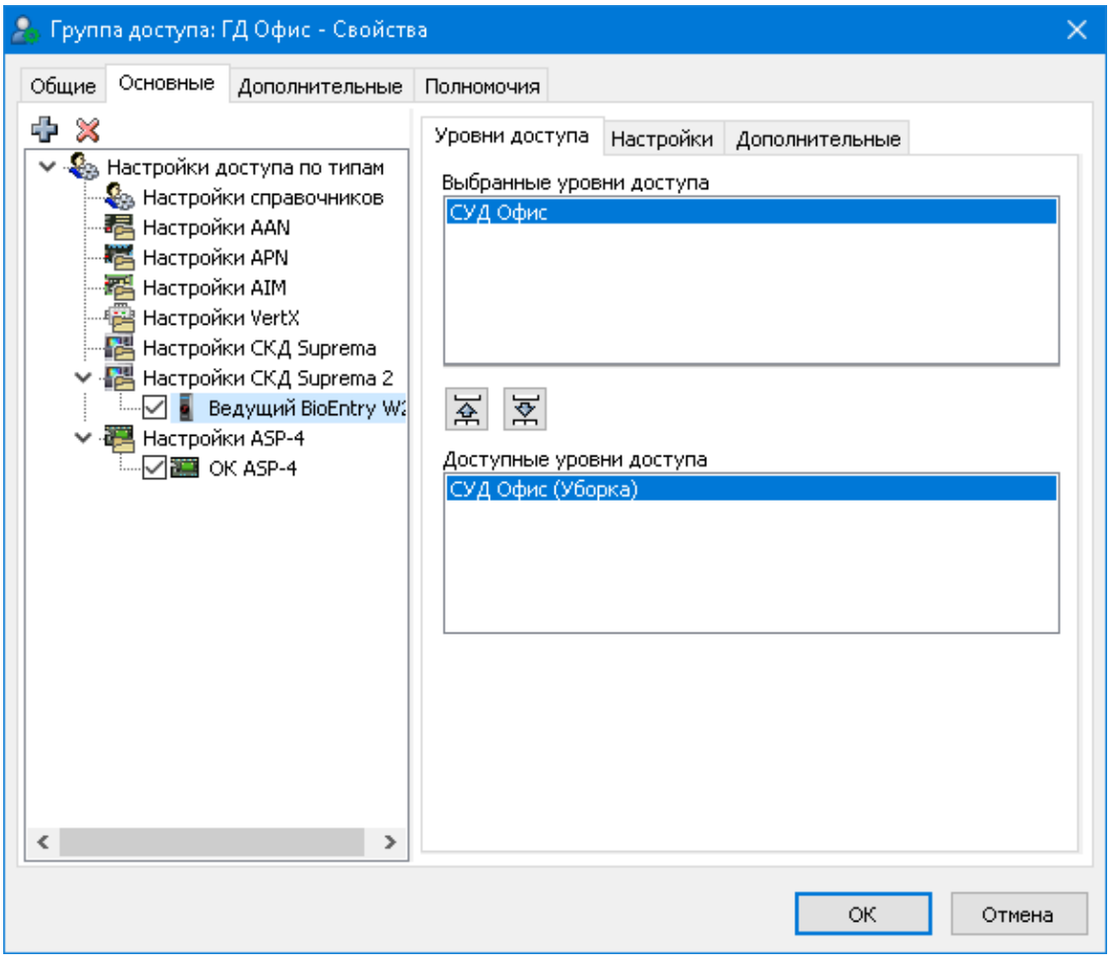
- «ГД Офис» — для сотрудников офиса,
- «ГД Офис + Кабинет» — для директора,
- «ГД Офис + Кабинет (Уборка)» — для уборщицы.

Создайте группы доступа:

1. К объекту типа *Папка* добавьте объект типа *Группа доступа* .
2. На вкладке **«Основные»**, группы доступа, в левой части окна выделите пункт *Настройки СКД Suprema 2* и с помощью кнопки **Добавить контроллер** или пункта контекстного меню включите в ее состав контроллер, ведущий в офис.
3. В правой части окна переместите список уровней доступа «СУД Офис» в **Выбранные уровни доступа**.
4. На вкладке общие задайте имя «ГД Офис» и нажмите **ОК**.

Аналогично создайте две другие группы доступа:

- «ГД Офис + Кабинет», куда включите «СУД Офис» контроллера, ведущего в офис, и «СУД Кабинет» контроллера, ведущего в кабинет,
- «ГД Офис + Кабинет (Уборка)», куда включите «СУД Офис (Уборка)» контроллера, ведущего в офис, и «СУД Кабинет (Уборка)» контроллера, ведущего в кабинет.



Группа доступа «ГД Офис»

Добавление в базу данных владельцев карт и отпечатков

Для работы с базой данных владельцев карт и идентификаторов используется приложение «Картотека». В окне ***Картотека***, на вкладке **«Владельцы карт»**, создайте необходимое количество владельцев карт, и занесите им отпечатки.

Назначение групп доступа

В приложении «Картотека» назначьте сотрудникам группы доступа с помощью группового редактирования или вкладки **«Доступ»**, в окне ***Владелец карты***:

- сотрудникам офиса — «ГД Офис»,
- директору — «ГД Офис + Кабинет»,
- уборщице — «ГД Офис + Кабинет (Уборка)».

Проверка доступа

Проверьте настройки доступа:
- все сотрудники группы доступа «ГД Офис» должны иметь доступ только на считыватели офиса по будням с 9:00 до 18:00,
- директор должен иметь доступ на все считыватели по будням с 9:00 до 18:00,
- уборщица должна иметь доступ на все считыватели по будням с 7:00 до 9:00.

1.2.1 Варианты создания групп доступа

Есть два подхода к созданию групп доступа: одна ГД на сотрудника и несколько ГД на сотрудника.

Рассмотрим варианты создания групп доступа на следующем примере:
- на заводе есть проходная, столовая и шесть цехов,
- все сотрудники пользуются столовой и проходной,
- сотрудники делятся на шесть групп, каждая из которых может проходить только в один из шести цехов.

Одна группа доступа на сотрудника

Для настройки доступа можно создать шесть групп доступа, в каждой из которых будут считыватели столовой, проходной и одного из шести цехов. У каждой из шести групп сотрудников будет по одной группе доступа. Такой вариант конфигурирования доступа называется *одна группа доступа на сотрудника*.

Вариант создания ГД — *одна группа доступа на сотрудника* — подходит для небольшого предприятия с маленьким количеством групп сотрудников и зон доступа.

Несколько групп доступа на сотрудника

Предположим на заводе произошли изменения, после которых половина сотрудников первого цеха получила доступ во второй цех, а половина сотрудников пятого — в шестой. Таким образом на предприятии появились две новых группы сотрудников, у которых права доступа отличаются от уже существующих.

Для двух новых групп сотрудников можно создать еще две группы доступа.

Второй способ — поменять существующие группы доступа следующим образом:

1. вынести проходную и столовую в отдельную группу доступа,
2. для каждого цеха создать отдельные группы.

В этом случае сотрудникам придется назначать несколько групп доступа.

Например, у сотрудников первого цеха будет две группы доступа: «ГД 1-й цех» и «ГД столовая + проходная».

Такой вариант конфигурирования доступа называется *несколько групп доступа на сотрудника*.

Вариант *несколько групп доступа на сотрудника* подходит предприятиям со сложной системой доступа и большим количеством групп сотрудников: он позволяет не создавать лишние группы доступа, а обойтись назначением нескольких групп сотруднику.

Обратите внимание: Группы доступа не рекомендуется редактировать во время работы системы. Произведенные изменения можно выполнить позже, выбрав один из режимов применения изменений.

1.2.2 Назначение групп доступа

Назначение групп доступа

По умолчанию группа доступа назначается сотруднику в окне ***Владелец карты***, на вкладке **«Доступ»**. При этом карты владельца автоматически наследуют все группы доступа владельца.

Группу доступа можно назначить и карте. Такая карта перестает наследовать группы доступа владельца.

Например, сотруднику с двумя картами назначена группа доступа *Офис.* У первой карты нет собственной группы доступа, а у второй карты указана собственная группа доступа — *Склад*. По первой карте сотрудник сможет проходить в офис, так как она наследует права владельца, а по второй — только на склад.

Назначать группу доступа карте рекомендуется в случае, когда у сотрудника должны быть карты с разным доступом. Также собственную группу доступа удобно назначать гостевым картам, когда хранить настройки во владельце неудобно, например, из-за включенного КПВ.

Чтобы появилась возможность назначить группу доступа карте, выберите пункт меню «Настройки / Настройки картотеки» в приложении *Картотека*. В открывшемся окне, в группе параметров **Выбор типа создаваемой карты**, выберите пункт *Карта имеет собственные настройки* — таким образом, вновь создаваемые карты будут иметь собственные настройки доступа.

Если вы хотите перенести настройки доступа от владельца к карте или наоборот, воспользуйтесь процедурой переноса прав доступа от владельца к карте и от карты к владельцу.

1.2.3 Хранение настроек доступа

Дополнительные настройки доступа

У контроллеров существуют дополнительные настройки доступа, такие как дата и время активации/деактивации владельца, настройки КПВ, использование альтернативного времени при проходе, исключение/ разрешение ПИН команд и другие.

Задавать дополнительные настройки доступа, как и назначать группы

доступа, рекомендуется в окне ***Владелец карты***. При этом карты владельца автоматически наследуют все настройки владельца.

Задавать дополнительные настройки в карте рекомендуется, если у владельца должны быть карты с разным доступом. По умолчанию дополнительные настройки доступа можно назначать только владельцу, назначение настроек карте необходимо включить в меню картотеки.

Помимо владельца карты и идентификатора дополнительные настройки доступа могут храниться в других объектах. Хранение настроек в разных объектах позволит добиться более гибкой системы прав доступа, однако это рекомендуется делать только опытным пользователям.

1.3 Ограничение оборудования

Объекты подсистемы Управление доступом являются логическими и их конфигурирование не зависит от установленного оборудования. Но возможности того или иного оборудования накладывают ограничения на использование объектов. Имеют значение следующие ограничения в возможностях оборудования:

- количество карт, которые могут храниться в памяти контроллера,
- количество уровней доступа, которые могут храниться в памяти контроллера,
- количество уровней доступа, которые могут быть назначены одной карте.

Поэтому при конфигурировании объектов подсистемы Управление доступом администратору комплекса необходимо исходить из возможностей установленного оборудования.

При загрузке идентификаторов в контроллер могут возникнуть ситуации, когда контроллер не может обработать всю совокупность настроек идентификатора.

Для проверки правильности настроек идентификаторов перед отгрузкой на контроллер используйте диагностику идентификаторов.

1.4 Диагностика идентификаторов

Подсистема Управление доступом позволяет проверить правильно ли сконфигурированы идентификаторы.

Предусмотрены следующие способы проверки:

- просмотр настроек доступа, которые будут использованы для конкретного идентификатора.
- проверка идентификатора на ошибки / предупреждения. При этом:
  - ошибкой считается фатальная ситуация, которая препятствует загрузке карты в контроллер (например, слишком большой номер карты).
  - предупреждением считаются следующие ситуации:
    - настройки карты заполнены некорректно, но карту возможно загрузить в контроллер. В этом случае будут использовать настройки по умолчанию.
    - контроллер не может обработать всю совокупность настроек идентификатора. В этом случае загружается максимально возможное число первых значений.

Рекомендуется устранить предупреждения до загрузки идентификатора в контроллер.

Диагностика идентификаторов

Для проверки всех идентификаторов в базе на панели приложения «Картотека» нажмите кнопку **Проверить базу идентификаторов**. Если ошибки есть, откроется окно Список идентификаторов с ошибками.

Для проверки одного идентификатора, в окне идентификатора, на вкладке **«Основные»** нажмите кнопку **Проверить идентификатор**, или выберите пункт контекстного меню идентификатора «Проверить идентификатор». Если ошибки есть, откроется окно ***Результаты проверки идентификатора***.

Проверка карты на ошибки проводится в соответствии с типом контроллера, список ошибок / предупреждений зависит от типа контроллера.

Особенности идентификаторов

У идентификаторов есть следующие особенности, которые следует учитывать:

- Идентификатор в один и тот же момент может принадлежать только одному владельцу или же может быть не выданным.
- При удалении из базы данных информации о владельце карты, выданные ему идентификаторы сохраняются в базе, но при этом автоматически деактивируются, не загружаются в контроллер и доступ по ним получить нельзя. Такой идентификатор может быть активирован и использован в дальнейшем.
- В случае, если карта не выдана и по ней совершен проход, в сообщении будет указано, что владелец карты не найден.

1.5 Объекты подсистемы Управление доступом

В разделе перечислены объекты подсистемы Управление доступом.

1.5.1 Группа доступа

 **Группа доступа** — логический объект, представляет собой совокупность прав и привилегий доступа сотрудников на контролируемой территории.

Настройки

Все настройки объекта расположены на вкладках

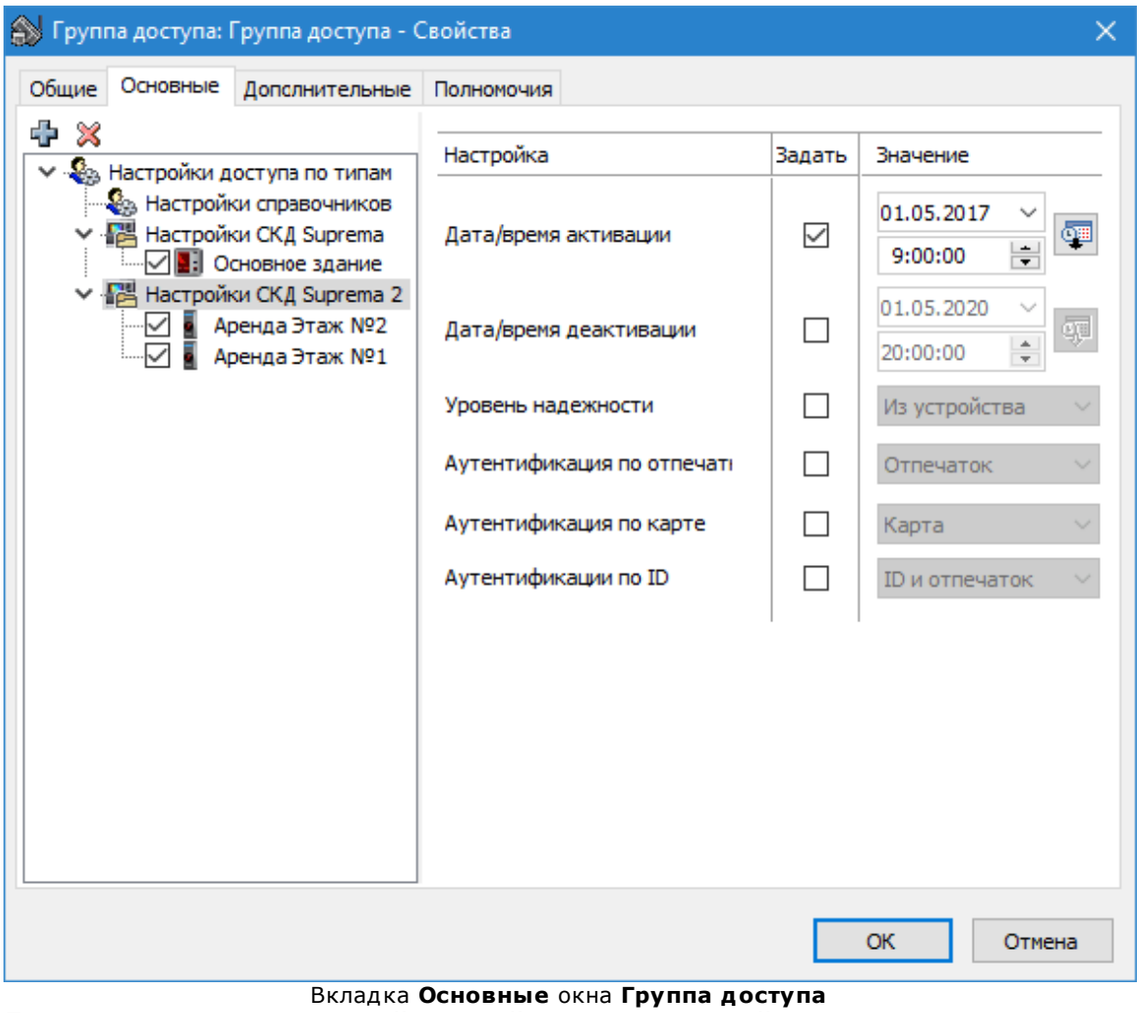
Общие
Основные
Дополнительные
Полномочия

Вкладка **«Основные»** окна редактирования свойств объекта *Группа доступа* поделена на две части:

- слева находится список драйверов установленного оборудования,
- справа — настройки драйверов.

При конфигурировании группы доступа придерживайтесь следующего порядка:

- В левой части окна выделите необходимый Вам драйвер и с помощью кнопки **Добавить контроллер** или пункта контекстного меню включите в ее состав контроллеры, с которыми Вы будете работать в этой группе доступа.
- Так как в рамках группы доступа могут использоваться несколько контроллеров одного драйвера, для которых требуется указать одинаковые настройки (например, дата и время активации идентификатора), эти настройки вынесены на уровень драйвера. Настройки драйвера распространяются на все контроллеры, которые входят в состав драйвера. Также для каждого контроллера можно использовать свои собственные настройки (вкладка **«Настройки»**). Рекомендуется использовать настройки драйверов, так как обычно для всех контроллеров, включенных в состав одной группы доступа, указываются одинаковые настройки.
- Для каждого контроллера укажите локальный уровень доступа, который будет использоваться для данной группы доступа.



Вкладка **Основные** окна **Группа доступа**

Далее рассмотрим настройки драйверов и настройки контроллеров разного типа.

Настройки справочников

Настройки СКД Suprema

Настройки СКД Suprema 2

Для драйвера Настройки справочников используется следующая настройка:

- **Макет карты** — настройка определяет, какой макет будет применен при печати данной карты на принтере. Нажмите кнопку **Выбрать объект** и укажите макет в открывшемся диалоговом окне ***Выбрать объект***.

Драйвер СКД Suprema

Вкладка с настройками драйверов представляет собой таблицу со следующими столбцами:

- **Настройка** — имя настройки.

- **Задать** — при выборе этого флажка данная настройка будет определена явным образом. Если нет этого флажка, это означает, что:
  - настройка будет использоваться по умолчанию,
  - настройка будет указана в идентификаторе,
  - настройка будет указана в другой группе доступа (в том случае, если для идентификатора используется две и более групп доступа).

- **Значение** — в этом столбце укажите, с каким значением настройка будет использоваться в системе.

Для драйвера СКД Suprema в группе доступа используются следующие настройки:

- **Администратор** — флажок позволяет задать расширенные настройки для владельца карты. В этом случае сотрудник сможет свободно перемещаться между зонами и при использовании контроллеров BioStation T2 вход в меню на устройстве будет доступен только этому владельцу.

- **Проброс карты** — при выборе этого флажка владелец карты сможет осуществлять проход только по карте, независимо от настроек контроллера и настроек, заданных в поле **Режим аутентификации**.

- **Дата и время активации** — дата и время начала периода учетной записи владельца (с этого момента отпечатки и карты, принадлежащие владельцу, будут распознаваться на считывателях).

- **Дата и время деактивации** — дата и время окончания периода действия учетной записи владельца карты (с этого момента отпечатки и карты перестанут распознаваться на считывателях).

- **Надежность распознавания** — данная настройка задает вероятность предоставления доступа незарегистрированному пользователю. Например, если задана вероятность 1/1000 (**Самая низкая**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средняя**).

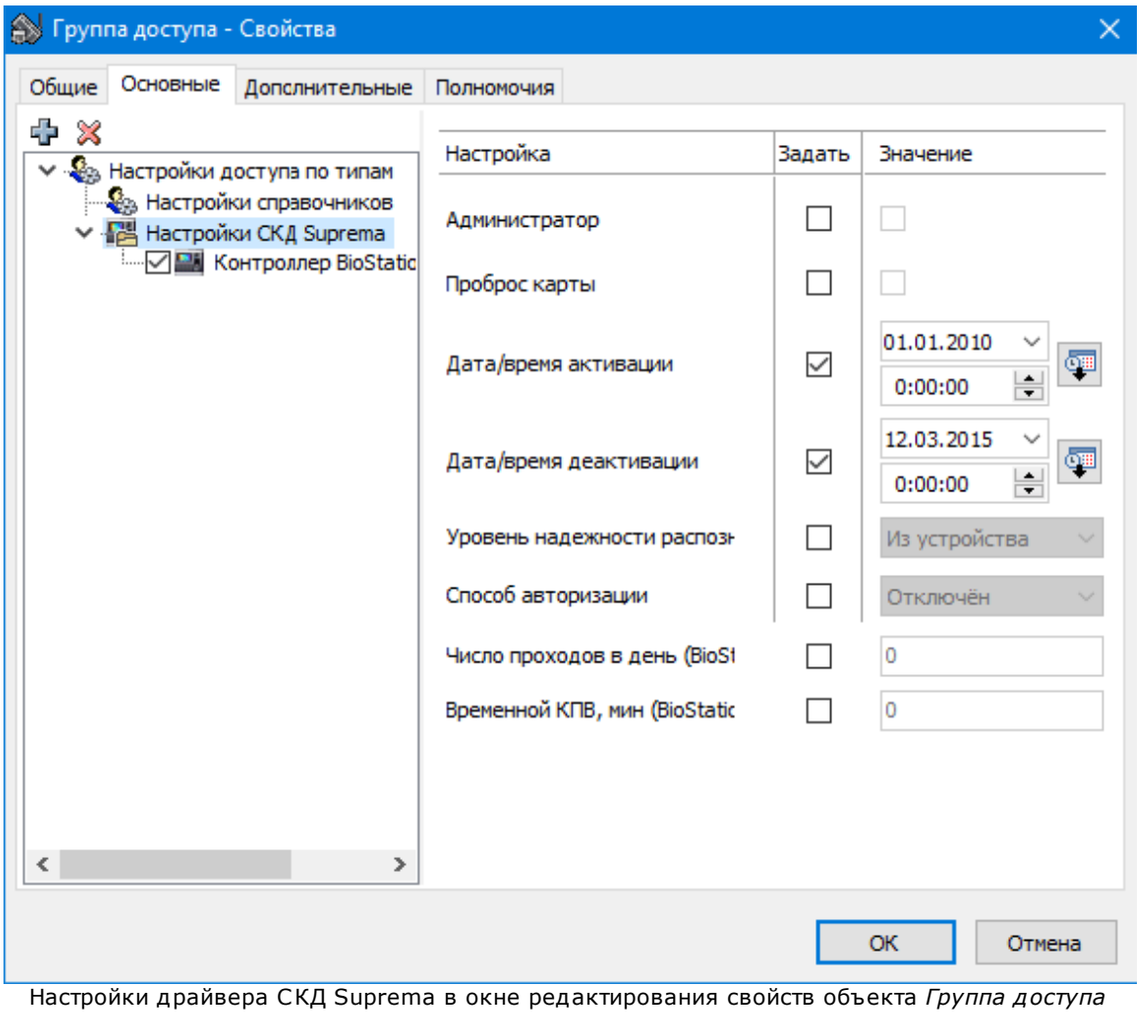
- **Режим аутентификации** — настройка позволяет задать способ

аутентификации в режиме 1:1 для данного владельца карты. Например, для определенного владельца можно настроить проход только по карте, в то время как для других сотрудников будет задан режим **Отпечаток и пароль**. Данная настройка недоступна, если задан режим аутентификации по отпечатку пальца.

Обратите внимание: так как не все контроллеры поддерживают предлагаемые режимы аутентификации, ознакомьтесь с настройками контроллера. В том случае, если необходима аутентификация только по карте, воспользуйтесь настройкой **Проброс карты**.

- **Число проходов в день (BioStation)** — в этом поле укажите число проходов, которые могут быть осуществлены владельцем карты за день. Настройка доступна для контроллеров BioStation.

- **Временной КПВ, мин (BioStation)** — настройка позволяет задать частоту повторных проходов для сотрудника в течение одного рабочего дня. Настройка доступна для контроллеров Biostation.



Настройки драйвера СКД Suprema в окне редактирования свойств объекта *Группа доступа*

Драйвер СКД Suprema 2

Вкладка с настройками драйверов представляет собой таблицу со следующими столбцами:

- **Настройка** — имя настройки.

- **Задать** — при выборе этого флажка данная настройка будет определена явным образом. Если нет этого флажка, это означает, что:
  - настройка будет использоваться по умолчанию,
  - настройка будет указана в идентификаторе,
  - настройка будет указана в другой группе доступа (в том случае, если для идентификатора используется две и более групп доступа).

- **Значение** — в этом столбце укажите, с каким значением настройка будет использоваться в системе.

Для драйвера СКД Suprema 2 в группе доступа используются следующие настройки:

- **Дата/время активации** — дата и время начала периода учетной записи владельца (с этого момента отпечатки и карты, принадлежащие владельцу, будут распознаваться на считывателях).

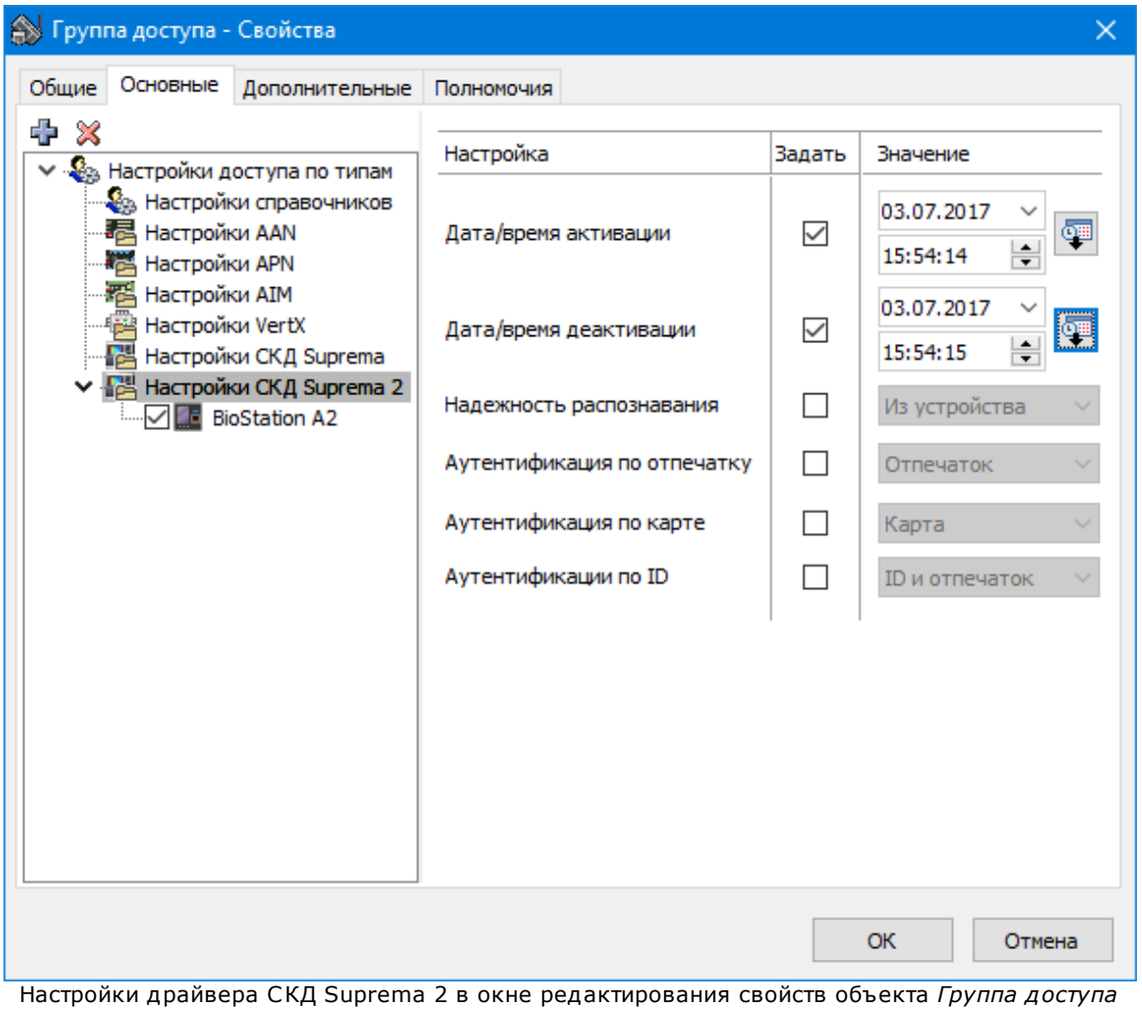
- **Дата/время деактивации** — дата и время окончания периода действия учетной записи владельца карты (с этого момента отпечатки и карты перестанут распознаваться на считывателях).

- **Надежность распознавания** — данная настройка задает вероятность предоставления доступа незарегистрированному пользователю. Например, если задана вероятность 1/1000 (**Самая низкая**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средняя**).

- **Аутентификация по биоданным** — настройка позволяет задать режим для идентификации данного пользователя на устройстве с помощью отпечатка: *Биоданные*, *Биоданные и Пни*, *Запрещен*, *Из устройства*.

- **Аутентификация по карте** — настройка позволяет задать режим для верификации данного пользователя на устройстве с помощью карты: *Карта*, *Карта и отпечаток/лицо*, *Карта и ПИН*, *Карта и отпечаток/лицо или ПИН*, *Карта, отпечаток/лицо и ПИН, Запрещен, Из устройства.*

- **Аутентификация по ID** — настройка позволяет задать режим для верификации данного пользователя на устройстве с помощью ID: *ID и отпечаток/лицо*, *ID и ПИН*, *ID и отпечаток/лицо или ПИН*, *ID и отпечаток/лицо и ПИН, Запрещен, Из устройства.*



Настройки драйвера СКД Suprema 2 в окне редактирования свойств объекта *Группа доступа*

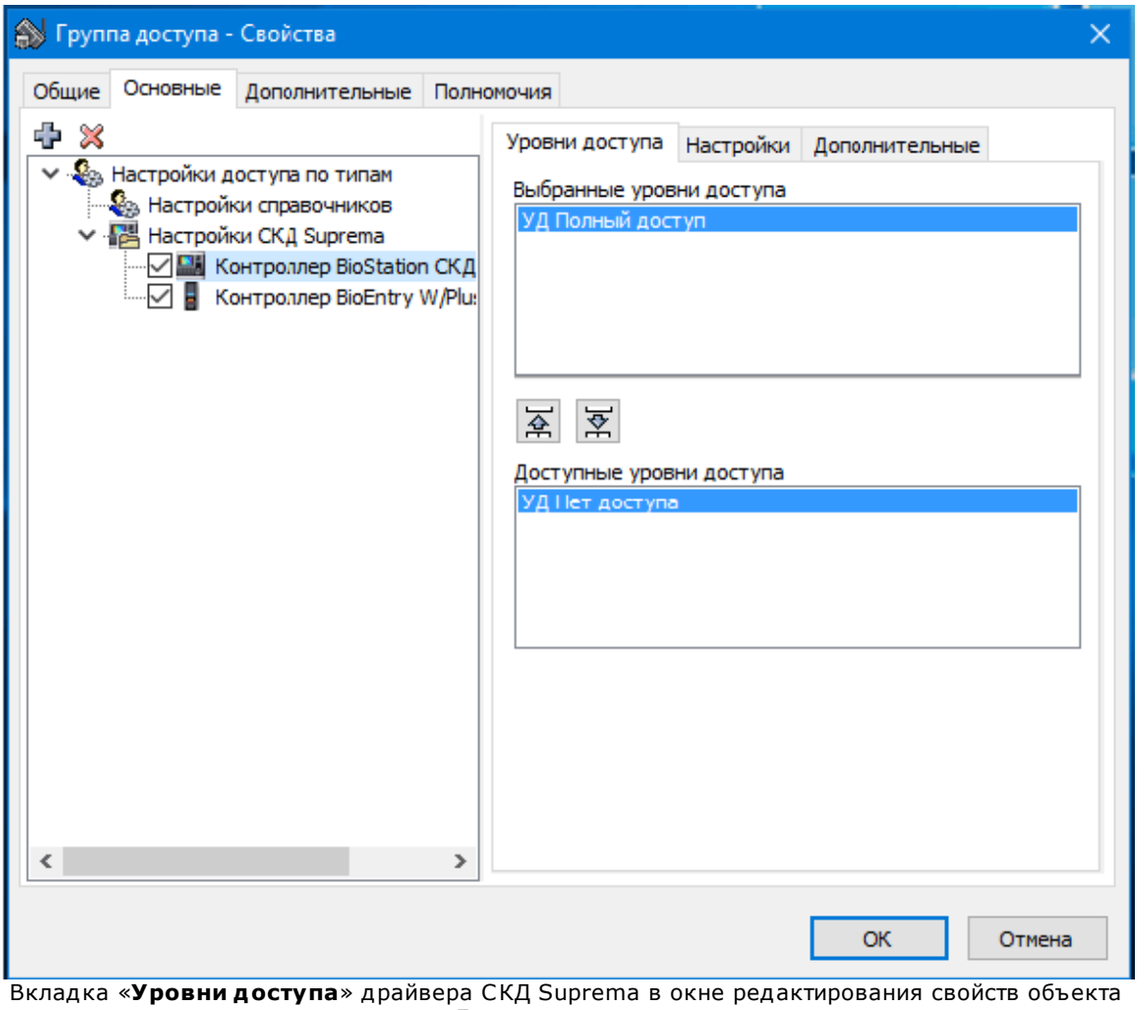
Обратите внимание: так как не все контроллеры поддерживают предлагаемые режимы аутентификации, ознакомьтесь с настройками контроллера.

Обратите внимание: с помощью данных настроек можно переопределить настройки доступа в том случае, если на контроллере разрешен режим индивидуальной аутентификации.

Контроллеры СКД Suprema

В случае работы с контроллерами СКД Suprema для группы доступа используются настройки, расположенные на вкладках «**Уровни доступа**», «**Настройки**» и «**Дополнительные**». Закладки «**Настройки**» и «**Дополнительные**» рекомендуется использовать в том случае, если необходимо задать для контроллера собственные настройки, которые отличаются от настроек, заданных для всего драйвера в целом.

На закладке «**Уровни доступа**» укажите локальные уровни доступа, которые будут использоваться в рамках данной группы доступа. Для этого выберите уровень доступа в поле **Доступные уровни доступа** и перенесите его в поле **Выбранные уровни доступа** кнопкой **Добавить**.

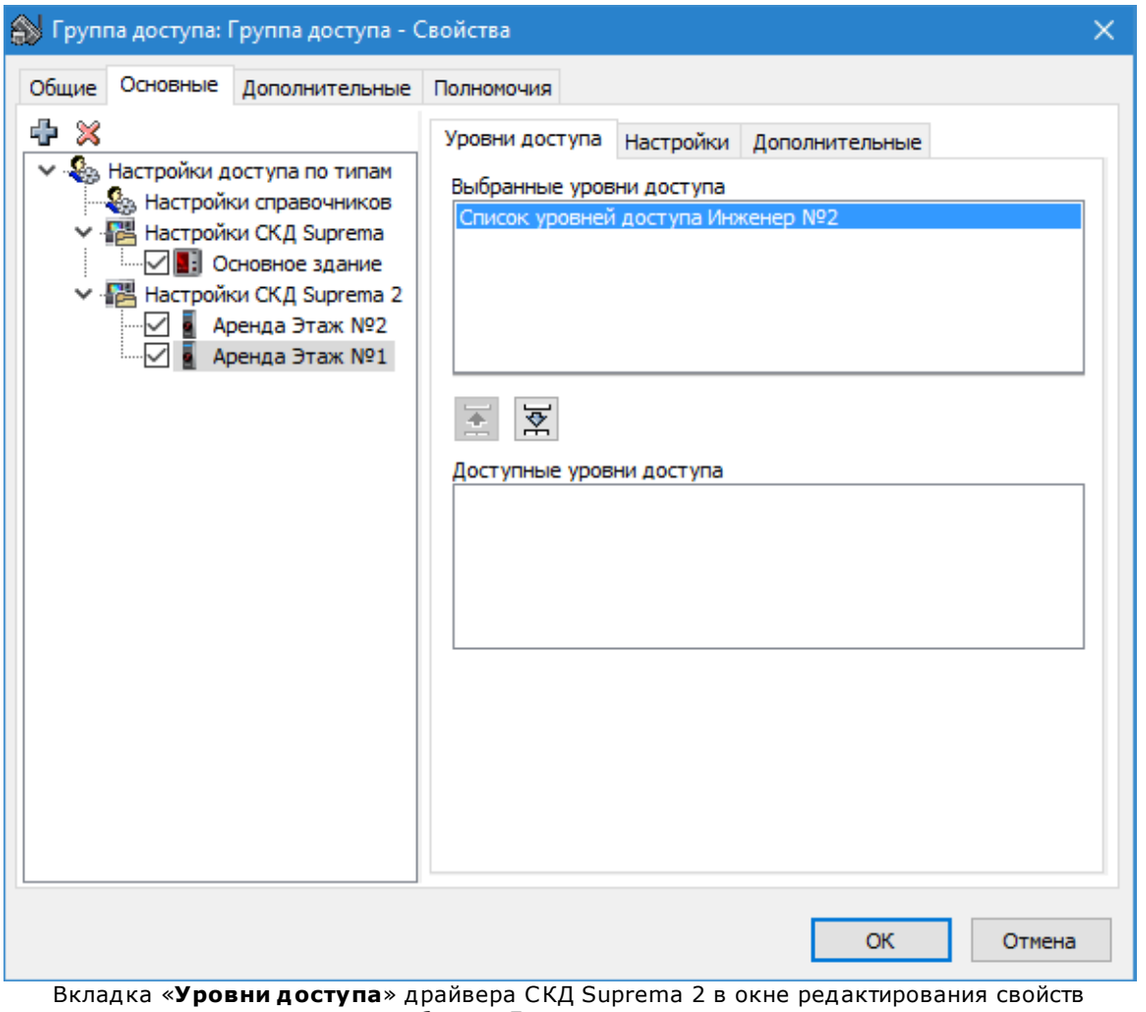


Вкладка «**Уровни доступа**» драйвера СКД Suprema в окне редактирования свойств объекта *Группа доступа*

Контроллеры СКД Suprema 2

В случае работы с контроллерами СКД Suprema 2 для группы доступа используются настройки, расположенные на вкладках «**Уровни доступа**», «**Настройки**» и «**Дополнительные**». Закладки «**Настройки**» и «**Дополнительные**» рекомендуется использовать в том случае, если необходимо задать для контроллера собственные настройки, которые отличаются от настроек, заданных для всего драйвера в целом.

На закладке «**Уровни доступа**» укажите списки локальных уровней доступа, которые будут использоваться в рамках данной группы доступа. Для этого выберите список уровеней доступа в поле **Доступные уровни доступа** и перенесите его в поле **Выбранные уровни доступа** кнопкой **Добавить**.



Вкладка «**Уровни доступа**» драйвера СКД Suprema 2 в окне редактирования свойств объекта *Группа доступа*

Команды управления	Описание
Показать число идентификаторов	При выполнении команды открывается окно с информацией о количестве идентификаторов, за которыми закреплена эта группа доступа.

1.5.2 Расширенные настройки карт

Расширенные настройки карт — логический объект, позволяющий указать, каким образом должны идентифицироваться карты на считывателях VertX, <%SKD%>Suprema 2 и ASP-4. В одном объекте типа *Расширенные настройки карт* (далее РНК) можно указать по одному шаблону карты VertX / Формату карт для каждого контроллера.

РНК необходимо указывать для каждой карты оборудования VertX.
Применение РНК в контроллерах ASP-4.
Применение РНК в контроллерах <%SKD%>Suprema 2.

Настройки
Все настройки объекта расположены на вкладках
Общие
VertX
Suprema 2 и ASP-4
Дополнительные

Полномочия

Команды
Объект не поддерживает команд управления и клиентских команд.

1.5.3 Идентификатор

 **Идентификатор** — логический объект системы, который ассоциируется с физическим объектом на руках сотрудника — картой, брелоком, ключом и т.д.

Настройки
Все настройки объекта расположены на вкладках
Основные
Эксперт
Общие
Полномочия

На вкладке **«Эксперт»** можно выполнить следующее:

- кнопка **Дополнительные настройки** — с помощью этой кнопки открывается диалоговое окно ***Дополнительные настройки идентификатора***.

В этом диалоговом окне можно установить дополнительные настройки идентификатора (рекомендуется опытным пользователям):

- **Код выдачи** — номер версии одной и той же карты. Используется только для карт магнитного формата в том случае, когда печатается и кодируется карта с прежней информацией (настройка используется только для оборудования Apollo).

- **Расширенные настройки карт** — укажите объект типа *Расширенные настройки карт*, в котором указано, каким образом данная карта должна идентифицироваться на считывателях VertX (настройка используется для оборудования VertX).

- кнопка **Собственная группа доступа** — с помощью этой кнопки открывается диалоговое окно ***Собственная группа доступа***, где можно изменить настройки групп доступа, закрепленные за идентификатором (рекомендуется опытным пользователям).

- кнопка **Очистить** — кнопка позволяет очистить собственные настройки доступа для данного идентификатора. После этого для идентификатора будут использоваться настройки тех групп доступа, которые указаны в поле **Список групп доступа** на вкладке **«Основные»**.

- кнопка **Загрузить** — кнопка позволяет загрузить в объект настройки, сохраненные ранее в файле формата *.xml.

- кнопка **Сохранить** — кнопка позволяет сохранить настройки объекта в файл формата *.xml.

Если для карты заданы собственные права доступа, то в зависимости от выбранного стиля оформления приложения «Картотека» и установленного оборудования вкладка **«Основные»** может выглядеть следующим образом:

максимальный стиль
минимальный стиль

Если права доступа заданы у владельца карты, то вкладка **«Основные»** будет выглядеть следующим образом:

- **Общие поля**
  - **Активность** — настройка определяет, используется ли идентификатор в системе. Если флажок снят, идентификатор не будет восприниматься считывателем (при этом будет поступать сообщение *Доступ запрещен, карта неизвестна контроллеру*).

Обратите внимание: если снять флажок **Активность** на вкладке **«Доступ»** объекта *Владелец карты*, доступ по карте будет запрещен.

  - **Свои права** — информационный флажок, который отображает тип хранения настроек доступа. Если флажок активен, карта имеет собственные настройки. В противном случае права доступа заданы у владельца карты.

  - кнопка **Проверить идентификатор** — нажмите на эту кнопку, чтобы проверить сконфигурированный идентификатор до его загрузки в контроллеры. Если в процессе проверки идентификатора будут найдены ошибки, откроется диалоговое окно ***Результаты проверки идентификатора***. Если ошибок нет, сообщение об этом появится в диалоговом окне ***Информация***.

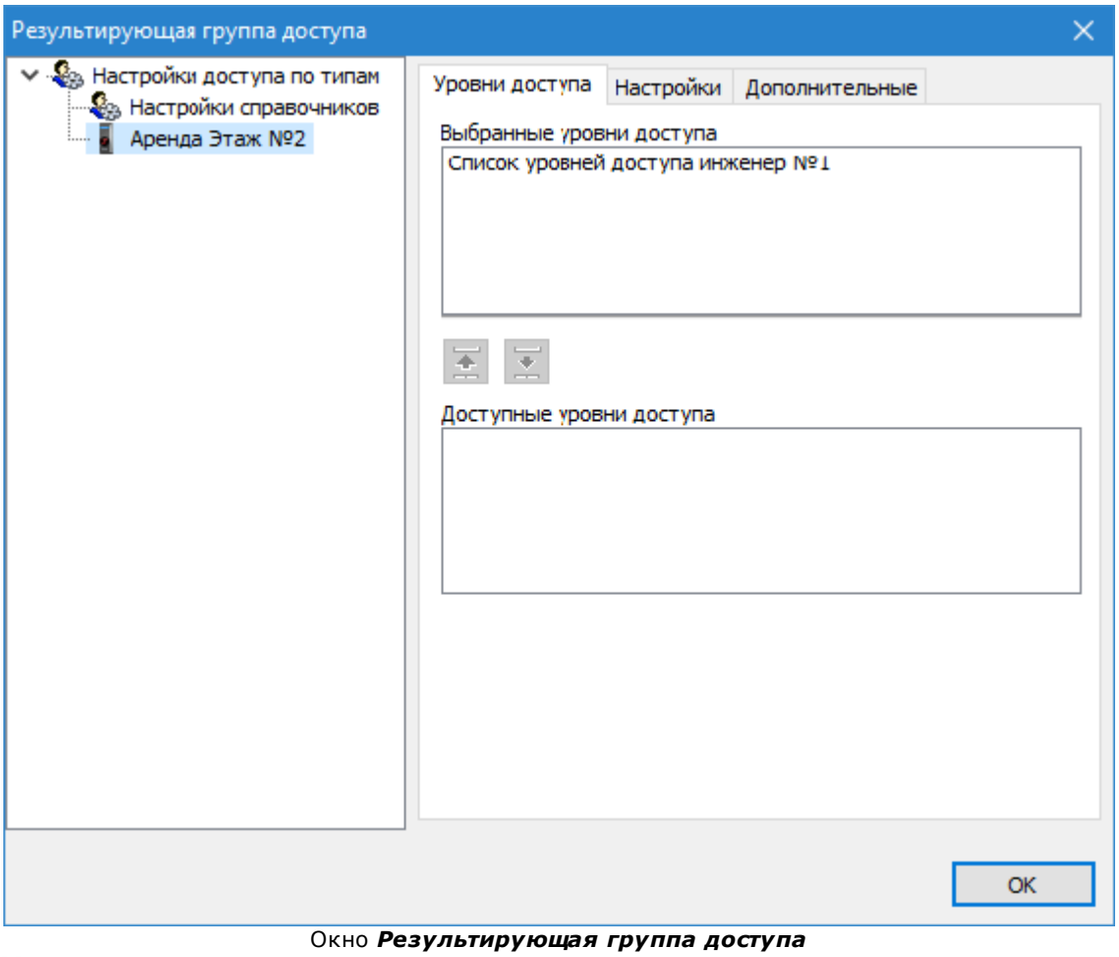
  - кнопка **Показать объединенную группу доступа** — нажмите на эту кнопку, чтобы посмотреть всю совокупность настроек, которые будут использованы для конкретного идентификатора. Откроется диалоговое окно ***Результирующая группа доступа***.

В этом диалоговом окне можно посмотреть всю совокупность настроек доступа, которые будут использованы для конкретного идентификатора.

Окно разделено на две части:

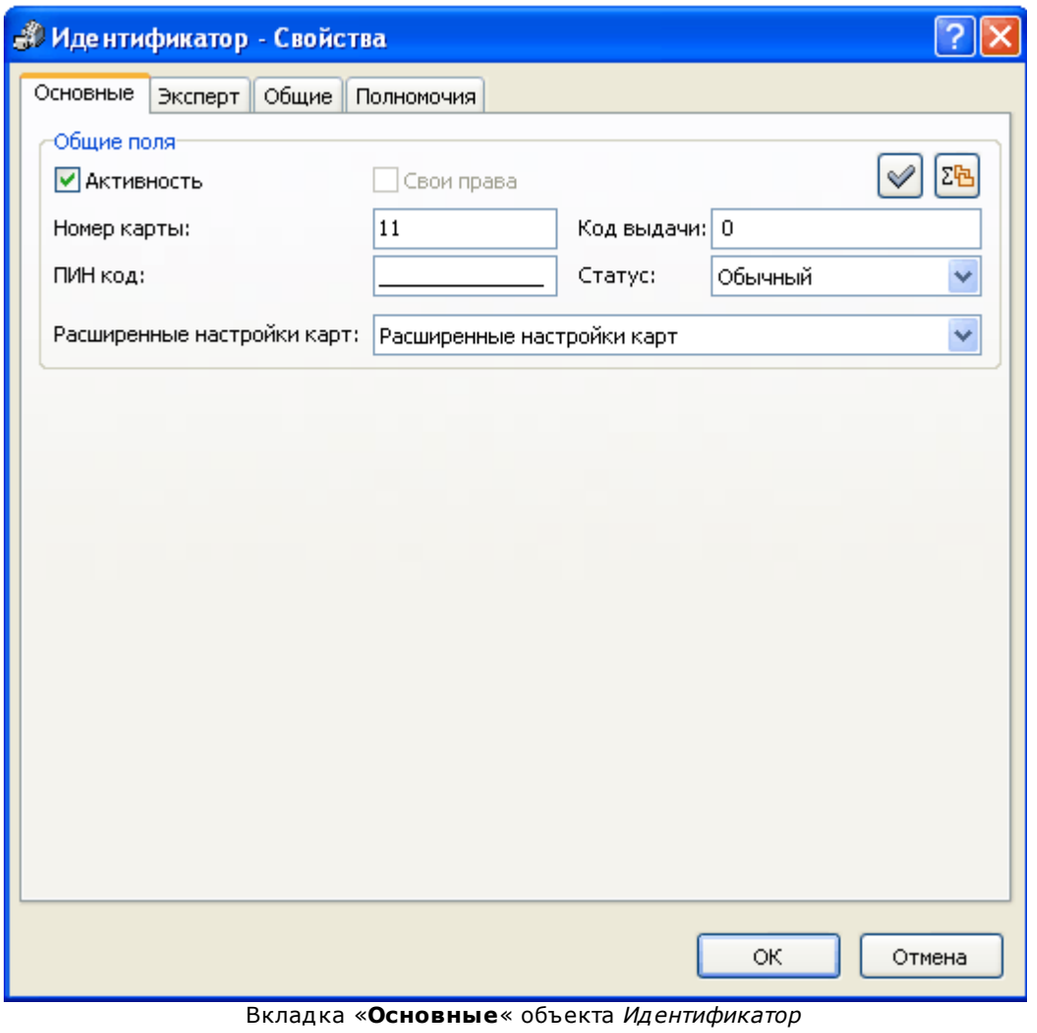
- слева — находится список контроллеров, которые указаны в настройках групп доступа этого идентификатора.
- справа — настройки этого идентификатора для каждого контроллера.

Настройки предназначены только для просмотра и не доступны для редактирования.



Окно ***Результирующая группа доступа***

- **Номер карты** — номер данного идентификатора.
  В том случае, если к компьютеру подключен внешний считыватель карт PR–A08 фирмы Parsec и в данном приложении «Картотека» используется модуль ***USB считыватель карт Parsec***, номер карты можно вводить автоматически.
  В случае добавления группы идентификаторов в этом поле находится диапазон добавляемых номеров.



Вкладка «**Основные**« объекта *Идентификатор*

- **ПИН–код** — укажите персональный идентификационный номер, который владелец данного идентификатора будет вводить на клавиатуре считывателя в режиме *Карта и ПИН* или *Карта или ПИН*.
- **Код выдачи** — номер версии одной и той же карты. Используется только для карт магнитного формата в том случае, когда печатается и кодируется карта с прежней информацией.
- **Статус** — укажите текущий статус идентификатора: обычный, утерян, уничтожен или изъят.
- **Расширенные настройки карт** — укажите объект типа *Расширенные настройки карт*, в котором указано, каким образом данная карта должна идентифицироваться на считывателях Suprema 2.

Обратите внимание: APACS Bio может работать с картами CSN длиной максимум 4 байта, это 32 бита. Карты длиной более 4 байт следует настроить, как 4-х байтные.

Команды

Объект не поддерживает команд управления и клиентских команд.

1.5.4 Владелец карты

Владелец карты — объект системы, содержащий информацию о сотруднике.

Настройки

Все настройки объекта расположены на следующих вкладках

Основные
Дополнительные
Дополнительные поля 1 - 10
Дополнительные поля 11 - 20
Доступ
Suprema СКД
ASP-4
Эксперт
Выдачи
Биоданные
Работы
Полномочия
Общие

Вкладка «**Доступ**» имеет различный вид в зависимости от используемого оборудования и стиля оформления приложения «Картотека»:

Оборудование Apollo: максимальный и минимальный стиль,

Так выглядит вкладка **«Доступ»** объекта *Владелец карты* при использовании максимального стиля оформления «Картотеки» и оборудования:

- Apollo AAN-100/32,
- Apollo AAN-100/32, Apollo AIM-4SL/2SL/1SL и APN-35,
- Apollo AAN-100/32 и Suprema,
- Apollo и Suprema.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, карты не будут восприниматься считывателем (при этом будет поступать сообщение *Доступ запрещен, карта неизвестна контроллеру*). Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу.

  Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

- При нажатии на кнопку **Точный доступ** откроется окно ***Точный доступ и список исключений***, предназначенное для расширения или

ограничения прав доступа в определенные помещения для выбранного сотрудника. Данная настройка доступна при использовании оборудования Apollo.

- **Даты/времена активации/деактивации** — группа настроек позволяет указать срок действия учетной записи данного владельца.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца будут использоваться те настройки активации/деактивации, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
  - **Дата и время активации** — дата и время начала периода действия учетной записи владельца (с этого момента все карты, принадлежащие владельцу, будут распознаваться на считывателях).

  - **Дата и время деактивации** — дата и время окончания периода действия учетной записи владельца карты (с этого момента карты перестанут распознаваться на считывателях).

Обратите внимание: если на контроллерах Apollo AAN-100/32 хранится дата деактивации без времени, то эта дата будет последним днем активности учетной записи владельца. **Например**, если дата деактивации указана 09.05, а время деактивации не указано, то учетная запись владельца будет активна 09.05 и деактивируется только 10.05 в 00:00.

  - кнопка **Установить текущую дату** — позволяет указать текущую дату.

  - кнопка **Установить текущее время** — позволяет указать текущее время.

- **экспертные** - настройка зарезервирована для использования в будущем.

- **Дополнительные настройки** — группа дополнительных настроек для владельца карты.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца будут использоваться те настройки, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
  - **Не контролировать КПВ** — поставьте этот флажок, чтобы исключить информацию о принадлежащих владельцу картах из системы КПВ.

  - **Альтернативное время** — поставьте этот флажок, чтобы для данного владельца использовалось увеличенное время открытия и закрытия двери при проходе.

  - **Запрос ПО перед отказом** — если стоит этот флажок, на компьютер дежурного оператора дополнительно будет поступать запрос о допуске сотрудника, несмотря на то, что контроллером уже принято решение о запрете.

- **Запрос ПО перед разрешением** — если стоит этот флажок, на компьютер дежурного оператора дополнительно будет поступать запрос о допуске сотрудника, несмотря на то, что контроллером уже принято решение о допуске.

- **экспертные** - настройка зарезервирована для использования в будущем.

Так выглядит вкладка «Доступ» объекта *Владелец карты* при использовании минимального стиля оформления картотеки и оборудования:

- Apollo AAN-100/32,
- Apollo AAN-100/32, AIM-4SL/2SL/1SL и APN-35,
- Apollo AAN-100/32,
- Apollo и Suprema.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, то при предъявлении карты поступит сообщение *Доступ запрещен, карта неизвестна контроллеру*. Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу.

Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

Малые контроллеры Apollo: максимальный и минимальный стиль,

Так выглядит вкладка **«Доступ»** объекта *Владелец карты* максимального стиля оформления «Картотеки» и оборудования:

- Apollo AIM-4SL/2SL/1SL и APN-35,
- Apollo AIM-4SL/2SL/1SL и APN-35 и Suprema.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, карты не будут восприниматься считывателем (при этом будет поступать сообщение *Доступ запрещен, карта неизвестна контроллеру*). Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу.

Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок

следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

- **Дополнительные настройки** — группа дополнительных настроек для владельца карты.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца будут использоваться те настройки, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
  - **Альтернативное время** — поставьте этот флажок, чтобы для данного владельца использовалось увеличенное время открытия и закрытия двери при проходе.

  - **Не контролировать КПВ** — поставьте этот флажок, чтобы исключить информацию о принадлежащих владельцу картах из системы КПВ.

- **экспертные** - настройка зарезервирована для использования в будущем.

Так выглядит вкладка «Доступ» объекта Владелец карты при использовании минимального стиля оформления «Картотеки» и оборудования:
- Apollo AIM-4SL/2SL/1SL и APN-35,
- Apollo AIM-4SL/2SL/1SL и Suprema.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, то при предъявлении карты поступит сообщение *Доступ запрещен, карта неизвестна контроллеру*. Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу. Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

Оборудование VertX: максимальный и минимальный стиль,

Так выглядит вкладка **«Доступ»** объекта *Владелец карты* при максимального стиля оформления «Картотеки» и оборудования:
- VertX,
- VertX и Apollo AIM-4SL/2SL/1SL,
- VertX, Apollo AIM-4SL/2SL/1SL и APN-35 и Suprema.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/

выключения доступа по всем картам с наследуемым доступом. Если флажок снят, карты не будут восприниматься считывателем (при этом будет поступать сообщение *Доступ запрещен, карта неизвестна контроллеру*). Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу.

Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

- **Даты/времена активации/деактивации** — группа настроек позволяет указать срок действия учетной записи данного владельца.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца будут использоваться те настройки активации/деактивации, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:

  - **Дата и время активации** — дата и время начала периода действия учетной записи владельца (с этого момента все карты, принадлежащие владельцу, будут распознаваться на считывателях).

  - **Дата и время деактивации** — дата и время окончания периода действия учетной записи владельца карты (с этого момента карты перестанут распознаваться на считывателях).

  - кнопка **Установить текущую дату** — позволяет указать текущую дату.

  - кнопка **Установить текущее время** — позволяет указать текущее время.

- **экспертные** - настройка зарезервирована для использования в будущем.

- **Дополнительные настройки** — группа дополнительных настроек для владельца карты.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного идентификатора будут использоваться те настройки, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
  - **Альтернативное время** — поставьте этот флажок, чтобы для данного владельца использовалось увеличенное время открытия и закрытия двери при проходе.

- **Не контролировать КПВ** — поставьте этот флажок, чтобы исключить информацию о принадлежащих владельцу картах из системы КПВ.

- **Исключить ПИН** — если стоит этот флажок, данному владельцу не требуется вводить ПИН–код в режиме считывателя *Карта и ПИН*. Настройка используется только для контроллеров VertX.

- **Разрешать ПИН команды** — если стоит этот флажок, владелец может управлять реле защелки с помощью команд, набранных на клавиатуре считывателя.

- **экспертные** - настройка зарезервирована для использования в будущем.

Так выглядит вкладка **«Доступ»** объекта *Владелец карты* при использовании минимального стиля оформления «Картотеки» и оборудования:
- VertX,
- Apollo и VertX.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, то при предъявлении карты поступит сообщение *Доступ запрещен, карта неизвестна контроллеру*. Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу. Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

Полный набор оборудования: максимальный и минимальный стиль.

Так выглядит вкладка **«Доступ»** объекта *Владелец карты* максимального стиля оформления «Картотеки» и оборудования:
- Apollo AAN-100/32 и VertX,
- Apollo и VertX,
- Suprema, Apollo AAN-100/32 и VertX.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, то при предъявлении карты поступит сообщение *Доступ запрещен, карта неизвестна контроллеру*. Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу. Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет.

Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

- При нажатии на кнопку **Точный доступ** откроется окно ***Точный доступ и список исключений***, предназначенное для расширения или ограничения прав доступа в определенные помещения для выбранного сотрудника. Данная настройка доступна при использовании оборудования Apollo.

- **Даты / времена активации/деактивации** — группа настроек позволяет указать срок действия учетной записи данного владельца.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца будут использоваться те настройки активации / деактивации, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
  - **Дата и время активации** — дата и время начала периода учетной записи владельца (с этого момента все карты, принадлежащие владельцу, будут распознаваться на считывателях).

  - **Дата и время деактивации** — дата и время окончания периода действия учетной записи владельца карты (с этого момента карты перестанут распознаваться на считывателях).

  - кнопка **Установить текущую дату** — позволяет указать текущую дату.

  - кнопка **Установить текущее время** — позволяет указать текущее время.

- **Экспертные -** настройка зарезервирована для дальнейшего использования.

- **Дополнительные настройки** — группа дополнительных настроек для владельца карты.
  - Если выбран пункт из групп доступа, поля заблокированы и для данного владельца будут использоваться те настройки, которые указаны в закрепленных за ним группах доступа.

  - Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
    - **Не контролировать КПВ** — поставьте этот флажок, чтобы исключить информацию о принадлежащих владельцу картах из системы КПВ.

    - **Альтернативное время** — поставьте этот флажок, чтобы для данного владельца использовалось увеличенное время открытия и закрытия двери при проходе.

    - **Запрос ПО перед разрешением** — если стоит этот флажок, на компьютер дежурного оператора дополнительно будет поступать запрос о допуске сотрудника, несмотря на то, что контроллером уже принято решение о допуске.

    - **Запрос ПО перед отказом** — если стоит этот флажок, на компьютер

дежурного оператора дополнительно будет поступать запрос о допуске сотрудника, несмотря на то, что контроллером уже принято решение о запрете.

- **Исключить ПИН** — если стоит этот флажок, данному владельцу не требуется вводить ПИН–код в режиме считывателя *Карта и ПИН.* Настройка используется только для контроллеров VertX.

- **Разрешать ПИН команды** — если стоит этот флажок, владелец может управлять реле защелки с помощью команд, набранных на клавиатуре считывателя.

Обратите внимание: дополнительные настройки недоступны для оборудования Suprema.

- **Экспертные -** настройка зарезервирована для дальнейшего использования.

Так выглядит вкладка «Доступ» объекта Владелец карты при использовании минимального стиля оформления «Картотеки» и оборудования:

- Apollo AAN-100/32,
- Apollo и VertX,
- Suprema, Apollo AAN-100/32 и VertX.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, то при предъявлении карты поступит сообщение *Доступ запрещен, карта неизвестна контроллеру*. Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу. Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

Для оборудования Suprema СКД вид вкладки **«Доступ»** не зависит от стиля оформления приложения «Картотека».

Так выглядит вкладка «Доступ» объекта Владелец карты при использовании оборудования:

- Suprema СКД.

- **Общие поля**
- **Активность** — настройка дает возможность оперативного включения/выключения доступа по всем картам с наследуемым доступом. Если флажок снят, то при предъявлении карты поступит сообщение *Доступ запрещен, карта неизвестна контроллеру*. Для карт с собственными настройками доступ будет разрешен даже тогда, когда флажок **Активность** не установлен.

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу.

Если за одним владельцем закреплено несколько групп доступа с разными настройками, использование настроек определяется по приоритету. Группа доступа, которая располагается в этом поле первой, имеет максимально высокий приоритет. Чтобы изменить порядок следования групп доступа, выделите объект в поле **Список групп доступа** и воспользуйтесь кнопками **Переместить вверх** и **Переместить вниз**.

- **Даты / времена активации/деактивации** — группа настроек позволяет указать срок действия учетной записи данного владельца.
- Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца будут использоваться те настройки активации / деактивации, которые указаны в закрепленных за ним группах доступа.

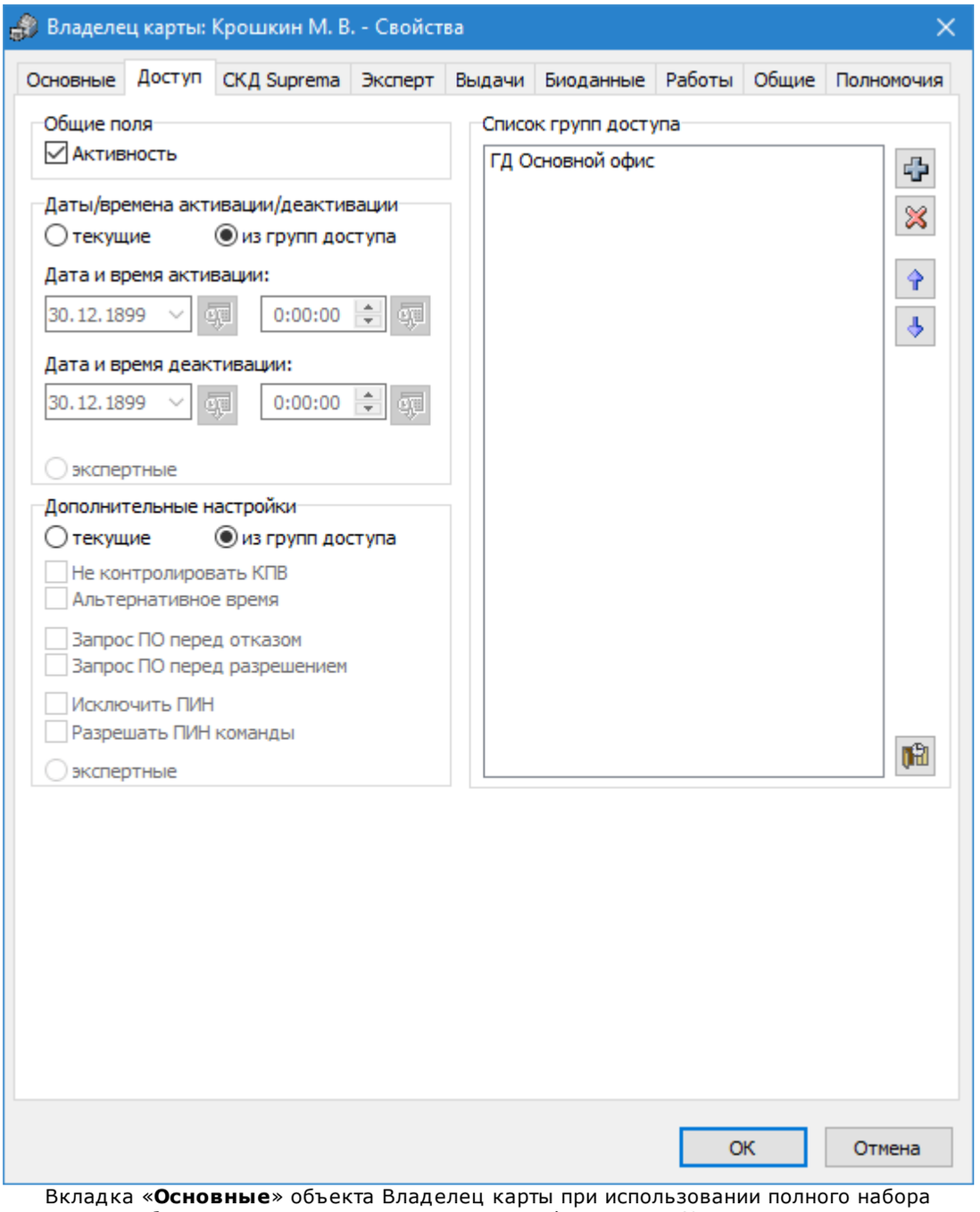
- Чтобы использовать для владельца карты собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
  - **Дата и время активации** — дата и время начала периода учетной записи владельца (с этого момента все карты, принадлежащие владельцу, будут распознаваться на считывателях).

  - **Дата и время деактивации** — дата и время окончания периода действия учетной записи владельца карты (с этого момента карты перестанут распознаваться на считывателях).

  - кнопка **Установить текущую дату** — позволяет указать текущую дату.

  - кнопка **Установить текущее время** — позволяет указать текущее время.

  - **экспертные -** настройка зарезервирована для дальнейшего использования.



Вкладка «**Основные**» объекта Владелец карты при использовании полного набора оборудования и максимального стиля оформления «Картотеки»

На вкладке «**СКД Suprema**» укажите следующие настройки:

- **PIN** — введите PIN-код от 4 до 16 цифр. Данный режим аутентификации доступен для устройств с клавиатурой, для которых выбран соответствующий режим в настройках контроллера.

- В группе параметров **СКД Suprema** укажите следующие настройки:
  - При выборе пункта **Из групп доступа** поля заблокированы, и для данного владельца будут использоваться те настройки, которые указаны в закрепленных за ним группах доступа.

  - **Текущие** — при выборе этого пункта для каждого из владельцев карты можно переопределить ряд настроек, задающихся на вкладке «**Биометрия**»:

- **Администратор** — флажок позволяет задать расширенные настройки для владельца карты. В этом случае сотрудник сможет свободно перемещаться между зонами и при использовании контроллеров BioStation T2 вход в меню на устройстве будет доступен только этому владельцу.

- **Проброс карты** — при выборе этого флажка владелец карты сможет осуществлять проход только по карте, независимо от настроек контроллера и настроек, заданных в поле **Режим аутентификации**.

- **Надежность распознавания** — данная настройка задает вероятность предоставления доступа незарегистрированному пользователю. Например, если задана вероятность 1/1000 (**Самая низкая**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средняя**).

- **Режим аутентификации** — настройка позволяет задать способ аутентификации в режиме 1:1 для данного владельца карты. Например, для определенного владельца можно настроить проход только по карте, в то время как для других сотрудников будет задан режим *Отпечаток и ПИН*. Данная настройка недоступна, если задан режим аутентификации по отпечатку пальца.

  Обратите внимание: так как не все контроллеры поддерживают предлагаемые режимы аутентификации, ознакомьтесь с настройками контроллера. В том случае, если необходима аутентификация только по карте, воспользуйтесь настройкой **Проброс карты**.

- **Число проходов в день (BioStation)** — в этом поле укажите число проходов, которые могут быть осуществлены владельцем карты за день. Настройка доступна для контроллеров BioStation.

- **Временной КПВ (BioStation)** — настройка позволяет задать частоту повторных проходов для сотрудника в течение одного рабочего дня. Настройка доступна для контроллеров BioStation.

- **Эксперт** — настройка зарезервирована для использования в будущем.

- В группе параметров **СКД Suprema 2** укажите следующие настройки:
  - При выборе пункта **Из групп доступа** поля заблокированы, и для данного владельца будут использоваться те настройки, которые указаны в закрепленных за ним группах доступа.

  - **Текущие** — при выборе этого пункта для каждого из владельцев карты можно переопределить ряд настроек, задающихся на вкладке «**Биометрия**»:

    Обратите внимание: с помощью данных настроек можно переопределить настройки доступа в том случае, если на контроллере разрешен режим индивидуальной аутентификации.

    - **Надежность распознавания** — данная настройка задает вероятность предоставления доступа незарегистрированному пользователю.

Например, если задана вероятность 1/1000 (**Самая низкая**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средняя**).

- **Режим аутентификации** — группа настроек позволяет задать способ аутентификации в режиме 1:1 для данного владельца карты. Например, для определенного владельца можно настроить проход только по карте, в то время как для других сотрудников будет задан режим *Биоданные и ПИН*. Данная настройка недоступна, если задан режим аутентификации по отпечатку пальца.

Обратите внимание: так как не все контроллеры поддерживают предлагаемые режимы аутентификации, ознакомьтесь с настройками контроллера.

  - **Карта** — выберите режим, который будет использоваться для верификации пользователя на устройстве с использованием карты (*Карта*, *Карта и биоданные*, *Карта и ПИН*, *Карта и биоданные или ПИН*, *Карта*, *биоданные и ПИН*, *Запрещен*, *Из устройства*). Если выбран режим *Запрещен*, то сотрудник не сможет получить доступ по карте. При выборе режима *Из устройства* для верификации пользователя будет использоваться режим, указанный на вкладке «**Режимы**» объекта *Контроллер СКД Suprema 2*.

  - **Биоданные** — выберите режим, который будет использоваться для идентификации пользователя на устройстве (*Биоданные*, *Биоданные и ПИН*, *Запрещен*, *Из устройства*). Если выбран режим *Запрещен*, то сотрудник не сможет получить доступ по биоданным. При выборе режима *Из устройства* для идентификации пользователя будет использоваться режим, указанный на вкладке «**Режимы**» объекта *Контроллер СКД Suprema 2*.

  - **ID** — выберите режим, который будет использоваться для верификации пользователя на устройстве с использованием ID (*ID и биоданные*, *ID и ПИН*, *ID и биоданные или ПИН*, *ID, биоданные и ПИН, Запрещен*, *Из устройства*). Если выбран режим *Запрещен*, то сотрудник не сможет получить доступ по ID. При выборе режима *Из устройства* для верификации пользователя будет использоваться режим, указанный на вкладке «**Режимы**» объекта *Контроллер СКД Suprema 2*.

- **Эксперт** — настройка зарезервирована для использования в будущем.

На вкладке **«Эксперт»** можно выполнить следующее:

- кнопка **Дополнительные настройки** — с помощью этой кнопки открывается диалоговое окно ***Дополнительные настройки идентификатора***.

В этом диалоговом окне можно установить дополнительные настройки идентификатора (рекомендуется опытным пользователям):

- **Код выдачи** — номер версии одной и той же карты. Используется только

для карт магнитного формата в том случае, когда печатается и кодируется карта с прежней информацией (настройка используется только для оборудования Apollo).

- **Расширенные настройки карт** — укажите объект типа *Расширенные настройки карт*, в котором указано, каким образом данная карта должна идентифицироваться на считывателях VertX (настройка используется для оборудования VertX).

- кнопка **Собственная группа доступа** — с помощью этой кнопки открывается диалоговое окно ***Собственная группа доступа***, где можно изменить настройки групп доступа, закрепленные за идентификатором (рекомендуется опытным пользователям).

- кнопка **Очистить** — кнопка позволяет очистить собственные настройки доступа для данного идентификатора. После этого для идентификатора будут использоваться настройки тех групп доступа, которые указаны в поле **Список групп доступа** на вкладке **«Основные»**.

- кнопка **Загрузить** — кнопка позволяет загрузить в объект настройки, сохраненные ранее в файле формата *.xml.

- кнопка **Сохранить** — кнопка позволяет сохранить настройки объекта в файл формата *.xml.

На вкладке **«Биоданные»** расположена таблица занесенных отпечатков и лиц владельца.

Для работы с таблицей на панели инструментов находятся следующие кнопки:

- **Добавить отпечаток** — кнопка позволяет добавить новый отпечаток. При нажатии на кнопку в нижней части вкладки станут доступны настройки занесения отпечатка.
- **Добавить лицо** — кнопка позволяет добавить лицо. При нажатии на кнопку в нижней части вкладки станут доступны настройки занесения лица.
- **Удалить** — кнопка удаляет выбранный в таблице отпечаток/лицо.
- **Проверить отпечаток** — кнопка откроет окно ***Проверка отпечатка***, которое позволяет сравнить выбранный отпечаток с приложенным на считыватель пальцем.

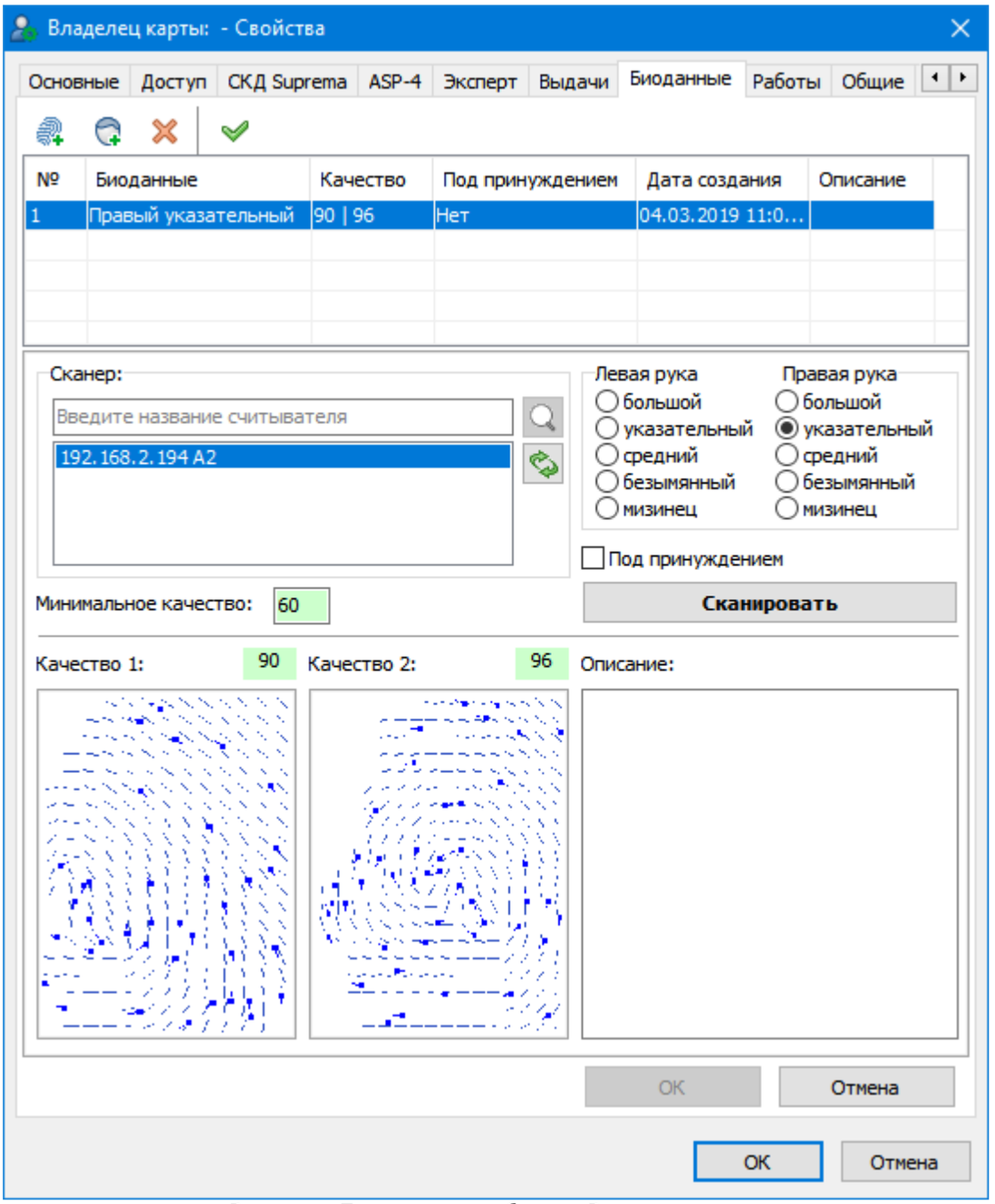
Для редактирования уже занесенных биоданных выберите строчку в таблице и скорректируйте настройки в нижней части вкладки.

Таблица содержит следующие столбцы:

- **№** — порядковый номер данных, записанных в таблицу.
- **Биоданные** — в этой колонке отображается информация о занесенных биоданных. Например, запись *Левый большой* говорит о том, что для сканирования был использован большой палец левой руки, а запись *Лицо* говорит о том, что в таблицу было занесено лицо пользователя.
- **Качество** — в этой колонке отображается полученное при сканировании качество отпечатка/лица.
- **Под принуждением** — колонка отображает, является ли данный отпечаток отпечатком под принуждением.
- **Дата создания** — колонка отображает дату и время занесения

отпечатка/лица.

- **Описание** — колонка отображает информацию, добавленную при занесении отпечатка/лица в поле **Описание**.



Вкладка «**Биоданные**» объекта *Владелец карты*

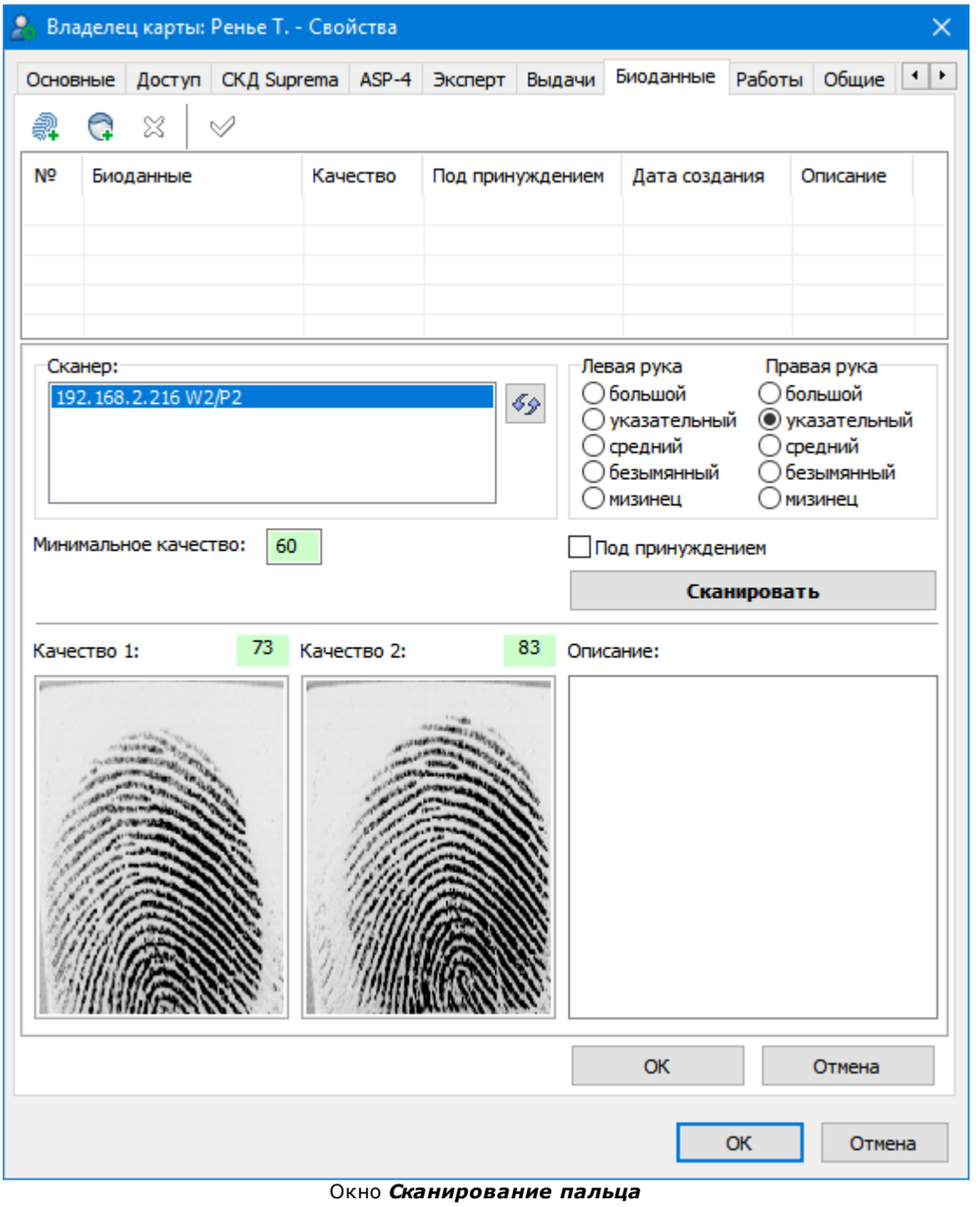
Добавление и редактирование отпечатка

При добавлении или редактировании отпечатка в нижней части вкладки становятся доступны следующие настройки:

- **Сканер** — укажите контроллер, с помощью которого будет осуществляться сканирование – BioMini или другой из добавленных в конфигурацию контроллеров. С помощью кнопки **Обновить** можно обновить список доступных сканеров.
  Над списком сканеров находится поле поиска. Начните вводить название устройства, и список сканеров будет автоматически обновляться в соответствии с вводимой информацией.
- В группе параметров **Левая рука** и **Правая рука** выберите палец,

который был использован для сканирования отпечатка.

- **Под принуждением** — поставьте этот флажок, чтобы сканируемый палец был занесен в память контроллера как «тревожный». **Например**, в ситуации, когда сотрудника принуждают войти в помещение, он может приложить палец, который был внесен в базу как «тревожный». В систему поступит сообщение *Доступ разрешен под принуждением*.
- **Минимальное качество** — в этом поле укажите качество отпечатка от 0 до 100. Рекомендуемое значение, обеспечивающее возможность занесения любого отпечатка с необходимым набором отличительных черт для однозначной идентификации, равно 60. Каждый отпечаток сканируется дважды.
- **Качество 1**, **Качество 2** — в этих полях отображается полученное при сканировании качество первого и второго отпечатка.
- **Первый шаблон**, **Второй шаблон** — поля содержат схемы отсканированных отпечатков.
- **Описание** — укажите необходимую информацию о сканировании.
- Кнопка **ОК** — нажмите, чтобы сохранить отпечаток.
- Кнопка **Отмена** — нажмите, чтобы завершить редактирования отпечатка без сохранения изменений.



Окно ***Сканирование пальца***

Добавление и редактирование лица

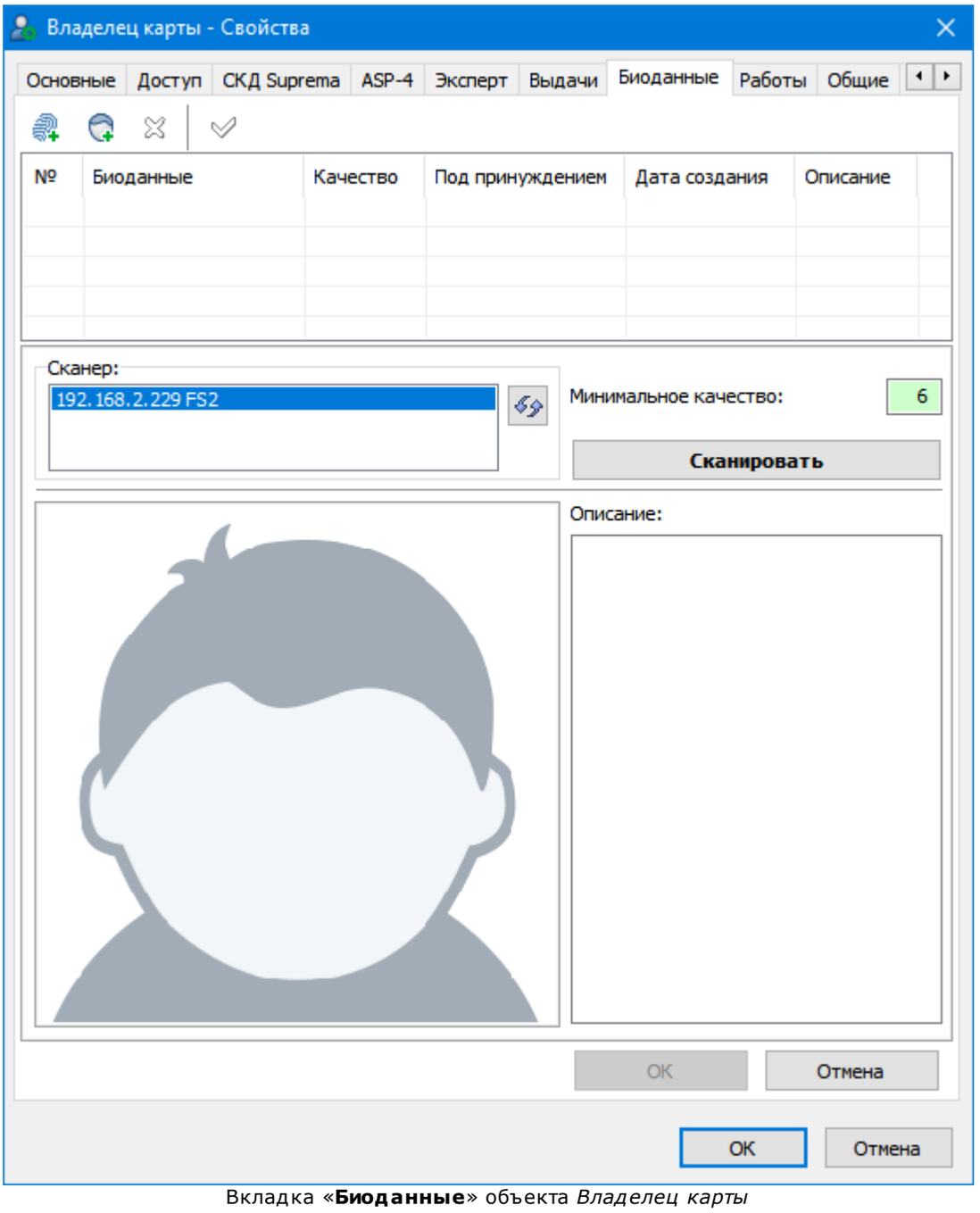
При добавлении или редактировании лица в нижней части вкладки становятся доступны следующие настройки:

- **Сканер** — укажите контроллер, с помощью которого будет осуществляться сканирование. С помощью кнопки **Обновить** можно обновить список доступных сканеров.
- Над списком сканеров находится поле поиска. Начните вводить название устройства, и список сканеров будет автоматически обновляться в соответствии с вводимой информацией.
- **Минимальное качество занесения** — укажите минимальное качество сканирования лица от 1 до 9. Если сканирование проходит в темном помещении, контроллер будет раз за разом пытаться отсканировать лицо, пока не добьется указанного значения, в этом случае для быстрого занесения лица рекомендуется снизить минимальное качество. Заносите лица с максимальным качеством, так вы избежите ошибок при распознавании.

- **Описание** — укажите необходимую информацию о сканировании.

После сканирования рядом с описанием будет размещен снимок отсканированного лица, он же будет показан на контроллере при успешной авторизации сотрудника. Для того чтобы на экране контроллера отображалось фото из вкладки **«Основные»** окна редактирования владельца карты, сделайте следующее:

Откройте файл [APACS]\bin\ApcSysExt\ApcSecurityManager \tApcSysExtRegistry.xml и в строке <KeyValue Name="DownloadPhoto" vType="Bool" vValue="false"/> поменяйте значение vValue на true.



Вкладка «**Биоданные**» объекта *Владелец карты*

Обратите внимание: в режиме 1:N, когда для прохода нужно отсканировать только лицо, контроллер может работать с 3000 лицами в базе. В режиме 1:1, когда для прохода нужно отсканировать лицо и предъявить карту/набрать ПИН, контроллер может работать с 30000 лицами в базе.

Команды

Объект не поддерживает команд управления и клиентских команд.