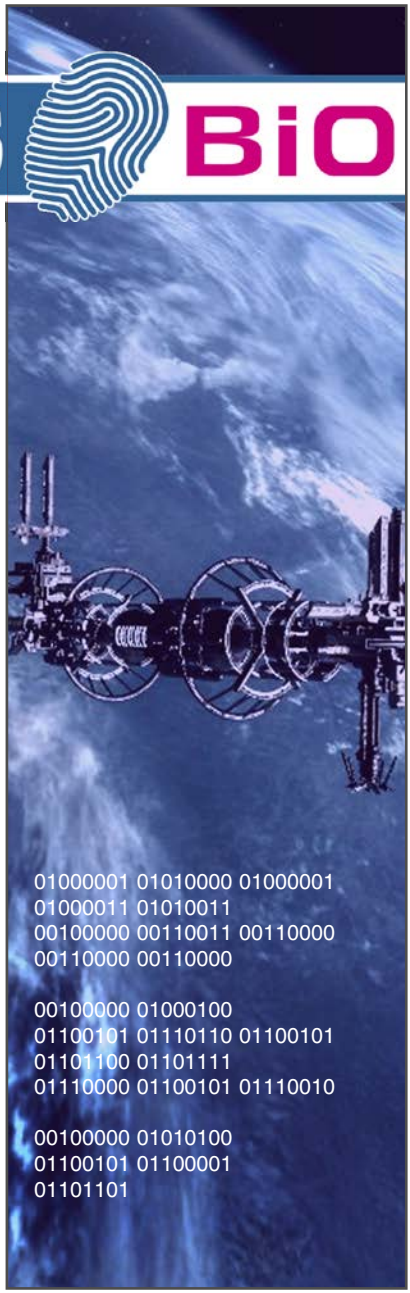
APACS BiO

Драйвер «Управление доступом»



Руководство пользователя

1 Введение

Драйвер «Управление доступом» ПК APACS Bio позволяет конфигурировать и управлять правами доступа и привилегиями сотрудников на контролируемой территории.

Драйвер обладает следующими характерными особенностями:

- позволяет гибко назначать права доступа пользователям в рамках контролируемой территории,
- позволяет работать как с одним, так и с несколькими однотипными контроллерами,
- предоставляет возможность проверки наличия ошибок и неточностей при настройке прав доступа,
- позволяет эффективно и максимально полно использовать возможности оборудования.

Таким образом, драйвер «Управление доступом» предоставляет детальную и глобальную поддержку возможностей оборудования на уровне программного обеспечения.

В текущей версии драйвер поддерживает следующее оборудование:

- контроллеры СКД Suprema: BioEntry W/Plus, BioLite, BioStation, BioStation T2, Xpass/S2,
- контроллеры СКД Suprema 2: BioStation A2, BioStation L2, BioStation 2, BioEntry W2, BioEntry W/Plus, BioLite, Xpass/S2.

1.1 Основные объекты драйвера «Управление доступом»

Основу драйвера «Управление доступом» составляют следующие объекты: *Владелец карты*, *Идентификатор*, *Группа доступа*.

Владелец карты – объект системы, содержащий информацию о сотруднике.

Идентификатор – логический объект системы, который ассоциируется с физическим объектом на руках сотрудника – картой, брелком, ключом и т.д.

Группа доступа – логический объект, представляющий собой совокупность прав и привилегий доступа сотрудников на контролируемой территории.

Эти объекты позволяют гибко назначать права доступа пользователям в рамках контролируемой территории.

1.1.1 Связь владельцев карт и идентификаторов

Связь владельцев карт и идентификаторов осуществляется с помощью объекта *Выдача*. Этот объект является простой ссылкой и не содержит дополнительных настроек, поэтому процесс выдачи карты владельцу является простым и удобным. Одному владельцу могут быть выданы сразу несколько идентификаторов. А идентификатор в один и тот же момент может принадлежать только одному владельцу или же может быть не выданным.

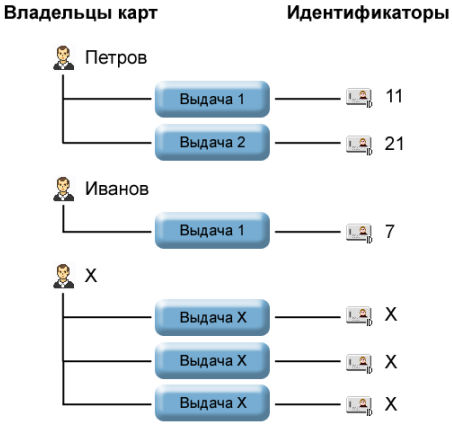


Рисунок Связь между владельцами карт и идентификаторами

Связь между идентификатором и владельцем легко разорвать, при этом идентификатор сохраняется в базе данных и может быть использован в дальнейшем.

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. Чтобы использовать эти идентификаторы в дальнейшем, в их настройках требуется поставить флажок **Активность** (подробнее см. настройки объекта *Идентификатор*).

Наличие связи между владельцем карт и идентификатором позволяет дополнять сообщения, поступающие от контроллера, информацией о владельце карты. В случае если карта не выдана, в сообщении будет указано, что владелец карты не найден.

Такой подход позволяет отслеживать и сохранять в базу данных информацию о том, какой владелец какой картой владел во время регистрации того или иного события. Это удобно использовать в случае, когда карты выдаются разным посетителям.

1.1.2 Группа доступа

На одном объекте может быть использовано несколько контроллеров доступа. Поэтому назначать права удобнее сразу на несколько контроллеров, которые имеют свой собственный список уровней доступа (УД), временных зон (ВЗ) и т.д. Для назначения прав сразу на несколько контроллеров используется объект *Группа доступа* (ГД).

В состав ГД могут быть включены локальные списки уровней доступа разных контроллеров.

Например, на объекте есть два контроллера BioEntry W2: BioEntry W2_*№1* и BioEntry W2_*№2* и сконфигурирована *ГД Инженер*, в которую входят ссылки на оба контроллера и для каждого контроллера указаны ссылки на его локальные объекты Список уровней доступа *инженер №1* и *Список уровней доступа инженер №2*. Если какой-либо пользователь будет включен в *ГД Инженер*, то система будет точно знать какие локальные объекты должны быть прогружены в каждый из контроллеров.

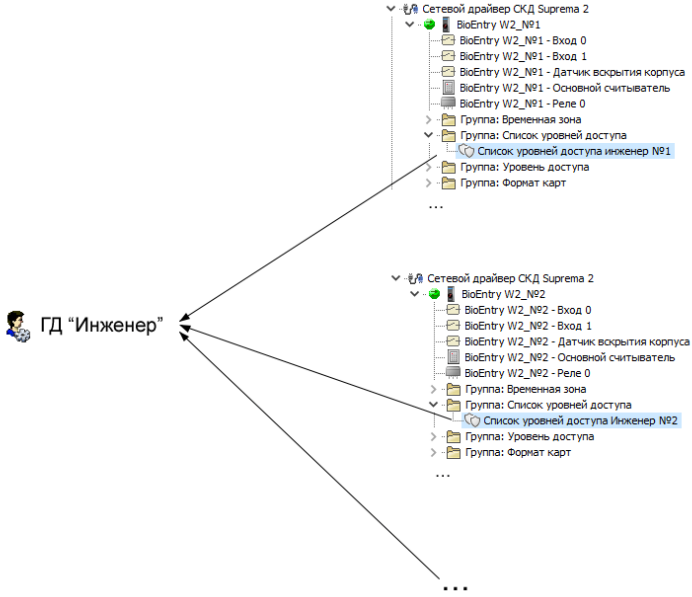


Рисунок Группа доступа Инженер

Назначение нескольких ГД

Ещё одной возможностью комплекса является возможность включения пользователя сразу в несколько ГД. Данную возможность можно использовать для выделения на объекте определенных зон доступа, в которые будут впоследствии включены пользователи.

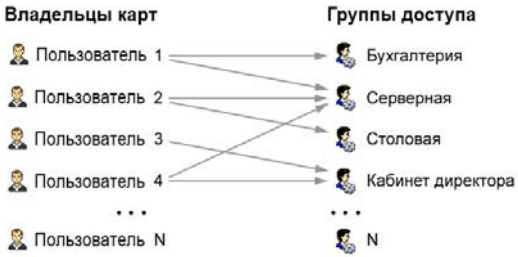


Рисунок Назначение пользователям нескольких различных групп доступа

Например, на объекте можно выделить следующие зоны доступа: *ГД Офис*, *ГД Прихожая* и *ГД Столовая*. Тогда сотрудника офиса можно включать во все ГД, а, например, сотрудника столовой включить только в *ГД Прихожая* и *ГД Столовая*.

Типы настроек доступа

Настройки доступа, закрепленные за сотрудником с помощью групп доступа, можно разделить на следующие типы:

- *списковые* — представляют собой список из нескольких значений (например, список уровней доступа),
- *дискретные* — представляют собой одно из нескольких известных значений (например, настройки со значением *Да/Нет*, настройки даты и времени).

Суммирование настроек доступа

Если за одним сотрудником закреплено несколько групп доступа с разными настройками, то происходит суммирование настроек. То, каким образом будут суммированы настройки, определяется по типу самих настроек и их приоритету:

- максимально высокий приоритет имеют настройки, указанные явно в настройках карты/владельца карты (см. далее п. «1.2 Дополнительные настройки доступа»),
- далее настройки располагаются по приоритету в том порядке, в каком группы доступа, назначенные сотруднику, указаны в списке (см. далее п. «3.4 Идентификатор», поле Список групп доступа).

Списковые настройки просто складываются и располагаются по приоритету. Например, сотруднику назначены две группы доступа, в первой указаны два локальных уровня доступа: *УД Офис* и *УД Бухгалтерия*, во второй— три: *УД Кабинет директора*, *УД Серверная* и *УД Столовая*. В

результате для сотрудника будут использоваться пять локальных уровней доступа со следующим приоритетом:

- *УД Офис*,
- *УД Бухгалтерия*,
- *УД Кабинет директора*,
- *УД Серверная*,
- *УД Столовая*.

Для дискретных настроек используются следующие правила:

- если настройка не используется (в группе доступа не стоит флажок **Задать**), настройка не учитывается.
- если в группах доступа, назначенных сотруднику, указаны разные значения дискретных настроек (например, в одной группе доступа стоит флажок **Исключить из зоны КПВ**, а в другой группе — не стоит), для сотрудника используется значение с более высоким приоритетом.

1.2 Дополнительные настройки доступа

При загрузке карт в контроллеры, кроме номера карты и уровней доступа, также зачастую загружаются дополнительные настройки, такие как:

1. дата/время активации/деактивации,
2. уровень надежности,
3. настройки аутентификации.

В комплексе есть возможность задавать значение данных настроек как в самих экземплярах карт/владельцев карт, так и в объектах ГД. Исходя из этого, в комплексе ПК APACS Bio предусмотрены два стиля оформления приложения «Картотека»: *максимальный* и *минимальный*.

Максимальный стиль предполагает, что все настройки доступа задаются в экземплярах владельцев карт. В большинстве случаев рекомендуется использовать этот подход, так как при его использовании можно сразу однозначно определить, какие настройки доступа заданы и используются для владельца карты.

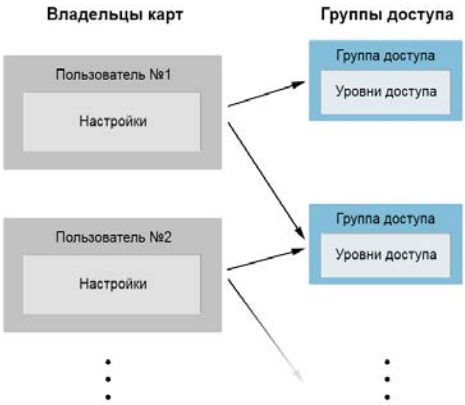


Рисунок Максимальный стиль оформления «Картотеки»

Минимальный стиль предполагает, что все настройки доступа указываются в объектах *Группа доступа*, назначенных сотрудникам. При таком подходе финальный набор значений настроек определяется суммированием всех настроек из ГД, куда входит сотрудник (см. п. 1.1.2 Группа доступа).

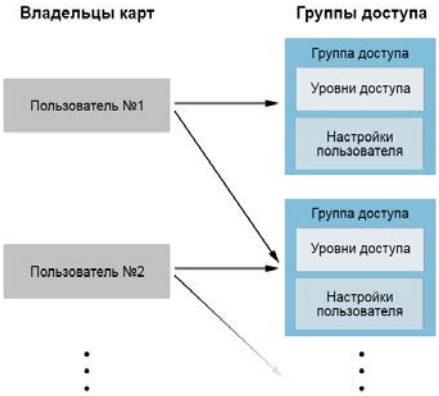


Рисунок Минимальный стиль оформления «Картотеки»

1.3 Назначение прав доступа

В комплексе ПК APACS Bio права доступа задаются у владельца карты и все выданные ему карты наследуют заданные настройки. При использовании такого подхода карты будут хранить только собственные настройки (такие как номер, ПИН код и т.д).

2. Права доступа задаются у владельца карты и все выданные ему карты наследуют заданные настройки. При использовании такого подхода карты будут хранить только собственные настройки (такие как номер, ПИН код и т.д).

Обратите внимание: в ПК APACS Bio не поддерживаются карты с собственными настройками, настройки доступа всегда наследуются от владельца карты.

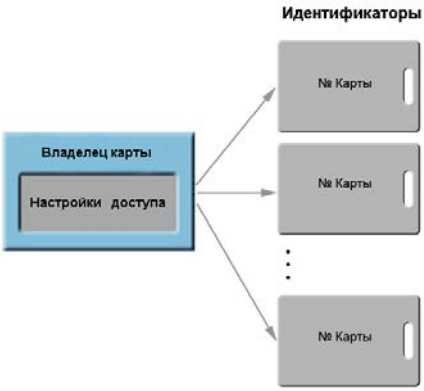


Рисунок Задание настроек доступа у владельца карты

Тип хранения настроек доступа, который будет использоваться, указывается при создании или выдаче идентификаторов. Для работы с APACS Bio необходимо задать тип хранения настроек доступа *Права наследуются от владельца карты*. Для этого выберите меню «Настройки/Настройки картотеки» и в группе параметров **Выбор типа создаваемой карты** выберите пункт и в нем.

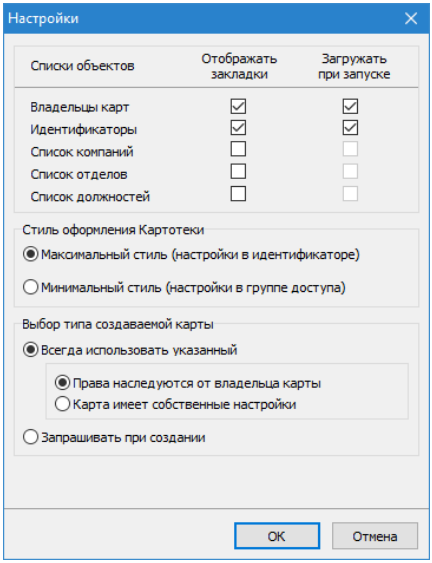


Рисунок Окно ***Настройки***

1.4 Связь драйвера и оборудования

Объекты драйвера «Управление доступом» являются логическими, и их конфигурирование не зависит от установленного оборудования. Но возможности того или иного оборудования накладывают ограничения на использование объектов. Обратите внимание на ограничения возможностей оборудования: количество отпечатков и пользователей, которые могут храниться в памяти контроллера, ограничено и зависит от типа используемого контроллера.

Поэтому при конфигурировании объектов драйвера «Управление доступом» администратору комплекса необходимо исходить из возможностей установленного оборудования.

2 Конфигурирование прав доступа

Рассмотрим примерный порядок конфигурирования системы для определения прав доступа сотрудников.

Подготовка

На подготовительном этапе рекомендуется выполнить следующее:

- При конфигурировании прав доступа рекомендуется опираться на возможности конкретного оборудования, которое установлено на объекте. Ознакомьтесь с документацией на оборудование и определите, какие функции оборудования Вы будете использовать.
- В рамках контролируемой территории выделите зоны доступа (например, основная рабочая зона, серверная, кабинет директора, столовая и т.п.).
- Определите временные границы работы на предприятии (например, сотрудники работают с понедельника по пятницу с 9:00 до 18:00, приходящие уборщицы работают с понедельника по пятницу с 8:00 до 9:00).
- Определите контроллеры, которые будут контролировать вход и выход из зон доступа в течение временных границ.
- Разделите сотрудников на группы в зависимости от зон, в которых они работают, и временных границ.

Создание локальных списков уровней доступа

В ПК APACS Bio сконфигурируйте локальные списки уровней доступа (конфигурирование системы осуществляется в окне ***Проводник*** приложения «Консоль»). Для этого:

- Занесите в систему информацию о временных границах работы на предприятии. Создайте столько объектов типа *Временная зона* для используемого оборудования, сколько временных границ используется на предприятии.
- Исходя из количества зон доступа и временных рамок работы, создайте локальные уровни доступа (объекты типы *Уровень доступа* для используемого оборудования).

- Сгруппируйте уровни доступа в списки, для этого используется объект *Список уровней доступа*.

Например, на предприятии следующие зоны доступа — основная рабочая зона, серверная и кабинет директора. Временные рамки работы: все сотрудники работают с 9:00 до 18:00, уборщицы — с 8:00 до 9:00. Поэтому требуется создать два объекта *Временная зона*: *ВЗ Рабочий день* и *ВЗ Уборка*, и следующие уровни доступа и списки уровней доступа:

- *Основная зона* — доступ всем сотрудникам в основную рабочую зону в течение *ВЗ Рабочий день*,
- *Доступ в серверную* — доступ в серверную для сотрудников технического отдела в течение *ВЗ Рабочий день*,
- *Доступ в кабинет директора* — доступ для директора в течение *ВЗ Рабочий день*.

Чтобы уборщицы могли ходить по помещениям во время своей временной зоны, требуется создать:

- *Основная зона «Уборка»* — доступ в основную рабочую зону в течение *ВЗ Уборка*,
- *Доступ в серверную «Уборка»* — доступ в серверную в течение *ВЗ Уборка*,
- *Доступ в кабинет директора «Уборка»* — доступ в кабинет в течение *ВЗ Уборка*.

А также необходимо создать объект *Список уровней доступа*, куда будут включены *Доступ в серверную «Уборка»* и *Доступ в кабинет директора «Уборка»*.

Выбор подхода конфигурирования групп доступа

Далее выберите, как Вы будете конфигурировать группы доступа и где будут хранится настройки доступа:

- настройки доступа указываются в группах доступа, которые после назначаются идентификаторам/владельцам карт,
- настройки доступа указываются отдельно для каждого владельца карты.

В зависимости от этого выберите стиль оформления приложения «Картотека»: минимальный или максимальный.

Заполнение базы данных владельцев карт и идентификаторов

Для работы с базой данных владельцев карт и идентификаторов используется приложение «Картотека». В окне ***Картотека*** на закладке **«Владельцы карт»** создайте необходимое количество владельцев карт. Назначьте им идентификаторы.

Выберите подход к хранению прав доступа:

- права доступа задаются в настройках карты.
- права доступа задаются у владельца карты и все выданные ему карты наследуют заданные настройки.

И назначьте группы доступа владельцам карт или идентификаторам, в зависимости от выбранного подхода.

При необходимости используйте процедуры переноса прав доступа (подробнее см. п. «3.6 Перенос настроек доступа»).

3 Объекты драйвера «Управление доступом»

Далее рассмотрим настройки объектов *Группа доступа*, *Идентификатор*, *Владелец карты* и *Расширенные настройки карт*.

3.1 Группа доступа

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

Объект создается в приложении «Консоль» в окне ***Проводник*** путем добавления к объектам типа *Папка*.

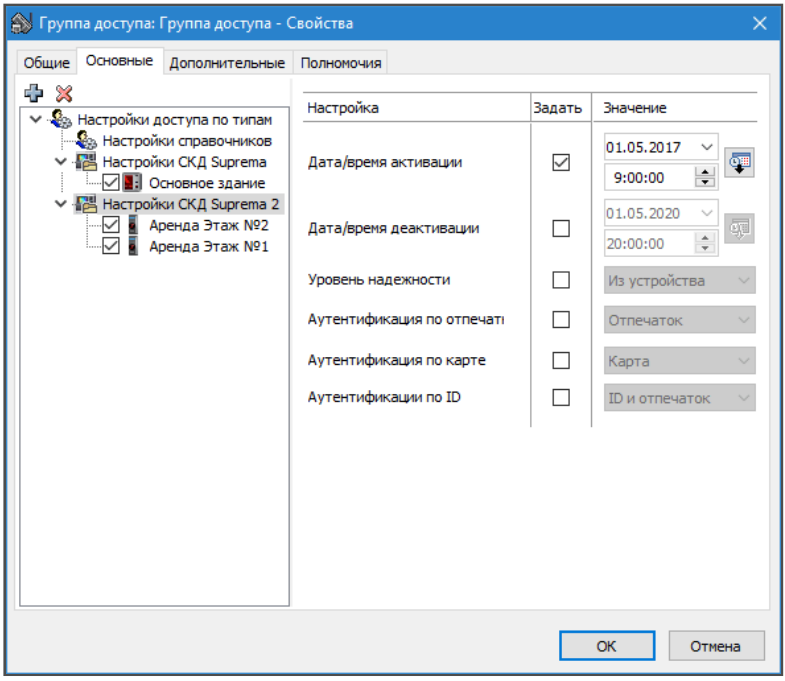


Рисунок Окно редактирования свойств объекта *Группа доступа*

Закладка **«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 (закладка **«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 или список локальных уровней доступа, который будет использоваться для данной группы доступа.

Далее рассмотрим настройки драйверов и настройки контроллеров разного типа.

Закладка с настройками драйверов представляет собой таблицу со следующими столбцами:

- **Настройка** – имя настройки,
- **Задать** – поставив этот флажок, Вы указываете, что данная настройка будет определена явным образом. Если нет этого флажка, это означает, что:
  - o настройка будет использоваться по умолчанию,
  - o настройка будет указана в идентификаторе,
  - o настройка будет указана в другой группе доступа (в том случае, если для идентификатора используется две и более групп доступа).
- **Значение** – в этом столбце Вы указываете, с каким значением настройка будет использоваться в системе.

3.1.1 Настройки драйверов в составе группы доступа

Драйвер Настройки справочников

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

Для драйверов **СКД Suprema** 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/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).
- **Уровень надежности распознавания** — данная настройка задает вероятность предоставления доступа незарегистрированному пользователю. Например, если задана вероятность 1/1000 (**Самый низкий**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средний**).
- **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.

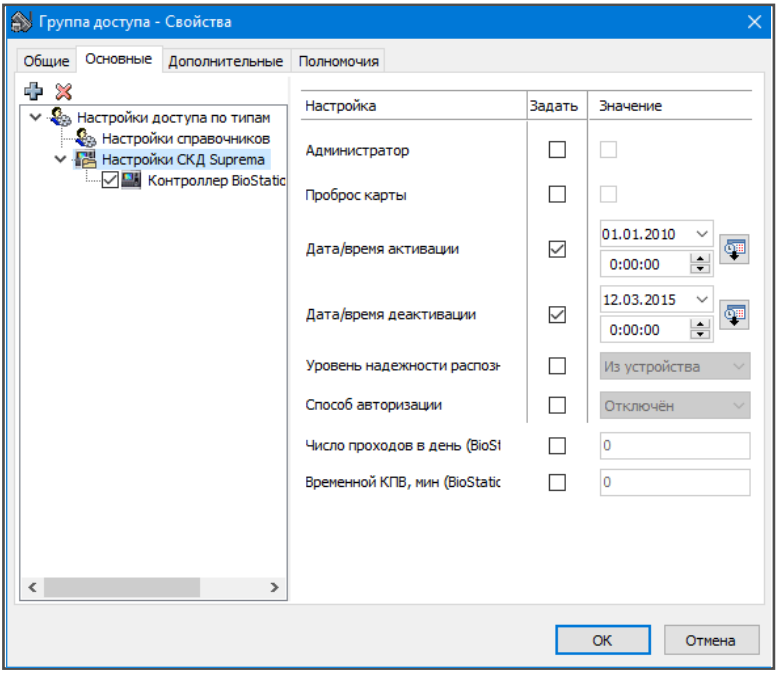


Рисунок Настройки драйвера СКД Suprema в окне редактирования свойств объекта *Группа доступа*

Драйвер СКД Suprema 2

Для драйверов **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).
- **Уровень надежности** – данная настройка задает вероятность предоставления доступа незарегистрированному пользователю. Например, если задана вероятность 1/1000 (**Самый низкий**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средний**).
- **Аутентификация по отпечатку** – выберите режим, который будет использоваться для идентификации пользователя на устройстве: **Отпечаток**, **Отпечаток и ПИН**.

- **Аутентификация по карте** – выберите режим, который будет использоваться для верификации пользователя на устройстве с использованием карты: **Карта**, **Карта и отпечаток**, **Карта и отпечаток и ПИН**, **Карта и отпечаток или ПИН**.
- **Аутентификация по ID** – в этой группе параметров находятся режимы, которые используются для верификации пользователя на устройстве с использованием ID: **ID и ПИН**, **ID и отпечаток**, **ID и отпечаток и ПИН**, **ID и отпечаток или ПИН**.

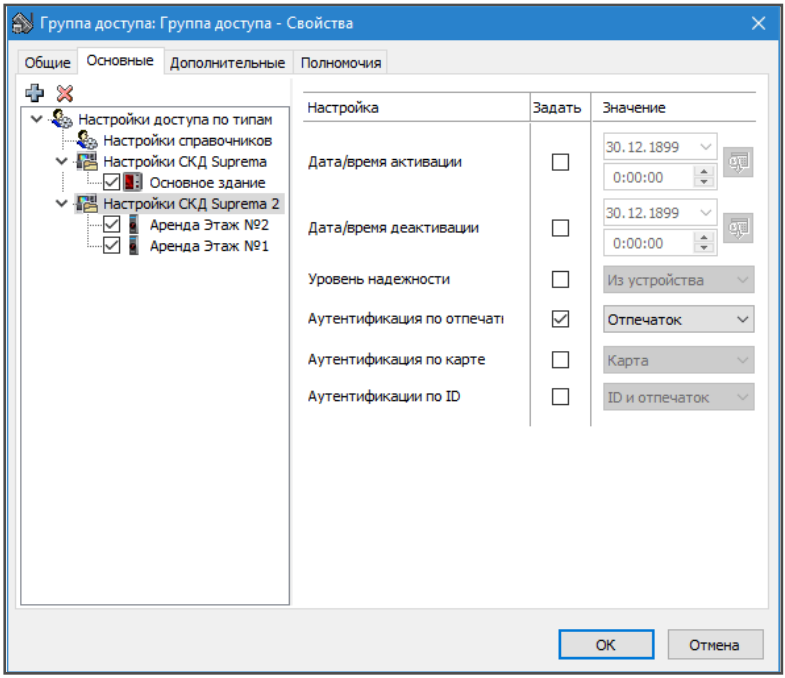


Рисунок Настройки драйвера СКД Suprema 2 в окне редактирования свойств объекта *Группа доступа*

3.1.2 Настройки контроллеров в составе группы доступа

Контроллеры СКД Suprema

В случае работы с контроллерами СКД Suprema для группы доступа используются настройки, расположенные на закладках **«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**.

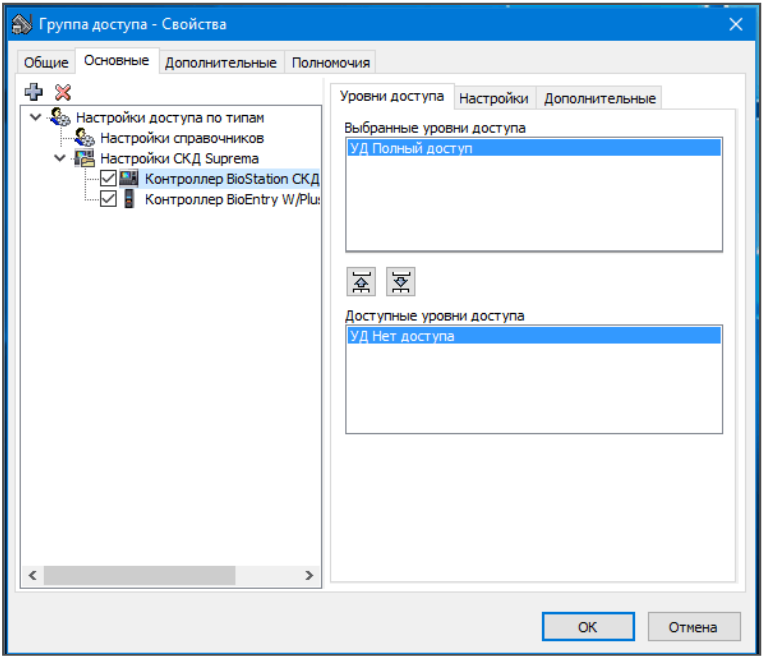


Рисунок Закладка **«Уровни доступа»** драйвера СКД Suprema в окне редактирования свойств объекта *Группа доступа*

Контроллеры СКД Suprema 2

В случае работы с контроллерами СКД Suprema 2 для группы доступа используются настройки, расположенные на закладках **«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**.

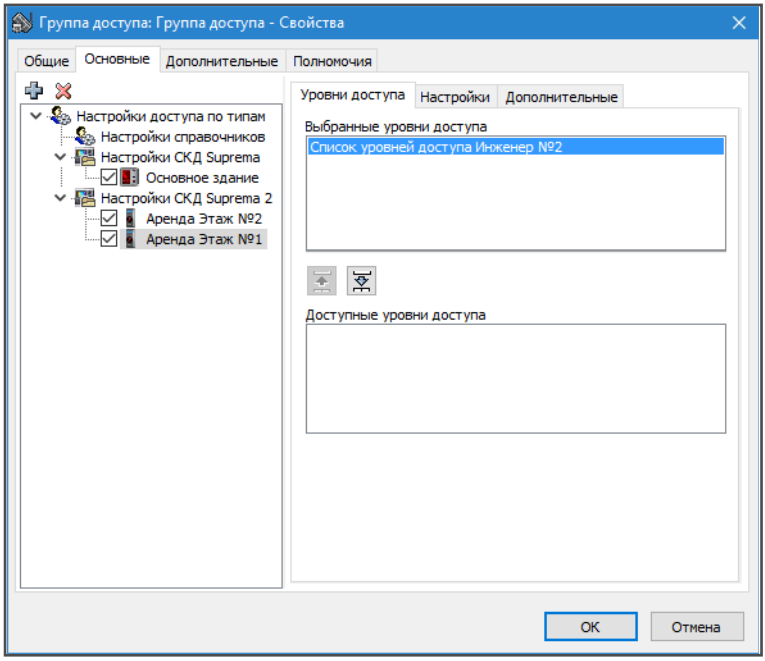


Рисунок Закладка **«Уровни доступа»** драйвера СКД Suprema 2 в окне редактирования свойств объекта *Группа доступа*

3.1.3 Команды объекта Группа доступа

Объект *Группа доступа* поддерживает команду ***Показать число идентификаторов***. При выполнении команды открывается окно с информацией о количестве идентификаторов, за которыми закреплена эта группа доступа.

3.3 Режимы применения изменений при редактировании групп доступа

При редактировании объектов типа *Группа доступа* в конфигурации системы происходит следующее:

- изменения объектов сохраняются на сервере APACS Bio,
- изменение найденных пользователей/идентификаторов,
- загрузка пользователей/идентификаторов в контроллеры.

Процесс применения новых настроек и загрузки в контроллеры может занимать достаточно много времени, в течение которого карты могут быть «нерабочими» (еще не загруженными в контроллер). Поэтому при редактировании этих объектов оператору предлагается выбрать режим сохранения изменений:

- *немедленная отработка изменений* — изменения объектов сохраняются на сервере APACS Bio и сразу же загружаются в контроллеры. Этот режим удобно использовать в случае единичных изменений объектов или когда на предприятии мало контроллеров и карт и загрузка происходить быстро.
- *сохранение изменений на сервере APACS Bio, а после загрузка карт в контроллеры по решению оператора* — в этом режиме контроллеры становятся рассинхронизированными с базой данных карт и после для синхронизации обязательно на контроллерах нужно выполнить команду ***Загрузить карты***. Режим удобно использовать в случае множественных изменений объектов или когда редактирование происходит в течение работы системы контроля доступа.
- *отложенные изменения* — в этом режиме изменения объектов откладываются (не сохраняются на сервере APACS Bio и не загружаются в контроллеры). После оператор самостоятельно решает, как поступить с отложенными изменениями. Режим удобно использовать для редактирования нескольких объектов, настройки которых пересекаются (например, несколько групп доступа, в состав которых включены одинаковые локальные уровни доступа).

Способ сохранения изменений можно выбрать до начала редактирования групп доступа или во время редактирования.

Чтобы выбрать способ сохранения до начала редактирования, в приложении «Консоль» выберите пункт меню «Настройки / Настройки применения изменений групп доступа» окна ***Главная панель***. Откроется диалоговое окно ***Настройки применения изменений групп доступа***, где можно выбрать следующие режимы:

- **Запрашивать после каждого редактирования** — в этом режиме после каждого редактирования объекта типа *Группа доступа* будет открываться диалоговое окно ***Выберите тип отработки изменений***, где можно указать, как поступить с последним изменением объекта.
- **Откладывать применение изменений** — в этом режиме все изменения групп доступа откладываются и заносятся в диалоговое окно ***Отложенные запросы***, которое можно вызвать из меню «Окно». После, закончив редактирование групп доступа, можно указать, каким образом сохранить изменения.
- **Сохранять изменения и загружать карты в контроллер** — в этом режиме изменения групп доступа сразу же сохраняются на сервер APACS Bio и загружаются в контроллеры.
- **Сохранять изменения, но не загружать карты в контроллер** — в этом режиме изменения сразу же сохраняются на сервер APACS Bio, но не загружаются в контроллеры. Чтобы загрузить изменения, для каждого контроллера выполните команду ***Загрузить карты***.

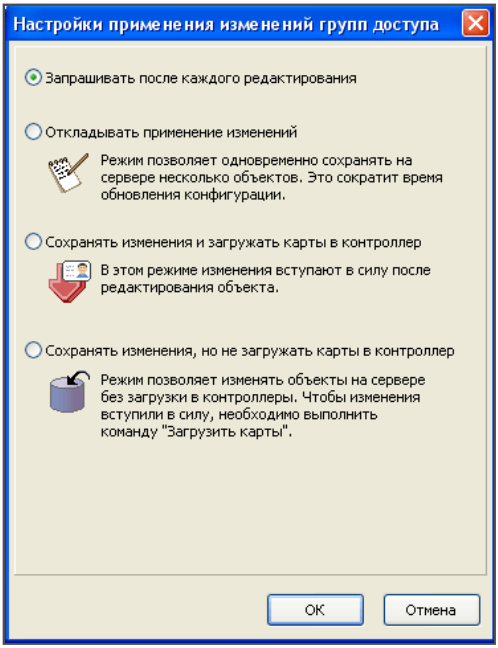


Рисунок Окно ***Настройки применения изменений групп доступа***

Если режим сохранения изменений не выбран или же выбран режим **Запрашивать после каждого редактирования**, после каждого изменения группы доступа будет открываться диалоговое окно ***Выберите тип отработки изменений***, где можно указать, как поступить с последним изменением объекта. Выберите способ сохранения и нажмите кнопку **Далее**.

Чтобы в дальнейшем использовать выбранный способ, поставьте флажок **Всегда использовать выбранный тип**.

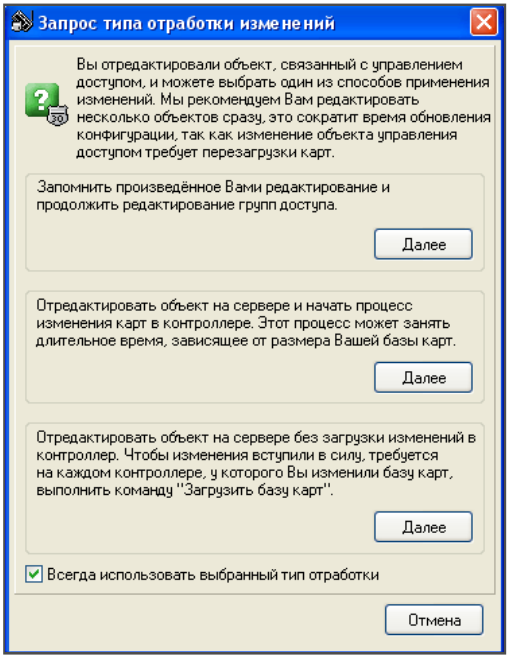


Рисунок Окно ***Выберите тип отработки изменений***

Если выбран режим отложенных изменений, после каждого редактирования объектов типа *Группа доступа* будет открываться диалоговое окно ***Отложенные запросы***. В этом окне требуется указать, как поступить с отложенными запросами по редактированию.

- **Список отложенных изменений** — в этой таблице находится список изменений, которые еще не вступили в силу. Для каждого объекта указывается:
  - имя объекта,
  - текущее состояние,
  - время последнего изменения.

  Чтобы отказаться от редактирования объекта, выделите информацию о нем в таблице и нажмите кнопку **Отменить редактирование**. Настройки объекта вернуться в первоначальное состояние.
- **Завершить отработку отложенных запросов** — укажите, как следует поступить с отложенными запросами:
  - **Отработать полностью — сохраняются объекты, отрабатываются идентификаторы**
  - **Сохранить изменения объектов без отработки идентификаторов**
  - **Отказ от изменений — все изменения теряются**
  - кнопка **Отработать запросы сейчас** — с помощью этой кнопки можно применить изменения немедленно.

- кнопка **Скрыть окно** — нажмите на эту кнопку, чтобы поместить окно ***Отложенные запросы*** в меню «Окно» ***Главной панели***.

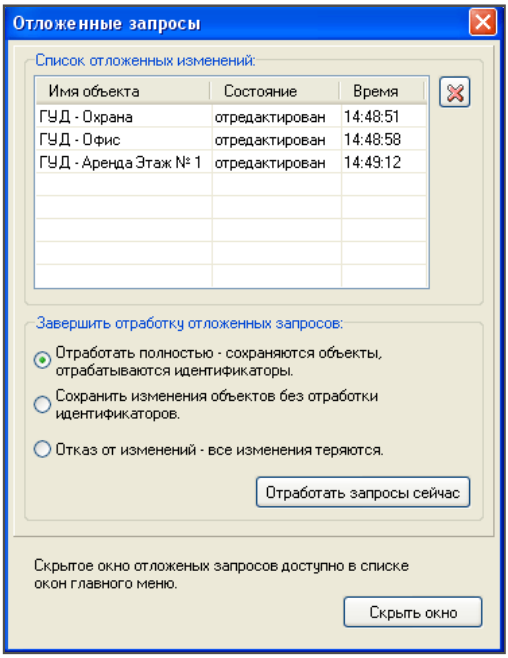


Рисунок Окно ***Отложенные запросы***

Если в диалоговом окне ***Отложенные запросы*** был выбран режим **Отработать полностью** и нажата кнопка **Отработать запросы сейчас**, изменения в группах доступа будут сохранены на сервере APACS Bio и идентификаторы загружены в контроллеры. После выполнения откроется диалоговое окно ***Результаты загрузки идентификаторов*** с отчетом о загрузке идентификаторов. С помощью кнопки **Сохранить** можно сохранить отчет в файл формата *.txt.

Если в диалоговом окне ***Отложенные запросы*** был выбран режим **Сохранить изменения объектов без отработки идентификаторов** и нажата кнопка **Отработать запросы сейчас**, изменения в группах доступа будут сохранены на сервере APACS Bio, но идентификаторы не будут загружены в контроллеры. После выполнения откроется диалоговое окно ***Список контроллеров*** со списком контроллеров, для которых необходимо загрузить идентификаторы. Это можно сделать с помощью команды ***Загрузить карты***.

3.4 Идентификатор

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

Работа с идентификаторами осуществляется в рамках приложения «Картотека». Создать новые объекты данного типа можно на закладке **«Идентификаторы»** окна ***Картотека*** с помощью кнопки **Добавить**.

Настройки объекта находятся на закладках **«Основные»** и **«Эксперт»**. Закладка **«Эксперт»** позволяет задать собственные настройки доступа для конкретного идентификатора, эту закладку рекомендуется использовать только опытным операторам комплекса.

3.4.1 Закладка «Основные»

Закладка **«Основные»** выглядит 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 закладке **«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 ***Ошибки, найденные при проверке идентификатора***. Если ошибок нет, сообщение об этом появится в диалоговом окне ***Информация***.

Обратите внимание: настройка **Проверить идентификатор** недоступна для контроллеров Suprema.

  - кнопка **Показать объединенную группу доступа** — нажмите на эту кнопку, чтобы посмотреть всю совокупность настроек, которые будут использованы для конкретного идентификатора (подробнее см. п «3.4.3 Просмотр настроек идентификатора»).
  - **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 (см. «Apc: Глава 6 Картотека 6.5 Клиентский модуль USB считыватель карт Parsec»).

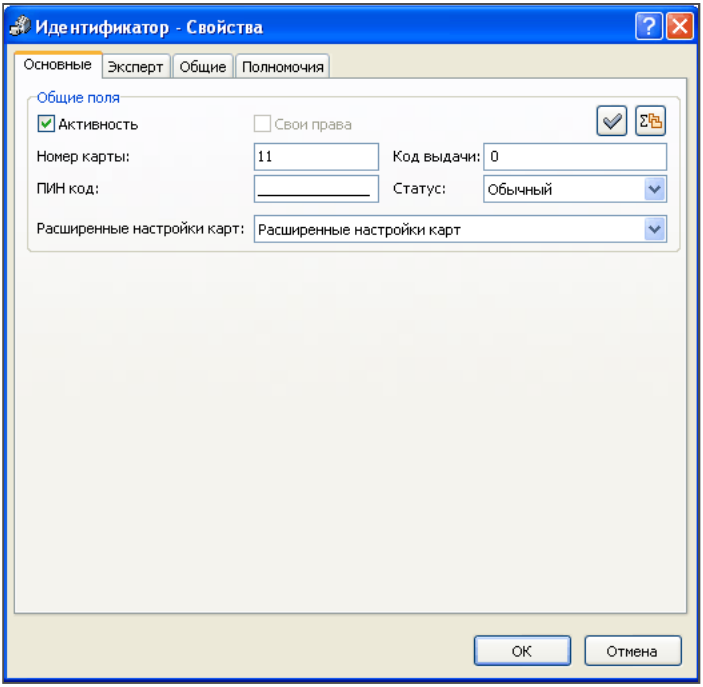


Рисунок Закладка «**Основные**« объекта *Идентификатор*

- **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** — настройка не используется для контроллеров Suprema.

3.4.3 Просмотр настроек идентификатора

Чтобы посмотреть всю совокупность настроек, которые будут использованы для конкретного идентификатора, на закладке **«Основные»** нажмите кнопку **Показать объединенную группу доступа**. Откроется диалоговое окно ***Результирующая группа доступа***. 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.

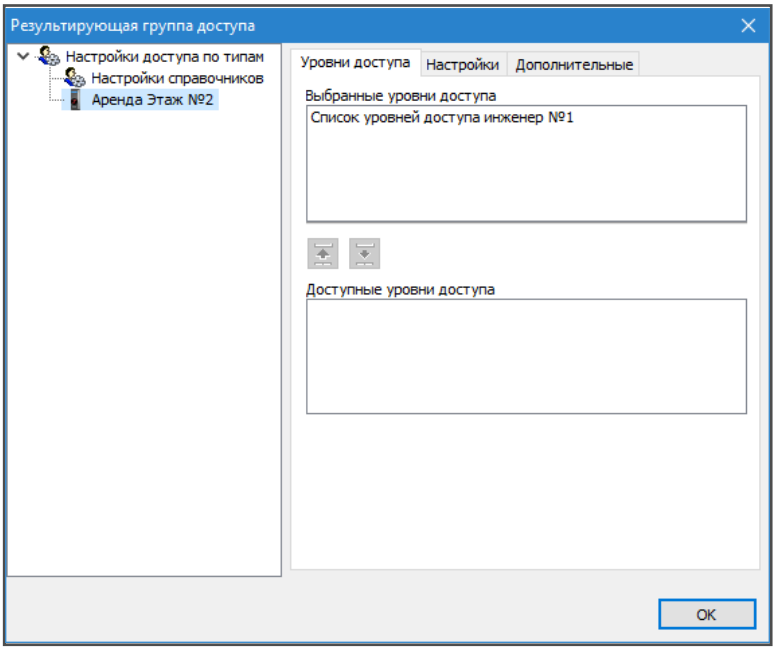


Рисунок Окно ***Результирующая группа доступа***

3.4.4 Закладка «Эксперт»

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

- кнопка **Дополнительные настройки** — с помощью этой кнопки открывается диалоговое окно ***Дополнительные настройки идентификатора***. В этом окне можно указать следующие настройки (рекомендуется опытным пользователям):
  - **Код выдачи** — настройка не используется для контроллеров Suprema.
  - **Расширенные настройки карт** — настройка не используется для контроллеров Suprema.

- кнопка **Собственная группа доступа** — настройка зарезервирована.
- 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 закладке **«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.

3.5 Владелец карты

Владелец карты — логический объект системы, содержащий информацию о сотруднике. Работа с владельцами карт осуществляется в рамках приложения **«Картотека»**. Создать новые объекты данного типа можно на закладке **«Владельцы карт»** окна ***Картотека*** с помощью кнопки **Добавить** (подробнее о работе с объектом Владелец карты см. «Арс: Глава 6 Картотека 6.3 Работа с объектами»).

Все настройки объекта расположены на закладках **«Основные»**, **«Доступ»**, **«Эксперт»**, **«Выдачи»** и **«Работы»**. Закладка **«Эксперт»** позволяет задать собственные настройки доступа для конкретного владельца карты, эту закладку рекомендуется использовать только опытным операторам комплекса. При использовании оборудования Suprema так же указываются настройки на закладке **«Биоданные»**. При использовании оборудования СКД Suprema и СКД Suprema 2 необходимо задать соответствующие настройки на закладке **«СКД Suprema»**.

Закладка **«Основные»** предназначена для ввода информации о сотруднике (подробнее о работе с этой закладкой см. «Арс: Глава 6 Картотека 6.3.1.1 Добавление объекта Владелец карты»).

3.5.1 Закладка «Доступ»

На вкладке **«Доступ»** находятся следующие настройки:

- **Общие поля**
  - **Активность** — настройка определяет, активен ли владелец карты в системе. Если флажок снят, владелец карты не будет восприниматься считывателем.

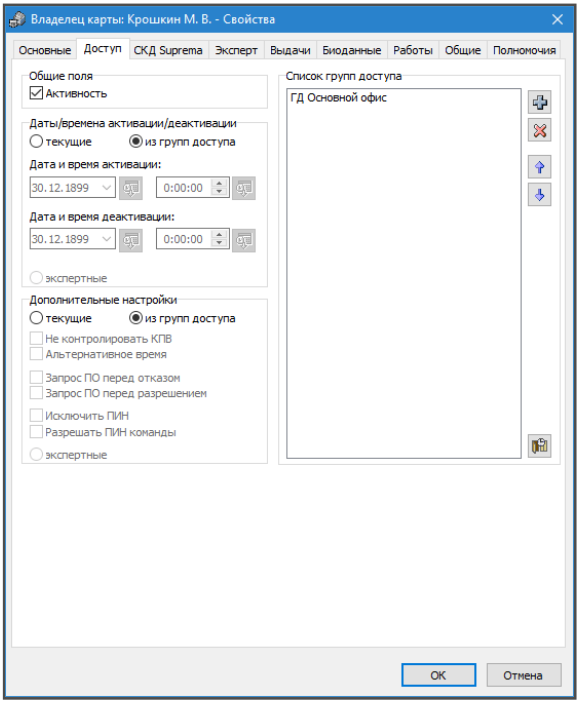


Рисунок Закладка **«Основные»** объекта *Владелец карты* при использовании полного набора оборудования и максимального стиля оформления «Картотеки»

- **Список групп доступа** — в этом поле с помощью кнопок **Добавить** и **Удалить** сформируйте список групп доступа, которые будут назначены этому владельцу карты.
  Если за одним идентификатором 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 прав доступа владельца карты.
  - Если выбран пункт **из групп доступа**, поля заблокированы и для данного владельца карты будут использоваться те настройки активации / деактивации, которые указаны в закрепленных за ним группах доступа.

- Чтобы использовать для владельца 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 карты (с этого момента карта будет распознаваться на считывателях).
  - **Дата и время деактивации** — дата и время окончания периода действия карты (с этого момента карта перестанет 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 настроек не используется для контроллеров Suprema.

3.5.2 Закладка «СКД Suprema»

На закладке **«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.
- **СКД Suprema**
  - 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, заданных на закладке **«Биометрия»**:
    - **Администратор** — флажок позволяет задать расширенные настройки для владельца карты. В этом случае сотрудник сможет сободно 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**.
    - **Уровень проверки отпечатков** — данная настройка задает вероятность предоставления доступа незарегистрированному пользователю. Например, если задана вероятность 1/1000 (**Самый низкий**), то в 1 случае из 1000 отпечаток незарегистрированного пользователя может быть принят за отпечаток, имеющийся в базе. Рекомендованное для выбора значение — 1/100000 (**Средний**).

- **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 (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.

- **СКД Suprema 2** – в этой группе параметров укажите настройки для контроллеров СКД Suprema 2.
  - 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, заданных на закладке **«Биометрия»** и **«Режимы»**:
  - **Уровень проверки отпечатков** – в этом поле выберите уровень распознавания отпечатка пальца на устройстве: **Средний, Выше среднего, Высокий**. Чем выше выбранный уровень надежности, тем тщательнее будет проверяться отпечаток и тем ниже вероятность предоставления доступа незарегистрированному пользователю.
  - **Режим аутентификации** — в этой группе параметров укажите режим для доступа, который будет использоваться на контроллере.
  - **Эксперт** — настройка зарезервирована для использования в будущем.

3.5.3 Закладка «Эксперт»

На закладке **«Эксперт»** находятся следующие настройки:

- кнопка **Дополнительные настройки** — настройка заблокирована. Для владельца карты данная настройка не используется.
- кнопка **Собственная группа доступа** — с помощью этой открывается диалоговое окно ***Собственные настройки доступа***, где можно изменить настройки групп доступа, закрепленные за владельцем карты

(рекомендуется опытным пользователям). Работа с этим окном аналогична работе с окном редактирования свойств объекта *Группа доступа* (см. п. «3.1 Группа доступа»).

- кнопка **Очистить** — кнопка позволяет очистить собственные настройки доступа для данного владельца карты. После этого для владельца карты будут использоваться настройки тех групп доступа, которые указаны в поле **Список групп доступа** на закладке **«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.

3.5.4 Закладка «Выдачи»

На закладке **«Выдачи»** находится информация об идентификаторах, выданных этому сотруднику (о работе с этой закладкой см. «Apc: Глава 6 Картотека 6.4 Выдача идентификатора»).

3.5.5 Закладка «Биоданные»

На закладке **«Биоданные»** требуется указать следующие группы параметров:

- **Уровень надежности 1:1** — зарезервировано.
- При нажатии на кнопку **Добавить** откроется окно ***Сканирование пальца***.

В окне ***Сканирование пальца*** укажите следующие настройки:

- В поле **Найденные сканеры** укажите сканер, с помощью которого будет осуществляться сканирование – BioMini или другой из добавленных в конфигурацию контроллеров. С помощью кнопки **Обновить** можно обновить список доступных сканеров.
- При сканировании отпечатка с помощью сканера BioMini изображение отпечатка будет отображаться в области **Рисунок**.
- **Мин. Качество** – в этом поле укажите качество отпечатка от 0 до 100. Данное абстрактное значение задает минимальное количество уникальных особенностей отдельного отпечатка, совокупность которых является достаточной для однозначной идентификации человека. Занесение отпечатков следует осуществлять с максимально возможным качеством, однако, в силу физиологических особенностей, значение 100 практически недостижимо для большинства людей. Рекомендуемое значение, обеспечивающее возможность занесения любого отпечатка с необходимым набором отличительных черт для однозначной идентификации, равно 60.

  Каждый отпечаток сканируется дважды:
  - **Качество 1** — качество первого отпечатка,
  - **Качество 2** — качество второго отпечатка.

Обратите внимание: данная настройка доступна только для устройства BioMini.

- В группе параметров **Левая рука** и **Правая рука** выберите палец, который был использован для сканирования отпечатка.
- При нажатии на кнопку **Сканировать**, в строке **Состояние** будет последовательно отображаться информация о действиях, которые необходимо выполнить для сканирования отпечатка.
- При помощи кнопки **Стоп** можно прервать сканирование.
- В поле **Описание** укажите необходимую информацию о сканировании.

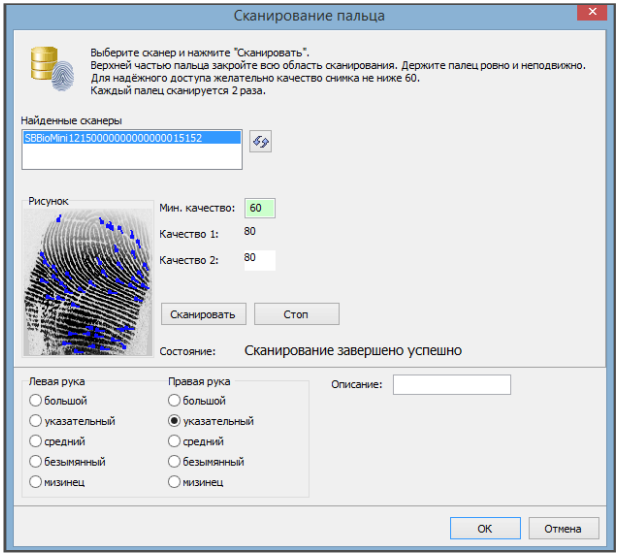


Рисунок Окно ***Сканирование пальца***

По завершению сканирования, информация о владельце появится в таблице на закладке **«Биоданные»**:

- **№** — в этой колонке отображается порядковый номер данных, записанных в таблицу.
- **Тип шаблона** — в этой колонке отображается информация о типе биометрических данных. Например, *Палец Suprema*.
- **Дата создания** — в этой колонке отображается дата и время внесения отпечатка в базу данных.
- **№ пальца** — в этой колонке отображается информация о том, какой палец был использован при сканировании. Например, запись *Левый большой* говорит о том, что для сканирования был использован большой палец левой руки.
- **Размер, байт** — в этой колонке отображается размер изображения отпечатка в байтах.
- **Качество** — в этой колонке отображается полученное при сканировании качество отпечатков.
- **Описание** — в этой колонке отображается информация, которая была

указана в поле **Описание** окна ***Сканирование пальца***.
С помощью кнопок **Редактировать** и **Удалить** можно изменить информацию о владельце или удалить ее, соответственно.

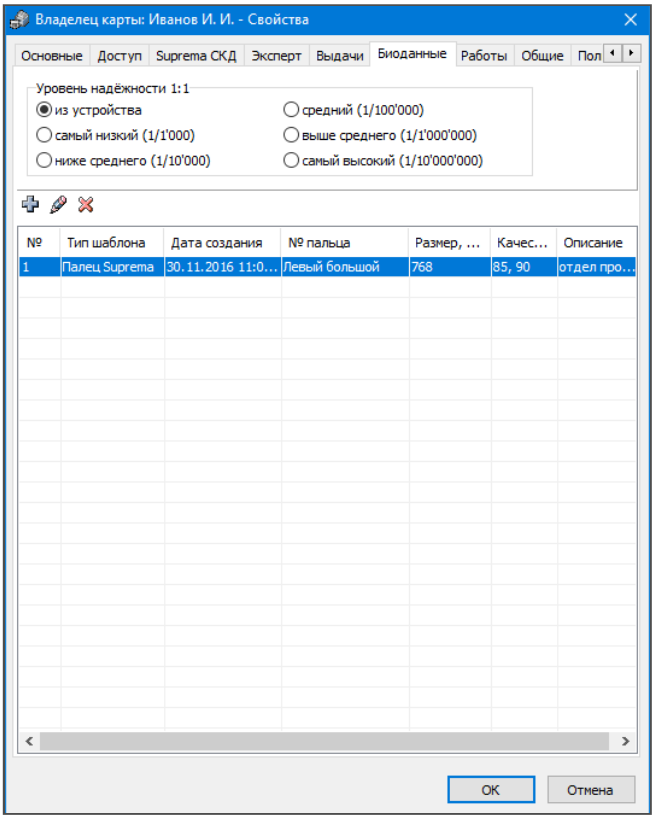


Рисунок Закладка **«Биоданные»** объекта *Владелец карты*

3.5.6 Закладка «Работы»

На закладке **«Работы»** можно закрепить за владельцем карты объект типа *Работа*, который будет использоваться при составлении отчетов рабочего времени с учетом графиков в приложении «Учет рабочего времени» (см. «Арс: Глава 8 Учет рабочего времени»).