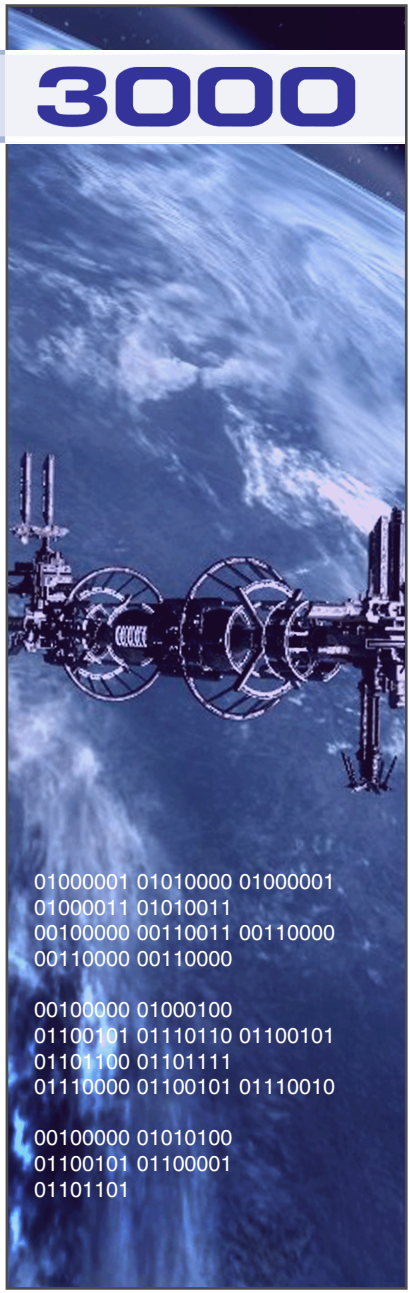
APACS 3000

Драйвер «Управление доступом»



Руководство пользователя

1 Введение **SeM-4**
1.1 Основные объекты драйвера «Управление доступом» SeM-4
1.1.1 Связь владельцев карт и идентификаторов SeM-4
1.1.2 Группа доступа SeM-5
1.2 Дополнительные настройки доступа SeM-8
1.3 Назначение прав доступа SeM-9
1.4 Связь драйвера и оборудования SeM-11
1.5 Диагностика идентификаторов SeM-12
2 Конфигурирование прав доступа **SeM-13**
3 Объекты драйвера «Управление доступом» **SeM-16**
3.1 Группа доступа SeM-16
3.1.1 Настройки драйверов в составе группы доступа SeM-17
3.1.2 Настройки контроллеров в составе группы доступа . . SeM-25
3.1.3 Команды объекта Группа доступа SeM-32
3.2 Расширенные настройки карт SeM-33
3.3 Режимы применения изменений при редактировании групп доступа и расширенных настроек карт SeM-34
3.4 Идентификатор SeM-39
3.4.1 Вкладка «Основные» SeM-39
3.4.2 Проверка идентификатора SeM-48
3.4.3 Просмотр настроек идентификатора SeM-52
3.4.4 Вкладка «Эксперт» SeM-53
3.5 Владелец карты SeM-54
3.5.1 Вкладка «Доступ» SeM-55
3.5.2 Вкладка «Suprema СКД» SeM-55
3.5.3 Вкладка «Эксперт» SeM-58
3.5.4 Вкладка «Выдачи» SeM-58
3.5.5 Вкладка «Биоданные» SeM-58
3.5.6 Вкладка «Работы» SeM-61
3.6 Перенос настроек доступа SeM-61

1 Введение

Драйвер «Управление доступом» ПК APACS 3000 позволяет конфигурировать и управлять правами доступа и привилегиями сотрудников на контролируемой территории.

Драйвер обладает следующими характерными особенностями:

- позволяет гибко назначать права доступа владельцам карт/идентификаторам 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 Apollo AAN–100/32,
- контроллеры Apollo AIM–4SL/2SL/1SL и APN–35,
- контроллеры VertX V1000, V2000 и EDGE.

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 владельцам карт/идентификаторам 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.

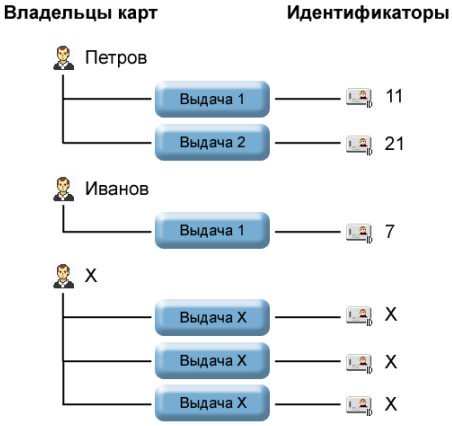


Рисунок Связь между владельцами карт и идентификаторами

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 набор 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 уровни доступа разных контроллеров,
- настройки точного доступа и список исключений считывателей контроллеров Apollo.

Например, на объекте есть два контроллера AAN-100: *AAN_№1* и *AAN_№2* и сконфигурирована *ГД Инженер*, в которую входят ссылки на оба контроллера и для каждого контроллера указаны ссылки на его локальные объекты *Уровень доступа инженер №1* и *Уровень доступа инженер №2*. Если какая-либо карта будет включена 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 карты/владельца карты сразу в несколько ГД. Данную возможность можно использовать для выделения на объекте определенных зон доступа, в которые будут впоследствии включены карты/владельцы карт.

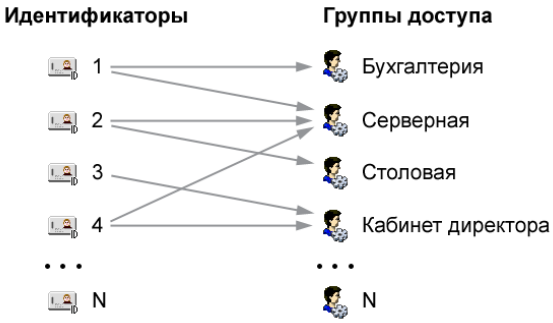


Рисунок Назначение сотрудникам нескольких различных групп доступа

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*.

Обратите внимание: для назначения нескольких ГД необходимо, чтобы используемые контроллеры поддерживали режимы, в которых разрешено суммирование настроек доступа. Например, использование 6 уровней доступа, использование 32 уровней доступа, использование точного доступа в Apollo и т.д. Подробнее см. п. «1.4 Связь драйвера и оборудования».

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. исключение из КПВ,
3. использование альтернативного времени при проходе,
4. запрос ПО перед отказом/разрешением доступа,
5. исключение/разрешение ПИН команд,
6. точный доступ и список исключений для контроллеров Apollo.

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 3000 предусмотрены два стиля оформления приложения «Картотека»: *максимальный* и *минимальный*.

Максимальный стиль предполагает, что все настройки доступа задаются в экземплярах карт/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 карты/владельца карты.

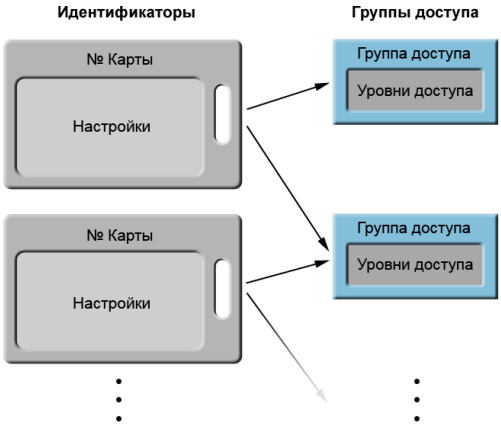


Рисунок Максимальный стиль оформления «Картотеки»

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).

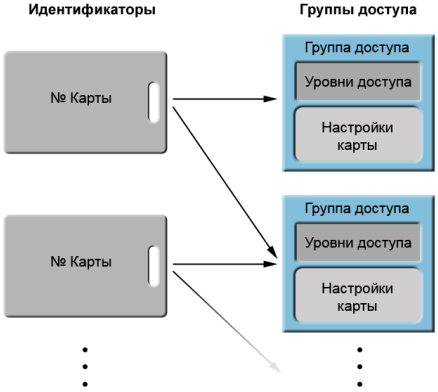


Рисунок Минимальный стиль оформления «Картотеки»

1.3 Назначение прав доступа

Начиная с ПК APACS 3000 v.6.3, в комплексе поддерживается два подхода к назначению прав доступа:

1. Права доступа задаются в настройках карты, после чего она выдается владельцу. При таком подходе карта будет являться «самостоятельной», то есть будет иметь доступ не зависимо от того, выдана она владельцу или нет.

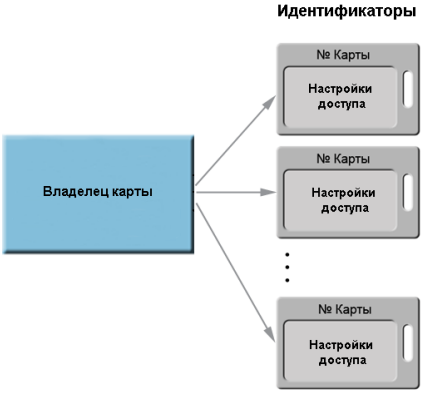


Рисунок Задание настроек доступа у идентификаторов

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: если настройки доступа заданы у владельца карты и ему назначена карта с собственными настройками доступа, то настройки доступа владельца для этой карты использоваться не будут.

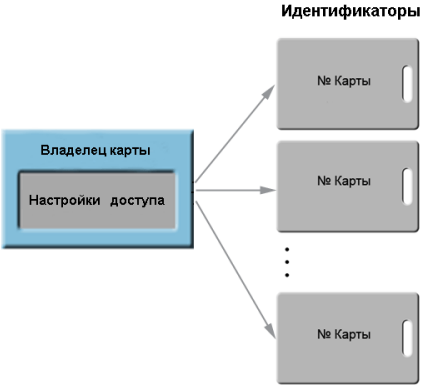


Рисунок Задание настроек доступа у владельца карты

Второй подход к хранению прав доступа предпочтительнее для большинства владельцев карт, поэтому рекомендуется перенести права доступа от карт к владельцам.

Рассмотрим подробнее процедуру переноса прав:

1. Выполните стандартную процедуру перехода на версию 6.3.
2. Проверьте работоспособность всех основных компонентов комплекса, используемых на вашем объекте. Создайте резервную копию базы данных.
3. Выберите несколько (желательно разнотипных) сотрудников и для них протестируйте процедуру переноса прав от карт к владельцам (подробнее см. п. «3.6 Перенос настроек доступа»). Убедитесь, что режимы и решения продолжают корректно работать для владельцев с измененной структурой хранения прав доступа. Создайте резервную копию базы данных.
4. Выберите всех сотрудников, для которых целесообразно использовать новый подход, и выполните процедуру переноса прав от карт к владельцам.
5. Еще раз убедитесь в работоспособности всех частей решения.

Обратите внимание: при переносе прав доступа от карт к владельцам, если у владельца было несколько карт, то результат такой операции будет неизвестен, т.к. у выданных карт могут быть разные настройки прав доступа. Поэтому перед запуском процедуры переноса рекомендуется вручную обработать таких владельцев и изменить права доступа в индивидуальном порядке.

Тип хранения настроек доступа, который будет использоваться, указывается при создании или выдаче идентификаторов. Чтобы каждый раз не указывать тип хранения настроек доступа, можно задать настройки в окне ***Настройки приложения Картотека***. Тогда идентификатор будет создаваться с указанными настройками по умолчанию.

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. 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.

Например, драйвер «Управление доступом» позволяет назначать несколько групп доступа для одного идентификатора, но контроллер APN–35 поддерживает работу карты, которой назначен только один уровень доступа.

Поэтому при конфигурировании объектов драйвера «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. Например, идентификатору назначены семь уровней доступа, а для контроллера AAN–100 включена настройка **Использовать 6 уровней доступа**.

В этом случае идентификатор загружается в контроллер с максимально возможными настройками. При этом:

- в случае списковых настроек (например, список уровней доступа) загружается максимально возможное число первых значений. То есть, если идентификатору назначены семь уровней доступа, а для контроллера AAN-100 включена настройка **Использовать 6 уровней доступа**, в контроллер будет загружены первые шесть уровней доступа данного идентификатора.
- если для идентификатора не заданы значения настроек, которые обязательно должны быть указаны и необходимы в работе контроллера, будет использоваться значение по умолчанию.

Обратите внимание: на контролируемом объекте рекомендуется использовать однотипные контроллеры, так как это значительно упрощает конфигурирование и эксплуатацию системы. Если же на объекте возникает необходимость добавить малый контроллер, то рекомендуется добавлять автономные контроллеры AIM–4SL/2SL/1SL к основным контроллерам AAN–100/32 и EDGE Host к V1000/V2000.

1.5 Диагностика идентификаторов

Драйвер «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.

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

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.

Например, контроллер Apollo APN–35 позволяет назначать только один уровень доступа для карты/владельца карты, контроллер AAN–100 — несколько уровней доступа на карту/владельца карты. Исходя из этих возможностей, необходимо решить, как будут назначены идентификаторам группы доступа: одна группа доступа на владельца карты/карту или несколько.

- 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 уровней доступа

В ПК APACS 3000 сконфигурируйте локальные уровни 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).

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:

- *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*.

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 идентификатора/владельца карты.

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

Создание групп доступа

Далее требуется определить, каким образом локальные уровни доступа будут перенесены на уровень программного комплекса и каким образом Вы будете конфигурировать группы доступа. Возможны следующие подходы:

- группы доступа соответствуют группам сотрудников, и одному идентификатору назначается только одна группа доступа,
- группы доступа соответствуют локальным уровням доступа, в течение которых разрешен доступа в эти зоны, и одному идентификатору назначается несколько групп доступа.

Рассмотрим это на примерах.

В первом случае нужно создать следующие объекты типа *Группа доступа (ГД)*:

- для уборщиц — *ГД «Уборщица»*, где указать уровни доступа *Основная зона «Уборка»*, *Доступ в серверную «Уборка»* и *Доступ в кабинет директора «Уборка»*,
- для сотрудников техотдела, которые имеют право доступа в основную рабочую зону и в серверную — *ГД «Техотдел»*, где указать уровни доступа *Основная зона* и *Доступ в серверную*,
- для директора, который имеет право доступа в основную рабочую зону и в свой кабинет — *ГД «Директор»*, где указать уровни доступа *Основная зона* и *Доступ в кабинет директора*,

- для всех остальных сотрудников — *ГД «Сотрудник»*, где указать уровень доступа *Основная зона*.

Таким образом, в идентификаторах, выданных уборщицам, указана *ГД «Уборщица»*, в идентификаторах сотрудников техотдела — *ГД «Техотдел»*, в идентификаторе директора — *ГД «Директор»*, в идентификаторах остальных сотрудников — *ГД «Сотрудник»*.

Во втором случае требуется создать по одному объекту типа *Группа доступа (ГД)* для каждого локального уровня доступа:

- *ГД Основная зона* соответствует уровню доступа *Основной зоне* (доступ всем сотрудникам в основную рабочую зону в течение *ВЗ Рабочий день*),
- *ГД Доступ в серверную* — *УД Доступ в серверную* (доступ в серверную для сотрудников технического отдела в течение *ВЗ Рабочий день*),
- *ГД Доступ в кабинет директора* — *УД Доступ в кабинет директора* (доступ для директора в течение *ВЗ Рабочий день*).
- *ГД Основная зона «Уборка»* — *УД Основной зоне «Уборка»* (доступ для уборщиц в основную рабочую зону в течение *ВЗ Уборка*),
- *ГД Доступ в серверную «Уборка»* — *УД Доступ в серверную «Уборка»* (доступ для уборщиц в серверную в течение *ВЗ Уборка*),
- *ГД Доступ в кабинет директора «Уборка»* — *УД Доступ в кабинет директора «Уборка»* (доступ для уборщиц в кабинет в течение *ВЗ Уборка*).

Исходя из этого идентификаторам требуется назначить:

- идентификаторам уборщиц требуется назначить следующие группы доступа: *ГД Основная зона «Уборка»*, *ГД Доступ в серверную «Уборка»* и *ГД Доступ в кабинет директора «Уборка»*,
- идентификаторам сотрудников техотдела — *ГД Основная зона* и *ГД Доступ в серверную*,
- идентификатору директора — *ГД Основная зона* и *ГД Доступ в кабинет директора*,
- идентификаторам всех остальных сотрудников — *ГД Основная зона*.

Второй подход конфигурирования групп доступа предполагает, что контроллер позволяет назначать несколько уровней доступа на одну карту/владельца карты.

Исходя из возможностей оборудования, выберите способ конфигурирования и создайте группы доступа.

Заполнение базы данных владельцев карт и идентификаторов

Для работы с базой данных владельцев карт и идентификаторов используется приложение «Картотека». В окне ***Картотека*** на вкладке **«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*.

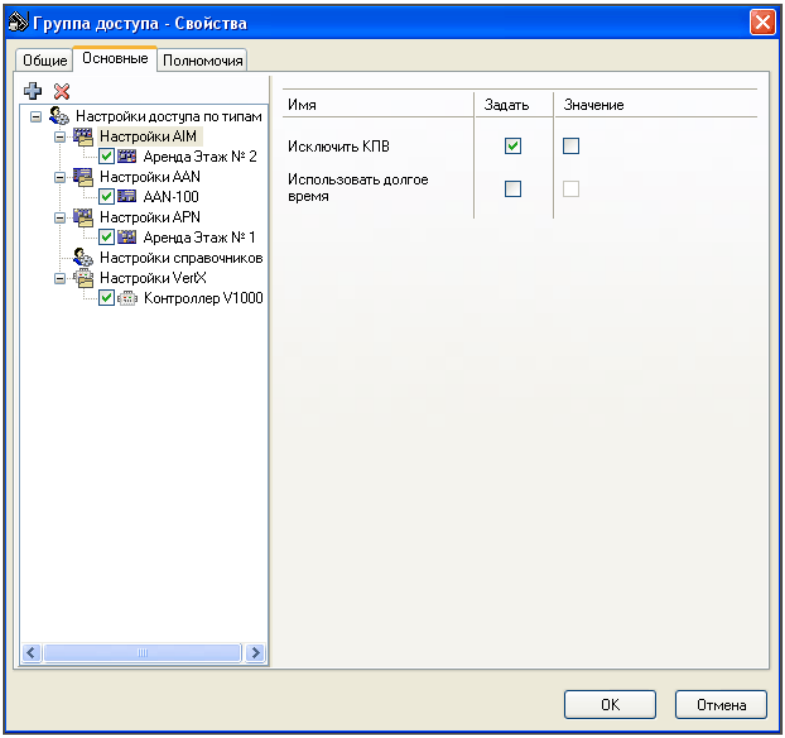


Рисунок Окно редактирования свойств объекта *Группа доступа*

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.

Далее рассмотрим настройки драйверов и настройки контроллеров разного типа.

Вкладка 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

Драйвера AIM и APN

Для драйверов **AIM** и **APN** в группе доступа используются следующие настройки:

- **Исключить КПВ** – настройка определяет, требуется ли хранить информацию о расположении сотрудника в зонах КПВ.
- **Альтернативное время** – настройка определяет, требуется ли для сотрудника использовать увеличенное время открытия и закрытия двери при проходе.

Драйвер AAN

Для драйверов **AAN** в группе доступа используются следующие настройки:

- **Альтернативное время** – настройка определяет, требуется ли для сотрудника использовать увеличенное время открытия и закрытия двери при проходе.

- **Исключить КПВ** – настройка определяет, требуется ли хранить информацию о расположении сотрудника в зонах КПВ.
- **Дата активации** – настройка определяет дату начала периода действия выданной карты (то есть, период распознавания карты на считывателе).
- **Время активации** – настройка определяет время начала периода действия выданной карты (то есть, период распознавания карты на считывателе).
- **Дата деактивации** – настройка определяет дату окончания периода действия выданной карты.
- **Время деактивации** – настройка определяет время окончания периода действия выданной карты (то есть, период распознавания карты на считывателе).

Обратите внимание: дата и время активации / деактивации выданной карты определяется настройкой основного контроллера Apollo **Использовать время активации / деактивации** (см. «Apl: Глава 2 Объекты основных контроллеров 2.4 Основной контроллер»):

- Если выбрана настройка **Только в дни активации / деактивации**, выданная карта действует начиная с даты и времени начала и заканчивая датой и временем окончания действия карты. Например, карта действует с 8:00 10 января по 20:00 10 февраля.
- Если выбрана настройка **Каждый день**, выданная карта действует ежедневно в течение определенного времени, начиная с даты начала до заканчивая датой окончания. Например, карта действует ежедневно с 8:00 до 20:00 с 10 января по 10 февраля.

При этом обратите внимание на то, что данная настройка дополняет существующие права доступа в системе.

- **Запрос ПО перед проходом** – настройка определяет, требуется ли дополнительно посылать на компьютер дежурного оператора запрос о допуске владельца карты, несмотря на то, что контроллером уже принято решение о допуске.
- **Запрос ПО перед отказом** – настройка определяет, требуется ли дополнительно посылать на компьютер дежурного оператора запрос о запрещении допуска владельца карты, несмотря на то, что контроллером уже принято решение о запрете.

  С помощью настроек **Запрос ПО перед проходом/отказом** можно организовать режим запроса на компьютер, при котором решение о доступе принимает дежурный оператор (см. «Apl: Глава 5 Режимы оборудования Apollo»).

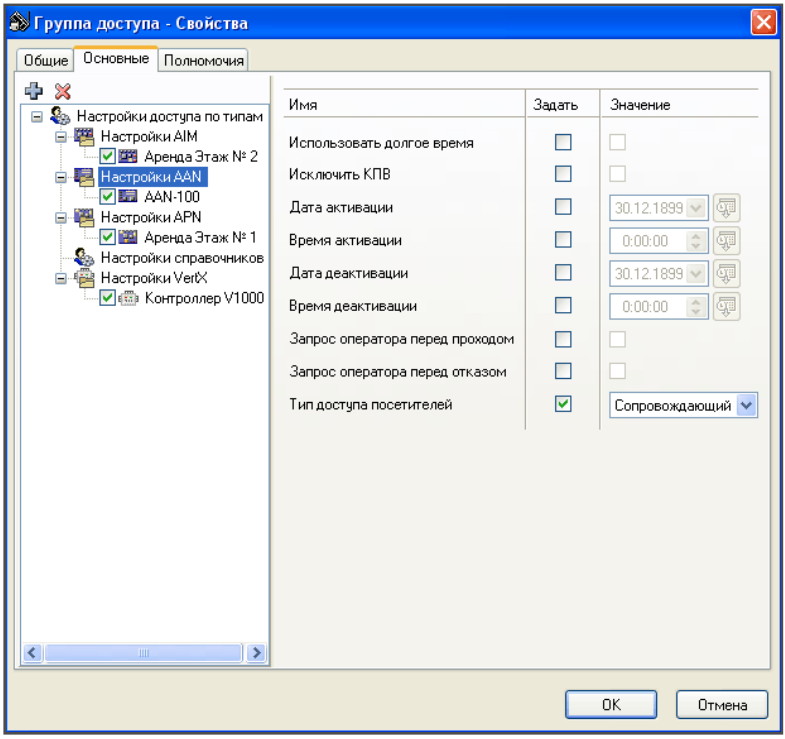


Рисунок Настройки драйвера AAN в окне редактирования свойств объекта *Группа доступа*

- **Тип карты** – настройка определяет тип выданного идентификатора:
  - *Сотрудник* — обычный идентификатор сотрудника. Доступ по такому идентификатору выдается в соответствии с настройками уровней доступа в системе.
    Следующие типы идентификаторов используются для организации режима сопровождения посетителей (см. п. «Apl: Глава 5 Режимы оборудования Apollo 5.2 Режим сопровождения посетителей»):
  - *Посетитель без сопровождения* — идентификатор аналогичен обычному идентификатору сотрудника. Такой идентификатор может быть выдан людям, которые часто посещают предприятие и могут передвигаться по территории без сопровождения, но не являются сотрудниками.
  - *Сопровождающий* — сотрудник с данным идентификатором имеет право проводить посетителей. Доступ по идентификатору сопровождающего выдается аналогично обычному идентификатору сотрудника.

- *Посетитель с сопровождением* — доступ по данному идентификатору может быть получен только после подтверждения идентификатором сопровождающего.

Обратите внимание: если выбран тип карты *сопровождающий* или *посетитель*, далее в настройках каждого контроллера, включенного в группу доступа, требуется указать: для посетителя – группу посетителей, для сопровождающего — список групп посетителей.

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 VertX

Для драйвера **VertX** используются следующие настройки:

- **Исключить КПВ** – настройка определяет, требуется ли хранить информацию о расположении сотрудника в зонах КПВ.
- **Альтернативное время** – настройка определяет, требуется ли для сотрудника использовать увеличенное время открытия и закрытия двери при проходе.
- **Дата / время активации** – настройка определяет дату и время начала активации выданной карты (то есть, с какого момента карта будет распознаваться на считывателях).
- **Дата / время деактивации** – настройка определяет дату и время окончания активации выданной карты (то есть, с какого момента карта перестанет распознаваться на считывателях).
- **Исключить ПИН** – настройка определяет, требуется ли владельцу карты вводить ПИН–код в режиме считывателя *Карта и ПИН*.
- **Разрешать ПИН команды** – настройка определяет, может ли владелец данной карты управлять реле защелки с помощью команд, набранных на клавиатуре считывателя.

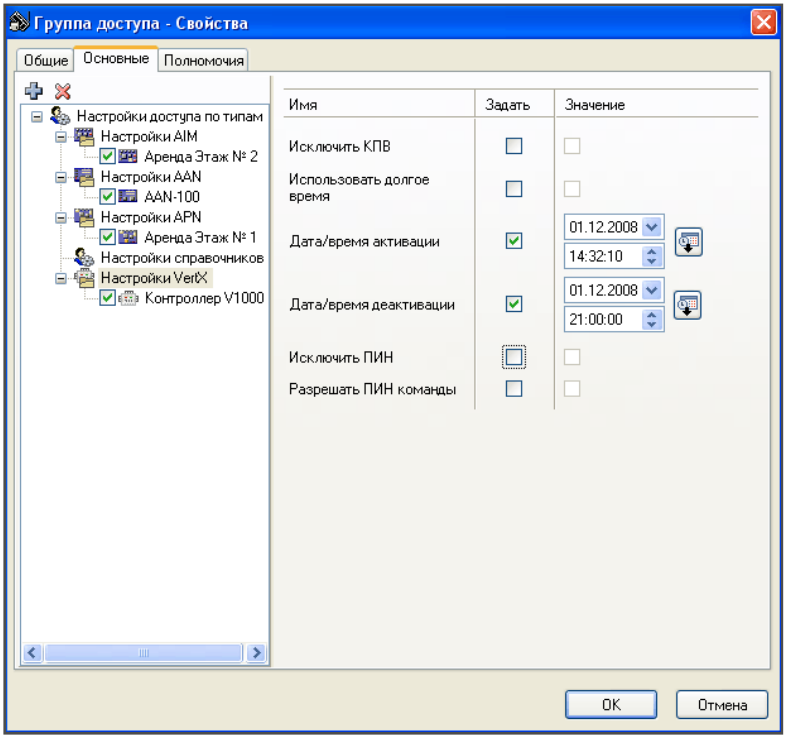


Рисунок Настройки драйвера VertX в окне редактирования свойств объекта *Группа доступа*

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).

- **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.

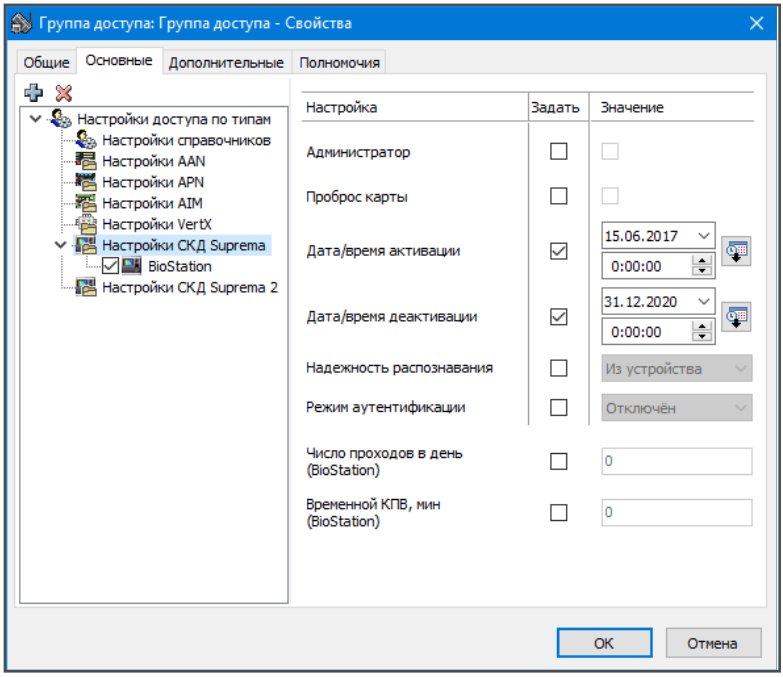


Рисунок Настройки драйвера СКД Suprema в окне редактирования свойств объекта *Группа доступа*

Драйвер СКД Suprema 2

Для драйверов **СКД Suprema 2** 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 отпечатку** — настройка позволяет задать режим для идентификации данного пользователя на устройстве с помощью отпечатка: *Отпечаток*, *Отпечаток и Пин*, *Запрещен*, *Из устройства*.
- **Аутентификация по карте** — настройка позволяет задать режим для верификации данного пользователя на устройстве с помощью карты:

Карта, *Карта и отпечаток*, *Карта и ПИН*, *Карта и отпечаток или ПИН*, *Карта, отпечаток и ПИН*, *Запрещен*, *Из устройства*.

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

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.

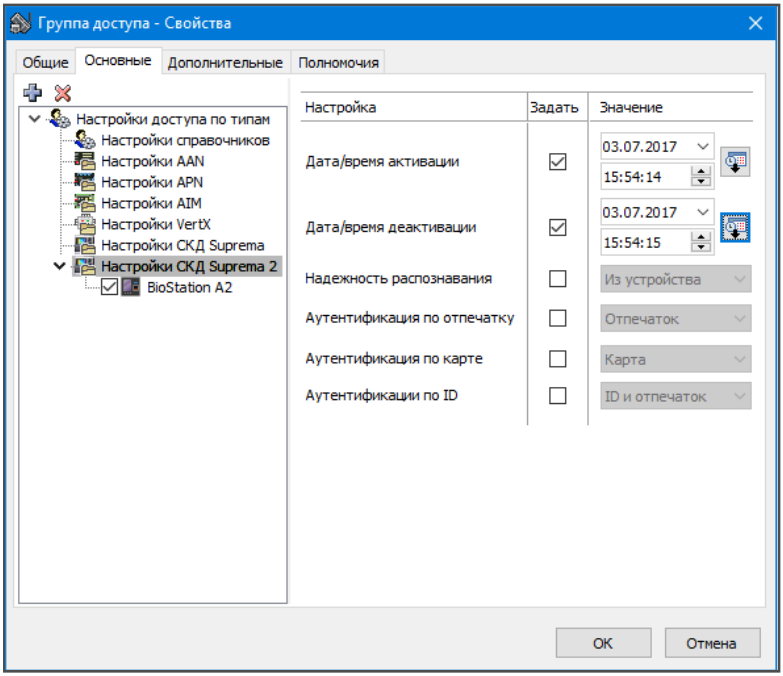


Рисунок Настройки драйвера СКД Suprema 2 в окне редактирования свойств объекта *Группа доступа*

3.1.2 Настройки контроллеров в составе группы доступа

Контроллер AIM–4SL/1SL/2SL

В случае работы с контроллером AIM–4SL/1SL/2SL для группы доступа используются настройки, расположенные на вкладках **«Уровни доступа»**, **«Точный доступ»** и **«Настройки»**. Вкладку **«Настройки»** рекомендуется использовать в том случае, если Вы хотите задать для контроллера собственные настройки, которые отличаются от настроек, заданных для всего драйвера в целом.

На вкладке **«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**.

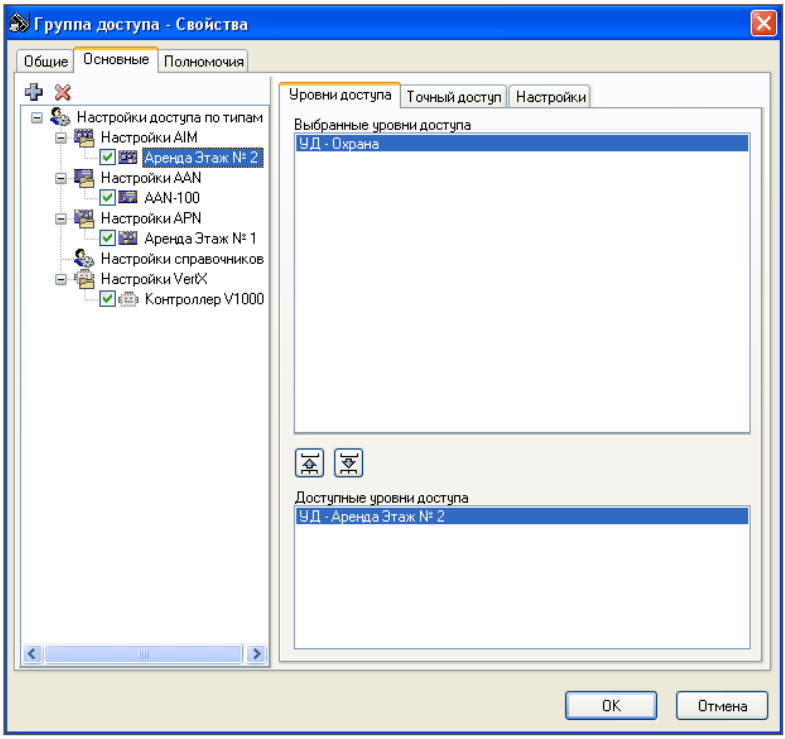


Рисунок Вкладка **«Уровни доступа»** драйвера AIM в окне редактирования свойств объекта *Группа доступа*

На вкладке **«Точный доступ»** можно указать доступ в определенные помещения в течение указанного времени и, таким образом, расширить права доступа.

Для этого нужно указать, через какие считыватели и в течение какой временной зоны может проходить сотрудник. В поле **Считыватели** выделите

считыватель, в поле **Временные зоны** — временную зону, которую хотите закрепить за этим считывателем, и нажмите кнопку **Добавить** — считыватель и временная зона будут перенесены в поле **Точный доступ**.

Обратите внимание: чтобы использовать функцию Точный доступ, в настройках контроллера AIM–4SL/1SL/2SL требуется поставить флажок **Использовать точный доступ**.

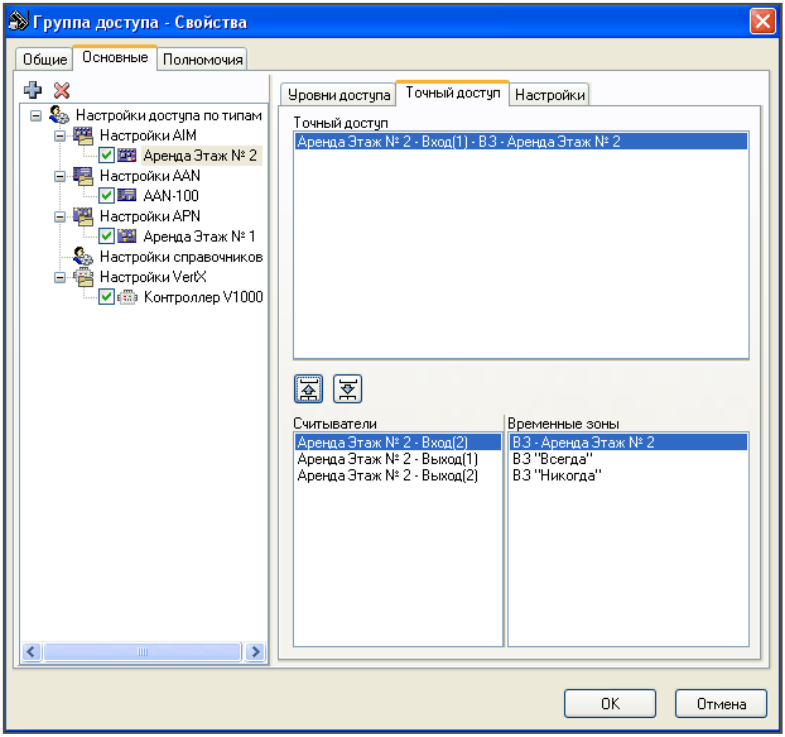


Рисунок Вкладка **«Точный доступ»** драйвера AIM в окне редактирования свойств объекта *Группа доступа*

Контроллер AAN–100/32

В случае работы с контроллером AAN–100/32 для группы доступа используются настройки, расположенные на вкладках **«Уровни доступа»**, **«Точный доступ»**, **«Список исключений»** и **«Настройки»**. Вкладку ««**Настройки**«» рекомендуется использовать в том случае, если Вы хотите задать для контроллера собственные настройки, которые отличаются от настроек, заданных для всего драйвера в целом.

На вкладке **«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**.

Далее находятся настройки, с помощью которых можно организовать режим сопровождения посетителей (см. п. «Apl: Глава 5 Режимы оборудования Apollo 5.2 Режим сопровождения посетителей»).

- **Тип карты** — в этом поле можно переопределить настройку, заданную для драйвера контроллеров AAN–100/32 (не рекомендуется). Для этого поставьте флажок **Задать** и выберите тип карты в поле **Значение**.
  - *Сотрудник* — обычный идентификатор сотрудника. Доступ по такому идентификатору выдается в соответствии с настройками уровней доступа в системе.
    Следующие типы идентификаторов используются для организации режима сопровождения посетителей (см. п. «Apl: Глава 5 Режимы оборудования Apollo 5.2 Режим сопровождения посетителей»):
  - *Посетитель без сопровождения* — идентификатор аналогичен обычному идентификатору сотрудника. Такой идентификатор может быть выдан людям, которые часто посещают предприятие и могут передвигаться по территории без сопровождения, но не являются сотрудниками.
  - *Сопровождающий* — сотрудник с данным идентификатором имеет право проводить посетителей. Доступ по идентификатору сопровождающего выдается аналогично обычному идентификатору сотрудника.
  - *Посетитель с сопровождением* — доступ по данному идентификатору может быть получен только после подтверждения идентификатором сопровождающего.
- **Группа посетителей** — настройка позволяет ограничить возможности сопровождающего проводить посетителей. Если для посетителя указана группа, значит, он может проходить только с сопровождающим этой группы. Чтобы использовать настройку, поставьте флажок **Задать** и укажите группу посетителей в поле **Значение**.
  Например, посетители могут быть разделены на группы *Клиенты*, *Комиссия*, *Семинаристы*.

Обратите внимание: если посетитель не включен в группу посетителей, то такой посетитель может проходить с любым сопровождающим.

- **Список групп посетителей** — настройка позволяет ограничить возможности сопровождающего проводить посетителей, указав список групп посетителей, которых может проводить один сопровождающий. Например, один человек сопровождает группу посетителей аудиторской проверки, другой — группу клиентов, третий — и клиентов, и аудиторов.

Обратите внимание: если для сопровождающего не указан список групп посетителей, которые он может проводить, то такой сопровождающий может проводить любого посетителя из любой группы.

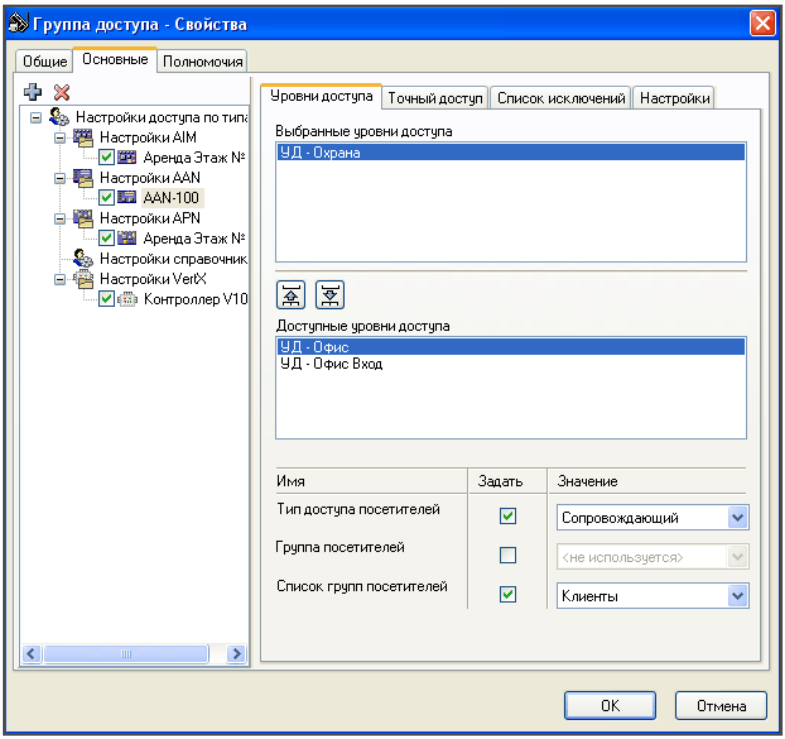


Рисунок Вкладка **«Уровни доступа»** драйвера AAN в окне редактирования свойств объекта *Группа доступа*

На вкладке **«Точный доступ»** можно указать доступ в определенные помещения в течение указанного времени и, таким образом, расширить права доступа.

Для этого нужно указать, через какие считыватели и в течение какой временной зоны может проходить сотрудник. В поле **Считыватели** выделите считыватель, в поле **Временные зоны** — временную зону, которую хотите закрепить за этим считывателем, и нажмите кнопку **Добавить** — считыватель и временная зона будут перенесены в поле **Точный доступ**.

Обратите внимание: чтобы использовать функцию Точный доступ, в настройках контроллера AAN–100/32 требуется поставить флажок **Точный доступ**.

На вкладке **«Список исключений»** можно ограничить перемещение сотрудника в пределах уровней доступа, указав те считыватели, через которые ему будет запрещен проход.

Для этого выделите считыватели в поле **Доступные считыватели** и кнопкой **Добавить** перенесите их в поле **Выбранные считыватели**.

Обратите внимание: чтобы использовать функцию Список исключений, в настройках контроллера AAN–100/32 требуется поставить флажок **Список исключений**.

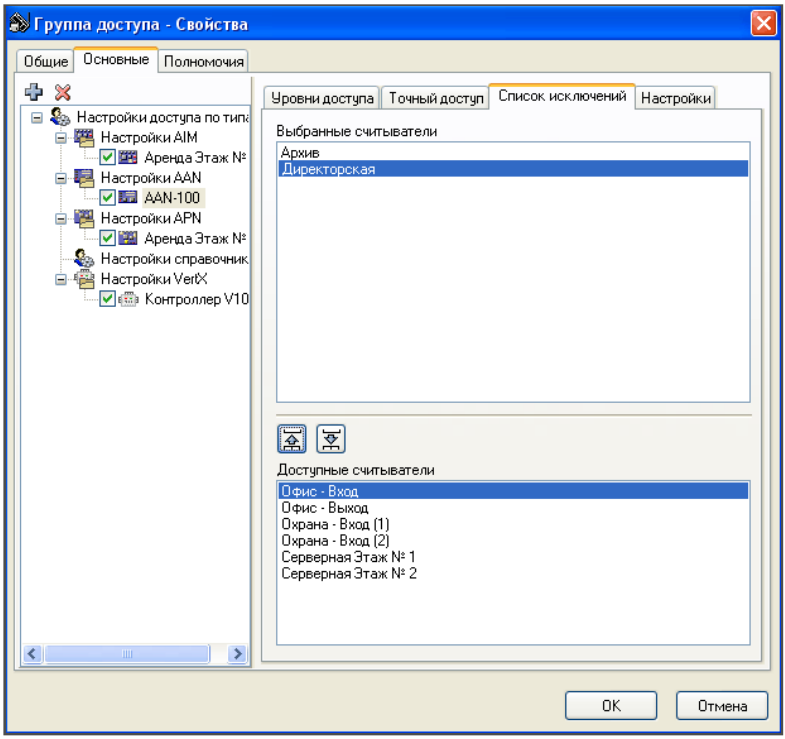


Рисунок Вкладка **«Список исключений»** драйвера AAN в окне редактирования свойств объекта *Группа доступа*

Контроллер APN–35

В случае работы с контроллером APN–35 для группы доступа используются настройки, расположенные на вкладках **«Уровни доступа»** и **«Настройки»**. Вкладку **«Настройки»** рекомендуется использовать в том случае,

если Вы хотите задать для контроллера собственные настройки, которые отличаются от настроек, заданных для всего драйвера в целом.

На вкладке **«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**.

Контроллер VertX

В случае работы с контроллером VertX для группы доступа используются настройки, расположенные на вкладках **«Уровни доступа»** и **«Настройки»**. Вкладку **«Настройки»** рекомендуется использовать в том случае, если Вы хотите задать для контроллера собственные настройки, которые отличаются от настроек, заданных для всего драйвера в целом.

На вкладке **«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**.

- **Группа лифтовых реле, если ВЗ активна** — если хотите указать группу лифтовых реле, которые будут доступны пользователю во время активности назначенной ему временной зоны, поставьте флажок **Задать** и выберите группу реле в поле **Значение**.
- **Группа лифтовых реле, если ВЗ неактивна** — если хотите указать группу лифтовых реле, которые будут доступны пользователю во время неактивности назначенной ему временной зоны, поставьте флажок **Задать** и выберите группу реле в поле **Значение**.

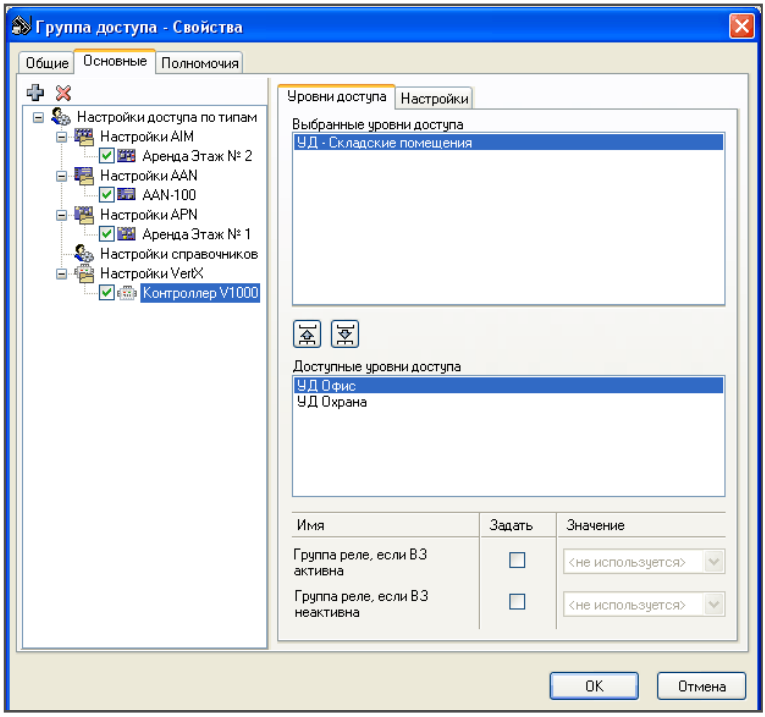


Рисунок Вкладка **«Уровни доступа»** драйвера VertX в окне редактирования свойств объекта *Группа доступа*

Контроллеры СКД Suprema

В случае работы с контроллерами Suprema СКД для группы доступа используются настройки, расположенные на вкладках **«Уровни доступа»**, **«Настройки»** и **«Дополнительные»**. Вкладки **«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 вкладке **«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**.

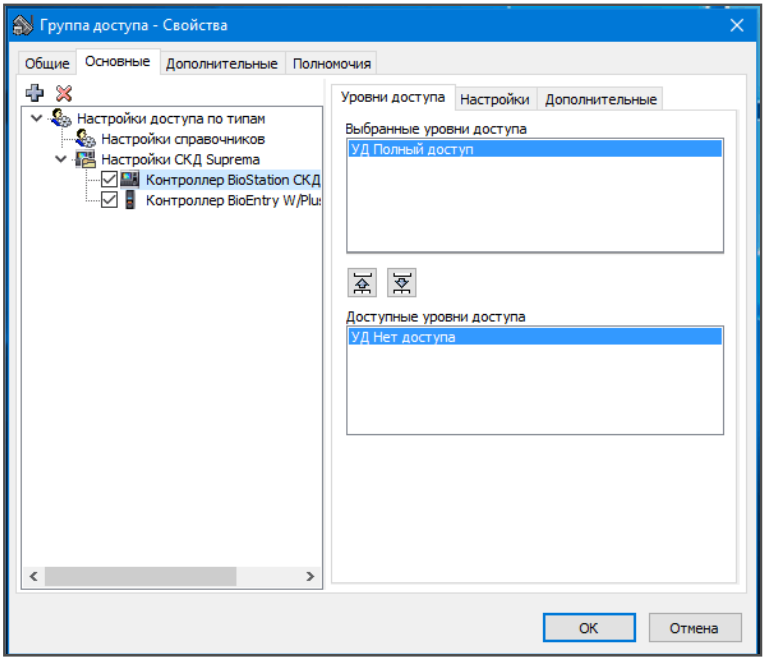


Рисунок Вкладка **«Уровни доступа»** драйвера СКД Suprema в окне редактирования свойств объекта *Группа доступа*

Контроллеры СКД Suprema 2

В случае работы с контроллерами Suprema СКД для группы доступа используются настройки, расположенные на вкладках **«Уровни доступа»**, **«Настройки»** и **«Дополнительные»**. Вкладки **«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 вкладке **«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**.

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.

3.2 Расширенные настройки карт

Расширенные настройки карт — логический объект, позволяющий указать, каким образом должны идентифицироваться карты на считывателях VertX. В одном объекте типа *Расширенные настройки карт* можно указать по одному шаблону карты VertX для каждого контроллера.

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

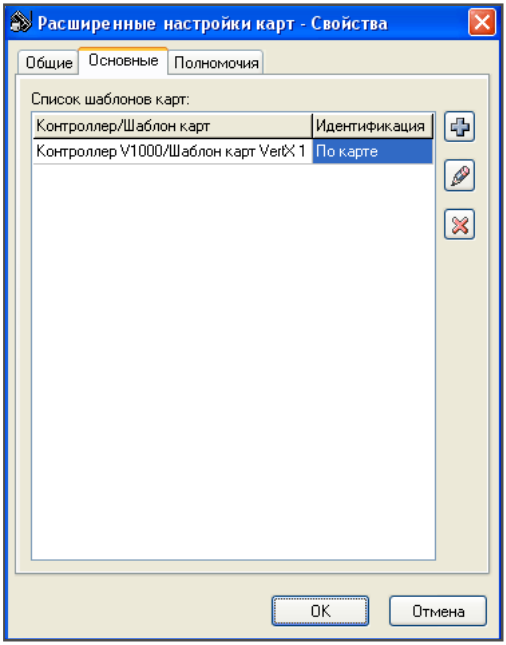


Рисунок Окно редактирования свойств объекта *Расширенные настройки карт*

На вкладке **«Основные»** окна редактирования свойств объекта находится таблица **Список шаблонов карт**. В эту таблицу требуется включить по одному объекту типа *Шаблон карты VertX* для каждого используемого в системе контроллера VertX и в поле **Идентификация** указать, каким образом карты должны идентифицироваться на считывателях VertX:

- *по карте* — карта будет идентифицирована на считывателе, если на считывателе указан режим *Только карта* или режим *Карта и ПИН*,
- *по карте или по ПИНу* — карта будет идентифицирована при любом режиме считывателя (в том числе при режимах *Только карта* и *Только ПИН*). При этом на входе должен быть предъявлен идентификатор, соответствующий режиму считывателя.

Например, если в качестве режима считывателя указан режим *Карта и ПИН*, то для прохода требуется считать карту и набрать ПИН-код на клавиатуре считывателя.

- *по ПИНу* — карта будет идентифицирована на считывателе, если на считывателе указан режим *Только ПИН*.

Обратите внимание: для идентификации карт *по карте или ПИНу* или *по ПИНу*, необходимо для каждой из этих карт указывать уникальный ПИН-код.

3.3 Режимы применения изменений при редактировании групп доступа и расширенных настроек карт

При редактировании объектов типа *Группа доступа* и *Расширенные настройки карт* в конфигурации системы происходит следующее:

- изменения объектов сохраняются на сервере APACS 3000,
- происходит поиск всех идентификаторов, которым назначены эти группы доступа и за которыми закреплены эти объекты типа *Расширенные настройки карт*,
- изменение найденных идентификаторов,
- загрузка 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 3000 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 3000, 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 3000 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 3000 и загружаются в контроллеры.
- **Сохранять изменения, но не загружать карты в контроллер** — в этом режиме изменения сразу же сохраняются на сервер APACS 3000, но не загружаются в контроллеры. Чтобы загрузить изменения, для каждого контроллера выполните команду ***Загрузить карты***.

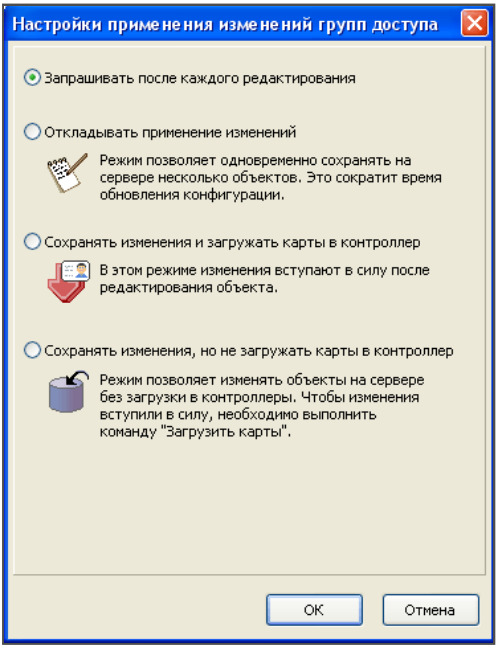


Рисунок Окно ***Настройки применения изменений групп доступа***

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**.

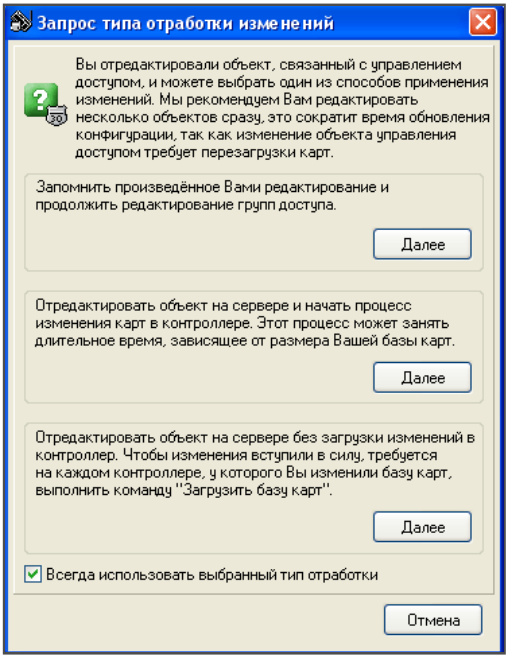


Рисунок Окно ***Выберите тип отработки изменений***

Если выбран режим отложенных изменений, после каждого редактирования объектов типа *Группа доступа* и *Расширенные настройки карт* 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***.

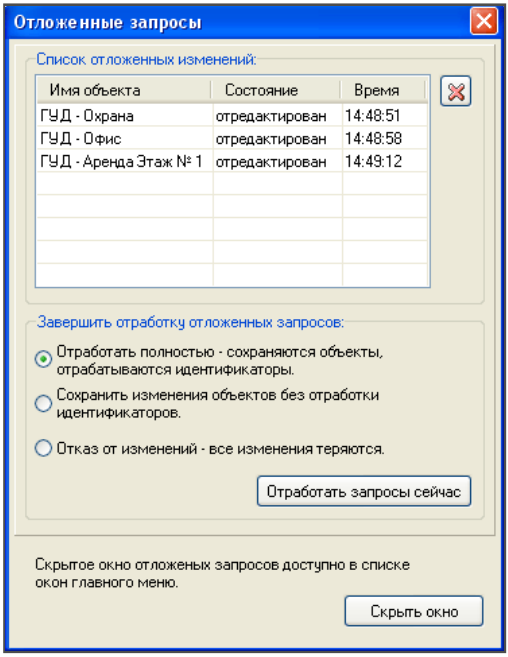


Рисунок Окно ***Отложенные запросы***

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 3000 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 3000, 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 вкладке **«Идентификаторы»** окна ***Картотека*** с помощью кнопки **Добавить**.

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

3.4.1 Вкладка «Основные»

В зависимости от выбранного подхода к хранению прав доступа, настройки на вкладке **«Основные»** будут различны.

Если права доступа задаются 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 ***Ошибки, найденные при проверке идентификатора***. Если ошибок нет, сообщение об этом появится в диалоговом окне ***Информация*** (подробнее см. п. «3.4.2 Проверка идентификатора»).
  - 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»).

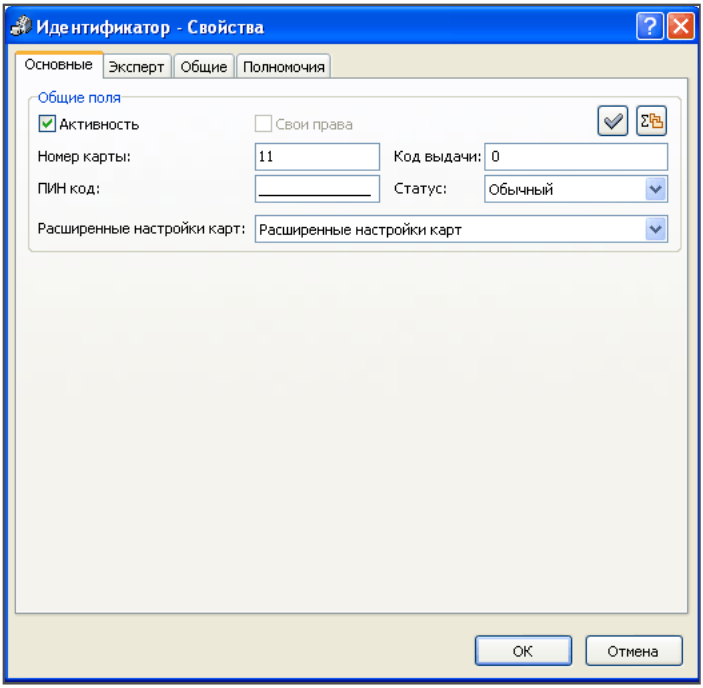


Рисунок Вкладка «**Основные**« объекта *Идентификатор* при условии, что права доступа задаются у владельца карты

- **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 VertX. Настройка используется только для контроллеров VertX.

Если для карты заданы собственные права доступа, то в зависимости от выбранного стиля оформления приложения «Картотека» и установленного оборудования вкладка **«Основные»** имеет разный интерфейс. Далее рассмотрим настройки, которые будут находиться на вкладке **«Основные»**.

Максимальный стиль оформления

Максимальный стиль оформления предполагает, что из приложения «Картотека» можно настраивать права доступа сотрудников и редактировать настройки групп доступа, закрепленные за идентификатором. Поэтому в идентификаторах находится максимальное количество настроек. Рассмотрим эти настройки:

- **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*).
  - кнопка **Проверить идентификатор** — нажмите на эту кнопку, чтобы проверить сконфигурированный идентификатор до его загрузки в контроллеры. Если в процессе проверке идентификатора будут найдены ошибки, откроется диалоговое окно ***Ошибки, найденные при проверке идентификатора***. Если ошибок нет, сообщение об этом появится в диалоговом окне ***Информация*** (подробнее см. п. «3.4.2 Проверка идентификатора»).
  - 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. «Арс: Глава 6 Картотека 6.5 Клиентский модуль USB считыватель карт Parsec»).
  - **ПИН–код** — укажите персональный идентификационный номер, который владелец данного идентификатора будет вводить на клавиатуре считывателя в режиме *Карта и ПИН* или *Карта или ПИН*.
  - **Статус** — укажите текущий статус идентификатора: обычный, утерян, уничтожен или изъят.
  - **Шаблон** — выберите шаблон идентификатора. При смене шаблона Вам будет предложено применить настройки шаблона к идентификатору.
  - кнопка **Применять настройки шаблона идентификатора** — нажмите на эту кнопку, если хотите изменить настройки идентификатора в соответствии с выбранным шаблоном.

- **Расширенные настройки карт** — укажите объект типа *Расширенные настройки карт*, в котором указано, каким образом данная карта должна идентифицироваться на считывателях VertX. Настройка используется только для контроллеров VertX.
- **Макет для печати** — укажите макет, который будет использоваться при печати идентификатора.
- кнопка **Предварительный просмотр** — позволяет посмотреть макет в окне ***Просмотр макетов карт*** (см. «Арс: Глава 9 Редактор макетов карт»).
- кнопка **Печать** — позволяет распечатать карту.

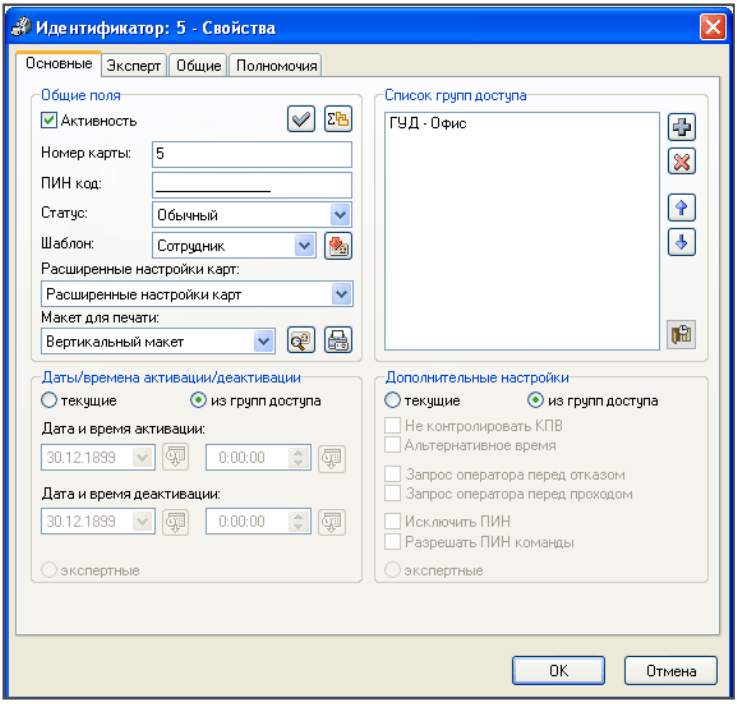


Рисунок Вкладка **«Основные»** объекта *Идентификатор* при использовании полного набора оборудования и максимального стиля оформления «Картотеки»

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

- При использовании контроллеров Apollo с помощью кнопки **Точный доступ** можно расширить или ограничить права доступа в определенные помещения для выбранного сотрудника. Откроется окно ***Точный доступ и список исключений***.

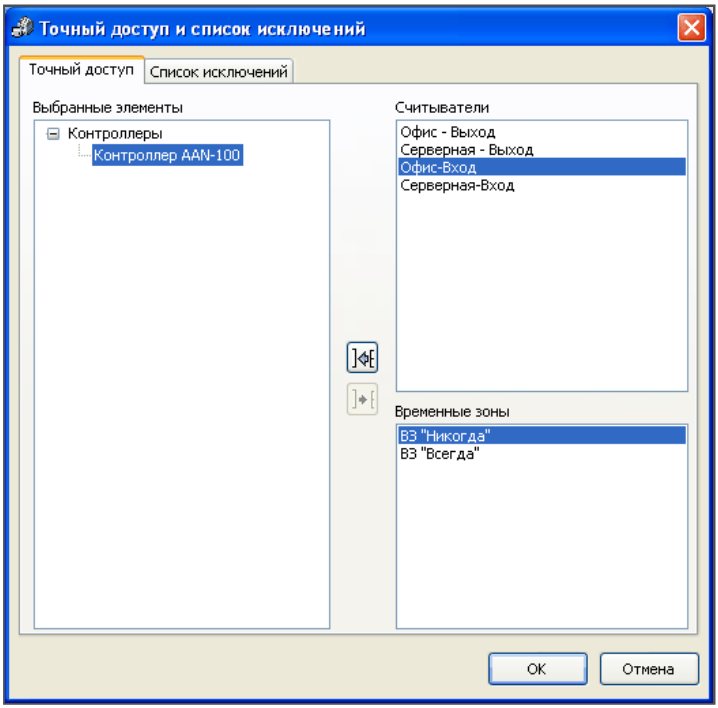


Рисунок Окно ***Точный доступ и список исключений*** вкладка **«Точный доступ»**

В этом окне на вкладке **«Точный доступ»** можно разрешить доступ в определенные помещения в течение указанного времени. Для этого в левой части окна выделите контроллер, справа в поле **Считыватели** появятся доступные для него считыватели. Выберите считыватель и в поле **Временные зоны** укажите временную зону, которую хотите закрепить за этим считывателем, и нажмите кнопку **Добавить**. Считыватель с указанной временной зоной будет добавлен в дерево к выделенному контроллеру. Чтобы удалить считыватель, выберите его в дереве и нажмите кнопку **Удалить**.

Обратите внимание: для идентификации карт по карте или ПИНу или по ПИНу, необходимо для каждой из этих карт указывать уникальный ПИН-код.

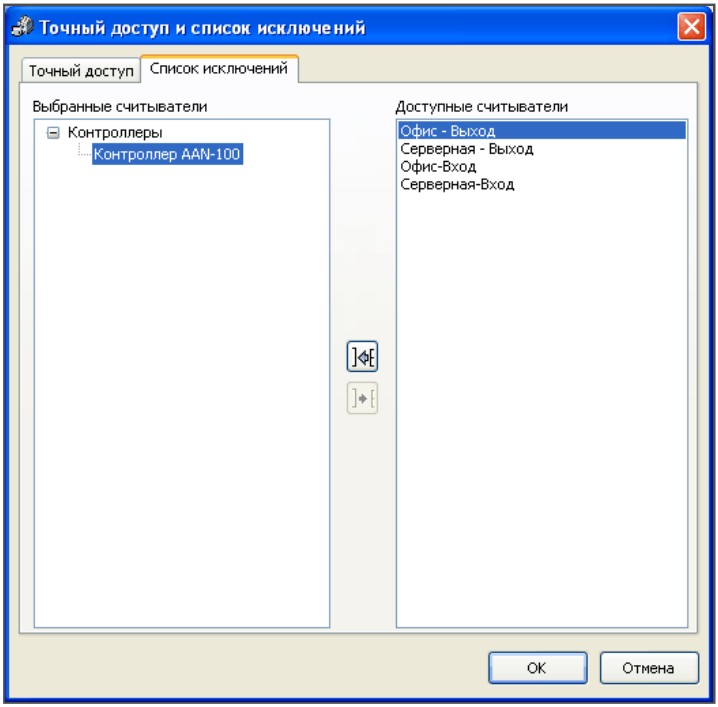


Рисунок Окно ***Точный доступ и список исключений*** вкладка **«Список исключений»**

На вкладке **«Исключения»** можно ограничить перемещение сотрудника в пределах уровней доступа, указав те считыватели, через которые ему будет запрещен проход. Для этого в левой части окна выделите контроллер, справа в поле **Доступные считыватели** появятся доступные для него считыватели. Выберите считыватели и нажмите на кнопку **Добавить** – выбранные считыватели будут добавлены в дерево как дочерние объекты выделенного контроллера. Чтобы удалить считыватель, выделите его в дереве и нажмите кнопку **Удалить**.

Обратите внимание: чтобы использовать функцию *Список исключений*, в настройках контроллера AAN-100/32 требуется поставить флажок **Список исключений**.

- **Даты / времена активации/деактивации** — группа настроек позволяет указать срок действия данного идентификатора. Используется для контроллеров VertX и Apollo AAN–100/32.
  - Если выбран пункт **из групп доступа**, поля заблокированы и для данного идентификатора будут использоваться те настройки активации / деактивации, которые указаны в закрепленных за

ним группах доступа.

- Чтобы использовать для идентификатора 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 дополнительных настроек идентификатора.
  - 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 идентификатора собственные настройки, отличающиеся от заданных в группах доступа, выберите пункт **текущие**. Поля разблокируются, и можно будет указать:
    - **Исключить из зоны КПВ** — поставьте этот флажок, чтобы информация о карте не хранилась в системе КПВ. Настройка недоступна для оборудования Suprema.
    - **Альтернативное время** — поставьте этот флажок, чтобы для владельца данного идентификатора использовалось увеличенное время открытия и закрытия двери при проходе. Настройка недоступна для оборудования Suprema.
    - **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. Настройка доступна для оборудования Apollo AAN-100/32.
    - **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. Настройка доступна для оборудования Apollo AAN-100/32.
    - С помощью настроек **Запрос ПО перед отказом/разрешением** можно организовать режим запроса на компьютер, при котором решение о доступе принимает дежурный оператор (см. «Apl: Глава 5 Режимы оборудования Apollo»). Настройки используются только для

контроллеров AAN–100/32.

- **Исключить ПИН** — если стоит этот флажок, владельцу данного идентификатора не требуется вводить ПИН–код в режиме считывателя *Карта и ПИН*.
  Настройка используется только для контроллеров VertX.
- **Разрешать команды с ПИН** — если стоит этот флажок, владелец данного идентификатора может управлять реле защелки с помощью команд, набранных на клавиатуре считывателя.
  Настройка используется только для контроллеров VertX.
- **экспертные** — настройка зарезервирована для использования в будущем.

Минимальный стиль оформления

Минимальный стиль оформления приложения «Картотека» предполагает, что все настройки доступа настраиваются в рамках объекта *Группа доступа*, а «Картотека» используется только для создания идентификаторов, закрепления за ними групп доступа и выдачи идентификаторов сотрудникам. Для идентификаторов используются те настройки, которые указаны в закрепленных за ними группах доступа. Поэтому на вкладке **«Основные»** объекта *Идентификатор* находится минимальное количество настроек.

Обратите внимание: при использовании оборудования Suprema СКД и минимального стиля оформления «Картотеки» вид вкладки **«Основные»** аналогичен виду вкладки при использовании максимального стиля.

Рассмотрим эти настройки:

- **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*).
  - 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*** (подробнее см. п. «3.4.2 Проверка идентификатора»).
  - 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»).

- **ПИН–код** — укажите персональный идентификационный номер, который владелец данного идентификатора будет вводить на клавиатуре считывателя в режиме *Карта и ПИН* или *Карта или ПИН*.
- **Статус** — укажите текущий статус идентификатора: обычный, утерян, уничтожен или изъят.
- **Шаблон** — выберите шаблон идентификатора. При смене шаблона Вам будет предложено применить настройки шаблона к идентификатору.
- кнопка **Применять настройки шаблона идентификатора** — нажмите на эту кнопку, если хотите изменить настройки идентификатора в соответствии с выбранным шаблоном.
  При нажатии на эту кнопку появится сообщение *Даты активации и деактивации идентификатора были изменены. Чтобы увидеть новые значения включите максимальный стиль в настройках картотеки.*
- **Расширенные настройки карт** — укажите объект типа *Расширенные настройки карт*, в котором указано, каким образом данная карта должна идентифицироваться на считывателях VertX. Настройка используется только для контроллеров VertX.

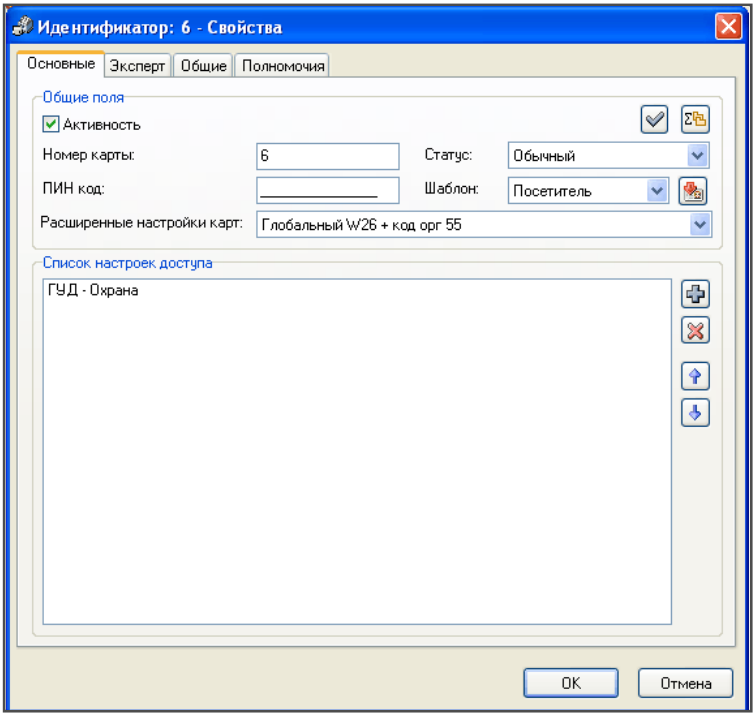


Рисунок Вкладка **«Основные»** объекта *Идентификатор* при использовании минимального стиля оформления «Картотеки» и полного набора оборудования

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

3.4.2 Проверка идентификатора

ПК APACS 3000 предоставляет возможность проверить сконфигурированный идентификатор до его загрузки в контроллеры. Для этого на вкладке **«Основные»** объекта *Идентификатор* нажмите кнопку **Проверить идентификатор** или выберите аналогичный пункт контекстного меню.

Если будут найдены ошибки, откроется диалоговое окно ***Ошибки, найденные при проверке идентификатора***. Окно разделено на две части:

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

Если в процессе проверки идентификатора ошибки не найдены, сообщение об этом появится в диалоговом окне ***Информация***.

Также предусмотрена возможность проверки сразу нескольких идентификаторов. Для этого на вкладке **«Идентификаторы»** окна ***Картотека*** выделите идентификаторы и воспользуйтесь пунктом контекстного меню «Проверить идентификатор».

Если в процессе проверки выделенных идентификаторов ошибки не найдены, сообщение об этом появится в диалоговом окне ***Информация***.

Если при проверке будут найдены ошибки, откроется диалоговое окно ***Список идентификаторов с ошибками***. В этом окне будет представлен список идентификаторов и ошибок, найденных при проверке. Для получения более подробной информации, выделите идентификатор и дважды щелкните по нему левой клавишей мыши или нажмите кнопку **Подробно**. Откроется диалоговое окно ***Ошибки, найденные при проверке идентификатора***.

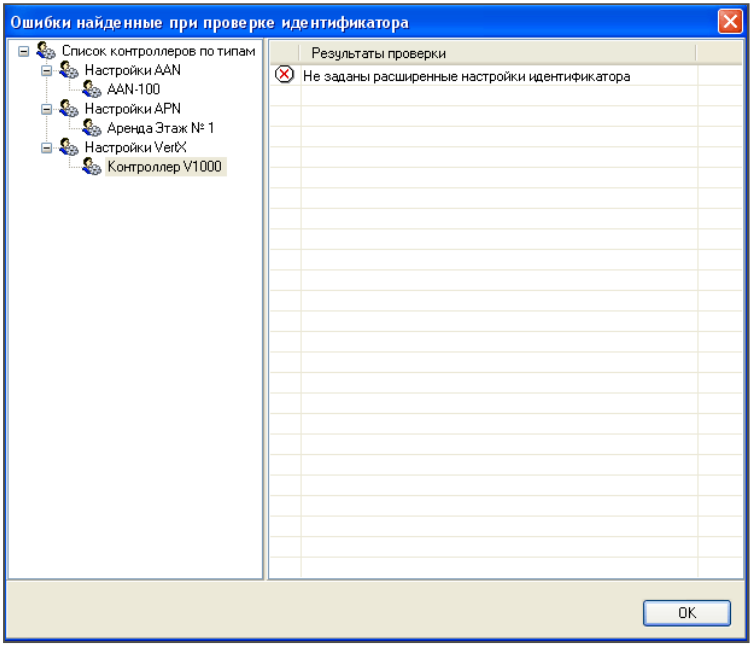


Рисунок Окно ***Ошибки, найденные при проверке идентификатора***

Возможные ошибки и предупреждения, возникающие при конфигурировании групп доступа

1 Группа предупреждений, связанных с тем, что в идентификаторе заданы настройки, использование которых отключено на контроллере. Чтобы задействовать эти настройки, включите их на контроллере. В противном случае настройки не будут действовать, несмотря на то, что они указаны в идентификаторе.

- ***Задано время активации, но оно отключено на контроллере*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Хранить время активации**)
- ***Задано время деактивации, но оно отключено на контроллере*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Хранить время деактивации**)
- ***Задана дата активации, но она отключена на контроллере*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Хранить дату активации**)
- ***Задана дата деактивации, но она отключена на контроллере*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Хранить дату деактивации**)
- ***Заданы настройки режима сопровождения посетителей, но он отключен у контроллера*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Режим сопровождения посетителей**)
- ***Задан точный доступ, но его использование отключено у контроллера*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Точный доступ**; в настройках контроллера AIM-4SL вкладка **«Основные»**, настройка **Использовать точный доступ**)
- ***Задан список исключений, но его использование отключено у контроллера*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Список исключений**)
- ***Задан ПИН-код, но его использование отключено на контроллере*** (в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройка **Размер ПИНа**; в настройках контроллера AIM-4SL вкладка **«Основные»**, настройка **Тип ПИНа**)

2 Группа предупреждений, связанных с тем, что совокупность настроек, заданных для идентификатора, превышает совокупность настроек контроллера, и контроллер не может обработать все настройки идентификатора. В этом случае загружается максимально возможное число первых значений (которые определяются по приоритету).

- ***Превышено число уровней доступа*** — число уровней доступа, назначенных идентификатору, превышает число используемых уровней доступа, которые указанны на контроллере. Например,

для идентификатора назначено семь уровней доступа, тогда как на контроллере включена настройка **6 уровней доступа**. Рекомендуется либо назначить идентификатору меньше уровней доступа, либо увеличить число используемых уровней доступа в настройках контроллера.

(в настройках контроллера AAN-100/32 вкладка **«Конфигурация базы карт»**, настройки **6 уровней доступа** и **32 уровня доступа**; в настройках контроллера AIM-4SL вкладка **«Основные»**, настройки **Использовать 6 уровней доступа** и **Использовать 32 уровня доступа**).

3 Группа предупреждений, связанных с тем, что в настройках идентификатора указаны объекты, которые были удалены. Рекомендуется отредактировать настройки в соответствии с текущей конфигурацией системы.

- ***Задана удаленная группа посетителей***
  Объект *Группа посетителей* используется для настройки режима сопровождения посетителей в контроллерах Apollo.
- ***Задан удаленный список групп посетителей***
  Объект *Список групп посетителей* используется для настройки режима сопровождения посетителей в контроллерах Apollo.
- ***Задана удаленная группа лифтовых реле***
  Объект *Группа лифтовых реле* используется в настройках уровней доступа контроллеров VertX, указывается в настройках группы доступа.
- ***Задан удаленный шаблон карт***
  Объект *Шаблон карт VertX* содержит информацию о параметрах используемых в системе карт, этот объект необходимо указать в настройках объекта *Расширенные настройки карт*.
- ***Заданы удаленные уровни доступа***
  Объект *Уровень доступа* представляет собой список считывателей контроллеров с закрепленными за ними временными зонами, этот объект необходимо указать в настройках группы доступа.
- ***Заданы удаленные временные зоны***
  Объект *Временная зона* используется в настройках уровней доступа контроллеров Apollo и VertX.
- ***Заданы удаленные считыватели***
  Объект *Считыватель* отвечает за настройку и управление физическим объектом – считывателем, подключенным к контроллерам Apollo и VertX.
- ***Задана удаленная группа доступа***
  Объект *Группа доступа* представляет собой совокупность прав и привилегий доступа сотрудников на контролируемой территории.

4 Группа предупреждений и ошибок, связанных с тем, что для идентификатора заданы не все настройки. Рекомендуется указать недостающие настройки.

- ***Не указана группа посетителей*** — в настройках группы доступа выбран тип идентификатора «посетитель с сопровождением», но не указана группа посетителей, в которую этот посетитель должен быть включен.
- ***Не указан список групп посетителей*** — в настройках группы доступа выбран тип идентификатора «сопровождающий», но не указан список групп посетителей, которых ему разрешено проводить.
- ***Не указан тип доступа*** — в настройках контроллера AAN-100/32 включен режим сопровождения посетителей, но в группе доступа не указан тип карты: посетитель, сопровождающий или сотрудник.
- ***Не задан ни один уровень доступа*** — в группе доступа, назначенной идентификатору, не задан ни один уровень доступа.
- ***Не задана дата активации*** — у контроллера AAN-100/32 включена настройка **Хранить дату активации**, но эта настройка не задана в группе доступа.
- ***Не задана дата деактивации*** — у контроллера AAN-100/32 включена настройка **Хранить дату деактивации**, но эта настройка не задана в группе доступа.
- ***Не задано время активации*** — у контроллера AAN-100/32 включена настройка **Хранить время активации**, но эта настройка не задана в группе доступа.
- ***Не задано время деактивации*** — у контроллера AAN-100/32 включена настройка **Хранить время деактивации**, но эта настройка не задана в группе доступа.
- ***Не заданы расширенные настройки идентификатора*** — при настройке группы доступа на базе оборудования VertX не был указан объект *Расширенные настройки карт*. Этот объект позволяет указать, каким образом должны идентифицироваться карты на считывателях VertX.
- ***Не задан ПИН код*** — при настройке группы доступа на базе оборудования VertX в расширенных настройках карты указана идентификация карты по ПИН, но ПИН код не задан в настройках идентификатора.

3.4.3 Просмотр настроек идентификатора

Чтобы посмотреть всю совокупность настроек, которые будут использованы для конкретного идентификатора, на вкладке **«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.

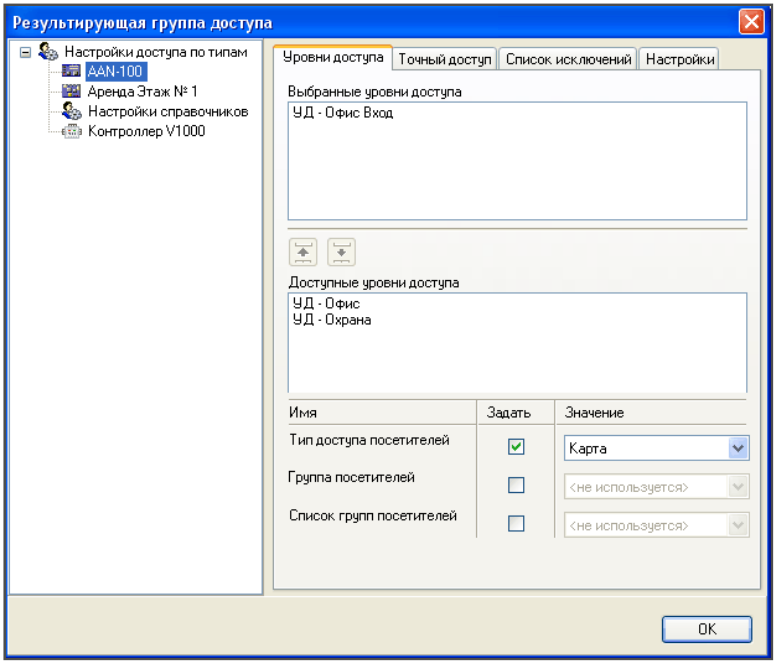


Рисунок Окно ***Результирующая группа доступа***

3.4.4 Вкладка «Эксперт»

На вкладке **«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** — 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 ***Собственные настройки доступа***, где можно изменить настройки групп доступа, закрепленные за идентификатором (рекомендуется опытным пользователям). Работа с этим окном аналогична работе с окном редактирования свойств объекта *Группа доступа* (см. п. «3.1 Группа доступа»).

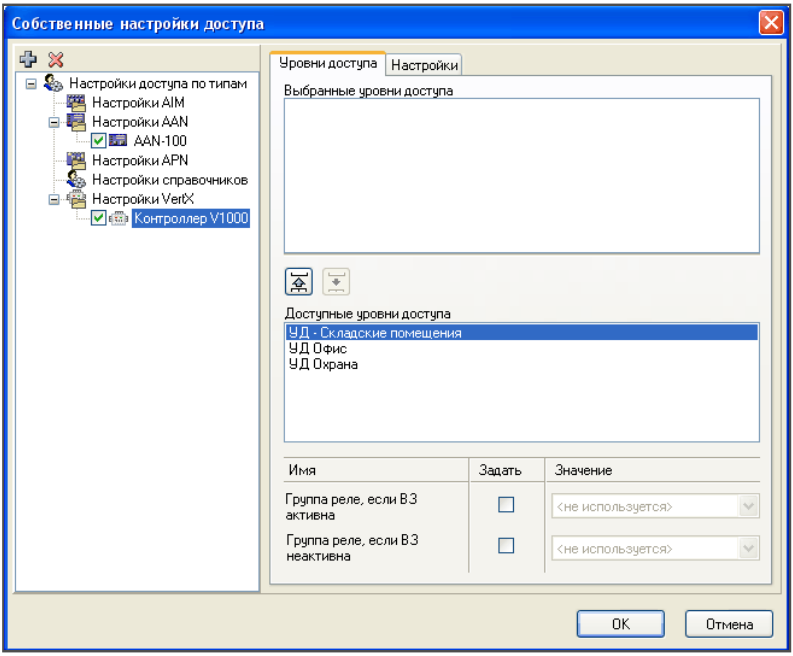


Рисунок Окно ***Собственные настройки доступа***

- 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.

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 вкладке **«Владельцы карт»** окна ***Картотека*** с помощью кнопки **Добавить** (подробнее о работе с объектом Владелец карты см. «Apc: Глава 6 Картотека 6.3 Работа с объектами»).

Все настройки объекта расположены на вкладках **«Основные»**, **«Доступ»**, **«Эксперт»**, **«Выдачи»** и **«Работы»**. Вкладка **«Эксперт»** позволяет задать собственные настройки доступа для конкретного владельца карты, эту

вкладку рекомендуется использовать только опытным операторам комплекса. При использовании оборудования Suprema так же указываются настройки на вкладке **«Биоданные»**. При использовании оборудования Suprema СКД необходимо задать соответствующие настройки на вкладке **«Suprema СКД»**.

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

3.5.1 Вкладка «Доступ»

В зависимости от оборудования, с которым работает ПК APACS 3000, и выбранного стиля оформления приложения **«Картотека»** вкладка **«Доступ»** имеет разный интерфейс. Настройки, которые будут находиться на этой вкладке аналогичны соответствующим настройкам доступа вкладки **«Основные»** объекта *Идентификатор* (о работе с этой вкладкой см. п. «3.4.1 Вкладка «Основные»).

3.5.2 Вкладка «Suprema СКД»

На вкладке «**Suprema СКД**» 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 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**.
    - **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 (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.

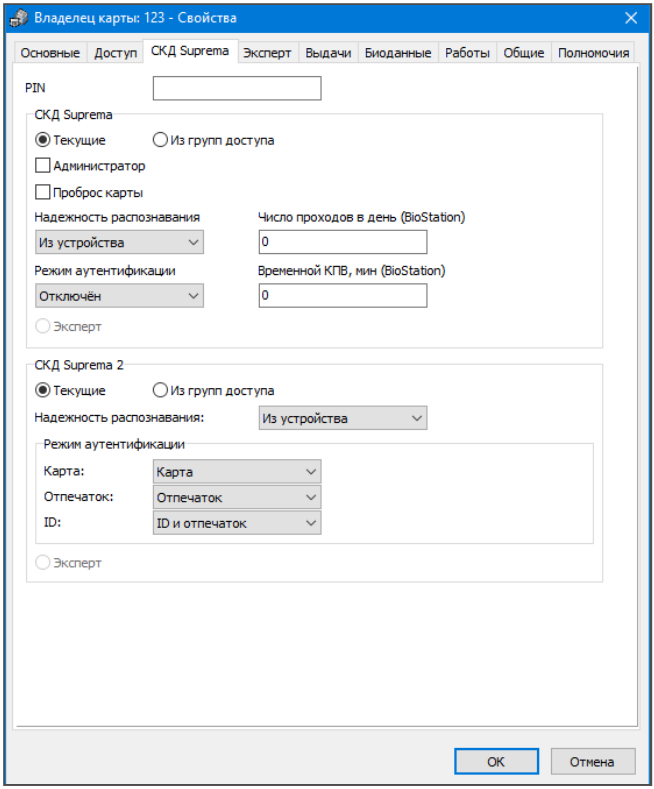


Рисунок Вкладка «**СКД Suprema**» объекта *Владелец карты*

- 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»**:
    - **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 *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.

- **Карта** — выберите режим, который будет использоваться для верификации пользователя на устройстве с использованием карты (*Карта*, *Карта и отпечаток*, *Карта и ПИН*, *Карта и отпечаток или ПИН*, *Карта*, *отпечаток 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*.
- **Отпечаток** — выберите режим, который будет использоваться для идентификации пользователя на устройстве (*Отпечаток*, *Отпечаток и ПИН*, *Запрещен*, *Из устройства*). Если выбран режим *Запрещен*, то сотрудник не сможет получить доступ по отпечатку пальца. 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 отпечаток*, *ID и ПИН*, *ID и отпечаток или ПИН*, *ID*, *отпечаток 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.

3.5.3 Вкладка «Эксперт»

На вкладке **«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 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.

3.5.4 Вкладка «Выдачи»

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

3.5.5 Вкладка «Биоданные»

На вкладке **«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.

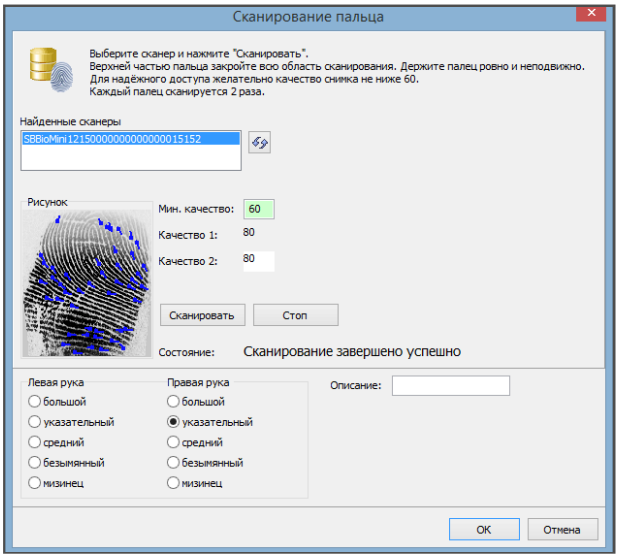


Рисунок Окно ***Сканирование пальца***

По завершению сканирования, информация о владельце появится в таблице на вкладке «**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.

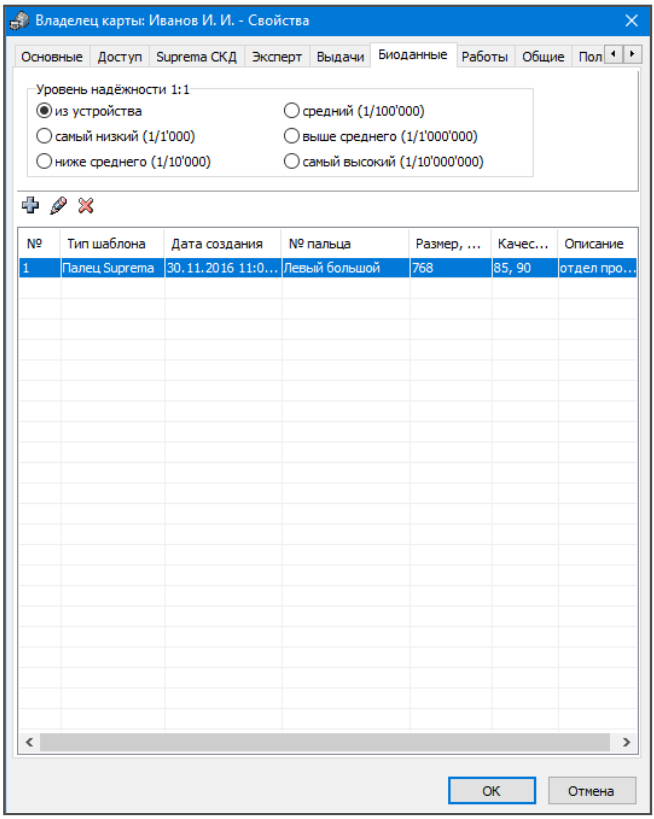


Рисунок Вкладка «**Биоданные**» объекта *Владелец карты*

3.5.6 Вкладка «Работы»

На вкладке **«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. «Apc: Глава 8 Учет рабочего времени»).

3.6 Перенос настроек доступа

Начиная с ПК APACS 3000 v 6.3, в комплексе появилась возможность задания прав доступа в настройках владельцев карт. Возможность назначения прав доступа в настройках идентификаторов была сохранена.

Для большинства владельцев карты предпочтительнее использовать новый подход к хранению прав доступа, поэтому рекомендуется перенести настройки доступа от карт к владельцам. Для удобства переноса прав доступа между объектами *Владелец карты* и *Идентификатор* предусмотрены соответствующие функции. Далее подробнее рассмотрим возможные варианты переноса прав доступа.

Перенос настроек доступа владельцам карт

Для того чтобы перенести права доступа от идентификаторов владельцам карт, в окне ***Картотека*** на вкладке **«Владельцы карт»** выделите владельцев карт и выберите пункт меню «Обслуживание/Перенос настроек доступа владельцам карт» окна ***Основная панель***. Откроется окно ***Перенос настроек доступа владельцам карт***, где требуется указать какие настройки доступа идентификаторов будут перенесены в настройки владельцев карт.

В группе параметров **Список групп доступа** укажите, что следует сделать с группами доступа владельца карты:

- **Не изменять** — выберите это поле, если хотите, чтобы настройки групп доступа владельца карты, при переносе прав доступа, остались неизменными.
- **Заменить** — выберите этот пункт, если хотите, чтобы настройки групп доступа владельца карты были перезаписаны настройками групп доступа идентификатора.
- **Добавить** — выберите этот пункт, если хотите, чтобы настройки групп доступа идентификатора были добавлены к настройкам групп доступа владельца карты. При этом группы доступа идентификатора будут добавлены в конец списка.

В группе параметров **Собственная группа доступа**, укажите:

- **Не изменять** — выберите этот пункт, если хотите оставить неизменной собственную группу доступа владельца карты.
- **Заменить** — выберите этот пункт, если хотите заменить собственную группу доступа владельца карты собственной группой доступа идентификатора.

В группе параметров **Для владельцев нескольких карт** выберите действие, которое будет выполняться при переносе настроек доступа из нескольких идентификаторов владельцу:

- **Пропускать** — выберите эту настройку, если хотите, чтобы владелец

нескольких карт при переносе настроек доступа, был пропущен.

- **Использовать первый идентификатор** — выберите эту настройку, если хотите, чтобы владельцу карты были перенесены настройки первого идентификатора. При этом из всех идентификаторов данного владельца будут удалены настройки доступа.

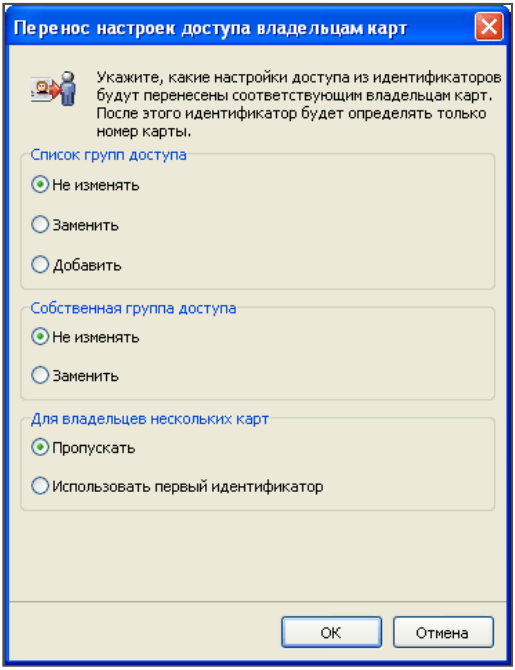


Рисунок Окно ***Перенос настроек доступа владельцам карт***

После того как все параметры заданы, нажмите кнопку **OK**. Права доступа от идентификаторов будут перенесены соответствующим владельцам карт, после чего идентификатор будет определяться только номером карты.

Перенос настроек доступа в идентификаторы

Для того чтобы перенести права доступа от владельцев карт в идентификаторы, в окне ***Картотека*** на вкладке **«Владельцы карт»** выделите владельцев карт, настройки доступа которых хотите перенести в выданные им идентификаторы, и выберите пункт меню «Обслуживание/Перенос настроек доступа в идентификаторы» окна ***Основная панель***. Откроется окно ***Перенос настроек доступа в идентификаторы***, в этом окне укажите следующие настройки:

- **Очистить настройки доступа владельца** — поставьте этот флажок, если хотите, чтобы после переноса настроек доступа, все настройки доступа владельца карты были очищены.

Обратите внимание: в случае если у карты были заданы свои права доступа, то настройки прав доступа владельца карты ей перенесены не будут.

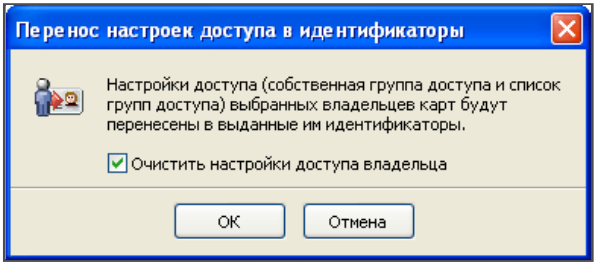


Рисунок Окно ***Перенос настроек доступа в идентификаторы***

Изменение настроек доступа идентификаторов

Для того чтобы изменить настройки доступа конкретных идентификаторов, воспользуйтесь одним из следующих способов:

- в окне ***Картотека*** на вкладке **«Идентификаторы»** выделите нужные идентификаторы и выберите пункт контекстного меню «Изменить тип доступа».
- в окне ***Картотека*** на вкладке **«Идентификаторы»** выделите нужные идентификаторы и нажмите кнопку **Групповое редактирование** на панели инструментов окна ***Основная панель***.

В открывшемся окне выберите нужный тип хранения прав доступа и примените к выделенным идентификаторам.