

APACS



BiO

Подсистема синхронизации с Active Directory

Руководство пользователя

01000001 01010000 01000001
01000011 01010011
00100000 00110011 00110000
00110000 00110000

00100000 01000100
01100101 01110110 01100101
01101100 01101111
01110000 01100101 01110010

00100000 01010100
01100101 01100001
01101101



Соглашения, используемые в книге

В этой книге используются следующие соглашения о шрифтах:

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



Так выделяется информация, которая приводится в документации для примера.



Так выделяется информация, на которую следует обратить внимание.

Содержание

1 Введение	AcD-4
1.1 Состав решения	AcD-4
1.2 Принципы конфигурирования	AcD-4
2 Конфигурационная утилита для ADSync	AcD-5
2.1 Настройки службы синхронизации с AD	AcD-8
3 Утилита для импорта изменений пользователей	AcD-16

1 Введение

Подсистема синхронизации с Active Directory (далее AD) позволяет синхронизировать информацию, находящуюся на сервере AD, с базой данных APACS Bio. Решение поддерживает как автоматическую, так и ручную синхронизацию данных.

Данное решение удобно использовать в случае, когда на предприятии для хранения учетных данных сотрудников используется Active Directory. Использование данного решения позволит уменьшить время переноса информации, а также сократить количество ошибок.

В текущей версии поддерживается импорт и синхронизация пользователей и их свойств (группы доступа, фотография и т.д.) из AD в APACS Bio.

1.1 Состав решения

Подсистема AD состоит из трех основных компонентов:

- Служба синхронизации с AD,
- Конфигурационная утилита для ADSync,
- Утилита для импорта изменений пользователей.

Служба синхронизации с AD — это внутренняя служба сервера APACS Bio, которая отслеживает и накапливает изменения объектов, находящихся на сервере AD, а также синхронизирует изменения с базой данных APACS Bio в соответствии с заданными настройками.

Конфигурационная утилита для ADSync используется для настройки службы синхронизации, настройки идентификации удаленных пользователей и проведения начального импорта пользователей.

Утилита для импорта изменений пользователей предназначена для ручного импорта изменений.

1.2 Принципы конфигурирования

Для конфигурирования подсистемы синхронизации с AD необходимо выполнить следующие действия:

1. Задать настройки службы синхронизации с AD с помощью конфигурационной утилиты для ADSync (подробнее см. п. 2 Конфигурационная утилита для ADSync).
2. Выбрать способ идентификации удаленных пользователей. Выбор способа идентификации необходим из-за специфики удаления объектов на сервере AD.
3. Провести начальный импорт объектов из AD в APACS Bio. Для этого можно воспользоваться одним из следующих способов:
 - автоматически с помощью конфигурационной утилиты для ADSync (кнопка **Начальный импорт**),
 - вручную с помощью утилиты для импорта изменений пользователей (подробнее см. п. 3 Утилита для импорта изменений пользователей).
4. Запустить службу синхронизации с AD. Для этого воспользуйтесь файлом [APACS Bio]\bin\ApcADSyncReRegister.bat, где [APACS Bio] —

каталог, где установлен ПК APACS Bio. Файл необходимо запустить с правами администратора.

2 Конфигурационная утилита для ADSync

Утилита предназначена для настройки и запуска службы синхронизации с AD, настройки идентификации удаленных пользователей и проведения начального импорта изменений.

Запуск утилиты

Для того чтобы запустить конфигурационную утилиту, требуется выполнить следующее:

1. Запустить сервер ПК APACS Bio.
2. Запустить файл [APACS Bio]\bin\ArcADSyncMainAppl.exe с правами администратора, где [APACS Bio] – каталог, где установлен комплекс ПК APACS Bio. Для того чтобы проверить наличие прав администратора, воспользуйтесь утилитой *Информация о текущем пользователе* (подробнее см. «Utl: Утилиты 15 Утилита «Информация о текущем пользователе Windows»).
3. Далее необходимо подключиться к серверам AD и APACS Bio. Для этого в окне *Авторизация в APACS Bio* необходимо указать **Логин** и **Пароль** учетной записи администратора ПК APACS Bio. По умолчанию это пользователь *Admin* с паролем *Bio*.

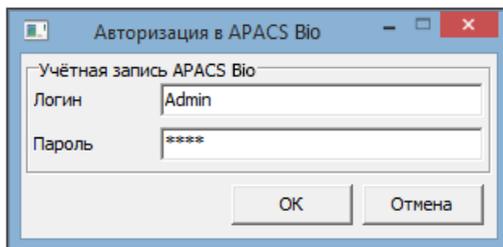


Рисунок окно *Авторизация в APACS Bio*

В окне *Авторизация в Active Directory* требуется указать следующие настройки:

- **Адрес сервера** — в этом поле требуется указать ip-адрес сервера AD.
- **Метод авторизации** — в этой группе параметров требуется указать метод авторизации, который будет использован для подключения к серверу AD:
 - о **Войти от текущего пользователя** — при выборе этого метода будут использованы учетные данные текущего пользователя компьютера.
 - о **С учетной записью** — при выборе этого метода необходимо будет ввести учетные данные записи пользователя, который обладает правом на доступ к серверу AD. При выборе этой настройки разблокируется поле **Пароль**.

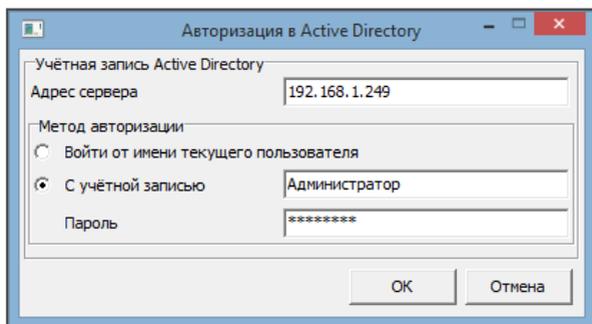


Рисунок окно *Авторизация в Active Directory*

4. После этого откроется окно *Конфигурационная утилита для ADSync*.
Работа с утилитой

Все настройки окна утилиты находятся на вкладках «**Основные**» и «**Управление**».

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

- Кнопка **Настройки** позволяет задать настройки службы синхронизации с AD и начального импорта пользователей. При нажатии на эту кнопку откроется окно *Настройки службы синхронизации с AD*. (подробнее см. п. 2.1 Настройки службы синхронизации с AD).
- Кнопка **Начальный импорт** позволяет выполнить первоначальный импорт пользователей из AD в APACS Bio в соответствии с настройками, заданными в окне *Настройки службы синхронизации с AD*.



Обратите внимание: начальный импорт может занять длительное время, поэтому его рекомендуется выполнять во время минимальной загруженности системы.

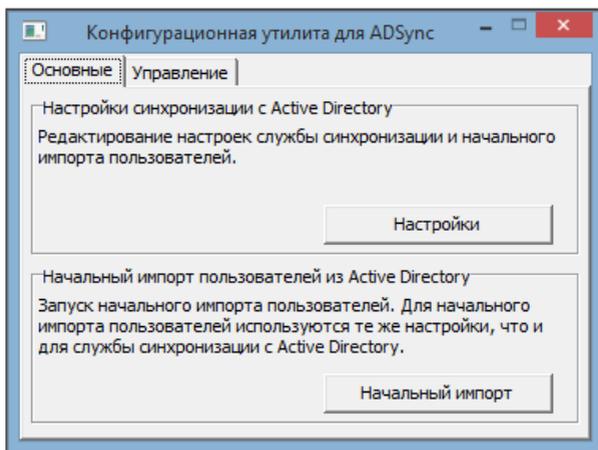


Рисунок окно *Конфигурационная утилита для ADSync* вкладка «Основные»

На вкладке «Управление» находятся следующие настройки:

- **Служба синхронизации с Active Directory** — в этой группе параметров с помощью кнопок **Старт** и **Стоп** можно запустить или остановить работу службы AD.
В поле **Состояние службы** указано текущее состояние службы: *Запущена* или *Остановлена*.
- **Идентификация удаленных пользователей** — в этой группе параметров выберите способ корректировки схемы AD для идентификации удаленных пользователей. Корректировка схемы необходима из-за специфики удаления объектов на сервере AD.
 - **Сгенерировать скрипт** — нажмите на эту кнопку, чтобы сохранить скрипт на компьютере. При необходимости сгенерированный скрипт можно отредактировать, после чего его необходимо запустить на сервере AD.
При нажатии на эту кнопку, откроется стандартное диалоговое окно Windows *Сохранить*, в этом окне укажите путь к папке, где должен быть сохранен скрипт.
 - **Скорректировать схему** — нажмите на эту кнопку, если хотите, чтобы схема AD была скорректирована автоматически с использованием настроек службы.

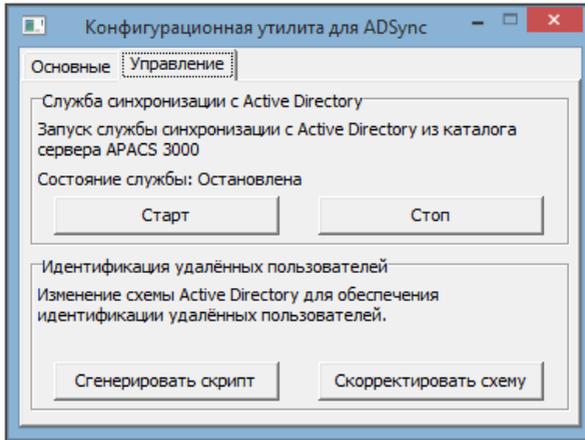


Рисунок окно *Конфигурационная утилита для ADSync* вкладка «Управление»

2.1 Настройки службы синхронизации с AD

Настройки службы синхронизации с AD — логический объект системы, использующийся в работе подсистемы синхронизации с AD. С его помощью указываются соответствия полей пользователей AD и владельцев карт APACS Bio, а также задаются настройки для работы службы синхронизации с AD.

Все настройки находятся на вкладках «**Основные**», «**Соответствия ключевых полей**», «**Соответствия полей**», «**Дополнительные**».

На вкладке «**Основные**» требуется указать следующие настройки:

- **Учетная запись APACS Bio** — в этой группе параметров в полях **Логин** и **Пароль** укажите учетные данные администратора ПК APACS Bio. По умолчанию это пользователь *Admin* с паролем *Bio*.
- **Учетная запись Active Directory** — в этой группе параметров укажите данные учетной записи Active Directory.
 - **Адрес сервера** — в этом поле укажите ip-адрес сервера AD.
 - **Метод авторизации** — в этой группе параметров укажите какой метод авторизации на сервере AD будет использоваться:
 - **Использовать системные настройки службы** — при выборе этого метода будут использованы системные настройки службы.
 - **С учетной записью** — при выборе этого метода необходимо будет ввести учетные данные записи пользователя, который обладает правом на доступ к серверу AD. При выборе этой настройки разблокируется поле **Пароль**.
- Кнопка **Заполнить данными текущей сессии** позволяет автоматически заполнить реквизиты для подключения службы к серверам данными текущей сессии.

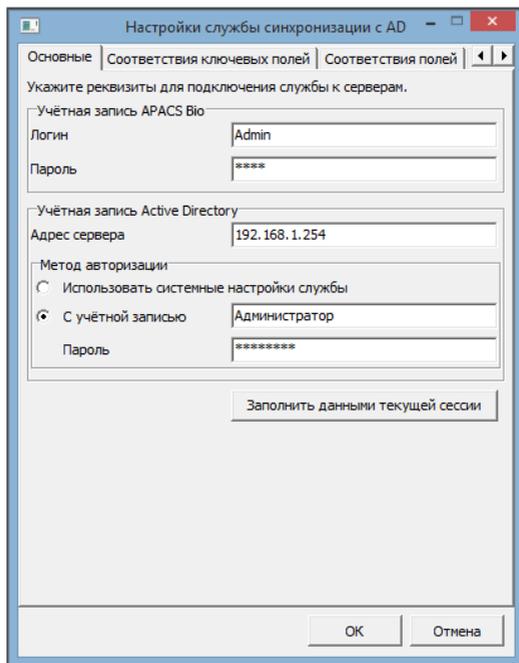


Рисунок окно *Настройки службы синхронизации с AD* вкладка «**Основные**»

На вкладке «**Соответствия ключевых полей**» необходимо указать атрибуты пользователя в AD и соответствующие им свойства владельца карты в APACS Bio, которые будут являться ключевыми при синхронизации. Ключевыми называются поля, комбинация значений которых однозначно определяет пользователя.

Работа с вкладкой «**Соответствия ключевых полей**» аналогична работе с вкладкой «**Соответствие полей**».

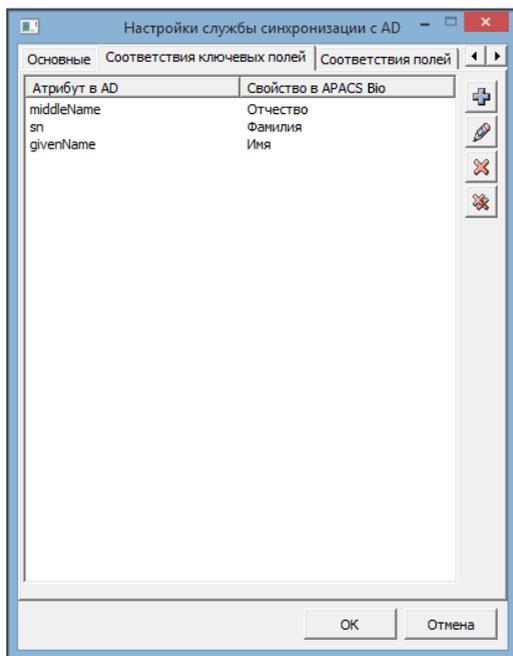


Рисунок окно *Настройки службы синхронизации с AD* вкладка «Соответствия ключевых полей»

На вкладке «Соответствия полей» требуется указать атрибуты пользователя в AD и соответствующие им свойства владельцев карт в APACS Bio.

Для работы с этой вкладкой используются кнопки **Добавить**, **Редактировать**, **Удалить** и **Удалить все**.

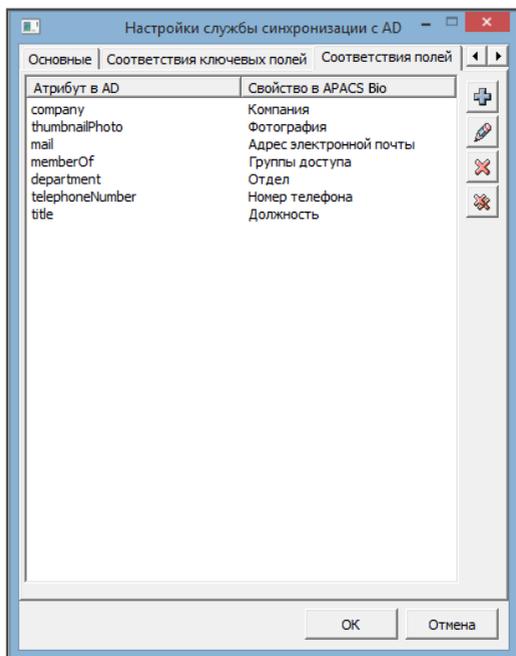


Рисунок окно *Настройки службы синхронизации с AD* вкладка «Соответствия полей»

Для того чтобы добавить соответствие, нажмите кнопку **Добавить**. Откроется окно *Редактор соответствия полей*. В этом окне находятся следующие настройки:

- В полях **Атрибуты пользователя AD** и **Свойства владельца карты** требуется указать атрибуты пользователя AD и соответствующие им свойства владельца карты в APACS Bio.
- **Автоматический выбор соответствия** — поставьте этот флажок, если хотите, чтобы соответствия для полей проставлялись автоматически. Если для выбранного поля не задано соответствие, то значение соответствующего поля останется без изменений и его можно будет изменить вручную.

Если при задании соответствий были выбраны поля, у которых может быть несколько значений (например, такие поля как **Пол**, **Статус**, **Категория**, **Группа доступа**), то разблокируется группа параметров **Соответствия значений перечисляемых полей**. Редактирование этой группы осуществляется с помощью кнопок **Добавить**, **Редактировать**, **Удалить** и **Удалить все**.

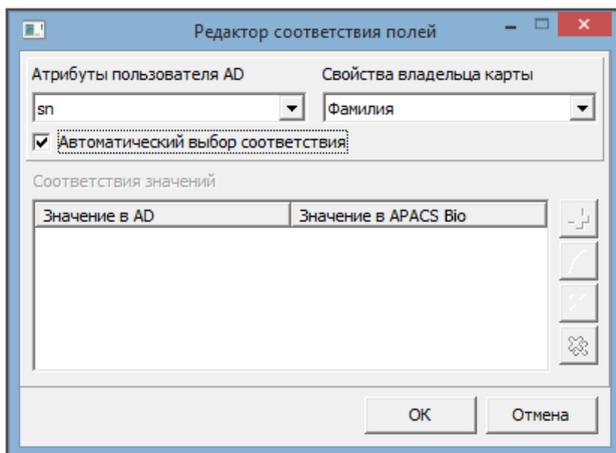


Рисунок окно *Редактор соответствия полей*

С помощью кнопки **Добавить** можно добавить соответствия значений для перечисляемых полей.

Если соответствия значений задаются для полей **Категория**, **Статус** или **Пол**, то при нажатии на кнопку **Добавить** откроется окно **Редактор соответствия значений**.

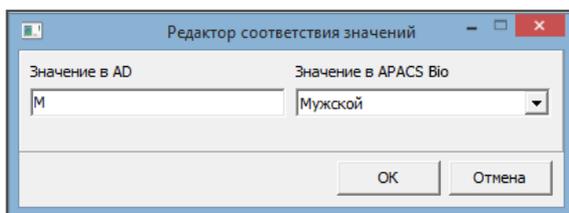


Рисунок окно *Редактор соответствия значений*

В этом окне требуется каждому значению поля **Значение в APACS Bio** указать соответствующее значение в поле **Значение в AD**.



Например, задано соответствие полей **Пол** в APACS Bio и **description** в AD. Для этих полей требуется указать соответствие значений. Свойство **Пол** в APACS Bio имеет три значения: *Мужской*, *Женский* и *Не указан*. Для каждого из этих значений укажем соответствующие значения для атрибута **description**: *M*, *J* и *N*.

Тогда, если у пользователя AD в поле **description** будет указано значение *M*, то после импорта у владельца карты в APACS Bio в поле **Пол** будет указано значение *Мужской*.

Если соответствия задаются для поля **Группа доступа**, то откроется окно **Редактор соответствия групп доступа**.

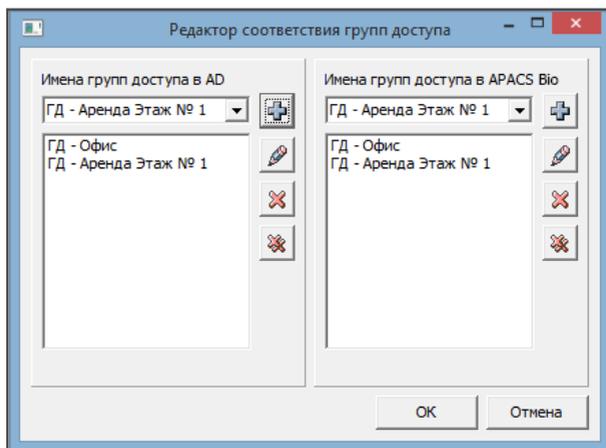


Рисунок окно *Редактор соответствия групп доступа*

В этом окне требуется указать соответствия между именами групп доступа в AD и APACS Bio.

- **Имена групп доступа в AD** — в этом поле требуется выбрать имя одной или нескольких групп доступа в AD. Список имен формируется с помощью кнопок **Добавить**, **Редактировать**, **Удалить** и **Удалить все**.
- **Имена групп доступа в APACS Bio** — в этом поле требуется выбрать имя одной или нескольких групп доступа в APACS Bio. Список имен формируется с помощью кнопок **Добавить**, **Редактировать**, **Удалить** и **Удалить все**.



Например, выбрано такое соответствие: группа *ГД-Вход* в AD соответствует списку из групп *ГД-Охрана* и *ГД-Офис* в APACS Bio. Тогда пользователям, которым в AD назначена группа *ГД-Вход*, после импорта в APACS Bio будут назначены группы *ГД-Охрана* и *ГД-Офис*.

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

- **Если не найден владелец карты с соответствующим ключом** — в этой группе параметров укажите, что требуется делать службе, в случае, если владелец карты с соответствующим ключом не был найден:
 - **Пропустить** — выберите эту настройку, если хотите, чтобы владелец карты был пропущен.
 - **Добавить** — выберите эту настройку, если хотите, чтобы новый владелец карты был добавлен в базу данных APACS Bio.
- **Если найден владелец карты с соответствующим ключом** — в этой группе параметров укажите, что требуется делать службе, в случае, когда найден владелец с соответствующим ключом:
 - **Пропустить** — выберите эту настройку, если хотите, чтобы владелец карты был пропущен.

- **Обновить** — выберите эту настройку, если хотите, чтобы данные владельца карты в APACS Bio были обновлены в соответствии с изменениями в AD.
- **Если соответствующий владельцу пользователь был удален** — в этой группе параметров укажите, что требуется сделать с владельцем карты, когда пользователь, соответствующий этому владельцу, был удален:
 - **Пропустить** — выберите эту настройку, если хотите, чтобы соответствующий владелец карты был пропущен. В этом случае владелец карты не будет удален из базы APACS Bio.
 - **Снять активность идентификаторов** — выберите эту настройку, чтобы у соответствующих владельцев карт в APACS Bio деактивировались идентификаторы.
 - **Удалить** — выберите эту настройку, если хотите, чтобы соответствующий владелец карты был удален из базы данных APACS Bio.

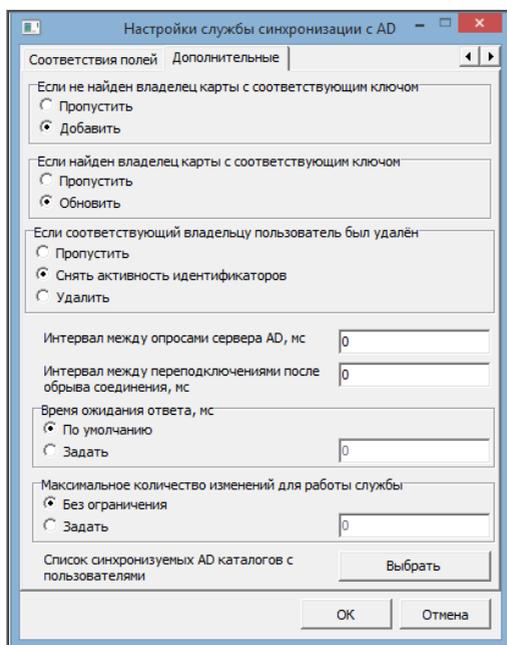


Рисунок окно *Настройки службы синхронизации с AD* вкладка «Дополнительные»

- **Интервал между опросами сервера AD, мс** — в этом поле укажите интервал опроса сервера AD на наличие изменений.
- **Интервал между переподключениями после обрыва соединения, мс** — укажите интервал времени, по истечению которого будут повторяться попытки подключения к серверу AD в случае разрыва соединения.

- **Время ожидания ответа, мс** — в этой группе параметров укажите время ожидания ответа:
 - **По умолчанию** — выберите эту настройку, если хотите, чтобы использовалось время ожидания, заданное по умолчанию.
 - **Задать** — выберите эту настройку, если хотите задать ручную время ожидания ответа.
- **Максимальное количество изменений для работы службы** — в этой группе параметров укажите максимально возможное количество изменений, которые может обработать служба:
 - **Без ограничения** — выберите эту настройку, если хотите, чтобы не было ограничения на число обрабатываемых изменений.
 - **Задать** — выберите эту настройку, если хотите указать ручную максимально возможное число изменений, которые могут быть загружены службой.
- Кнопка **Выбрать** позволяет задать список синхронизируемых AD каталогов с пользователями. При нажатии на эту кнопку откроется окно **Выбор каталогов для синхронизации**, где будет представлено дерево каталогов сервера AD. Для выбора определенного каталога необходимо напротив поставить флажок. С помощью пунктов контекстного меню можно выделить всю отдельно взятую ветвь либо снять выделение с ветви.



Обратите внимание: информация о пользователях, находящихся во вложенных каталогах, синхронизироваться не будет, если вложенный каталог не выделен явно.

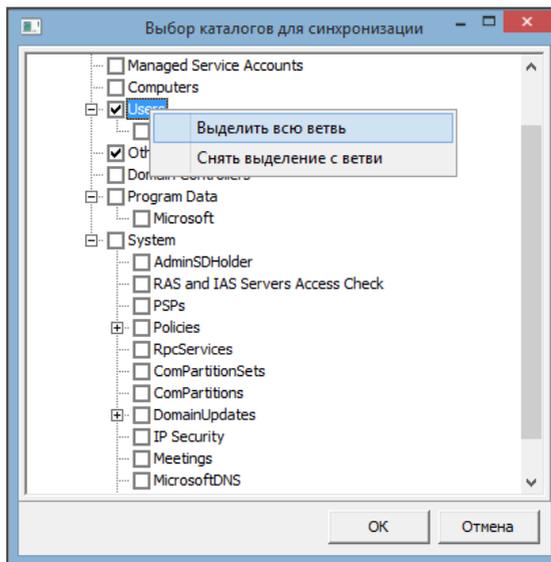


Рисунок окно **Выбор каталогов для синхронизации**

После первоначальной настройки службы будет предложено выполнить коррекцию схемы AD. Открывается окно **Требуется коррекция схемы AD**, где необходимо выбрать метод корректировки схемы AD для идентификации удаленных пользователей:

- **Выберите метод:**
 - **Сгенерировать скрипт изменения схемы AD** — выберите этот метод, если хотите сохранить скрипт изменения схемы AD на компьютере. При необходимости сгенерированный скрипт можно отредактировать, после чего его необходимо запустить на сервере AD. При нажатии на кнопку **ОК**, откроется стандартное диалоговое окно Windows **Сохранить**, в этом окне выберите папку, в которой будет сохранен скрипт.
 - **Автоматически изменить схему AD** — выберите этот метод, если хотите, чтобы схема AD была скорректирована автоматически с использованием настроек службы.

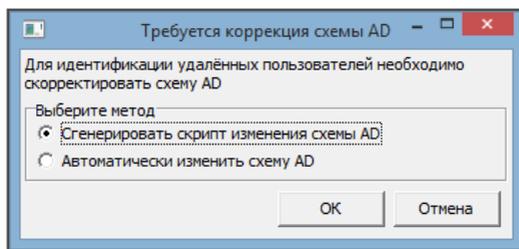


Рисунок окно **Требуется коррекция схемы AD**

3 Утилита для импорта изменений пользователей

Утилита предназначена для ручного импорта изменений пользователей. Для работы данная утилита использует настройки, заданные в окне **Настройки службы синхронизации с AD**.

Запуск утилиты

Чтобы запустить утилиту запустите файл [APACS Bio]\ArcADSyncHandImport.exe, где [APACS Bio] — каталог, где установлен ПК APACS Bio. Откроется окно **Утилита для импорта изменений пользователей**.

Интерфейс окна утилиты

В окне **Утилита для импорта изменений пользователей** содержится подробная информация об изменениях пользователей в AD. Информация оформлена в виде таблицы, где находятся следующие поля:

- **USN изменения** — в этом поле указан уникальный номер изменения,
- **Тип изменения** — в этом поле указан тип изменения,
- **Ключевые атрибуты** — в этом поле перечислены ключевые атрибуты пользователя AD,

- **Детальная информация** — в этом поле представлена подробная информация о пользователе AD.

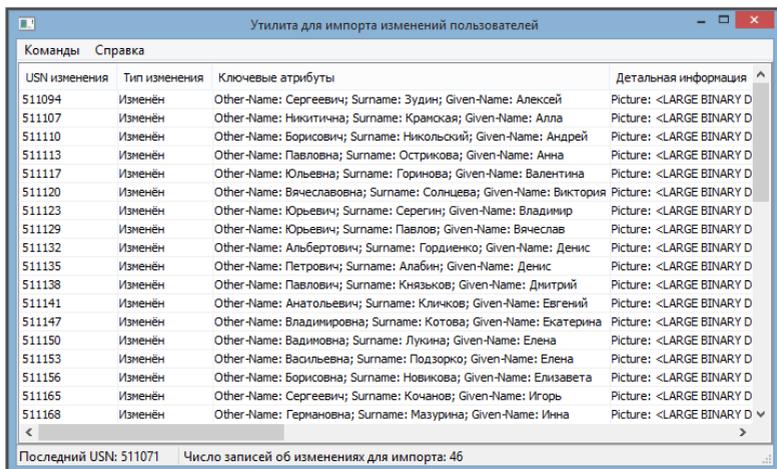


Рисунок окно *Утилита для импорта изменений пользователей*

Для работы с этим окном используются пункты основного меню и пункты контекстного меню. С их помощью можно:

- обновить список изменений,
- импортировать все изменения в APACS Bio,
- импортировать все изменения до выбранного включительно,
- изменить последний USN — при выборе пункта меню «Команды/Изменить последний USN» отруется окно *Изменение USN*, где можно указать номер изменения, начиная с которого будут отображаться изменения в окне *Утилита для импорта изменений пользователей*.

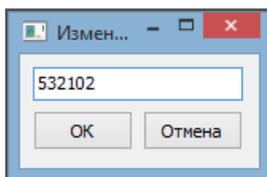


Рисунок окно *Изменение USN*

- Просмотреть информацию о записи. Для этого дважды щелкните левой клавишей мыши по строке с записью. Откроется окно *Просмотр данных для импорта пользователя*.

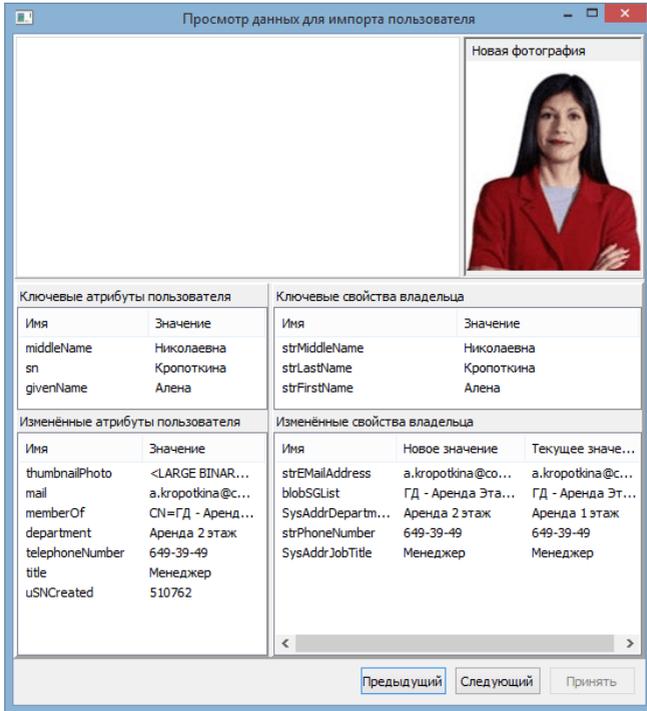


Рисунок окно *Просмотр данных для импорта пользователя*

Окно *Просмотр данных для импорта пользователя* состоит из нескольких частей:

- В верхней части находится список изменений, связанных с владельцем карты и поле **Новая фотография**, где отображается последняя добавленная фотография пользователя.
- В нижней части находится следующая информация:
 - **Ключевые атрибуты пользователя** и **Ключевые свойства владельца** — в этих таблицах находятся имена атрибутов пользователя и свойств владельца, которые были выбраны в качестве ключевых, и их значения в AD и APACS Bio соответственно.
 - **Изменённые атрибуты пользователя** — в этой таблице находится список имен атрибутов пользователей, которые были изменены, и их значений.
 - **Изменённые свойства владельца** — в этой таблице находятся изменённые свойства владельца. В полях таблицы указаны **Имя** свойства, его текущее и новое значения.
- Кнопки **Предыдущий** и **Следующий** позволяют перейти к просмотру изменений предыдущего и следующего пользователей соответственно.
- Кнопка **Принять** позволяет импортировать изменения в APACS Bio.