Тел.: (495) 363-37-53; (4012) 51-05-64; e-mail: info@1c-bitrix.ru, http://www.1c-bitrix.ru

1С-Битрикс: Управление сайтом

Руководство по настройке модуля AD/LDAP интеграция

Содержание

Введение

При интеграции сайта (корпоративного портала) с информационной системой организации может возникнуть потребность в разграничении прав доступа сотрудников компании на доступ к ресурсам сайта и его управлению.

Стандартным решением данной задачи является создание нескольких групп пользователей сайта (корпоративного портала) с различным уровнем. При этом необходимо распределение сотрудников по этим группам, для наделения их соответствующими правами на доступ и управление сайтом. В этом случае администратор может столкнуться с необходимостью дублирования уже существующих групп пользователей корпоративной сети в системе управления сайтом (корпоративного портала).

Возникает и другая сложность. Чтобы изменить уровень прав или добавить нового пользователя одновременно в корпоративной сети и в системе управления сайтом (корпоративном портале), необходимо выполнить настройку дважды:

- изменить/создать бюджет пользователя в корпоративной сети;
- выполнить ту же операцию в системе управления сайтом.

С помощью модуля **AD/LDAP интеграция** можно установить соответствие между группами пользователей корпоративной сети и группами пользователей системы управления сайтом. Это позволит организовать централизованное управление всеми группами пользователей корпоративной информационной системы.

В руководстве приводится описание, основные возможности и механизм работы модуля **AD/LDAP интеграция** системы *"1С-Битрикс: Управление сайтом"*. Так же рассматривается механизм настройки модуля и задания соответствий групп пользователей сайта и корпоративной сети.

⚠ ***Примечание**: работа модуля **AD/LDAP интеграция** системы "1С-Битрикс: Корпоративный портал" абсолютно идентична работе модуля системы "1С-Битрикс: Управление сайтом". Поэтому в руководстве слово «сайт» можно рассматривать как синоним слова «корпоративный портал»*

Глава 1. Основные возможности модуля

Модуль **AD/LDAP интеграция** реализован с учетом особенностей работы **LDAP** (**Lightweight Directory Access Protocol**) и **AD** (**Active Directory**) протоколов, один из которых должен быть установлен на корпоративном сервере.

В основе работы перечисленных протоколов лежит принцип хранения информации в виде записей, обладающих набором атрибутов и хранящихся в базе данных с древовидной иерархической структурой. Таким образом, при настройке на сервере локальной вычислительной сети **LDAP** или **AD** протокола информация о группах пользователей будет представляться в следующем виде (Рис. 1.1):

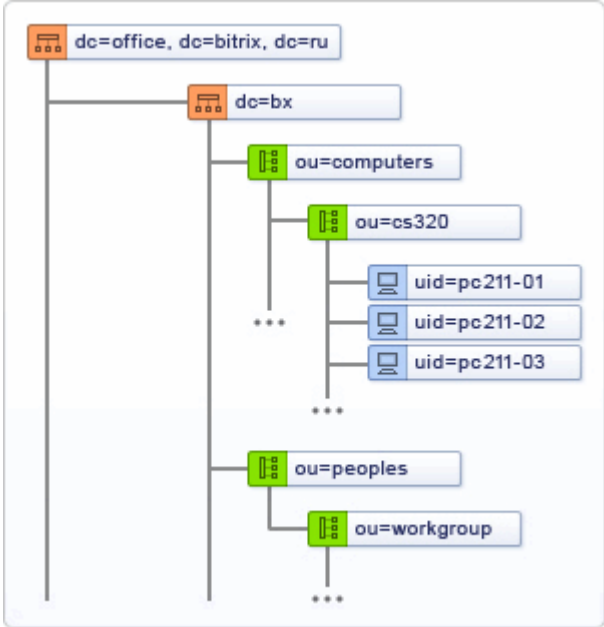

Рис. 1.1 Структура записей

Используя данную структуру хранения данных, модуль **AD/LDAP интеграция** позволяет настраивать соответствие групп пользователей корпоративной сети группам пользователей сайта.

Соответствие групп пользователей задается в специальной **Таблице соответствий** в административном разделе сайта. При этом возможно несовпадение имен групп пользователей сайта с именами групп пользователей корпоративной сети. Например, группе пользователей корпоративной сети **Techsupport**, к которой относятся сотрудники технической поддержки корпоративной сети, может быть поставлена в соответствие группа пользователей **Techsupport stuff**, созданная на сайте. Теперь сотрудники службы технической поддержки корпоративной сети смогут выполнять обязанности сотрудников службы технической поддержки сайта.

Группы пользователей внутри компании обладают правами на доступ к определенным ресурсам корпоративной сети, а сопоставленные им группы пользователей на сайте обладают правами на доступ к ресурсам сайта. Например, группа пользователей **Techsupport** наделена правами на доступ к почтовому серверу сети, а группа пользователей сайта **Techsupport stuff** обладает правами на доступ к модулю **Техподдержка**.

В соответствии с приведенным выше примером, пользователь, относящийся к группе **Techsupport** корпоративной сети, при попытке авторизации на сайте будет добавлен в группу пользователей сайта **Techsupport stuff**. После чего в системе автоматически будет заведен бюджет данного пользователя, на основе его данных, которые хранятся на корпоративном сервере.

Допустима привязка пользователя к одной, двум или более группам. В системе могут быть настроены группы пользователей, для которых не установлено соответствие с группами пользователей в корпоративной сети. Принадлежность пользователей к такой группе задается вручную администратором системы. Все изменения бюджета пользователя на корпоративном сервере будут автоматически учтены в бюджете пользователя в системе управления сайтом во время его следующей авторизации. Изменения затронут только те группы, для которых задано соответствие группам пользователей корпоративной сети.

Таким образом, модуль **AD/LDAP интеграция** позволяет:

- интегрировать систему *"1С-Битрикс: Управление сайтом"* в корпоративную сеть;
- настроить соответствие групп пользователей корпоративной сети и групп пользователей сайта;
- автоматически создавать бюджет пользователя после его регистрации исходя из **Таблицы соответствий** (данные для создания бюджета пользователя запрашиваются из базы данных корпоративного сервера);
- централизованно управлять изменениями бюджетов пользователей системы через корпоративный сервер.

Модуль **AD/LDAP интеграция** так же позволяет использовать **NTML авторизацию**. Чтобы ею воспользоваться, нужен веб-сервер **IIS** или **Apache** с модулем **mod_ntlm** или **mod_auth_sspi**.

Глава 2. Схема работы модуля

Общая схема работы модуля может быть описана следующей последовательностью действий:

1. Пользователь заходит на сайт и авторизуется (вводит логин и пароль, используемый для авторизации в корпоративной сети);
2. Система обращается к указанному в настройках AD/LDAP серверу и проверяет наличие пользователя с указанными данными (паролем и логином) в базе пользователей на корпоративном сервере:
   - если пользователя с такими данными в корпоративной сети не существует, то система запрещает вход на сайт;
   - если пользователь существует, то определяется группа пользователей корпоративной сети, к которой он относится, и сопоставленная ей группа пользователей сайта (с помощью **Таблицы соответствий**).
3. Далее проверяется наличие бюджета данного пользователя в системе:
   - если бюджет пользователя не найден, то система получает данные о пользователе из базы данных корпоративного сервера и создает его бюджет.
   - Если бюджет пользователя в системе уже был создан, т. е. пользователь уже авторизовался на сайте, то система проверяет, были ли произведены какие-либо изменения с бюджетом пользователя на корпоративном сервере. Если да, то соответствующие изменения производятся и с бюджетом пользователя в системе управления сайтом.
4. Пользователь получает разрешение на доступ к ресурсам сайта и авторизуется. Права пользователя определяются в зависимости от настроек группы пользователей сайта, к которой он был приписан.

⚠ ***Примечание**: если пользователь сайта, принадлежащий группе (одной или нескольким) из **Таблицы соответствий**, будет удален из списка пользователей корпоративной сети, то при попытке получить доступ к ресурсам сайта он получит отказ в авторизации. При этом бюджет этого пользователя будет сохранен в системе управления сайтом.*

⚠ ***Примечание**: чтобы разрешить такому пользователю авторизацию на сайте через стандартный интерфейс, в настройках данного пользователя в административном разделе сайта нужно установить значение поля со списком **Тип авторизации** равным **внутренняя проверка** и обновить регистрационную информацию (логин и пароль).*

⚠ ***Примечание**: если в **AD** дереве существует N-доменов (например, соответствуют подразделениям компании OD1, OD2…) и в этих доменах есть группы с одинаковыми именами, то в **Таблице соответствий** эти группы будут отображены N-раз. Для избегания путаницы в настройках AD/LDAP сервера можно поменять **Атрибут названия группы**, указав, например, **DistinguishedName (DN)**. В итоге вместо названий групп будут отображены **DN** групп.*

Глава 3. Настройка AD/LDAP авторизации

Настройка модуля **AD/LDAP интеграция** производится в административном разделе сайта на странице **AD/LDAP интеграция** (*Настройки* > *Настройки продукта* > *Настройки модулей* > *AD/LDAP интеграция*). Ее удобнее производить после создания сервера LDAP. Описание настроек модуля дано ниже.

Создание сервера

Создайте запись с указанием сведений о корпоративном сервере, база данных которого будет использована для установления соответствий групп пользователей, параметров сервера и соответствия групп пользователей.

Каждая запись регламентирует доступ к одному корню дерева каталогов. Если сведения о группах пользователей корпоративной сети хранятся в базах данных нескольких серверов или в нескольких базах данных одного сервера, то следует создать несколько записей, регламентирующих доступ к ним.

Переход к форме создания сервера (Рис. 3.1) осуществляется по ссылке **Создать**, расположенной на форме **импорта пользователей**, или с помощью кнопки **Добавить**, расположенной на контекстной панели страницы **AD/LDAP** (*Настройки* > *AD/LDAP*).

⚠ ***Примечание**: Данные для заполнения полей необходимо запросить у системного администратора.*

На закладке **Сервер** формы указываются сведения о корпоративном сервере и параметры доступа к базе данных групп пользователей, расположенной на нем.

⚠ ***Примечание**. При редактировании существующего сервера, кроме нижеперечисленных полей становятся доступными еще поля: **Код** и **Последнее изменение**.*

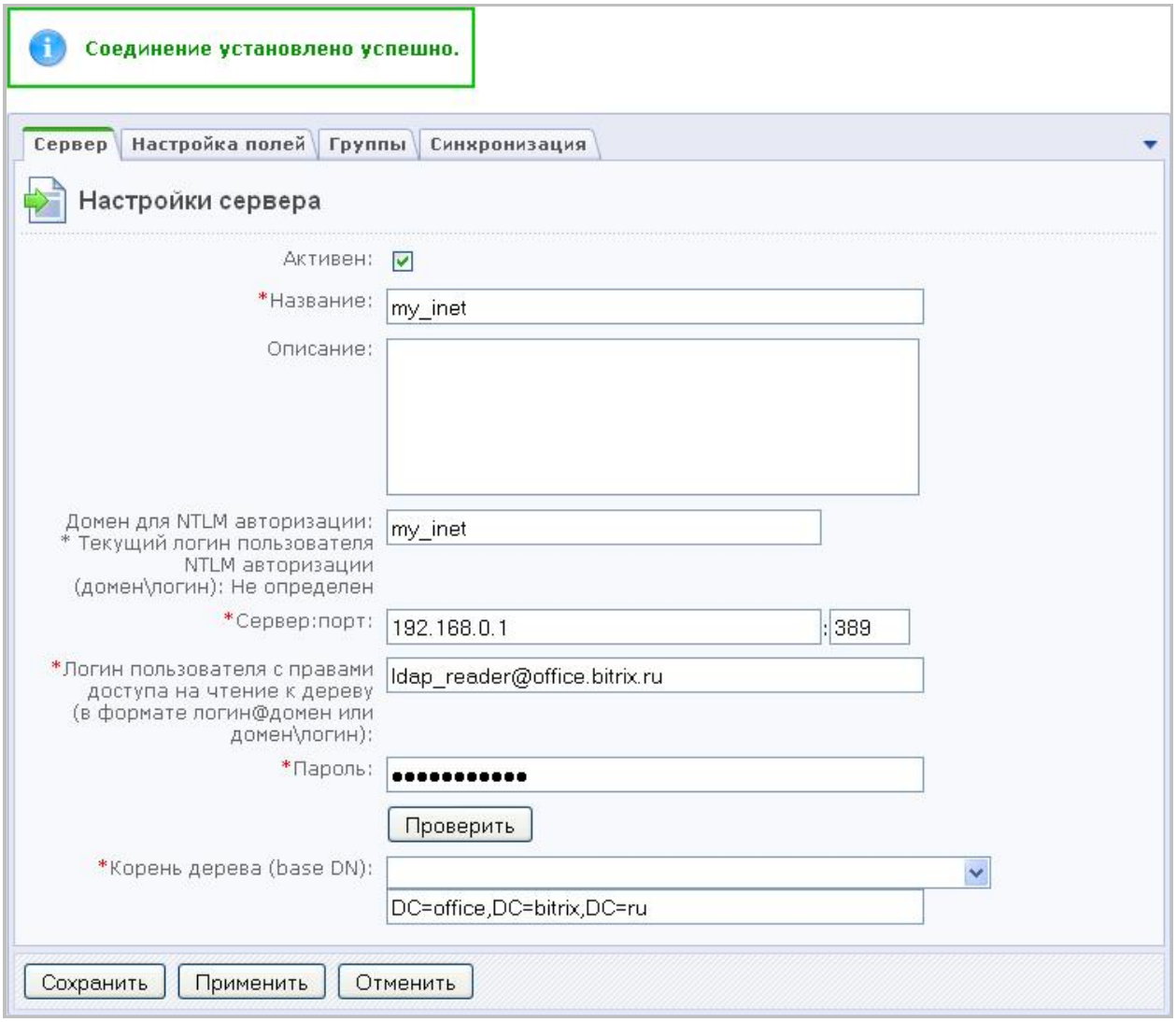

Рис. 3.1 Создание сервера

Ø Заполните поля на закладке **Сервер** (Рис. 3.1):

- **Активен** - при авторизации пользователя поиск его бюджета будет осуществлен в соответствии с параметрами данной записи.
- **Название** - укажите название на латинице.
- **Описание** - произвольное описание создаваемой записи.
- **Домен для NTLM авторизации** - используется для определения нужного **AD\LDAP** сервера при авторизации в виде **<домен\логин>**(задается на латинице), а также при автоматической NTLM авторизации (должно соответствовать домену организации).

Такой вид будет указывать на конкретную запись, в соответствии с которой должен быть осуществлен поиск бюджета пользователя на корпоративном сервере. Если имеется несколько **LDAP**-серверов, то использование этого поля становится необходимым, так как на разных серверах могут быть пользователи с одинаковым именем. В этом случае с помощью мнемонического имени будет определяться запись, указывающая на сервер и корень дерева каталогов, в котором следует искать бюджет пользователя, используемый для его авторизации на сайте.

- **Сервер:порт** - задается адрес корпоративного сервера с базой данных групп пользователей и порт, по которому к нему будет осуществляться обращение (389 порт является стандартным для обращения к **LDAP** серверу).
- **Логин пользователя с правами доступа на чтение к дереву** - указывается логин для выполнения административного входа на сервер (в формате **логин@домен** или **домен\логин**).
- **Пароль** - указывается пароль для выполнения административного входа на сервер.

⚠ ***Примечание**: для проверки введенных выше данных и установления пробного соединения с сервером служит кнопка **Проверить**. В случае если проверка была произведена успешно, сервер возвратит список доступных корней деревьев. Если же при проверке произошла ошибка, то вверху страницы будет выведена надпись красного цвета с указанием причины ошибки.*

- **Корень дерева (base DN)** - в появившемся после успешной проверки поле со списком выбирается корень дерева каталогов, в котором будет осуществляться поиск бюджетов авторизуемых пользователей:

Ø Перейдите в закладку **Настройка полей** (Рис. 3.2). На этой закладке необходимо провести настройку соответствий полей, выбираемых при импорте.

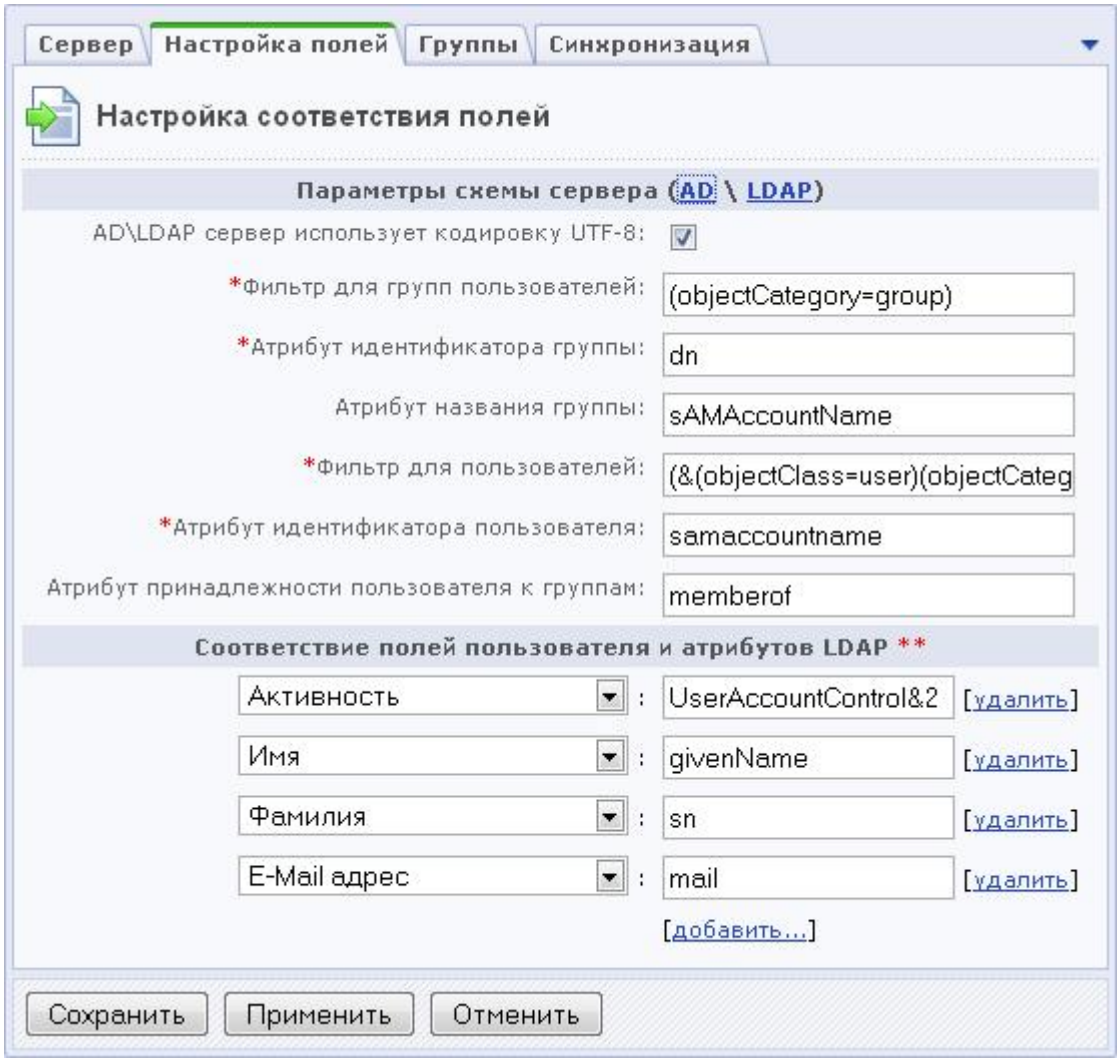

Рис. 3.2 Настройка полей сервера

Стандартные значения данных параметров как для **LDAP**, так и для **AD** сервера подставляются в поля формы автоматически.

Ø Чтобы автоматически настроить данные, нажмите на ссылку **AD** или **LDAP** в зависимости от сервера (Рис. 3.2).

Если вам необходимо добавить поля в групп **Соответствие полей пользователя и атрибутов AD (LDAP)**, то воспользуйтесь ссылкой **добавить…**. В настройках **LDAP**-сервера необходимо указывать минимально необходимые поля, такие как **Активность**, **Имя**, **Фамилия**, **E-Mail адрес**, т.е. поля которые необходимо постоянно переносить (синхронизировать из **AD**). Остальные поля можно настроить при импорте в форме **импорта пользователей** в закладке **Настройка полей**.

Каждое из полей, добавленное в эту группу будет проверяться на изменения при синхронизации и, при несоответствии, изменяться на стороне *"1С-Битрикс: Управление сайтом"*. То есть, если пользователь изменил какое-либо поле в своем профиле на сайте, то при последующей синхронизации полю будет возвращено прежнее значение.

Поэтому рекомендуется при первичном импорте пользователей добавить максимально возможное число полей, а после импорта, если используется периодическая синхронизация, удалить поля, которые не нуждаются в периодической проверке.

Ø Перейдите на закладку **Группы**.

Ø Чтобы добавить названия групп пользователей в таблицу, нужно нажать кнопку **Обновить список групп** (Рис. 3.3). Параллельно будет произведена проверка параметров, введенных в предыдущих разделах.

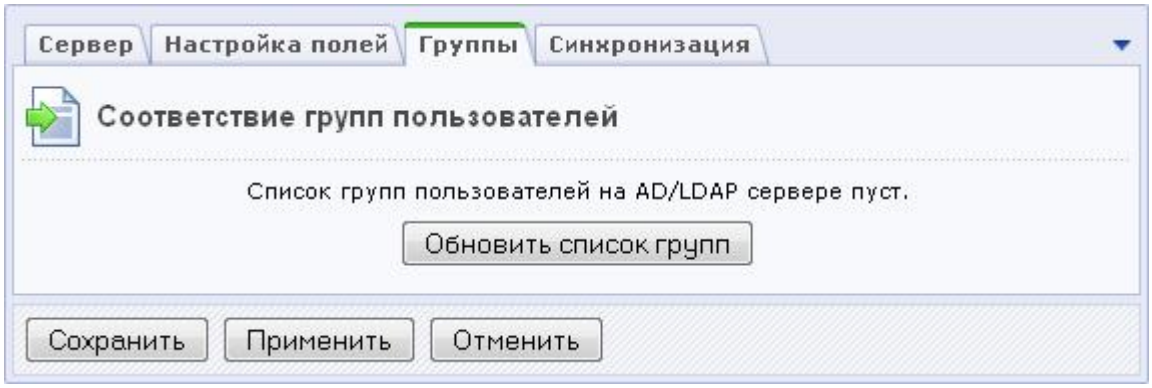

Рис. 3.3 Закладка Группы

После обновления списка групп пользователей в данном разделе отобразится **Таблица соответствий**, строки которой имеют формат выпадающий список (Рис. 3.4):

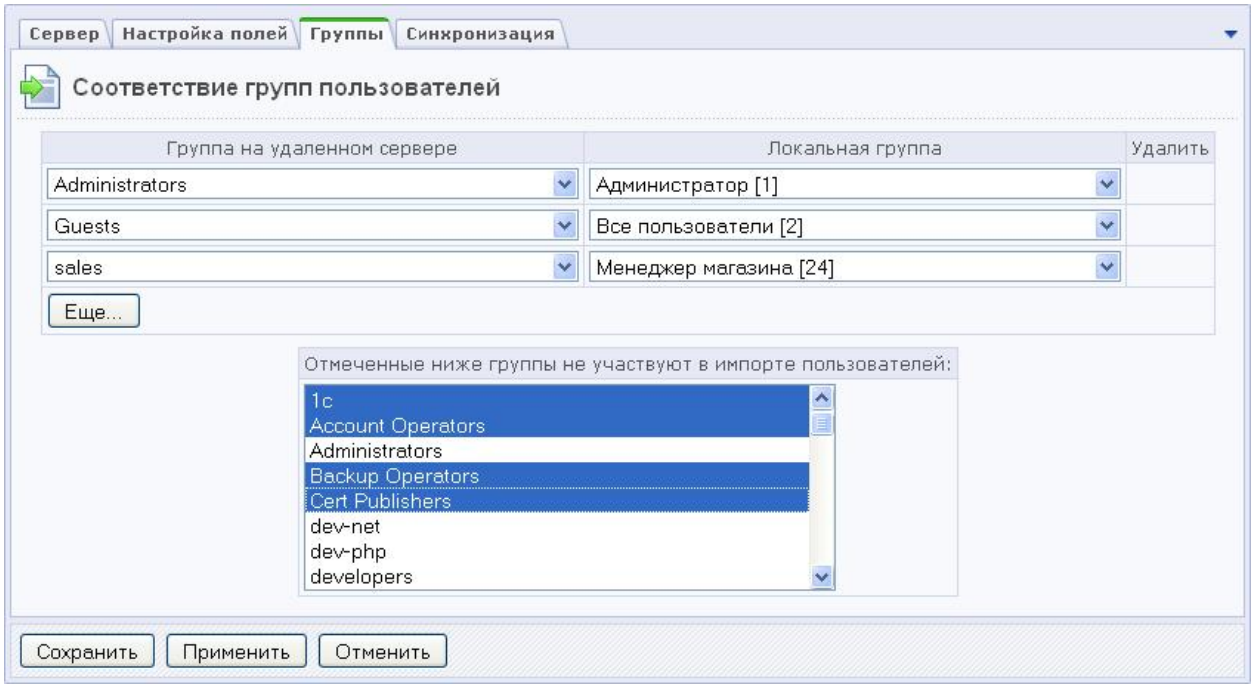

Рис. 3.4 Настройка соответствий групп пользователей

Ø Выполните настройку соответствий групп пользователей: выбирая группы на удаленном сервере, назначьте им в соответствие группы на корпоративном портале.

Ø При необходимости в поле **Отмеченные ниже группы не участвуют в импорте пользователей** укажите группы, которые не должны участвовать в импорте. Группы, отмеченные в этом поле не будут участвовать в импорте, даже если они будут выбраны в качестве источника в колонке **Группа на удаленном сервере**.

В столбце таблицы **Группа на удаленном сервере** осуществляется выбор групп пользователей корпоративной сети. В столбце **Локальная группа** выбираются группы пользователей сайта, которые ставятся в соответствие группам пользователей корпоративной сети. Таким образом, в одной строке таблице будет размещена группа пользователей корпоративной сети и поставленная ей в соответствие группа пользователей сайта.

Для того, чтобы удалить строку соответствия из таблицы, нужно установить флажок в поле **Удалить** и нажать кнопку **Применить**.

С помощью кнопки **Еще…** производится добавление пустых строк в **Таблицу соответствий**.

Если необходимо пользователей из одной и той же группы на сервере прописать в две разные локальные группы на корпоративном портале, то выберите эту группу в колонке **Группа на удаленном сервере** несколько раз и для каждой строки назначьте свои группы в колонке **Локальная группа**.

Если в качестве **Локальной группы** в двух строках выбрана одна из имеющихся групп, а в **Группах на удаленном севере** – две разных, то в группу добавятся только те пользователи, которые есть в обеих группах.

Ø Перейдите на закладку **Синхронизация** (Рис. 3.5).

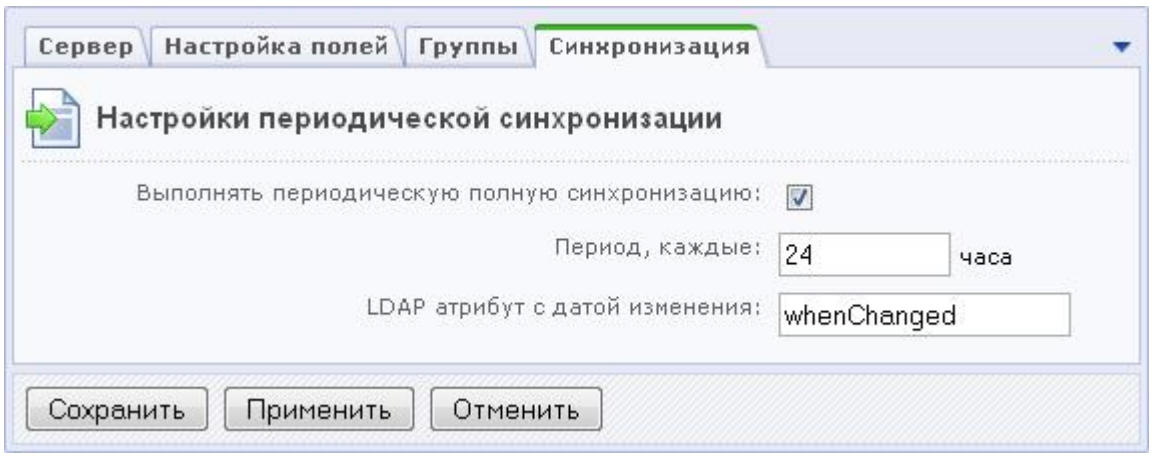

Рис. 3.5 Настройка периодической синхронизации

Если есть необходимость обеспечить периодическую синхронизацию баз, то:

Ø Установите флаг в поле **Выполнять периодическую полную синхронизацию**. Станут активными поля, расположенные ниже.

Ø Введите периодичность синхронизации в часах в поле **Период, каждые**.

Ø Введите **LDAP атрибут с датой изменения** для ведения лога изменений.

⚠ ***Примечание**: для периодической синхронизации удобно использовать **Агенты** - технология, позволяющая запускать необходимые функции во время обычной жизни сайта/корпоративного портала без использования каких-либо внешних программ. Подробней об использовании агентов смотрите в пользовательской документации продукта.*

Ø Сохраните внесенные изменения с помощью кнопки **Сохранить**.

После сохранения запись будет добавлена в список на странице **AD/LDAP** (Рис. 3.6):

		ID	Дата изм.	Название	Акт.	UTF-8	Симв.код	Сервер
☐		2	11.11.2009 10:45:08	My Server	Да	Да		192.168.0.1
☐		1	11.11.2009 10:28:01	Сервер Active Directory	Да	Да		192.168.1.1
Выбрано: 2	Отмечено: 0							

Рис. 3.6 Список серверов

NTLM-авторизация

Поддержка **NTLM-авторизации** по умолчанию включена в дистрибутив продукта. Для этого пакет модулей сервера **Apache**, поставляемого в составе пакета *"Битрикс: Веб-окружение"* включен модуль **mod_auth_sspi**. Если вы не используете рекомендуемый компанией "1С-Битрикс" пакет, то вам необходимо сделать следующее:

Ø Загрузите модуль **mod_auth_sspi** по ссылке http://sourceforge.net/projects/mod-auth-sspi/.

Ø Скопируйте его в папку *c:\<путь_до_папки>\apache\modules*.

Ø В файле **httpd.conf** добавьте строку

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so.
```

Ø В файле **.htaccess** добавьте следующие строки:

```
AuthName "My Intranet"
AuthType SSPI
SSPIAuth On
SSPIPackage NTLM
SSPIDomain MYDOMAIN
SSPIPerRequestAuth On
SSPIAuthoritative On
SSPIOfferBasic On
Require valid-us
```

⚠ ***Примечание**: при использовании стандартного пакета "Битрикс: Веб-окружение" указанные строчки в этом файле необходимо **раскомментировать**.*

Дальнейшие действия одинаковы как для использования пакета *"Битрикс Веб-окружение"*, так и для тех, кто использует другие способы установки продукта.

Ø В строке **SSPIDomain MYDOMAIN** файла смените **MYDOMAIN** на имя вашего домена.

Ø Сохраните внесенные изменения.

Настройка модуля

Ø В административном разделе перейдите на станицу настроек модуля **AD/LDAP интеграция** (*Настройки > Настройки продукта > Настройки модулей > AD/LDAP интеграция*) (Рис. 3.7).

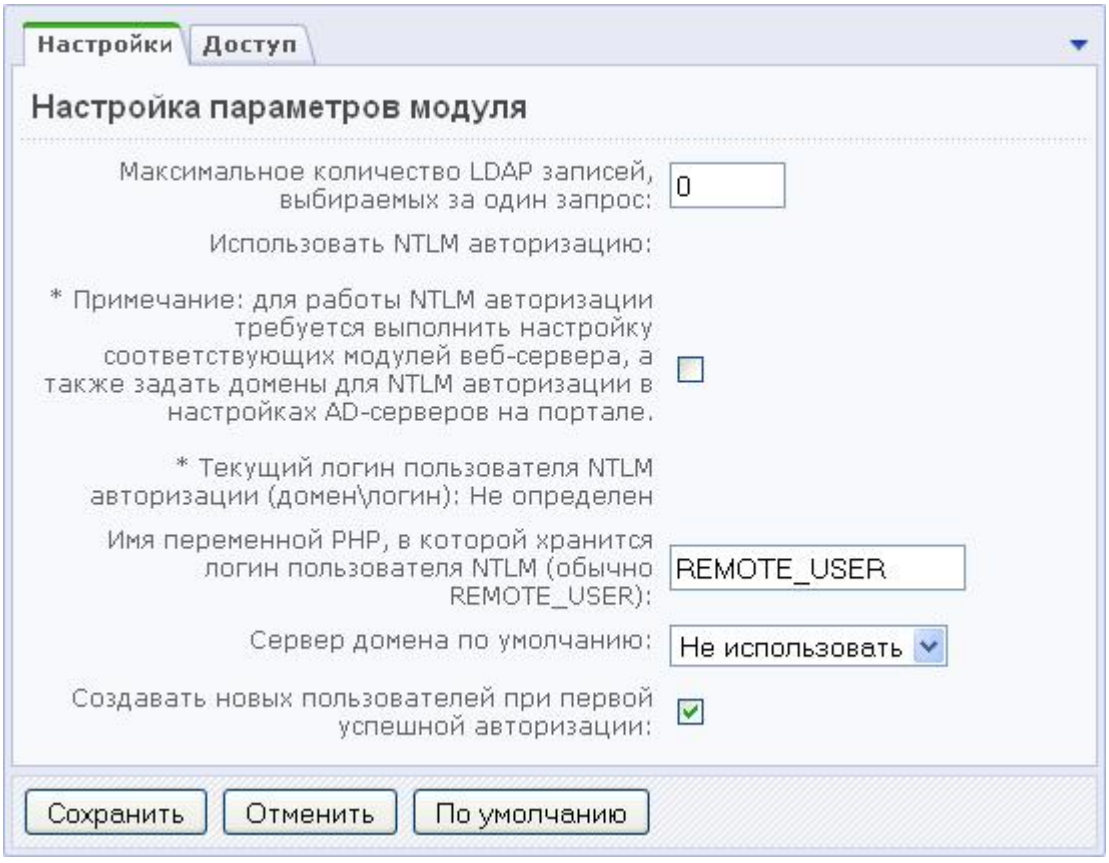

Рис. 3.7 Настройки модуля AD/LDAP интеграция

Ø В поле **Ограничение по количеству одновременно выбираемых LDAP записей** установите число отличное от **0**.

⚠ ***Примечание**: при большом числе одновременно регистрирующихся пользователей возможно замедление работы **LDAP**-сервера. Выбор конкретного числа одновременно обрабатываемых записей необходимо подобрать опытным путем в зависимости от конкретных условий.*

Ø Если используется NTLM авторизация, то установите флажок в поле **Использовать NTLM авторизацию**.

Ø Если в силу каких-то причин вы используете для хранения логина пользователя в другой переменной массива **$_SERVER**, то в поле **Имя переменной PHP, в которой хранится логин пользователя NTLM** измените имя переменной на нужное. Учтите при этом, что большинство модулей продукта используют именно переменную **REMOTE_USER**.

⚠ ***Примечание**: в поле **REMOTE_USER** содержится значение **логин** или **домен\логин**. Вся аутентификация происходит на уровне веб-сервера без каких либо паролей, хешей и т.д.*

Ø Если в локальной сети используется несколько **LDAP**-серверов, то в поле **Сервер домена по умолчанию** необходимо выбрать тот, который используется для NTML-авторизации.

Ø При необходимости поставьте флажок в поле **Создавать новых пользователей при первой удачной авторизации**. Использование этой опции позволяет не дожидаться очередной автоматической синхронизации данных новому пользователю, добавленному в LDAP-сервер.

Ø Сохраните внесенные изменения.

⚠ ***Примечание**. Опция **Создавать новых пользователей при первой удачной авторизации** при использовании протокола AD позволяет «зафиксировать» пользователей, имеющих доступ к сайту. Напроимер, создается пять учетных записей, снимется флажок с опции и вход в систему имеют только указанные пять пользователей.*

⚠ ***Примечание**: необходимо помнить, что компьютер, на котором размещен сервер **Apache,** должен быть включен в домен **Windows**.*

⚠ ***Примечание**: в некоторых случаях при работе с **Internet Explorer** возможны ситуации сбоя в работе "1С-Битрикс: Корпоративный портал". Проблема выражается в сбое в работе кнопок в административной и публичных частях. Для решения этой проблемы добавьте в корневой файл **.htaccess** строку **SSPIPerRequestAuth On**.*

Глава 4. Импорт из LDAP-directory

Чтобы осуществить импорт пользователей из LDAP-directory, выполните следующее:

Ø Перейдите на страницу **Импорт пользователей** (*Настройки* > *Пользователи* > *Импорт пользователей*).

Ø В форме импорта пользователей в качестве источника данных выберите **Active Directory / LDAP** и нажмите кнопку **Далее** (Рис. 4.1):

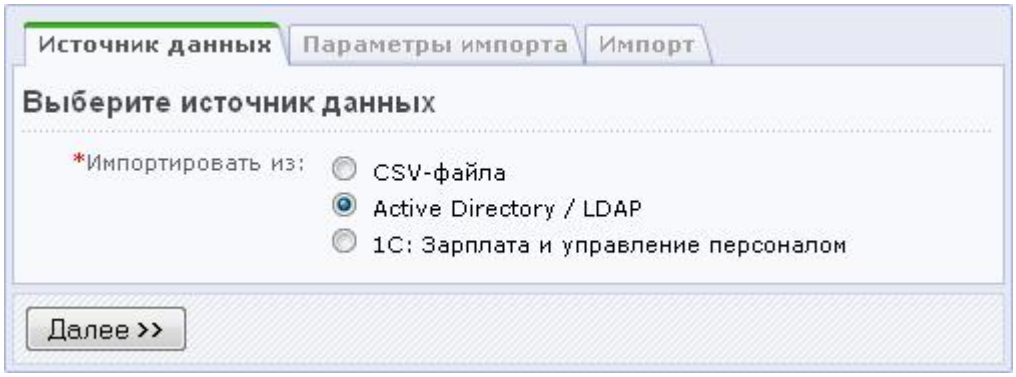

Рис. 4.1 Выбор источника данных

Ø На втором шаге импорта (закладка **Параметры импорта**) в выпадающем списке выберите сервер, который будет использован для импорта и нажмите кнопку **Далее** (Рис. 4.2).

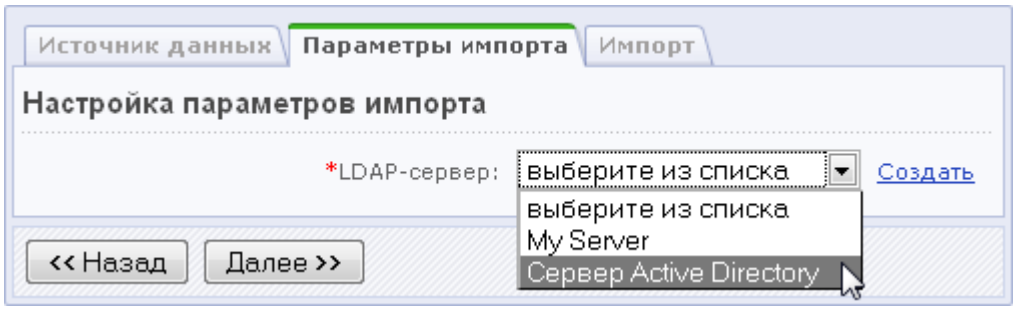

Рис. 4.2 Выбор сервера

⚠ ***Примечание**: если сервер еще не настроен, то нажмите на ссылку **Создать**. Откроется форма создания AD/LDAP-сервера (описание процедуры создания сервера смотрите выше в разделе **Создание сервера**).*

Ø После выбора сервера в форме появятся импортируемые поля (Рис. 4.3). При необходимости вы можете снять флажки с дополнительных полей, которые не нужно импортировать.

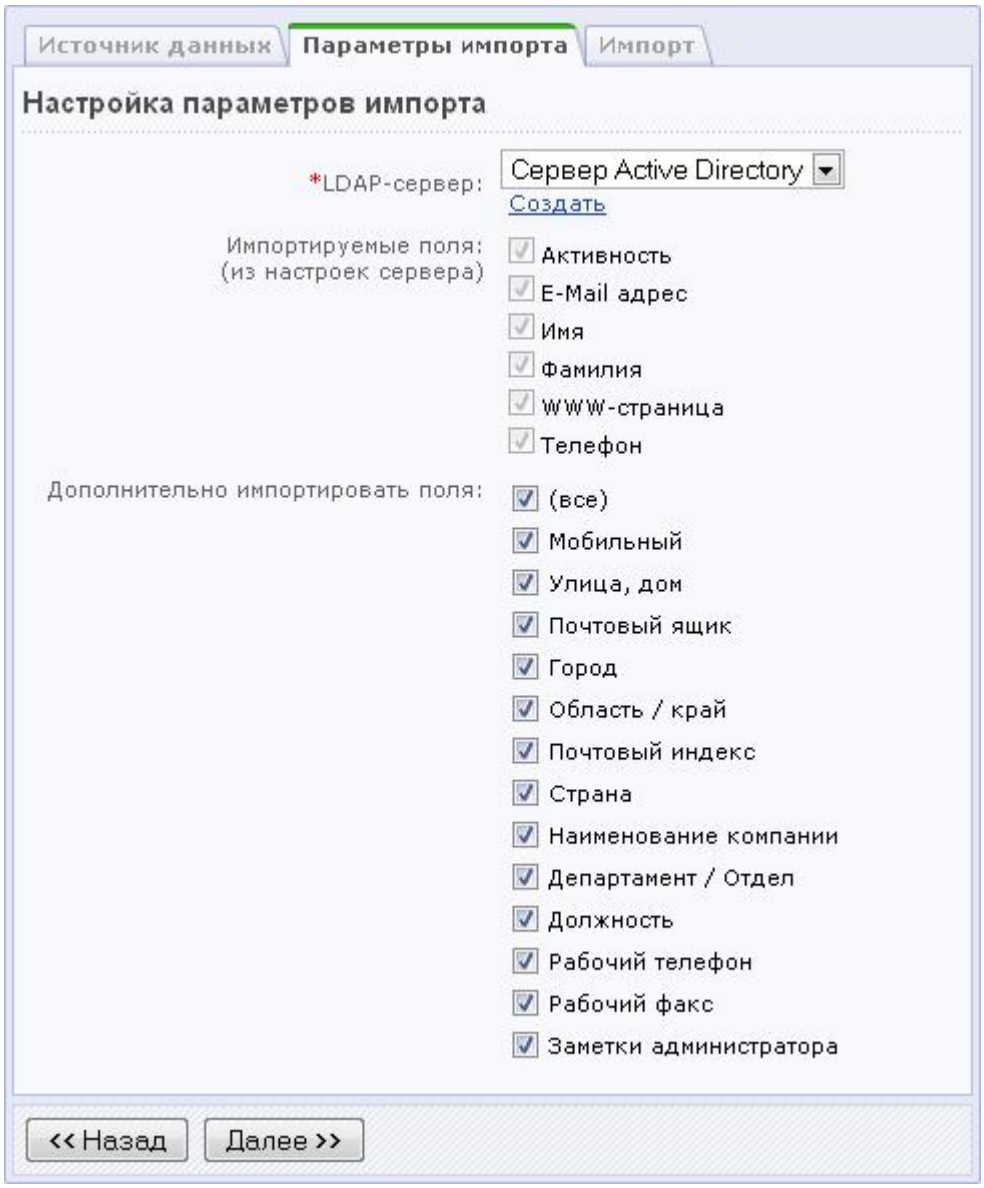

Рис. 4.3 Импортируемые поля

Ø Нажмите кнопку **Далее**. Мастер перейдет к третьему шагу. Будет автоматически произведен импорт, система сообщит об его завершении и количестве добавленных записей.

Заключение

В руководстве рассмотрена работа и настройка модуля **AD/LDAP интеграция**, параметры настройки **NTML-авторизации**.

При возникновении вопросов по работе модуля обращайтесь на форумы компании ″1С-Битрикс″:

http://dev.1c-bitrix.ru/community/forums/

Если у вас возникнут вопросы в ходе работы с продуктом, вы можете обратиться в службу **Технической поддержки** компании "1С-Битрикс":

http://dev.1c-bitrix.ru/support/.