



# 1С-Битрикс: Управление сайтом

Курс «Администратор. Модули»





## Содержание

<b>Введение</b> .....	<b>3</b>
<b>AD/LDAP интеграция</b> .....	<b>4</b>
НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ МОДУЛЯ.....	4
СХЕМА РАБОТЫ МОДУЛЯ .....	6
НАСТРОЙКА МОДУЛЯ.....	7
ПРИНАДЛЕЖНОСТЬ ПОЛЬЗОВАТЕЛЕЙ К ПОДРАЗДЕЛЕНИЯМ НА AD-СЕРВЕРЕ .....	8
РЕГИСТРАЦИЯ СЕРВЕРА.....	9
NTLM-АВТОРИЗАЦИЯ .....	15
NTLM АВТОРИЗАЦИЯ НА LINUX .....	16
Немного теории .....	16
Файл bx_ntlm.php.....	17
Настройка «1С-Битрикс: 1С-Битрикс: Управление сайтом».....	17
Настройка браузеров сотрудников .....	18
ПРОВЕРКА РАБОТЫ LDAP .....	20
Пример использования скрипта.....	21
ПРОБЛЕМЫ И РЕШЕНИЯ .....	23
После изменения профиля AD пользователя данные возвращаются в исходное значение. ....	23
Для AD-пользователей не работает галка "Запомнить меня на этом компьютере" .....	23
Доступ к разделу Extanet без NTLM .....	23
ИМПОРТ ПОЛЬЗОВАТЕЛЕЙ.....	24



## Введение

---

Курс для пользователей, осуществляющих администрирование сайтов. Второй сертификат в линейке администрирования. Первый курс - Администратор. Базовый - дает базовые понятия по работе с системой "1С-Битрикс: Управление сайтом" и описывает работу модулей:

- Главный модуль,
- Управление структурой,
- Информационные блоки,
- Поиск.

Курс **Администратор. Модули** позволяет освоить методы выполнения расширенных задач по администрированию модулей, не относящихся к коммерческой деятельности.

Получаемые навыки:

- методы работы с модулями системы некоммерческого плана;
- работа с инструментами поисковой оптимизации и контроля за посещаемостью сайта;
- методы импорта пользователей с помощью сервера LDAP;
- организация документооборота и бизнес-процессов;
- работа с инструментами защиты сайта от несанкционированного доступа;
- работа с инструментами обеспечения жизнеспособности сайта при повышенной нагрузке;



## AD/LDAP интеграция

---

При проведении интеграции сайта с информационной системой организации может возникнуть потребность в разграничении прав сотрудников компании на доступ к ресурсам сайта и его управлению.

Стандартным решением данной задачи является создание нескольких групп пользователей сайта 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.

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

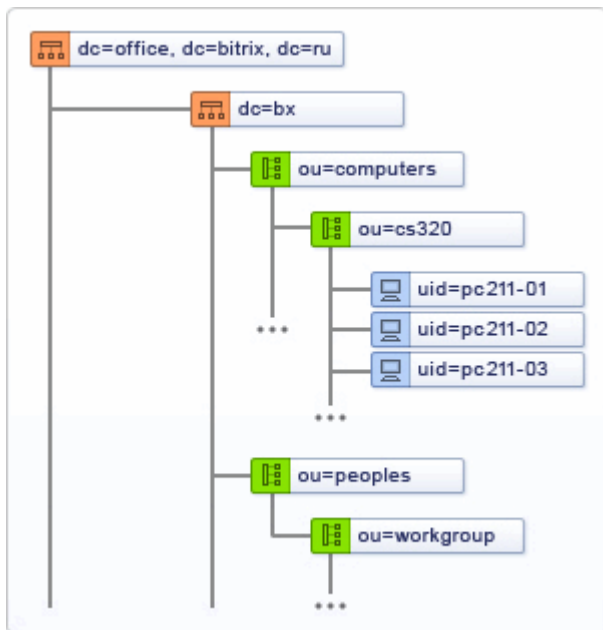
- изменить/создать бюджет пользователя в корпоративной сети;
- выполнить ту же операцию в системе управления сайтом.

Модуль **AD/LDAP интеграция** позволяет исключить подобные повторные операции и сократить затраты времени и труда на управление группами пользователей корпоративной информационной системы. С его помощью можно установить соответствие между группами пользователей корпоративной сети и группами пользователей системы управления сайтом, что позволяет организовать централизованное управление всеми группами пользователей корпоративной информационной системы.

В главе приводится описание основных возможностей и механизма работы модуля **AD/LDAP интеграция** системы **Bitrix Framework**. Так же здесь рассматриваются процессы настройки модуля и задания соответствий групп пользователей сайта и корпоративной сети.

### Назначение и возможности модуля

**AD/LDAP** модуль 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:



Используя данную структуру хранения данных, модуль **AD/LDAP** 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. В результате 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 **Техническая поддержка**.

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 данных, хранящихся 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. При этом изменения за-



тронут пользователей только тех групп, для которых задано соответствие группам пользователей корпоративной сети.

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

- интегрировать проекты, созданные на **Bitrix Framework** 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 **NTLM авторизацию**. Чтобы ею воспользоваться, нужен веб-сервер IIS или Apache с модулем **mod\_ntlm** или **mod\_auth\_sspi**.

### Схема работы модуля

Общая схема работы модуля может быть описана следующей последовательностью действий:

1. Пользователь заходит на сайт и авторизуется (вводится логин и пароль, используемые пользователем 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 выполнены какие-либо изменения в бюджете пользователя на корпоративном сервере. Если да, то соответствующие изменения выполняются и с бюджетом пользователя на сайте.
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.



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.

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.

## Настройка модуля

Настройка модуля осуществляется в административном разделе на странице настроек модуля **AD/LDAP интеграция**:

- Перейдите на страницу **Настройки модуля** (*Настройки > Настройки продукта > Настройки модулей > AD/LDAP интеграция*).

Настройка параметров модуля

E-mail для пользователей, у которых он не указан: no@email

Использовать NTLM авторизацию<sup>1</sup>:

Текущий логин пользователя NTLM авторизации (домен\логин): Не определен

Имя переменной PHP, в которой хранится логин пользователя NTLM (обычно REMOTE\_USER): REMOTE\_USER

Сервер домена по умолчанию: Не использовать

Создавать новых пользователей при первой успешной авторизации:

Сохранить Отменить По умолчанию

- В поле **E-mail для пользователей, у которых он не указан** укажите e-mail для пользователей, не указавших его.
- Если используется NTLM авторизация, то установите флажок в поле **Использовать NTLM авторизацию**.



**⚠ Примечание:** Для работы NTLM авторизации требуется выполнить настройку соответствующих модулей веб-сервера, а также задать домены для NTLM авторизации в настройках AD-серверов на сайте.

- 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.

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

**⚠ Примечание:** опция **Создавать новых пользователей при первой удачной авторизации** при использовании протокола AD позволяет "зафиксировать" пользователей, имеющих доступ к сайту.

Например, создается пять учетных записей, снимется флажок с опции и вход в систему имеют только указанные пять пользователей.

- Сохраните внесенные изменения.

**⚠ 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: Управление сайтом**". Проблема выражается в сбое в работе кнопок в административной и публичных частях. Для решения этой проблемы добавьте в корневой файл **.htaccess** строку: `SSPIPerRequestAuth On`

## **Принадлежность пользователей к подразделениям на AD-сервере**

Необходимо специальным образом определить на AD-сервере принадлежность пользователей к подразделениям, иерархию подразделений компании, а также начальников подразделений. При импорте пользователей в «1С-Битрикс: Управление сайтом», эта структура также импортируется, при этом пользователям сразу назначаются нужные подразделения. Также, что более просто, можно задать одно фиксированное подразделение всем пользователям из AD.

Для задания структуры компании в AD используются всего 2 специальных свойства пользователя:



- **department** - символьное наименование подразделения, к которому относится данный пользователь.
- **manager** - DN (Distinguished name, уникальный идентификатор в AD) пользователя, являющегося начальником данного.

На основании этой связи и строится иерархия компании:

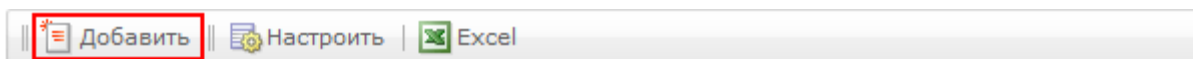
- Если начальник находится в другом подразделении, то это определяет связь между подразделениями: подразделение **manager**'а считается вышестоящим над данным. При этом текущий пользователь будет считаться начальником своего подразделения.
- Если **manager** - в том же подразделении, то никаких дополнительных действий предпринято не будет, и это единственный способ явно указать, что пользователь сам не является начальником подразделения. Из чего можно сделать вывод, что для всех подчиненных в подразделении должен быть задан начальник из него же.
- Если у пользователя не задано подразделение, но задан начальник, он считается принадлежащим тому же подразделению, что и начальник. Для начальника будут также действовать все те же правила и умолчания, так что такие "умолчательные" определения могут выстроиться в последовательную цепочку.
- Если задано подразделение, но нет начальника - данное подразделение попадает в корень структуры компании, и пользователь сам будет его начальником.
- Если же у пользователя нет ни подразделения, ни начальника, ему будет присвоено подразделение по умолчанию, задаваемое в настройках модуля.

## Регистрация сервера

Создание записи об AD/LDAP сервере выполняется в административном разделе сайта, в которой указываются все необходимые сведения о сервере 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.

- Перейдите на страницу **Active Directory/LDAP серверы** (*Настройки > AD/LDAP*) и нажмите кнопку **Добавить**, расположенную на контекстной панели.



Откроется форма создания новой записи.

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

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

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



Сервер    Настройка полей    Группы    Синхронизация

### Настройки сервера

Код: 1  
Последнее изменение: 01.12.2010 11:45:25

Активен:

\*Название:

Описание:

Домен для NTLM авторизации:

\* Текущий логин пользователя NTLM авторизации (домен\логин): Не определен

\*Сервер:порт:

\*Логин пользователя с правами доступа на чтение к дереву (в формате логин@домен или домен\логин):

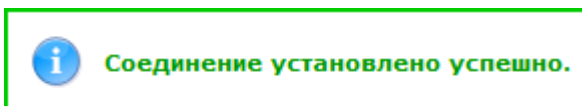
\*Пароль:

\*Корень дерева (base DN):

- **Активен** - отметьте данную опцию, чтобы при авторизации пользователя поиск его бюджета мог быть осуществлен в соответствии с параметрами данной записи.
- **Название** - укажите название создаваемой записи для обращения к ней в списке.
- **Описание** - произвольное описание создаваемой записи сервера.
- **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.

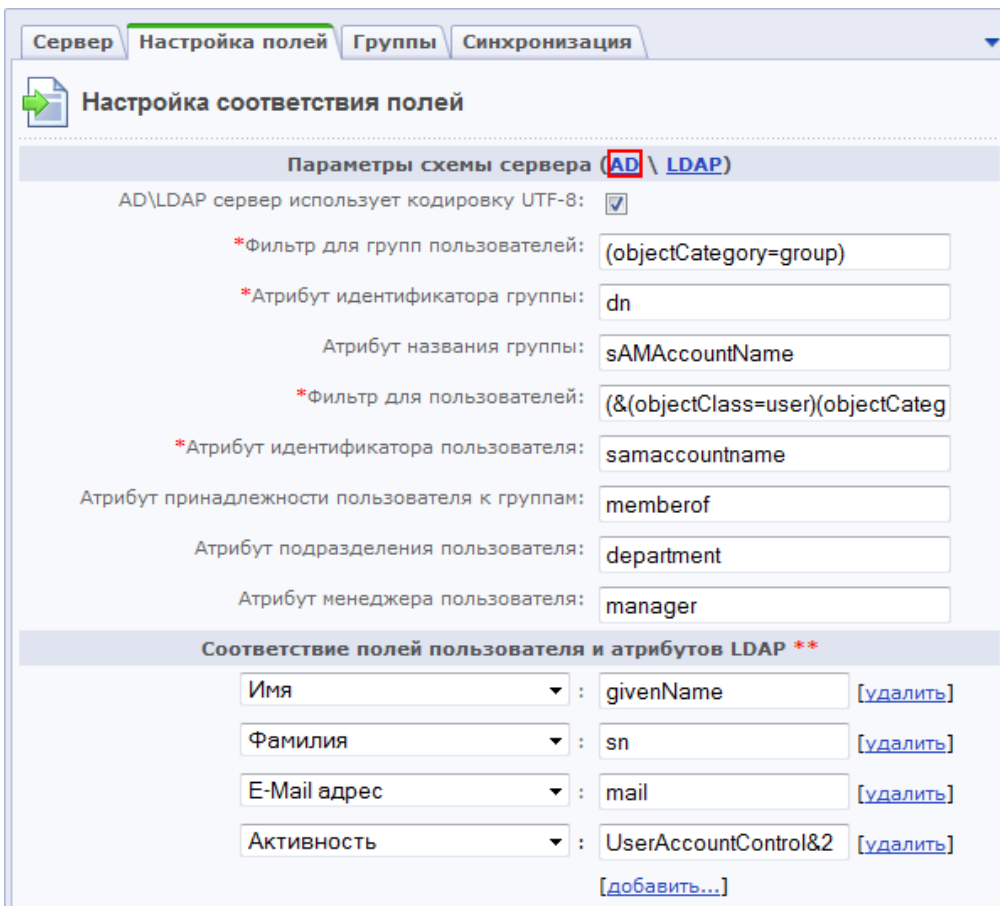
- **Сервер:порт** - укажите адрес корпоративного сервера с базой данных групп пользователей и порт, по которому к нему будет осуществляться обращение (**389** порт является стандартным для обращения к LDAP серверу).
- **Логин пользователя с правами доступа на чтение к дереву** - укажите логин для выполнения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



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** - укажите корень дерева каталогов, в котором будет осуществляться поиск бюджетов авторизуемых пользователей.
- На закладке **Настройка полей** указываются значения параметров для схемы данных бюджетов пользователей, хранимых на сервере.

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



Сервер **Настройка полей** Группы Синхронизация

**Настройка соответствия полей**

Параметры схемы сервера **AD \ LDAP**

AD\LDAP сервер использует кодировку UTF-8:

\*Фильтр для групп пользователей: (objectCategory=group)

\*Атрибут идентификатора группы: dn

Атрибут названия группы: sAMAccountName

\*Фильтр для пользователей: (&(objectClass=user)(objectCateg

\*Атрибут идентификатора пользователя: samaccountname

Атрибут принадлежности пользователя к группам: memberof

Атрибут подразделения пользователя: department

Атрибут менеджера пользователя: manager

Соответствие полей пользователя и атрибутов LDAP \*\*

Имя	:	givenName	[удалить]
Фамилия	:	sn	[удалить]
E-Mail адрес	:	mail	[удалить]
Активность	:	UserAccountControl&2	[удалить]

[добавить...]



Пользовательское поле	Атрибут LDAP	Действие
Имя	cn	удалить
Фамилия	sn	удалить
E-Mail адрес	email	удалить
Активность	UserAccountControl&2	удалить

Выбор типа сервера осуществляется путем нажатия ссылки с соответствующим названием в заголовке раздела.

Если стандартные значения данных параметров были изменены на корпоративном сервере, то соответствующие изменения нужно внести в значения параметров в форме.

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.

## Отделы и структура компании

Секция позволяет настроить параметры импорта структуры компании на сайт.



**Отделы и структура компании**

Импортировать структуру компании из AD:

Подразделение, внутрь которого будет импортирована структура компании: [Нет]

Импортировать в структуру компании пользователей, у которых не указано подразделение:

Название подразделения по умолчанию (пустое значение соответствует корневому подразделению данного сервера):

- Используйте опцию **Импортировать структуру компании из AD**, если хотите импортировать структуру компании из AD при синхронизации данных пользователей корпоративной сети с сайтом.
- Укажите **Подразделение, внутрь которого будет импортирована структура компании** с AD-сервера. Если выбрать **нет**, то структура будет импортироваться в корень дерева подразделений.

**⚠ Примечание:** Указание фиксированного места для импорта очень полезно, если в компании несколько филиалов, каждый со своим сервером. Тогда в структуре компании можно вручную создать подразделение для каждого филиала, и в настройках каждого сервера выбрать свое.

Если при импорте имена подразделений в AD совпадут с существующими на сайте - будут использованы существующие подразделения.

- Используйте опцию **Импортировать в структуру компании пользователей, у которых не указано подразделение** для того, чтобы пользователи, у которых не указано подразделение в Active Directory также импортировались в структуру сайта.
- Укажите **Название подразделения по умолчанию (пустое значение соответствует корневому подразделению данного сервера)** к которому будут причислены пользователи, у которых не указано подразделение.
- На закладке **Группы** осуществляется загрузка групп пользователей корпоративной сети и сайта в **таблицу соответствий** и задание соответствий этих групп.

Сервер    Настройка полей    **Группы**    Синхронизация

**Соответствие групп пользователей**

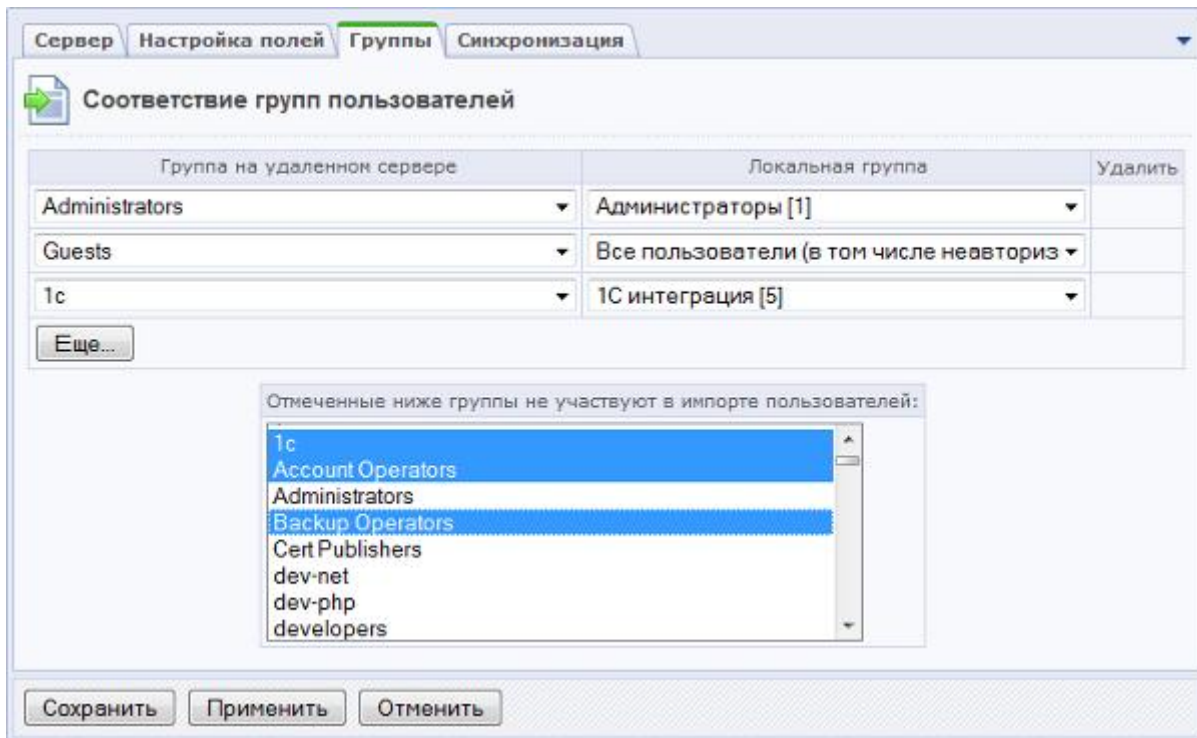
Список групп пользователей на AD/LDAP сервере пуст.

- Чтобы добавить названия групп пользователей в таблицу, нужно нажать кнопку **Обновить список групп**.



Параллельно будет произведена проверка параметров, введенных в предыдущих разделах.

После обновления списка групп пользователей в данном разделе отобразится **таблица соответствий**:



- 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 таблицы 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** выполняется добавление пустых строк в **таблицу соответствий**.
- 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**.

Если необходимо пользователей из одной и той же группы на сервере прописать в две разные локальные группы на сайте, 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 сервере** – две разных, то в локальную группу добавятся только те пользователи, которые есть в обеих группах.

- Если есть необходимость обеспечить периодическую синхронизацию баз, то перейдите на закладку **Синхронизация**:



- Поставьте флажок в поле **Выполнять периодическую полную синхронизацию**. Станут активными поля, расположенные ниже.
- Введите периодичность синхронизации в часах в поле **Период, каждые**.
- Введите атрибут **LDAP атрибут с датой изменения** для ведения лога изменений.

Для периодической синхронизации удобно использовать **Агенты** - технология, позволяющая запускать необходимые функции во время обычной жизни сайта без использования каких-либо внешних программ. Подробнее об использовании агентов смотрите в [пользовательской документации](#) продукта.

- Для сохранения записи и возврата к списку серверов нажмите кнопку **Сохранить**.
- После сохранения запись будет добавлена в список на странице **Active Directory/LDAP серверы**.

<input type="checkbox"/>	<input type="checkbox"/>	ID	Дата изм.	Название	Акт.	UTF-8	Симв.код	Сервер
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	22.09.2010 11:31:19	Corp	Да	Да	my_inet	192.168.0.1

Выбрано: 1 | Отмечено: 0

Для изменения или удаления записи нужно выбрать соответствующий пункт в меню действий выбранной записи.

## 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:

- [Загрузите](#) модуль **mod\_auth\_sspi**.
- Скопируйте его в папку `c:\<путь_до_папки>\apache\modules\.`
- В файле **httpd.conf** добавьте строку:

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

- 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
```

При использовании стандартного пакета **Битрикс: Веб-окружение** указанные строчки в этом файле необходимо не создавать, а раскомментировать.

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

- В строке **SSPIDomain MYDOMAIN** файла **.htaccess** смените **MYDOMAIN** на имя вашего домена.
- Сохраните внесенные изменения.

## NTLM авторизация на Linux

Для сайта наличие NTLM авторизации, т.е. возможности входить на без ввода логина/пароля (используя данные авторизации Windows на AD сервере), является крайне удобной особенностью. Техническая реализация не совсем простая, особенно когда сайт работает на Linux.

Рассмотрим вариант решения этой задачи.

Если говорить в общем, то вся настройка NTLM складывается из трех частей:

- настройка AD сервера в Битриксе;
- изменение параметров безопасности на клиенте;
- конфигурирование веб сервера.

Последняя часть самая сложная, кроме того, нет универсального рецепта для всех конфигураций. Если ваша установка отличается от описанных ниже, то вам придется самим искать варианты решений.

## Немного теории

Реализовать NTLM авторизацию на Linux возможно, так как браузер умеет передавать хеш пароля в NTLM запросе.

Если говорить упрощенно, браузер генерирует по определенному методу хеш пароля пользователя (модифицированный md4). Затем использует этот хеш в качестве ключа



для шифрования кодового слова, генерируемого веб-сервером в процессе авторизации. Важно отметить, существует два хеша: первый не передается через сеть, для пароля он постоянный, второй зависит от первого и меняется при каждой авторизации.

Если веб-сервер будет знать методы получения хешей и первый хеш пароля, то он сможет проверить подлинность пользователя. Первый промежуточный хеш можно получить, зная исходный пароль после успешной традиционной авторизации пользователя. Т.е. первый раз при входе на сайт пользователь должен ввести свой пароль в форме авторизации на самой странице. А затем для NTLM авторизации будет использоваться хеш пароля, сохраненный в дополнительном пользовательском поле (в моем случае оно заводится автоматически).

Традиционный NTLM требует постоянного соединения с веб-сервером, поэтому в прежних реализациях NTLM авторизации приходилось отказываться от nginx, что отрицательно сказывалось на производительности. В рекомендуемом способе такого ограничения нет.

### Файл `bx_ntlm.php`

- Скачайте файл [bx\\_ntlm.php](#)
- Разместите его в папке `/bitrix/php_interface/`
- Подключите файл к исполнению в `/bitrix/php_interface/init.php`:

```
require(dirname(__FILE__) . '/bx_ntlm.php');
```

### Настройка «1С-Битрикс: 1С-Битрикс: Управление сайтом»

Далее нужно зарегистрировать в системе [сервер AD/LDAP](#) и [настроить модуль AD/LDAP](#).

При настройка модуля учтите, что 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.

Помните при этом, что большинство модулей продукта используют именно переменную **REMOTE\_USER**. 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.

Если в локальной сети используется несколько LDAP-серверов, то в поле Сервер домена по умолчанию необходимо выбрать тот, который используется для NTLM-авторизации. Даже если LDAP-сервер один, то все равно желательно указать значение этого поля, чтобы сотрудникам не требовалось вводить домен при первом входе на сайт.

Надо обязательно включить опцию **Создавать новых пользователей при первой успешной авторизации**, чтобы хеши паролей хранились в локальной базе.

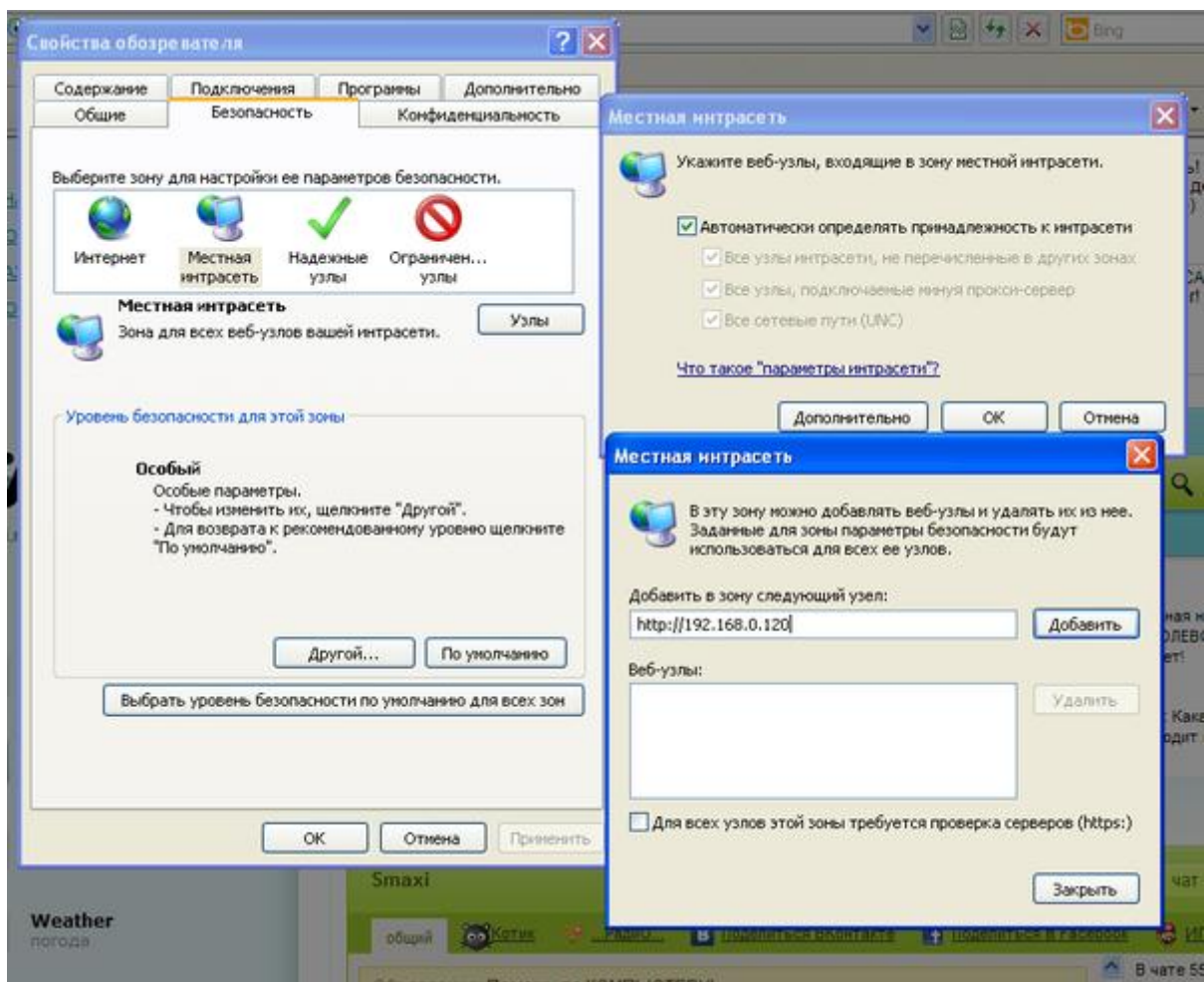


**⚠ Внимание !** В некоторых случаях при работе с Internet Explorer возможны ситуации сбоя в работе "1С-Битрикс: Управление сайтом". Проблема выражается в сбое в работе кнопок в административной и публичных частях. Для решения этой проблемы добавьте в корневой файл **.htaccess** строку: `SSPIPerRequestAuth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

## Настройка браузеров сотрудников

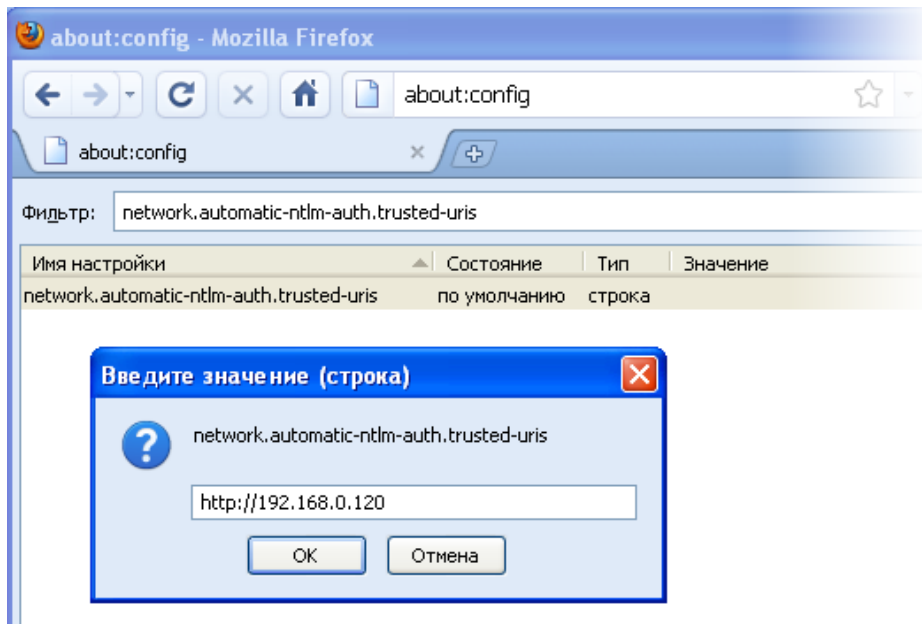
### Internet Explorer

Для успешной NTLM авторизации нужно, чтобы веб-сервер находился в зоне Local Intranet.



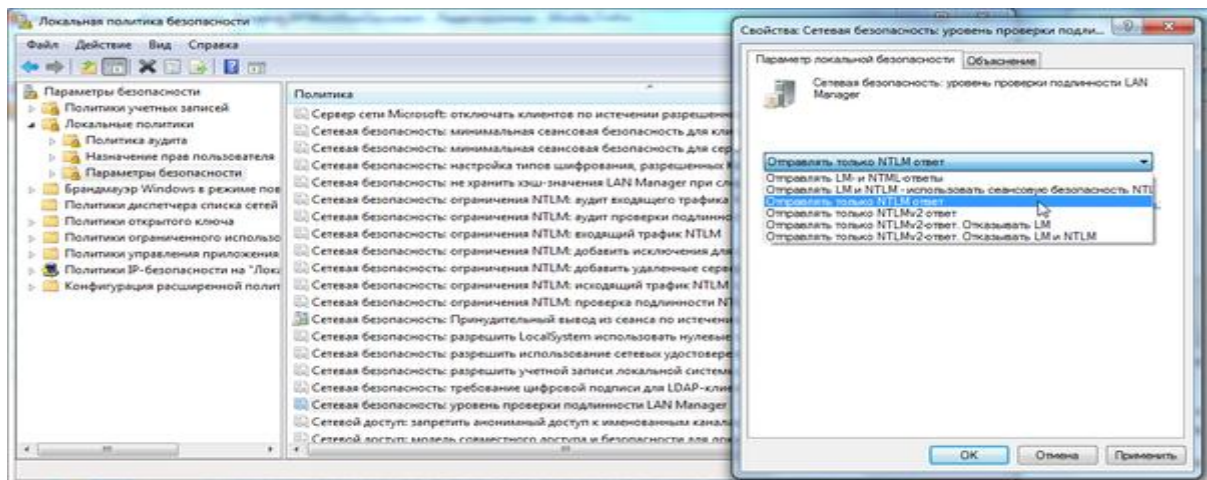
### Mozilla Firefox

Добавить веб-сервер к списку доверенных URI для автоматической NTLM-авторизации (через параметр `network.automatic-ntlm-auth.trusted-uris` на странице `about:config`)



## Отключение NTLM v2

На клиентских машинах может потребоваться отключить NTLM v2, т.к. текущая реализация поддерживает только NTLM первой версии. Делается это в Панели управления (*Панель управления > Администрирование > Локальные параметры безопасности > Сетевая безопасность: уровень проверки подлинности LAN Manager*):



## Конфигурирование веб-сервера

В PHP требуется наличие расширения **mcrypt**, сама версия PHP должна быть не ниже 5.1.2 чтобы была функция **hash**. NTLM модуль на веб сервере должен быть выключен.

## Как работает

После первого входа на сайт пользователь увидит стандартное окно авторизации Windows. После ввода логина и пароля откроется форма авторизации «1С-Битрикс: Управление сайтом» (т.е. NTLM авторизация первый раз не сработает).



После успешной авторизации хеш пароля автоматически сохранится в пользовательском свойстве UF\_NTLM\_HASH, и в последующие разы авторизация будет подхватываться автоматически.

## Итоги

Предложенный механизм не реализует полноценную NTLM авторизацию, но позволяет малыми усилиями получить аналогичный результат, при этом он достаточно безопасный.

## Преимущества:

- простота настройки для администратора (без необходимости делать настройку веб сервера);
- работа через nginx;
- переносимость между серверами, платформами и конфигурациями (Apache - IIS, Windows - Linux).

## Недостатки:

- промежуточный хеш пароля пользователя хранится в базе, если злоумышленник получит доступ к чтению БД или просмотр чужого пользовательского профиля, может использовать эту информацию как отправную точку для атаки;
- пользователю при первой авторизации на сайте потребуется вводить пароль;
- в текущей реализации нет поддержки NTLM второй версии, в данном случае это вопрос в большей степени удобства настройки, чем безопасности.

## Проверка работы LDAP

При импорте пользователей из LDAP/AD возникает много вопросов связанных с импортом пользователей и групп пользователей: у кого-то не импортируются пользователи, у других выгружаются "не те" подразделения, у третьих проблемы с авторизацией и т.д.

Служба техподдержки компании «1С-Битрикс» разработала специальный скрипт, который будет без API продукта, но по тем же алгоритмам, выполнять фильтрацию данных в AD по произвольному фильтру.

### [Скачать скрипт](#)

Запустив скрипт в браузере вы увидите следующую не сложную форму:

Хост	<input type="text"/>	Порт	<input type="text" value="389"/>	
Логин	<input type="text"/>			
Пароль	<input type="password"/>	<input type="checkbox"/>	Скрыть	
BaseDN	<input type="text"/>	Получить BaseDN	<input type="button" value="v"/>	
Строка фильтра	<input type="text"/>	Пользователи	Группы	Свой
Выводимые поля	<input type="text"/>	Очистить		
<input type="button" value="Запросить"/>				



- Заполните поля **Хост**, **Логин**, **Пароль**, а также **BaseDN** (возможные варианты для вашего сервера можно получить нажав на кнопку **Получить BaseDN**).
- Укажите заранее заданный или свой фильтр.
- Нажмите **Запросить**.

Система выведет результаты выборки. Скриптом выбираются только поля указанные в поле **Выводимые поля**. Если оставить поле **Выводимые поля** пустым, то будут выведены все возвращаемые из AD поля.

#	dn	sAMAccountName
1	CN=Exchange Servers,OU=Microsoft Exchange Security Groups,DC=office,DC=bitrix,DC=ru	Exchange Servers
2	CN=Exchange Organization Administrators,OU=Microsoft Exchange Security Groups,DC=office,DC=bitrix,DC=ru	Exchange Organization Administrators
3	CN=Exchange Recipient Administrators,OU=Microsoft Exchange Security Groups,DC=office,DC=bitrix,DC=ru	Exchange Recipient Administrators
4	CN=Exchange View-Only Administrators,OU=Microsoft Exchange Security Groups,DC=office,DC=bitrix,DC=ru	Exchange View-Only Administrators
5	CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security Groups,DC=office,DC=bitrix,DC=ru	ExchangeLegacyInterop
6	CN=RAS and IAS Servers,CN=Users,DC=office,DC=bitrix,DC=ru	RAS and IAS Servers
7	CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=office,DC=bitrix,DC=ru	Pre-Windows 2000 Compatible Access
8	CN=Exchange Domain Servers,CN=Users,DC=office,DC=bitrix,DC=ru	Exchange Domain Servers
9	CN=Performance Monitor Users,CN=Builtin,DC=office,DC=bitrix,DC=ru	Performance Monitor Users
10	CN=Performance Log Users,CN=Builtin,DC=office,DC=bitrix,DC=ru	Performance Log Users
11	CN=Network Configuration Operators,CN=Builtin,DC=office,DC=bitrix,DC=ru	Network Configuration Operators
12	CN=Incoming Forest Trust Builders,CN=Builtin,DC=office,DC=bitrix,DC=ru	Incoming Forest Trust Builders
13	CN=Group Policy Creator Owners,CN=Users,DC=office,DC=bitrix,DC=ru	Group Policy Creator Owners
14	CN=Domain Guests,CN=Users,DC=office,DC=bitrix,DC=ru	Domain Guests
15	CN=Domain Computers,CN=Users,DC=office,DC=bitrix,DC=ru	Domain Computers
16	CN=Distributed COM Users,CN=Builtin,DC=office,DC=bitrix,DC=ru	Distributed COM Users
17	CN=Cert Publishers,CN=Users,DC=office,DC=bitrix,DC=ru	Cert Publishers
18	CN=Domain Users,CN=Users,DC=office,DC=bitrix,DC=ru	Domain Users
19	CN=Remote Desktop Users,CN=Builtin,DC=office,DC=bitrix,DC=ru	Remote Desktop Users

### Пример использования скрипта

Необходимо чтобы в выгрузке на сайт участвовали только пользователи, принадлежащие к одной группе:

```
CN=Guests,CN=Builtin,DC=office,DC=bitrix,DC=ru
```

Составляем фильтр:

```
(&(&(objectClass=user)(objectCategory=PERSON))(memberof=CN=Guests,CN=Builtin,DC=office,DC=bitrix,DC=ru))
```

Вводим его в поле и получаем:



Хост	<input type="text" value="192.168.0.5"/>	Порт	<input type="text" value="389"/>	
Логин	<input type="text" value="ldap_reader@office.bitrix.ru"/>			
Пароль	<input type="password" value="*****"/>	<input checked="" type="checkbox"/>	Скрыть	
BaseDN	<input type="text" value="DC=office,DC=bitrix,DC=ru"/>	Получить BaseDN	<input type="button" value="v"/>	
Строка фильтра	<input type="text" value="(&amp;(objectCategory=group)(sAMAccountName=Event Log Reader)"/>	<input type="button" value="Пользователи"/>	<input type="button" value="Группы"/>	<input type="button" value="Свой"/>
Выводимые поля	<input type="text" value="dn,sAMAccountName"/>	<input type="button" value="Очистить"/>		
<input type="button" value="Запросить"/>				

Найдено 1 записей

#	dn	sAMAccountName
1	CN=Event Log Readers,CN=Builtin,DC=office,DC=bitrix,DC=ru	Event Log Readers

Теперь переносим результаты в продукт:

Сервер **Настройка полей** Группы Синхронизация

### Настройка соответствия полей

Параметры схемы сервера (AD \ LDAP)

AD\LDAP сервер использует кодировку UTF-8:

\*Фильтр для групп пользователей:

\*Атрибут идентификатора группы:

Атрибут названия группы:

\*Фильтр для пользователей:

\*Атрибут идентификатора пользователя:

Атрибут принадлежности пользователя к группам:

Проверять привязку пользователя в свойствах группы:

Атрибут подразделения пользователя:

Атрибут менеджера пользователя:

Соответствие полей пользователя и атрибутов LDAP \*\*

Активность	:	<input type="text" value="UserAccountControl&amp;2"/>	<input type="button" value="[удалить]"/>
Имя	:	<input type="text" value="givenName"/>	<input type="button" value="[удалить]"/>
Фамилия	:	<input type="text" value="sn"/>	<input type="button" value="[удалить]"/>
Е-Mail адрес	:	<input type="text" value="mail"/>	<input type="button" value="[удалить]"/>

Теперь при выгрузке пользователей, продукт будет использовать новый фильтр для выборки пользователей из AD.



## Проблемы и решения

### После изменения профиля AD пользователя данные возвращаются в исходное значение.

Дело в том, что для пользователей, авторизующихся через **Active Directory**, при каждом входе происходит синхронизация профиля с сервером AD, при этом все локально сделанные настройки перезаписываются данными, указанными на сервере.

Изменить такое поведение можно:

- либо установив для данного пользователя локальную авторизацию (для этого нужно вручную задать ему тот же пароль, что и в AD и изменить **Тип авторизации** на **Внутренняя проверка на странице редактирования пользователя**). Тогда авторизация пользователя будет проходить не через AD, а локально;
- либо внести изменения данных пользователя не на сайте, а в AD. Тогда на сайте они тоже автоматически изменятся при синхронизации с сервером;
- либо уменьшить количество полей, по которым осуществляется синхронизация, в настройках AD сервера на сайте (*Настройки > AD/LDAP, закладка **Настройка полей***). В этом случае можно при импорте пользователей из AD/LDAP (*Настройки > Пользователи > Импорт пользователей*), например, указать нужные нам поля, а потом в настройках AD сервера на сайте удалить все поля. Тогда у пользователя будут первоначально заданы все необходимые данные, и впоследствии, он сможет менять их.

### Для AD-пользователей не работает галка "Запомнить меня на этом компьютере"

Запомнить пароль не возможно т.к. при авторизации AD-пользователей система обращается к указанному в настройках AD/LDAP серверу и проверяет наличие пользователя с указанными логином и паролем в базе пользователей на *корпоративном сервере* и дальше уже происходит авторизация (см. урок [Схема работы модуля](#)).

Из соображений безопасности сайт не сохраняет у себя логин и пароль.

### Доступ к разделу Extanet без NTLM

Чтобы корректно настроить доступ к папке `/extanet/` без авторизации через NTLM, необходимо:

- В файле `/.htaccess` добавить строки:

```
AuthName "My Intranet"

AuthType SSPI

SSPIAuth On

SSPIPackage NTLM

SSPIDomain MYDOMAIN
```



```
SSPIPerRequestAuth On
SSPIAuthoritative On
SSPIOfferBasic On
Require valid-user
```

- В файлах `/extanet/.htaccess` и `/bitrix/.htaccess` добавить строку:

```
Satisfy any
```

- В `/bitrix/admin/.htaccess` добавить:

```
Satisfy all
```

В результате NTLM авторизация будет работать для всех папок в публичной части сайта, кроме `/extanet/`, а также в административной части сайта.

## **Импорт пользователей**

Импорт пользователей из **Active Directory / LDAP** в систему производится на странице административного раздела **Импорт пользователей** (*Настройки > Пользователи > Импорт пользователей*).

Подробнее про процедуру импорта смотрите в курсе **Администратор. Базовый**, урок [Импорт пользователей из LDAP-directory](#).