**Практическая работа № 7.**

**Тема:** «Управление группами, пользователями и компьютерами домена».

**Цель работы:** Научиться управлять пользователями, группами и компьютерами домена. Данные операции составляют основу повседневной работы администратора компьютерной сети предприятия.

**Краткое теоретическое введение.**

Для достижения поставленной цели рассматриваются следующие объекты домена и операции управления ими:

* Учетные записи пользователей и компьютеров
* Управление пользователями
* Управление группами
* Управление компьютерами

**Учетные записи пользователя и компьютера**

Учетные записи пользователей и учетные записи компьютеров в Active Directory представляют собой физические объекты, как компьютер или пользователь.

Группы, а также учетные записи пользователей и компьютеров называются участниками безопасности. Участники безопасности являются объектами каталогов, которым автоматически назначают коды безопасности (SID) для доступа к ресурсам домена.

Учетная запись пользователя или компьютера используется для следующих целей:

* Проверка подлинности пользователя или компьютера.
* Разрешение или запрещение доступа к ресурсам домена.
* Аудит действий, выполняемых с использованием учетной записи пользователя или компьютера. Аудит помогает при наблюдении за безопасностью учетных записей.

**Учетные записи пользователей**

Учетные записи пользователей, созданные автоматически при установке домена, называются встроенными учетными записями пользователей. После установки Active Directory контейнер Users, расположенный в оснастке Active Directory — пользователи и компьютеры, отображает встроенные учетные записи пользователей: «Администратор», «Гость».

Учетная запись администратора имеет самые большие права и разрешения в домене, а учетная запись гостя — ограниченные права и разрешения.

* Учетная запись «Администратор»

При помощи учетной записи «Администратор» можно полностью контролировать домен, назначать права пользователей и разрешения управления доступом для пользователей домена. Эта запись должна использоваться только для задач, выполнение которых требует учетных данных администратора. По умолчанию учетная запись «Администратор» назначается членом групп Администраторы, Администраторы домена, Администраторы предприятия, Владельцы-создатели групповой политики и Администраторы схемы в Active Directory. Она не может быть удалена или перемещена из группы «Администраторы», но ее настоятельно рекомендуется переименовать. Поскольку коды безопасности (SID) учетных записей сохраняются, переименованная учетная запись сохраняет все остальные свойства, в том числе описание, пароль, принадлежность к группам, профиль пользователя, учетную информацию, а также любые разрешения и права пользователя.

* Учетная запись «Гость»

Учетная запись Гость используется теми, кто не имеет действительной учетной записи в домене. Если учетная запись пользователя отключена (но не удалена), он также может воспользоваться учетной записью «Гость». Учетная запись «Гость» не требует пароля.

Учетной записи «Гость», как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. По умолчанию учетная запись «Гость» является членом встроенной группы Гости и глобальной группы Гости домена, позволяющих пользователям входить в домен. По умолчанию она отключена, и рекомендуется оставить ее в этом положении.

**Защита учетных записей пользователей**

Для обеспечения безопасности проверки подлинности пользователя следует создавать отдельные учетные записи для каждого пользователя сети, применяя для этого оснастку «Active Directory — пользователи и компьютеры». Каждая учетная запись пользователя (включая учетные записи администратора и гостя) может быть добавлена в группу для управления правами и разрешениями, назначенными этой учетной записи. Использование соответствующих этой сети учетных записей и групп позволяет проверить подлинность входящего в сеть пользователя и возможность предоставления ему разрешенных ресурсов.

Повысить защиту домена от атак можно с помощью надежных паролей и политики блокировки учетных записей. Применение политики блокировки учетных записей снижает вероятность проникновения злоумышленника в домен путем повторных попыток. Политика блокировки учетных записей позволяет установить число неудачных попыток входа в систему, после которых учетная запись отключается.

**Параметры учетных записей**

Каждая учетная запись пользователя Active Directory имеет ряд параметров, относящихся к безопасности и определяющих, как производится проверка подлинности данной учетной записи при входе в сеть. Параметры пароля и безопасности для учетных записей можно настроить указанными ниже способами.

* Потребовать смену пароля при следующем входе в систему

Задает требование смены пользователем пароля при следующем входе в сеть. Параметр используется, когда необходима уверенность в том, что никто, кроме пользователя, не знает его пароля.

* Запретить смену пароля пользователем

Не разрешает пользователю менять пароль. Параметр используется при необходимости контролировать учетную запись пользователя, например, учетную запись гостя или временную учетную запись.

* Срок действия пароля не ограничен

Снимает временные ограничения на использование пароля.

* Хранить пароль, используя обратимое шифрование

Позволяет пользователю входить в сеть Windows с компьютеров Apple.

* Отключить учетную запись

Не разрешает использовать данную учетную запись для входа в сеть. Многие администраторы используют отключенные учетные записи в качестве шаблонов для часто употребляемых учетных записей пользователей.

* Требовать смарт-карту для интерактивного входа в сеть

Требует наличия смарт-карты для входа в сеть в интерактивном режиме.

* Учетная запись доверена для делегирования

Позволяет службе использовать данную учетную запись для выполнения операций от имени других пользователей в сети.

* Учетная запись важна и не может быть делегирована
* Использовать для данной учетной записи тип шифрования DES

Обеспечивает поддержку шифрования с алгоритмом DES (Data Encryption Standard).

**Управление пользователями:**

Управление пользователями домена включает в себя следующие операции:

* Создание новой учетной записи пользователя
* Смена пароля пользователя
* Копирование учетной записи пользователя
* Перемещение учетной записи пользователя
* Установка времени входа
* Отключение или включение учетной записи пользователя
* Сопоставление сертификата учетной записи пользователя
* Изменение основной группы пользователя
* Удаление учетной записи пользователя

**Создание новой учетной записи пользователя**

Чтобы создать новую учетную запись пользователя, используя интерфейс Windows, откройте оснастку Active Directory — пользователи и компьютеры.

В дереве консоли щелкните правой кнопкой мыши папку, в которую добавляется учетная запись пользователя, выделите пункт Создать, а затем выберите команду Пользователь.

В поле Имя введите имя пользователя. В поле Инициалы введите инициалы пользователя. В поле Фамилия введите фамилию пользователя.

В поле Имя входа пользователя введите имя входа пользователя, к которому добавляется суффикс UPN (@ имя домена), а если доменов в сети несколько то выберите суффикс UPN в раскрывающемся списке.

В полях Пароль и Подтверждение введите пароль пользователя, а затем выберите соответствующие параметры пароля.

Смена пароля пользователя, копирование или перемещение учетной записи пользователя, отключение или включение учетной записи, смена основной группы пользователя, а также ее удаление осуществляется выбором соответствующей операции, доступной после щелчка правой кнопкой по учетной записи пользователя.

Чтобы установить время входа, щелкните учетную запись пользователя правой кнопкой мыши и выберите команду Свойства.

На вкладке Учетная запись выберите команду Время входа и установите часы, когда пользователю разрешен или запрещен вход в систему.

**Управление компьютерами**

Каждый компьютер, который присоединяется к домену, имеет учетную запись компьютера. Так же, как и учетные записи пользователей, учетные записи компьютеров предоставляют возможность проверки подлинности и аудита доступа компьютера к сети и к ресурсам домена. Учетная запись компьютера должна быть уникальной. Учетная запись компьютера создается при подключении компьютера к домену.

Учетные записи компьютеров и пользователей добавляются, отключаются, восстанавливаются и удаляются с помощью оснастки Active Directory — пользователи и компьютеры.

Чтобы выполнить операцию с учетной записью компьютера используя интерфейс Windows, откройте оснастку Active Directory — пользователи и компьютеры, выберите компьютер и соответствующую команду, доступную при щелчке правой кнопкой мыши.

**Управление группами**

Группы используются для объединения учетных записей пользователей, учетных записей компьютеров и учетных записей групп в управляемые элементы. Использование групп позволяет упростить обслуживание и администрирование сети.

В Active Directory существует два типа групп: группы распространения и группы безопасности. Группы распространения используются только приложениями электронной почты (например, Exchange) для отправки сообщений электронной почты группам пользователей. Группы распространения могут быть использованы для создания списков рассылки электронной почты, а группы безопасности для задания разрешений на использование общих ресурсов.

Группы безопасности обеспечивают эффективное управление доступом к ресурсам сети. Использование групп безопасности позволяет выполнять следующие действия:

* Назначать права пользователя группе безопасности в Active Directory.
* Назначать разрешения на использование ресурсов для групп безопасности.

Не следует путать разрешения с правами пользователей. Разрешения задаются для групп безопасности, использующих общие ресурсы. Разрешения определяют, кто может получить доступ к данному ресурсу и уровень доступа. Права пользователя, заданные для групп безопасности, определяют, что может делать член данной группы в области действий домена или на локальном компьютере рабочей группы.

Группы безопасности перечислены в избирательных таблицах управления доступом, которые определяют разрешения на ресурсы и объекты. Администраторам следует назначать разрешения для ресурсов (общих файлов, принтеров, и т. д.) группам безопасности, а не отдельным пользователям. Разрешения назначаются группе один раз, вместо назначения прав каждому отдельному пользователю. Каждая учетная запись при добавлении к группе получает права, заданные данной группе в Active Directory, и разрешения, определенные для данной группы на ресурсе.

Группы безопасности могут использоваться в качестве адресатов электронной почты, как и группы распространения. Сообщение электронной почты, отправленное группе, отправляется всем членам группы.

Управление группами включает в себя следующие операции:

* Создание новой группы
* Добавление участника группы
* Преобразование типа группы
* Изменение области действия группы
* Удаление группы
* Поиск групп, в которые входит пользователь

**Создание новой группы**

Чтобы создать новую группу щелкните правой кнопкой мыши папку, в которую добавляется новая группа.

Выделите пункт Создать, а затем выберите команду Группа. Введите имя создаваемой группы. Задавая тип группы, выберите один из предложенных вариантов: группа безопасности или группа распространения.

Задавая область действия группы, выберите один из предложенных вариантов: локальная в домене, глобальная или универсальная (только для групп распространения).

Группы с локальной доменной областью действия могут включать учетные записи и группы с глобальной областью действия, а также группы с универсальной областью действия и группы с локальной доменной областью действия только из данного домена.

Группы с глобальной областью действия могут включать учетные записи и группы с глобальной областью действия из данного домена.

Группы с универсальной областью действия могут включать учетные записи и группы с глобальной областью действия, а также группы с универсальной областью из любого домена.

**Добавление участника группы**

Чтобы добавить участника группы выберите команду Свойства данной группы и на вкладке «Члены групп» нажмите кнопку Добавить.

В поле Введите имена выбираемых объектов введите имя пользователя, группы или компьютера, добавляемых к выбранной группе и нажмите кнопку OK. Можно воспользоваться кнопками «Дополнительно» и «Поиск», а затем выбрать добавляемый объект из списка доступных в домене.

**Преобразование типа группы**

Чтобы преобразовать тип группы выберите папку, включающую группу, тип которой необходимо изменить. В области сведений щелкните правой кнопкой мыши необходимую группу и выберите команду Свойства.

На вкладке Общие в группе Тип группы выберите тип группы.

**Изменение области действия группы**

Чтобы изменить область действия группы выберите папку, включающую группу, для которой необходимо изменить область действия. В области сведений щелкните правой кнопкой мыши необходимую группу и выберите команду Свойства.

На вкладке Общие в разделе Область действия группы выберите область действия группы.

**Удаление группы**

Чтобы удалить группу выберите папку, включающую группу, которую необходимо удалить.

На панели сведений щелкните правой кнопкой мыши необходимую группу и выберите команду Удалить.

**Поиск групп, в которые входит пользователь**

Чтобы найти группы, в которые входит пользователь, в дереве консоли Active Directory щелкните узел Пользователи.

Можно также выбрать папку, содержащую учетную запись пользователя. На панели сведений щелкните правой кнопкой мыши учетную запись пользователя и выберите команду Свойства. Выберите вкладку Член групп и определите, в какие группы входит данный пользователь.

**Задания к практической работе**

1. Создание групп

Создайте две группы безопасности с локальной доменной областью действия, например, группу Разработчики и группу Менеджеры.

Создайте две группы безопасности с глобальной областью действия, например, группу Инженеры и группу Экономисты.

1. Создание учетных записей пользователей и помещение их в группы

Создайте по одной учетной записи для каждой из созданных групп, задавая в качестве параметра человеческие имена.

Создайте одну учетную запись, которую поместите в каждую из созданных групп.

1. Включение групп в другие группы

Поместите глобальную группу Инженеры в локальную группу Разработчики, а глобальную группу Экономисты в локальную группу Менеджеры.

4. Создайте учетную запись для нового компьютера WorkStation1, который предполагается подключить к домену.

5. Создайте произвольную группу, учетную запись пользователя и учетную запись компьютера. Выполните с ними все описанные в теоретическом разделе работы операции по управлению ими и после показа результатов преподавателю, удалите эти временные объекты.

**Контрольные вопросы:**

1. Какие типы групп могут быть созданы в домене?
2. Чем отличаются группы безопасности от групп распространения?
3. Назовите порядок размещения пользователей и групп в группах домена большого предприятия с несколькими доменами.
4. В чем главное отличие групп локального компьютера от групп домена?
5. Почему уровень безопасности сети на основе домена выше, чем в одноранговой сети?
6. В чем отличие глобальных и локальных доменных групп?
7. Какие группы могут быть отнесены к универсальным группам домена?
8. Как создается учетная запись компьютера в домене?
9. Как создается учетная запись пользователя домена?
10. Какими учетными записями должен обладать пользователь для того, чтобы он мог выполнить первоначальное присоединение компьютера к домену?