**Введение**

Ключевой частью Вашей работы в качестве администратора является создание учетных записей пользователей, и эта глава покажет Вам, как это делается.

Учетные записи пользователей позволяют Microsoft Windows 2000 отслеживать информацию о пользователях и управлять их правами доступа и привилегиями. При создании учетных записей пользователя, основными средствами управления учетными записями, которые Вы используете, являются:

|  |  |
| --- | --- |
| • | Оснастка Active Directory – пользователи и компьютеры (Active Directory Users And Computers), используемая для управления учетными записями в пределах домена Active Directory. |
| • | Оснастка Локальные пользователи и группы – для управления учетными записями на локальном компьютере. |

В этой главе описывается создание учетных записей домена, а также локальных пользователей и групп.

**Предварительная настройка и организация учетной записи пользователя**

Наиболее важными аспектами создания учетных записей является предварительная настройка и организация учетных записей. Без подходящих политик Вы вскоре обнаружите, что Вам нужно переделывать все учетные записи пользователей. Поэтому, до создания учетных записей, определите политики, которые Вы будете использовать для их настройки и организации.

**Политики присвоения имен учетных записей**

Основной политикой, которую Вам необходимо будет установить, является схема именования для учетных записей. Учетным записям пользователя присваиваются отображаемые имена и имена входа. Отображаемое имя (или полное имя) – это выводимое имя пользователя, используемое в пользовательских сеансах. Имя входа используется для входа в домен. Имена входа были коротко рассмотрены в разделе Главы 7 *«Имена для входа, Пароли и Открытые сертификаты».*

**Правила для отображаемых имен**

В Windows 2000 отображаемое имя обычно является объединением имени и фамилии пользователя, но Вы можете установить для него любое строковое значение. Отображаемые имена должны соответствовать следующим правилам:

|  |  |
| --- | --- |
| • | Локальные отображаемые имена должны быть уникальными на рабочей станции. |
| • | Отображаемые имена должны быть уникальными в домене. |
| • | Отображаемые имена должны состоять не более, чем из 64 символов. |
| • | Отображаемые имена могут содержать буквенно-цифровые и специальные символы. |

**Правила для имен входа**

Имена входа должны соответствовать следующим правилам:

|  |  |
| --- | --- |
| • | Локальные имена входа должны быть уникальными на рабочей станции, а глобальные – уникальными в домене. |
| • | Длина имени входа может достигать 104 символов. Однако использование имён длиннее 64 символов неудобно. |
| • | Имя входа Microsoft Windows NT версии 4.0 или более ранних имеют все учетные записи, его значением по умолчанию являются первые 20 символов имени входа Windows 2000. Имя входа Microsoft Windows NT версии 4.0 или более ранних версий должно быть уникальным в домене. |
| • | Пользователи, осуществляющие вход в домен с компьютера, работающего под управлением ОС Windows 2000, могут использовать имена входа Windows 2000 или имена входа, совместимые с Windows NT версии 4.0 и более ранними версиями, независимо от режима работы домена. |
| • | Имена входа не могут содержать некоторые символы. Недопустимыми символами являются:  " / \ [ ] : ; | = , + \* ? < > |
| • | Имена входа могут содержать любые другие специальные символы, включая пробелы, точки, тире и подчеркивания. Но, как правило, использовать пробелы в учетных записях не рекомендуется. |

**Примечание.** Хотя Windows 2000 хранит имена пользователей в том же регистре, что был использован при вводе, они не являются чувствительными к регистру. Например, Вы можете получить доступ к учетной записи «Администратор», используя имя пользователя «Администратор» или «администратор». Таким образом, имена пользователей не чувствительны к регистру, хотя строчные и заглавные буквы в них поддерживаются.

**Схемы именования**

Известно, что в небольших организациях в качестве имен входа обычно используются имена или фамилии пользователей. Но в организации любого размера может быть несколько Томов, Диков и Гарри. Лучше сразу выбрать правильную схему присвоения имен и убедиться, что другие администраторы используют её, чем переделывать схему именования при возникновении проблемы. Для присвоения имен Вам следует использовать согласованную процедуру, которая обеспечит поддержку расширяющейся базы пользователей, уменьшит вероятность возникновения конфликтов имен, и будет гарантировать, что учетным записям присвоены безопасные имена, предотвращающие их использование не по назначению. Если Вы последуете этим рекомендациям, то типы схем присвоения имен, которые Вы можете использовать, включают:

|  |  |
| --- | --- |
| • | **Имя и первая буква фамилии пользователя.** Для создания имени входа соедините имя пользователя и первую букву его фамилии. Для William Stanek используйте имя «*williams*. Эта схема присвоения имен не подходит для больших организаций. |
| • | **Первый инициал и фамилия пользователя.** Для создания имени входа соедините первую букву имени пользователя с его фамилией. Для William Stanek используйте имя «*wstanek*»*.* Эта схема присвоения имен также непрактична для больших организаций. |
| • | **Первый инициал, второй инициал и фамилия пользователя.** Для создания имени входа соедините первый инициал, второй инициал и фамилию пользователя. Для William R. Stanek Вы могли бы использовать имя «*wrstanek*». |
| • | **Первый инициал, второй инициал и первые пять букв фамилии пользователя.** Для создания имени входа, соедините первый инициал, второй инициал и первые пять букв фамилии. Для William R. Stanek используйте имя «*wrstane*». |
| • | **Имя и фамилия пользователя.** Соедините имя и фамилию пользователя с помощью символов подчерк ( \_ ) или тире ( - ). Для William Stanek Вы могли бы использовать имя «*william\_ stanek*» или «*william-stanek*». |

**Совет.** В условиях повышенных требований к безопасности Вы можете задать в качестве имени входа числовой код. Этот числовой код должен быть не короче 20 символов. Используйте этот строгий метод присвоения имен в сочетании со считывателями смарт-карт, чтобы позволить пользователям быстро входить в домен. Вы можете не волноваться, поскольку у пользователей останутся отображаемые имена, которые могут читать люди.

**Политики паролей и учетных записей**

Учетные записи Windows 2000 используют пароли и открытые сертификаты, чтобы удостоверять доступ к сетевым ресурсам. Данный раздел посвящен паролям.

**Безопасные пароли**

Пароль – это чувствительная к регистру строка, которая содержит до 104 символов в Службе каталога Active Directory и до 14 символов в Диспетчере безопасности Windows NT (Windows NT Security Manager). Допустимыми символами для паролей являются буквы, цифры и специальные символы.

После установки пароля для учетной записи, Windows 2000 сохраняет его в зашифрованном формате в базе данных учетных записей.

Недостаточно просто иметь пароль. Чтобы избежать неавторизованного доступа к сетевым ресурсам, нужно использовать *безопасные пароли.* Разница между обычным и безопасным паролем заключается в том, что безопасный пароль трудно угадать и взломать. Трудными для взлома пароли делает комбинация всех возможных типов символов – включая строчные и заглавные буквы, цифры и специальные символы. Например, вместо использования **happydays** в качестве пароля, используйте **haPPy2Days&**, **Ha\*\*y!dayS**, или даже **h\*PPY%d\*ys**

К сожалению, неважно насколько безопасный пароль Вы первоначально установите, поскольку в конечном счете, пользователь выбирает пароль самостоятельно. Поэтому Вам потребуется настроить политики для управления учетными записями. Политики для управления учетными записями являются подмножеством политик, конфигурируемых как групповая политика.

**Установка Политик для управления учетными записями**

Как Вам уже известно из предыдущих разделов, Вы можете применять групповые политики на различных уровнях внутри сетевой структуры. Вы настраиваете локальные групповые политики в соответствии с описанием в разделе «*Управление локальными групповыми политиками»* Главы 4.

Как только Вы начали работать с нужным контейнером групповой политики, Вы можете настроить политики, выполнив следующие шаги:

|  |  |
| --- | --- |
| 1. | Найдите узел **Политики учетных записей (Account Policies)**, спускаясь по дереву консоли. Разверните **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)** и затем **Параметры безопасности (Security Settings)**, как показано на рисунке 8-1 |
| 2. | Теперь можно управлять политиками учетных записей через узлы **Политика паролей (Password Policy)**, **Политика блокировки учетной записи (Account Lockout Policy)** и **Политика Kerberos (Kerberos Policy)**.  **Примечание.** Политики Kerberos не используются для локальных компьютеров, они доступны только для групповых политик, которые относятся к сайтам, доменам и подразделениям.  **Рисунок 8-1. Для установки политик паролей и общего использования учетных записей используйте содержимое узла Политики учетных записей. Дерево консоли отображает название компьютера или домена, который Вы конфигурируете. Убедитесь, Что Вы конфигурируете нужный сетевой ресурс.**  **Рисунок 8-2. При работе с локальными политиками Вы увидите как локальную, так и действующую политику.** |
| 3. | Чтобы начать конфигурирование политики, дважды нажмите на неё или щелкните по ней правой кнопкой мыши и выберите **Свойства (Properties)**. Откроется диалоговое окно **Свойства (Properties)** для данной политики. |
| 4. | Для локальной политики диалоговое окно **Свойства (Properties)** такое же, как показано на Рисунке 8-2. Действующая для компьютера политика отображена, но недоступна для изменения. Несмотря на это, Вы можете изменять параметры локальной политики. Используйте поля, предназначенные для конфигурирования локальной политики. Для локальной политики пропустите остающиеся шаги - эти шаги используются для глобальных групповых политик.  **Примечание.** Политики сайта, домена и подразделения имеют преимущество над локальными политиками. |
| 5. | Для сайта, домена или подразделения окно **Свойства (Properties)** такое же, как показано на Рисунке 8-3.  **Рисунок 8-3. Определяйте и конфигурируйте глобальные политики групп, используя диалоговое окно Свойства (Properties) для каждой из них.** |
| 6. | Все политики либо определены, либо не определены. Это значит, что они либо сконфигурированы для использования, либо нет. Политика, которая не определена в текущем контейнере, может быть унаследована от другого контейнера. |
| 7. | Установите или снимите флажок «Определить следующие параметры политики в шаблоне», чтобы указать, определена политика или нет. |

**Совет.** Политики могут иметь дополнительные поля для их конфигурирования. Обычно этими полями являются переключатели **Включен** и **Отключен**. **Включен** задействует ограничения политики, **Отключен** их отменяет

В следующих разделах данной главы *«Настройка политик паролей», «Настройка политик блокировки учетных записей» и «Настройка политик Kerberos»* описаны отдельные процедуры для работы с политиками учетных записей. Следующий раздел данной главы *«Просмотр действующих политик»* расскажет Вам больше о просмотре действующих политик на локальном компьютере.

**Просмотр действующих политик**

Во время работы с политиками учетных записей и присвоением прав пользователей Вам часто бывает необходимо просмотреть политику, действующую на локальную систему. Действующей является применённая на данный момент политика и, как описано в Главе 4 *«Управление Групповой политикой»*, она зависит от последовательности, в которой политики были применены.

Выполните следующие шаги, чтобы просмотреть политику, действующую на локальную систему:

|  |  |
| --- | --- |
| 1. | Откройте параметры локальной политики для системы, с которой Вы хотите работать, как показано в разделе Главы 4 «*Управление локальными групповыми политиками*», или выберите **Параметры локальной политики (Local Policy Settings)** в меню **Администрирование (Administrative Tools)** (если эти инструменты установлены и Вы работаете на компьютере, который хотите проверить). |
| 2. | Откройте узел политики, которую Вы хотите проверить. На Рисунке 8-4 изображен узел Политика паролей. |
| 3. | В случае локальных политик, графа **Параметры компьютера (Computer Management)** заменена графами **Локальные параметры (Local Setting)** и **Действующие параметры (Effective Setting)**. Графа **Локальные параметры (Local Setting)** отображает параметры локальной политики. Графа **Действующие параметры (Effective Setting)** отображает параметры политик, примененные на данном локальном компьютере. |
| 4. | Если Вы столкнулись с конфликтами политик, пересмотрите разделы «*В каком порядке применять несколько политик?*» и «*Когда применяются групповые политики?*» Главы 4. |

**Настройка политик учетных записей**

Как Вы узнали из предыдущего раздела, существует три типа политик для управления учетными записями: политики паролей, политики блокировки учетных записей и политики Kerberos. Следующий раздел описывает настройку каждой из этих политик.

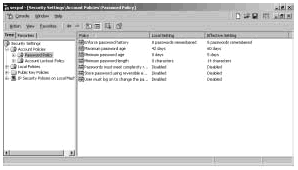


Рисунок 8-4. Локальные политики отображают как действующие параметры, так и локальные параметры.

**Настройка политик паролей**

Политики паролей контролируют безопасность паролей и они включают:

|  |  |
| --- | --- |
| • | Требовать неповторяемости паролей |
| • | Максимальный срок действия паролей |
| • | Минимальный срок действия паролей |
| • | Минимальная длина пароля |
| • | Пароль должен отвечать требованиям сложности |
| • | Хранить пароли всех пользователей в домене, используя обратимое шифрование |

Использование этих политик описано в следующих разделах.

**Требовать неповторяемости паролей**

Политика «Требовать неповторяемости паролей» определяет, как часто старые пароли могут быть использованы повторно. С помощью этой политики Вы можете побудить пользователей к выбору паролей, не входящих в общеизвестный набор. Windows 2000 может хранить до 24 паролей для каждого пользователя, но по умолчанию хранит в истории паролей только один.

Чтобы выключить эту функцию, установите размер истории паролей равным нулю. Чтобы включить – установите длину истории паролей, используя поле «хранимых паролей». В этом случае Windows 2000 будет отслеживать старые пароли с помощью истории паролей, которая уникальна для каждого пользователя, и пользователи не смогут заново использовать любой из хранимых паролей.

**Примечание.** Вы не должны разрешать пользователям менять пароли немедленно, чтобы они не смогли обойти политику «Требовать неповторяемости паролей». Это помешает пользователям изменять свои пароли несколько раз подряд, чтобы вернуться к старым паролям.

**Максимальный срок действия паролей**

Политика «Максимальный срок действия паролей» определяет, как долго пользователи могут пользоваться паролями перед их обязательной сменой. Целью этой политики является периодически заставлять пользователей менять их пароли. При использовании этой возможности установите значение, которое более всего подходит для вашей сети. Как правило, следует указывать тем меньший срок, чем выше уровень безопасности, и наоборот.

Срок действия пароля по умолчанию составляет 42 дня, но Вы можете присвоить ему любое значение от 0 до 999. Значение 0 означает, что срок действия пароля никогда не истекает. Несмотря на то, что, возможно, Вы хотели бы установить неистекающий срок действия пароля, пользователи должны менять пароль регулярно для поддержания безопасности сети. Если требования к безопасности высоки, подойдут значения 30, 60 или 90 дней. Если безопасность не очень важна, то подойдут значения 120, 150 или 180 дней.

**Примечание.** Windows 2000 уведомляет пользователей о приближении окончания срока действия пароля. Если до окончания срока действия пароля остается менее 30 дней, то пользователи каждый раз во время входа в систему видят предупреждение о необходимости сменить пароль в течении определенного срока.

**Минимальный срок действия паролей**

Политика «Минимальный срок действия паролей» определяет, как долго пользователи должны сохранять свой пароль перед тем, как смогут его сменить. Вы можете использовать это поле, чтобы помешать пользователям обманывать систему паролей путем ввода нового пароля и дальнейшей его замены на старый.

Windows 2000 по умолчанию позволяет пользователям изменять пароли немедленно. Чтобы помешать этому, установите определенный минимальный срок. Приемлемые значения этого параметра находятся в промежутке от трех до семи дней. Таким образом, ваши пользователи будут менее склонны к использованию бывших в употреблении паролей, располагая при этом возможностью при желании поменять их в приемлемый срок.

**Минимальная длина пароля**

Политика «Минимальная длина пароля» устанавливает минимальное количество символов для пароля. Если Вы не меняли параметры, установленные по умолчанию, Вам придется это сделать очень скоро. По умолчанию разрешены пустые пароли (пароли, в которых нет символов), что определенно не является правильным подходом.

Как правило, из соображений безопасности, Вам понадобятся пароли по меньшей мере из восьми символов. Причиной этому является то, что длинные пароли обычно труднее взломать, чем короткие. Если Вам необходимо обеспечить более серьезную безопасность, установите минимальную длину паролей 14 символов.

**Пароль должен отвечать требованиям сложности**

Помимо основных политик для управления паролями и учетными записями, Windows 2000 включает средства для создания дополнительных элементов управления паролями. Эти возможности доступны в фильтрах паролей, которые могут быть установлены на контроллер домена. Если Вы установили фильтр пароля, разрешите политику «Пароль должен отвечать требованиям сложности». В этом случае все пароли должны будут соответствовать требованиям безопасности фильтра.

Например, стандартный фильтр Windows NT (PASSFILT.DLL) требует использования безопасных паролей, которые соответствуют следующим рекомендациям:

|  |  |
| --- | --- |
| • | Пароли должны быть не менее шести символов в длину. |
| • | Пароль не должен содержать имя пользователя, такие как «stevew», или части его полного имени, такие как Steve. |
| • | Пароли должны использовать три или четыре доступных типа символов: строчные буквы, заглавные буквы, цифры и специальные символы. |

**Хранить пароли, используя обратимое шифрование**

Пароли, хранящиеся в базе данных паролей, зашифрованы. В общем случае, шифрование не может быть снято. Если Вы хотите разрешить отмену шифрования, примените политику «Хранить пароли всех пользователей в домене, используя обратимое шифрование». Пароли будут храниться с использованием обратимого шифрования и смогут быть восстановлены в аварийной ситуации. Случаи с забыванием пароля к таковым не относятся. Любой администратор может изменить пароль пользователя.

**Настройка политик блокировки учетных записей**

Политики блокировки учетных записей контролируют, как и когда учетные записи блокируются доменом или локальной системой.

Эти политики:

|  |  |
| --- | --- |
| • | Пороговое значение блокировки |
| • | Блокировка учетной записи на (Длительность блокировки учетной записи) |
| • | Сброс счетчика блокировки через |

**Пороговое значение блокировки**

Политика «Пороговое значение блокировки» устанавливает количество попыток входа в систему, после которого учетная запись будет заблокирована. Если Вы решили использовать блокировку учетных записей, нужно установить в этом поле значение, предотвращающее несанкционированное проникновение, но оставляющее достаточное количество попыток пользователям, испытывающим трудности при доступе к своим учётным записям

Основной причиной, по которой пользователи не могут получить доступ к своей учетной записи с первого раза, является то, что они забыли свой пароль. В этом случае им может понадобиться несколько попыток, чтобы войти в систему. У пользователей рабочей группы также могут быть проблемы с доступом к удаленной системе, в которой их текущий пароль не совпадает с ожидаемым удаленной системой.

Если это произойдет, несколько неправильных попыток входа могут быть записаны удаленной системой до того, как пользователь получит возможность ввести верный пароль. Причиной является то, что Windows 2000 может попытаться автоматически войти на удаленную систему. В доменном окружении этого не произойдет, благодаря функции «Один вход».

Вы можете установить для порога блокировки любое значение от 0 до 999. Значение порога блокировки по умолчанию установлено равным 0, это значит, что учетная запись не будет блокироваться из-за неправильных попыток входа. Любое другое значение устанавливает определенный порог блокировки. Помните, что чем выше значение порога блокировки, тем выше риск, что хакер сможет получить доступ к вашей системе. Приемлемые значения для этого порога находятся между 7 и 15. Это достаточно много, чтобы исключить ошибку пользователя и достаточно мало, чтобы отпугнуть хакеров.

**Длительность блокировки учетной записи**

При превышении порога блокировки, политика «Блокировка учетной записи» устанавливает её длительность. Вы можете установить соответствующее значение, используя величину от 1 до 99,999 минут, или на неограниченное время, путем установки этого параметра равным 0.

Наиболее безопасной политикой является установка неограниченного времени блокировки. В этом случае только администратор может разблокировать учетную запись. Это помешает хакерам повторить попытку получения доступа к системе и вынудит пользователей, чьи учетные записи заблокированы, прибегнуть к помощи администратора, что само по себе является хорошей идеей. Поговорив с пользователем, Вы можете выяснить, что он делает неправильно и помочь ему избежать проблем.

**Совет.** Если учетная запись заблокирована, обратитесь к диалоговому окну Свойства для данной учетной записи в оснастке Active Directory – Пользователи и компьютеры. Щелкните по вкладке Учетная запись и снимите флажок «Учетная запись заблокирована». Это разблокирует учетную запись.

**Сброс счетчика блокировки через**

Каждый раз при неудавшейся попытке входа в систему Windows 2000 увеличивает значение порога, который отслеживает число неправильных попыток входа. Политика «Сброс счетчика блокировки через» определяет, как долго сохраняется значение порога блокировки. Счетчик порога блокировки учетной записи сбрасывается одним из двух способов. Если пользователь входит в систему успешно, счетчик порога сбрасывается. Если период ожидания для политики «Сброс счетчика блокировки через» после последней неудачной попытки входа истек, счетчик также сбрасывается.

По умолчанию, установлено сохранение порога в течение одной минуты, но Вы можете установить любое значение от 1 до 99,999 минут. Как и с Порогом блокировки учетной записи, необходимо выбрать значение, которое находится в равновесии между нуждами безопасности и нуждами пользователей. Подходящее значение находится в диапазоне от одного до двух часов. Этот период ожидания должен быть достаточно большим, чтобы заставить взломщиков ждать дольше, чем им хотелось бы, перед новой попыткой получить доступ к учетной записи.

**Примечание.** Неудачные попытки входа на рабочую станцию через заставку защищенную паролем не увеличивают значение порога блокировки. Также, если Вы блокируете сервер или рабочую станцию используя Ctrl+Alt+Delete, неудачные попытки входа через окно Снятие блокировки компьютера не будут учитываться.

**Настройка политик Kerberos**

Kerberos версии 5 является основным механизмом проверки подлинности, используемым в домене Active Directory. Kerberos использует билеты службы и билеты пользователя для идентификации пользователей и сетевых служб. Как Вы догадываетесь, билеты службы используются служебными процессами Windows 2000, а билеты пользователя пользовательскими процессами. Билеты содержат зашифрованные данные, подтверждающие подлинность пользователя или службы.

Вы можете контролировать длительность билета, его возобновление и применение, используя следующие политики:

|  |  |
| --- | --- |
| • | Принудительные ограничения входа пользователей |
| • | Максимальный срок жизни билета службы |
| • | Максимальный срок жизни билета пользователя |
| • | Максимальный срок жизни для возобновления билета пользователя |
| • | Максимальная погрешность синхронизации часов компьютера |

Эти политики описаны в следующем разделе.

**Внимание.** Только администраторы, полностью понимающие пакет безопасности Kerberos, должны менять эти политики. Установка неправильных параметров для данных политик может повлечь серьезные проблемы в сети. В большинстве случаев параметры политики Kerberos, установленные по умолчанию, работают как надо.

**Принудительные ограничения входа пользователей**

Политика «Принудительные ограничения входа пользователей» обеспечивает включение ограничений пользовательской учетной записи. Например, если время входа пользователя ограничено, данная политика осуществляет это ограничение. По умолчанию, данная политика разрешена и отменять ее следует только при исключительных обстоятельствах.

**Максимальный срок жизни**

Политики «Максимальный срок жизни билета службы» и «Максимальный срок жизни билета пользователя» устанавливают максимальный срок, в течение которого билет службы или пользователя имеет силу. По умолчанию, билеты службы имеют максимальную длительность 41,760 минут, а билеты пользователя – 720 часов.

Вы можете изменить длительность билетов. Для билетов службы эффективные значения находятся в диапазоне от 0 до 99,999 минут. Для билетов пользователя – от 0 до 99,999 часов. Нулевое значение выключает истечение срока жизни. Любые другие значения устанавливают определенный срок жизни билета.

Билет с истекшим сроком жизни может быть возобновлен. Для возобновленного билета устанавливается срок жизни в соответствии с политикой «Максимальный срок жизни для возобновления билета пользователя». По умолчанию период возобновления билета составляет 60 дней. Вы можете установить период возобновления от 0 до 99,999 дней. Нулевое значение выключает максимальный период обновления, а любые другие значения устанавливают его определенный срок.

**Максимальная погрешность**

Политика «Максимальная погрешность синхронизации часов компьютера» является одной из немногих политик Kerberos, которую Вам, возможно, придется изменить. По умолчанию компьютеры в домене должны быть синхронизированы друг с другом в течение пяти минут. Если это условие не выполняется, аутентификация не происходит.

Если у Вас есть удаленные пользователи, которые входят в домен без синхронизации их часов с сетевым сервером времени, Вам может понадобиться установить этот параметр. Его диапазон - от 0 до 99,999

Первым шагом к обеспечению безопасности корпоративной сети среднего размера является понимание того, какими уязвимостями могут воспользоваться злоумышленники. Главной задачей злоумышленника, проникшего в сеть, является повышение привилегий созданного им плацдарма для получения более широкого доступа. После повышения привилегий очень тяжело предотвратить дальнейшие действия злоумышленника. Злоумышленники используют различные механизмы повышения привилегий, но чаще всего они связаны с атаками на имеющиеся в системе учетные записи, особенно, если они обладают правами администратора.

В корпоративных сетях среднего размера зачастую принимаются меры по обеспечению безопасности обычных учетных записей пользователей, а учетные записи служб остаются без внимания, что делает их уязвимыми и популярными целями злоумышленников. После получения злоумышленником контроля над важной учетной записью с высоким уровнем доступа к сети, вся сеть будет оставаться ненадежной, пока не будет полностью создана заново. Поэтому уровень безопасности всех учетных записей является важным аспектом обеспечения безопасности сети.

Внутренние угрозы, так же как и внешние, могут причинить значительный ущерб корпоративной сети среднего размера. Внутреннюю угрозу создают не только злоумышленники, но и те пользователи, которые могут нанести ущерб ненамеренно. Одним из примеров могут служить на первый взгляд безобидные попытки пользователей получить доступ к ресурсу в обход мер безопасности. Из соображений удобства пользователи и службы также очень часто получают более широкие права, чем необходимо для работы. Хотя такой подход гарантирует пользователям доступ к ресурсам, необходимым для выполнения работы, он также увеличивает опасность успешной атаки на сеть.

**Аннотация**

Как уже было сказано во введении, управление безопасностью всех типов учетных записей в сети является важным аспектом управления рисками корпоративной сети среднего размера. Во внимание должны приниматься как внешние, так и внутренние угрозы. Решение по защите от таких угроз должно быть сбалансировано с точки зрения безопасности и функциональности сетевых ресурсов, соответствующей потребностям среднего бизнеса.

Данный документ поможет представителям среднего бизнеса осознать риски, связанные с административными учетными записями и учетными записями служб, учетными записями по умолчанию и учетными записями приложений. Приведенные сведения являются основой для разработки и реализации мер по снижению этих рисков. Для этого необходимо рассказать о сути этих учетных записей, о том, как их различать, как определять права, необходимые для работы, и как снижать риски, связанные с повышенными привилегиями учетных записей служб и администраторов.

В рамках инициативы корпорации Майкрософт «Защищенные компьютерные системы» используемые в Microsoft® Windows Server™ 2003 параметры по умолчанию рассчитаны на обеспечение защиты службы каталогов Active Directory® от различных угроз. Однако уровень безопасности учетных записей администраторов корпоративной сети среднего размера можно усилить еще больше, изменив некоторые их параметры. Кроме того, службы, не входящие в состав операционной системы Windows Server 2003 и устанавливаемые другими приложениями, также необходимо защитить. В данном документе описываются способы обеспечения безопасности этих учетных записей и служб, а также содержатся рекомендации по контролю над использованием и управлением административными полномочиями.