**Встроенные средства защиты Active Directory**

# Local Administrator Password Solution (LAPS)

Пароль локального администратора необходим, когда нельзя использовать доменный аккаунт для аутентификации. Например, если узел не имеет соединения с корпоративной сетью и отсутствуют кэшированные учетные данные пользователей с привилегиями администратора. Есть некоторые сложности, связанные с паролями локальных администраторов:

* использование одинакового пароля для нескольких узлов, что увеличивает поверхность атаки pass-the-hash;
* поддержание сложных и уникальных паролей, а также их предоставление при необходимости;
* регулярная смена этих паролей.

Для централизованного управления паролями локальных администраторов существует решение от Майкрософт LAPS, которое состоит из следующих компонентов:

* клиент Group Policy Client-Side Extension — расширение групповой политики, устанавливаемое на каждый узел под управлением LAPS;
* инструменты для управления (management tools) — утилиты, устанавливаемые на узел, с которого выполняется настройка LAPS;
* Active Directory (AD) для хранения паролей.

Клиент LAPS периодически проверяет, не истек ли срок действия пароля локального администратора, и если это так, задает ему новое случайное значение и отправляет этот пароль в AD. Передача пароля от узла в AD осуществляется с использованием шифрования Kerberos. Текущие пароли LAPS сохраняются в объектах компьютеров в Active Directory в атрибуте *msLAPS-Password* в открытом виде, срок действия пароля хранится в атрибуте *msLAPS-PasswordExpirationTime*. Разрешения на чтение объектов AD недостаточно для доступа к этому атрибуту; компьютеру или пользователю необходимо также иметь особое разрешение *Control Access*. Узел под управлением LAPS имеет только право записывать новый пароль.

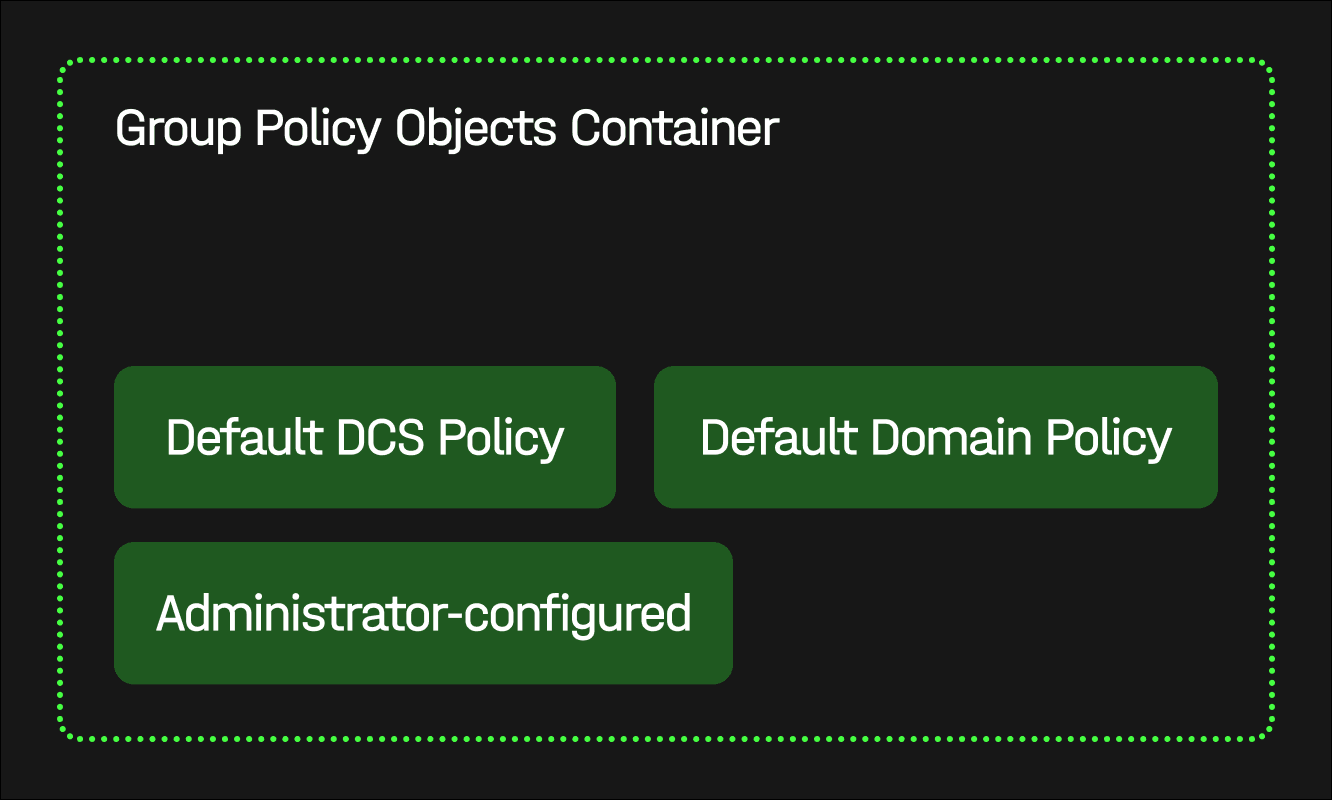
С использованием LAPS могут быть настроены следующие параметры:

* имя учетной записи локального администратора (по умолчанию встроенный пользователь — *Administrator*);
* сложность пароля;
* длина пароля;
* максимальный срок действия пароля.

# Group Policy Object (GPO)

Групповые политики — фреймворк в Windows, устанавливаемый на контроллеры доменов, серверы и клиентские машины, с помощью которого можно управлять конфигурацией AD DS. Параметры групповых политик задаются с помощью объектов групповой политики (GPO).

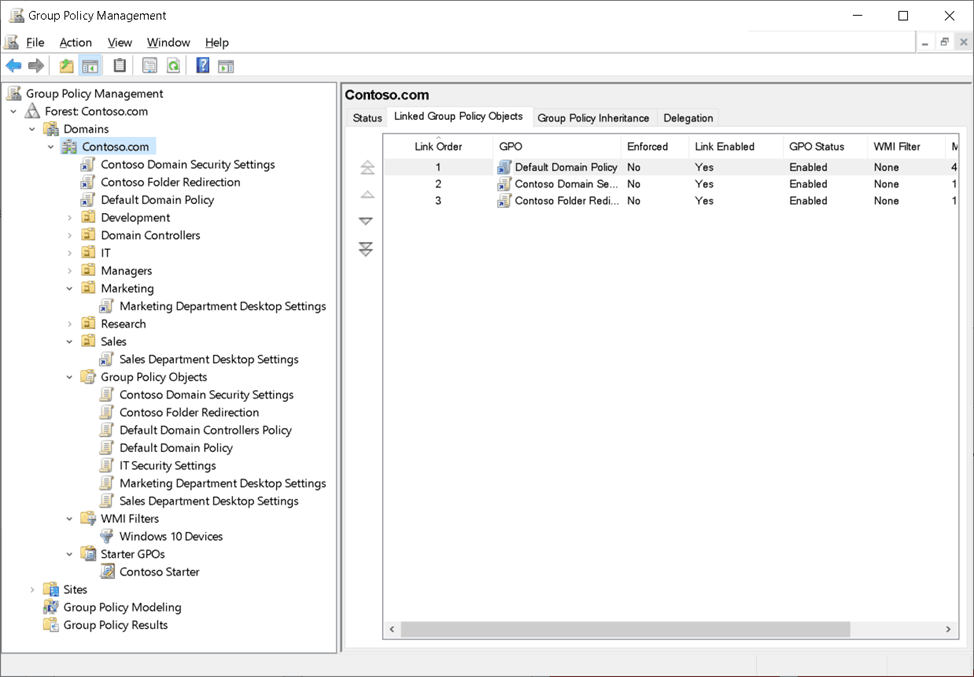
Этот фреймворк хранится в контейнере *Group Policy Objects* в AD.



*Рисунок 1. Контейнер Group Policy Objects*

Политика *Default Domain Controllers* формируется автоматически при создании контроллера домена и определяет его конфигурацию. Политика *Default Domain* формируется автоматически при создании контроллера домена и определяет конфигурацию по умолчанию, применяемую для пользователей и компьютеров в домене. Политики *Administrator-configured* создаются администратором для управления конфигурацией определенной группы ресурсов.

С помощью GPO можно настраивать параметры для большого количества пользователей или рабочих станций и применять их на разных уровнях — от локальных компьютеров до домена. В первую очередь групповые политики используются для определения параметров, которыми пользователь не может управлять. Кроме того, они могут применяться для стандартизации окружения рабочих станций на уровне подразделений (OU) или всей организации. С помощью групповых политик могут задаваться дополнительные свойства безопасности, расширенные системные параметры и другое.

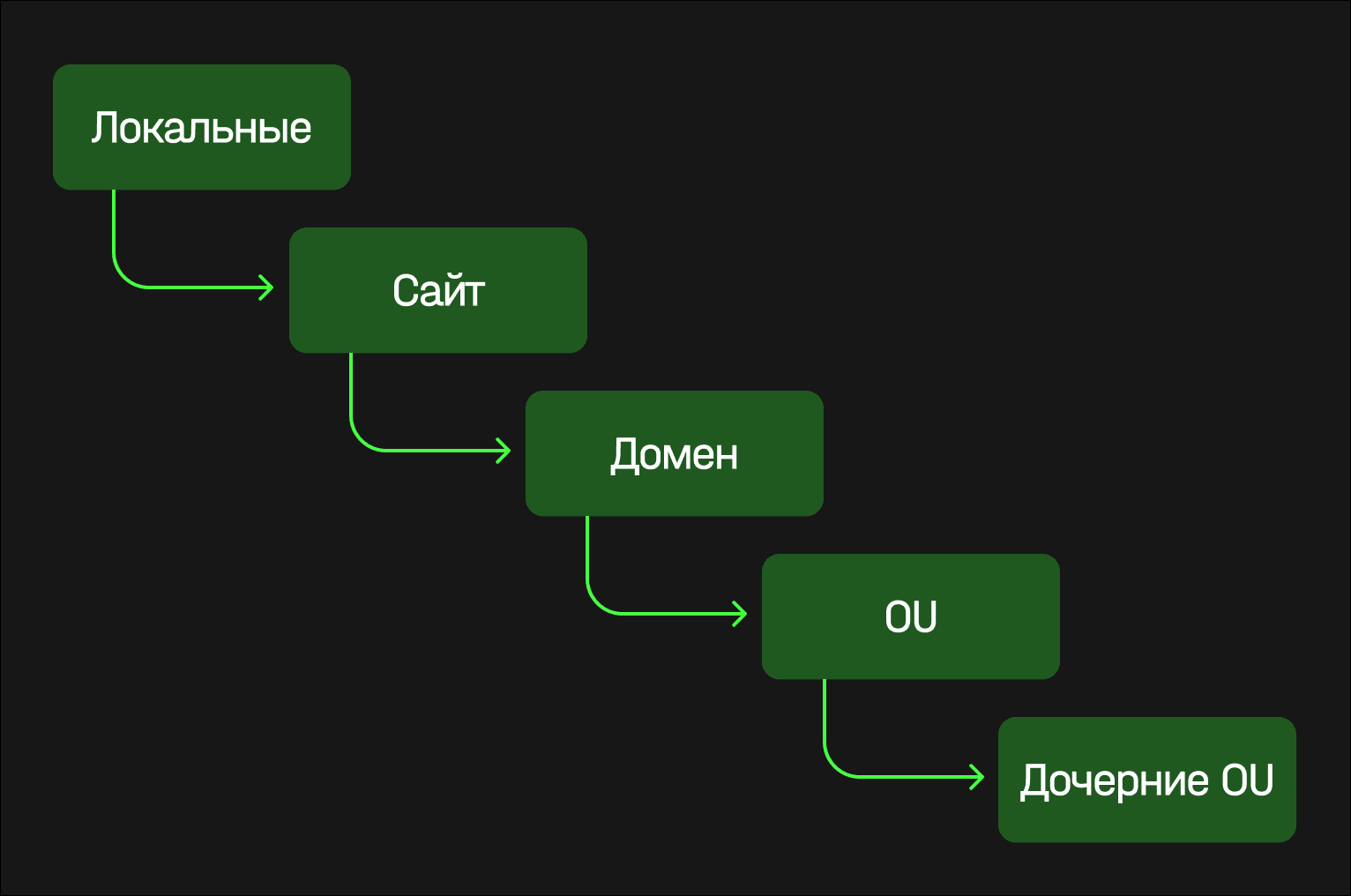


*Рисунок 2. Управление групповыми политиками*

В AD DS объекты групповых политик могут быть применены на следующих уровнях:

* сайты (в контексте AD речь идет о подсетях, а не веб-сайтах),
* домены,
* OU.

Конфигурация, определенная в GPO, используется для всех рабочих станций и пользователей внутри сайта, домена или OU (включая дочерние). GPO может быть связан с несколькими доменами, OU или сайтами.



*Рисунок 3. Порядок обработки GPO*

Например, политика, применяемая на уровне домена, может быть заменена политикой, применяемой на уровне OU для входящих в него объектов. Порядок использования GPO можно просматривать и изменять на вкладке Group Policy Inheritance.

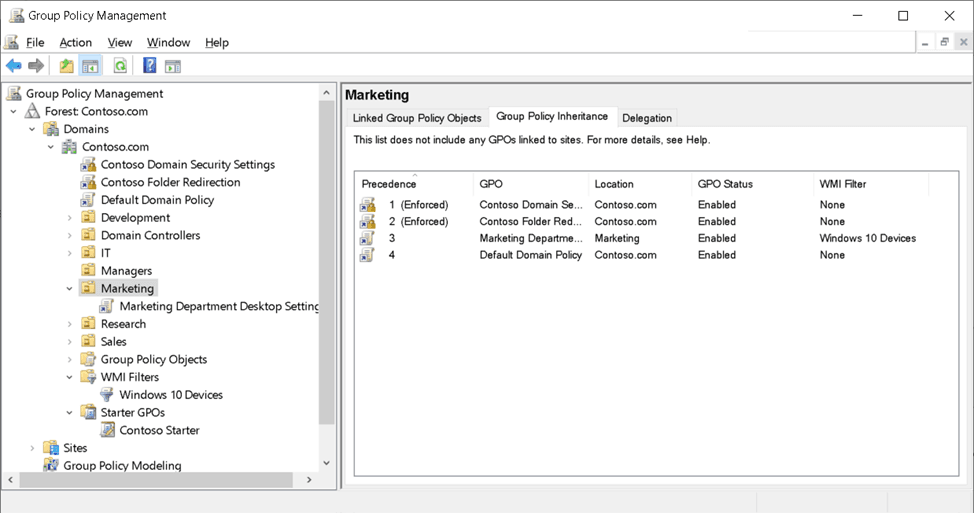


Рисунок 4. Group Policy Inheritance

# Журналирование и мониторинг

В Windows доступны девять категорий политики аудита, каждую из которых можно включить для событий Success или Failure или Success и Failure.

| **Категория** | **Регистрируемые события** | **Подкатегории** |
| --- | --- | --- |
| Account Logon Events | Вход в учетную запись при проверке подлинности учетной записи субъекта безопасности домена на контроллере домена. События выхода из нее не регистрируются | Credential Validation |
| Kerberos Service Ticket Operations |
| Kerberos Authentication Service |
| Other Account Logon Events |
| Account Management | Управление пользователями и группами. Например, пользователи и группы должны отслеживаться при создании, изменении или удалении учетной записи пользователя или компьютера, группы безопасности или группы рассылки, а также при переименовании, отключении или включении учетной записи пользователя или компьютера, при изменении пароля пользователя или компьютера | User Account Management |
| Computer Account Management |
| Security Group Management |
| Distribution Group Management |
| Application Group Management |
| Other Account Management Events |
| Directory Service Access | Доступ субъекта безопасности к объекту Active Directory с собственным указанным списком контроля доступа (SACL) | Directory Service Access |
| Directory Service Changes |
| Directory Service Replication |
| Detailed Directory Service Replication |
| Logon events | Вход при проверке подлинности локального субъекта безопасности на локальном компьютере. События входа записывают имена при входе в домен. События выхода при аудите по категориям не создаются | Logon |
| Network Policy Server |
| IPsec Main Mode |
| IPsec Extended Mode |
| Other Logon (Logoff) Events |
| Logoff |
| Account Lockout |
| IPsec Quick Mode |
| Special Logon |
| Object Access | События при доступе к определенным объектам с включенным аудитом (например, «Открыт», «Чтение», «Переименовано», «Удалено» или «Закрыто»). После включения этой категории аудита администратор должен по отдельности определить, для каких объектов будет включен аудит | File System |
| Registry |
| Kernel Object |
| SAM |
| Certification Services |
| Application Generated |
| Handle Manipulation |
| File Share |
| Filtering Platform Packet Drop |
| Filtering Platform Connection |
| Other Object Access Events |
| Policy Change | Изменения в политиках назначения прав пользователя, брандмауэра Windows, а также в политиках доверия или аудита | Audit Policy Change |
| Authentication Policy Change |
| Authorization Policy Change |
| MPSSVC Rule-Level Policy Change |
| Filtering Platform Policy Change |
| Other Policy Change Events |
| Privilege Use | События, связанные с использованием привилегий. Например, запуск ПО от имени администратора |  |
| Sensitive Privilege Use |
| Nonsensitive Privilege Use |
| Other Privilege Use Events |
| Process Tracking | Аудит отслеживания процесса для таких событий, как активация программы, завершение процесса, обработка дублирования и косвенный доступ к объектам. Это полезно для отслеживания вредоносных пользователей и программ, которые они используют | Process Creation |
| Process Termination |
| DPAPI Activity |
| RPC Events |
| System Events | События, влияющие на безопасность компьютера и его системы или на журнал безопасности. Например, завершение работы и перезапуск компьютера, сбои питания, изменения системного времени, инициализации пакетов проверки подлинности, очистки журналов аудита и множество других событий | Security State Change |
| Security System Extension |
| System Integrity |
| IPsec Driver |
| Other System Events |

# Настройка политик аудита

Политики аудита можно настраивать с помощью групповых политик, утилиты auditpol.exe, API или регистра. Рекомендуемыми являются первые два метода. Администратор может выбрать: включить аудит по категориям или по подкатегориям.

# Управление обновлениями

Для централизованного управления обновлениями в Windows существуют два инструмента: Windows Server Update Services (WSUS) и Configuration Manager.

# WSUS

Сервер WSUS позволяет централизованно управлять процессом обновления программных продуктов Microsoft на узлах сети и автоматизировать его. Этот сервер может поставлять ПО на другие серверы WSUS в корпоративной сети. Администратор самостоятельно определяет, какие серверы WSUS будут подключаться напрямую к Microsoft Update.

Для управления обновлениями с помощью этого инструмента в среде AD используются групповые политики. Благодаря им администратор регулирует конфигурацию обновлений как для рабочих станций, так и для пользователей. Для последних могут быть настроены параметры окна предупреждения о необходимости перезагрузки, а также возможность доступа к Windows Update.

# Configuration Manager

Configuration Manager позволяет централизованно управлять конфигурацией узлов сети. Основные возможности этого инструмента:

* управление приложениями: позволяет создавать, администрировать, развертывать и отслеживать приложения на узлах сети;
* управление обновлениями: позволяет поставлять и устанавливать на узлах сети обновления ПО, недоступного в Microsoft Update;
* развертывание ОС;
* аналитика узлов сети: выполняет сбор данных об их готовности к установке обновления ПО;
* доступ к ресурсам компании: позволяет предоставлять пользователям в организации доступ к данным и приложениям из удаленных расположений (например, к профилям Wi-Fi, VPN, к электронной почте и сертификатам);
* проверка соответствия требованиям: позволяет отслеживать и исправлять параметры конфигурации клиентских устройств в организации, если они нарушают требования;
* защита конечных точек: позволяет централизованно управлять конфигурацией Windows Defender.

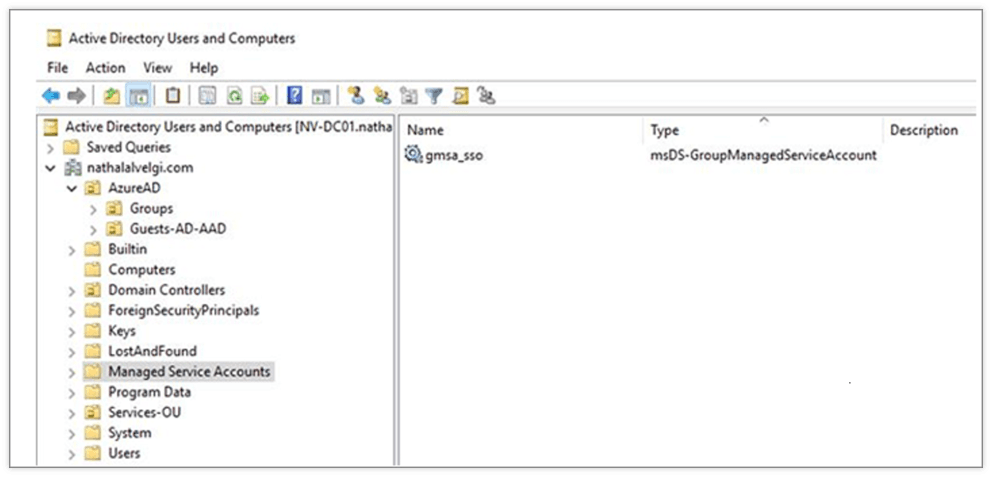
# Управляемые учетные записи служб

Управляемые учетные записи служб (Managed Service Accounts, MSA) — это специальный тип доменных учетных записей, использующийся для безопасного запуска служб. MSA предоставляют автоматизированное управление паролями, упрощенное управление именами служб (SPN), а также возможность делегировать управление другим администраторам. Для ситуаций, когда требуется использование одной учетной записи экземплярами служб на разных серверах, были созданы групповые управляемые учетные записи служб (gMSA).

Преимущества MSA (gMSA):

* использование сложных паролей для учетных записей служб (по умолчанию 240 символов);
* автоматическая смена пароля (по умолчанию через 30 дней);
* отсутствие избыточных прав (например, у этого типа учетных записей отсутствует право локального входа на узел);
* ограничение протокола аутентификации (можно использовать только Kerberos);
* упрощенное управление SPN (учетная запись автоматически переименовывается при изменении свойств сервера).

MSA (gMSA) создаются в Active Directory. По умолчанию для них используется специальный контейнер, расположенный в доменном разделе и называющийся Managed Service Accounts.



*Рисунок 5. Managed Service Accounts*

# Пароли

Параметры парольной политики домена устанавливаются с помощью *Default Domain*. Администратор может настраивать следующие параметры:

* *Enforce password history* — определяет количество предыдущих паролей, которые будут храниться в AD и не могут использоваться повторно.
* *Maximum password age* — срок действия пароля (в днях).
* *Minimum password age* — определяет, как часто пользователь может менять пароль. Если не ограничивать частоту смены, то пользователь может использовать любимый старый пароль, стерев историю паролей.
* *Minimum password length* — минимальная длина пароля.
* *Password must meet complexity requirements* — задает требования к сложности паролей пользователей. При включении этого параметра пользователю запрещено использовать имя своей учетной записи в пароле (не более чем два символа подряд из username или firstname). Кроме того, в пароле должны использоваться три типа символов из следующего списка: цифры (0–9), символы в верхнем регистре, символы в нижнем регистре, спецсимволы ($, #, % и т. п.).
* *Store passwords using reversible encryption* — при включении этого параметра пароли хранятся с использованием обратимого шифрования, что является менее безопасным. Однако он может применяться, если необходимо предоставить доступ к паролю.

Кроме того, администратор может настроить параметры блокировки учетных записей:

* *Account lockout threshold* — количество неверных попыток ввода пароля перед блокировкой.
* *Account lockout duration* — продолжительность блокировки учетной записи.
* *Reset account lockout counter after* — количество минут до сброса счетчика неверных паролей.

Политика паролей применяется на всех пользователей домена, но, начиная с Windows Server 2008, могут быть созданы парольные политики для отдельных групп пользователей, например администраторов. Такие политики называются *Fine-Grained Password Policies*.

# Аудит учетных записей

Периодический аудит учетных записей в AD позволяет выявить следующие проблемы безопасности:

* незаблокированные учетные записи, например уволенных сотрудников;
* избыточные права: в соответствии с принципом минимальных привилегий пользователи должны обладать доступом только к тем данным и операциям, которые необходимы для выполнения их обязанностей. Однако в ряде случаев у пользователя могут появиться избыточные права (например, при переходе сотрудника на другую должность у его учетной записи могут остаться привилегии, которые больше не нужны);
* учетные записи без владельца: сюда относятся технические, тестовые и другие учетные записи, не закрепленные за конкретным сотрудником;
* слабые пароли: для проверки сложности паролей можно сравнить их хеш-коды из базы данных AD (файл *ntds.dit*) со словарем простых или распространенных паролей, например с помощью модуля DSInternals.