ТЕМА 5.2. МЕХАНИЗМЫ БЕЗОПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

В данной теме рассматриваются следующие вопросы:

- Идентификаторы безопасности (SID).
- Маркеры защиты.
- Списки управления доступом (ACL).
- Доменные службы Active Directory.
- Виды групп пользователей.

Лекции – 2 часа, лабораторные занятия – 2 часа, самостоятельная работа – 2 часа.

Экзаменационные вопросы по теме:

- Механизмы безопасности в операционных системах семейства Windows.

5.2.1. Идентификаторы безопасности (SID)

Идентификатор безопасности (SID) — это уникальное значение переменной длины, используемое для идентификации доверенного лица. Каждая учетная запись имеет уникальный идентификатор безопасности, выданный центром сертификации, таким как контроллер домена Windows, и хранящийся в базе данных безопасности. Каждый раз, когда пользователь входит в систему, система получает идентификатор безопасности для этого пользователя из базы данных и помещает его в маркер доступа для этого пользователя. Система использует SID в маркере доступа для идентификации пользователя во всех последующих взаимодействиях с безопасностью Windows. Если идентификатор SID используется в качестве уникального идентификатора пользователя или группы, его нельзя использовать повторно для идентификации другого пользователя или группы [1].

Безопасность Windows использует идентификаторы безопасности в следующих элементах безопасности:

- в дескрипторах безопасности для идентификации владельца объекта и основной группы;
- в записях контроля доступа для определения доверенного лица, для которого разрешен, запрещен или проверен доступ;
- в маркерах доступа — для идентификации пользователя и групп, к которым принадлежит пользователь.

В дополнение к уникально созданным идентификаторам безопасности для конкретного домена, назначенным определенным пользователям и группам, существуют хорошо известные идентификаторы безопасности, которые определяют универсальные группы и универсальных пользователей. Например, известный идентификатор безопасности Все (Everyone) идентифицируют группу, в которую входят все пользователи.

Большинству приложений никогда не требуется работать с идентификаторами безопасности. Так как имена известных идентификаторов безопасности могут различаться, следует использовать функции для создания идентификатора безопасности на основе предопределенных констант, а не имени хорошо известного идентификатора безопасности. Например, английская версия операционной системы Windows для США имеет хорошо известный идентификатор безопасности с именем BUILTIN\Administrators, который может иметь другое имя в международных версиях системы.

Если вам нужно работать с идентификаторами безопасности, не управляйте ими напрямую. Вместо этого используйте следующие функции.

Таблица 5.2.1. Функции Windows API для работы с идентификаторами безопасности

Функция	Описание
AllocateAndInitializeSid	Выделяет и инициализирует идентификатор безопасности с указанным количеством дополнительных учетных данных
ConvertSidToStringSid	Преобразует идентификатор безопасности в формат строки, подходящий для отображения, хранения или транспорта
ConvertStringSidToSid	Преобразует идентификатор безопасности строкового формата в допустимый функциональный идентификатор безопасности
CopySid	Копирует идентификатор безопасности источника в буфер

EqualPrefixSid	Проверяет два значения префикса SID на равенство. Префикс SID — это весь идентификатор безопасности, за исключением последнего значения подчиненного
EqualSid	Проверяет два идентификатора безопасности на равенство. Они должны точно совпадать, чтобы считаться равными
FreeSid	Освобождает ранее выделенный идентификатор безопасности с помощью функции **AllocateAndInitializeSid**
GetLengthSid	Извлекает длину идентификатора безопасности
GetSidIdentifierAuthority	Извлекает указатель на центр идентификатора для идентификатора sid
GetSidLengthRequired	Извлекает размер буфера, необходимого для хранения идентификатора безопасности с указанным числом вложенных учетных данных
GetSidSubAuthority	Извлекает указатель на указанную вложенную проверку подлинности в идентификаторе безопасности
GetSidSubAuthorityCount	Извлекает количество вложенных учетных данных в идентификаторе безопасности
InitializeSid	Инициализирует структуру SID
IsValidSid	Проверяет допустимость идентификатора безопасности, проверяя, что номер редакции находится в пределах известного диапазона и что количество вложенных авторов меньше максимального
LookupAccountName	Извлекает идентификатор безопасности, соответствующий указанному имени учетной записи
LookupAccountSid	Извлекает имя учетной записи, соответствующее указанному идентификатору безопасности

5.2.2. Маркеры защиты

Маркер доступа — это объект, описывающий контекст безопасности процесса или потока. Сведения в маркере включают удостоверение и привилегии учетной записи пользователя, связанной с процессом или потоком. Когда пользователь входит в систему, система проверяет пароль пользователя, сравнивая его с информацией, хранящейся в базе данных безопасности. Если пароль прошел проверку подлинности, система создает маркер доступа. Каждый процесс, выполняемый от имени этого пользователя, имеет копию этого маркера доступа [2].

Система использует маркер доступа для идентификации пользователя, когда поток взаимодействует с защищаемым объектом или пытается выполнить системную задачу, требующую привилегий. Маркеры доступа содержат следующие сведения:

- Идентификатор безопасности (SID) для учетной записи пользователя
- Идентификаторы безопасности для групп, членом которых является пользователь
- Идентификатор безопасности входа, который идентифицирует текущий сеанс входа в систему.
- Список привилегий, которыми пользовались пользователи или группы пользователей.
- Идентификатор безопасности владельца
- Идентификатор безопасности для основной группы

- DACL по умолчанию, используемый системой, когда пользователь создает защищаемый объект без указания дескриптора безопасности.
- Источник маркера доступа
- Является ли маркер основным или маркером олицетворения
- Необязательный список ограничений идентификаторов безопасности
- Текущие уровни олицетворения
- Другая статистика.

Каждый процесс имеет основной маркер, описывающий контекст безопасности учетной записи пользователя, связанной с процессом. По умолчанию система использует первичный маркер, когда поток процесса взаимодействует с защищаемым объектом. Кроме того, поток может олицетворять учетную запись клиента. Олицетворение позволяет потоку взаимодействовать с защищаемыми объектами с помощью контекста безопасности клиента. Поток, олицетворяющий клиента, имеет как основной маркер, так и маркер олицетворения.

Используйте функцию **`OpenProcessToken`**, чтобы получить дескриптор основного маркера процесса. Используйте функцию **`OpenThreadToken`** для получения дескриптора маркера олицетворения потока.

Для управления маркерами доступа можно использовать следующие функции.

Таблица 5.2.2. Функции для управления маркерами доступа

Функция	Описание
`AdjustTokenGroups`	Изменяет сведения о группе в маркере доступа.
`AdjustTokenPrivileges`	Включает или отключает привилегии в маркере доступа. Он не предоставляет новые привилегии и не отменяет существующие.
`CheckTokenMembership`	Определяет, включен ли указанный идентификатор безопасности в указанном маркере доступа.
`CreateRestrictedToken`	Создает новый маркер, который является ограниченной версией существующего маркера. Ограниченный маркер может иметь отключенные идентификаторы БЕЗОПАСНОСТИ, удаленные привилегии и список ограниченных идентификаторов БЕЗОПАСНОСТИ.
`DuplicateToken`	Создает новый токен олицетворения, дублирующий существующий маркер.
`DuplicateTokenEx`	Создает новый основной маркер или маркер олицетворения, который дублирует существующий маркер.
`GetTokenInformation`	Извлекает сведения о маркере.
`IsTokenRestricted`	Определяет, содержит ли маркер список ограничивающих идентификаторов безопасности.
`OpenProcessToken`	Извлекает дескриптор основного маркера доступа для процесса.
`OpenThreadToken`	Извлекает дескриптор маркера доступа олицетворения для потока.
`SetThreadToken`	Назначает или удаляет токен олицетворения для потока.
`SetTokenInformation`	Изменяет владельца маркера, основную группу или DACL по умолчанию

.

5.2.3. Списки управления доступом (ACL)

Дескриптор безопасности содержит сведения о безопасности, связанные с защищаемым объектом. Дескриптор безопасности состоит из структуры SECURITY_DESCRIPTOR и связанных с ней сведений о безопасности [3]. Дескриптор безопасности может содержать следующие сведения о безопасности:

- Идентификаторы безопасности для владельца и основной группы объекта.
- DACL, указывающий права доступа, разрешенные или запрещенные определенным пользователям или группам.
- SACL, указывающий типы попыток доступа, которые создают записи аудита для объекта.
- Набор битов элементов управления, которые определяют значение дескриптора безопасности или его отдельных членов.

Приложения не должны напрямую управлять содержимым дескриптора безопасности. API Windows предоставляет функции для задания и получения сведений о безопасности в дескрипторе безопасности объекта. Кроме того, существуют функции для создания и инициализации дескриптора безопасности для нового объекта.

Списки управления доступом (ACL) состоят из записей управления доступом (ACE). Каждый ACE в ACL идентифицирует доверенного лица и указывает права доступа, разрешенные, запрещенные или регистрируемые для этого доверенного лица [4]. Дескриптор безопасности для защищаемого объекта может содержать два типа списков управления доступом: DACL и SACL.

Список управления доступом на уровне пользователей (DACL) определяет доверенных лиц, которым разрешен или запрещен доступ к защищаемому объекту. Когда процесс пытается получить доступ к защищаемому объекту, система проверяет ACE в DACL объекта, чтобы определить, следует ли предоставить доступ к нему. Если у объекта нет DACL, система предоставляет полный доступ всем пользователям. Если DACL объекта не имеет ACE, система отклоняет все попытки доступа к объекту, так как DACL не разрешает какие-либо права доступа. Система проверяет ACE в последовательности, пока не найдет один или несколько ACE, которые разрешают все запрошенные права доступа, или пока не будет отказано в любом из запрошенных прав доступа.

Системный список управления доступом (SACL) позволяет администраторам регистрировать попытки доступа к защищенному объекту. Каждый ACE указывает типы попыток доступа со стороны указанного доверенного лица, которые приводят к созданию системой записи в журнале событий безопасности. ACE в SACL может создавать записи аудита при сбое попытки доступа и/или при успешном выполнении.

Предоставляется несколько функций, которые извлекают сведения об управлении доступом из списка управления доступом (ACL). К ним относятся функции для определения прав доступа, которые ACL предоставляет или проверяет для указанного доверенного лица. Другие функции позволяют извлекать сведения о записях управления доступом (ACE) в ACL [5].

Функция **GetExplicitEntriesFromAcl** извлекает массив EXPLICIT_ACCESS структур, описывающих ACE в списке ACL. Это может быть полезно при копировании сведений ACE из одного ACL в другой. Например, вызов **GetExplicitEntriesFromAcl** для получения сведений об ACE в одном списке управления доступом может сопровождаться передачей возвращенных EXPLICIT_ACCESS структур в вызове функции **SetEntriesInAcl** для создания эквивалентных ACE в новом списке управления доступом.

Функция **GetEffectiveRightsFromAcl** позволяет определить действующие права доступа, предоставляемые DACL указанному доверенному лицу. Действующие права доступа доверенного лица — это права доступа, предоставляемые DACL доверенному лицу или

любым группам, членом которых является попечитель. **GetEffectiveRightsFromAcl** проверяет все ACE, разрешенные и запрещенные в доступе, в указанном DACL.

Чтобы определить права доступа доверенного лица к объекту, выполните следующие действия.

1. Вызовите функцию **GetSecurityInfo** или **GetNamedSecurityInfo**, чтобы получить указатель на DACL объекта.
2. Вызовите функцию **GetEffectiveRightsFromAcl**, чтобы получить права доступа, предоставляемые DACL указанному доверенному лицу.

Функция **GetAuditedPermissionsFromAcl** позволяет проверить SACL, чтобы определить права доступа, проверенные для указанного доверенного лица или для любых групп, членом которых является это доверенное лицо. Проверяемые права указывают типы попыток доступа, которые приводят к тому, что система создает запись аудита в журнале событий безопасности. Функция возвращает две маски доступа: одну, содержащую права доступа, отслеживаемые для неудачных попыток доступа, а другую — права доступа, отслеживаемые для успешного доступа. **GetAuditedPermissionsFromAcl** проверяет все ACE с системным аудитом в SACL.

5.2.4. Доменные службы Active Directory

Каталог — это иерархическая структура, в которой хранятся сведения об объектах в сети. Служба каталогов, например, службы домен Active Directory (AD DS), предоставляет методы хранения данных каталога и предоставления этих данных сетевым пользователям и администраторам. Например, AD DS хранит сведения об учетных записях пользователей, таких как имена, пароли, номера телефонов и т. д., а также позволяет другим авторизованным пользователям в той же сети получить доступ к этой информации [6].

Active Directory хранит сведения об объектах в сети и предоставляет эту информацию администраторам и пользователям, которые могут легко найти и использовать ее. Active Directory использует структурированное хранилище данных в качестве основы для логической иерархической организации сведений в каталоге.

Это хранилище данных, также известное как каталог, содержит сведения о объектах Active Directory. Эти объекты обычно включают общие ресурсы, такие как серверы, тома, принтеры и сетевые учетные записи пользователя и компьютера.

Безопасность интегрирована с Active Directory с помощью проверки подлинности входа и управления доступом к объектам в каталоге. С помощью одного входа в сеть администраторы могут управлять данными каталога и организацией по всей сети, а авторизованные пользователи сети могут получать доступ к ресурсам в любой точке сети. Администрирование на основе политики облегчает управление даже очень сложной сетью.

Active Directory также включает следующие компоненты:

- **Схема** — набор правил, который определяет классы объектов и атрибутов, содержащихся в каталоге, ограничения и ограничения экземпляров этих объектов, а также формат их имен.
- **Глобальный каталог**, содержащий сведения о каждом объекте в каталоге. Это позволяет пользователям и администраторам находить сведения о каталоге независимо от того, какой домен в каталоге фактически содержит данные.
- **Механизм запроса и индекса**, чтобы объекты и их свойства могли быть опубликованы и найдены сетевыми пользователями или приложениями.
- **Служба репликации**, которая синхронизирует данные каталога по сети. Все контроллеры домена в домене участвуют в репликации и содержат полную копию

всех сведений о каталоге для своего домена. Любые изменения данных каталога реплицируются в домене на все контроллеры домена.

Администраторы используют Active Directory для хранения и организации объектов в сети (таких как пользователи, компьютеры, устройства и т. д.) в безопасную иерархическую структуру содержания, известную как логическая структура. Хотя логическая структура Active Directory представляет собой иерархическую организацию всех пользователей, компьютеров и других физических ресурсов, основу логической структуры составляют лес и домен. Леса, являющиеся границами безопасности логической структуры, могут быть структурированы таким образом, чтобы обеспечить автономию и изоляцию данных и служб в организации таким образом, чтобы они могли как отражать идентичность сайтов и групп, так и устранять зависимости от физической топологии [7].

Домены могут быть структурированы в лес, чтобы обеспечить автономию данных и сервисов (но не изоляцию), а также оптимизировать репликацию в заданном регионе. Такое разделение логической и физической структур улучшает управляемость и снижает административные затраты, поскольку на логическую структуру не влияют изменения физической структуры. Логическая структура также позволяет контролировать доступ к данным. Это означает, что вы можете использовать логическую структуру для разделения данных на отдельные отсеки, чтобы можно было контролировать доступ к ним, контролируя доступ к различным отсекам.

Данные, хранящиеся в Active Directory, могут поступать из множества различных источников. При таком большом количестве различных источников данных и таком большом количестве различных типов данных Active Directory должна использовать некий тип стандартизированного механизма хранения, чтобы поддерживать целостность хранимых данных. В Active Directory объекты используются для хранения информации в каталоге, и все объекты определены в схеме. Определения объектов содержат такую информацию, как тип данных и синтаксис, которую каталог использует для обеспечения достоверности сохраненных данных. Никакие данные не могут храниться в каталоге, если сначала в схеме не определены объекты, используемые для хранения данных. Схема по умолчанию содержит все определения объектов, необходимые для функционирования Active Directory; однако вы также можете добавить в схему определения объектов.

Хотя каталог предоставляется вам через логическую структуру, состоящую из таких элементов, как домены и леса, сам каталог реализуется через физическую структуру, состоящую из базы данных, которая хранится на всех контроллерах домена в лесу. Хранилище данных Active Directory обрабатывает весь доступ к базе данных. Хранилище данных состоит как из сервисов, так и из физических файлов. Эти службы и физические файлы делают каталог доступным и управляют процессами чтения и записи данных внутри базы данных, которая существует на жестком диске каждого контроллера домена.

Структура Active Directory и архитектура хранения

Структура и архитектура хранения Active Directory состоят из четырех частей:

- **Домены и леса Active Directory**. Леса, домены и организационные единицы (OU) составляют основные элементы логической структуры Active Directory. Лес определяет один каталог и представляет собой границу безопасности. Леса содержат домены.
- **Поддержка системы доменных имен (DNS) для Active Directory**. DNS предоставляет службу разрешения имен для определения местоположения контроллера домена и иерархическую структуру, которую Active Directory может использовать для обеспечения соглашения об именах, которое может отражать организационную структуру.

- **Схема**. Схема предоставляет определения объектов, которые используются для создания объектов, хранящихся в каталоге.
- **Хранилище данных**. Хранилище данных — это часть каталога, которая управляет хранением и получением данных на каждом контроллере домена.

На рис. 5.2.1 показана структура данных и архитектура хранения Active Directory.

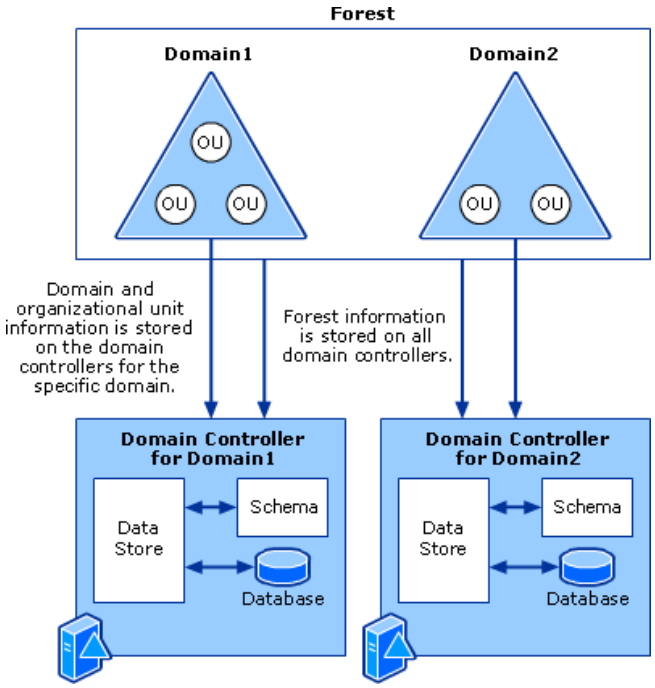

Рис. 5.2.1. Структура данных Active Directory и архитектура хранения

Домены и леса Active Directory

Домены разделяют каталог на более мелкие разделы в одном лесу. Такое разделение приводит к большему контролю над тем, как реплицируются данные, что позволяет установить эффективную топологию репликации и не тратить пропускную способность сети на репликацию данных там, где она не требуется. Подразделения позволяют группировать ресурсы в домене для целей управления, например, применения групповой политики или делегирования контроля администраторам.

На рис. 5.2.2 показаны взаимосвязи подразделений, доменов и лесов.

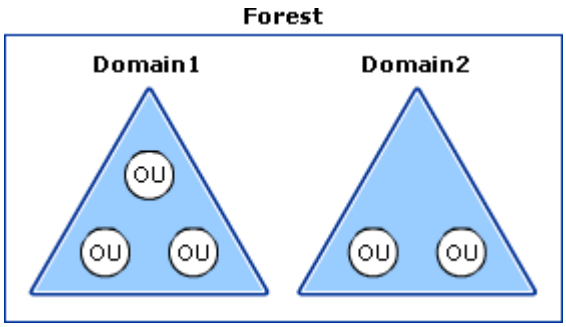

Рис. 5.2.2 Логическая архитектура леса

Поддержка DNS для Active Directory

Active Directory использует DNS в качестве механизма определения местоположения контроллера домена. При выполнении любой из основных операций Active Directory, таких как проверка подлинности, обновление или поиск, компьютеры, присоединенные к домену, используют DNS для поиска контроллеров домена Active Directory, а эти контроллеры домена используют DNS для поиска друг друга. Например, когда сетевой пользователь с учетной записью пользователя Active Directory входит в домен Active

Directory, компьютер пользователя использует DNS для обнаружения контроллера домена для домена Active Directory, в который пользователь хочет войти.

Чтобы войти в сеть, состоящую из леса Active Directory, клиентская рабочая станция сначала должна иметь возможность найти ближайший контроллер домена. Контроллер домена необходим для первоначальной аутентификации как рабочей станции, так и пользователя и для последующей авторизации пользователя к файлам и ресурсам, к которым пользователю необходим доступ. Поддержка, предоставляемая Active Directory через DNS, позволяет клиентской рабочей станции обнаружить контроллер домена.

Схема Active Directory

Схема Active Directory содержит определения всех объектов, которые используются для хранения информации в каталоге. Для каждого леса существует одна схема. Однако копия схемы существует на каждом контроллере домена в лесу. Таким образом, каждый контроллер домена имеет быстрый доступ к любому определению объекта, которое ему может понадобиться, и каждый контроллер домена использует одно и то же определение при создании данного объекта. Хранилище данных использует схему для предоставления определений объектов, а хранилище данных использует эти определения для обеспечения целостности данных. В результате все объекты создаются единообразно, и не имеет значения, какой контроллер домена создает или изменяет объект, поскольку все контроллеры домена используют одно и то же определение объекта.

На рис. 5.2.3 показана связь схемы с хранилищем данных в архитектуре схемы.

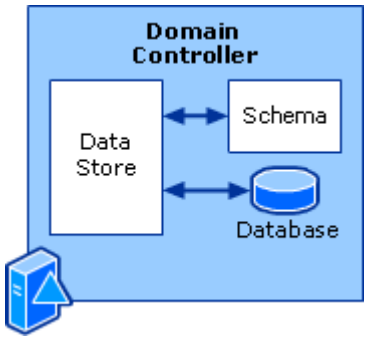

Рис. 5.2.3. Архитектура схемы

Хранилище данных Active Directory

Хранилище данных Active Directory состоит из нескольких компонентов, которые вместе предоставляют услуги каталогов клиентам каталогов. Эти компоненты включают в себя следующее:

- Четыре интерфейса:
  - Облегченный протокол доступа к каталогам (LDAP)
  - Репликация (REPL) и интерфейс управления контроллером домена
  - API обмена сообщениями (MAPI)
  - Менеджер учетных записей безопасности (SAM)
- Три компонента услуги:
  - Агент системы каталогов (DSA)
  - Уровень базы данных
  - Расширяемый механизм хранения данных (ESE)
- База данных каталога, в которой фактически хранятся данные.

На рис. 5.2.4 показаны взаимосвязи этих компонентов в архитектуре хранилища данных.

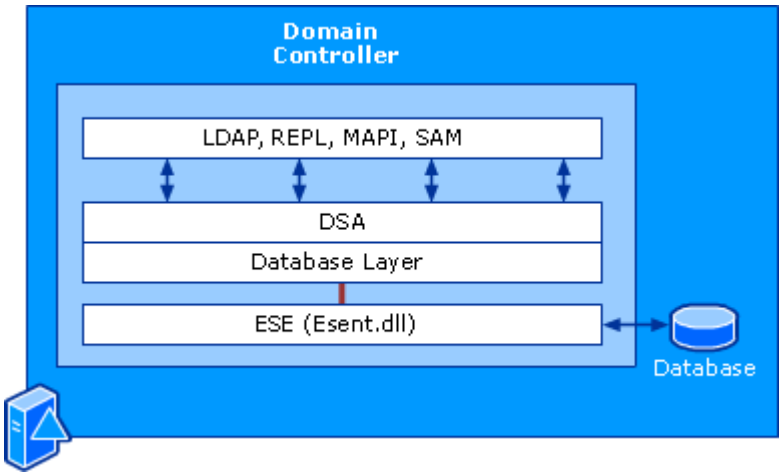

Рис. 5.2.4. Архитектура хранилища данных

5.2.5. Виды групп пользователей

Active Directory имеет две формы общих субъектов безопасности: учетные записи пользователей и учетные записи компьютера. Эти учетные записи представляют собой физическую сущность, которая является пользователем или компьютером. Учетная запись пользователя также может использоваться в качестве выделенной учетной записи службы для некоторых приложений [8].

Группы безопасности — это способ объединения учетных записей пользователей, учетных записей компьютеров и других групп в управляемые единицы. Работа с группами вместо отдельных пользователей помогает упростить обслуживание сети и администрирование.

Active Directory имеет два типа групп:

- **Группы безопасности**. Используйте для назначения разрешений общим ресурсам.
- **Группы рассылки**: создание списков рассылки электронной почты.

Группы безопасности

Группы безопасности могут обеспечить эффективный способ назначения доступа к ресурсам в сети. С помощью групп безопасности можно выполнять следующие действия.

- **Назначение прав пользователей группам безопасности в Active Directory**. Например, включив пользователя в группу **Администраторы схемы**, можно предоставить ему разрешение изменять схему Active Directory.
- **Назначение разрешения группам безопасности для ресурсов**. Группы безопасности могут быть использованы в списках управления доступом (DACLs), определяющих разрешения на ресурсы и объекты. Когда администраторы назначают разрешения для ресурсов, таких как общие папки или принтеры, они должны назначать эти разрешения группе безопасности вместо отдельных пользователей. Разрешения назначаются группе один раз вместо нескольких раз каждому отдельному пользователю. Каждая учетная запись, добавленная в группу, получает права, назначенные этой группе в Active Directory. Пользователь получает разрешения, определенные для этой группы.

Группу безопасности также можно использовать в качестве сущности электронной почты. Отправка сообщения электронной почты в группу безопасности отправляет сообщение всем членам группы.

Группы рассылки

Группы рассылки можно использовать только для отправки электронной почты в коллекции пользователей с помощью почтового приложения, например, Exchange Server. Группы рассылки не включены в систему безопасности, поэтому их нельзя включить в списки управления доступом.

Область действия группы

Каждая группа имеет область, определяющий степень применения группы в дереве домена или лесу. Область группы определяет, где можно предоставить разрешения сети для группы. Active Directory определяет следующие три области для групп:

- Универсальная
- Глобальная
- Локальная в домене

Таблица. 5.2.3. Свойства универсальных групп.

Может включать:	Учетные записи из любого домена в одном лесу. Глобальные группы из любого домена в одном лесу. Другие универсальные группы из любого домена в одном лесу
Допустимые преобразования	Можно преобразовать в локальную область домена, если группа не является членом какой-либо другой универсальной группы. Можно преобразовать в глобальную область, если группа не содержит другую универсальную группу
Может предоставлять разрешения	В любом домене в одном лесу или доверенных лесах
Может быть членом:	Другие универсальные группы в том же лесу. Локальные группы домена в одном лесу или доверенных лесах. Локальные группы на компьютерах в одном лесу или доверенных лесах

Таблица 5.2.4. Свойства глобальных групп.

Может включать:	Учетные записи из одного домена Другие глобальные группы из того же домена
Допустимые преобразования	Можно преобразовать в универсальную область если группа не является членом другой глобальной группы
Может предоставлять разрешения	В любом домене в одном лесу или доверенных доменах или лесах
Может быть членом:	Универсальные группы из любого домена в одном лесу Другие глобальные группы из того же домена Локальные группы домена из любого домена в одном лесу или из любого доверенного домена

Таблица 5.2.5. Свойства локальных в домене групп.

Может включать:	Учетные записи из любого домена или любого доверенного домена Глобальные группы из любого домена или любого доверенного домена Универсальные группы из любого домена в одном лесу Другие локальные группы домена из того же домена Учетные записи, глобальные группы и универсальные группы из других лесов и из внешних доменов

Допустимые преобразования	Можно преобразовать в универсальную область если группа не содержит другую локальную группу домена.
Может предоставлять разрешения	В том же домене
Может быть членом:	Другие локальные группы домена из того же домена Локальные группы на компьютерах в одном домене, за исключением встроенных групп с известными идентификаторами безопасности (SID)

Список использованных источников

1. Идентификаторы безопасности
https://learn.microsoft.com/ru-ru/windows/win32/secauthz/security-identifiers

2. Маркеры доступа
https://learn.microsoft.com/ru-ru/windows/win32/secauthz/access-tokens

3. Дескрипторы безопасности
https://learn.microsoft.com/ru-ru/windows/win32/secauthz/security-descriptors

4. Списки управления доступом
https://learn.microsoft.com/ru-ru/windows/win32/secauthz/access-control-lists

5. Получение сведений из ACL
https://learn.microsoft.com/ru-ru/windows/win32/secauthz/getting-information-from-an-acl

6. Обзор доменных служб Active Directory
https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

7. Структура Active Directory и технологии хранения
https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-server-2003/cc759186(v=ws.10)

8. Группы безопасности Active Directory
https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/manage/understand-security-groups