Вопросы пункт 1

Диспетчер учетных записей (SAM - Security Account Manager)

Диспетчер учетных записей безопасности (SAM) — это база данных, которая присутствует на компьютерах под управлением операционных систем Windows, в которых хранятся учетные записи пользователей и дескрипторы безопасности для пользователей на локальном компьютере.

- Объекты SAM включают следующее:
- SAM_ALIAS: локальная группа
- SAM_GROUP: группа, которая не является локальной группой.
- SAM_USER: учетная запись пользователя
- SAM_DOMAIN: домен
- SAM_SERVER: учетная запись компьютера

Монитор безопасности (SRM - Security Reference Monitor)

Все более важным аспектом операционных систем является безопасность. Перед выполнением действия операционная система должна убедиться, что это действие не является нарушением системной политики. Например, устройство может быть доступно или не всем запросам.

Windows использует список управления доступом (ACL), чтобы определить, какие объекты имеют определенную безопасность. Монитор справки по безопасности в режиме ядра Windows предоставляет подпрограммы для работы драйвера с управлением доступом.

Маркер доступа (access token)

Маркер доступа (англ. Access token) — программный объект операционных систем класса **Microsoft Windows**, содержит информацию по безопасности сеанса и идентифицирует пользователя, группу пользователей и пользовательские привилегии.

Маркер доступа — это объект, инкапсулирующий дескриптор безопасности процесса[1]. Прилагаемый к процессу, дескриптор безопасности идентифицирует собственника объекта[2][3]. Пока маркер используется для представления только информации по безопасности, он технически свободен по своему содержанию и может содержать любые данные. Маркер доступа используется Windows, когда процесс пытается взаимодействовать с объектами, дескрипторы безопасности которых требуют контроль доступа[1]. Маркер доступа представлен системным объектом типа *Token* . По причине того, что маркер — обычный системный объект, доступ к самому маркеру может быть проконтролирован с помощью дескриптора безопасности, но это обычно никогда не делается на практике.

Маркер доступа генерируется сервисом входа в систему, когда пользователь регистрируется и его подлинность успешно установлена, определяя права пользователя в дескрипторе безопасности, заключенном в маркер. Маркер прилагается к каждому процессу, созданному сессией пользователя (процессы, собственником которых является пользователь)[1]. Когда бы такой процесс ни запрашивал любой ресурс, доступ к которому контролируется, Windows смотрит в дескрипторе безопасности в маркере доступа, имеет ли пользователь, владелец данного процесса, право доступа к данным, и, если да, какие операции (чтение, запись/изменение) ему дозволены. Если операция дозволена в контексте данного пользователя, Windows позволяет процессу её продолжать, если нет, то отказывает в доступе.

https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D0%BA%D0%B5%D1%80_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0

Маркер доступа состоит из различных полей, включая, но не ограничиваясь, следующие:

- идентификатор;
- идентификатор ассоциированной сессии входа в систему. Сессия обслуживается сервисом идентификации и заполняется идентификационными пакетами с коллекцией всей информации (мандат), сообщенной пользователем во время входа в систему. Мандат используется для доступа к удаленным системам без необходимости переидентифицировать клиента, предусматривающий, что все вовлеченные системы делятся информацией по идентификации.
- идентификатор пользователя. Это поле наиболее важное и защищено от записи.
- идентификатор групп, частью который является пользователь (или, точнее, субъект). Позволяющая получить доступ к различным объектам, ассоциированным с сессией.
- ограничивающие идентификаторы группы (поле не обязательно). Это дополнительное множество групп, не дающее дополнительного доступа, но ограничивающее его: доступ к объекту открыт только, если он также открыт для одной из этих групп. Данный вид групп не может быть ни удалён, ни отключён.
- привилегии, то есть специальные возможности пользователя. Большинство привилегий по умолчанию отключено, чтобы исключить возможные повреждения от плохо защищённых программ. Начиная с Windows XP Service Pack 2 и Windows Server 2003, привилегии могут

быть удалены из маркера доступа вызовом AdjustTokenPrivileges() с атрибутом SE_PRIVILEGE_REMOVE.

Идентификатор безопасности (SID - Security Identifier)

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

Если идентификатор sid используется в качестве уникального идентификатора пользователя или группы, его нельзя использовать повторно для идентификации другого пользователя или группы.

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.

Привилегии пользователя

Привилегия — это право учетной записи, например учетной записи пользователя или группы, выполнять различные связанные с системой операции на локальном компьютере, такие как завершение работы системы,

загрузка драйверов устройств или изменение системного времени. Привилегии отличаются от прав доступа двумя способами:

Привилегии управляют доступом к системным ресурсам и задачам, связанным с системой, в то время как права доступа управляют доступом к защищаемым объектам.

- Системный администратор назначает привилегии учетным записям пользователей и групп, в то время как система предоставляет или запрещает доступ к защищаемому объекту на основе прав доступа, предоставленных в ACE в списке DACL объекта.

Каждая система имеет базу данных учетных записей, в которой хранятся привилегии, которыми пользовались учетные записи пользователей и групп. Когда пользователь входит в систему, система создает маркер доступа , содержащий список привилегий пользователя, включая привилегии, предоставленные пользователю или группам, к которым принадлежит пользователь. Обратите внимание, что привилегии применяются только к локальному компьютеру. учетная запись домена может иметь разные привилегии на разных компьютерах.

Когда пользователь пытается выполнить привилегированную операцию, система проверяет маркер доступа пользователя, чтобы определить, имеет ли пользователь необходимые привилегии, и если да, она проверяет, включены ли эти привилегии. Если пользователь не проходит эти тесты, система не выполняет операцию.

Права пользователя (user rights)

Права пользователя определяют методы, с помощью которых пользователь может войти в систему. Права пользователей применяются на уровне локального устройства и позволяют пользователям выполнять задачи на устройстве или в домене. К правам пользователя относятся права на вход и

разрешения. Права входа определяют, кто имеет право на вход на устройство и как они могут войти в систему. Разрешения прав пользователя управляют доступом к ресурсам компьютера и домена, а также могут переопределять разрешения, заданные для определенных объектов. Права пользователя управляются в групповая политика в разделе **Назначение прав пользователя**.

Каждое право пользователя имеет постоянное имя и связанное с ним имя групповая политика. Имена констант используются при ссылке на пользователя в событиях журнала. Параметры назначения прав пользователя можно настроить в следующем расположении в консоли управления групповая политика (GPMC) в разделе **Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Назначение прав пользователя** или на локальном устройстве с помощью редактора локальных групповая политика (gpedit.msc).

https://learn.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/user-rights-assignment

Права пользователя

Когда пользователь пытается выполнить действие, требующее прав администратора, контроль учетных записей активирует *запрос на согласие*. Запрос уведомляет пользователя о том, что произойдет изменение, и просит предоставить разрешение на продолжение:

- Если пользователь утверждает изменение, действие выполняется с наивысшим доступным уровнем прав
- Если пользователь не утверждает изменение, действие не выполняется и приложение, запросившее это изменение, не будет запущено

Объект доступа

Объектом доступа (или просто объектом) мы будем называть **любой элемент операционной системы, доступ к которому пользователей и других**

субъектов доступа может быть произвольно ограничен. Ключевым словом в данном определении является слово «произвольно».

Субъекты безопасности выполняют действия (включая чтение, запись, изменение или полный контроль) с объектами. Объекты включают файлы, папки, принтеры, разделы реестра и объекты доменные службы Active Directory (AD DS). Общие ресурсы используют списки управления доступом (ACL) для назначения разрешений. Это позволяет диспетчерам ресурсов применять управление доступом следующими способами:

- Запрет доступа для несанкционированных пользователей и групп
- Установка четко определенных ограничений на доступ, предоставляемый авторизованным пользователям и группам

Владельцы объектов обычно предоставляют разрешения группам безопасности, а не отдельным пользователям. Пользователи и компьютеры, добавленные в существующие группы, принимают разрешения этой группы. Если объект (например, папка) может содержать другие объекты (например, вложенные папки и файлы), он называется контейнером. В иерархии объектов связь между контейнером и его содержимым выражается путем ссылки на контейнер в качестве родительского. Объект в контейнере называется дочерним, а дочерний наследует параметры управления доступом родительского объекта. Владельцы объектов часто определяют разрешения для объектов-контейнеров, а не для отдельных дочерних объектов, чтобы упростить управление доступом.

Субъект доступа

Общие ресурсы доступны пользователям и группам, не являющимся владельцем ресурса, и их необходимо защитить от несанкционированного использования. В модели управления доступом пользователи и группы (также называемые субъектами безопасности) представлены уникальными идентификаторами безопасности (SID). Им назначаются права и разрешения, которые информируют операционную систему о том, что может делать каждый

пользователь и группа. У каждого ресурса есть владелец, который предоставляет разрешения субъектам безопасности. Во время проверка управления доступом эти разрешения проверяются, чтобы определить, какие субъекты безопасности могут получить доступ к ресурсу и как они могут получить к нему доступ.

Субъект доступа – это лицо или процесс, действия которого регламентируются правилами разграничения **доступа**: учетная запись, пользователь или иная сущность, выполняющая какие-либо действия с объектами **доступа**

Олицетворение (impersonation)

Олицетворение (impersonation) — средство, используемое в модели защиты **Windows**, предоставляющее возможность отдельному потоку выполняться в контексте защиты отличном от контекста защиты процесса, т. е. действовать от лица другого пользователя.
Олицетворение, например, применяется в модели программирования "клиент-сервер". При заимствовании прав сервер временно принимает профиль защиты клиента, который обращается к ресурсу. Тогда сервер может работать с ресурсом от имени клиента, а система защиты проводить проверку его прав доступа

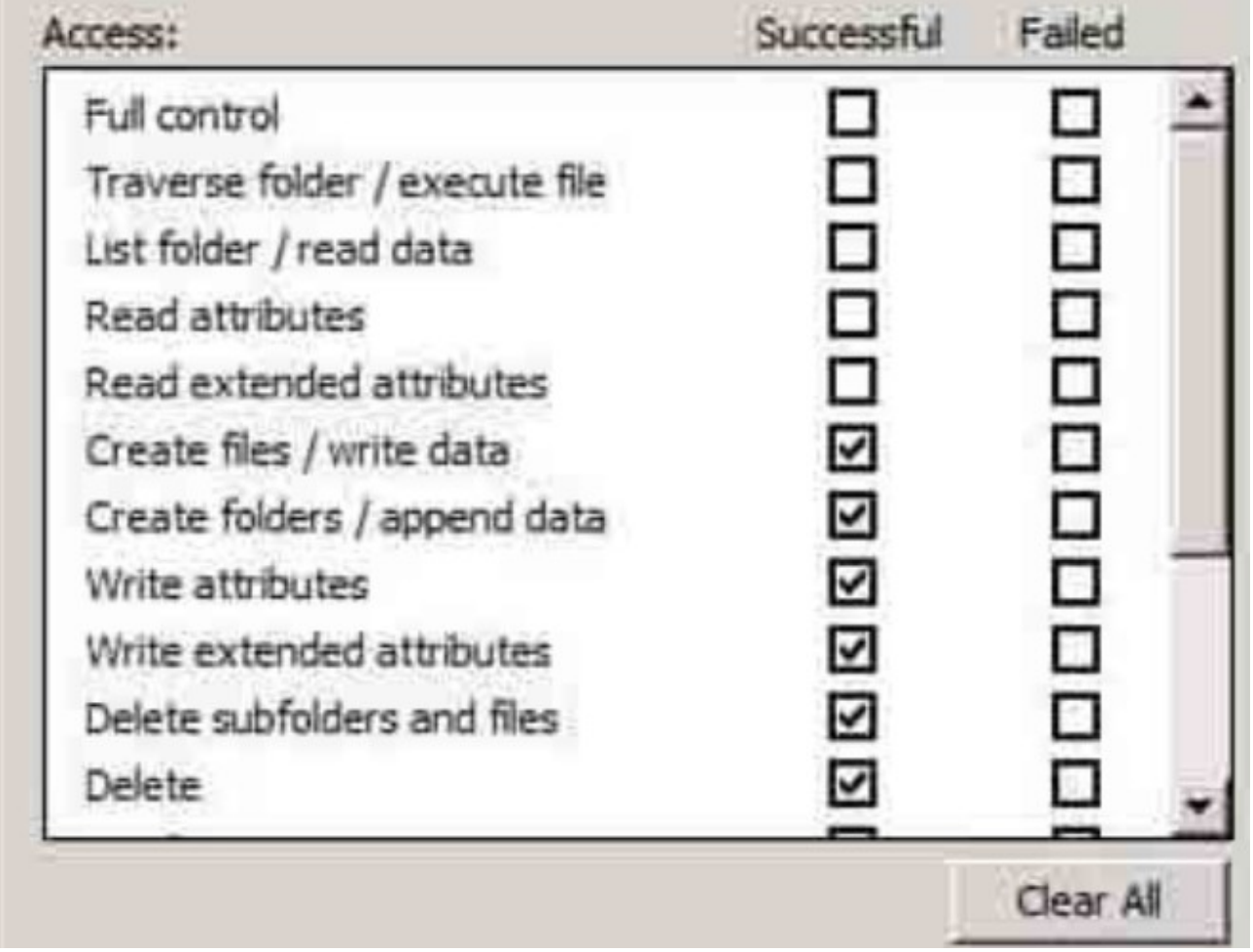
Обычно серверу доступен более широкий круг ресурсов, чем клиенту, и при олицетворении сервер должен терять часть исходных прав доступа. Однако, сервисы олицетворения потенциально опасны и могут быть использованы, наоборот, для повышения привилегий (расширения возможностей текущей учетной записи пользователя до возможностей более привилегированной учетной записи, обычно *суперпользователя*, например, такой как учетная запись администратора или запись SYSTEM). Расширение привилегий может дать злоумышленнику возможность получить уровень прав, достаточный для осуществления несанкционированного доступа к конфиденциальным данным.

Список контроля доступа (ACL - Access Control List)

Список управления доступом (ACL) — это список ACE, созданных операционной системой для управления поведением безопасности, связанным с определенным (защищенным) объектом определенного типа. В Windows существует два типа списков управления доступом:

Access Control List (ACL) — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

В системе с моделью безопасности, основанной на ACL, когда субъект запрашивает выполнение операции над объектом, система сначала проверяет список разрешённых для этого субъекта операций, и только после этого даёт (или не даёт) доступ к запрошенному действию.



https://mega-obzor.ru/spisok-upravleniya-dostupom-acl.html

Список управления доступом – это в основном список, прикрепленный к объекту, определяющий, какие субъекты безопасности (пользователи, группы, компьютеры и т. д.) имеют доступ к объекту и какой уровень доступа им разрешен.

В Windows 7 списки управления доступом правильнее называть дискреционными списками управления доступом (DACL), поскольку они могут настраиваться и управляться администраторами по своему усмотрению.

Существует также другой тип ACL в Windows, называемый System access control list (SACL), который используется для управления генерацией сообщений аудита, когда аудит объектов был настроен в файловой системе.

Системный список управления доступом (SACL) позволяет администраторам регистрировать попытки доступа к защищенному объекту. Каждый ACE определяет типы попыток доступа указанного доверенного лица, которые заставляют систему генерировать запись в журнале событий безопасности. ACE в SACL может генерировать записи аудита, когда попытка доступа терпит неудачу, когда она успешна, или и то, и другое.

Учетная запись

Учётная запись — запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе.

Учётная запись, как правило, содержит сведения, необходимые для идентификации пользователя при подключении к системе, информацию для авторизации и учёта. Это имя пользователя (***логин***) и пароль. Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде для обеспечения его безопасности. Для аутентификации могут использоваться аппаратные средства (вырабатывающие одноразовые ключи, считывающие биометрические характеристики и т. п.), а также одноразовые пароли.

- Учетные записи обычных пользователей предназначены для повседневной работы.
- Учетные записи администратора предоставляют полный контроль над компьютером и должна использоваться только при необходимости.
- Учетные записи гостя предназначены главным образом для лиц, которые должны временного использования компьютера.

Учётная запись Microsoft (англ. *Microsoft account*, ранее известен как: **Microsoft Wallet**, **Microsoft Passport**, **.NET Passport**, **Microsoft Passport Network** и **Windows Live ID**) — сервис идентификации и авторизации в сетевых сервисах корпорации Microsoft, таких как OneDrive, Microsoft 365, Bing, Microsoft Edge, Outlook, Skype, Xbox Network, MSN, Microsoft Store[1].

Домен

Windows network technology enables you to create network domains. A domain is a group of connected Windows computers that share user account information and a security policy.

Сетевая технология Windows позволяет создавать сетевые домены. Домен - это группа соединенных друг с другом компьютеров с фигурным размером Windows; в матче информацию об учетных записях пользователей и политику защиты поставить не удалось. Контроллер домена управляет информацией об учетных записях пользователей для всех членов домена.

Домен Windows NT — собрание участников безопасности (все объекты Active Directory), имеющих единый центр (который называется контроллером домена), использующий единую базу, известную как Active Directory, начиная с Windows 2000, Active Directory Domain Services в Windows Server 2008 и Server 2008 R2, также известный как NT Directory Services на NT операционных системах Windows, или NTDS (то есть учётные записи находятся не на каждом в отдельности компьютере, а на контроллере домена, т. н. сетевой вход в

систему), единую групповую и локальную политики, единые параметры безопасности (применимо к томам с файловой системой NTFS), ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, эксплуатирующей большое число компьютеров. Также становится возможным создать для каждого аккаунта перемещаемый профиль, который будет храниться на выделенном для профилей сервере. В результате пользователи могут работать со своим «Рабочим столом», «Моими документами» и прочими индивидуально настраиваемыми элементами с любого компьютера домена. Стоит заметить, что при больших объёмах профиля время входа пользователя в систему может быть значительно увеличено.

В отличие от рабочих групп, работающих по принципу одноранговой сети, домен реализует клиент-серверную модель.

Домены обычно состоят из компьютеров в одной локальной сети. Однако компьютеры, присоединённые к домену, могут продолжать обмениваться данными со своим контроллером домена через VPN или подключение к Интернету. Это позволяет предприятиям и учебным заведениям удалённо управлять ноутбуками, которые они предоставляют своим сотрудникам и учащимся.

Рабочая группа — это термин Microsoft для компьютеров Windows, подключённых через одноранговую сеть. Рабочие группы — это ещё одна организационная единица для компьютеров Windows в сети. Рабочие группы позволяют этим машинам обмениваться файлами, доступом в Интернет, принтерами и другими ресурсами по сети. Одноранговая сеть устраняет необходимость в сервере для аутентификации.

Каждый компьютер Windows, не присоединённый к домену, является частью рабочей группы. Рабочая группа — это группа компьютеров в одной локальной сети. В отличие от домена, ни один компьютер в рабочей группе не

контролирует другие компьютеры — все они объединены на равных. Для рабочей группы пароль также не требуется.

https://zawindows.ru/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B4%D0%BE%D0%BC%D0%B5%D0%BD-windows-%D0%B8-%D0%BA%D0%B0%D0%BA-%D0%BE%D0%BD-%D0%B2%D0%BB%D0%B8%D1%8F%D0%B5%D1%82-%D0%BD%D0%B0-%D0%BC%D0%BE%D0%B9/

Контрольные вопросы

Перечислите типы учетных записей.

- Учетные записи обычных пользователей предназначены для повседневной работы.
- Учетные записи администратора предоставляют полный контроль над компьютером и должна использоваться только при необходимости.
- Учетные записи гостя предназначены главным образом для лиц, которые должны временного использования компьютера.

Перечислите способы создания учетных записей.

- Через параметры Windows (семья и другие пользователи).
- Через командную строку от имени администратора.
- Создание пользователя в «Локальные пользователи и группы» lusrmgr
- Через control userpasswords2.

Что понимается под идентификацией пользователя?

Идентификация используется для определения, существует ли конкретный пользователь в системе. Проводится, например, по номеру телефона или логину.

В процессе идентификации используется **набор данных, который уникально идентифицирует объект безопасности (например, пользователя, группу, компьютер, учетную запись службы) в общей службе каталогов**.

Что понимается под аутентификацией пользователей?

Аутентификация — это процесс подтверждения права на доступ с помощью ввода пароля, пин-кода, использования биометрических данных и других способов.

Аутентифика́ция (англ. *authentication* ← греч. αὐθεντικός [authentikos] «реальный, подлинный» ← αὐτός [autos] «сам; он самый») — процедура проверки подлинности, например:

- проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов;
- подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;
- проверка контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Перечислите возможные идентификаторы при реализации механизма идентификации.

Проводится, например, по номеру телефона или логину.

В процессе идентификации используется **набор данных, который уникально идентифицирует объект безопасности (например, пользователя, группу, компьютер, учетную запись службы) в общей службе каталогов**.

Перечислите возможные идентификаторы при реализации механизма аутентификации.

В качестве идентификаторов в системах аутентификации обычно используют набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи). В системах идентификации такими идентификаторами являются физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).

Какой из механизмов (аутентификация или идентификация) более надежный? Почему?

А?

Аутентификация, поскольку помимо идентификатора, там есть и данные, по которым можно убедиться в том, что данный пользователь выдает себя за себя. Персональный ключ, роговица глаза — по ним также можно идентифицировать субъекта, но при этом это тоже является средством аутентификации.

Структура маркера доступа.

- 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

Структура 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.

- The revision level of the **SID** structure
- A 48-bit identifier authority value that identifies the authority that issued the SID
- A variable number of subauthority or *relative identifier* (RID) values that uniquely identify the trustee relative to the authority that issued the SID

The combination of the identifier authority value and the subauthority values ensures that no two SIDs will be the same, even if two different SID-issuing authorities issue the same combination of RID values. Each SID-issuing authority issues a given RID only once.

Значение SID включает компоненты, предоставляющие сведения о структуре **SID** , и компоненты, которые однозначно идентифицируют доверенного лица. Sid состоит из следующих компонентов:

- **Идентификатор владельца (Revision)**: Этот байт определяет версию структуры SID.

- **Количество подкомпонентов (Sub-authority Count)**: Этот байт указывает, сколько подкомпонентов (Sub-authorities) содержит SID.
- **Идентификатор аутентификации (Identifier Authority)**: Этот 6-байтный блок определяет организацию, которая создала SID. Этот блок также может содержать идентификатор аутентификации, который определяет тип объекта (например, пользователь, группа или компьютер).
- **Подкомпоненты (Sub-authorities)**: Подкомпоненты представляют собой 32-битные значения, которые уникально идентифицируют объект безопасности внутри организации, определенной идентификатором аутентификации. Количество подкомпонентов определяется значением "Количество подкомпонентов".

Сочетание значения центра идентификатора и значений подчиненного авторизации гарантирует, что два идентификатора безопасности не будут одинаковыми, даже если два разных центра, выдающего ИД безопасности, выдают одинаковое сочетание значений RID. Каждый центр, выдающий ИД безопасности, выдает заданный RID только один раз.