+12. Управление пользователями и группами пользователей в Windows: понятие дискреционной системы безопасности, типы Windows-пользователей, группы пользователей, возможности API управления пользователями и группами.

**Понятие дискреционной системы безопасности**

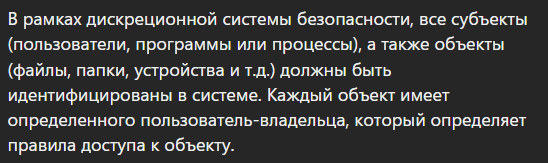
**Дискреционная система безопасности** - это **система безопасности, которая определяет доступ к объектам в компьютерной системе** на основе разрешений, предоставленных владельцем объекта.

Это означает, что **владелец объекта контролирует, кто может получить доступ к этому объекту** и какие действия могут быть выполнены с ним.

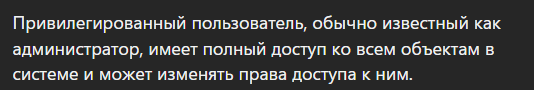
* все **субъекты и объекты компьютерной системы** должны быть **однозначно идентифицированы**;
* **для любого объекта** компьютерной системы **определен пользователь-владелец**;
* в компьютерной системе существует **привилегированный пользовател**ь, обладающий **правом полного доступа к любому объекту** (или правом становиться владельцем любого объекта).

Дискреционное разграничение доступа реализуется обычно **в виде матрицы доступа**, **строки** которой соответствуют субъектам компьютерной системы, а **столбцы** — ее объектам. Элементы матрицы доступа **определяют права доступа субъектов к объектам**.

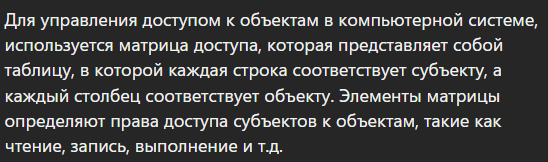
Последнее свойство определяет **невозможность существования в компьютерной системе потенциально недоступных объектов**, владелец которых отсутствует.









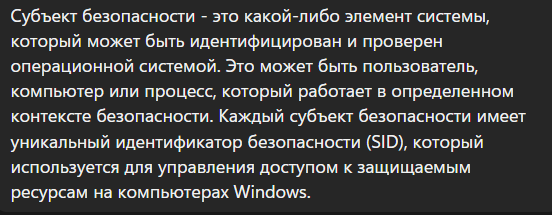




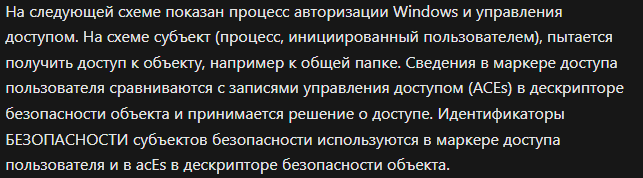
Проверка прав доступа субъекта к объекту производится в момент открытия этого объекта в процессе субъекта.

Остановимся на **недостатках** дискреционного разграничения доступа. Прежде всего, к ним относится статичность разграничения доступа — права доступа к уже открытому субъектом объекту в дальнейшем не изменяются независимо от изменения состояния компьютерной системы.

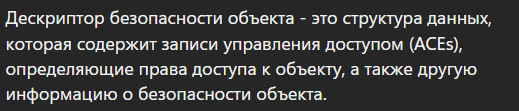
**Доп инфа\***

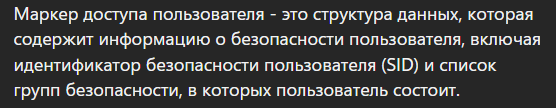




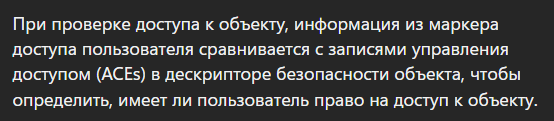




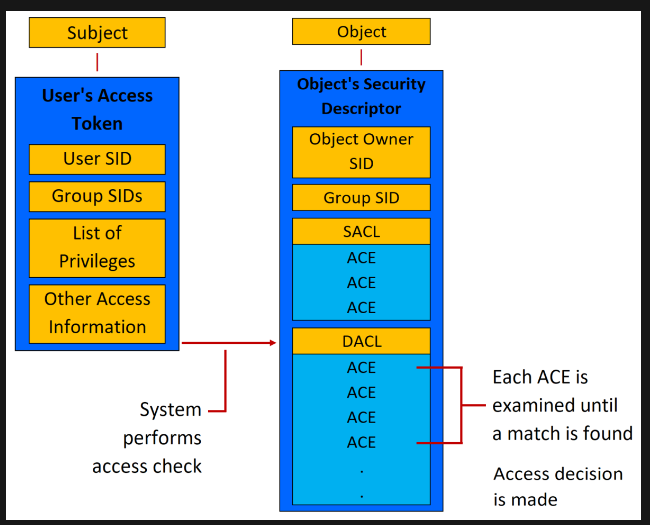












В безопасности, на самом базовом уровне, всё сводится к *субъектам* и *объектам*.

Субъект - это то, от кого вы защищаете.

Объект - это то, что вы защищаете.

Субъекты и объекты используются в аутентификации (authentication) - проверка кто вы; авторизации (authorization) - предоставление доступа к чему-либо и аудите (auditing) - отслеживание, кто получил доступ.

Примером субъекта - служит **пользователь**. Объектом - **файл**.

Существует такое понятие как **принципал безопасности** (Принципал безопасности - это всё, чему может быть назначен SID и предоставлены права доступа к чему-либо). В Windows принципалами безопасности являются **Пользователи** (Users), **Компьютеры** (Computers) и **Группы** (Groups). А начиная с Windows Vista принципалом безопасности так же является **Служба** (Service), которая теперь тоже имеет SID.

**SID (Security Identifier) - это уникальный идентификатор безопасности, который присваивается каждому пользователю, группе и объекту в операционной системе Windows.**

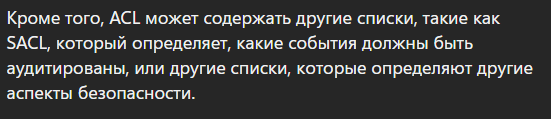
**ACL (Access Control List) - это список правил, который определяет, какие пользователи и группы имеют доступ к определенному ресурсу, например, файлу или папке. Этот список содержит записи управления доступом (ACE), которые определяют права доступа для каждого пользователя или группы**

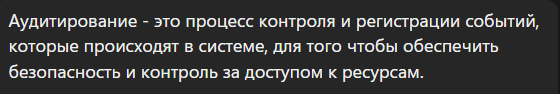
**ACE (Access Control Entry) - это запись в ACL, которая содержит информацию о правах доступа для пользователя или группы. ACE может определять, может ли пользователь читать, записывать или выполнять определенные действия с ресурсом.**

Дескриптор безопасности для защищаемого объекта может содержать два типа ACL: DACL и SACL.

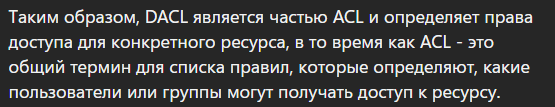
DACL (Discretionary Access Control List) - DACL содержит записи управления доступом (ACE), которые определяют права доступа для каждого пользователя или группы.

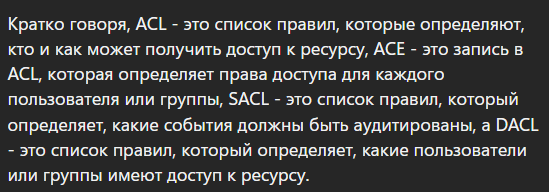
SACL (System Access Control List) - это часть дескриптора безопасности объекта, который отвечает за аудит доступа к ресурсу.

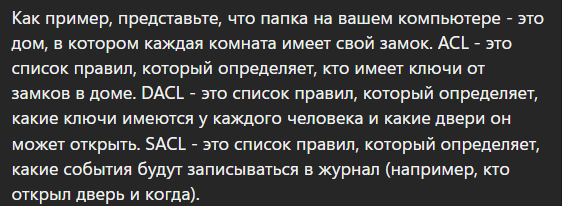


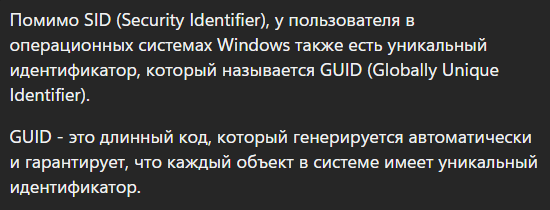


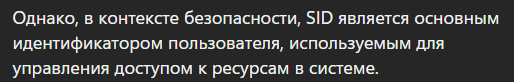




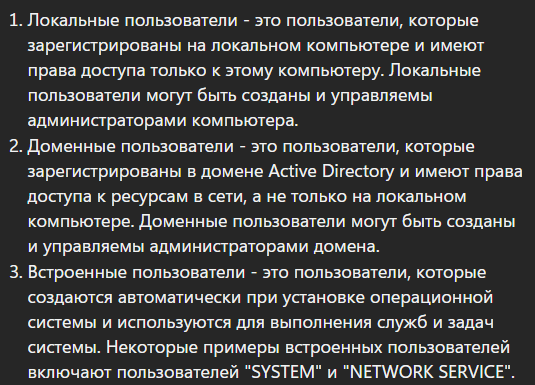


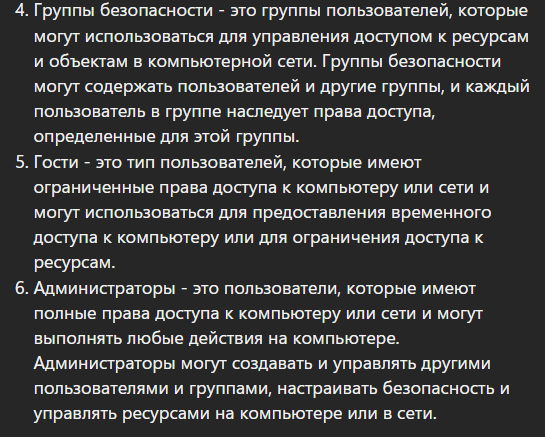






**Типы Windows-пользователей**





Пользователи групп наследуют у группы права.

**Группы пользователей**

Группы — это объекты, являющиеся **участниками системы безопасности** (security principals) и **предназначенные для управления доступом к ресурсам**.

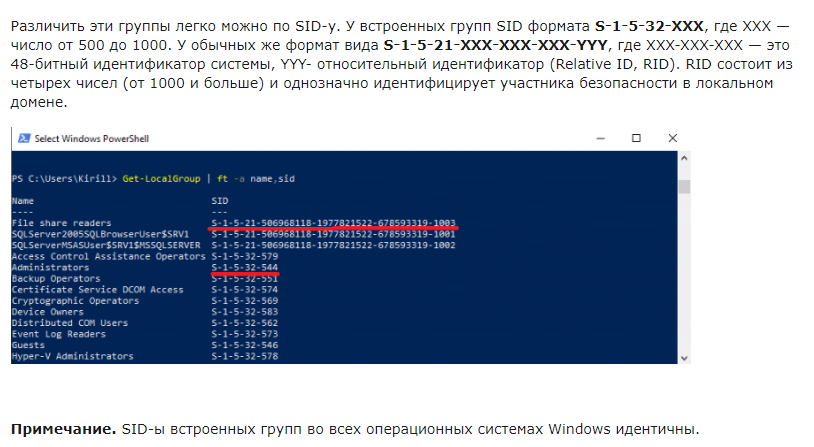
Каждой группе **присваивается уникальный идентификатор безопасности** (Security Identifier, SID), который сохраняется в течение всего срока службы.

**Условно группы можно разделить по области их действия:**

Локальные группы

Локальные группы безопасности создаются на локальном компьютере, и использовать их можно для управления доступом к ресурсам, находящимся только на этом компьютере. Управляются они менеджером учетных записей безопасности (Security Account Manager, SAM). \*mmc в лабе

Локальные группы можно условно разделить на два типа — встроенные (BuiltIn) и дополнительно созданные. Встроенные группы — это группы, имеющиеся в операционной системе по умолчанию, например та же группа Administrators. Ну а дополнительно созданные — группы, созданные вручную, для предоставления доступа к локальным ресурсам, например общим папкам.

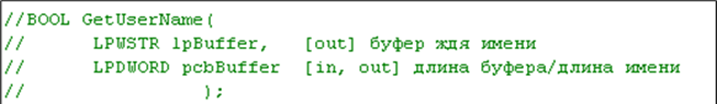




**API управления пользователями и группами**

Пользователи

1.   Имя текущего пользователя

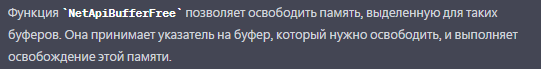


2.   Информация о пользователей

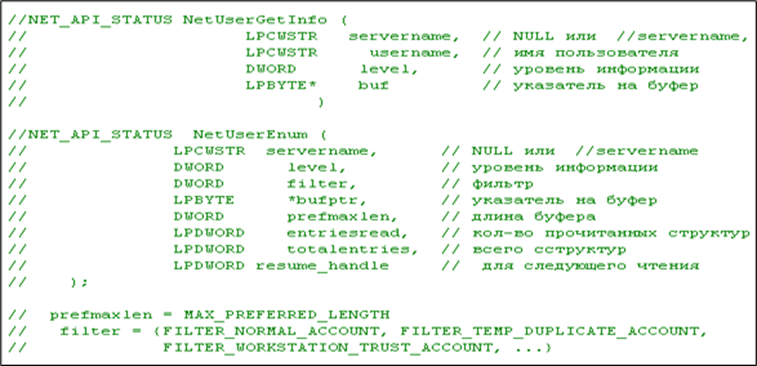


3.   Освободить память

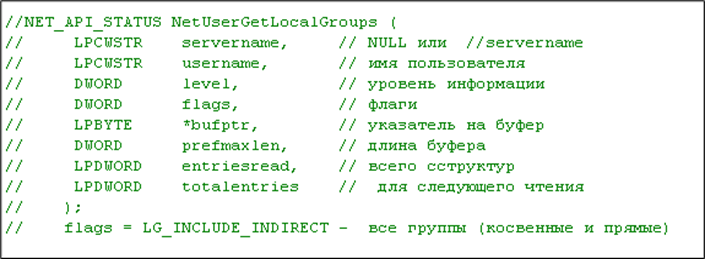




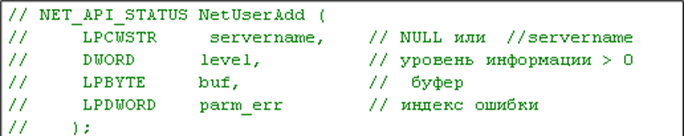
4.  Получить коллекцию пользователей



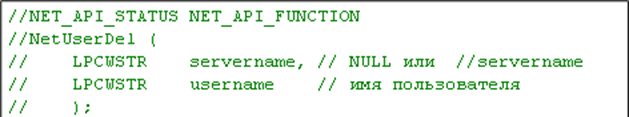
5.   Группы пользователя



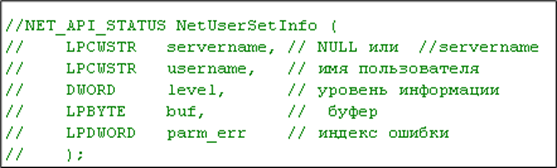
6.   Добавить пользователя



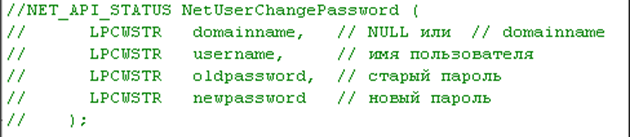
7.   Удалить пользователя



8. Изменить информацию о пользователе

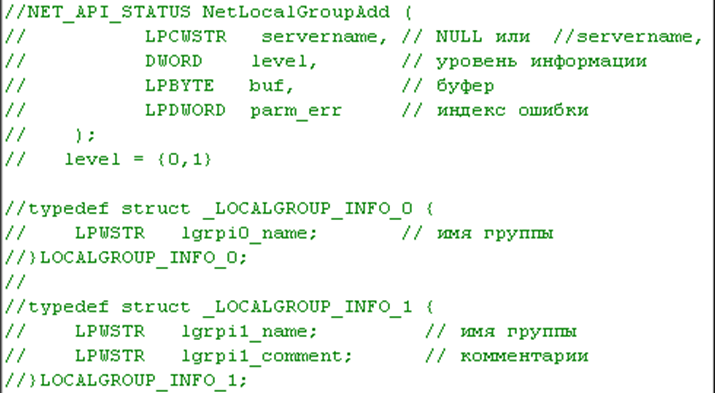


9.   Изменить пароль

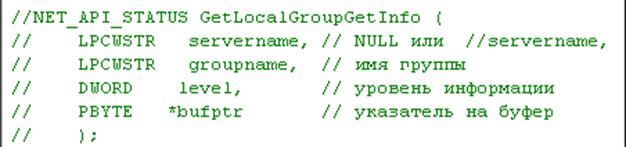


Группы

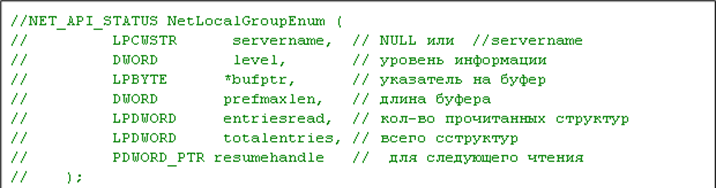
10.   Добавление группы



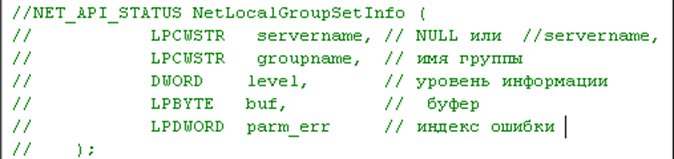
11. Получить информацию о группе



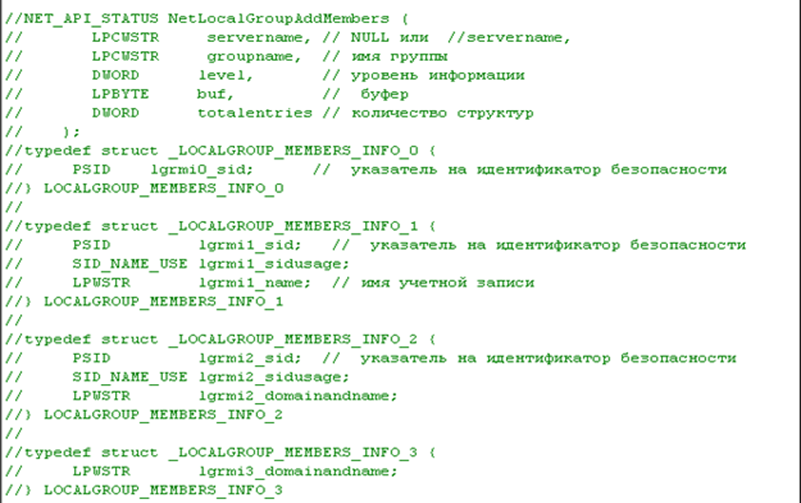
12.  Получить коллекцию  групп



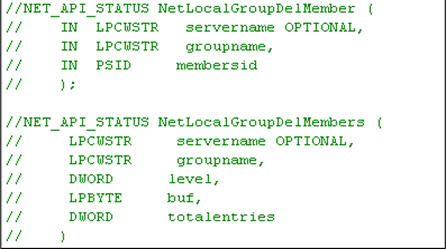
13.   Изменить информацию о группе



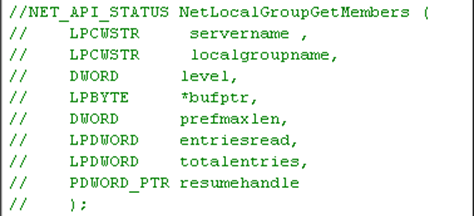
14. Добавление членов локальной группы (исп. INFO\_3)



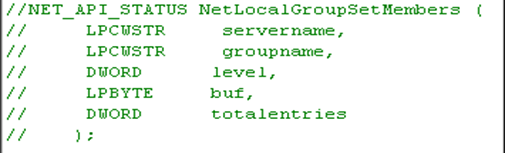
15.   Удаление  членов  группы



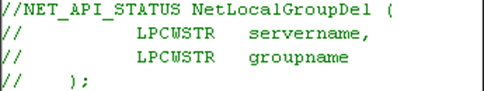
16.   Получить коллекцию членов группы



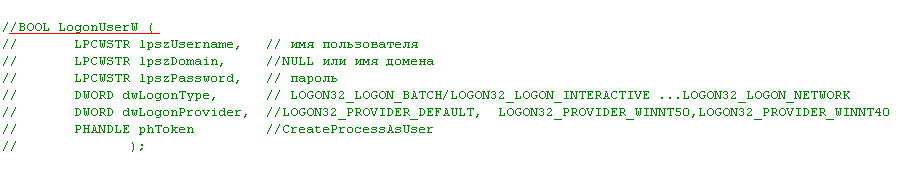
1. 17. **Установка членов локальной группы**(**из локальной группы удаляются все члены не принадлежащие списку и добавляются члены из списка**)



18.   Удалить группу



19.   Подключение пользователя (аутентификация)

****

