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

Дискреционное разграничение доступа к объектам характеризуется следующим набором свойств:

* все субъекты и объекты компьютерной системы должны быть однозначно идентифицированы;
* для любого объекта компьютерной системы определен пользователь-владелец;
* владелец объекта обладает правом определения прав доступа к объекту со стороны любых субъектов компьютерной системы;
* в компьютерной системе существует привилегированный пользователь, 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. В целях сокращения затрат памяти матрица доступа может задаваться в виде списков прав субъектов (для каждого из них создается список всех объектов, к которым разрешен доступ со стороны данного субъекта) или в виде списков контроля доступа (для каждого объекта информационной системы создается список всех субъектов, которым разрешен доступ к данному объекту).

Достоинства:

* простая реализация (проверка прав доступа субъекта к объекту производится в момент открытия этого объекта в процессе субъекта)
* хорошая изученность (в наиболее распространенных операционных системах универсального назначения типа Microsoft Windows и Unix применяется именно эта модель разграничения доступа).

Недостатки:

* статичность разграничения доступа — права доступа к уже открытому субъектом объекту в дальнейшем не изменяются независимо от изменения состояния компьютерной системы.
* не обеспечивает защиты от утечки конфиденциальной информации.
* автоматическое назначение прав доступа субъектам (из-за большого количества объектов в информационной системе в качестве субъектов доступа остаются только ее пользователи, а значение элемента матрицы доступа вычисляется с помощью функции, определяющей права доступа порожденного пользователем субъекта к данному объекту компьютерной системы).

**типы Windows-пользователей**

Все учетные записи в зависимости от своих функциональных возможностей разделяются на три типа:

* администратор компьютера
* ограниченная учетная запись
* гостевая учетная запись

Пользователь с ограниченной учетной записью может выполнять операции со своим паролем (создание, изменение, удаление), изменять рисунок своей учетной записи, параметры настройки рабочего стола, а также просматривать файлы. Учетная запись администратора позволяет выполнять следующие операции:

* Создание, удаление и редактирование учетных записей пользователей (в том числе и собственной учетной записи);
* Операции со своим паролем (создание, редактирование, удаление);
* Установка и удаление программ и оборудования, редактирование их параметров и свойств;
* Чтение всех общих файлов;
* Внесение изменений в конфигурацию на уровне системы.

Что касается гостевой записи, то она формируется автоматически в процессе установки системы, и предназначена для сторонних пользователей, не имеющих на данном компьютере собственных учетных записей. Под учетной записью гостя нет доступа к файлам, папкам, параметрам и приложениям, которые защищены паролем.

**Группа** это просто набор учетных записей пользователей, которые объединены по какому-либо признаку, например, пользователи одной группы могут работать в одном отделе.

**Группы пользователей**

* Администраторы. Неограниченный доступ.
* Операторы архива. Права создания резервной копии даже тех объектов, к которым не имеют доступа.
* Опытные пользователи.
* Пользователи системного монитора. Есть чудесная вещь под названием Системный монитор(perfmon.msc), с помощью которого можно отследить использование различных ресурсов компьютером. А группа дает доступ к данному инструменту.
* Операторы настройки сети. Члены группы могут изменять параметры TCP/IP.
* Пользователи удаленного рабочего стола. Пользователи этой группы смогут входить в систему через удаленный рабочий стол.
* Пользователи журналов производительности. 4-ая группа дает только поверхностный доступ к Системному монитору. Данная группа дает более полные права.
* Пользователи DCOM. Пользователи группы могут манипулировать объектами распределенной модели DCOM.
* Криптографические операторы.
* Читатели журнала событий.

возможности API управления пользователями и группами

1. Имя текущего пользователя. GetUserName (буфер имени, длина буфера)
2. Информация о пользователей NetUserGetInfo (servername, username, уровень инфы, буфер)
3. Освободить память NetApiBufferFree
4. Получить коллекцию пользователей NetUserEnum
5. Группы пользователя NetUserGetLocalGroups
6. Добавить пользователя NetUserAdd
7. Удалить пользователя NetUserDel
8. Изменить информацию о пользователе NetUserSetInfo
9. Изменить пароль NetUserChangePassword
10. Добавление группы NetLocalGroupAdd
11. Получить информацию о группе GetLocalGroupInfo
12. Получить коллекцию групп NetLocalGroupEnum
13. Изменить информацию о группе NetLocalGroupSetInfo
14. Добавление членов локальной группы (исп. INFO\_3) NetLocalGroupAddMembers
15. Удаление членов группы NetLocalGroupDelMember
16. Получить коллекцию членов группы NetLocalGroupGetMembers
17. Установка членов локальной группы NetLocalGroupSetMembers
18. Удалить группу NetLocalGroupDel
19. Подключение пользователя LogUserW