# **14 лаба USER-HT-COM-DLL**

### --- что спрашивает по лабе

Спрашивает по экз. вопросу

**Дискреционное разграничение доступа к объектам**

**Что такое группы пользователей**

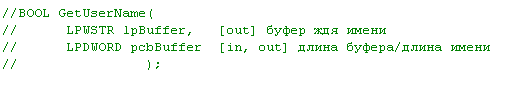
**Какие группы пользователей бывают**

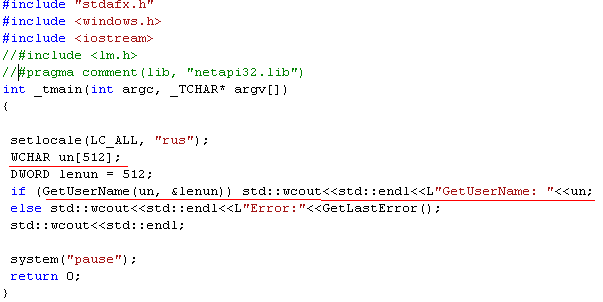
**Функции управления пользователями/группами**

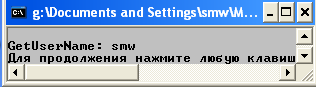
### Лекция\_ Users&Groups in Windows

#### **Управление пользователям**

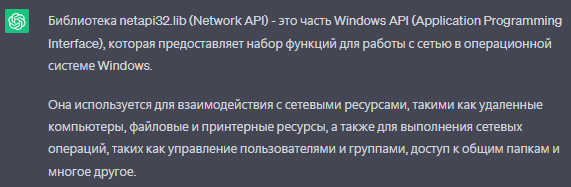
1. **Имя текущего пользователя**

****

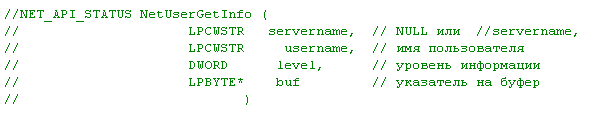
****

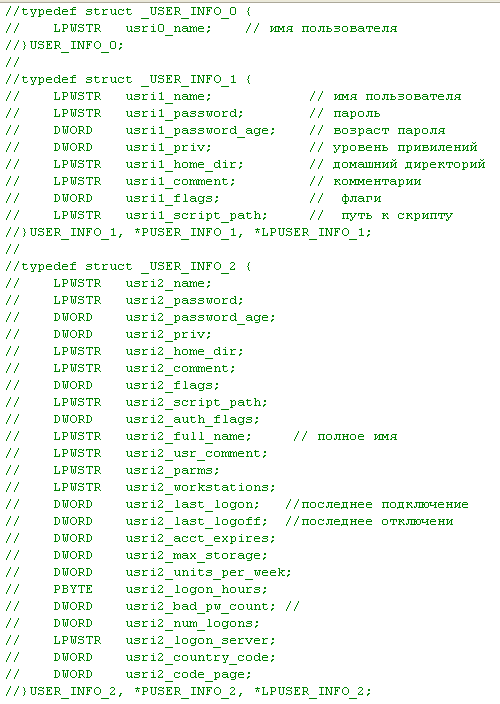
****

1. **netapi32.lib**

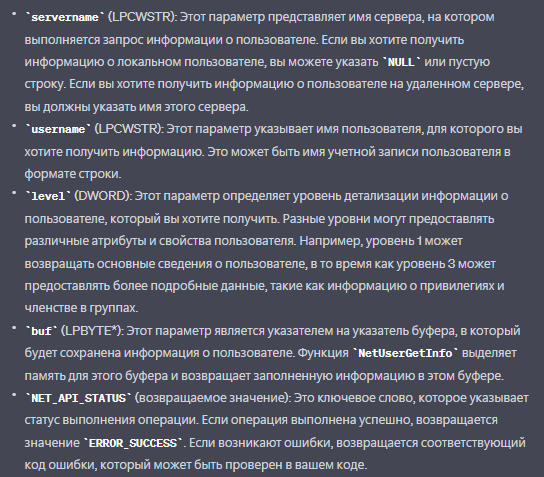


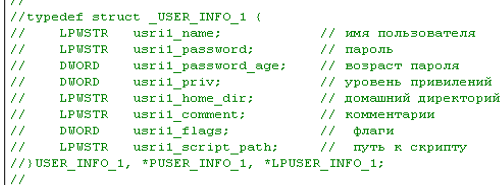
1. **Информация о пользователе**

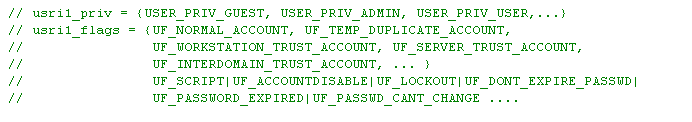


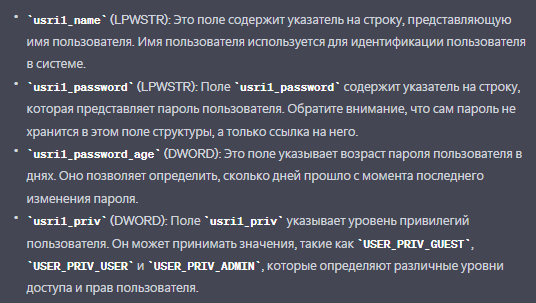


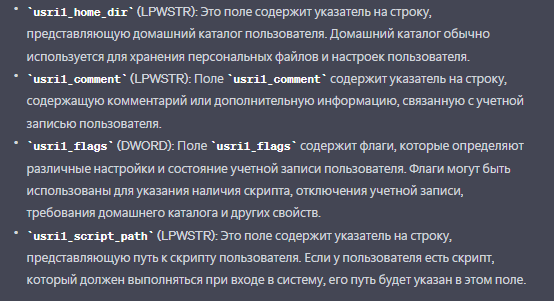






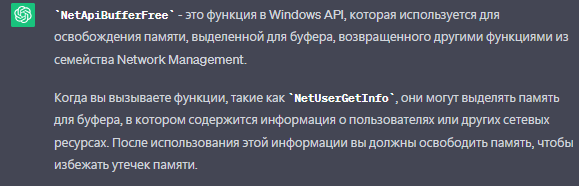


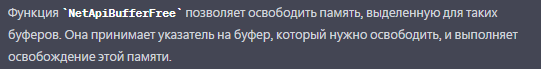




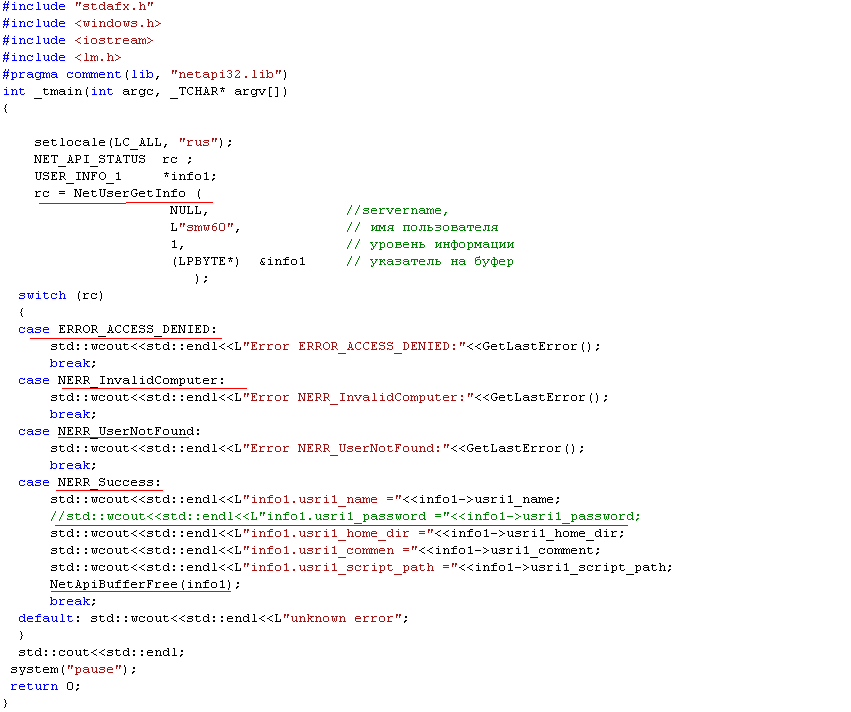
1. **Освободить память**

****

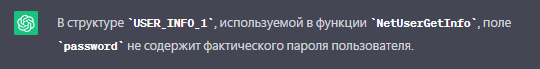


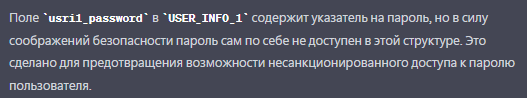


1. **Пример**



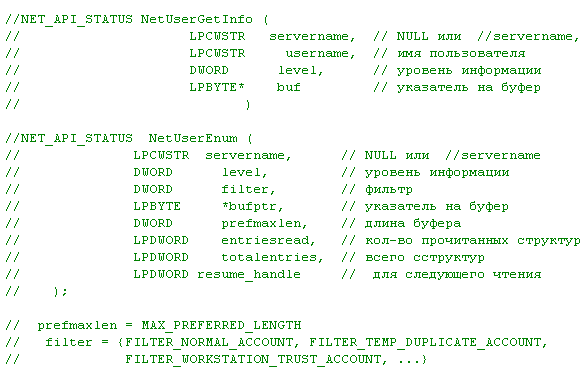


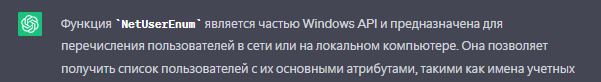


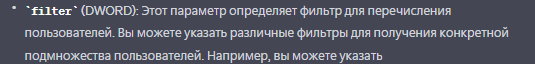




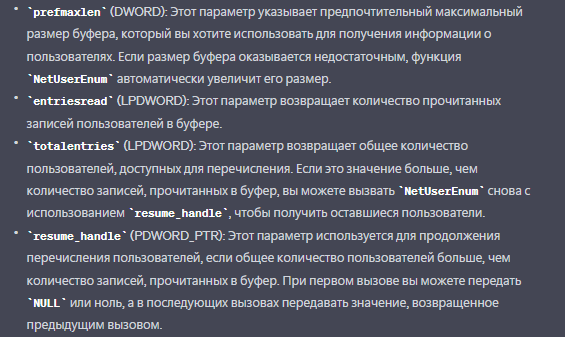
1. **Получить коллекцию пользователей**

****



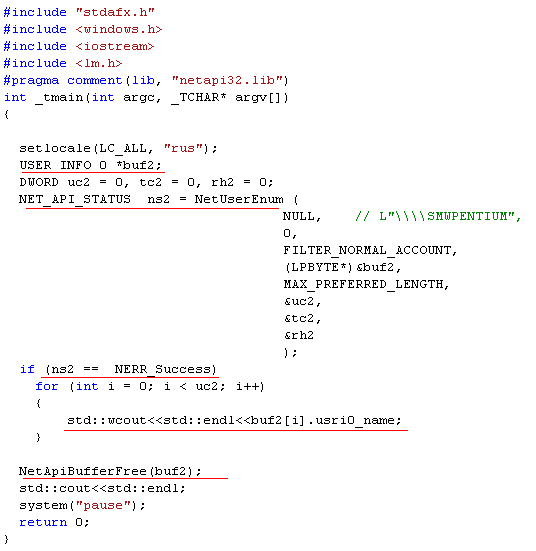




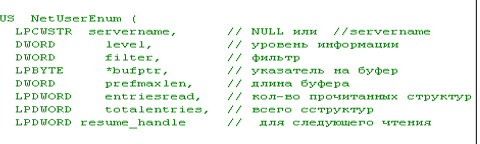


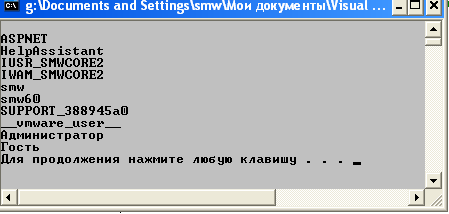


1. **Пример**

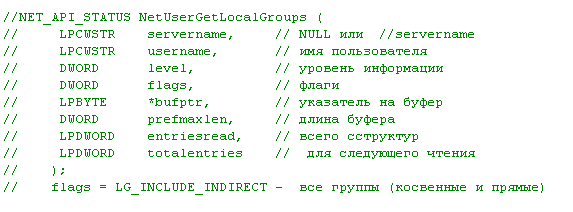
****

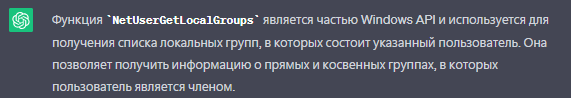


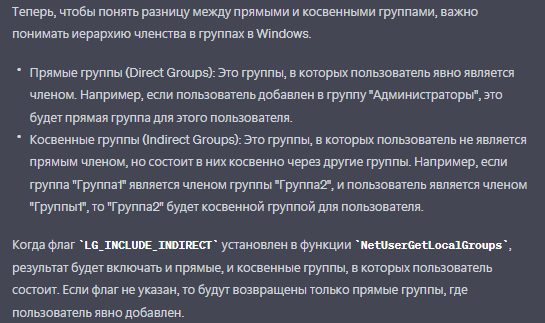


****

1. **Группы пользователя**

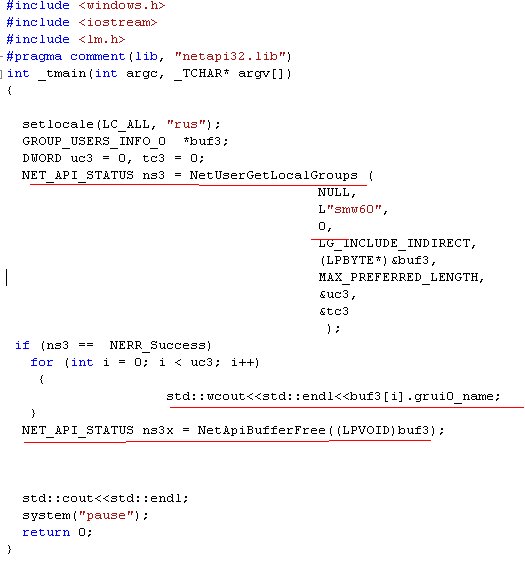


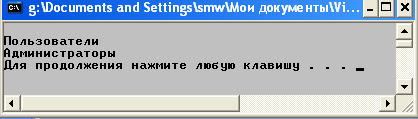




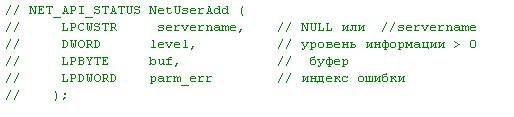


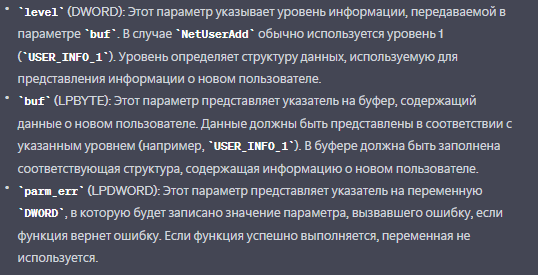
1. **Пример**

****

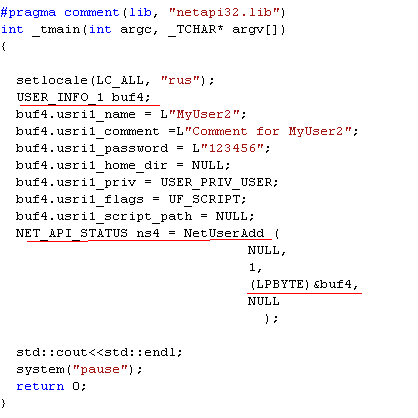
****

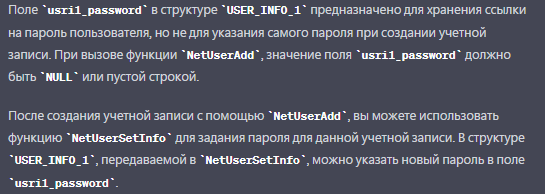
1. **Добавить пользователя**

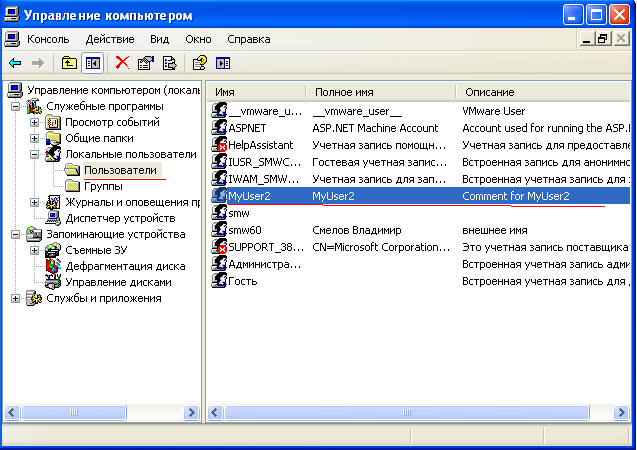
****



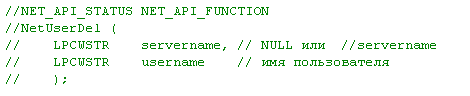
1. **Пример**

****

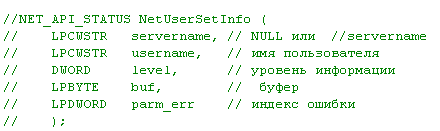


****

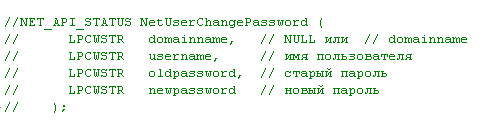
1. **Удалить пользователя**

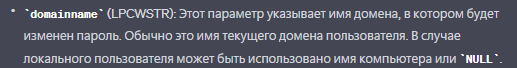
****

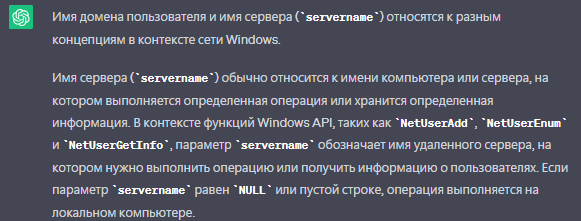
1. **Изменить информацию о пользователе**

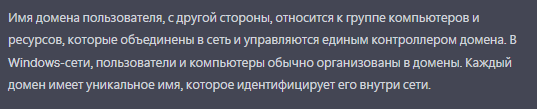
****

1. **Изменить пароль**

****

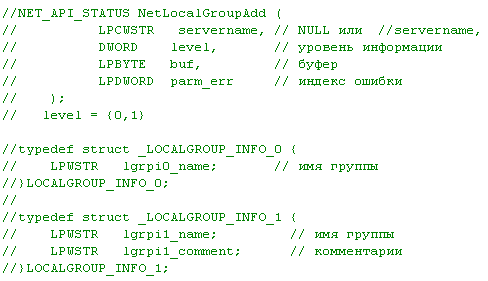






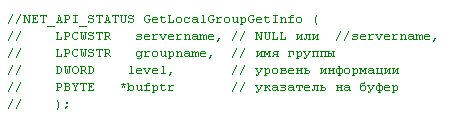
#### **Управление группами**

1. **Добавление группы**

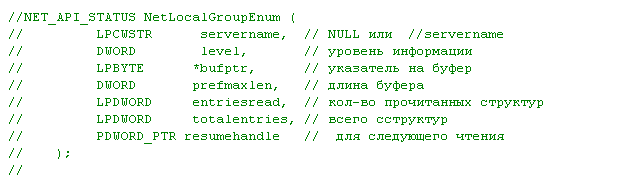
****



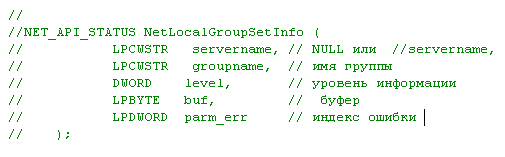
1. **Получить информацию о группе**



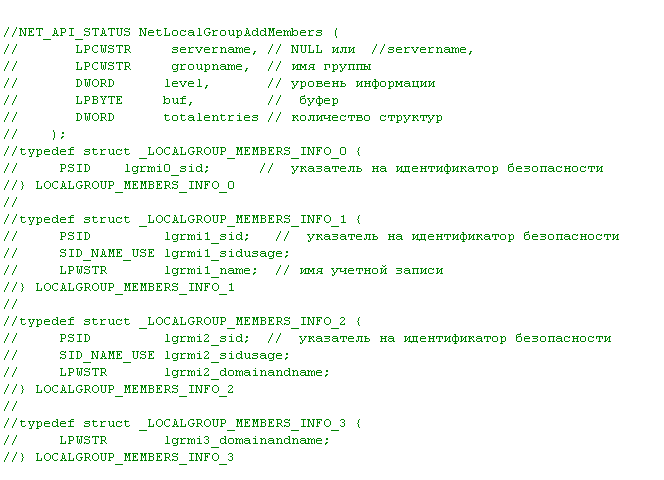
1. **Получить коллекцию групп**

****

1. **Изменить информацию о группе**

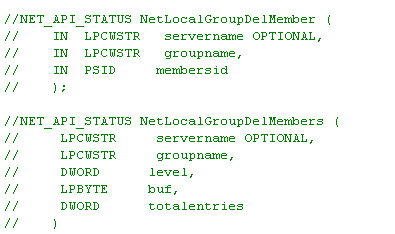
****

1. **Добавление членов локальной группы (исп. INFO\_3)**

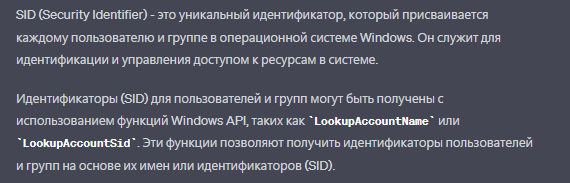
****



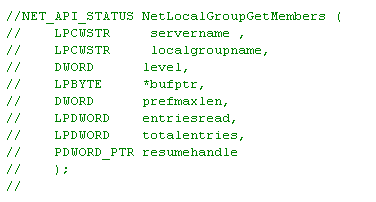
1. **Удаление членов группы**

****

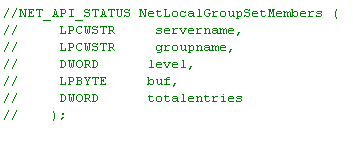




1. **Получить коллекцию членов группы**



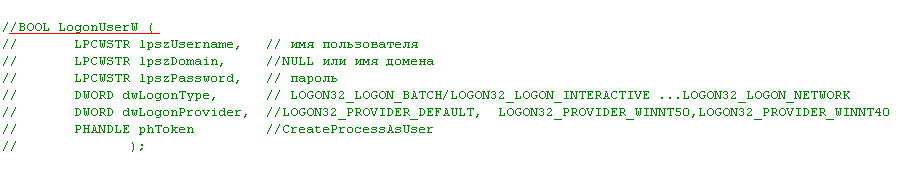
1. **Установка членов локальной группы** (**из локальной группы удаляются все члены не принадлежащие списку и добавляются члены из списка**)

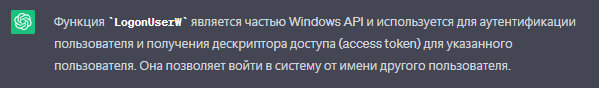
****

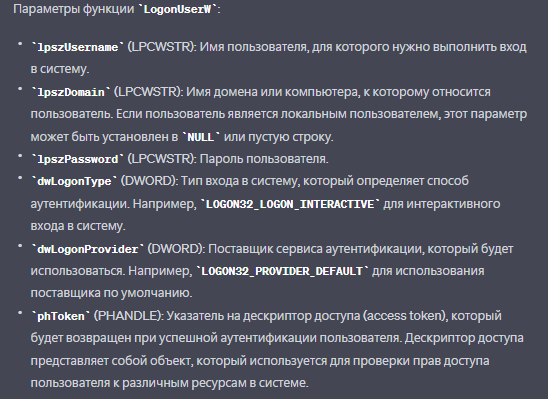
1. **Удалить группу**

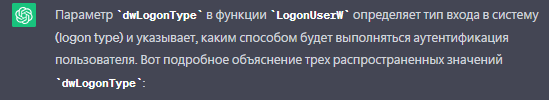


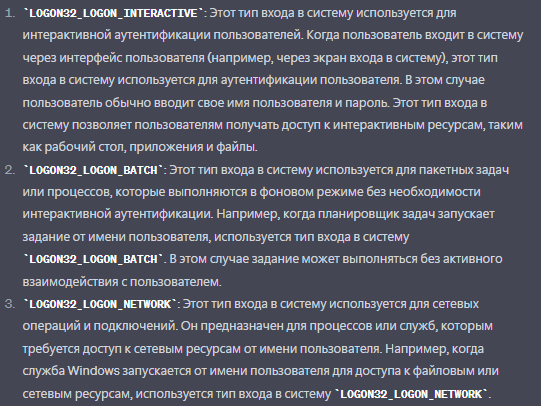
1. **Подключение пользователя**

****





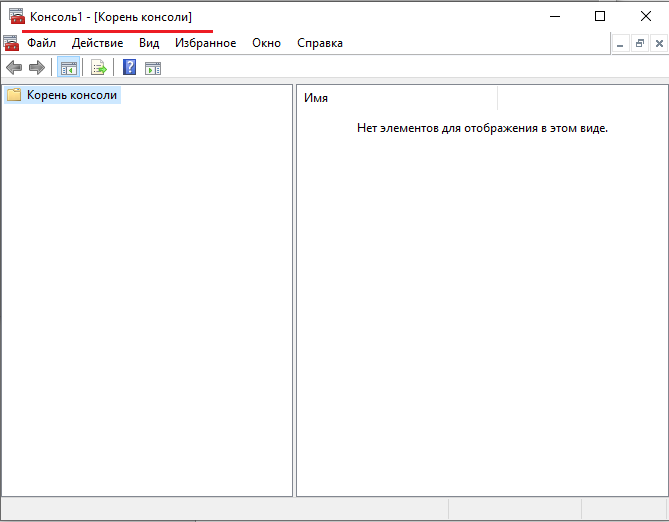


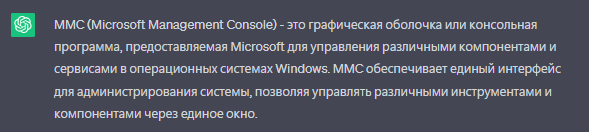


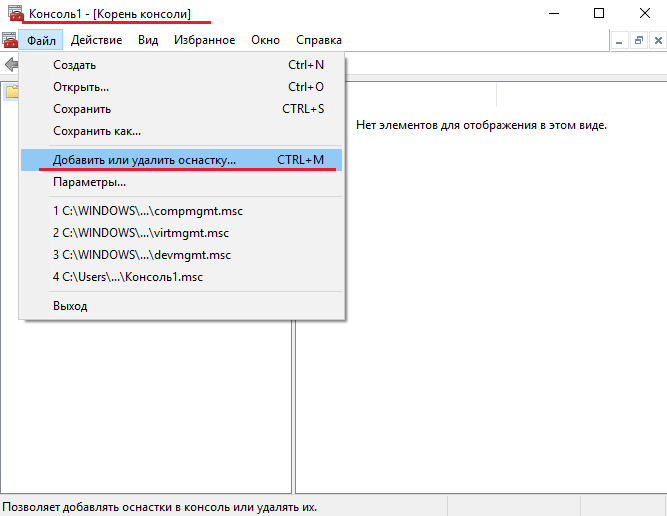


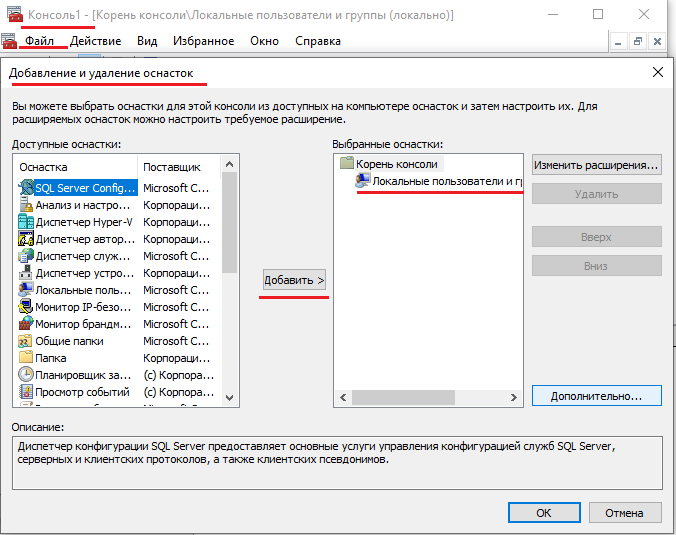
### Лекция\_ mmc

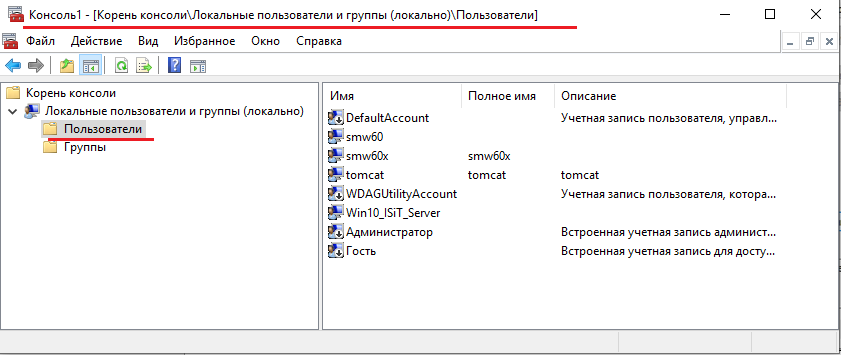
1. **mmc**

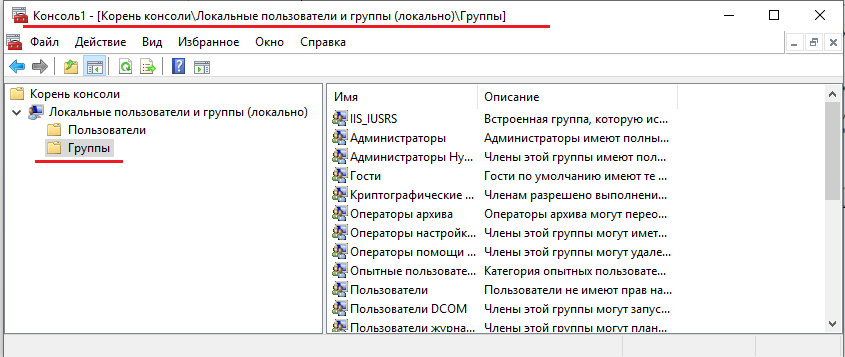
****



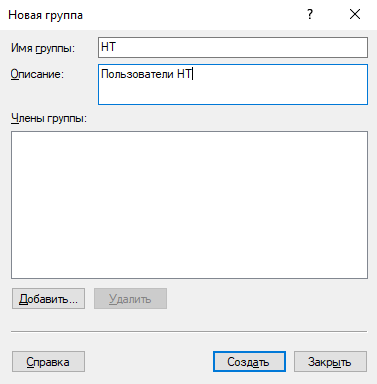
****

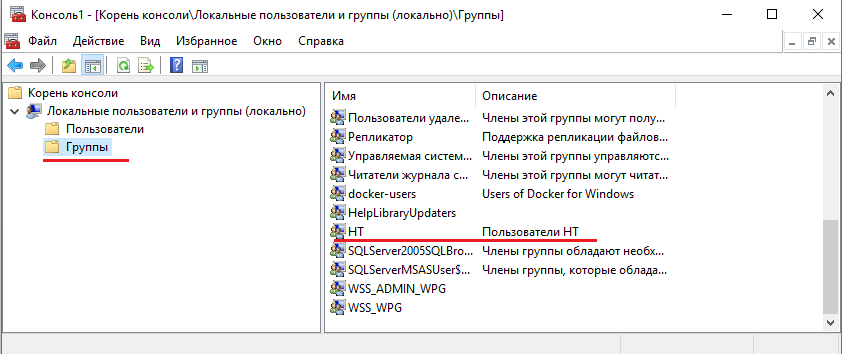
****

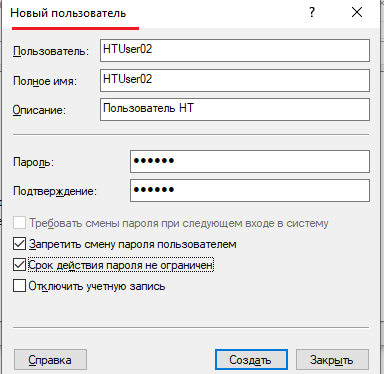
****

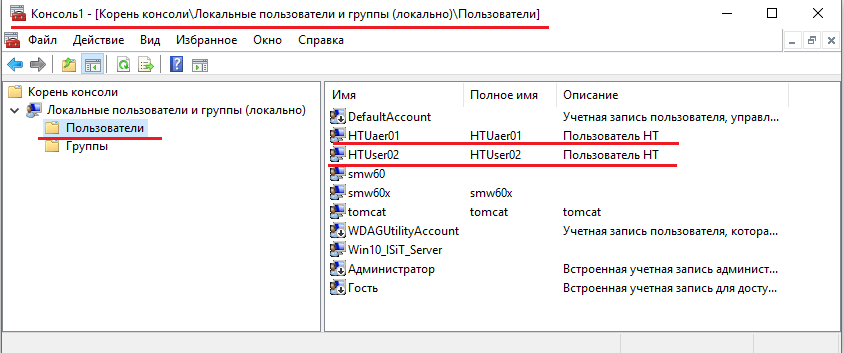
****

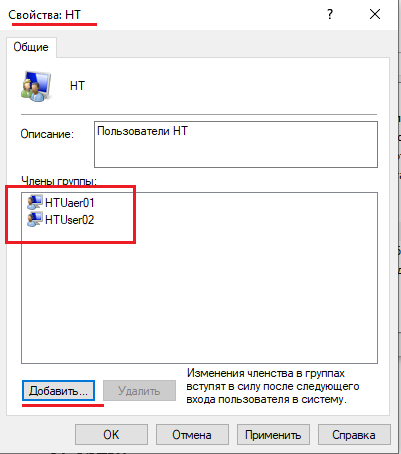
#### **Создание групп/юзеров**

****

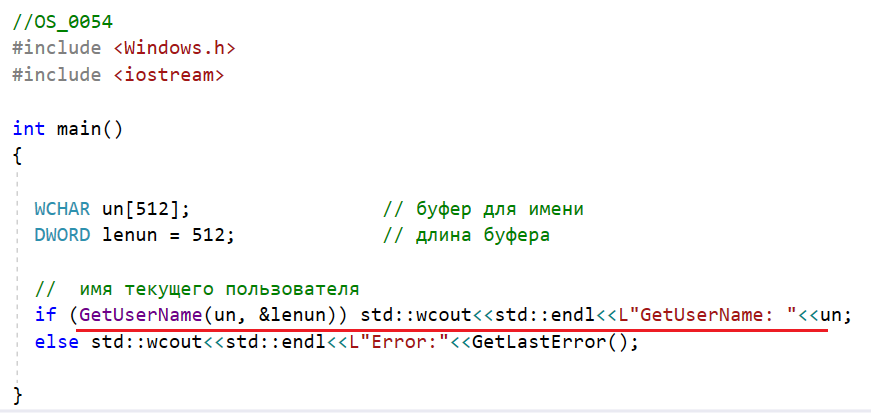
****

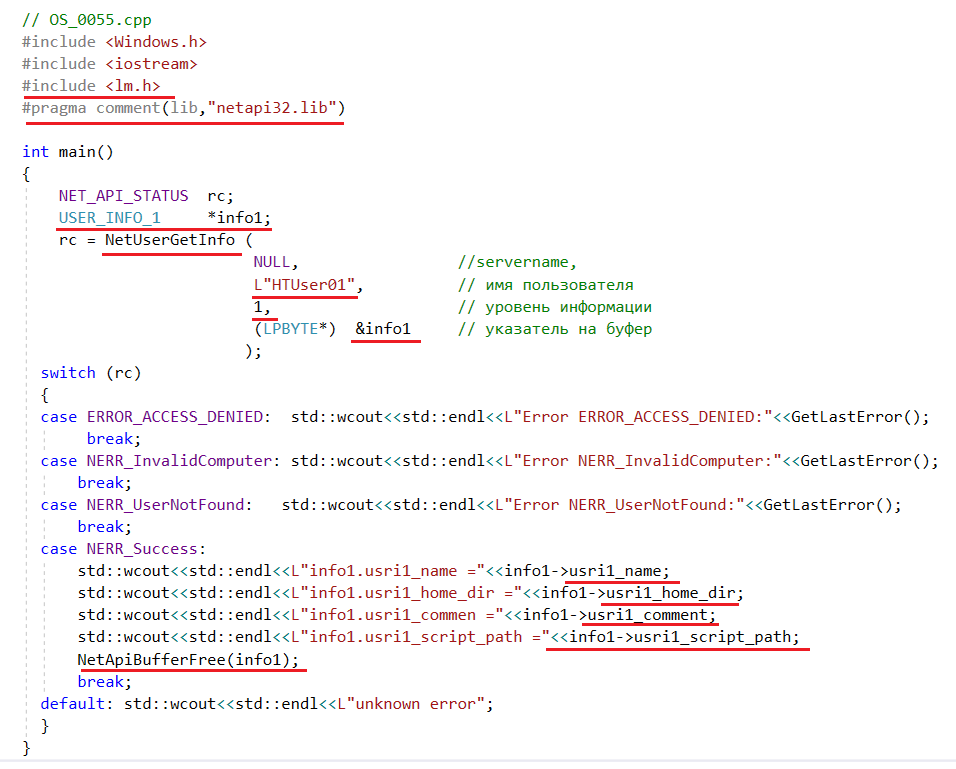
****

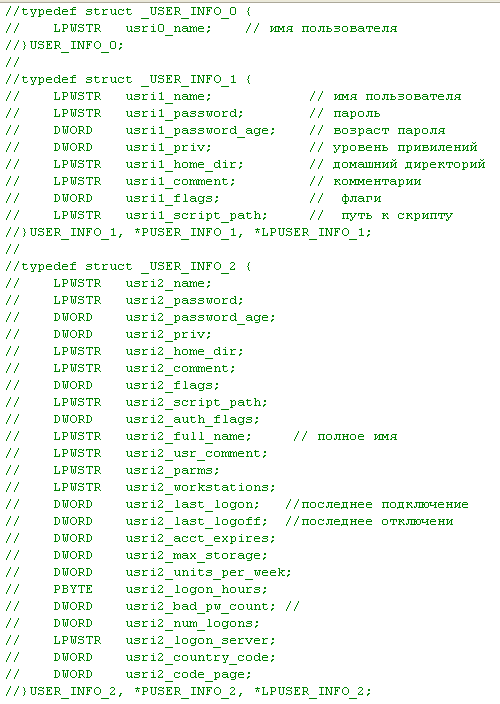
****

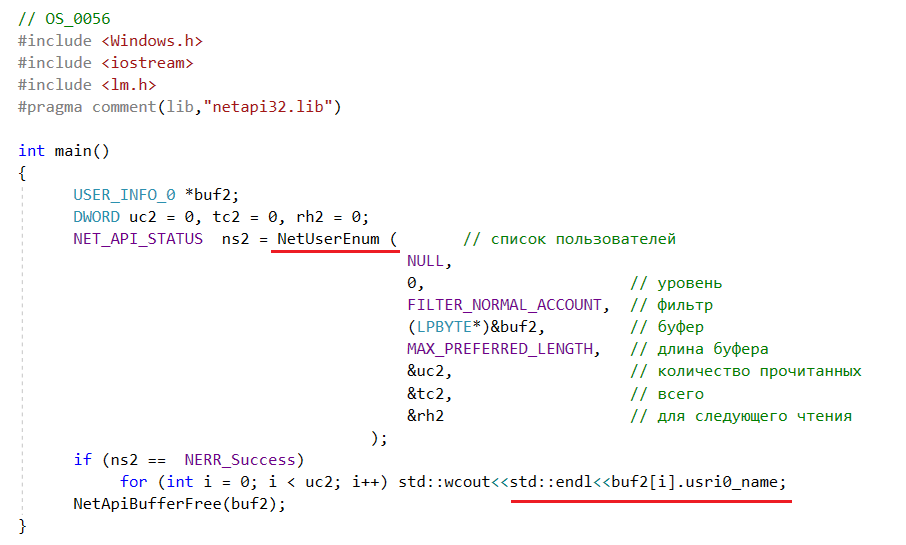
****

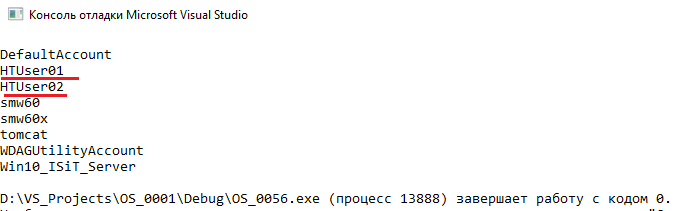


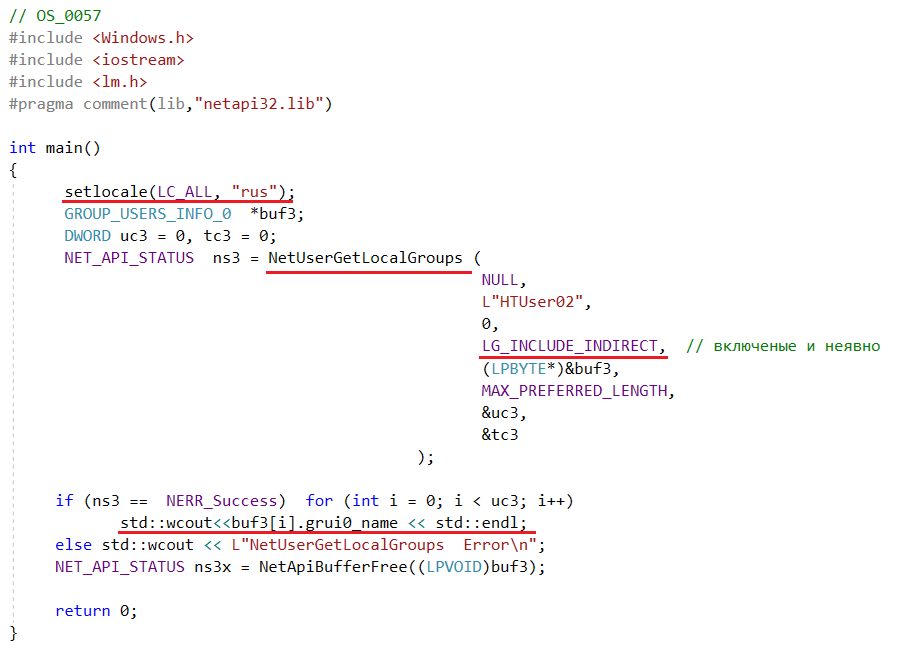
****

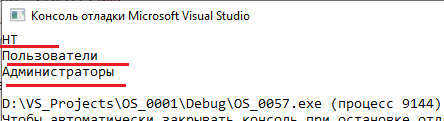
****



****

****

****

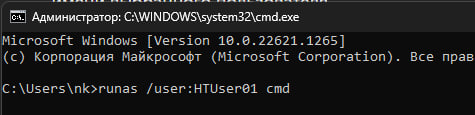
****

### Код лабы и гайд

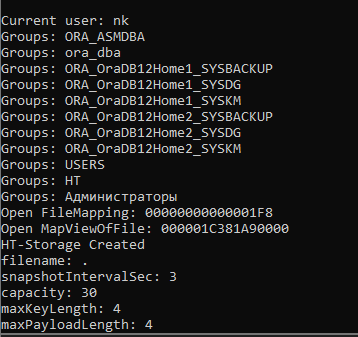
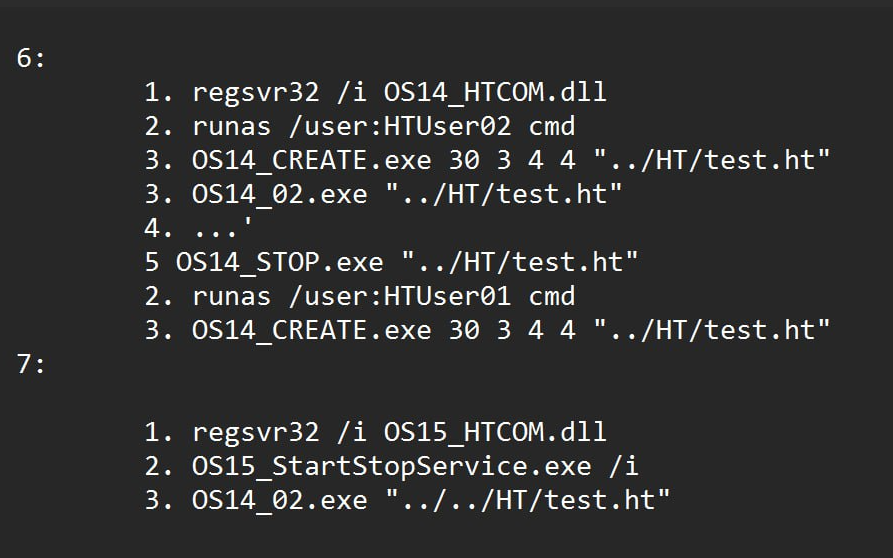
1. Создаем группу; юзеров; добавляем юзеров в группу
2. Как в прошлой лабе собираем проекты / регистрируем dll в реестр (regsvr32 /I OS14\_HTCOM.dll) и открываем консоли

#### **Консоли**

**Несколько консолей нужно открыть от юзера HTUser01:**

1. Для начала закинуть папку с проектом куда-то в C:\Users чтобы новые юзеры могли получить доступ к папке
2.  enter, новая консоль от юзера
3. HTUser01 должен находиться в группе HT для create/open

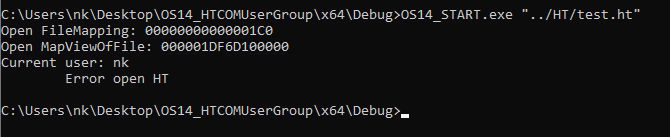
**OS14\_CREATE.exe 30 3 4 4 "../HT/test.ht" "HT"**



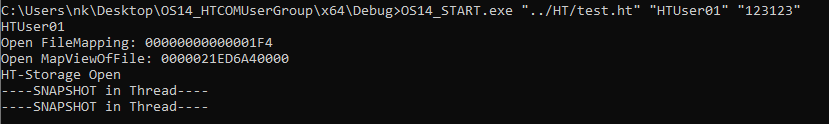
Должно создавать только если текущ польз находится в группе HT и только если он АДМИН; и если такая группа существует

**OS14\_START.exe "../HT/test.ht"**



Open работает только если текущ польз ТОЛЬКО в HT

**OS14\_START.exe "../HT/test.ht" "HTUser01" "123123"**

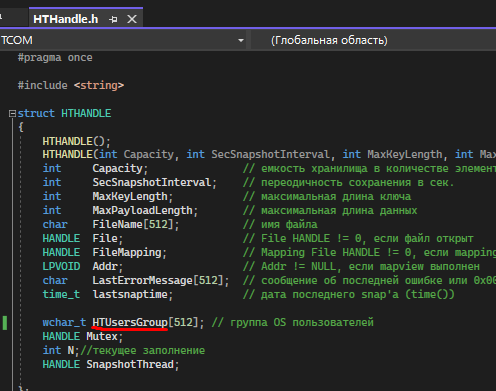


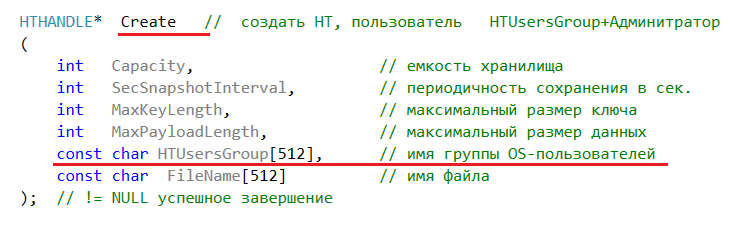
Запуск через пользователя и его пароль, должна проходить аутентификация на пароль и польз должен быть в группе

**OS14\_STOP.exe "../HT/test.ht"**

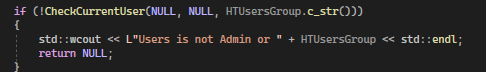
**OS14\_STOP.exe "../HT/test2.ht"**

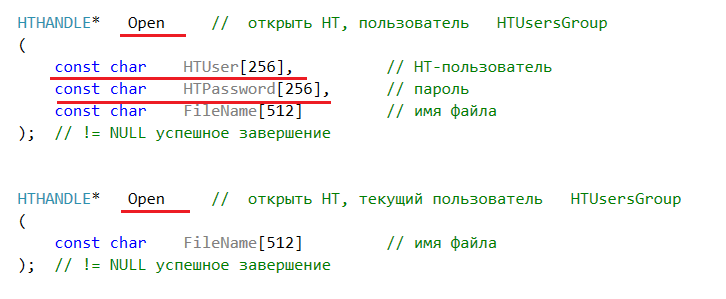
#### **Модификации**



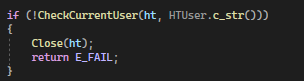




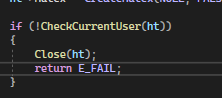












1. В функции **Create**  добавлен параметр **HTUsersGroup**, указывающий имя группы пользователей, которым разрешен доступ к HT-хранилищу. Функция должна создавать HT-хранилище только в том случае, если:

* существует группа пользователей заданная параметром **HTUsersGroup**;
* текущий пользователь является членом группы, заданной параметром **HTUsersGroup**;
* текущий пользователь является администратором (является членом группы **Администраторы**).

1. Функции **Open** является перегруженной.
2. Функция **Open** с одним параметром определяет имя текущего пользователя и выполняется в том случае, если текущий пользователь является членом группы заданной при создании HT-хранилища (функция **Create**).
3. Функция **Open** с тремя параметрами выполняется в том случае, если:

* пользователь с именем, указанным параметром **HTUser,** является членом группы, заданной при создании HT-хранилища (функция **Create**);
* пароль, заданный параметром **HTPassword** является корректным.

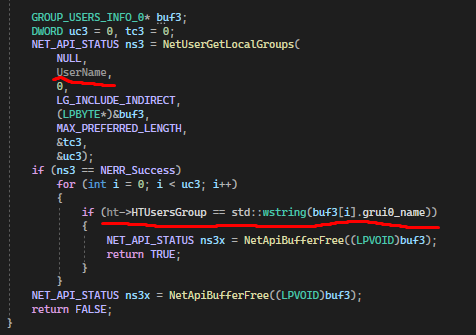
1. В блоке управления **HTHANDLE** добавлено поле **HTUsersGroup,** которое после выполнения функции **Open** заполняется именем группы пользователей, которое задается при создании HT-хранилища (функция **Create**).

#### **CheckCurrentUser**

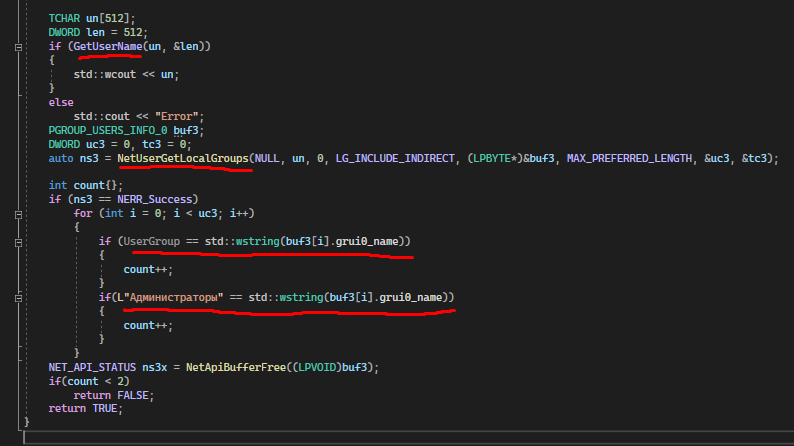
Если просто open(filename), то получает текущего пользователя, потом его группу и сравнивает группу с той которую указывали при Create HT:

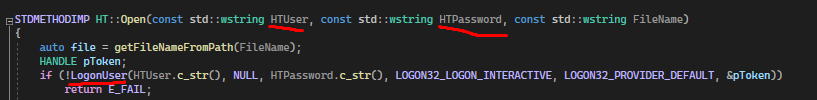


Если передан юзернейм open(filename, htuser,htpassword) то получает по юзернейму локальные группы и также сравнивает их:



При create проверяет что текущ польз состоит в группе HT(и что такая группа существует) и только если он админ:





Здесь идет аутентификация пользователя по паролю через функцию **LogonUser()**

### Задания:

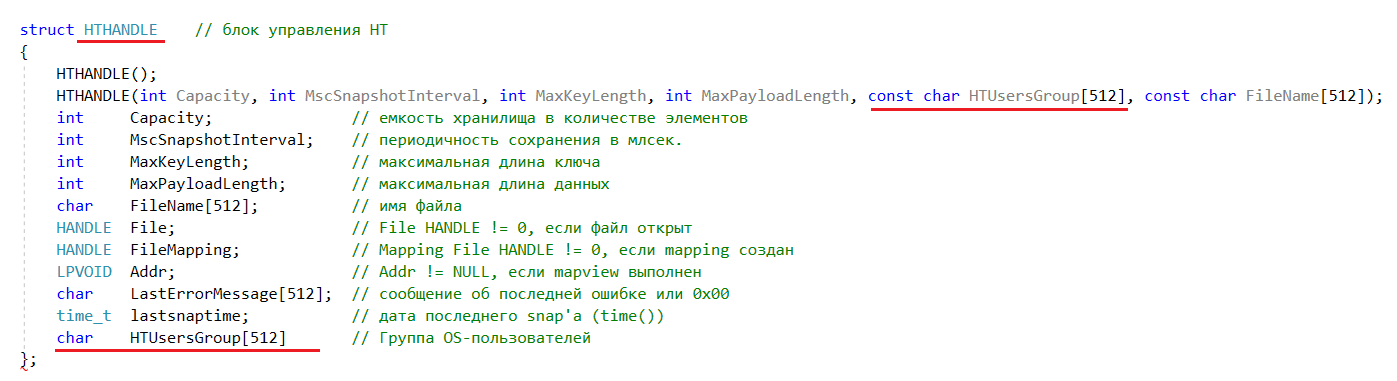
1. ***Используйте результаты лабораторных работ 10 – 13***.

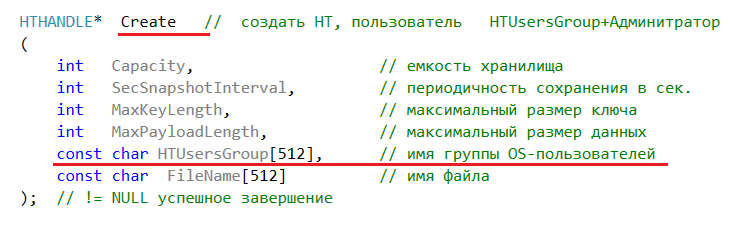
**Задание 01.Windows**

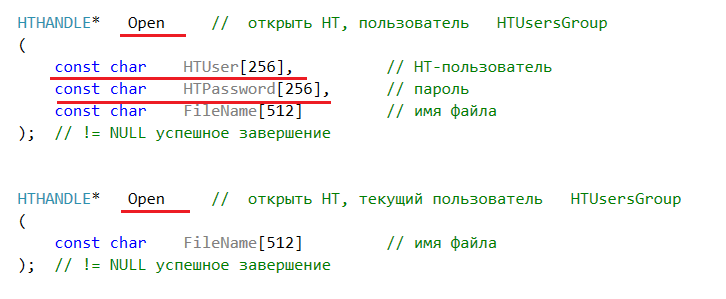
1. Средствами Windows (**mmc**, оснастка: Локальные пользователи и группы) создайте группу пользователей с именем **HT**.
2. Средствами Windows (mmc, оснастка: Локальные пользователи и группы) создайте пользователей с именем **HTUser01, HTUser02**.
3. Включить пользователей **HTUser01, HTUser02** в группу **HT**.

**Задание 02.Windows**

1. Внесите изменение в HT API, разработанный (и доработанный) в предыдущих лабораторных работах.







1. В функции **Create**  добавлен параметр **HTUsersGroup**, указывающий имя группы пользователей, которым разрешен доступ к HT-хранилищу. Функция должна создавать HT-хранилище только в том случае, если:

* существует группа пользователей заданная параметром **HTUsersGroup**;
* текущий пользователь является членом группы, заданной параметром **HTUsersGroup**;
* текущий пользователь является администратором (является членом группы **Администраторы**).

1. Функции **Open** является перегруженной.
2. Функция **Open** с одним параметром определяет имя текущего пользователя и выполняется в том случае, если текущий пользователь является членом группы заданной при создании HT-хранилища (функция **Create**).
3. Функция **Open** с тремя параметрами выполняется в том случае, если:

* пользователь с именем, указанным параметром **HTUser,** является членом группы, заданной при создании HT-хранилища (функция **Create**);
* пароль, заданный параметром **HTPassword** является корректным.

1. В блоке управления **HTHANDLE** добавлено поле **HTUsersGroup,** которое после выполнения функции **Open** заполняется именем группы пользователей, которое задается при создании HT-хранилища (функция **Create**).

**Задание 02.Windows**

1. Разработайте приложение **OS14\_HTCOM.**
2. Приложение **OS14\_HTCOM** представляет собой DLL-библиотеку (**OS14\_HTCOM.dll**), реализующую COM-компонент **OS14**.
3. Приложение **OS14\_HTCOM** функционально повторяет приложение **OS13\_HTCOM** (разработано в предыдущей лабораторной работе), но с учетом изменений API, описанных в предыдущих заданиях.

**Задание 03.Windows**

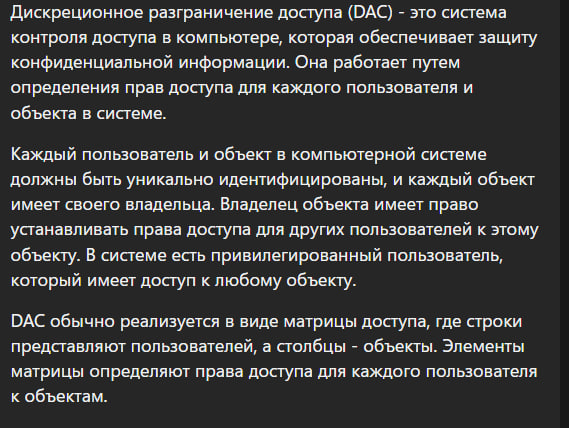
1. Разработайте приложения функционально-аналогичные приложениям в предыдущей лабораторной работе, предназначенные для тестирования **OS14\_HTCOM.**
2. Продемонстрируйте работоспособность приложения **OS14\_HTCOM.**
3. **КОНЕЦ**

## **Экзамен**

### 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 (Discretionary Access Control — DAC) система контроля доступа 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).**





**Последнее свойство определяет невозможность существования в компьютерной системе потенциально недоступных объектов, владелец которых отсутствует. Но реализация права полного доступа к любому объекту посредством предварительного назначения себя его владельцем не позволяет привилегированному пользователю (администратору) использовать свои полномочия незаметно для реального владельца 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).**

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

**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.**

**При использовании дискреционного разграничения доступа не существует возможности проверки, не приведет ли разрешение доступа к объекту для некоторого субъекта к нарушению безопасности информации в компьютерной системе (например, владелец базы данных с конфиденциальной информацией, дав разрешение на ее чтение другому пользователю, делает этого пользователя фактически владельцем защищаемой информации). Иначе говоря, дискреционное разграничение доступа не обеспечивает защиты от утечки конфиденциальной информации.**

**Наконец, к недостаткам дискреционного управления доступом относится 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 и 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. С помощью соответствующих ссылок можно включать и отключать учетную запись гостя (в первом случае сторонние пользователи смогут войти в систему, во втором – нет).**

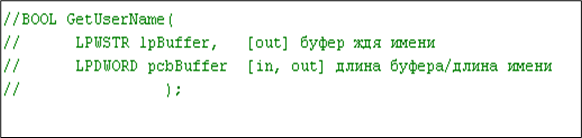
**Группа** это просто набор учетных записей пользователей, которые объединены по какому-либо признаку, например, пользователи одной группы могут работать в одном отделе. При этом отметим, что одна учетная запись пользователя может входить более чем в одну группу. Каждая группа имеет свою учетную запись и наделена своими правами и полномочиями. Эти права и полномочия передаются каждому члену группы.

**Группы пользователей**

* **Администраторы. Неограниченный доступ.**
* **Операторы архива. Члены данной группы имеют права создания резервной копии даже тех объектов, к которым не имеют доступа.**
* **Опытные пользователи. Толку от них немного, так как группа включена только для совместимости с предыдущими версиями**
* **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. Члены данной группы могут выполнять криптографические операции.**
* **Читатели журнала событий. Думаю объяснять нету смысла, все предельно ясно.**

**возможности API управления пользователями и группами**

**1. Имя текущего пользователя**

****

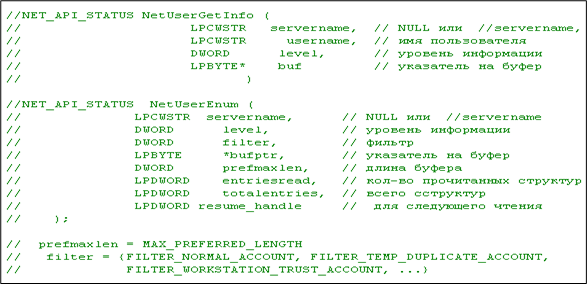
**2. Информация о пользователей**

****

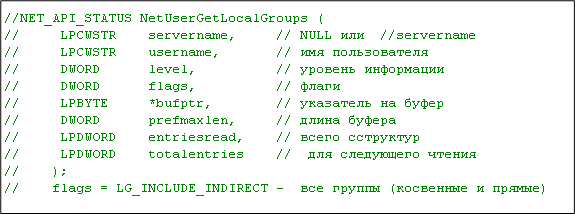
**3. Освободить память**

****

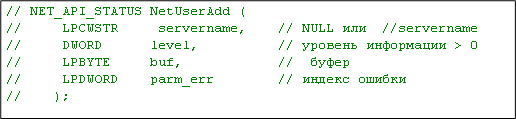
**4. Получить коллекцию пользователей**

****

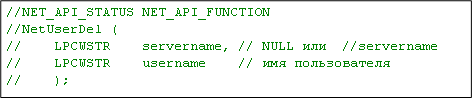
**5. Группы пользователя**

****

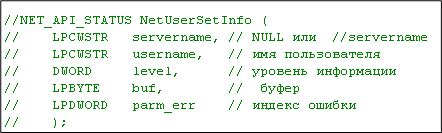
**6. Добавить пользователя**

****

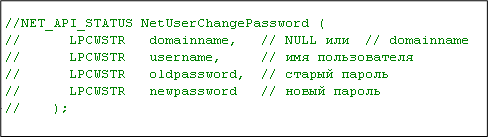
**7. Удалить пользователя**

****

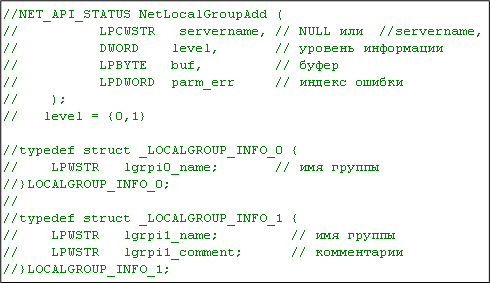
**8. Изменить информацию о пользователе**

****

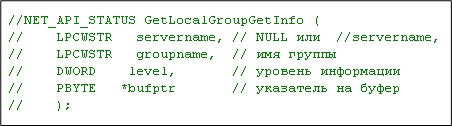
**9. Изменить пароль**

****

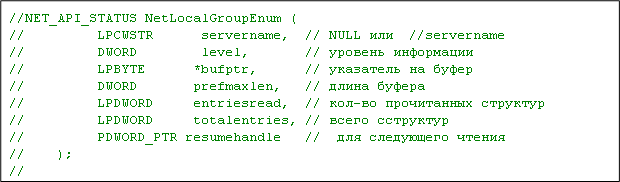
**10. Добавление группы**

****

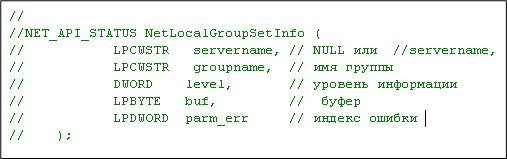
**11. Получить информацию о группе**

****

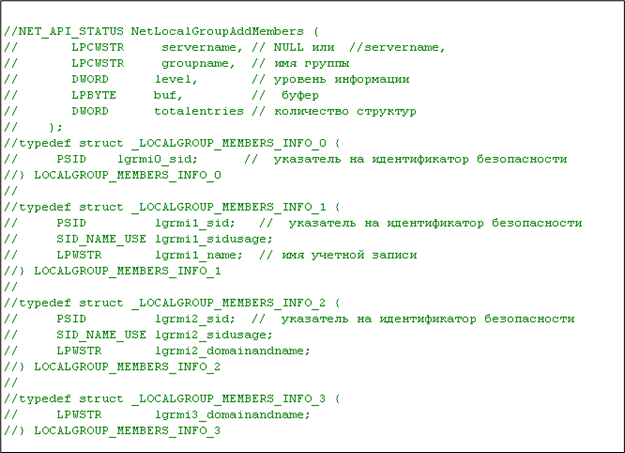
**12. Получить коллекцию групп**

****

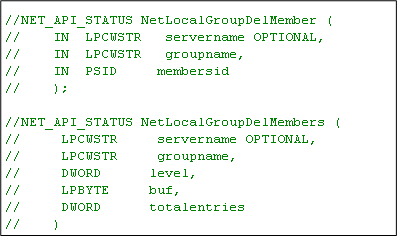
**13. Изменить информацию о группе**

****

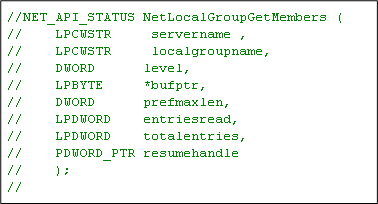
**14. Добавление членов локальной группы (исп. INFO\_3)**

****

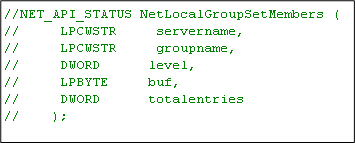
**15. Удаление членов группы**

****

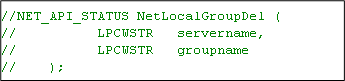
**16. Получить коллекцию членов группы**

****

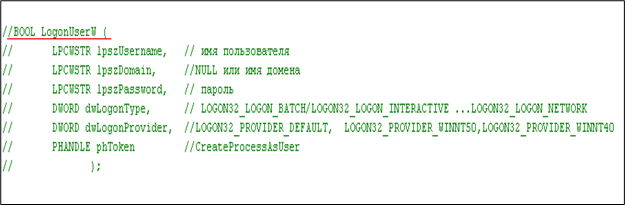
**17. Установка членов локальной группы**

****

**18. Удалить группу**

****

**19. Подключение пользователя**

****