

## Лабораторная работа №2

### Пользователи. Безопасность файловой системы ОС Windows

#### 1. Пользователи и группы пользователей

Для управления группами пользователей и более детального управления пользователями в ОС Windows XP следует воспользоваться оснасткой «**Локальные пользователи и группы**» консоли управления (mmc). Для запуска консоли управления необходимо выполнить: «**Пуск -> Панель управления -> Администрирование -> Управление компьютером**». В появившемся окне необходимо выбрать «**Локальные пользователи и группы**». Доступ к этой оснастке также можно получить, набрав в командной строке `lusrmgr.msc`.

Чтобы добавить учетную запись нового пользователя, щелкните правой кнопкой мыши на папке Пользователи и выберите из выпадающего меню команду «**Новый пользователь...**». В открывшемся окне введите данные для создания новой учетной записи. Чтобы удалить учетную запись пользователя, щелкните правой кнопкой мыши на названии учетной записи в правом окне программы и выберите из выпадающего меню «Удалить».

Для каждого пользователя можно отключить срок действия пароля, запретить смену пароля пользователем, отключить учетную запись, а также назначить путь к профилю и сценарий входа в систему.

Для того, чтобы добавить учетную запись пользователя в ту или иную группу, щелкните правой кнопкой мыши на названии группы и из выпадающего меню выберите «**Добавить в группу**». В появившемся окне нажмите кнопку «**Добавить...**», в открывшемся диалоге – введите или выберите имя пользователя.

Работа с учетными записями также может осуществляться с помощью системной утилиты `net user`:

```
NET USER [имя_пользователя [пароль | *] [параметры]] [/DOMAIN]
        имя_пользователя {пароль | *} /ADD [параметры] [/DOMAIN]
        имя_пользователя [/DELETE] [/DOMAIN]
```

`NET USER` - эта команда создает и изменяет учетные записи пользователей на компьютере. Если используется без параметров, то выводит список учетных записей пользователей для данного компьютера. Информация об учетных записях пользователей хранится в базе данных учетных записей.

`Имя_пользователя` - задает имя пользователя, которое необходимо добавить, удалить, изменить или вывести на экран. Длина имени пользователя не должна превосходить 20 знаков.

`пароль` - Назначает или изменяет пароль для учетной записи пользователя. Пароль должен отвечать установленным требованиям на длину - быть не короче, чем значение, установленное параметром `/MINPWLEN` в команде `NET ACCOUNTS`, и в то же время не длиннее 14 знаков.

`*` - Вызывает открытие специальной строки ввода пароля. Пароль не выводится на экран во время его ввода в этой строке.

`/ADD` - Добавляет учетную запись пользователя в базу данных учетных записей.

`/DELETE` - Удаляет учетную запись пользователя из базы данных учетных записей.

Допустимыми являются следующие параметры:

1. /ACTIVE:{YES | NO} - Активизирует учетную запись или делает ее не активной. Если учетная запись не активна, пользователь не может получить доступ к серверу. По умолчанию используется значение YES (т.е. учетная запись активна).
2. /COMMENT:"текст" - Добавляет описательный комментарий об учетной записи (длиной не более 48 знаков). Текст должен быть заключен в кавычки.
3. /COUNTRYCODE:nnn - Использует кодовую страницу нужного языка для вывода справки и сообщений об ошибках. Значение 0 означает выбор кодовой страницы по умолчанию.
4. /EXPIRES:{дата | NEVER} - Устанавливает дату истечения срока действия учетной записи. Если используется значение NEVER, то время действия учетной записи не имеет ограничений срока действия. Дата истечения срока действия задается в формате дд/мм/гг или мм/дд/гг, в зависимости от того, какая кодовая страница используется. Месяц может быть указан цифрами, названием месяца или трехбуквенным его сокращением. В качестве разделителя полей должен использоваться знак косой черты (/).
5. /FULLNAME:"имя" - Указывает настоящее имя пользователя (а не кодовое имя, заданное параметром имя\_пользователя). Настоящее имя следует заключить в кавычки.
6. /HOMEDIR:путь - Указывает путь к домашнему каталогу пользователя. Этот каталог должен существовать.
7. /PASSWORDCHG:{YES | NO} - Определяет, может ли пользователь изменять свой пароль. По умолчанию используется значение YES (т.е. изменение пароля разрешено).
8. /PASSWORDREQ:{YES | NO} - Определяет, является ли указание пароля обязательным. По умолчанию используется значение YES (т.е. пароль обязателен).
9. /PROFILEPATH[:путь] - Устанавливает путь к профилю пользователя.
10. /SCRIPTPATH:путь - Устанавливает расположение пользовательского сценария для входа в систему.
11. /TIMES:{промежуток | ALL} - Устанавливает промежуток времени, во время которого пользователю разрешен вход в систему. Этот параметр задается в следующем формате:  
день[-день][,день[-день]],время[-время][,время[-время]]  
Время указывается с точностью до одного часа. Дни являются днями недели и могут указываться как в полном, так и в сокращенном виде. Время можно указывать в 12- и 24-часовом формате. Если используется 12-часовой формат, то можно использовать am, pm, a.m. или p.m. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Разделителем полей указания дней недели и времени является запятая, разделителем при использовании нескольких частей является точка с запятой.
12. /USERCOMMENT:"текст" - Позволяет администратору добавлять или изменять текст комментария к учетной записи.

Кроме учетных записей, создаваемых администратором системы, после установки системы в ней присутствуют встроенные учетные записи:

1. Администратор
2. Гость
3. HelpAssistant - удаленный помощник.
4. Support\_388945a0 - используется для удаленной помощи и поддержки производителей.

Также существует утилита, позволяющая получить информацию о пользователях вошедших в систему PsLoggedOn:

psloggedon.exe [-l] [-d domain] [-x] [\\computername] или psloggedon.exe [username]

- l - показать только локальных пользователей.
- d - показать только пользователей домена domain.
- x - не показывать время входа в систему.

## 2. Идентификаторы безопасности

В ОС Windows вводится общее понятие «участник безопасности», как некоторый специальный объект. К участникам безопасности относятся пользователи, группы пользователей, компьютеры и службы идентификации объектов в системе. Каждому участнику безопасности присваивается идентификатор безопасности SID (Security Identifier). SID имеет следующую структуру: S-R-X-Y-Y-...-Y-RID. S – это символ означающий, что SID выписывается в строковом виде (на самом деле это некоторая структура языка Си), R – версия SID (на сегодняшний день существует только одна первая версия), X – идентификатор учетных данных, принимающий значение от 0 до 5, и определяющий уровень службы, выдавшей SID, Y-Y-...-Y – идентификатор домена, RID – относительный идентификатор пользователя. SID пользователя или группы может быть получен с помощью следующих утилит:

1. `whoami /user /SID` – выводит SID текущего пользователя,
2. `psgetsid <имя>` - возвращает SID по имени,
3. `psgetsid <SID>` - возвращает имя по SID,

## 3. Маркер доступа

Когда участник безопасности начинает работу в системе ему выдается маркер доступа AT (Access Token), который содержит всю основную информацию, необходимую для обеспечения безопасности системы. Разрешение на доступ участника безопасности к объектам системы принимается на основе сравнения маркера доступа с параметрами безопасности объекта.

Маркер доступа текущего пользователя может быть получен с помощью утилиты `whoami`:

```
whoami /user /all
```

## 4. Информация о файловой системе

Существует ряд утилит позволяющих собрать информацию о файловой системе используемой на рабочей станции.

1. `DiskExt` - утилита возвращающая список и расположение логических дисков на компьютере.
  2. `NTFSInfo` - утилита возвращающая информацию о файловой системе NTFS, расположенной на логическом томе.
  3. `Handle` - утилита, возвращающая список открытых файлов.
- Список параметров данных утилит можно получить вызвав их с ключом `/help`.

## 5. Разрешения на доступ к объектам

Для каждого объекта операционной системы создается список контроля доступа DACL, содержащий записи об объектах безопасности и действиях над объектом, разрешенных им. DACL доступен через графический интерфейс. Редактирование DACL доступно только владельцу объекта, либо тем пользователям, которым владелец выдаст это право. Чтобы узнать или отредактировать список контроля доступа необходимо на объекте щелкнуть правой кнопкой мыши, выбрать **Свойства** и зайти на закладку **Безопасность**. В открывшемся окне будет доступен список пользователей с разрешением

на доступ к данному объекту. Чтобы добавить пользователя необходимо нажать на кнопку **Добавить** и вписать имя пользователя в открывшемся окне.

Управление списками контроля доступа возможно также и с помощью системной утилиты `cacls`:

`CACLS <имя_Файла> [/T] [/E] [/C] [/G имя:доступ] [/R имя [...]] [/P имя:доступ [...]] [/D имя [...]]`

<имя\_Файла> - Вывод таблиц управления доступом.

/T - Замена таблиц управления доступом для указанных файлов в текущем каталоге и всех подкаталогах.

/E - Изменение таблицы управления доступом вместо ее замены.

/C - Продолжение при ошибках отказа в доступе.

/G имя:доступ - Определение разрешений для указанных пользователей.

Возможны четыре типа доступа:

R – Чтение, W – Запись, C - Изменение (запись), F - Полный доступ

/R имя - Отзыв разрешений для пользователя (только вместе с /E).

/P имя:доступ - Замена разрешений для указанного пользователя. Кроме перечисленных выше четырех видов доступа возможен пятый тип: N – Отсутствие доступа.

/D имя - Запрет на доступ для указанного пользователя.

## 6. Шифрованная файловая система

Шифрование данных — это способ обеспечения дополнительной безопасности. Шифрование представляет собой процесс преобразования данных в непонятный код. После того как данные зашифрованы, для их расшифровки необходим пароль или ключ. Незашифрованные данные называются открытым текстом (plain text), а зашифрованные — зашифрованным или шифрованным текстом (cipher text).

EFS (Encrypting File System — Файловая система с шифрованием) – это технология Windows XP, которая используется для хранения зашифрованных файлов в разделах NTFS. Шифрование файлов добавляет еще один уровень безопасности файловой системы. Пользователь, обладающий нужным ключом, может работать с зашифрованными файлами, как если бы шифрование не использовалось. Пользователь, не имеющий нужного ключа, не сможет получить доступ к информации. Предусмотрен агент восстановления, который может использоваться администратором в случае, если владелец не может предоставить ключ, необходимый расшифровки файлов или папок.

Для применения EFS пользователь указывает, что папка или файл в разделе NTFS должна быть зашифрована. Шифрование незаметно для пользователя, который имеет доступ к файлу. В то же время пользователь, не имеющий прав доступа к файлу, не сможет выполнить дешифрование, даже если этот пользователь имеет полный набор полномочий NTFS. Он все равно получит сообщение об ошибке и не увидит содержимое файла.

Чтобы зашифровать папку или файл с помощью графического интерфейса, необходимо нажать правую кнопку мыши и выбрать свойства. В открывшемся окне на вкладке **Общие** нажмите кнопку **Другие** и выберите пункт «Шифровать содержимое для защиты данных». Следует помнить, что при шифровании папки шифруются только файлы в ней, список же файлов остается открытым. В графическом интерфейсе Windows шифрованные файлы подсвечиваются зеленым цветом.

Шифрование и расшифрование файлов можно производить также используя системную утилиту `cipher`:

`CIPHER [/параметр команды] [имя файла]`

/e - Указывает, что файлы и папки следует зашифровать

/d - Указывает, что файлы и папки следует расшифровать

/s:dir - Указывает, что выбранную операцию (шифрование или дешифрование следует выполнить также для вложенных папок.

/I - Игнорирует любые ошибки, возникшие в процессе. По умолчанию у CIPHER завершает работу при возникновении ошибок.

/f - Принудительное шифрование или дешифрование файлов и папок независимо от их текущего состояния. Обычно файлы, уже находя в требуемом состоянии, пропускаются.

/q - Запуск в режиме минимальной информации, с выводом только важнейших сведений.

Запуск утилиты без параметров вводит список файлов текущей директории, с указанием зашифрованы они или нет.

## Задания к лабораторной работе:

**Задание 1.** С помощью оснастки `lusrmgr.msc` выполните следующие действия:

1. Создайте группу NAUTILIUS
2. Создайте учетную запись NEMO в группе NAUTILIUS
3. Для учетной записи NEMO явным образом пропишите путь к профилю (папку для профиля выберите самостоятельно)

**Задание 2.** Напишите пакетный файл `2.bat`, выполняющий следующие действия:

1. Создает учетную запись INDIA с обязательной явной установкой всех параметров команды `net user`.
2. Выводит список всех учетных записей, зарегистрированных в системе.
3. Выводит список пользователей вошедших в систему.

**Задание 2.** Используя утилиты, напишите пакетный файл `3.bat`, записывающий следующую информацию в файл `user.txt`:

1. SID текущего пользователя (администратора)
2. SID пользователя NEMO
3. SID группы NAUTILIUS
4. Имя участника безопасности с SID: S -1-1-0

**Задание 3.** Запишите в файл `token.txt` значения полей маркера доступа текущего пользователя. Из анализа маркера доступа определите, в какие группы входит данный пользователь и SID этих групп.

**Задание 4.** Создайте пакетный файл `4.bat`, записывающий в файл `fs.txt` следующую информацию о файловой системе:

1. Список и расположение логических дисков на компьютере.
2. Информацию о файловой системе NTFS, расположенной на логическом томе C:\.
3. Список открытых файлов.

**Задание 5.** Создайте на диске C:\ файл `1.txt` и с помощью графического интерфейса выдайте разрешение пользователю NEMO на доступ только для чтения данного файла. Также установите аудит всех действий пользователей из группы NAUTILIUS на любой доступ к данному файлу.

**Задание 6.** Реализуйте файл пакетной обработки `6.bat` выполняющий следующие действия:

1. Выводит список контроля доступом для файла `1.txt`
2. Выдает пользователю NEMO право на запись в файл `1.txt`.
3. Выдает группе NAUTILIUS полный доступ к файлу `1.txt`.

**Задание 7.** Создайте на диске C:\ файл `cpf.txt`. Используя графический интерфейс зашифруйте его. Напишите файл пакетной обработки `7.bat` выполняющий следующие действия:

1. Выводит список файлов в корневом каталоге диска C:\ с указанием зашифрованных файлов.
2. Расшифровывает файл `cpf.txt`.